Cyberspace Governance: The Imperative for National and Economic Security

Technical Report · December 2015

DOI: 10.13140/RG.2.1.2407.8321

1 author:

Eman Dandaura
Nasarawa State University
21 PUBLICATIONS **68** CITATIONS

SEE PROFILE

INTERNATIONAL CONFERENCE ON CYBERSPACE GOVERNANCE:

The Imperative For National & Economic Security

4TH -7TH November 2015
@ Shehu Musa Yar'dua Centre, Abuja

PROCEEDINGS

TABLE OF CONTENT

A Critical Assessment of Nigeria's Presence on the Cyberspace

U. M. Mbanaso,
Centre for Cyberspace Studies
Nasarawa State University, Keffi, Nigeria
uche.magnus@mbanaso.org

G. A. Chukwudebe & E. E. Atimati
Dept. of Electrical & Electronic Engineering,
Federal University of Technology Owerri, Nigeria
gachukwudebe@futo.edu.ng, inomen@gmail.com

***Abstract*—This paper presents a study of the Nigerian Presence in Cyberspace. The Cyberspace (Internet) is now critical to every nation's socio-economic, cultural and political activities. When it is disrupted or fails, can grind a nation to standstill. On the contrary, its correct functioning and pliability is transforming modern society with exceptional pecuniary and social benefits. With nearly all traditional activities increasingly moving to the Internet, Cyberspace has become a new stage for innovations, enterprises, social networking, criminality and war. For this study, the United Nations (UN) e-governance framework was used, the highlights of the United Nations E-Government Survey report of 2014 was analyzed to show the ranking of the world leaders, West African countries and where Nigeria stands. The Internet penetration growth and evolving Internet infrastructure provisioning in Nigeria were reviewed and a critical assessment of Nigerian presence on the Cyberspace was carried out using The UN online presence index methodology between the months of August and September 2015. The web content, interactivity, the currency of information, downloadable documents, etc. were used to compare various sectors of the Nigerian economy: all tiers of government, academia, and the organized private sector. The study revealed that organized private sector and private educational institutions are doing better than government educational institutions and ministries. Based on international best practices, a list of recommended actions for increasing cyberspace presence and achieving e-governance for improved services and productivity in Nigeria and similar developing countries is proffered.**

***Keywords*—Cyberspace; Nigeria, information economy; e-governance; cyber innovations, cybercrime; on-line Presence; and Internet presence.**

I. INTRODUCTION

Cyberspace is rapidly becoming an indispensable domain for individuals, businesses and governments worldwide. It is a platform that already underpins many economies of the world in the provisioning of critical services such as governance, financial transactions, the supply of electricity, water, delivery of goods and services in almost all sectors. This interactive world of interdependent digital networksthat are broadly used to control, process, share, collaborate and communicate information is now a vital infrastructure of the 21st century that its disruption or failure can grind a country to a halt.

Prior to 1992, access to basic telecoms services and Internet in Nigeria was a big issue until the establishment of Nigerian Communications Commission (NCC) [1]. NCC's policy and institutional reforms for the liberalization of the telecoms sector, to a greater extent influenced Internet growth and penetration rate in Nigeria. Since end of 1990s, Nigeria Internet penetration has been growing rapidly with the heavy importation of VSAT technology across the country and popularization of Internet cafés. By the beginning of 2000s, three international submarine cables namely SAT3, GLO1 and MainOne exposed Nigerian cyberspace to the global interconnectivity. Subsequently, the GSM's entrance into the country, contributed to the explosion of Internet access with the roll out of 3G mobile technology. Presently, Mobile Internet bandwidth accounts to about 55% of Internet connectivity in Nigeria.

Just like in other parts of the world, many people in sub-Saharan African have access to the Internet through mobile networks using laptops, tablets and other smart devices. Live statistic on October 3, 2015, has it that Nigeria has over 80 million Internet users out of world average of over 3 billon users. Consistently, Nigeria has maintained its lead in the growth of the number of Internet users in Africa, although as the adoption of Cyberspace as the mainstream of human enterprise is increasing, cyber-criminality is also increasing at a fast pace worldwide.

This paper examines Nigeria's presence on the Cyberspace, gauging its visibility in terms of emerging modern society that is digitally driven, its preparedness in the face of growing conspiracy and conflicts. The United Nations' 4- stage model framework for benchmarking the various stages in evolution of e-government services of countries is utilized to investigate the Web presence of various tiers of Nigerian government, ministries as well as tertiary institutions and the organized private sector [2]. The highlights of the United Nations 2014 e-government survey of its 193 countries was analyzed and top ranking countries worldwide presented. Based on international best practices, a list of imperative actions is proffered for improving Cyberspace presence of Nigeria and other sub-Saharan African countries; so as toachieve security and economic sustainability.

II. LITERATURE REVIEW- CYBERSPACE AND ECONOMIC SUSTAINABILITY

A. *Internet Infrastructure Provisioning in Nigeria*

Indisputably, the economic growth of many countries today is dependent upon Internet Infrastructure Capacity (IIC), implying that the provision of affordable Internet bandwidth to citizenry is vital to inclusive cyberspace growth underpinning the much touted knowledge-based economy. Conversely, the International Telecommunication Union (ITU) report, identified broadband capacity as a key propeller of Cyberspace and determinant of any nation's competitiveness in this information age [3]. Internet infrastructure in Nigeria kicked off in ad-hoc manner without at first, any clear direction. This was so because the Nigerian Telecommunication (NITEL), a government owned and the only voice-carrier in the 1990s was under crisis. This prompted unplanned introduction of pockets of Internet access through dial-ups and VSAT at inception. Arguably, the failure of NITEL to have provided national leadership and direction at inception is attributable to poor Internet infrastructure provisioning in the country, which has continuously posed challenges till date.

However, towards the end of 1990s, Nigeria Internet penetration began to grow with heavy importation of VSAT technology across the country, and popularized by Internet cafés. In the beginning of 2000s, three international submarine cables namely SAT3, GLO1 and MainOne exposed Nigerian Cyberspace to the global interconnectivity. Although, lack of metropolitan optical fibre networks across the country at inception was inimical to low take off of Internet accessibility in many parts of the country. Subsequently, GSM entrance into the country, though mainly voice carrier at that time contributed to the explosion of Internet access with the introduction of 3G mobile network. Presently, Mobile Internet bandwidth accounts to about 55% of Internet connectivity in Nigeria.In a recent study conducted by Ericsson[4] on consumer expectations, revealed that 84% of mobile phones have access to the Internet through mobile networks. Equally, laptops, tablets and other smart devices use mobile broadband to gain access to the Internet.

The establishment of Nigerian Communications Commission (NCC) in 1992 somehow ushered in a new era of leadership impetus in the country with respect to telecoms industry [1]. This brought about policy and institutional reforms with the liberalization of the telecoms sector, which to a greater extent has influenced Internet growth and penetration rate in Nigeria. Ever since its inception, NCC has championed the provision of affordable and reliable broadband access with some degree of success.

The roll out of five-year National Broadband Plan (NBP) by NCC in 2013to accelerate not only affordable Internet access, but equally, fast, reliable, available and ubiquitous Internet connectivity to every nook and cranny, have set a paradigm shift in terms of policy, regulation and compliance. The NBP made provision among others to sell seven metropolitan infrastructural backbone nicknamed "infraCo" to seven companies to provide high speed broadband infrastructure on the basis of geo-political zones in Nigeria. So far, Lagos and North Central have been awarded, with five others to follow [1][5]. Conversely, it is instructive that World Bank Report [6], in recognition of critical importance of Internet accessibility, identified broadband capacity as a key propeller of economic prosperity and determinant of a nation's competitiveness in this information age.

For Nigeria, NCC is simply a regulator, the private sector driven telecoms industry is a significant player in the provision of universal broadband access. Consequently, various stakeholders have called for need for the government and telecoms industry to work together in order to achieve the objectives and goals of NBP.

Like power, telecoms industry is a critical infrastructure that all other critical sectors rely upon. But the telecoms industry is worried about the multifaceted challenges it faces. The industry is worried about the protection of the sector against willful destructions, thefts, as well as multiple taxations imposed by certain elements of the government and communities [7][8]. The protection of telecoms infrastructure is critical in the life of any nation, more so a developing nations.

B. *Internet Penetration Growth in Nigeria*

With 177,155,754 populations, as at December 31, 2013, Nigeria had 67,319,186 Internet users, against 1,125,721,038 African populations with 297,885,898 Internet Users. This represents 38.0% of Nigerians having access to the Internet, which is about 22.6% of Internet users in Africa. Table I shows growth pattern of Internet penetration in Nigeria, indicating astronomical growth of 143% in Internet usage for the period. Consistently, Nigeria has maintained its lead in the growth of the number of Internet users in Africa. Conversely, Nigeria, which had same number of Internet users (55 million) like the United Kingdom in 2012, witnessed 14% leap in one year in contrast to the UK, which showed a marginal increase of two million users in 2013 (from 55 to 57 million). It infers that the adoption of Cyberspace as the mainstream of human enterprise in Nigeria will increase productivity and economic growth.

TABLE 1: INTERNET PENETRATION GROWTH IN NIGERIA [3].

Year	Number of Internet Users	Population Estimates	Percentage (%) of the population
2000	200,000	142,895,600	0.1 %
2006	5,000,000	159,404,137	3.1 %
2009	23,982,200	149,229,090	16.1 %
2011	45,039,711	155,215,573	26.5 %
2013	67,319,186	177,155,754	38%
2014	70,101,452	178,516,904	45%

C. *Conflicts and Conspiracy Worldwide and the Nigerian Cyberspace*

As the number of users is increasing so are the criminals. It is no longer headlines that the Cyberspace is challenged continually by vulnerabilities, threats and risks.Unlike in the past fifteen years; cyber conflicts are no longer strange or bewildering. With the spate of one state orchestrated attackagainst another nation's cyber infrastructure, a relatively new phenomenon - cyber warfare now in human lexicon can scarcely be disputed. State actors are unfulfilled with erecting defensive barriers alone but working painlessly to build offensive capabilities that can assault their rivals in a slightest provocation. Intensifying this challenge is that no one whether an individual, organization or government can boast of exact profile of the evolving threats and vulnerabilities springing thereof [9]. There is a hard evidence that most advanced countries including USA, UK, Russia, China, among others are developing 'Cyber Command' in anticipation of eventual major cyber conflicts as argued in [10].

Cyber criminality is a well-established trend, as Nigerian Cyberspace is constantly under pressure by malicious activities, especially those targeted to the financial sector and unsuspecting users. The Central Bank of Nigeria (CBN), asserted that in 2007 alone, the financial industry lost N7.3 Billion to cybercrime[11]. From global perspective, Nigerian Cyberspace is a conduit for growing cyber-criminality where cybercrimes are flourishing [12].

The common mischievous criminality is the unleashing of Phishing attacks on Nigerians to steal their sensitive digital information, and subsequently use the same for financial gains. The philosophy behind phishing is the exploitation of psychology of human weakness (or social engineering) to obtain sensitive information such as usernames, passwords, and bank card details by posing as a trustworthy entity in digital interactions. This is largely manifested as emails directing victims to rogue websites, demanding personal sensitive information, and sometime with threats of blocking victim's account on failing to adhere to their request. Lately, this type of criminality has extended to social media such as Facebook, Twitter, Myspace, LinkedIn etc.

Another prevailing crime is the touted email scam (alias 419), which leverages SPAM techniques to solicit for shared financial gains with little or no investment, usually, by presenting bogus projects already executed, which payments may have been deferred for one reason or another. This was said to originate from Nigeria, these criminals use all manners of tricks, still based on social engineering to con their victims to use their bank account to repatriate tied up money. In some instances, they solicit for financial help for Charity organizations that do not exit, plundering on the conscience of their victims to support a just cause. However, there is no solid evidence that this sort of crime or its equivalent has not spread worldwide or it is only emanating from Nigeria. In addition, Cyber Stalking is gaining momentum in Nigeria, which uses the power of Cyberspace technologies to repeatedly harass or threaten victims through most times email spamming.

In other developments, Nigeria has witnessed organized and coordinated hacking attacks, particularly targeted to the financial sector and government Web assets. Hacking poses significant threat to the gains of open Cyberspace, and it is done for a variety of purposes and benefits depending on the perpetrators. In Nigeria, beside attacks on the financial systems, significant breeches have been observed within government Websites, news and entertainment industry. In 2013, Sahara Reporters suffered massive distributed denial of service attacks (DDoS), of which the perpetrators and motivation remain uncovered.

Although, it is good news that number of Internet users in Nigeria is increasing, it is important to investigate the impact in terms of economic improvement. In other words what the citizens are using the Internet for; downloading music, chatting in Facebook, phishing, or studying online. One method of evaluation is to use the UN e-governance framework. This will be discussed in the following section.

D. *Benchmarking Cyberspace Presence using United Nations E-Government Framework*

The day-to-day business of government or any organization is built on information. Information is a critical resource that helps organizations to manage operations effectively[13]. With the revolutionary changes that Information and Communication Technology (ICT) is bringing to our global society, organizations and governments worldwide have embraced ICT for governance. Many countries have put in place appropriate ICT infrastructure and adopted e-governance because of its numerous benefits, namely; increased accountability and transparency, reduced cost of governance and corruption, elimination of bureaucracy, equal access to information and efficient service delivery[13].

By definition, E-Government is "the use of ICT, and particularly, the Cyberspace(Internet), as a platform for exchanging information, providing services and transacting with citizens, businesses, and other arms of government" [14]. Evidence has shown that E-government has a link with sustainable economic development; it boosts productivity in areas such as entrepreneurship, innovation, research and development, distance learning, e-health, e-agriculture, e-trade and other fields [13]. Consequently, the UN has evolved a robust e-government model for benchmarking development of its 193 member countries [15].

The United Nations E-Government Survey is produced by the United Nations Department of Economic and Social Affairs. The Survey is carried out every two years using a robust E-Government Development framework. The published e-government surveys since 2003 are available at UN website. The framework involves determination of an E-Government Development Index (EGDI); which is a composite measurement of the capacity and willingness of countries to use e-government for ICT-led development. By ranking the

performance of countries on a relative scale, the index provides a valuable input for policy making and agenda setting and a benchmarking tool for monitoring progress of countries.

The *E-Government Development Index*is calculated from the Web Measure Index (Online Presence Index), the Telecommunication Infrastructure Index and the Human Capital Index. The Web measure index is based upon the four-stage model and countries are ranked according to what they provide online [15]. The Telecommunications infrastructure index is a composite weighted average index of six primary indices based on basic infrastructural indicators, which define a country's ICT infrastructure capacity. These are: PC's/1000 persons; Internet users/1000 persons; telephone lines/1000 persons; online population; mobile phones/1000 persons; and TV's/1000 persons. While the Human capital index is calculated from the adult literacy rate and the combined primary, secondary and tertiary gross enrolment ratio [16]. A detailed description of the methodology, as well as a country-by-country assessment for each stage of online service development, is provided in the survey reports[15] [16].

The United Nations E-Government Survey report of 2012 and 2014 were studied. In 2012, Nigeria was ranked 163 out of 192 countries with EGDI of 0.268[15]. The Republic of Korea was the world leader with EGDI of (0.9283), followed by the Netherlands (0.9125), the United Kingdom (0.8960) and Denmark (0.8889), with the United States, Canada, France, Norway, Singapore and Sweden following closely behind. [14] & [15].

In the 2014 UN Report, some countries improved, however, the Republic of Korea retained its world leadership position with Australia (2nd) and Singapore (3rd) taking the second and third positions respectively. Nigeria also improved;Nigeria was ranked 141 out of 193 countries with EGDI of 0.2929.Globally, Europe was leading with the highest regional EGDI followed by the Americas led by the United States of America (ranked 7th globally); Asia led by the Republic of Korea; Oceania led by Australia; and Africa led by Tunisia (ranked 75th globally).

With an average of 0.8368, the top 25 countries are far ahead of the rest of the world (world average of 0.4721). Progress in Africa remains relatively slow and uneven. For the top 20 African countries, Nigeria ranks 19. The regional EGDI average in Africa is 0.2661. Six countries (Tunisia, Mauritius, Egypt, Seychelles, Morocco and South Africa) have EGDI values above the world average of 0.4712, placing them among the top 50 per cent of the world. On the other hand, about 30 per cent (16 countries) of the 54 African countries are at the bottom 10 per cent of the world ranking.

Forbenchmarking on-line presence of countries, the United Nations has devised a 4- stage framework Fig. 1 [13].Any country's E-Government services can evolve from Stage 1, static web site with basic information to the Stage 4 - Connected stage, where a country has web pages for all its organs properly integrated to an interactive web portal. This UN Framework and stipulated benchmarks are to encourage use of e-governance for development since the resources and capabilities of governments vary considerably. From UN's latest report, there was good progress in online service delivery in 2014 because all the 193 United Nations member States had some form of online presence, as compared to 18 countries with no online presence in 2003 and 3 countries in 2012.

Some of the developing countries have found ways to leapfrog traditional development cycles by deploying mobile technology for bridging the digital divide. They have reoriented their public sector governance systems towards user-centric approaches visible on their websites through multichannel service delivery features [13]. In order to critically asses Nigeria Cyberspace presence, an investigation ofWeb presence of both government and private enterprises was carried out. The survey methodology and results are in the following sections.

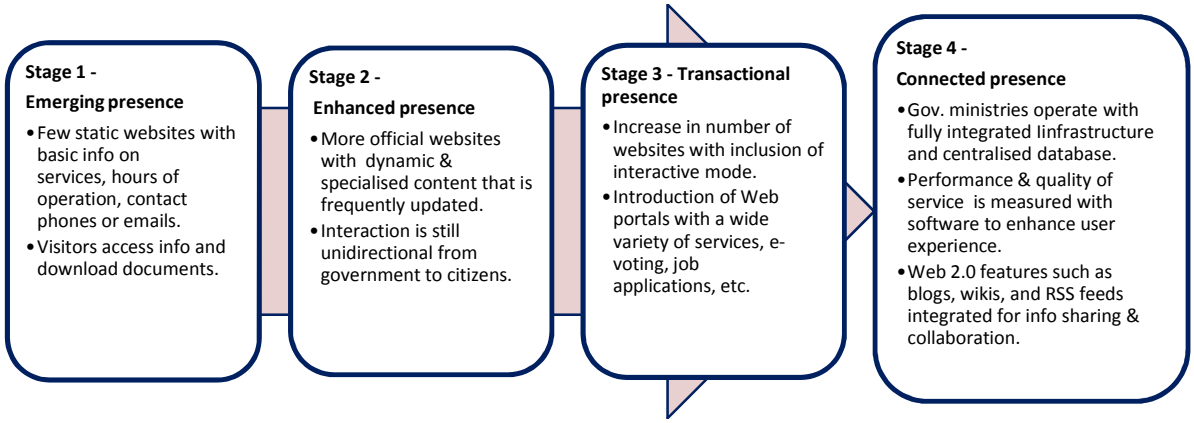


Fig. 1: E-Government 4 - Stage Framework Model for Development [13].

III. METHODOLOGY- CYBERSPACE PRESENCESURVEY OF NIGERIAN ORGANIZATIONS

In assessing Nigeria's presence on the Cyberspace a detailed survey and analysis was carried. The UN online presence index methodology as carried out in 2012 was adopted in generating an online index [2]. The survey was carried out between the months of August and September 2015. The online index was gotten by grading each website based on the following yardstick: *essential information and content of the site, currency of information, downloadable documents, newsletters, reports and databases*. The interactive nature of the site (its ability to receive feedback from clients or customers), blogs, chat forums help features, two-way communication of the site, its ability to respond to emails, and language translations were also investigated. The availability of these benchmarks was used to form an online index used to compare various websites. Sectors such as government, academia, finance, business, oil and gas and telecommunication industries were investigated.

These features were categorized into stages; Stage one: a website presence with necessary information but not frequently updated. Stage two: more recent and constantly updated websites, downloadable materials that are current. Stage three represents a website that allows for two way communication with users, where transactions can be made. Stage four is used to classify a website which is a one stop hub where access to all the necessary information is present in various languages to all users at home and abroad.

Online index values of 0 to 0.25 reveals that the website was seen to be in stage one, 0.25 to 0.5 was seen to be in stage two with few interactive but not stand alone interaction. Index rating of 0.5 to 0.75 reveals that the website was rated stage three and index of 0.75 to 1 was rated to be in stage four.

IV. RESULTS

E. National Presence

The availability of a national website was investigated and Nigeria was found not to have one as at the time of the survey. This is in contrast to a survey carried out in May 2014 were the nation had a website [13]. Other West African countries like Ghana and Senegal reviewed have a national presence on the Internet.

F. State Government

The Fig. 2 reflects the web presence of the 36 states including the FCT in Nigeria. About 36% of them were in stage three while one out of every six states is not hosted online. Most of these states with no web presence are the northern states of the country.

G. Local Government Areas (LGAs)

The survey revealed that of the 774 local government areas in the country only 28 LGAs had any form of web presence. All these local governments were found in one state, AkwaIbom. It is no surprise that as shown inFig. 2, AkwaIbomis one of the states rated amongst the best. The absence of a website for most local government areas which is the government closest to the people in the grass root is alarming.

H. Federal Ministries

The result reveals only one of the ministries is at Stage 3 while the majority is still in Stage 1 (Fig. 3). This is in total contrast to the survey carried out last year where all the ministries had an online presence [13], and this made access to government easier and available to more citizens. Out of the 30 ministries surveyed seven (23%) have no web presence.

I. Tertiary Institutions

As a result of the huge number of tertiary institutions, the results of the survey were categorized into the different levels, Universities (Federal, State and Private), Polytechnics and Colleges of Education (CoEs).

J. Universities

The survey revealed that more federal universities are partaking from the many benefits of Cyberspace with more than 97% of them being online to enable them provide easy services such as result checking, registration and payment of school fees (Fig. 4). Although, some have reached Stage 3, they are yet to be a one-stop shop hub were all that is needed from the university (information and other wise) can be gotten online, without physically going to the university.

Although most of the state universities investigated have reached up to Stage 2 with some necessary web features, about 16% of them are yet to have any form of web presence (Fig 5). It is worthy of note that most of these universities reside in the northern part of the country.

It is necessary to note that the private universities in the country have latched on to the many benefits of having a web presence. All the 46 private universities surveyed had web presence with majority of them being in Stage 2 and 28% being in Stage 3 (Fig. 6).

K. Polytechnics

The web presence of polytechnic investigated revealed that of the 44 polytechnics studied, five were not on the web (Fig. 7). It is worthy of note that most of the polytechnics 88% have a web presence and 84% of them have up to Stage 2 web presence.

Fig. 8 reveals that of the 34 colleges of education across the country surveyed only 68% of them have any form of web presence. This is very low compared to that of the universities and polytechnics. In total 153 public tertiary institutions were surveyed and (23) 15% of them had no form of web presence.

L. Secondary Schools

The secondary schools have warmed up to embracing the usefulness of Cyberspace. Out of the 24 Federal Government Colleges investigated, 62.5% of them were online with

features between Stage 1 and Stage 2. This is very encouraging when compared to the previous survey carried out in 2014 [13].

M. Businesses & Financial Sector

Microfinance banks and other commercial banks that were investigated revealed that of the 88 micro finance banks surveyed only 11 of them (12.5%) had any form of web presence. Commercial banks surveyed shows that commercial banks are all making use of the Internet to do business with their customers (Fig. 9).

The online presence of GSM companies (Moble Phone companies) in the country reveals that they are all online, and have keyed into providing excellent services to their customers via this medium (Fig. 10).

As seen from Fig. 11, the multinational oil and gas companies in the country have websites that are functioning and rated up to Stage 2. They have all bought into the many benefits of doing business online.

A few multinational companies that provide various services ranging from manufacturing to information technology services were investigated and the result of their online presence is as shown in Fig. 12. All the investigated companies and parastatals (35 of them) were seen to have web presence.

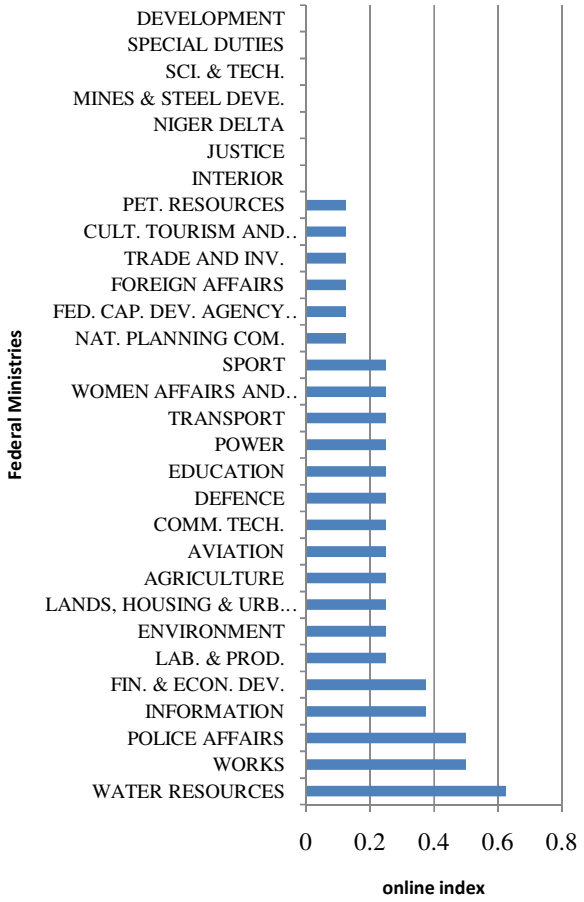


Fig 3: Online presence of Federal Ministries.

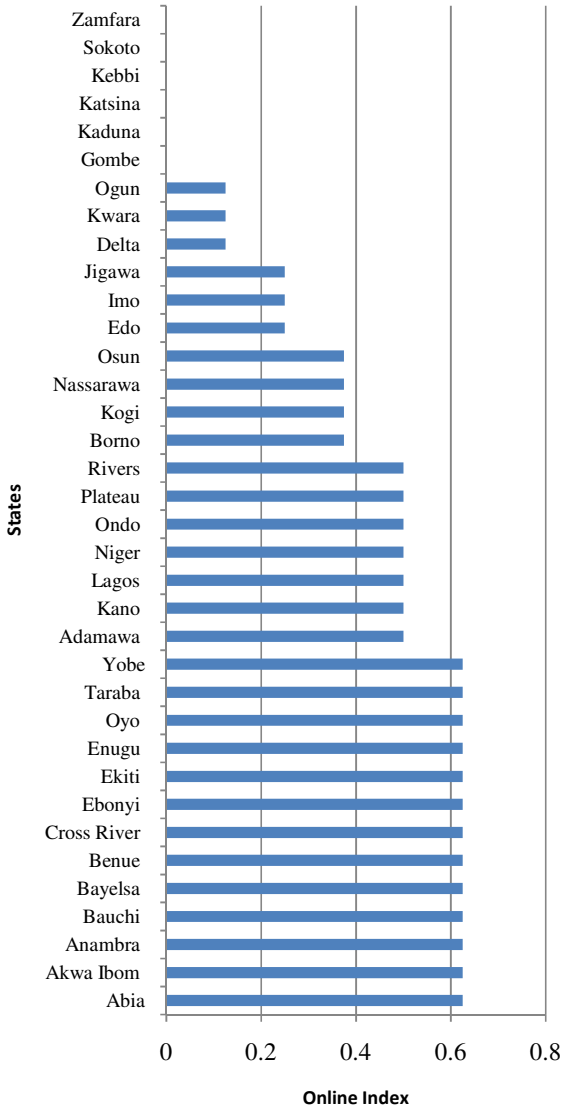


Fig. 2: Web presence of Nigeria State governments.

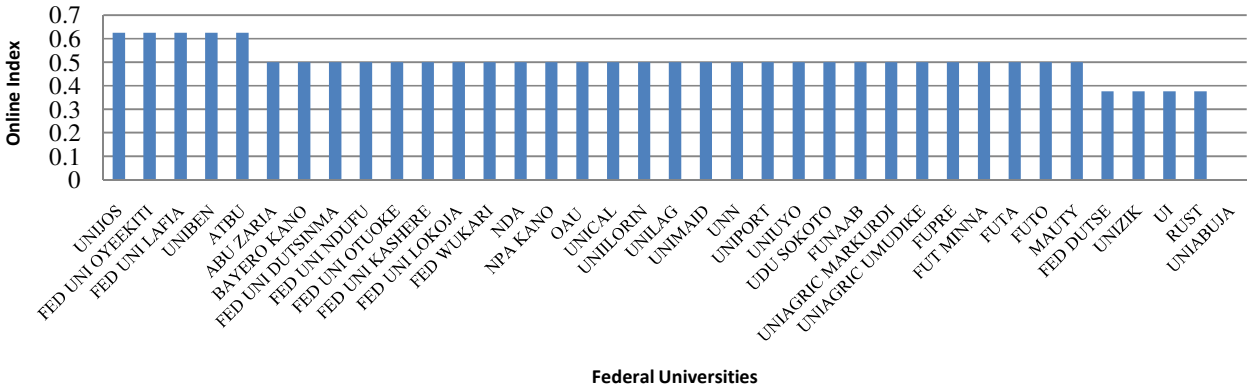


Fig 4: Online presence of Federal Universities.

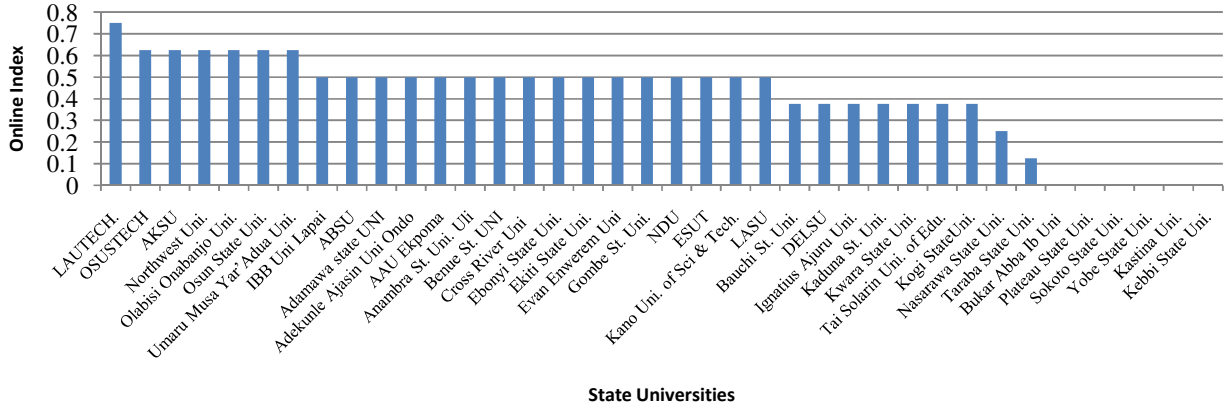


Fig 5: Web presence of State Universities.

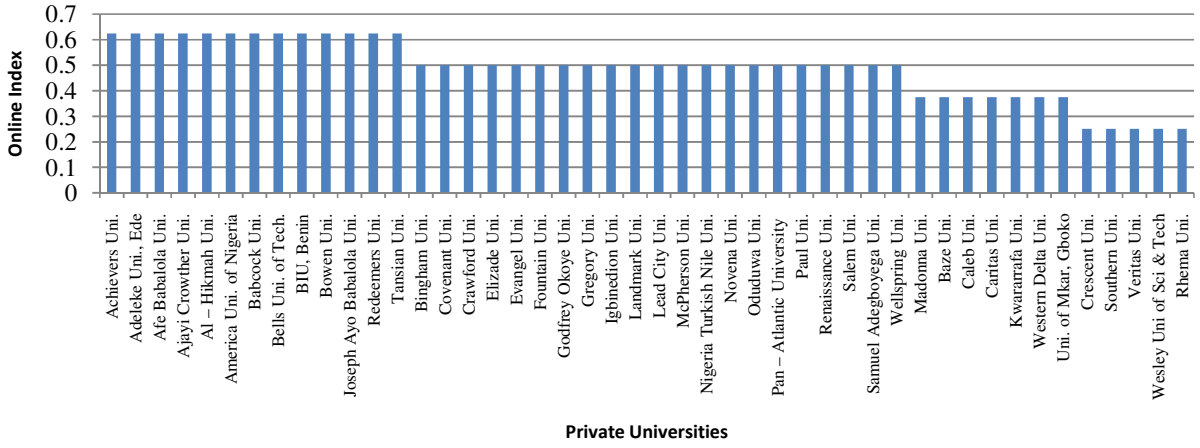


Fig 6: Online index of Private Universities.

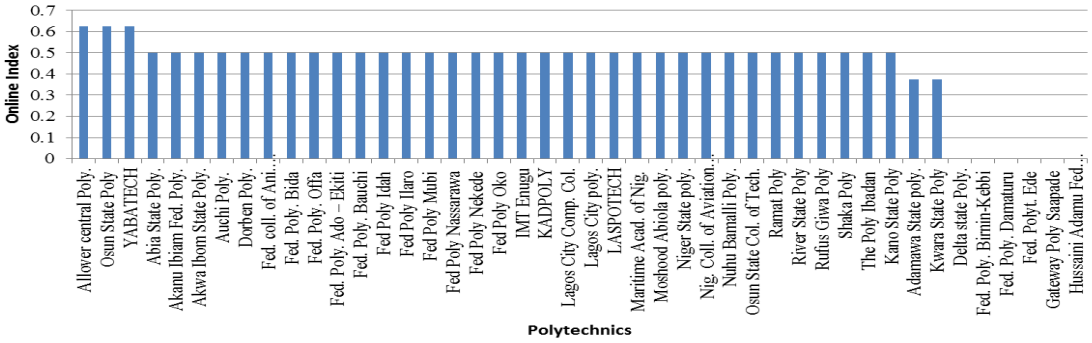


Fig 7: Online presence of Polytechnics.

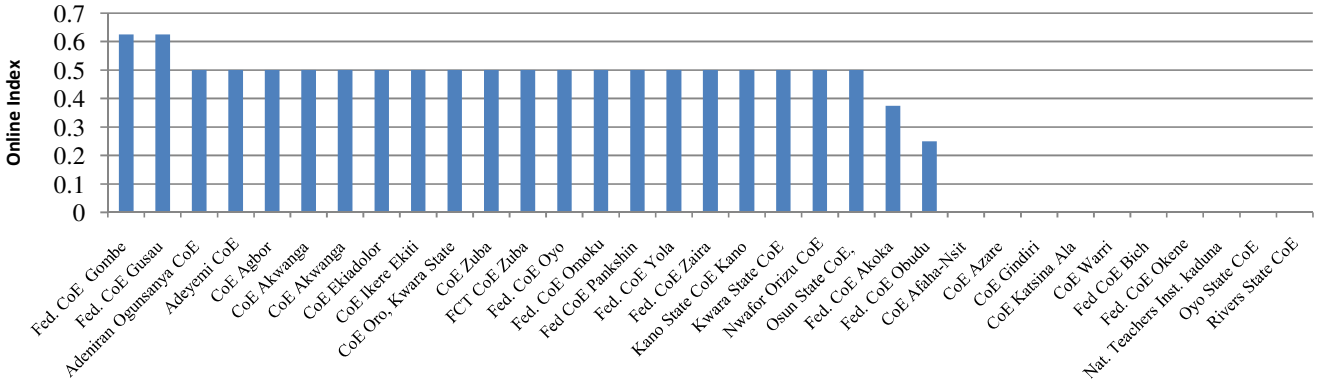


Fig. 8: Web presence index of Colleges of Education (CoE).

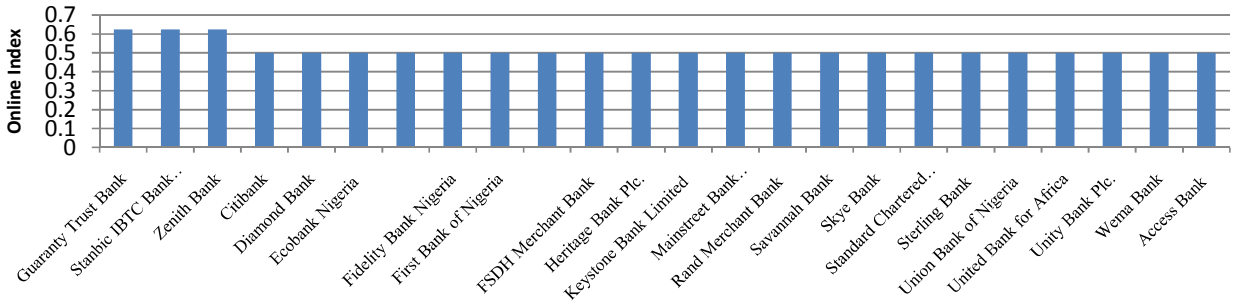


Fig. 9: Online Index of Commercial Banks.

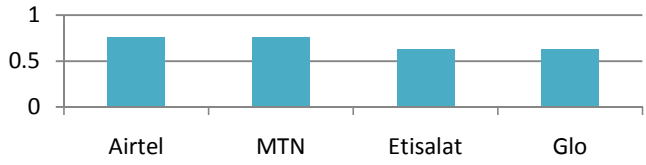


Fig 10: Telecommunication companies online presence.

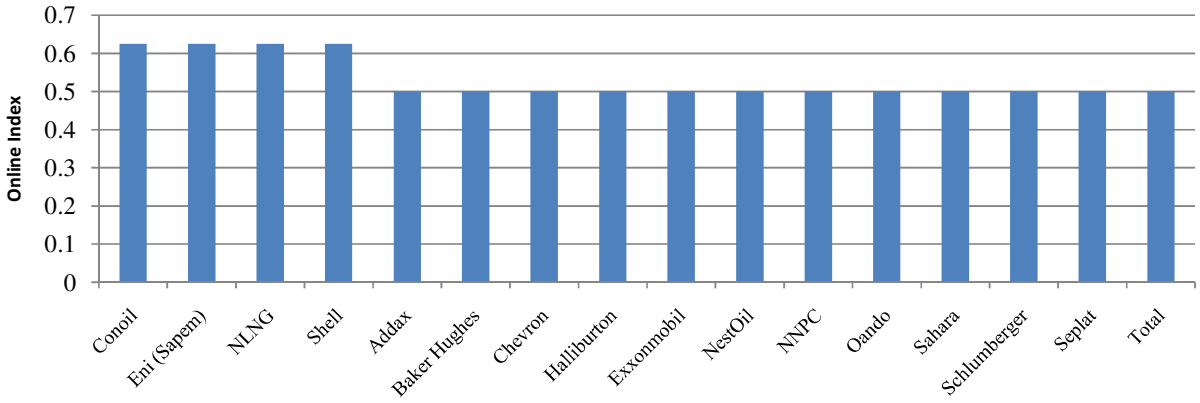


Fig 11: Oil and Gas multinationals web presence index.

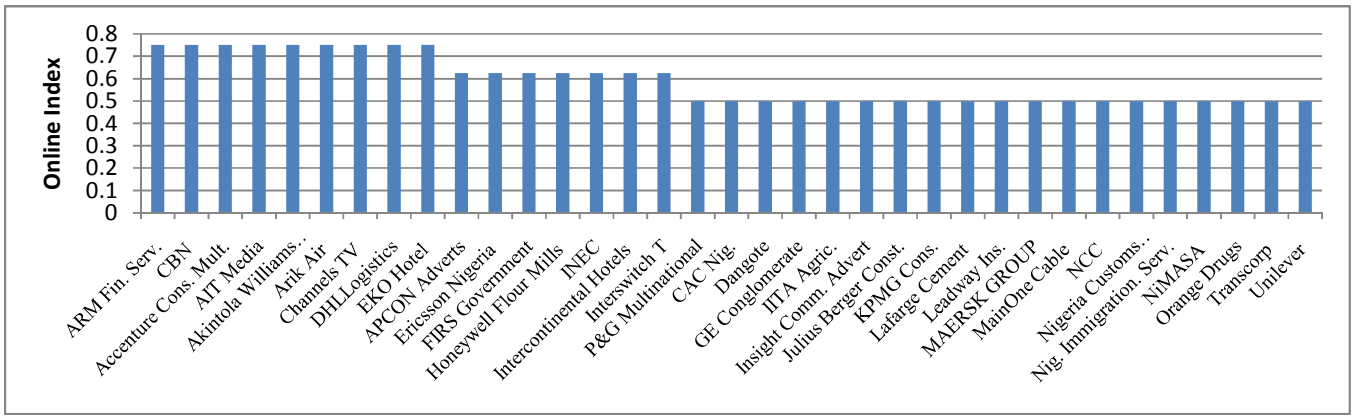


Fig 12: Online index for some Multinationals and Government Parastatals.

V. DISCUSSION

The results of the survey carried out August - September 2015 show a huge online presence of private universities, multinational companies, businesses, commercial banks, public tertiary institutions and states but very low presence for ministries, local government and microfinance banks. This reflects the huge digital divide as the latter (local government and microfinance banks) deal directly with the grass root. The LGAs have to be pulled on board, because they have key roles to play in providing grass-root information on basic items such as: numbering of houses, taxes on shops, cleaning and maintenance of roads, healthcare, primary and adult education, birth, death and marriage certificates.

The UN survey of 2014, ranked Nigeria 141 out of 193 countries, whereas 2012 ranked Nigeria 163, this is an improvement, probably due to Ministry of Communication Technology and other federal government ICT initiatives. An examination of the Nigerian National ICT Policy (2012) and the National Broadband Plan, 2013 - 2018 showed that these two documents addressed comprehensively needed requirements for use of ICT for sustainable development; all that is required is strict and honest implementation.

The future of Nigerian cyberspace is very bright because there are several application areas for e-government that will yield profit and sustainable development such as payment of taxes, import duty, government fines, feedback from masses/stakeholders, etc. The organizations (businesses) in Nigeria that adopted e-administration are reaping huge profits and delivering improved quality of service to their customers. This is evident in the survey conducted on businesses; as 100% of the manufacturing industries investigated were above Stage 2 of e-presence. The financial sector is another proof of the success of e-administration, as most banks offer e-services to their customers, have integrated their ICT infrastructure so that transaction can be done physically from any bank branch. This is in addition to integration of ATM facilities and mobile banking of various banks so that customers can withdraw from any ATM, use their smartphones, irrelevant of their bank. Thus, e-governance and ICT infrastructure has produced tremendous positive impact in banks and organized private sector.

With the increasing adoption of e-administration in the tertiary institutions, the positive impact felt in the banks can be replicated in schools in the areas of improved teaching and learning, research and development, planning and projection, accountability and administration. Dramatic life changing benefits can be quickly realized if appropriate ICT infrastructure is provided in school systems at all levels [13].

For sustainable economic development, there must be citizen feedback. From the study, Nigeria and many African countries' websites are yet to provide this feature, thus information dissemination is still one way, from government to citizens. Those in LGAs in rural areas and some towns do not even have the ICT infrastructure to access the websites.

On a positive note, presently, application forms for government/organization's use can be filled online, reducing the cost of travel and risk of life, thus some of the benefits of e-governance such as reduction in cost of governance, equality of access to information, elimination of bureaucracy, efficient service delivery, are beginning to be realized in the country.

At the time of the study, very few small and medium scale enterprises in Nigeria have websites and as such cannot be reached by the international community for e-commerce; access to ICT infrastructure can boost such businesses with greater profits and more job creation.

On cybersecurity, The Federal Government of Nigeria has since recognized the importance of cybersecurity and introduced several initiatives. In 2004, there was the Nigerian Cybercrime Working Group (NCWG), a 15-member committee, drawn from the government and private sector to look into legal and institutional framework for cybercrime in Nigeria [16]. The Committee developed the first Bill on Cybercrime and Critical Information Infrastructure Protection, which was conveyed to the National Assembly although sponsored by a private individual, but the Bill suffered a setback that was inexplicable.

In 2011, a National Committee was set up by National Security Adviser charged with the responsibility to harmonize the various Cybersecurity Bills pending at the National Assembly. The Cybersecurity 2011 Bill draft, was finally signed into law in 2015. In similar development, however, National Cybersecurity Policy and Strategy, was launched March, 2015. Additionally, some federal government institutions are confronting cyber criminality aligned with their constitutional mandates.

Equally, the Economic and Financial Crimes Commission (EFCC) established in 2003, is also fighting all sorts of digital financial crimes. EFCC works in collaboration with Financial Action Task Force on Money Laundering (FATF), an intergovernmental organization. The Independent Corruption Practices and Other Related Offences Commission (ICPC), established in 2000 has the mandate to receive and investigate reports of corrupt offences as created by the Act and in appropriate cases, prosecute the offender(s).

In the same vein, the Central Bank of Nigeria, regulating the banking industry, has set out frameworks as policy direction towards confronting the menace of digital fraud in the banking sector. The latest of such is the Biometric Verification Number (BVN), established 2014 as centralized biometric identification system for the banking industry. BVN gives a unique identity that can be verified across the Nigerian Banking sector and other financial institutions as part of Know Your Customer (KYC) program.

Whether the activities of these institutions are yielding the expected results is open to debate. Undoubtedly, use of ICT is a super game changer; recommendations to improve the present scenario are proffered in the following section.

VI. RECOMMENDATIONS

The Cyberspaceis now critical to every nation's socio-economic, cultural and political activities. When it is disrupted or fails, can grind a nation to standstill. Broadly speaking, there is a need for the Sub-Saharan African countries to have a change of attitude, provide the necessary legislation to support e-governance, provide ICT infrastructure and its supporting elements, train manpower and then restructure the interaction between government agencies. Itemized below are imperative actions for improving the Cyberspace presence of Nigeria and Sub-Saharan African countries.

i. Provision of affordable broadband infrastructure – For Nigeria, the FGN National Broadband plan is highly commendable and implementation should be given top priority. E-governance and e-business cannot be achieved with the present slow and expensive Internet access.
ii. Proper financing of ICT – The initial cost of ICT infrastructure is usually high; it must be put in the national budgets. It is also very important to budget for support and maintenance costs. The digital divide is rooted in the lack of e-infrastructure, which has hindered information-use and knowledge-creation.
iii. Appropriate staffing and establishment of ICT units in organizations - The establishment of ICT departments in all ministries and parastatals at the Federal, State and Local government levels should be made mandatory.
iv. Provision of steady power supply – Renewable power supply (solar and wind) should be used for ICT installations. Computers and networks need clean power to function optimally.
v. Cyberspace is a knowledge-based 'space' requiring the right people with the right skills in the right roles. Formal and structured capacity building must be in the national agenda. Hence, development of a relevant ICT skills framework to help build a pipeline of cyber workforce that has the capability to maintain, sustain and defend nation's Cyberspace is highly recommended. Imperatively, cyberspace growth today is a matter of people and skills.

vi. Use of Established System Development Practices - E-governance is an ICT project and many ICT projects fail because standard processes for System Development Life Cycle have not been followed. All government organs should have strategic plans and ICT Policies well aligned with organizational operations.

vii. Provision of a Secure Experience for Web Visitors - Any computer connected to the Internet is vulnerable to virus/worm infection or attack. There should be a *Centre with a phone number and email where cybercrime should be reported.*All government ICT infrastructure must be regularly conduct vulnerability and threat assessments and ensure standard compliance. This is in addition to having robust business continuity and disaster recoveryplan that is regularly tested, put in place.

viii. Regular review and update of Enabling Legislation – The level of Cybercrime is alarming and unpredictable; Cybercrime Act 2015 should be made enforceable so that law enforcement elements of government can effectively prosecute cyber offenders with proportionate punishmentaccordingly. Strict adherence and compliance of National Cybersecurity Policy and Strategy should be encouraged to ensure all government institutions migrate to e-government platform standardized. The various government tiers should adopt due process workflow and hierarchy, which should be reviewed and implemented in e-government applications.

ix. Greater interactivity with government officials. Government must increasingly begin to create channels for citizen feedback and interaction. This is in addition to placing greater emphasis on institutional linkages among the tiered government structures and acquisition of centralized databases and standards for interoperability to eliminate duplicate services.

VII. CONCLUSION

With nearly all traditional activities increasingly moving to the Internet, Cyberspace has becomethe platform for innovations, enterprises, social networking, criminality and war. Nigeria and some other West African Countries have started moving towards this direction as seen from the study. The relevant organs of government in charge of ICT and e-governance are commended for what they have achieved so far. It is vital for Nigeria and other sub-Saharan African countries to learn from global best practices and collaborate internationally to develop a harmonized framework with necessary defense against cyber-criminality and ware fare.

For Nigeria, there exists a digital divide within the country as seen from the survey conducted. The Federal Ministries and States have a Stage 2 online presence while the LGAs are yet to commence e-governance. Most tertiary institutions have established web presence while very few secondary schools have keyed in. Similarly in the business sector, most multinationals and banks are enjoying the benefits of e-business while microfinance banks are lagging behind.

Nigeria's ranking and the digital divide can be further improved and bridged respectively if the recommendations are given priority by all tiers of government. This will strengthen good governance with broad-based public participation, improve quality of life for the entire citizenry, and create more job opportunities for the youth.

REFERENCES

[1] NCC, "Nigerian Communications Commission (NCC)," [Online]. Available: http://www.ncc.gov.ng

[2] UN E-Government Survey (2012), From E-Government to Connected Governance, United Nations Department of Economic and Social Affairs/Division for Public Administration and Development Management, ST/ESA/PAD/SER.E/112, New York.[Online].

[3] International Telecomunication Unit (ITU), "Impact of Broadband on the Economy," ITU, 2012.

[4] Ericcson, "Internet Goes Mobile: Country Report Nigeria," April 2015. [Online].Available:http://www.ericsson.com/res/docs/2015/consumerlab/ericsson-consumerlab-Internet-goes-mobile-nigeria.pdf. [Accessed July 2015].

[5] E. Amaefule, "32.5 million Nigerians access Internet via telecoms networks," 12 May 2013. [Online]. Available: http://www.punchng.com/business/32-5-million-nigerians-access-Internet-via-telecoms-networks/. [Accessed May 2015].

[6] B. E. Okwuke, "Nigeria braces up for last mile broadband infrastructure," 24 February 2015. [Online]. Available: http://dailyindependentnig.com/2015/02/nigeria-braces-last-mile-broadband-infrastructure/. [Accessed 25 May

[7] Y. S. Abikoye Oluwafemi, "NIGERIA: Towards Enhancing Affordable Broadband Acces," Paradigm Initiative Nigeria, Lagos, 2015.

[8] The Broadband Commission, "The State of Broadband 2014:broadband for all," Switzerland, Geneva, 2014.

[9] U. M. Mbanaso and E. S. Dandaura, "The Cyberspace: Redefining a New World," *IOSR Journal of Computer Engineering (IOSR-JCE),* pp. 17-24, 2015.

[10] Nigerian Communications Commission (NCC), "National Broadband Plan Implementation: Juwah Exudes Optimism," The Communicator Magazine, Nigerian Communications Commission (NCC), Abuja, 2015.

[11] I. Nnadozie, "Nigeria will lose $15million to Cyber theft related cases by 2020," October 2013. [Online]. Available: http://www.thenigerianvoice.com/nvnews/126855/50/nigeria-will-lose-15million-to-cyber-theft-related.html. [Accessed May 2015].

[12] Balancing Act Africa, "Nigeria Ranked Third in the World for Cyber-Crime," [Online]. Available: http://www.balancingact-africa.com/news/en/issue-no-302/computing/nigeria-ranked-third/en#sthash.v598OgZB.dpuf.

[13] Chukwudebe G. N. and Atimati E. E. (2014), The Impact of E-Governance and ICT Infrastructure on Sustainable Economic Development. World Engineering Conference Nov. 2014. Abuja, Nigeria

[14] United Nations e-Government Survey 2008 From e-Government to Connected Governance, ST/ESA/PAD/SER.E/112 United Nations publication, 2008, New York.

[15] United Nations E-Government Survey 2014 E-Government For The Future We Want, United Nations publication, 2008, New York., http://www.unpan.org/e-government

[16] F. Oyesanya, "Review of Draft Nigerian Cybercrime Act," [Online]. Available: http://www.gamji.com/article3000/NEWS3561.htm.

The Use of Social Networking Service among Nigerian Youths between Ages 16 and 25 Years

U. M. Mbanaso[1], PhD; E.S. Dandaura[1] PhD; G.N. Ezeh[2] PhD; U.C. Iwuchukwu[2]
[1] *Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nasarawa State, Nigeria*
[2] *Electrical & Electronic Engineering Department, Federal University of Technology, Owerri, Imo State, Nigeria*
uche.magnus@mbanaso.org, dandaura@gmail.com, ugoezeh2002@yahoo.com, uchechi.iwuchukwu@futo.edu.ng

Abstract - **This paper presents an investigation of the use of social networking service among youths aged 16 through 25 years, in Nigeria. The convergence of information systems and networks, the internet and mobility has brought about a fundamental shift on how people generate and share information. Specifically, social media has emerged as a powerful tool in a digitally connected world, touching every aspect of human existence. This paradigm swing cuts across people of diverse age albeit affects each age category differently. This work presents the outcome of a study conducted in select towns in central part of Nigeria between January and June 2015. The focus was to determine how youths (age 16 through 25) use social media platforms in terms of the frequency, and purposes of social networking site usage. The survey revealed that, 99% of the respondents have social media accounts out of which 95.2% use smartphones to access various social media platforms. 46.4% from the respondents fall under the category of those very likely to use social platforms in a week, while 26.8% account for those who are extremely likely to use the social networking service within same time frame. Only 0.7% of the respondents were not likely to use social networking service within a week. Among the twelve social media platforms surveyed, Facebook ranked top as the most commonly used social networking channel with 91%, followed by WhatsApp (87%) and Tango ranked last at 1%. Based on the analysis of the result, it is highly likely that social media may have severe impact on young people who have no form of restrains with consequences of huge distractions and privacy intrusions. Conversely, the fact that social media is rapidly building social and communications habits into the youths point to its potential to enhance their learning habits if properly harnessed and formalize to aid pedagogy at secondary and tertiary levels.**

Keywords: Social media, young people, social networking, social sites, cyberspace, smart phones.

I. INTRODUCTION

The Cyberspace has brought about a socially connected digital society, which resulted from the evolution of the internet, information systems and networks, mobility and receptiveness of the people. Social media is fuelling a people-driven democracy with liberty and freedom of participation globally, which is beginning to affect our economic, political, social and relational fabrics of personal and business lives. The recent award of the 2015 Nobel Prize for peace to the It is fast becoming the most powerful social change of human history with ubiquitous and absorption of its tools across diverse ages, cultures and geography [1].

The receptiveness of the populace has continued to increase the power of social media that even now most businesses and organisations have adopted the platform to gain competitive advantages [1]. What appeals to people is that it presents higher possibility of powerful information digestion, that is, it delivers apt and direct short messages to its audience in a fashion that aid easy absorption of the content. Aside the social interconnection and influence, social media is fast replacing other traditional business tools used for marketing, advertisement, profiling, etc. due to the fact that cybercitizens spend much time using cyberspace domain for almost everything. Major brands are migrating to social networking platforms for competitive advantage [1]. Likewise, some security and intelligence agencies have indicated that social media platforms can aid in solving crimes within their jurisdiction [1]. However, one of the factors popularizing the social media platforms is how they connect people worldwide to interact, share content and engage in discussions of mutual interest that know no geographical boundaries. Conversely, young people essentially are interested in establishing their profiles, pushing their ideological beliefs, sharing assorted contents for diverse intents and purposes. Most youth primarily use the tools to re-connect with old friends, find new friends, share pictures and videos, seek for lovers and participate in engaging gossips. Behind all these incredible gains is the exposure of such youths to diverse risks, which can affect diverse people and culture in distinctive ways. As most traditional crimes now have digital equivalent, criminal minded elements are exploiting social media platforms for many nefarious activities to harm others. Invariably, being essentially vulnerable youths can easily be impacted negatively.

This paper presents an investigation of the use of social media among Nigerian youths aged between 16 to 25 years. The choice of this age grade is informed by the fact that the minimum age for enrolment into Nigerian Universities as contained in the regulations of the Joint Matriculation Examination Board (JAMB) is sixteen years, which means

ages 16-25 represent the common period the average Nigerian youth is in the tertiary institution as an undergraduate. The analysis of the result identified commonly used social networking platforms and frequency, the extent of usage, purposes as well as possible risks.

II. Literature Review: Social Media Platforms

Social media as defined by the Merriam-Webster dictionary is a form of electronic communication through which users can create online profiles and network within online communities to share content including photographs, videos, music, ideas and personal messages. This phenomenon has revolutionised the way people communicate, share information and human skills.[1].

Social networking service which is closely linked to social media deals with the sharing of information and multimedia content between users on similar platforms over electronic networks especially the internet and cyberspace. There are several social media platforms being used in Nigeria today and some popular ones such as Facebook and WhatsApp are discussed in this paper.

N. Facebook

Facebook is one of the most popular social media platforms used by both the young and the old. It is an online social media platform which provides several services such as social networking, online advertising, voice calls, instant messaging, video calls, video sharing and viewing, online market place, virtual gifts and notes. Facebook is headquartered in Menlo Park, California. Its website was launched on February 4, 2004, by Mark Zuckerberg with his Harvard College roommates and fellow classmates Eduardo Saverin, Andrew McCollum, Dustin Moskovitz and Chris Hughes [2]. The founders had initially limited the website's membership to Harvard students, but later expanded it to colleges in the Boston area, the Ivy League, and Stanford University.

It gradually added support for students in various other universities and later even to high-school students. Since 2006, anyone who is at least 13 years old was allowed to become a registered user of the website, though the age requirement may be higher depending on applicable local laws [3]. Upon registration on the website, users create their profiles and can add other users as friends. Users may join common interest groups and network with friends and friends of friends. Facebook had over 1.18 billion monthly active users as of August 2015 [4]. Because of the large volume of data users submit to the service, Facebook has in recent times increasingly come under scrutiny for their privacy policies.

O. WhatsApp

WhatsApp Inc. based in Mountain View, California, was founded in 2009 by Brian Acton and Jan Koum, both veterans of Yahoo! [5]. WhatsApp is a cross-platform internet-based instant messaging application that allows iPhone, BlackBerry, Android, Windows Phone and Nokia smart phone users to exchange text, image, video and audio messages for free. WhatsApp is especially popular with end users who do not have unlimited text messaging. In addition to basic messaging, WhatsApp provides group chat and location sharing options.

The application operates under a subscription business model. Upon installation, it creates a user account using one's phone number as the username. All the phone numbers from the device's phonebook are automatically compared with the central database of WhatsApp users and phonebook contacts already using the application are added to the user's WhatsApp contact list. In January 2015, WhatsApp introduced a voice calling feature for Android, iOS and Windows app; this helped WhatsApp to attract a completely different segment of the user population [6].

The application was equally made available on web browsers, although the user's mobile phone needs to be connected to the internet for the application to function. WhatsApp Inc. was acquired by Facebook on February 19, 2014, for approximately US$16 billion [7]. In January 2015, WhatsApp became the most globally popular messaging app with more than 600 million active users. In April 2015, WhatsApp reached 800 million active users. In September 2015 the user base grew to 900 million [8].

P. Twitter

Twitter was founded in March, 2006 by Jack Dorsey and is based in San Francisco. It is a social network platform that enables users to write and read short character messages called tweets. Twitter revolves around the principle of followers who are equally users, who choose to follow another Twitter user and can thus view tweets sent by that user. Whereas unregistered users can read tweets, one must be registered to send tweets.

Tweets are visible by default but users can restrict message delivery to followers. These tweets can be re-tweeted when forwarded via Twitter by users and can be monitored to discover those that are popular and trending. Users can update their profiles via text messages or with apps on smart phones. The platform was ranked third most-used social network in the world resulting from 6 million unique monthly visits and 55 million monthly visits. By 2015, Twitter recorded over 302 million active users [9].

Since inception, Twitter has been used for various purposes ranging from serving as a quick communication tool for political protesters as seen in the 2011 Egyptian protests, as a means of disseminating information rapidly as by the Boston Police to announce the arrest of the Boston Marathon Bomber, to celebrities sharing news with their fans, among many others.

Q. Youtube

YouTube is another very popular social media platform. It is a video sharing service that allows users to watch videos posted by other users and upload videos of their own. With the ubiquitous use of smart phones this platform has become the first choice in personal broadcasting and video sharing. Headquartered in San Bruno, California the service was created by three former PayPal employees, Chad Hurley, Steve Chen, and Jawed Karim in February 2005. In November 2006, it was bought by Google for US$1.65 billion and now operates as one of Google's subsidiaries.

Members and website visitors can share YouTube videos on a variety of web platforms by using a link or by embedding HTML code. Videos that have been uploaded to YouTube may appear on the YouTube website and can also be posted on other websites, though the files are hosted on the YouTube server. While several companies and organizations use YouTube to promote their businesses, the vast majority of YouTube videos are created and uploaded by amateurs from all over the world. Thus, there is wide range of videos available on YouTube. Some examples include amateur films, homemade music videos, sports bloopers, and other funny events caught on video. People also use YouTube to post instructional videos, such as step-by-step computer help, do-it-yourself guides, and other how-to-do videos. As Google offers revenue sharing for advertisement clicks generated on video pages, some users have been able to turn YouTube into a profitable enterprise [10].

R. Flickr

Flickr is an image and video hosting website and web services suite that was created by Ludicorp in 2004 and acquired by Yahoo in 2005. In addition to being a popular website for users to share and embed personal photographs, the service is widely used by photo researchers and by bloggers to host images that they embed in blogs and social media. The Verge reported in March 2013 that Flickr had a total of 87 million registered members and more than 3.5 million new images uploaded daily[11]. In August 2011 the site reported that it was hosting more than 6 billion images and this number continues to grow steadily according to reporting sources [12]. Photos and videos can be accessed from Flickr without the need to register an account but an account must be made in order to upload content onto the website.

Registering an account also allows users to create a profile page containing photos and videos that the user has uploaded and also grant users the ability to add another Flickr user as a contact. Flickr has official mobile apps covering a wide range of mobile phone platforms.

S. Google+

Google+ launched in June 2011 is an interest-based social network that is owned and operated by Google Inc. It is a platform focused on bringing all of Google together for users to experience. Google's efforts in social networking are many, and while none of them has seen the kind of global acceptance that its search, video, and email services have enjoyed, Google's most recent efforts in this space has advanced the state of the market in some unique ways. Google+ experienced strong growth in its initial years, although usage statistics have varied and user engagement have been relatively low [13].

Google+ Circles is a core feature of the Google+ Social Platform. It enables users to organize people into groups or lists for sharing [14] across various Google products and services. Once a circle is created, a Google+ user can share specific private content with that circle. For example, work themed content can be shared with only colleagues, and friends and family could see more personal content. The option to share Public or with Everyone is always available.[15] Since September 26, 2011 users can share Circles; it's a one-time share, so if the creator of the Circle updates the members, people's shared copies won't be updated.

T. Viber

Viber was founded by four Israeli and Belarusian partners: Talmon Marco, Igor Magazinnik, Sani Maroli and Ofer Smocha, with Marco as its CEO [16]. It was initially launched for iPhone on December 2, 2010, in direct competition with Skype. Viber is a mobile application that allows phone calls and text messages to all other users, whether mobile or landline, for free. It is available over WiFi or 3G with sound quality much better than a regular call with mobile carrier charges applicable when used over a 3G network. Once the application is installed, calls can also be made to numbers that do not have Viber at low rates using ViberOut. Viber works on most android, iphone, blackberry, windows, mac, nokia and bada devices.

Once Viber has been downloaded on a mobile phone an access code is received via SMS or a callback to activate it. This ensures that only the real owner of the phone number can get it registered and prevents others from obtaining the access code and placing calls with the caller ID. Viber first requires installation on a phone in order to work on a desktop operating system environment [16]. Viber has over 100 million monthly active users from its 280 million global registered users.

U. Tango

Tango was developed in September 2009 by Uri Raz and Eric Setton of TangoMe Inc. and is based in Mountain View, California. It is a third party voice over internet protocol

(VoIP) social media platform which offers video calls, voice calls and text messages over 3G, 4G and Wi-Fi networks. Tango is free except when used over 3G and 4G networks where data plan charges by the mobile carrier apply. Tango can be deployed using iphones, ipads, windows, and android devices. As at March 2014, there were over 200 million user and it was rated the twelfth most downloaded android phone app by PCMag.

It has a simpler interface and does not require usernames and passwords and once installed the app searches through existing phone contacts to pinpoint contacts already using Tango and highlight them as those reachable via the app. On the other hand, there are some key issues with Tango as it has poorer voice and video quality especially when video calls are being made. To use this app, both the sender and receiver must be registered on the social media platform with no possibility of calls to non-Tango users and landlines. Unlike the situation with some popular VoIP social media apps, Tango has no integration with other social media platforms, no conference calling and no instant messaging capability. These are some of the disincentives to the mass acceptance of Tango [17] [18].

V. LinkedIn

This social media platform was launched in 2003 in Mountain View California and was founded by Reed Hoffman, Allen Blue, Konstantin Guericke, Eric Ly and Jean-Luc Vaillant. Available in twenty-four languages, LinkedIn has been described as the most popular tool for professional networking. It is a social networking tool available to job seekers and professionals where users can invite other users and even non-users to connect. Inviters who get several rejections from invitees risk having their accounts restricted or closed. On this platform, users can get introduced to networks of contacts, new job and business opportunities, display products and services in their company profile pages, list job vacancies and search for potential candidates [19].

W. Myspace

Chris DeWolfe and Tom Anderson founded Myspace, which is headquartered at Beverly Hills, California, in 2002. It is a social networking website offering an interactive, user-submitted network of friends, personal profiles, blogs, groups, photos, music and videos. It was the biggest social media platform up till 2008 when it was overtaken by Facebook. Its influence on pop culture and music was widespread and is credited with the creation of unique URLs for companies and artistes. A major issue leading to the loss of popularity of Myspace was the inability to build an effective spam filter which led to vandalism, phishing, malware and spam. Myspace was re-launched in 2013 and has bulletin, instant messaging and access to radio stations as some of its features [20].

X. Blackberry Messenger

Blackberry Messenger (BBM) was launched by blackberry manufacturer Research in Motion in 2006. It is a proprietary internet-based pin instant messenger, video and telephony application included on blackberry devices, that enables messaging and voice calls between one or several users on the platform. Developed initially for only blackberry devices, by 2013 it became available to android and ios phones. With the release of BBM 5.0, users can send a QR Code to add each other to their respective contact lists rather than using an alphanumeric pin or an email address associated with the users' blackberry [21].

Y. Skype

First released in August 2003, Skype was created by Dane Janus Friis and Niklas Zennström in partnership with Ahti Heinla, Priit Kasesalu, and Jaan Tallinn, who developed the backend. It is an IP telephony service provider that can be used to make free voice and video calls over the Internet to any Skype subscriber or to any other non-user at low calling rates. It is relatively simple to download and install the software, which works on most computers and phones. A dedicated Skype phone can be used or desktop computers, notebooks, tablets, mobile phones and other mobile devices fitted with a headset, speakers, microphones or USB phone. Skype also enables file transfers, texting, video chat and videoconferencing. In September 2005, eBay acquired Skype for $2.6 billion [22] [23].

III. METHODOLOGY

This research was conducted by administering the questionnaire to three hundred and twenty-two (322) participants, selected randomly from five tertiary institutions within Plateau and Nasarawa States in central Nigeria. Two hundred and ninety-one (291) responded, which represents approximately 95% success rate. The design of sample questions took into cognizance the time it will take an average respondent to complete the questionnaire. The initial design was remodelled after a test-run on twelve participants to achieve an average of thirty minutes for a respondent to complete the questionnaire. This test-run helped gauge the participants' understanding of the questions posed, reaction and time it took to read before responding to each question. The outcome of the pre-test enabled the scaling of the questions to adapt to the psychology of the target population.

The survey instrument aimed to discover what characterised the frequency of and purpose for using different social media platforms by the youths as well as the impact such social media engagements has on the youths. The questions focused on finding key variables that can help determine the use and impact of social media on young people in these two states in Nigeria. The survey relied on measuring variables such as weekly usage, hourly usage, which specific

social media platforms the respondent frequently uses and for what purpose to determine the potential effect of social media service on young people.

The interrelationship between the questionnaire design, administration, processing and analysis provided factual information taking into account the factors that underpin component variance. Copies of the questionnaire were administered under strict confidentiality and privacy, although each respondent was given a pen as an incentive to take part in the survey. Statistical and quantitative methods were used to analyse the responses to evaluate and validate the important indicators relating to the investigation.

IV. RESULTS

The results obtained from analysis of the questionnaire retrieved are presented below.

A. Smart Phone Possession amongst Youths

The youths within the research area were critically reviewed to discover the number of those with smart phones, which is one of the essential devices needed to access social networks and social media. This data is tabulated in Table 1 and depicted in Figure 1 below.

Table 1: Smart phone possession.

Do you have a smart phone?	**Frequency**		**Cumulative**	
	Total	Percent	Total	Percent
Total	291	100	0	0
Yes	277	95.2	277	95.2
No	12	4.1	289	99.3
Not Applicable	2	0.7	291	100

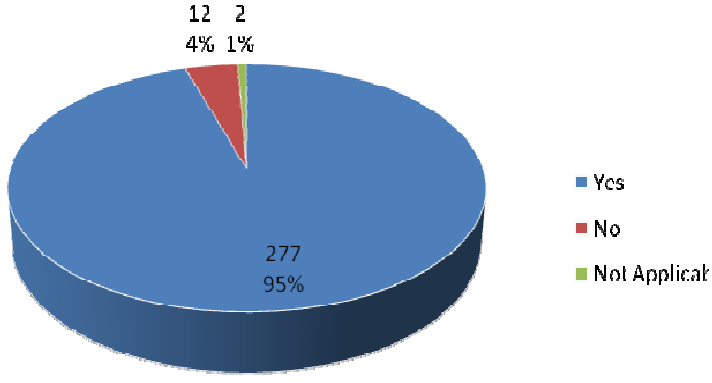


Fig. 1: Pie chart of smart phone possession.

B. Registration of a Social Media Account

In order to access social networks and share social media content, the intended user must have a registered and active social media account. Table 2 and Figure 2 presents the collated data analysed from the sample population of youths.

Table 2: Registration of a social media account.

Do you have any social media account?	**Frequency**		**Cumulative**	
	Total	Percent	Total	Percent
Total	291	100	0	0
Yes	288	99	288	99
No	2	0.7	290	99.7
Not Applicable	1	0.3	291	100

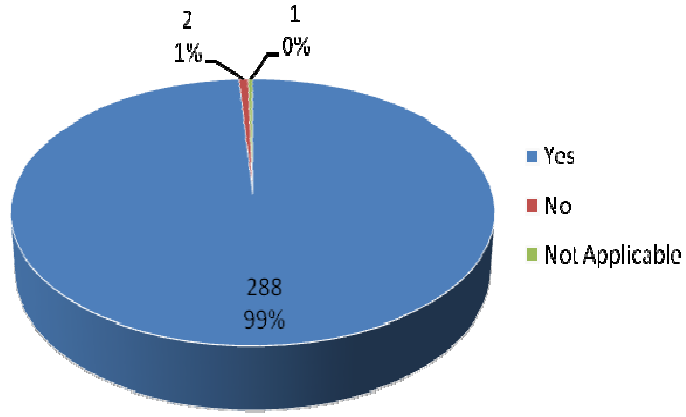


Fig.2: Pie chart on social media account registration.

C. Social Media Platform Usage

This result, as presented in Table 3. Figures 3 and 4 show analysis of the usage of the various social media platforms by sample population of youths investigated.

Table 3: Table on distribution of social media platform usage.

Social Media Platform	**User**	**Non User**	**Social Media Platform**	**User (%)**	**Non User (%)**	**Social Media Platform**	**Use %**
FaceBook	265	26	FaceBook	91	9	FaceBook	27.1
Twitter	142	149	Twitter	49	51	Twitter	14.5
WhatApp	254	37	WhatsApp	87	13	WhatsApp	25.9
Google+	97	194	Google+	33	67	Google+	9.9
LindkedIn	7	284	LindkedIn	2	98	LindkedIn	0.7
YouTube	40	251	YouTube	14	86	YouTube	4.1
Flickr	6	285	Flickr	2	98	Flickr	0.6
Viber	10	281	Viber	3	97	Viber	1.0
Skype	23	268	Skype	8	92	Skype	2.3

Myspace	8	283	Myspace	3	97	Myspace	0.8
BBM	124	167	BBM	43	57	BBM	12.7
Tango	3	288	Tango	1	99	Tango	0.3

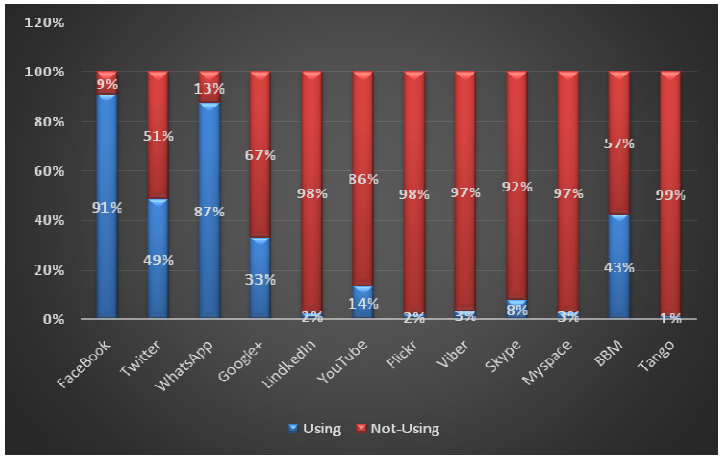


Fig. 3: Usage distribution across each of the 12 reviewed social media platforms.

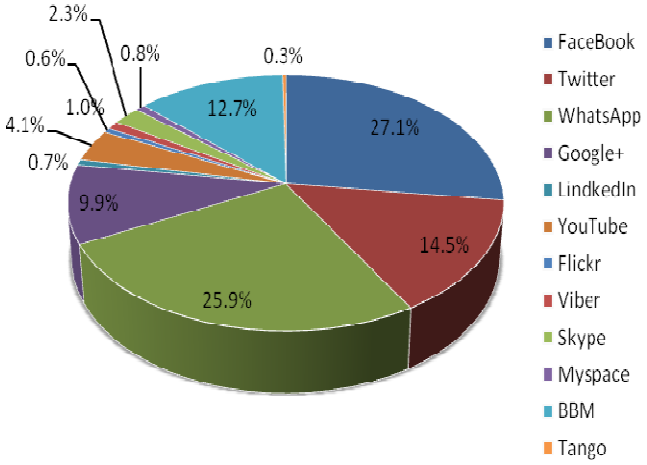


Fig.4: Usage distribution over the population of respondents.

D. *Weekly Usage of Social Networks*

Table 4 and Figure 5 below show respondents' rate of weekly usage of social networks services.

Table 4: Table on the weekly usage of social networks.

Weekly Usage	Frequency		Cumulative	
	Total	Percent	Total	Percent
Extremely likely	78	26.8	78	26.8
Very likely	135	46.4	213	73.2
Moderately likely	63	21.6	276	94.8
Slightly likely	10	3.4	286	98.3
Not at all likely	2	0.7	288	99
Not Applicable	3	1	291	100

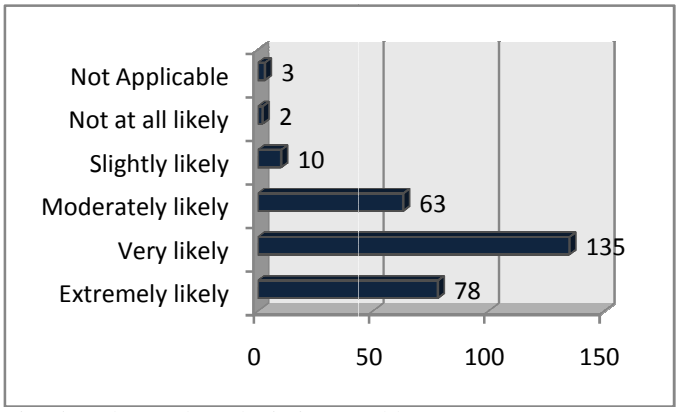


Fig. 5: Column chart depicting weekly usage rates.

E. *Impact of Social Media on Youth Education*

Data was collected and analysed critically to discover the perceived distractive impact of social media and social networking on education of the youths in the research area considered. Figure 6 graphically portrays this.

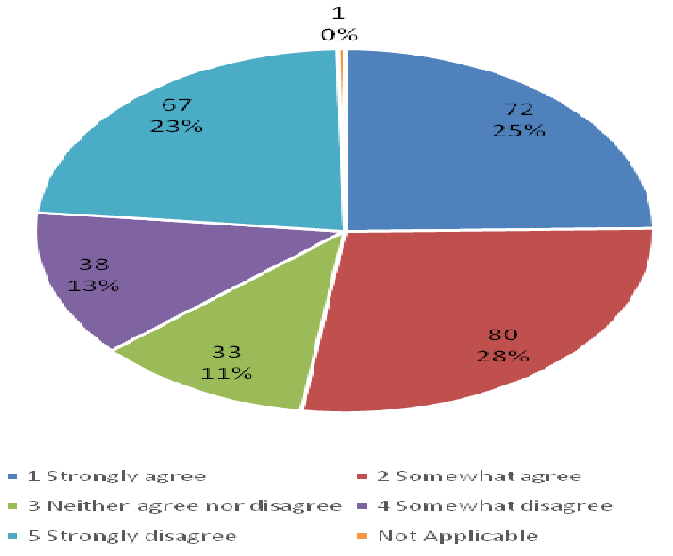


Fig. 6: Pie chart on impact of social media on studies.

F. Common Uses of Social Media Platforms

As discussed in this paper, there are many uses to which users deploy social networking service. Highlighted in Table 5 and Figure 7 are some key purposes for which youths within the research area use these platforms.

Table 5: Uses of social media platforms.

Purpose	Myspace	Youtube	BBM	Flickr	Whatsapp
Social	2	10	37	2	134
Studies	1	5	20	1	32
Gossip	1	2	7	1	16
Dating	0	0	9	0	21
General Information	1	21	51	1	51
Others	1	2	3	1	5
Not Applicable	286	251	164	286	32

Purpose	Twitter	Facebook	Google+	Viber	Skype	Tango
Social	51	196	8	5	17	2
Studies	12	11	54	1	1	1
Gossip	6	8	1	1	1	2
Dating	7	11	0	0	1	0
General Information	54	44	46	0	2	0
Others	2	1	1	1	0	0
Not Applicable	159	20	181	283	269	286

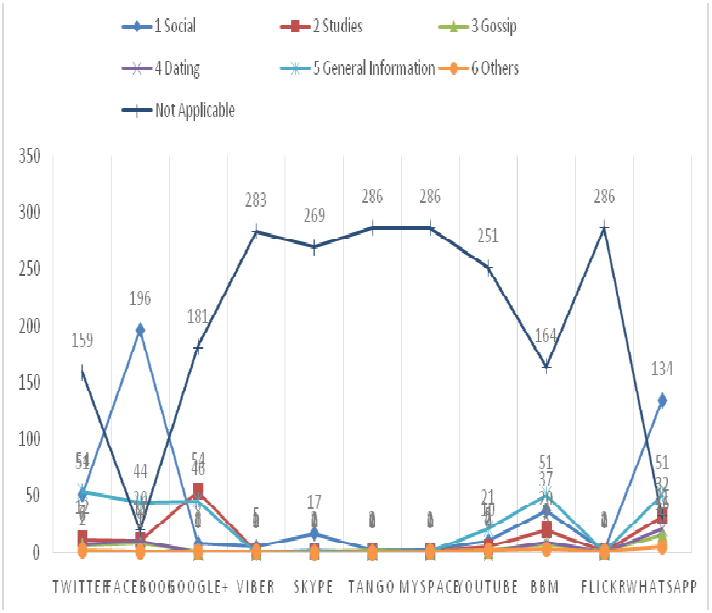


Fig. 7: Line chart on the common uses of the social media platforms investigated.

V. DISCUSSION

From the results depicted in Table 1 and Figure 1, 95.2% of the respondents have smart phones. This clearly underlines the fact that Nigerian youths are becoming increasing technology savvy and have a strong yearning for access to social networks and social media. They obviously have the desire for constant ubiquitous internet access which the mobile phone industry has rapidly keyed into by providing affordable smart phones in the Nigerian market place. Not to be left behind, the communication companies which are the major providers of internet access in Nigeria have progressively rolled out cheaper data plans and bundles to take their own market share. Since the youths make up more than fifty percent of the Nigerian population, they are readily a dynamic and investment worthy sector for the mobile phone industry and communication companies. To protect the youths from the exploitative tendencies of these big organisations and companies whose major concern is driving up their profits even to the detriment of everything else, checks and balances must be put in place to cap their excesses and ensure consumer protection, reasonable tariffs and quality products and services at all times. Furthermore mobile phone companies should be encouraged to manufacture, if not develop, the smart phones sold in Nigeria within the country to give gainful employment to the youths.

Registration of social media accounts among the youths investigated is 99% as portrayed in Table 2 and Figure 2. This shows that Nigerian youths of today desire an online presence, a forum where they can air their views on diverse topics, share information, knowledge, pictures, videos, music and other

social media content, meet and interact with other people and keep up to date on current affairs and trending events both locally and globally. This is simply a natural extension of human behaviour as man is a social being seeks to, and thanks to internet access, relate and interact as closely and regularly with people in his immediate environment as with people on any continent of the world. Therefore to shield youths from the criminality associated with cyberspace and internet usage, a suitable monitoring system must then be put in place to safeguard the various means of social networking, to ensure the privacy of cyber space users are not violated and that basic human rights are not infringed upon. Data and multimedia uploaded to personal online profiles should remain private except on the decision by the user to publicize same.

Table 3, Figures 3 and 4 reveal the distribution of usage of the twelve social media platforms under investigation. The platforms investigated were Facebook, Twitter, WhatsApp, Google+, LinkedIn, YouTube, Flickr, Viber, Skype, Myspace, Blackberry Messenger and Tango. The result shows that Facebook with 91% is the most popular social media platform amongst the youths surveyed. This is closely followed by WhatsApp with 87%. The least used social media platform is Tango, followed by Flickr with 1% and 2% respectively. The widespread popularity of Facebook is mainly due to its range of features like wall post, chat, call, video, gaming, like and share capabilities. The ease of its registration process, the multiple avenues through which connections can be made to its platform and its user friendly web interfaces have also greatly aided its wide adoption.

With Facebook having over 1.18 billion active monthly users spread across the globe, it has proven to be the most effective means by which users can locate long lost relationships and foster new ones. Business and employment opportunities also abound on this social network service, thereby adding to its appeal to the youths. Policy must thus be put in place to guide against the identity, security and privacy issues that abound with having such a dominant social networking entity. Cyberspace criminals who hack into user profiles and steal information, which they use for their nefarious activities, need to be checked in such a way as to guarantee a safer social networking service for the youth. One way to do this is for Facebook Inc. to ensure that registered users are duly informed of any changes in the security and privacy settings of their accounts before such changes take effect, giving them an opportunity to disallow changes not initiated by them. Facebook Inc. also needs to closely monitor and deregister social networking accounts used for fraudulent activities.

The weekly usage of social networks among the surveyed youths was investigated and results obtained are as shown in Table 4 and Figure 5. From the result, 46.4% of the respondents were found to be very likely to use social networks and 26.8% of them to be very likely. This shows that over 70% are active users of social networking services. Depending on the purpose of this significant percentage of users, it could be a healthy or unhealthy habit.

The survey shows that a great number of youths frequent social network sites on a regular basis, thus it is important to discover the impact of such usage on the education and studying habits of the youths as the catchment age of this research are those in the 16 to 25 years bracket which in the ideal Nigerian Education setting is the period when said youths are transiting from secondary to tertiary learning institutions. In this regards, a total of 53% of the respondents agree that social networking sites were sources of distraction to education and hindered good studying habits of the users. Besides the above revelation, there is also another concern about the possibility of these social networking services being used by criminal elements of the society to fraud unsuspecting users. The age bracket studied is highly vulnerable and can easily fall prey to abuses or even be psychologically held hostage or groomed into nefarious activities by unsuspecting co-users. This fact is perhaps most disturbing as there are already enough media reports of cases of youths in Africa who have ben radicalised, via such social networking sites, by Islamic fundamentalist groups like the Al-Queda and ISIS.

To counter this negative effect, youths should be encouraged to use social networking sites constructively and taught how to apply reasonable restraints. To this extent, institutions should create the necessary awareness to inculcate social networking discipline, as well as, formally create social media tools that can engage students in their school works by sharing and discussing topical issues. Social networking sites can help students to form study groups to support effective communications between students on the one hand and students and lecturers on the other. By doing so, the adverse impact of social media on youngsters can be reduced when they use the same tools for engaging in their studies. Gaming, idle chatting and other excessive social activities highlighted in Figure 7 can equally be minimised as much as possible. Conversely, social media can enhance students' perception of community, if the young people use it as productive tools.

VI. CONCLUSION

Social networking services have emerged as powerful, interactive and frequently used cyber-platforms that have many-sided impacts, which to a large extend depend on how the individual users deploy them. When used correctly, social networking sites can enhance the quality of life of the users in many respects. However, when abused, they could have overwhelming negative consequences, particularly on youths who are still impressionable. The study has shown an upswing in the use of social networking services by Nigerian youths using smartphones and mobile networks. This work concludes that notwithstanding that young people are developing social communications habits, with correct discipline, it can help

students study collaboratively and efficiently. Social networking services can help in the summation of collaborative knowledge of a study group or class thereby enhancing more efficiently and timely information flow to every stakeholder within the learning environment

REFERENCES

[1] S. Edosomwan, S.K. Prakasan, D. Kouame, J. Watson, T. Seymour, “The history of social media and its impact on business”, The Journal of Applied Management and Entrepreneurship, 2011, Vol. 16, No. 3. citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.458...pdf Retrieved 13 October, 2015.

[2] N. Carlson, "At Last – The Full Story Of How Facebook Was Founded". Business Insider, March 5, 2010.

[3] "Information For Parents and Educators". Facebook. Retrieved 9 October, 2015.

[4] "Facebook Reports First Quarter 2015 Results". April 22, 2015. Retrieved 9 October, 2015.

[5] Definition of whatsapp, http://searchmobilecomputing.techtarget.com/definition/WhatsApp . Retrieved 9 October, 2015.

[6] "Why WhatsApp Will Remain" (blog). Retrieved 9 October, 2015.

[7] Facebook's $18 Billion Deal Sets High Bar". The Wall Street Journal. pp. A1, A6. Retrieved 10 October, 2015.

[8] Albergotti, Reed; MacMillan, Douglas; Rusli, Evelyn M. (retrieved 10 October, 2015).

[9] https://en.m.wikipedia.org/wiki/Twitter. Retrieved 9 October 2015

[10] http://techterms.com/definition/youtube. Retrieved 10 October, 2015.

[11] "The man behind Flickr on making the service 'awesome again'". *The Verge. 2013-03-20*. Retrieved 2013-08-29.

[12] Parfeni, Lucian (2011-08-05). "Flickr Boasts 6 Billion Photo Uploads". *Softpedia*. Retrieved 2012-03-01.

[13] http://www.androidcentral.com/what-google-and-who-actually-uses-it retrieved 10/10/15

[14] Jump up to: a b c d *Siegler, M.G. (June 28, 2011).* "Google+ Project: It's Social, It's Bold, It's Fun, And It Looks Good — Now for the Hard Part". TechCrunch. Retrieved June 30, 2011.

[15] Jump up ^ Find people and create circles - Google+ Help. Support.google.com. Retrieved on 2013-11-29

[16] https://en.wikipedia.org/wiki/Viber retrieved 11/10/15

[17] http://voip.about.com/od/videoconferencing/fr/Tango-Free-Text-Voice-And-Video-Calls.htm

[18] http://www.bewebsmart.com/app-review/what-is-tango-okay-for-kids/

[19] J. Hempel, LinkedIn: How it’s changing business”, Fortune, 1 July, 2013, pp. 69 – 74.

[20] D. Tapscott, A.D. Williams, “Wikinomics: How man’s collaboration changes everything”, New York, Penguin, 2007.

[21] D. Dannenfeldt, “How blackberry works”, How Stuff Works, Retrieved 10 October 2015.

[22]http://searchunifiedcommunications.techtarget.com/definition/Skype

[23] http://www.webopedia.com/sgsearch/results?cx=partner-pub-8768004398756183%3A6766915980&cof=FORID%3A10&ie=UTF-8&q=skype

Internet of Things for Africa: Challenges and Opportunities

Maryleen Ndubuaku
Department of Electrical and Electronic Engineering
Federal University of Technology, Owerri
Imo State, Nigeria
ndubuakumaryleen@gmail.com

David Okereafor
Department of Electrical and Electronic Engineering
Federal University of Technology, Owerri
Imo State, Nigeria
dokereafor@yahoo.com

Abstract— Internet of Things (IoT) is an integrated part of Future Internet where physical and virtual "things" have identities and are seamlessly integrated into the information network. IoT is one technology that is penetrating the world so fast. It is being adopted to create smart homes, smart environment, connected automobile, wearables and industrial internet. No doubt, the African environment is gradually feeling the wave of this technology which is facilitated by the widespread use of smartphones, cheap bandwidth and availability of big data analytics. However, the African tech society seems to be slowly coming up to this reality. There are so many areas to be explored in the IoT which will add so much value to individuals, businesses and the government at large. Accompanying the IoT innovation are challenges some of which are peculiar to the African environment. This paper introduces the concept of internet of things, describes its level of development in Africa, highlights some challenges to be met during its deployment and states some areas of applications in the continent.

Keywords: *Internet of Things (IoT), Africa, IoT deployment, IoT applications.*

I. INTRODUCTION

The Internet of Things (IoT) refers to the use of intelligently connected devices and systems to harness data gathered by embedded sensors and actuators in machines and other physical objects [1]. The steps in IoT basically involve collecting data, aggregating them into a network and processing them or storing them for future improvements. For consumers, the IoT has the potential to deliver solutions that dramatically improve energy efficiency, security, health, education and many other aspects of daily life. For enterprises, IoT can underpin solutions that improve decision-making and productivity in manufacturing, retail, agriculture and other sectors.

IoT describes a system where items in the physical world, and sensors within or attached to these items, are connected to the Internet via wireless and wired Internet connections. These sensors can use various types of local area connections such as RFID, NFC, Wi-Fi, Bluetooth, and Zigbee. Sensors can also have wide area connectivity such as GSM, GPRS, 3G, and LTE [3].

The term "Internet of Things" was popularized by the work of the Auto-ID Center at the Massachusetts Institute of Technology (MIT). In 2002, its co-founder and former head Kevin Ashton was quoted in Forbes Magazine as saying, "We need an internet for things, a standardized way for computers to understand the real world" [2].

Since then, many visionaries have seized on the phrase "Internet of Things" to refer to the general idea of things, especially everyday objects that are readable, recognizable, locatable, addressable, and/or controllable via the Internet, irrespective of the communication means, including things that are non-electronic such as food and clothing. Examples of "things" include: People, Location (of objects), Time Information (of objects) or Condition (of objects) [5].

Many African countries have already taken advantage of IoT technology; from healthcare providers tracking the health of outpatients to utility companies using connected meters to check usage, find faults and pre-empt surges in demand. In fact, without legacy infrastructure in place, Africa can leapfrog in a number of areas that more developed countries would find difficult [8].

The Internet of Things (IoT) has the potential to offer a range of innovative new services and solutions to individuals across the region, and in doing so to begin to address some of the challenges it is facing including those arising from high levels poverty and the need to extend access to basic services to currently underserved populations [6].

The goal of this paper is to bring IoT in the context of Africa and scrutinize the barriers to its expansion as well as possible solutions with accompanying application areas.

II. IOT PROPERTIES AND ARCHITECTURE

From a technical point of view, the Internet of Things is not the result of a single novel technology; instead, several complementary technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world. These capabilities include:

a) *Communication and Cooperation:* Objects have the ability to relate with each other and with their surroundings via networks such as GSM and UMTS, Wi-Fi, Bluetooth, ZigBee and those referring to Wireless Personal Area Networks (WPANs). There are several reasons why objects will need to communicate with each other. For example for security purposes, an object can request authentication from other remote or near devices before granting access to particular information or services.

b) *Discoverability:* Objects can be located and addressed via discovery, look-up or name services, and can therefore be remotely accessed or configured.

c) *Identification:* Objects are uniquely identifiable. RFID, NFC (Near Field Communication) and optically readable bar codes are examples of technologies with which even passive objects which do not have built-in energy resources can be identified (with the aid of a "mediator" such as an RFID reader or mobile phone). Identification enables objects to be linked to information associated with the particular object and that can be retrieved from a server, provided the mediator is connected to the network (see Figure 1).

d) *Sensing:* Objects collect information about their surroundings with sensors, record it, forward it or react directly to it.

e) *Actuation:* Objects contain actuators to manipulate their environment (for example by converting electrical signals into mechanical movement). Such actuators can be used to remotely control real-world processes via the Internet.

f) *Embedded Information Processing:* Smart objects feature a processor or microcontroller, plus storage capacity. These resources can be used, for example, to process and interpret sensor information, or to give products a "memory" of how they have been used.

g) *Localization:* Smart things are aware of their physical location, or can be located. GPS or the mobile phone network are suitable technologies to achieve this, as well as ultrasound time measurements, UWB (Ultra-Wide Band), radio beacons (e.g. neighboring WLAN base stations or RFID readers with known coordinates) and optical technologies.

h) *User Interfaces:* Smart objects can communicate with people in an appropriate manner (either directly or indirectly, for example via a smartphone) [2].

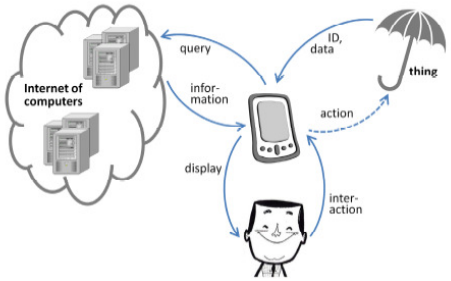


Figure 1: The smartphone as a mediator between people, things and the Internet [2].

IOT architecture consists of different suite of technologies supporting IOT. It serves to illustrate how various technologies relate to each other and to communicate the scalability, modularity and configuration of IOT deployments in different scenarios as shown in Figure 2. It is made up of the Sensor layer, Gateway and Network layer, Management Service layer and Applications layer.

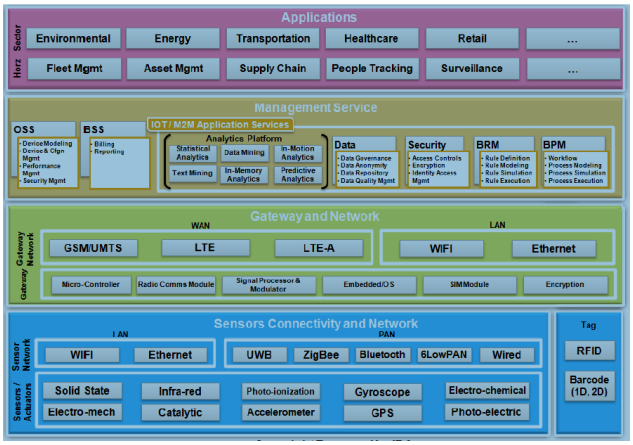


Figure 2: IOT Architecture [5].

III. SUCCESS FACTORS FOR IOT DEPLOYMENT IN AFRICA

There are several factors that hints to the fact that massive IoT deployment in Africa will amount to success. Most of them refer to cost of devices and introduction of new technology that will handle the communication and information processing aspects of IoT. They are:

1. Cheaper cost of sensors and bandwidth - Sensor prices have dropped to an average 60 cents from $1.30 in the past 10 years. The cost of bandwidth has also declined steeply, by a factor of nearly 40X over the past 10 years [14].
2. Cheap processing - The cost of processing has seen a sharp decrease of nearly 60 times since the past 10 years[14], thereby allowing more devices to smartly handle all the new data they are generating or receiving.
3. Introduction of Big Data Analytics – With the introduction of big data analytics, the millions of data which is turned out daily by the various connected "things" in the IoT network can be processed faster and better.
4. Widespread use of Smartphone – Smartphones have become a remote control or interface for most applications ranging from healthcare to automobile. Also, the number of smartphone users has increased since the past years. According to a report, the Smartphone penetration per capita in Middle East and Africa will have experienced an increase of 13.6% from 2.6% in 2011[19]. The affordability of the smartphone has also aided its spread in Africa.
5. Ubiquitous Wireless network – Wireless networks such as Wi-Fi have become cheaper and more accessible.
6. Alternative energy and ultralow power technologies: Availability of power to supply most devices that require automation has been a challenge in Africa but new technologies for energy harvesting, ultralow power devices have been a key enabler to IoT. Some devices today can power themselves as they tap energy from immediate environment. Example is wearable devices for body monitoring (temperature and heart rate) can power themselves with energy from vibration, pulse and heat.

IV. STATE OF IOT DEPLOYMENT IN AFRICA

Machine to Machine (M2M) solutions - a subset of the Internet of Things – already use wireless networks to connect devices to each other and the Internet, with minimal direct human intervention, to deliver services that meet the needs of a wide range of industries [1]. A M2M Service is a combination of devices or "machines" using network resources to communicate with remote application infrastructure for the purposes of monitoring and control, of either the "machine" itself, or of the environment [11].

Africa's most economically developed country, South Africa, has much of the infrastructure in place to lead the market. South Africa remains the biggest market for M2M followed by Kenya with deployments seen in vehicle tracking, monitoring air quality and railway track conditions. Elsewhere, Rwanda is connecting SIM cards to POS terminals in isolated areas to allow for the acceptance of credit card payments.

The Internet of Things represents an evolution of M2M through the coordination of multiple vendors' machines, devices and appliances connected to the Internet through multiple networks [1]. Table 1 shows the total M2M connections in the world and brings out the fact that Africa still lags behind in the use of Machine-to-Machine connections.

Table1: M2M connections by region [1].

Region	M2M % total connections (2013)
Africa	1.0%
Asia	2.1%
Europe	5.1%
Latin America	2.1%
Northern America	9.3%
Oceania	5.1%
Global	2.8%

Market analysts Gartner forecast the global IoT market to total more than 26bn devices by 2020 [7]. There are already a broad range of IoT deployments across Sub-Saharan Africa, with around seven million cellular M2M connections by mid-2014 [6].

Examples of current deployments include the following:

- Airtel Congo has partnered with a local vehicle tracking company to offer fleet location services to its customers.
- MTN Rwanda recently reported that the fastest growth in connections was in the area of point-of-sale (PoS) terminals, a market that had seen rapid growth over recent years. The market is being driven by the focus of financial institutions in the country on growing the number of payment cards in use. MTN in South Africa recently implemented its first smart metering project for the City of Johannesburg. This project aimed to install 50,000 meters by June 2014 as part of the first phase of the project, which is due to complete in 2015.
- In the health sector, Sequoia Technology provides a HIV diagnosis communications system using M2M GPRS printers and a dedicated GSM gateway. The solution allows for test results from far away

laboratories to reach the clinics much faster, savings lives in the process [6].

According to [6], the sub-region will witness a number of innovative new M2M approaches in areas as diverse as telematics, smart metering, mobile banking and finance, security solutions and smart cities. The total number of M2M connections in SSA is forecast to grow at a CAGR of 26% per annum, reaching 28 million connections by 2020.

In addition, Togo's Digital Minister, Cina Lawson declared that many African countries have already taken advantage of IoT technology; from healthcare providers tracking the health of outpatients to utility companies using connected meters to check usage, find faults and pre-empt surges in demand. She said that IoT is currently being used in Togo for vehicle tracking but thinks it will quickly be moved into mobile payments or into the area of logistics. She also sees great potential in agriculture where it could be used to improve yields. For her, internet penetration and connectivity remain a challenge; for IoT to work effectively it needs to rely on high speed internet connections [8].

Moreover, on May 14, 2015, MTN Business unveiled the first Pan African Internet of Things (IoT) platform. MTN's IoT platform enables networked devices to exchange information and perform actions without requiring manual assistance. MTN's IoT offering will give African enterprises, entrepreneurs and developers the means to enable and inspire growth by providing them with tools specific to their business needs, solving age-old business problems in better and more innovative ways. Also, MTN's dedicated IoT network will have a footprint spanning 23 countries, ensuring that these services offer a seamless experience for those who make use of them. MTN's IoT platform will provide benefits across a wide range of industries, including those integral to developing countries such as water and electricity supply, utility management, transport, retail, agriculture and mining [10].

V. CHALLENGES FACING IOT IN AFRICA AND SOLUTIONS

A. *Power Supply*

Due to the fact that things move around and are not connected to a power supply, their smartness needs to be powered from a self-sufficient energy source. Most batteries and power packs are either to heavy, thereby making the entire system bulky or they have a short lifespan and require frequent replacement or charging. Unfortunately, battery technology is making relatively slow progress, and "energy harvesting", i.e. generating electricity from the environment (using temperature differences, vibrations, air currents, light, etc.), is not yet powerful enough to meet the energy requirements of current electronic systems in many application scenarios. Hopes have been cast on future low-power processors and communications units for embedded systems that can function with significantly less energy. There are already some battery-free wireless sensors that can transmit their readings a distance of a few meters. Like RFID systems, they get the power they require either remotely or from the measuring process itself, for example by using piezoelectric or pyro electric materials for pressure and temperature measurements [2].

Solar energy is set to become the biggest trend. Installing slim and transparent solar panels on phones, cars and even buildings has already started providing consumers to keep going without ever having to worry about looking for the nearest plug. Other technologies are being explored: for example, British company Perpetuum uses electromagnetic energy to recharge devices. Thermal and RF are also being introducing to power devices and stretch batteries' lives. WiFi based sensors have too been developed to run on 2xAA batteries for over a year [13]. Recently, researchers at ETH Zurich University developed a new type of glass material that has the properties to double a smartphone battery life.

The energy puzzle is not complete without Central Processing Units (CPUs). The processing units are being pushed to a limit and need to be investigated further. CPU consumption got heightened by the rising number of IoT enabled devices signaling and sending data between one another [13].

B. *High Poverty Rate*

IoT uses technology to connect physical objects to the internet. For IoT adoption to grow in Africa, the cost of components that are needed to support capabilities such as sensing, tracking and control mechanisms need to be relatively inexpensive in the coming years. Gartner has forecast that most technology components such as radio, WiFi, sensor and GPS, could see a drop in cost of 15% to 45% from 2010 to 2015. The trend forecast by Gartner could incentivize organizations to pursue opportunities in IoT in the next one to three years [5].

C. *Network Capacity Constraints*

With convergences brought about by connected machines and smart mobile devices, there is an increasing demand for network infrastructure to support these data "hungry" devices with a certain level of expected QoS. New mobile applications that perform contextual-aware services may require frequent bursts of small blocks of data for updating and synchronizing. The issue of limited network capacity has prompted many global operators to develop initiatives that leverage technologies in unlicensed spectrum such as whitespace and increase the use of WiFi to offload mobile data traffic for wireless usage [5].

D. *Illiteracy*

According to [6], there has been significant progress in increasing adult literacy rates across Sub-Saharan Africa in recent years. Despite these advances, around 37% of the adult population still lack basic literacy skills, equivalent to over 170 million people. In addition to basic literacy, digital

literacy—the ability to effectively and critically navigate, evaluate and create information using a range of digital technologies—is also significantly lacking amongst the population in the region and must be addressed. Also, there needs to be adequate user education on privacy and security of their "things". This will involve understanding how to issue permissions and access to their connected "things".

E. Lack of Local Content

The vast majority of digital content and mobile applications and services accessible across Sub-Saharan Africa have been developed in more advanced markets. There has been little or no customization in terms of either the content or the languages available online. However, some localization approaches are now emerging. As of January 2013, there were said to be 146 developers in Nigeria, who between them had submitted 419 apps specifically for African BlackBerry consumers. Also, RIM is working with a number of universities and schools across Africa in order to teach and educate students on mobile application development, as part of its Blackberry Academic Programme [6].

F. Low Internet Penetration Rate

With an internet penetration rate of 16% in Africa and eight out of the 10 countries having the world's lowest internet access rates, there are major barriers to the adoption of the IoT. However, there is clear growth potential. Consulting firm McKinsey estimates that by 2025 Africa will have tripled internet penetration to over 50%, or around 600m people, and as it does not have the same extensive infrastructure as Western countries, it can adapt its cities for IoT solutions more easily [7].

G. Interoperability and Standards

Different industries today use different standards to support their applications. With numerous sources of data and heterogeneous devices, the use of standard interfaces between these diverse entities becomes important. If manufacturers are to realize the promise and potential of IoT, it is critical that the billions of things that make up IoT are able to connect and interoperate. Only through common frameworks based on truly open industry standards can secure reliable interconnections and shared information in IoT be achieved. It is with that goal in mind that organizations such as the Open Interconnect Consortium (OIC) and Industrial Internet Consortium (IIC) have been established [4].

H. Data Management

Without data there is no IoT. Data is the petrol of this industry and it needs to be kept safe and managed to ensure users benefit from everything IoT, M2M and other services have to offer. In a world where everything is connected, there will be large chunks of data turned out per second accompanied with the risk of being misused, stolen, as well as services providers not being able to cope with its enormity. Currently, Big Data solutions by companies like MySQL and Hadoop, deal with scale, capacity and processing tasks. In connection with other companies like Several nines, software management is becoming ever easier.

But the big challenge lies at the heart of IoT: so far IT has not had to deal with a unique dataset on its own. Current data makes it to databases the same way unstructured data does. Joe Skorupa, Gartner's vice president provided a solution by saying that Data centre operations and providers will need to deploy more forward-looking capacity management platforms that can include a data center infrastructure management (DCIM) system approach of aligning IT and operational technology (OT) standards and communications protocols to be able to proactively provide the production facility to process the IoT data points based on the priorities and the business needs [13].

I. Security Issues in IoT

As the IoT becomes a key element of the Future Internet and a critical national/international infrastructure, the need to provide adequate security for the IoT infrastructure becomes ever more important. Large-scale applications and services based on the IoT are increasingly vulnerable to disruption from attack or information theft and the consequences could be severe. For example, a smart meter—one which is able to send energy usage data to the utility operator for dynamic billing or real-time power grid optimization—must be able to protect that information from unauthorized usage or disclosure. Information that power usage has dropped could indicate that a home is empty, making it an ideal target for a burglary or worse [15]. Required measures in several areas to make the IoT secure from those with malicious intent, include:

- DoS/DDOS attacks are already well understood for the current Internet, but the IoT is also susceptible to such attacks and will require specific techniques and mechanisms to ensure that transport, energy, city infrastructures cannot be disabled or subverted.
- General attack detection and recovery/resilience to cope with IoT specific threats, such as compromised nodes, malicious code hacking attacks - Cyber situation awareness tools/techniques will need to be developed to enable IoT-based infrastructures to be monitored. Advances are required to enable operators to adapt the protection of the IoT during the lifecycle of the system and assist operators to proactively take the most appropriate protective action during attacks.
- Access control and associated accounting - these are necessary IoT schemes to support the various authorization and usage models that are required by users. The heterogeneity and diversity of the devices/gateways that require access control will require new lightweight schemes to be developed.

- Machine Learning - The IoT needs to handle virtually all modes of operation by itself without relying on human control. New techniques and approaches are required to lead to a self-managed IoT [12].

J. *Privacy Issues in IoT*

As much of the information in an IoT system may be personal data, there is a requirement to support anonymity and restrictive handling of personal information. Users should be equipped with necessary tools that allow them to define the policies for sharing their personal data with authorized persons and applications. There are a number of areas where advances are required:

- Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties. Technologies such as homomorphic and searchable encryption are potential candidates for developing such approaches.
- Techniques to support Privacy by Design concepts, including data minimization, identification, authentication and anonymity.
- Fine-grain and self-configuring access control mechanism emulating the real world [12].

VI. AREAS OF APPLICATIONS OF IOT IN AFRICA

A. *Smart Cities*

- Streetlights dim is based on ambient conditions to save energy costs.
- Real time updates for passengers via smart devices or display board.
- Self-driving autonomous vehicles enabling increased safety, reduced CO_2 emissions, more leisure and work time for motorists.
- Smart traffic lights using cameras at every signal, increasing average speed in the city.
- Street cameras reduce crime and enable faster emergency response times.
- Pay-as-you-drive car insurance charges users according to driving behavior and can enable substantial savings for drivers.

B. *Education*

- Students do not need to carry heavy books in a backpack. All school materials are loaded on the smart device.
- From the same smart device, you can connect to classmates and teachers to share knowledge and work collaboratively.
- Self-directed learning enables adults to address their skills gaps and engage in lifelong learning at a click of a button.

C. *Productivity*

- Management meetings are fact-based and use real-time data to make informed decisions.
- Proximity is no longer a challenge, cutting-edge video conferences enable easy communications
- When there is a purchase, the closest production factory to the customer is alerted and the customized item is created and delivered with minimum delay, avoiding inventories and the keeping the client satisfied
- Some items can be produced at home, using a 3D printer [1].
- Refrigerators lets you known when you are short of groceries [9]
- Your “smart” umbrella lets you know it would rain[9]

D. *Crowd control*

- A crowd control application will allow relevant authorities to estimate the number of people gathering at event sites and determine if necessary actions need to be taken during an emergency.
- Using location-based technologies such as cellular, WiFi and GPS, the application will generate virtual “heat maps” of crowds.
- These maps can be combined with sensor information obtained from street cameras, motion sensors and officers on patrol to evaluate the impact of the crowded areas.
- Emergency vehicles can also be informed of the best possible routes to take, using information from real-time traffic sensor data, to avoid being stuck among the crowds.

E. *Intelligent Lampposts*

- The intelligent streetlamp is a network of streetlamps that are tied together in a WAN that can be controlled and monitored from a central point, by the city or a third party.
- It captures data such as ambient temperature, visibility, rain, GPS location and traffic density

which can be fed into applications to manage road maintenance operations, traffic management and vicinity mapping.

F. Retail and Supply Chain

- In the retail sector, shopping assistant applications can be used to locate appropriate items for shoppers and provide recommendations of products based on consumer preferences.
- The application can reside in the shopper's personal mobile devices such as tablets and phones, and provide shopping recommendations based on the profile and current mood of the shopper.
- Using context-aware computing services, the application captures data feeds such as promotions, locations of products and types of stores, either from the malls' websites or open API if the mall allows it.
- Using the dynamic ordering tool, the network of smart objects will identify the types of commodities and decompose the order picking process to distributed sub-tasks based on area divisions. The application will plan the delivery routes centrally.

G. Healthcare

1) Elderly Family Member Monitoring

- This application creates the freedom for the elderly to move around safely outdoors, with family members being able to monitor their whereabouts.

2) Continuous and remote Patient Monitoring

- Continuous and remote patient monitoring requires the use of medical body sensors to monitor vital body conditions such as heartbeat, temperature and sugar levels. The application examines the current state of the patient's health for any abnormalities and can predict if the patient is going to encounter any health problems.

3) Smart Pills

- Smart pills are essentially ingestible sensors that are swallowed and can record various physiological measures.

4) *Tracking of medical items and information gathering*

- Tracking of drugs from manufacture to patient.
- Tracking of hospital equipment and instruments.
- Restriction of staff access and control of cross infection.
- Advance telemetry of inbound patient clinical data to hospital.
- Lifestyle and fitness monitoring as part of wellness program.

H. Transportation

a) Special Needs and Elderly Transportation Assistant

- The transportation assistant application serves to address the group of commuters with special needs and who require assistance as they commute using public transportation.

b) Accident Avoidance Detection

- The promise of IoT enhancing life for individuals and society has been shown in small-scale projects, such as the addition of GM OnStar to GM's cars. This automatically detects when the car has been in a collision, calls for assistance and provides the emergency services with the location [7].
- Vehicles can play a part in providing better road safety by monitoring and sensing each other on the roads.
- Monitoring traffic jams through cell phones of the users and deployment of intelligent transport systems (ITS) will make the transportation of goods and people more efficient.
- Transportation companies would become more efficient in packing containers since the containers can self- scan and weigh themselves. Use of IoT technologies for managing passenger luggage in airports and airline operations will enable automated tracking and sorting, increased per-bag read rates, and increased security [18].

I. Energy and Utilities Management

a. Facilities Energy Management

- Facilities energy management involves the use of a combination of advanced metering and IT and operational technology (OT) that is capable of tracking, reporting and alerting operational staff in real time or near real time.

b. Home Energy Management/Consumer Energy Management

- Home energy management (HEM) optimizes residential energy consumption and production.
- With integration of data, customers can understand their bills better and energy companies can relate better with customers and give better advice using facts gathered from user data.

J. Logistics Industry

- Logistics companies are tapping on traffic patterns, road congestions information from road cameras and sensors and early knowledge of weather conditions to make constant routing adjustments for their delivery

trips. This cross-domain information helps them increase their delivery efficiencies and reduce overall congestion costs [5].

K. Wildlife Conservation

- One innovative IoT solution is connecting endangered black rhinoceroses in eastern and central Africa to this global network. Each is given an ankle collar that relays movement and exact geo-location data back to anti-poaching teams that can quickly act if poaching is suspected [7].

L. Nomadic Farming

- IoT can help a Fulani or Maasai herdsman track the movement of his cattle real time, from the comfort of his hastily-erected hut, through his mobile phone. He can then call up a weather application, which gives him advice on where the best grazing area is, and where to water his livestock.
- While miles away, agricultural officials huddle over a screen keep track of the movement of nomadic communities and can make a quick call to community elders if they sense that conflict can take place when two herding groups meet. Danger can thus be avoided [9].

M. Aerospace and Aviation Industry

- IoT can help to improve safety and security of products and services by reliably identifying counterfeit products and elements. Aviation authorities report that at least 28 accidents or incidents in the United States have been caused by counterfeits [16]. It is possible to solve this problem by introducing electronic pedigrees for certain categories of aircraft parts, which document their origin and safety-critical events during their lifecycle (e.g., modifications). In this way, safety and operational reliability of aircrafts can be significantly improved [18].

N. Pharmaceutical industry

- Drug tracking and e-pedigrees allow for the detection of counterfeit products and keep the supply chain free of fraudsters.
- The smart labels on the drugs can also directly benefit patients, e.g. by enabling storing of the package insert, informing consumers of dosages and expiration dates, and assuring the authenticity of the medication.
- In conjunction with a smart medicine cabinet that reads information transmitted by the drug labels, patients can be reminded to take their medicine at appropriate intervals and patient compliance can be monitored [18].

O. Petroleum Industry

- IoT can help in reducing the number of accidents in the oil and gas industry by equipping the containers of hazardous chemicals with intelligent wireless sensor nodes.
- Wireless monitoring of petroleum personnel in critical onshore and offshore operations, container tracking, tracking of drill string components pipes, monitoring and managing of fixed equipment, etc.

P. Agriculture and Breeding

- With the application of identification systems, animal diseases can be controlled, surveyed, and prevented. Official identification of animals in national, intra community, and international commerce is already in place, while at the same time, identification of livestock that are vaccinated or tested under official disease control or eradication is also possible. Blood and tissue specimens can be accurately identified, and the health status of herds, regions, and countries can be certified by using IoT.
- With the Internet of Things, single farmers may be able to deliver the crops directly to the consumers not only in a small region like in direct marketing or shops but in a wider area. This will change the whole supply chain which is mainly in the hand of large companies now to a more direct, shorter chain between producers and consumers [18].

Q. Insurance industry

- If insurance clients are willing to accept electronic recorders in their car, which are able to record acceleration, speed, and other parameters, and communicate this information to their insurer, they are likely to get a cheaper rate or premium [17]. The insurer can save money by being involved in a very early stage of an impending accident and can trigger the most economic actions.

R. Recycling

- IoT and wireless technologies can be used to advance the efficiency and effectiveness of numerous important city and national environmental programs, including the monitoring of vehicle emissions to help supervise air quality, the collection of recyclable materials, the reuse of packaging resources and electronic parts, and the disposal of electronic waste (RFID used to identify electronic subcomponents of

PCs, mobile phones, and other consumer electronics products to increase the reuse of these parts and reduce e-waste)[18].

S. *Security*

- To fight against terrorist groups African armies can use connected Drones to get images of the field with low risk for soldiers. There are drones of all sizes, types, characteristics and color. A drone with a connected camera and a large wide range can send thousands of images of a dangerous field.
- The same drone can also be used for internal surveillance against security threats such as kidnapping, pipeline vandalism, armed robbery, violent riots, etc. In Natural parks, poaching can be fought by connecting localization devices on species like Rhinoceros and elephants.

VII. CONCLUSION

This paper introduces the reader to the emerging Internet of Things phenomenon. It describes the different properties that make up the technology and highlights the layers that make up its architecture. These technologies include the Sensor layer, Gateway and Network layer, Management Service layer and Applications layer.

The key IoT enabler in Africa as well as its current state of deployment and Machine-to-Machine connection in Africa is then explored. Specific examples of IoT deployment is given, while future trend in the industry is forecasted. Thereafter, challenges to the development of the phenomenon are highlighted. Such challenges include: scalability, interoperability and standards, data management and software complexity, power supply, cost over usability, network capacity constraints, illiteracy and lack of local content, trust, security and privacy issues among others. Solutions to these challenges are also suggested.

In addition, areas of applications of Internet of things are briefly described. These areas include: education, transportation, productivity, health care, insurance, supply chains, government, retails, energy management, wildlife conservation, aerospace and aviation industry, pharmaceutical and petroleum industries, agriculture, waste management, security and so on.

REFERENCES

[17] GSM Association, "Understanding the Internet of Things (IoT)", Connected Living Series, New Fetter Lane, London UK, pp. 1-10, July 2014

[18] Friedemann Mattern and Christian Floerkemeier, "From the Internet of Computers to the Internet of Things" Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich, pp. 2-18

[19] Lopez Research, "An Introduction to the Internet of Things (IoT) - Part 1. of *The IoT Series*", Lopert Research LLC, Chestnut Street, San Francisco, CA, pp. 2-6, November 2013

[20] John Wilhite, Shahram Mehraban, "Critical Factors for Successful Internet of Things Deployment", Automation World, http://www.automationworld.com/industrial-internet-things/critical-factors-successful-internet-things-deployment(2015)

[21] Info-communications Development Authority of Singapore, "The Internet of Things (IoT)", https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/InternetOfThings.pdf(2015)

[22] GSMA Intelligence, "The Mobile Economy Sub-Saharan Africa 2014", http://ssa.gsmamobileeconomy.com(2015)

[23] Finbarr Toesland, "Will Africa take the lead in the Internet of Things?" African Business, http://africanbusinessmagazine.com/sectors/infrastructure/will-africa-take-lead-internet-things/(2015)

[24] Team True – True Africa, "Cina Lawson-Togo Digital Minister on Internet of Things", http://trueafrica.co/article/cina-lawson-togos-digital-minister-on-the-internet-of-things/(2015)

[25] Lee Mwiti, "Not pie in the sky—the 'Internet of Things' is already with us in sub-Saharan Africa. We think", http://mgafrica.com/article/2015-07-22-not-a-pie-in-the-skythe-internet-of-things-is-already-with-us-in-sub-saharan-africa-we-think(2015)

[26] E Cloete, "MTN Business launches the first Pan African Internet of Things (IoT) platform", http://www.mtnblog.co.za/mtn-business-iot/

[27] MTN Business, "Machine to Machine (M2M)", http://www.mtnbusiness.com.ng/services-solutions/m2m(2015)

[28] Odulaja G.O, Awodele Oludele, Kuyoro Shade.O, "Security Issues in the Internet of Things", Computing, Information Systems, Development Informatics & Allied Research Journal, Vol. 6 No. 1. March 2015 – www.cisdijournal.net

[29] Joao Lima, "5 challenges facing the Internet of Things", Computer Business Review, http://www.cbronline.com/news/internet-of-things/5-challenges-facing-the-internet-of-things-4540286 (2015)

[30] Goldman Sach Group Inc. "The Internet of Things: making sense of the next mega trend", September 2014

[31] Wind River Systems Inc., "Security in the internet of things-lessons from the past for the connected future"

[32] CTV Deadly Fakes- CTV News, http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20020306/ctvnews848463(2015)

[33] V. Coroama, "The smart tachograph - individual accounting of traffic costs and its implications", Proceedings of Pervasive, pp. 135 - 152, Dublin, Ireland, May, 2006

[34] Debasis Bandyopadhyay, Jaydip Sen, "Internet of Things - Applications and Challenges in Technology and Standardization", Innovation Labs, Tata Consultancy Services Ltd. Kolkata, India, pp. 15-20, May 2011

[35] http://www.statista.com/statistics/203708/global-handset-penetration-per-capita-since-1996/

Novel Solution for Addressing Identity Theft and Cheating in Electronic Examinations using Mouse Dynamics

Meshach Baba and Victor Legbo Yisa
Department of Cyber Security Science
Federal University of Technology, Minna, Nigeria
babameshach01@futminna.edu.ng, victor.yisa@futminna.edu.ng

***Abstract*—Conducting examinations electronically has gained a lot of acceptance in the educational sector especially in Nigeria tertiary institutions; the complexity of electronic examinations has made it very difficult to verify the identity of students compared to writing exams in the traditional environment. In order to get good scores, an impostor may be used to write the exam for the student. This paper proposes the application of a continuous behavior-metric user authentication in electronics examination via mouse movement dynamics that will verify the identity of a student writing an electronic examination by comparing his mouse movement against the one in his profile. The proposed system will also be able to detect the identity of the imposter.**

Keywords*—e-examination; examinee; imposter; authentication; integrity; security; continuous mouse movement.*

I. INTRODUCTION

E-exam platform is a tool that is understood to advance the quality and equity in education by offering objective evaluations of written exams and equal access to anyone [1]. The platform has been able to reduce cost and time it takes for examination results to be ready. Due to the several benefits attached to e-examination, a large number of tertiary institutions around the world are now making use of it and Nigeria institutions are not exception.

The adoption and proliferation of information technology (IT) into tertiary institutions in Nigeria in conducting e-examination has been an area of interest for researchers over some years back, especially the security(authenticity and integrity) aspect. E-examination engages several parties such as the candidates, examiners, invigilators, examination authorities, information systems, thereby making it a complex and difficult system to deal with.

Several researches have been carried out on examination data at rest and in motion [2]; login in to a system through traditional means of authentication using username and password [3]; through the use of different form of Biometric security mechanism such as physiological mechanism (for example hand geometry, face, fingerprints, and iris) [4] [5] [2] [6] and behavioral mechanism (such as voice, signature, and keystrokes) [7] [8] [9].

Although most researchers have carried out their research in the area of authentication when candidate's login into the system, little research has been carried out in the area of what happens after the candidate's login into the system and how the identity of an imposter can be known when one is detected. Therefore, the integrity and authenticity of e-examination can still be compromise by some of the parties involved with the examination process. To eliminate this loophole, a new form of authentication is required.

Despite several researchers that have been carried out on e-examination, most researches have failed to address one major area which is the identification of the person who tries to impersonate someone within the examination venue.

Also a major challenge to the integrity of the e-examination within Nigeria institutions is that students do not get to see their results immediately as their results may take days to weeks to be released [2], thereby creating room for manipulation of results.

The research work is to propose a design of e-examination platform that will make use of continuous mouse dynamics that will continuously record and compare data from the mouse movement to the one already stored in the database. Also incorporated into the design will be the ability of detecting the impersonator within the examination center. The design will also enable the students to see their results immediately at the end of the exam. The result will also be automatically encrypted and stored on the database with a copy of the result mailed to the respective email address of the respective candidate immediately.

The main purposes of this research work are:

A. To design a system that will eliminate cheating by candidates and some dubious supervisor(s) after the candidate login into the e-examination platform through the use of continuous mouse movement monitoring and few cameras in the examination hall.
B. To detect and identify the identity of anyone that is trying to impersonate another candidate by comparing and analyzing the imposter's mouse movement logs with that on the database
C. To design a system that will prevent manipulation of candidates result at the end of each examination by storing encrypted result in the database and forwarding the result to the students and the administrative email immediately signed with digital signature

This research work will be limited to processes that take place during the conduction of the e-examination, but will not be considering the security aspect of the examiners, administrative personnel and examination questions

This paper is organized as follows: Section II describes background and related work. Section III presents the design and description of the system. Section IV discusses the Discusses the system and future work.

II. USER AUTHENTICATION

Authentication is used by all secure systems to ensure the confidentiality, authenticity integrity and availability of any document within it. It is always used as the first means of defense in any environment to secure systems against unintended use [10]. Since authentication is used in verifying and validating the identity of a person that is trying to access a particular resources in a secure system, it is now been implemented as the first line of defense by most e-examination platform to secure and protect the resources meant for students, lecturers, admin against malicious use.

A. Authentication Methods

There are several authentication methods in use today, but they can all be categorized into three factors (1) Knowledge Factors (2) Ownership Factors and (3) Inherence Factors [10] [11].

i. **Knowledge Factors:** This authentication factor has to do with something the user of any particular system knows. Examples of such type authentication are: password, pass phrase, challenge response (the user answer some predefine question) or personal identification number (PIN).

ii. **Ownership Factors:** this is a piece of device that the user of a system **has** such as cell phone, security token, wrist band, software token, phone, or ID card.

iii. **Inherence Factors:** this authentication factor is divided into something the user **is** or **does.** Examples of something the user **is** are DNA sequence signature, fingerprint, voice, retinal pattern, face, unique bio-electric signals while examples of something the user does are mouse movement mechanism and keystroke.

B. Advantages and disadvantages of each authentication method

Some of The weaknesses in each of the authentication method are discussed in Table 1 below.

Table 1 *Advantages and disadvantages of each authentication method.*

Factors	*Strength*	*Weakness*
Knowledge Factors	• Very low cost • Portability • familiar to users • No special equipment	• susceptible to sniffing • susceptible to brute force attack • can be guessed • User memory burden • Easily phishable • Cannot be use for continuous user authentication
Ownership Factors	• good usability • better security than knowledge factor • resistant to phishing and credential theft	• Can be stolen • More expensive than knowledge factor due device cost • More expensive to implement • Limited capabilities against advanced threats • Limited capabilities against advanced threats • Cannot be use for continuous user authentication
Inherence Factors	• better general security • No user memory burden • resistant to phishing and credential theft	• Low level of Acceptance due to privacy issues • High cost • Difficult to implement. • Enrollment process

Although most of the weaknesses highlighted in each of the authentication method in Table 1 can be eliminated by combining two more factors of authentication. Although, most combinations cannot be use for continuous authentication of examinee, some few of them can be use for it. Therefore, most authentication types will create loopholes that can compromise the integrity and authenticity of the e-examination as another examinee may help another person within the examination hall.

C. Mouse Biometric Authentication

Mouse biometric authentication makes use of the behavioral attributes of subject, when he/she is making use of the mouse. Since the way each person makes use of the

mouse while using the system is unique to each an individual. Therefore, attributes on how each person makes use of the mouse can be use in identifying the person. All biometric authentication system always involve two phases; the enrollment phase where the attributes of the subject mouse movement are collected and stored; and the verification phase which involves the identification of the subject by comparing the present attributes with the attributes stored in the database as enrollment signature [12].

1) Acquisition and Extraction Feature

Low level mouse events such as button up and button down, raw movement events generated by the mouse are intercepted and captured through the use of a software program. Several attributes such as event type, mouse action type, timestamp and cursor coordinates may be associated with each of the event. These low level mouse events are first aggregated and converted into high level abstraction (e.g. drag-and-drops, point-and-clicks, Common Movement, Silence, single click, double click etc.) in other to detect meaningful behavioral patterns that can be use in identifying a person [9] [12]. These features are extracted from each student during their first semester registration in the school.

III. RELATED WORK

[2] proposed the use of encryption for the exchange of examination questions and e-examination center when either internet or intranet is used. They went further to propose the use of fingerprint authentication biometric scheme to authenticate all the stakeholders involved with the examination.

[10] proposed the use of two authentication scheme, username/password with palm-based biometric authentication scheme to authenticate examinee, in both online-based and computer-based. They went further to incorporate the use of video capturing technique to improve the authenticity and integrity of the e-examination process.

[13] Designed a profile based authentication framework (PBAF) for secure online examination that comprises of two layer authentication. The first layer consists of the username and password and the second being the challenge questions. The username and password is used to login in into the online environment, and challenge questions are asked based on the students profile to ascertain the user, a user is not authenticated if answers to the challenge questions is in conflict with that in the students profile.

[14]also designed a system a system that continuously verify the authenticity of a candidate by comparing captured images with already stored images in the encrypted image bank collected during the registration period. If image captured during examinations do not match that in the image database captured for the user, a mismatch is declared and the candidate is not authenticated. Also to curb cheating in the examination hall, the system will warn the candidate if he is found not to be focused on the examination and is looking sideward's.

[8] Designed a Continuous Biometric User Authentication in Online Examinations. The system will continuously monitor the activities of the student by monitoring of the key stroke dynamics of the student. For the purpose of continuous monitoring, they considered some important metrics which can be recorded and used for user verification e.g. Typing speed; Keystroke seek-time; Flight-time; Characteristic sequences of keystrokes; and Examination of characteristic errors. The student keystrokes are identified based on these metrics at the point of registration and is stored in a database, these metrics are then compared with a new signature generated by the student during the examination.

IV. E-EXAMINATION SCHEME SECURITY REQUIREMENTS.

In other to have a successful e-examination, each stage of the examination must be secure. The various stages in e-examination are 1) preparation phase 2) examination enrolment and admission 3) examination conduction and 4) result announcement. The success of each examination starts from when students register for the courses (which proves whether an examinee will be eligible to write the exam), to when the results are announced. The security requirement for an examination schemes are confidentiality, authenticity, integrity and non-repudiation.

Confidentiality: only eligible exam participant should be allowed to see the questions and the result. And it should also be at the specified period of time. This means examinee should not be allowed to view examinations questions until it is time to write such examination paper and the examinee has been properly authenticated. The only examination participant that should be allowed access to the questions apart from the authenticated examinee should the lecturer (the examination participant that sets the questions) except in the case of external examination moderator been involved.

Integrity: The originality of the questions and results is of paramount importance whenever the issue of e-examination is raised. How do we know the questions are sent from course lecturer? Or was the question altered on transit? Or can someone change the result of a student? For an examination to be called a success, integrity of both the examination questions and students results must be maintained.

Non-Repudiation: for e-examination to be a success, the system should be able to hold each participating member accountable for their actions. This will prevent the examinee from denying not to have performed some certain actions (claiming not to be the person that wrote the exam). The e-examination system should also have the capability of preventing the examiner of denying the original questions sent by him to the e-examination system.

Authenticity: this should ensure that the identities of all participants of the examination are properly verified and

that they are granted access to only information that they are authorized to access and at the appropriate time.

V. PROPOSED E-EXAMINATION SYSTEM

The proposed system, shown in Figure 1, will make use of continuous mouse monitoring system with username and password to authenticate the examinee. The system will work in conjunction with few CCTV cameras placed at strategic location within the examination hall.

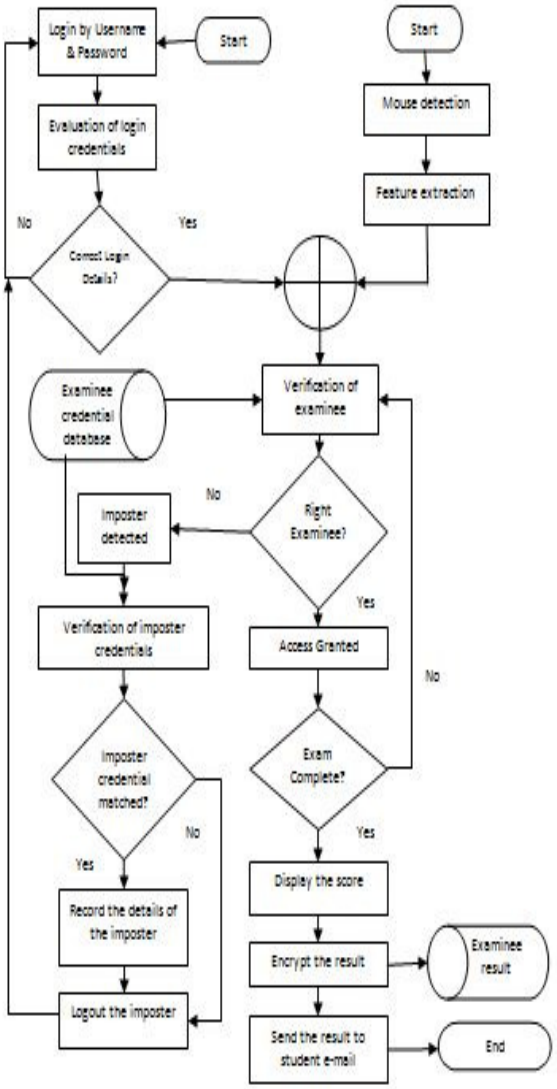


Fig. 1: *Proposed e-examination system with continuous authentication scheme.*

A. Design consideration

In designing the e-examination system, cost implication, confidentiality, authenticity, integrity and non-repudiation were considered and some assumptions were made.
The following assumptions were made.

Assumption 1: It was assumed that during the registration of the student, information's such as the courses qualified and registered for; name, student identification number and the department are stored on the database, which is important for authentication and detecting the identity of the imposter.

Assumption 2: It was also assumed that the mouse biometrics features for each student have been extracted and stored in the database before the day of the examination. Also, that the student has created username and password alongside their profile during this process.

Assumption 3: it was assumed that all connections between the database and any connecting device is using HTTPS as the connecting protocol

B. Authentication

Authenticating an examinee during an examination should not just end after he/she has been logged in into the system but ensuring the right examinee is taking the examination throughout the duration of the examination is necessary to avoid cheating. The propose system is shown the figure 1.0 above. The propose system will make use of two multimodal authentication method to log in examinee into the system. The authentication methods to be use are username and password in combination with continuous mouse movement monitoring.

When the examinee runs the application for the e-examination platform, he/she will be asked to enter a username and password to be authenticated first, but will be forced to use the mouse as the mouse cursor will be placed at the extreme end. Also after the user have authenticated, he/she will be ask to perform some few task with the mouse like selecting his/her faculty and department before been authorize to access the examination questions. These steps will allow necessary mouse movement features of the examinee to be collected and compared with the one on the database, before granting the candidate the authorization to write the examination. To achieve this, the username and the password of the authenticated examinee are compared with features extracted from the mouse movement with what is stored on the database to find a match. If the examinee is found to be a legitimate person for the credentials verified, he/she is authorized to write the examination, otherwise the system logouts the person. The MAC address of the system been use by the examinee with date and time the exam begins are stored in the database, when the exam ends, the time will also be recorded by the system

Throughout the duration of the examination of the examinee, the mouse movement software keeps running behind the scene to verify if the authorized examinee is still the person taking examination. If the answer is yes, the software checks if the examination time has expired or the examinee has ended the examination and if yes, the software stops extracting and comparing the features of the examinee.

.

C. Imposter Identification

If at some point during the examination, the features extracted from the authenticated examinee do not match with what is stored on the database, the system will flag the examinee as an imposter.

Since the system as discovered the presence of an imposter writing the examination, the features extracted from the imposter is compared with what is stored on the database to discover the identity of the imposter.

After the identity of the imposter has been discovered, the names, student identification number and the student department of both the imposter and the examinee are stored in the database labeled as cheat. The system will allow the imposter to continue with the exam for a short period of time as the system alerts the appropriate authority immediately. Though, if the short period of time frame given expires, the system automatically logs out the imposter and prevents him/her from login into the system with the same login credentials.

We propose the use of a mobile device by the proctors. This device will receive an alert indicating the presence of an imposter with all the information regarding the imposter and the system been used by the person. The device will only receive alert but will not be able to perform any other action. This will help the authority in catching the imposter during the act.

The presence of CCTV cameras will also help in validating the alert from the propose system, as the imposter cannot later deny not to have used that system at that particular period of time.

D. Result integrity

Immediately the examinee clicks the submit button on his/her examination platform, the results are encrypted and sent to the database through a secure channel of https using secure socket layer (SSL). The result is then displayed on the screen for the student to see but subject to final validation from the examination management.

The system will make use of public key cryptographic encryption scheme. The public key will take action when the student click submit button. The result can only be decrypted by the person authorized to use the private key.

The system will attach the MAC address of the system used by the examinee with the time and date he/she took examination. These values can letter be compared with what was recorded when the examinee was authenticated and authorized to write the examination. This feature will allow the detection of any manipulation of the results by third party as the timestamp will change and the mac address may also change if different system was used.

VI. CONCLUSION

In this paper, we have proposed a secure e-examination system that can be use in ensuring the authenticity, non-repudiation and integrity of the exam. The paper proposes the use of username and password with continuous mouse movement to authenticate and continuously ensure that the authenticated examinee remain the person writing the examination throughout the duration of the exam. The system uses the features of the continuous mouse movement to detect the identity of the imposter, thereby ensuring the integrity of the examination throughout. The system also uses some few CCTV cameras to monitor the activities of all the parties involved, therefore ensuring non-repudiation by the parties involved. We also propose the use of public key cryptographic algorithm to ensure that the integrity of the result is not compromised. Some features such as the time of login and logout; MAC address of the system are added to the result before encryption, which can be compare with similar feature stored in the database when the examinee logs into the system

REFERENCES

[1] R. Giustolisi, G. Lenzini, and G. Bella, "What Security for Electronic Exams? (Extended Abstract)," in *International Conference on Risks and Security of Internet and Systems (CRiSIS)*, 2013.

[2] O. Adebayo and S M Abdulhamid, "E- Exams System for Nigerian Universities with Emphasis on Security and Result Integrity," *International Journal of the Computer, the Internet and Management (IJCIM)*, vol. 18, no. 2, pp. 47.1-47.12, 2014.

[3] X. Ren and X. Wu, "A Novel Dynamic User Authentication Scheme," in *International Symposium on Communications and Information Technologies (ISCIT)*, 2012, pp. 713-717.

[4] M. M. Ramim and Y. Levy, "Towards a Framework of Biometric Exam Authentication in E-Learning Environments," in *Managing Worldwide Operations & Communications with Information Technology*, 2007, pp. 539-542.

[5] T. Ramu and T. Arivoli, "A Framework of Secure Biometric Based Online Exam Authentication: An Alternative to Traditional Exam," *International Journal of Scientific & Engineering Research*, vol. 4, no. 11, pp. 52-60, 2013.

[6] S. M. Al-Saleem and H Ullah, "Security Considerations and Recommendations in Computer-Based Testing," *The Scientific World Journal*, pp. 1-7, 2014.

[7] P. Bours and C. J. Fullu, "A Login System Using Mouse Dynamics," *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1072-1077, 2009.

[8] E. Flior and K. Kowalski, "Continuous Biometric User Authentication in Online Examinations," in *Seventh International Conference on Information Technology*, 2010, pp. 488-492.

[9] C Shen, Z Cai, and X Guan, "Continuous

Authentication for Mouse Dynamics: A Pattern-Growth Approach," in *Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP International Conference on*, Boston, MA, 2012, pp. 1 - 12.

[10] Y. Sabbah, I. Saroit, and A. Kotb, "An Interactive and Secure E-Examination Unit (ISEEU): A Proposed Model for Proctoring Online Exams," in *10th Roedunet International Conference (RoEduNet)*, 2011, pp. 1-5.

[11] A E Monge, "Matching Algorithms within a Duplicate Detection System," in *blletin of the IEEE Computer Society Technical Committee on Data Engineering.*, 2000.

[12] Z. Jorgensen and T. Yu, "On Mouse Dynamics as a Behavioral Biometric for Authentication," in *ASIACCS*, Hong Kong, China, 2011, pp. 476-482.

[13] Abrar Ullah, Hannan Xiao, Mariana Lilley, and Trevor Barker , "Using Challenge Questions for Student Authentication in online Exainations," *International Journal for Infonomics*, vol. 5, no. 3/4, pp. 631-639, 2012.

[14] Ayham Fayyoumi and Anis Zarrad, "Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems," *Advances in Internet of Things*, vol. 4, pp. 5-12, 2014.

Digital Forensic Analysis for Enhancing Information Security

Ojeniyi Joseph Adebayo, Idris Suleiman & Abdulmalik Yunusa Ade
Department of Cyber Security Science
Federal University of Technology
Minna, Nigeria
Ojeniyija@futminna.edu.ng
Adenijiadedapobolaji@yahoo.com, Sidris27@gmail.com

Ganiyu, S.O, and Alabi, I.O
Department of Information and Media Technology
Federal University of Technology
Minna, Nigeria
Shefiu.ganiyu@futminna.edu.ng
Isiaq.alabi@futminna.edu.ng

***Abstract*— Digital Forensics is an area of Forensics Science that uses the application of scientific method toward crime investigation. The thwarting of forensic evidence is known as anti-forensics, the aim of which is ambiguous in the sense that it could be bad or good. The aim of this project is to simulate digital crimes scenario and carry out forensic and anti-forensic analysis to enhance security. This project uses several forensics and anti-forensic tools and techniques to carry out this work. The data analyzed where gotten from result of the simulation. The results reveal that although it might be difficult to investigate digital crime but with the help of sophisticated forensic tools/anti-forensics tools it can be accomplished.**

***Index Terms*— Digital forensic, anti-digital forensic, image acquisition, image integrity, privacy.**

I. INTRODUCTION

Forensic Science is the science that deals with evidence presentation using scientific processes; while Digital forensic is a branch of Forensic Science that deals with careful extraction or mining of digital evidence that has probative value within a predefined scope in such a way that it can be admissible in the court of law without doubt or question being raised about its integrity.

Due to human inherent nature to invade and circumvent justice they make digital evidence acquisition difficult and almost impossible using some counter measure known as anti-digital forensics (or just anti-forensic). Anti-forensics is the means of thwarting forensic processes there by making forensic processes difficult, impossible or by delaying it and frustrating the forensic investigators and forensic tools. The rest of the paper is organized as follows: Section 2 presents related work, and two case studies are defined and experimentally investigated all through Sections 3 to 6. Section 7 concludes the paper.

II. RELATED WORKS

A. Enhanced Information through Forensics

Given that there are anti-forensic tools that can obfuscate, minimize or eliminate attack footprints, forensic analysis becomes harder [1].

In their work, Changwei, Anoop, and Duminda [1] aimed to use attack graphs in forensic examinations. The methodology they used included anti-forensic capabilities into attack graphs, so that the missing evidence can be explained by using longer attack paths that erase potential evidence. At the end of their work they were able to show how attack graphs could be used to help forensics investigators narrow down potential attack scenarios, along with evidence left by attackers. Observable limitation of their work from the anti-forensic techniques/tool vulnerability tools they used is the TrueCrypt. Most attackers no longer use TrueCrypt because of their presence it leaves as systems trace on the boot loader.

Balogun and Shao [2] in their work examined what data encoding adds to information security and then spotted out its influences on the digital forensics of disk drives. The purpose was to converse the obtainable methods and tools, in digital forensics, to find solutions to the problems posed by encryption. They used TrueCrypt as case study for their encryption solution to illustrate their ideas being conversed. They further talked about some features of TrueCrypt software that provides users with plausible deniability and non-repudiation abilities. This makes digital forensics examinations of encrypted disk drives stiffer and less actualaizable. The limitation in their work is the TrueCrypt boot loader traces.

Benjamin [3] researched on "Modelling and refinement of forensic data acquisition Specifications" his aim was to "defines a model of a special type of digital forensics tools, known as data acquisition tools" the intention of his work was to give a formal description against which implementations of data collecting procedures can be analyzed. The approach he used was the formal refinement language Event-B (Event-B of the data acquisition functionality of digital forensics tools). Event-B is an extension of Abrial's B method Abrial (1996) for modeling distributed systems.

B. Enhanced Information Security through Anti-Forensics

Changwei, Anoop and Duminda [1] worked on "A Model Towards Using Evidence From Security Events For Network Attack Analysis". They aim at "how to use the information obtained from security events to construct an attack scenario

and build an evidence graph." And the objectives of their works were "To achieve the accuracy and completeness of the evidence graph, to correlate evidence by reasoning the causality, and use an anti-forensics database and a corresponding attack graph to find the missing evidence", the methodology they employed where: prolog inductive reasoning, abductive reasoning, global reasoning and mapping the evidence to a logical attack graph to construct an evidence graph for network forensics analysis. And they arrived at having a proposed network forensics model, which extends a Prolog logic based system, MulVAL, to automate the causality correlation between evidence collected from security events in an enterprise network.

Johannes and Michael [4] researched on a work titled "Anti-forensic resilient memory acquisition" their objectives were:

i. To examine a number of simple anti-forensic techniques and test a representative sample of current commercial and free memory acquisition tools.
ii. To find out if current tools are resilient to very simple anti-forensic measures.
iii. To present a novel memory acquisition technique
iv. To then evaluate this technique's further vulnerability to subversion by considering more advanced anti-forensic attacks. The method they used was based on direct page table manipulation and PCI hardware introspection, without relying on operating system facilities.

The limitation of their work is its reliance on the operating system on finding the page tables in the first place. All addresses in CR3 and Page Tables are physical addresses.

Przemyslaw and Elias [5] carried out research on "Computer Anti-forensics Methods and Their Impact on Computer Forensic Investigation", the aim of their research was to test whether current known counter-forensics technology can efficiently interfere with computer forensics processes. And their major objectives was toward exploring the anti-forensics problem in various stages of computer forensic investigation from both a theoretical and practical point of view, To identify the most known computer anti-forensic techniques and test practically them against computer forensic software. They proved that not all counter-forensics techniques are efficient when compared against forensics software. Their major limitation was that the research was not carried about each individual technique against a range of different forensic tools. Also, the various anti-forensics techniques was not evaluated against packages specifically designed for detection of those techniques in order to develop a much clearer opinion as to whether it is possible to beat counter forensics.

C. *Enhanced Information Security through Counter-Anti-Forensics*

Marco, Alessandro, Alessandro, and Mauro [6] Carried out a work on "Countering Anti-Forensics by Means of Data Fusion". With the aim of analyzing analyze the possibility offered by the adoption of a data fusion framework in a Counter-Anti-Forensic (CAF) scenario". The methodology they employed was a theoretical framework, based on Dempster-Shafer Theory of Evidence. Their objectives were:

i. To synergically merge information provided by Image Forensics (IF) tools and Counter Anti-forensics (CAF) tools.
ii. To reveal traces introduced by anti-forensic algorithms.
iii. To account for the non-trivial relationships between IF and CAF techniques.
iv. To evaluate the proposed method within a representative forensic task, that is splicing detection in JPEG images, with the forger trying to conceal traces.

The limitation of their work was that they did not take into account the following facts:

i. IF tools may be searching for mutually exclusive traces, so some combinations of tool outputs could be excluded.
ii. For a given footprint, IF and CAF algorithms are expected to be in contradiction, so if both kinds of tools detect their footprint this should at least raise some doubts about the correctness of the outputs.
iii. Detecting some kinds of anti-forensic processing does not necessarily imply that the image is a fake.
iv. They were able to arrive at investigating the use of data fusion as a tool for countering Anti-forensics.

III. METHODOLOGY

A. *Introduction*

Before any forensic investigation can be carried out, there must have been a case at hand that needs evidence - especially evidence(s) relating to electronic media. As computer forensic examiners or investigators we have to beware of possible circumventing techniques that computer criminals employ to defeat digital forensic approach known as Anti-forensic; but the aim of this work is to make the forensic examiner to be pro-active in conducting proper and using reliable techniques and this pro-activity is the sole aim of this work. It will be un-wrapping some things the investigator has to put under consideration before, during and after forensic examination.

In this paper it is assumed that an actual crime that involves and greatly relies on digital evidence has actually occurred, some of the problem or cases this paper would be providing solution to would be done through forensic anti-forensics analysis. This would be better understood by analyzing and providing solution to the following fictitious cases assumed.

B. *Assumed Case*

In Federal University of Technology Minna, there was a law that nobody should for any reason copy any of the institution's file without authorization, but a disgruntled employee who has being asked to resign was caught copying some relevant files into his personal laptop from one of his colleague's company

computer whom he had quarrel with recently, as a result of his misconduct and his unethical behavior toward work and other staff. When his colleague caught him, he denied it in the presence of others and when his system was searched by the rest colleagues they found nothing incriminating or any unauthorized file in his possession pertaining to FUTMinna, and now a forensic investigator has being brought to the scene to help out, with the analysis.

Virtual environment would be used to simulate this crime, and the target offender's machine would be assumed to be running window 7, any windows operating system would work just fine as some of the tools used has also been tested with window 8 and window XP they all work fine, most of the tools used to carry out the analysis are operating system independent – meaning Linux, Solaris or apple IOS are not exceptional, the sharp difference between them boils downs to the their differences in File Systems, network configuration and their memory management. The methodology used in this work will be broken down into: Volatile data analysis and Non-volatile/persistent data analysis.

Before conducting forensics operation there are lots of things the forensics investigator has to put in mind in other to have valid evidence such as the operation mode of anti-forensics. The knowledge of anti-forensics to an examiner would make the examiner to know when his on track or not to an extent as this would program the mind of the examiner to be pro-active hence the essence of this work.

An anti-forensic researcher examines the forensic tools and their approaches and tries to identify its weakness by thwarting these forensics approaches and devising various techniques and tools. For a forensic examiner to be successful in his job, he must be good in handling most of the forensic tool effectively most especially the free/open source tools, it is a nice idea for him/her to also understand the Anti-forensic approaches and their various relative tools and sometimes weakness in anti-forensic approaches and in tools; for example – when a TrueCrypt is used leaves a trace (its boot loader) even in most cases due to human carelessness some fragment or traces of evidence/artefacts or anti-forensic operation might be detectable by the examiner.

Case Analysis:

From the above model of the case, it can be deduced that if the suspect copies the file to his computer, he may decide to delete it temporary after using it, using shift + delete key to permanently delete the file. Forensic has proven that what most people thinks they have permanently deleted either with the normal use of shift + delete or deleting files from recycling bin does not actually delete but only raise flag to the file system that the space is available for files to be written on to mark as an unallocated space, within the period the file system spends in doing some house-keeping routing, if certain forensic tools are used it can restore back the file that was taught to have been permanently deleted. Some criminal are aware of this and hence some time find hidden place that the file system and operating system cannot access such as Host protected areas with other lots of areas that even some sophisticated forensic tools would not be able to access. As computer forensic investigators, the investigators must be aware of this areas, this process of data hidden is one of the many anti-forensic processes. Forensic examiner has to be aware of anti-forensic processes. Every anti-forensic effort or approach is being built toward countering phases of forensic analysis either to delay the forensic processes or to even make it impossible.

C. Tools Employed

a. Installation of Virtual Machine(VMware workstation 10.0 as the virtual environment)
b. Installation of Guest Operating systems on the VMware's
   i. Kali Linux (test board)
   ii. Window 7
   iii. Forensic Investigation Tools (FTK)
   iv. AccessData FTK Imager
   v. DumpIt
   vi. WinHex, OSForensics (OSFclone, OSFmount, OSFPassMask)
   vii. Autopsy (Forensic suit),
   viii. SIFT (SAN Investigatory Forensic Tool)
   ix. SecreteLayer
   x. Time Stomp
   xi. Slacker.exe
   xii. FOCA

Guymager.

IV. ALGORITHM AND MODEL DEVELOPMENT

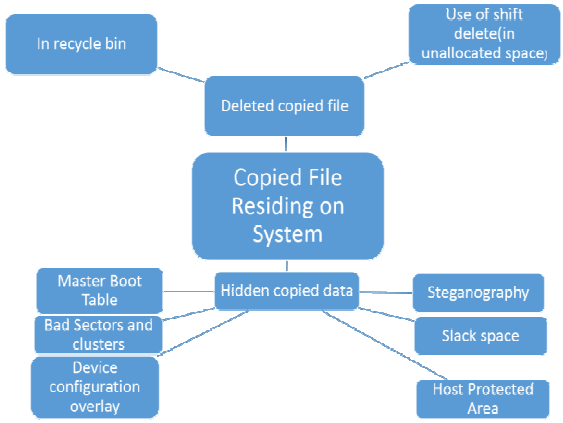


Figure 1: Case model.

Pseudo Code

Seized System;
while Copied file resides on system
The data is hidden;
if data is hidden
check:
- Master Boot Table,

- *Bad Sectors/clusters,*
- *Device Configuration overlay,*
- *Steganography,*
- *Slack Space, OR*
- *Host Protected Area;*

else

The data has been deleted;

if data has been deleted

check: Recycle bin OR Unallocated space;

V. EXPERIMENTAL WORK

After the text edit has been completed, the paper is ready

The experimental framework comprises the use of open forensic and anti-forensic tools and techniques to demonstrate how digital forensic analysis could be achieved using one of the numerous open source Forensic and Anti-forensic Tools, it involves the installation and setting up of test bed, the test bed or lab used here is on virtual machine which help to utilized the efficiency but yet less expensive forensic operation. VMware workstation 10 was used and window 7 ultimate was installed as guest operating system (OS) on the virtual machine, other forensic tools (FTs) were installed on the host OS while the Anti-Forensic tools (AFT) was ran on the guest OS. The figure below shows the different interface of the experiment

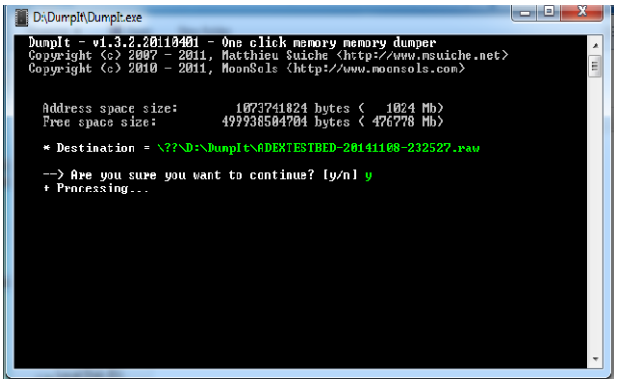


Fig 2: DumpIt capturing RAM image.

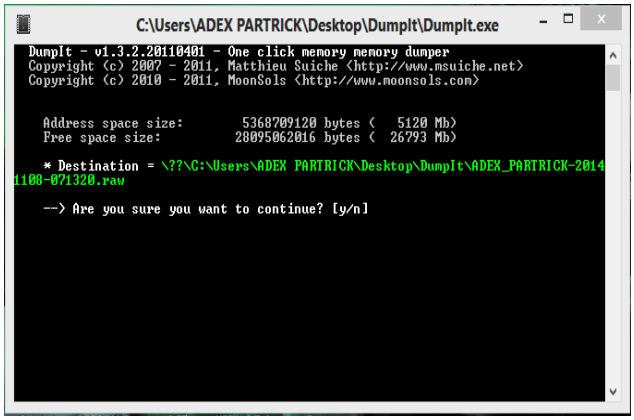


Fig. 3: DumpIt seeking to proceed to the RAM imaging.

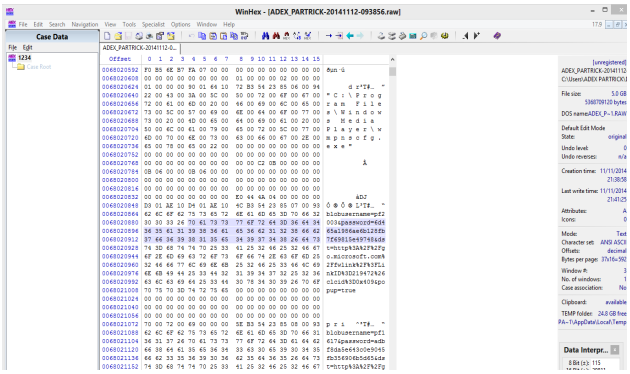


Fig. 4: WinHex returning various password hashes.

VI. RESULTS AND DISCUSSION

A. *Volatile Data Analysis*

The following forensic software where used and their results and impact are discussed below.

DumpIt

DumpIt is a volatile data imaging tools that has been used with any WinHex as a Hex Editor tool in other to capture the volatile data by imaging the RAM as shown in Fig. 2. The raw memory dump is generated in the current directory, only a confirmation question is prompted before starting as shown in Fig. 3. This raw memory dump generated was now used as item evidence in the WinHex. The easiest way to disrupt volatile data collection is by putting off the system, considering the fact that once power goes of the system, any stored data on the volatile memory is lost. Once the attacker can switch of the system before the arrival of the forensic examiner, the success of the forensic examination will be drastically reduced hence anti-forensic.

WinHex

The WinHex, was used to analyze the image of the raw memory dump generated by the DumpIt Tool, and as the image was hashed with a Message Digest 5 (MD5), SHA1 and SHA126 algorithm and it was compared before and after forensic operation to make sure its integrity was intact. When the content was searched for passwords WinHex returned various password hashes as show in Fig. 4. After the analysis of the image with WinHex it was able to get various passwords, and file logs such as the type of files and their extensions that was running and the resource they were using. And all this information was documented. AccessData FTK was also used to hash and compare hashes in relative to WinHex and exactly the same was generated, and when AccessData FTK Imager was used to do the raw dump memory analysis the same result was gotten.

B. Persistent Data Analysis

Some part of the analysis was carried out on virtual machine and other was carried out on the host computer, the reason is that, the analysis could be carried across various forensic laboratories that ordinarily would have involved several machine or impossible with just a single machine. Since the machine under investigation was installed on the virtual machine, the method used in getting evidence from the guest Operating System installed on the virtual machine was a little bit different. It involved imaging the virtual machine Hard Disk Drive (HDD) instead of the host machine or the physical machine.

Analysis of the Volatile Image Gotten from DumpIt Volatile Data Imager of the Seized System

After using WinHex to analyze the volatile image generated by DumpIt, we got the hex representation of the volatile data, since the hex data representation was not readable or understood by human, it was then converted into a messy plain text of which careful observation revealed some sensitive information such the hashed password was found. The hashes where imported into OSForensics tool rainbow table and it was compared to know hashed to reveal the plain text. The problem from here was that the username that corresponds to the various passwords was still not known.

Analysis of the Image Gotten from AccessData FTK imager of the Seized System

When the image was analyzed with AccessData FTK imager files incriminating was found in the bad sector and unallocated space. The file found on the unallocated space are possibly those file he deleted using Shit + Delete with the hope that he has actually deleted it from the recycle bin of which only sophisticated forensic tools can retrieve such as AccessData FTK imager.

The file found in the bad sectors where even more incriminating, this files must have being stored there for the sole aim of anti-forensic because merely searching the system will never reveal the presence of files on bad sectors, many forensic software would not even be able to search there for hidden files, when most forensic software comes across bad sector during scanning, they skip it and continue with the rest sectors/clusters. From the result gotten from analyzing his system RAM with DumpIt, one incredible observation is the presence of suspicious programs found, which was Slacker.exe, Slacker.exe is a command line anti-forensic tools used to hide files in slack space and also TimeStomp was found – TimeStomp is a metasploit tools used for manipulating MACB. Table 1 below is a fast representation of the meaning of MACB broken down by type of file system:

Table1 Show the Meaning of MACB on Various File System.

File System	M	A	C	B
FAT	Written	Accessed	Changed	-
NTFS	Modified	Accessed	MFT Modified	Created
Ext 2/3	Modified	Accessed	Changed	-
Ext 4	Modified	Accessed	Changed	Created
UFS	Modified	Accessed	Changed	-

Analysis of the Image Gotten from OSFclone Imaging/Cloning Tool

All the password discovered in WinHex where not in plain text, but hashes. But gratitude to the designers of OSForensics who has included rainbow table and dictionary list. Although, these are plug-in to the forensics tools. The hash value was computed and compared against known hashes on the rainbow table and it was successfully decrypted by finding a text that march the hash. To prevent the investigator from using the common password cracking techniques such as:

i. Dictionary
ii. Rainbow table
iii. And password guessing

A criminal may decide to use random string of data that cannot be found in the dictionary to avoid password guessing and dictionary attack, if the length of this string is considerable long it might just be impossible for even the rainbow table to crack the password a desperate criminal might even take the pain of memorizing hash value of a random string for password. For example if the word "forensic" is used as password and MD5 was used hash it, it would be "ad4642428b76i25b16c6dae5c84a9c", depending on importance of the file the criminal can memorize that long string of data, the beauty of this is that MD5 is a one hash function, so if the user enters this long string as password depending on the encryption algorithm used the value is going to change to something else. The implication of this is that the password the forensic examiner would be receiving be confusing to him and even the almighty rainbow table would be worthless in this kind of situation.

Analysis of the Image Gotten from Guymager Imaging Tool

The image that was gotten from Guymager imaging tool was loaded into Autopsy for case analysis, In the analysis of non-volatile data, the original image of the extracted system should be forensically clone or duplicated reason been that once the original image is contaminated, the evidence definitely would be doubtful or questionable. Because of the advancement in anti-forensic operation, like the use of logic zip or logic bomb, before trying to crack some of the file precaution must be taken reason been that there are some encryption algorithm that has more than two encryption key and decryption key. One of the key would be meant to alter to the bit of the file into another file entirely, some might even delete the file was used to access some of the criminal's private document. Cases of such have been reported recently.

Autopsy

After the image gotten from the Guymager was feed into Autopsy for analysis it showed all visited URL, deleted folders, directories, the content of the recycling bin, the MACE of each of the files, bookmarks, browsing history, cookies and all removable drives.

From the lists of URLs, it was discovered that he has visited Facebook and Gmail, this means from the passwords gotten from WinHex we can now relate them each to his account respectively, but there is still something missing which is his user names for the two account. For the user name to be extracted, looking at Facebook for example requires the following:

Email or Phone: Password:

From the above we can figure out the authentication SQL query to be:

If (email OR Phone AND Password) grant Access;

From the above it is obvious that since we have gotten his Facebook password we only need either the email and password or the phone number and his password to gain access.

For one to have access to Gmail, the credential requires are password and the corresponding email address, from the password gotten from the RAM and the email gotten from FOCA access to the Google account is sure. To get the email and/or phone number FOCA would get the job done. Observably, many a times when a site is visited with browsers, for instance Facebook, if the system is short down or the user opt out from surfing the site (Facebook) without logging out, the next time the browser is fired up, it loads the last logged in session, the magic behind this at the client side is the cookies which is like a token, or a value the server stores on the browser cache for identity remembrance, which this cookies the server can then remember who the user is and serve or load his last browsing session to him, the forensic examiner can use this little piece of information for forensic investigation. Other traces the forensic examiner may use is the browsing history, remembered password and bookmarks; if this artefacts are cleared it will harden the forensic investigation. Some dubious criminals that suspects forensic investigation might do the following to cover track:

i. Change file extension and header before deletion
ii. Alter the MACB file attributes
iii. Over slack spaces and unallocated spaces

Foca

When FOCA was used to query Federal University of Technology, using Google query option in FOCA search options, lots of information was harvested, but the one that was picked was CV of FUTMinna staffs and among it was his own inclusive. From his CV, his active emails including Gmail account name, and phone number was found

Most of this tools used to do this forensic analysis have almost exactly the same features to carry out basic forensic analysis, sadly on the seized system there was stegno files of which none of this tools actually took note of, I presume that it may be because it is a free/evaluation version. Further researched work should be carried out using same tools that are licensed with forensic analysis with lots of features. The best thing to do in other to avoid this FOCA from successfully given out information the forensic investigator may find interesting like your email address is to have many email accounts for various purpose. For example; the email that should be used in Curriculum Vitae should be different from the one used for social media, and also different from the one use for online trading or e-commerce, this same goes for phone numbers. The kind off sensitive information pasted on the internet should be minimal especially the social media as this is a pool or a rich resources for information retrieval

VII. CONCLUSION

In this paper we used the widely acceptable forensic methodology such as identifying, collecting, analyzing and reporting to analyze data. It has being able to point out hidden places on the logical and physical structure of the computer where evidence may resides, it has also introduced some forensic tools and their application to real life situation, due to human inherent element such as being bias as a result of sentiment cases, measure should be put in place to avoid investigators handling cases that he may pick interest in or that has to do with people that knows him directly or indirectly, if such issue arises where investigator has interest in the case, it should be awarded to external professional examiner

REFERENCES

[1] Changwei, L., Anoop, S., & Duminda, W. (2014). A Model Towards Using Evidence From Security Events. *A Model Towards Using Evidence From Security Events*, vol. *10*, 103-122

[2] M. Balogun & Y. Z. Shao, "Privacy Impacts of Data Encryption on the Efficiency". *International Journal of Advanced Computer Science and Applications,* vol. 4, no. 5, 2013, pp. 36-40

[3] A. Benjamin, "Modelling and refinement of forensic data acquisition", *Digital Investigation,* vol. 11, no. 2, 2014, pp. 90-101

[4] S. Johannes, & C. Michael, "Anti-forensic resilient memory acquisition", *Digital Investigation,* 2014

[5] P. Przemyslaw, and P. Elias, "Computer Anti-forensics Methods and Their Impact on", 2009, Retrieved September 3, 2014 from http://hdl.handle.net/10552/1508.

[6] F. Marco, B. Alessandro, P. Alessandro, and B. Mauro, "Countering Anti-Forensics by Means of Data Fusion", 2014.

Application Virtualization Techniques for Malware Forensics in Social Engineering

Joe-Uzuegbu C. K, Iwuchukwu U. C. and Ezema L. C
Department of Electrical/ Electronic Engineering,
Federal University of Technology Owerri, Imo State Nigeria.
joskie23@yahoo.co.uk, uchechi.iwuchukwu@futo.edu.ng, ezemms@yahoo.com

Abstract - **There is an increased trend in information insecurity, online fraud and social engineering activities today as a result of high dependence on the internet and social networks for communication, advertisement of products and services, etc. Malwares are most times, deliberately programmed as worms to appear as flash messages, online games, gift awards and in many other attractive forms for the user to access just at the click of a button. Several methods have been applied to minimize these infiltrations which include firewalls and antiviruses. However when confronted with a system infected with malware, a person's ability to investigate the system successfully depends on his knowledge, experience, and toolset. This is where there is a conundrum. People tend to avoid dealing with malware cases on their own due to inexperience and lack of knowledge but would rather outsource it to IT professionals either hired at that particular instance or employed within their organization. However, through careful preparation one can acquire knowledge, experience, and toolset that can eventually lead to working malware cases. The various procedures for investigating infiltrations into supposedly secure networks and computer systems are presented in this paper.**

Keywords— ***Malware, Toolset, Social Engineering, Infiltration***

I. INTRODUCTION

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

The term "social engineering" as an act of psychological manipulation is also associated with the social sciences, but its usage has caught on among computer and information security professionals. For instance, an individual walks into a building and posts an official-looking announcement to the company bulletin that says the number for the help desk has changed. So, when employees call for help the individual asks them for their passwords and ID's thereby gaining the ability to access the company's private information.

Social engineering could take various forms which include:

- Pretexting: This involves the act of creating and using an invented scenario to engage a targeted victim in a manner that increases the chance that the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. It is an elaborate lie, which usually involves some prior research or setup. The information obtained (e.g. date of birth, Social Security number, last bill amount) is used mostly for impersonation to establish legitimacy in the mind of the target.
- Phishing: This is a technique employed to fraudulently obtain private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business - a bank or credit card company - requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link (worm) to a fraudulent web page that seems legitimate with company logos and content, and has a form requesting everything from a home address to the personal identification number (PIN) of an automated teller machine (ATM) card.
- Vishing: This is also known as *Phone Phishing*. This technique uses a rogue interactive voice response (IVR) system to recreate a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted (typically through a phishing e-mail) to call in to the "bank" via a number (ideally toll free) provided in order to "verify" information. A typical system will reject log-ins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems transfer the victim to the attacker posing as a customer service agent for further questioning.
- Diversion Theft: This is often exercised by professional thieves with the objective of re-routing products and services on delivery.
- Spoofing: is a technique whereby one person or program successfully masquerades as another by falsifying data

and thereby gaining illegitimate advantage. Types of spoofing include caller ID, email, text and IP spoofing.

- Baiting: This technique, like the real-world Trojan horse, uses physical media and relies on the curiosity or greed of the victim. In this attack, the attacker leaves a malware-infected CD-ROM, or USB flash drive in a location sure to be found (bathroom, elevator, sidewalk, parking lot), gives it a legitimate-looking and curiosity-triggering label, and simply waits for the victim to use the device. An unsuspecting employee might find it and subsequently insert the disk into a computer to satisfy his curiosity, or a Good Samaritan might find it and turn it in to the company. In either case, as a consequence of merely inserting the disk into a computer to see the contents, the user would unknowingly install the auto-run malware on it. This act would likely give an attacker unfettered access to the victim's PC and, perhaps, the targeted company's internal computer network.
- Self-Cross Scripting Scam (Self-XSS): It is a technique used to gain control of victims' web accounts especially Facebook accounts. In this attack, the victim accidentally runs malicious code in his/her own web browser, thus exposing it to the attacker.
- Hacking: This includes various activities that aim at exploiting weaknesses or loopholes for the intent of gaining illegal and unauthorized access to a computer network for malicious purposes.

There are many more techniques of social engineering, but the focus of this research is on infiltrations bordering on social engineering activities like baiting, phishing, spoofing or hacking IDs of users of popular e-mail services such as Yahoo!, Gmail, Hotmail, etc.
Among the many motivations for deception are:

- Phishing credit card account details.
- Cracking into private e-mails and chat histories, manipulating them by using common editing techniques before using them to extort money and create distrust among individuals.
- Cloning websites of companies or organizations in order to destroy their reputation.
- Computer virus hoaxes
- Convincing users to run malicious code within the web browser via self-XSS attack to allow access to their web account.

What is a Malware?
Malware is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent of acting against the requirements of the computer user and does not include software that causes unintentional harm due to some deficiency.

Malware Forensics
It is the process of examining a system to:

- find malicious code,
- determine how it got there
- Discover the changes it caused to system.

The first place to start for improving one's skills is by exploring the strategy one should use. The purpose of starting with the strategy is twofold. First and foremost is to understand the techniques, examine the steps, and knowing what to look for. The second reason is to explore the various tools to use to carry out the process.

II. VIRTUALIZATION OPTIONS AND STRATEGY

Virtualization software provides a convenient and time-saving mechanism for building a malware analysis environment. Just be sure to establish the necessary controls to prevent malicious software from escaping your testing environment. With a fine-tuned lab, an analyst will be well on course toward making the most of his malware analysis skills. *VMware*, though frequently used, is not the only option for virtualization software you can use for malware analysis. Common alternatives include *Microsoft Virtual PC* and *Parallels Workstation.*

Virtual PC virtualizes a standard IBM PC compatible device and its associated hardware. Supported Windows operating systems can run inside Virtual PC.

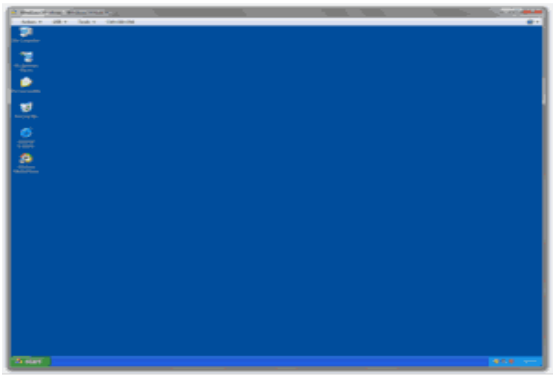


Fig. 2: Windows Virtual PC running Windows XP on a Windows 7 host.

Other operating systems such as Linux may run, but are not officially supported, and Microsoft does not provide the necessary "Virtual Machine Additions" (which include essential drivers) for Linux.
Virtual PC was originally developed as a Macintosh application for System 7.5 and released by Connectix in June 1997. The first version of Virtual PC designed for Windows-based systems, version 4.0, was released in June 2001.

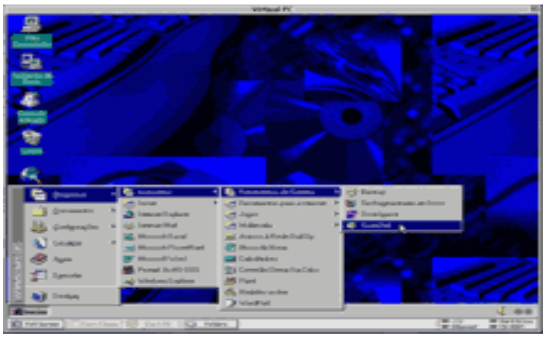


Fig. 3: Connectix Virtual PC version 3 in Mac OS 9, running an edition of Windows 95.

Connectix sold versions of Virtual PC bundled with a variety of guest operating systems, including Windows, OS/2, and Red Hat Linux. As virtualization's importance to enterprise users became clear, Microsoft took interest in the sector and acquired Virtual PC and Virtual Server (unreleased at the time) from Connectix in February 2003. Virtual PC 4 requires Mac OS 8.5 or later on a G3 or G4 processor, but running Windows ME, Windows 2000or Red Hat Linux requires Mac OS 9.0 or later. Virtual PC 4 was the first version with expandable drive images.

Virtual PC 5 requires Mac OS 9.1or newer or Mac OS X 10.1or later. For USB support, Mac OS X is recommended. To run Virtual PC 5 in Mac OS X, a 400 MHz or faster processor is required.

Earlier versions of Virtual PC supported the following features: (now removed in Microsoft Virtual PC 2004, 2007, and Windows Virtual PC):

- Older versions of Virtual PC (v5.0 or earlier) may have the hard disk formatted after creating the Virtual Hard Diskfile. Newer versions must partition and format the Virtual Hard Diskfile manually.
- A Virtual Switch available in Virtual PC version 4.1 or earlier allows adding multiple network adapters.
- Older operating systems are supported with Virtual Machine additions

Parallels Workstation is the first commercial software product released by Parallels, Inc., a developer of desktop and server virtualization software. The Workstation software consists of a virtual machine suite for Intel x86-compatible computers (running Microsoft Windows, Linux or Mac) which allows the simultaneous creation and execution of multiple x86 virtual computers. The product is distributed as a download package. Parallels Workstation has been discontinued for Windows and Linux as of 2013.

A. Implementation

Like other virtualization software, Parallels Workstation uses hypervisor technology, which is a thin software layer between Primary OS and host computer. The hypervisor directly controls some of the host machine's hardware resources and provides an interface to it for both virtual machine monitors and primary OS. This allows virtualization software to reduce overhead. Parallels Workstation's hypervisor also supports hardware virtualization technologies like Intel VT-x and AMD-V.

B. Features

Parallels Workstation is a hardware emulation virtualization software, in which a virtual machine engine enables each virtual machine to work with its own processor, RAM, floppy drive, CD drive, I/O devices, and hard disk– everything a physical computer contains. Parallels Workstation virtualizes all devices within the virtual environment, including the video adapter, network adapter, and hard disk adapters. It also provides pass-through drivers for parallel port and USB devices.

Because all guest virtual machines use the same hardware drivers irrespective of the actual hardware on the host computer, virtual machine instances are highly portable between computers. For example, a running virtual machine can be stopped, copied to another physical computer, and restarted.

Parallels Workstation is able to virtualize a full set of standard PC hardware, including:

- A 64bit processor with NX and AES-NI instructions.
- A generic motherboard compatible with IntelP965 chipset.
- Up to 64 GB of RAM.
- VGA and SVGA video cards with VESA VBE3.0 support and up to 256 MB of VRAM.
- A 1.44 MB floppy drive, which can be mapped to a physical drive or to an image file.
- Up to four IDE devices. This includes virtual hard drives that range in size from 20 MB to 128 GB each and CD/DVD-ROM drives. IDE devices can be mapped to physical drive or to an image file.
- Up to 16 SATA devices including hard disks and CD/DVD drives.
- Up to four serial ports that can be mapped to a real port, to a pipe or to an output file.
- Up to three bi-directional parallel ports, each of which can be mapped to a real port, to a real printer or to an output file.
- An Ethernet virtual network card compatible with Realtek RTL8029(AS) with full IPv6support.
- USB2.0 controller.
- An AC'97compatible sound card.
- A 104-key Windows enhanced keyboard and a PS/2 wheel mouse.
- Officially supported guest operating systems: Windows 7, Windows Vista, Windows XP

III. BENEFITS OF VIRTUALIZATION

The techniques and features that Virtual machines provide are useful for several scenarios:

- Running multiple operating systems simultaneously. Virtual machines allow you to run more than one operating system at a time. This way, you can run software written for one operating system on another (for example, Windows software on Linux or a Mac) without having to reboot to use it. Since you can configure what kinds of "virtual" hardware should be presented to each such operating system, you can install an old operating system such as DOS or OS/2 even if your real computer's hardware is no longer supported by that operating system.

- Easier software installations. Software vendors can use virtual machines to ship entire software configurations. For example, installing a complete mail server solution on a real machine can be a tedious task. With virtual machines, such a complex setup (then often called an "appliance") can be packed into a virtual machine. Installing and running a mail server becomes as easy as importing such an appliance into the VM.

- Testing and disaster recovery. Once installed, a virtual machine and its virtual hard disks can be considered a "container" that can be arbitrarily frozen, woken up, copied, backed up, and transported between hosts. In addition to that, with the use of another VM feature called "snapshots", one can save a particular state of a virtual machine and revert back to that state, if necessary. This way, one can freely experiment with a computing environment. If something goes wrong (e.g. after installing misbehaving software or infecting the guest with a virus), one can easily switch back to a previous snapshot and avoid the need of frequent backups and restores. Any number of snapshots can be created, allowing you to travel back and forward in virtual machine time. You can delete snapshots while a VM is running to reclaim disk space.

- Infrastructure consolidation. Virtualization can significantly reduce hardware and electricity costs. Most of the time, computers today only use a fraction of their potential power and run with low average system loads. A lot of hardware resources as well as electricity is thereby wasted. So, instead of running many such physical computers that are only partially used, one can pack many virtual machines onto a few powerful hosts and balance the loads between them

IV. BASIC PROCEDURE FOR MALWARE FORENSICS

- Examine the master boot record of the computer in question.
- Obtain information about the operating system and its configuration.
- Examine the volatile data.
- Examine the files on the system that were identified in volatile data.
- Hash the files on the system.
- Examine the programs ran on the system.
- Examine the auto-start locations.
- Examine the host-based logs.
- Examine file system artifacts.
- Malware searches.
- Perform a timeline analysis.
- Examine web browsing history.
- Examine specific artifacts.
- Perform a keyword search.
- Examine suspected malicious files.

V. TOOLS

After the process you want to use is documented then the next step is to identify the tools you will use in each examination step. There are numerous tools that can be employed, depending on user preference. The tools a user started out with are not the same ones he may use after getting relatively experienced; the important thing is each tool should help him to learn and grow. Over time, each tool will start to show its pros and cons.

A. Testing Environment

With your process and tools selected, it is finally time to stop the researching and to use the documented process and selected tools. To do this, a testing environment has to be set up. There is an inherent risk to using virtualization for the testing environment because the malware may be virtualization aware and behave differently than on a real computer. However, despite this risk, it is highly recommended to use virtualization as a testing environment. It is a lot faster to create multiple test systems (by copying virtual machines) and its snapshot feature makes it easier to revert mistakes.

There are various virtualization options available with great documentation such as VirtualBox and VMware. Pick a virtualization platform and install it using the provided instructions.

B. Procedure for Creating Virtual Machines (VMs)

One very important decision one needs to make is on what platform or operating systems to perform testing on. This not only includes the operating system versions (i.e. Windows 7 versus Windows 8) but what processor to use as well (32 bit versus 64 bit). A good choice is the VMware for the virtualization software and Windows 7 32 bit as the testing platform.

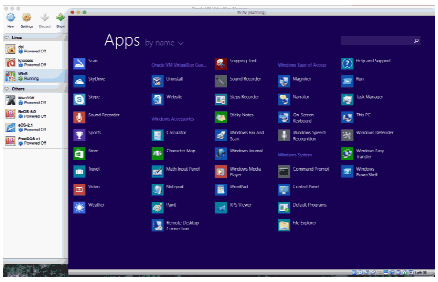


Fig 1: *A virtual Machine environment running on Windows 8.*

Before the VM is created the operating system of choice should be installed. After the installation some loopholes can be created to make it easy for the system to be compromised.
First disable security features. This includes the built-in firewall and the user account control.
The next step is to assign administrative privileges to the user account being used. This could be followed by installing vulnerable client-side applications (especially the ones targeted by exploit kits) including: Adobe flash, Adobe Reader, Java, Silverlight, Microsoft Office, Internet Explorer, and a non-patched operating system. At a minimum, make sure you don't patch the OS and install Java, Silverlight, Adobe reader, and Adobe flash. This will make the VM a very juicy target.
After the VM is created and configured multiple copies of it can be made. Using copies makes things easier during analysis without having to deal with snapshots.

C. Manually Infecting Systems

The first approach to improving your skills is a manual method to help show the basics. The purpose is to familiarize yourself with the artifacts associated with malware executing in the operating system you picked. These artifacts are key to be successful in performing malware forensics on a compromise system. The manual method involves you infecting your test VM and then analyzing it to identify the artifacts. The manual method consists of two parts: Using known and unknown samples.
However, before proceeding it is very important to isolate the virtual machine's network configuration to prevent the malware from calling home or attacking other systems.

D. Using Known Samples

While starting out, it is better to practice with a sample that is known. "Known" in this case means "documented" so that one can reference the documentation in order to help determine what the malware did. Again, we are trying to improve our ability to investigate a system potentially impacted with malware and not trying to reverse the malware. The documentation is just to help one to account for what the malware did to make it easier to spot the other artifacts associated with the malware running in the operating system.

There are various ways to find known samples such as finding them using information on antivirus websites since they list reports using their malware naming convention. For instance, Symantec's Threat Listing, Symantec's Response blog, Microsoft's Threat Reports, or Microsoft's Malware Encyclopedia to name a few. These are only a few but there are a lot more out there on antivirus websites. The key is to find malware with a specific name that you can search on such as Microsoft's Backdoor:Win32/Bergat.B. The next step then is to review the technical information to see the changes the malware makes.

A better route (if one can find it) is to use a hash of a known malware sample. Some websites share the hash of the sample they are discussing but this does not occur frequently. Another option is to look at the public sandboxes for samples that people submitted.
After picking a malware name or hash to use, then the next step is to actually find the malware.

Recall that the purpose of going through all of this is to improve the operator's malware forensic skills and not your malware analysis skills. We are trying to find malware and determine how the infection happened; not reversing malware to determine its functionality. The next step after acquiring the sample is just to infect the virtual machine (VM) with it and then power it down. If the VM has any previous snapshots then they should be deleted to make it easier.

Now that we have an infected image (i.e. the .vmdk file) we can analyze it using the process we outlined and the tools you selected earlier. At this point we are making sure the process and tools work. We are also looking to explore the artifacts created during the infection. Since the behavior of the known malware is known, there is no need to focus on it. We would rather focus on the artifacts created by a program executing in the operating system you selected. Artifacts such as program execution, logs, and file system.

E. Using Unknown Samples

Using a known sample is helpful to get one started but it gets old pretty quick. After you used a few different known samples it is not as challenging to find the artifacts. This is where you take the next step by using an unknown (to you) sample. Just download a random sample from one of the sources listed at malware sample sources for researchers. Infect your virtual machine (VM) with it and then power it down. If the VM has any snapshots then delete them to make it easier.
Now the examination stage can be carried out using the same process and tools that were used with a known malware sample. This method makes it a little more challenging because one may know what the malware did to the operating system.

F. Keeping production systems safe

When dealing with malware one should take precautions not to infect production systems. Such breaches can happen when handling malware improperly or when a specimen exploits a weakness in the VMware setup and escapes its sandbox. There have been several publicly announced vulnerabilities in VMware that, in theory, could allow malicious code from the virtual system to find its way onto the physical host. Here are some suggestions for mitigating these risks:

- Keep up with security patches from VMware.
- Dedicate the physical host to the VMware-based lab; don't use the system for other purposes.
- Do not connect the physical laboratory system to your production network.
- .Monitor the physical host with host-based intrusion detection (IDS) software, such as a file-integrity checker.
- Periodically re-image the physical host using cloning software, such as Norton Ghost. If this option is too slow, look to hardware modules, such as CoreRESTORE, for undoing changes to the system's state.

One of the challenges of using VMware for malware analysis is that malicious code can detect whether it is running within a virtual system, which indicates to the specimen that it is being analyzed. If the specimen's code cannot be modified to eliminate this functionality, VMware could be reconfigured to make it stealthier. The biggest problem with these settings is that they may slow down the virtual system's performance.

VI. CONCLUSION & RECOMMENDATION

The steps discussed above present a very cheap and convenient means of diagnosing the effects of malware on a host system. VMware emulation software is used in classrooms for teaching, but is only restricted to Windows XP and Windows 7 to adhere with Microsoft licensing requirements. Virtual PC and Parallels Workstation can be downloaded online and configured to user specifications.

While using these emulation software, it is important to properly configure them so as to minimize the risk of malware "breaking out" of the sandbox.

This work is restricted to improving the computer analyst's forensic skills. Further work still needs to be done on developing malware analytic and mitigation skills.

Every establishment operating a website or any online features needs to be vigilant and hold routine staff sensitization programmes on the dangers of social engineering; and regular training should be done especially for the IT staff of these establishments to investigate cheaper and more convenient ways of developing their malware forensic and mitigation skills.

REFERENCES

1. www.journeyintoir.blogspot.com/2014/06
2. www.zeltser.com/vmware-malware-analysis
3. VMware. Retrieved November 18, 2007 from http://www.vmware.com. Access Data. Retrieved August 10, 2007 from http://www.accessdata.com/
4. K. L. Asrigo, and D. L. Litty, "Using VMM-Based Sensors to Monitor Honeypots", In Proceedings of the 2nd ACM/USENIX International Conference on Virtual Execution Environments (VEE 2006), June, 2006.
5. Beyond the CPU: Defeating Hardware Based RAM Acquisition. Retrieved November 15, 2007 from http://i.i.com.com/cnwk.1d/i/z/ 200701/bh-dc-07-Rutkowskappt.pdf
6. B. Carrier, and J. Grand, "A hardware-based memory acquisition procedure for digital investigations", The International Journal of Digital Forensics & Incident Response. Retrieved November 15, 2007 from www.sciencedirect.com.
7. S. Crosby and D. Brown, "The Virtualization Reality", ACM Queue, December/January 2006-2007, pp.34-41
8. Data Center Management Research Report September 2007. Retrieved November 15, 2007 from http://www.novell.com/products/zenworks/orchestrator/data_center_research_report_sep2007.pdf
9. T. Garfinkel and M. Rosenblum, "A virtual machine introspection based architecture for intrusion detection", In Proceedings of the 10th Annual Symposium on Network and Distributed System Security (NDSS 2003), pages 191–206, Feb. 2003.
10. Grand Ideas Studio: Tribble. Retrieved November 15, 2007 from http://www.grandideastudio.com/src/portfolio.php?cat=&prod=14
11. Guidance Software, Inc. EnCase. Retrieved August 10, 2007 from http://www.guidancesoftware.com/
12. Hit by a Bus: Physical Access Attacks with Firewire. http://www.security-assessment.com/files/presentations /ab_firewire_rux2k6-final.pdf
13. Introducing Blue Pill. Retrieved November 15, 2007 from http://theinvisiblethings.blogspot.com/2006/06/introducingblue-pill.html
14. X. Jiang, X. Wang and D. Xu, "Stealthy malware detection through vmm-based "out-of-the-box" semantic view reconstruction", In Proceedings of the 14th ACM Conference on Computer and Communications Security (Alexandria, Virginia, USA, October 28 - 31, 2007). CCS '07. ACM, New York, NY, 128-138. DOI=http://doi.acm.org/ 10.1145/1315245.1315262
15. Kernel based Virtual Machine. Retrieved November 18, 2007 from http://kvm.qumranet.com/kvmwiki.
16. K. Kourai and S. Chiba, "HyperSpector: virtual distributed monitoring environments for secure intrusion detection", In Proceedings of the 1st ACM/USENIX international Conference on Virtual Execution Environments (Chicago, IL, USA, June 11 - 12, 2005). VEE '05. ACM, New York, NY, 197-207. DOI=http://doi.acm.org
17. L. Litty and D. Lie, "Manitou: a layer-below approach to fighting malware", In Proceedings of the 1st Workshop on Architectural and System Support For Improving Software Dependability, San Jose, California, October 21 - 21, 2006.
18. ASID '06. ACM, New York, NY, 6-11. DOI= http://doi.acm.org/10.1145/1181309.1181311
19. Microsoft Virtual PC Server. Retrieved July 15, 2007 from http://www.microsoft.com/windows/products/wi
20. National Security Agency Central Security Service – Technology Profile Fact Sheet. Retrieved November 15, 2007 from http://www.nsa.gov/techtrans/techt00011.cfm
21. Parallels. Retrieved July 25, 2007 from http://www.parallels.com/
22. ParavirtBenefits. Retrieved November 15, 2007 from http://virt.kernelnewbies.org/ ParavirtBenefits
23. B. D. Payne, R. Sailer, R. Cáceres, R. Perez, and W. Lee, "A layered approach to simplified access control in virtualized systems", SIGOPS Oper. Syst. Rev. vol. 41, no. 4, 2007. pp. 12-19. DOI=http://doi.acm.org/10.1145/1278901.1278905
24. L. Zeltser, "Virtualized Network Isolation for a Malware Analysis Lab", May 2007.

Forensic Live Response:Why an Object May be Evidence in the Court of Law?

Funminiyi Olajide

funminiyi.olajide@cu.edu.ng

***Abstract*—Volatile data, being vital to digital investigation, have become part of the standard items targeted in the course of forensic live response to a computer system. In traditional computer forensics where investigation is carried out on a dead system for example, hard disk, data integrity is the first and foremost issue for digital evidence validity in the court of law. In the context of live system forensics, volatile data are acquired from a running system. Due to the ever-changing and volatile nature, it is impossible to verify the integrity of volatile data. Let alone the integrity issue, a more critical problem is the data steadiness, data accuracy and validity of data on the note of proven whether an object found on the volatile memory may be used as evidence in the law court. This digital evidence is related to the data collected on a live system. In this paper, we concentrate on the consistency issue on live systems forensics on the fact that an object may be evidence gathered in the crime scene and can be used as evidence in the court of law. By examining the memory data and the concept of an investigation to determine what is required in an event-based analysis of digital forensics that includes an investigation process model. A physical crime scene data can be used to develop hypotheses and answer questions about an incident or crime. This can be used to argue out an object based evidence of an event.**

Keywords—Information, digital, evidence, data, volatile investigation memory

I. INTRODUCTION

Currently, there are few agreed upon definitions in the area of digital forensic research, most especially, the digital object, digital data and digital event in some developing nations of the world. Clearly, the definitions we are using on why an object may be evidence, even the most basic ones. A digital object is a distinct collection of digital data, such as a file, a hard disk sector, a network packet, a volatile data, a memory page, or a process, while digital data are data represented in a numerical form. With recent computers, it is common for the data to be internally represented in a binary encoding, but this is not a requirement [1]. Digital data in addition to its numerical representation has a physical representation. For example, the bits in a hard disk are magnetic impulses on platters that can be read with analog sensors [2].

The concept of an investigation can determine what is required in an event-based analysis and the notion of a physical crime scene can be used to develop hypotheses of an object for evidence based on the questions and answers. Hypotheses are developed by collecting objects that may have played a role in an event that was related to the incident. In this thought, each digital device is considered a digital crime scene, which is included in the physical crime scene where it is located. The investigation includes the preservation of the system, the search for digital evidence, and the reconstruction of digital events. The focus of the investigation is on the reconstruction of events using evidence so that hypotheses can be developed and tested.

According to Brian [3], network wires contain electric signals that represent network packets and keyboard cables contain electric signals that represent which keys were pressed. In this sense, a computer converts the electric signals to a digital representation [3], whereas digital photography and video are considered to be a digital representation of the light associated with physical objects. Therefore, the digital data can be stored on many mediums because each has different properties that determine how long the data will reside. For example, data will reside on a keyboard cable for a fraction of a second, but it may reside on a hard disk for a hard disk for years [4].

However, in today, digital forensic data analysis, digital object is considered to have a characteristic or unique feature, based on their creator and function and these objects may be used as evidence in the law court. For example, the characteristics of a hard disk sector will be different when it is used to store the contents of an ASCII text document versus a JPEG image. We can use the characteristics to identify the data. The state of an object is the value of its characteristics. If a letter were changed in an ASCII text document, then the object corresponding to the file would have a new state. Similarly the state of a running computer process changes every time data is written to its memory.

Some environments have developed policies and laws that forbid certain events from occurring [5], however, an incident is an event or sequence of events that can violate a policy and more specifically, a crime is an event or sequence or events that violate a law [6].

In particular, a digital incident is one or more digital events that violate a policy. Therefore, in response to an incident or crime, an investigation may begin to determine the hypotheses of an object following questions and answers [7]. This is because an investigation is a process that develops and tests hypotheses to answer questions about events that occurred and questions include “what caused the incident to occur”, “when did the incident occur”, “where did the incident occur” and why an object may be evidence’’. This is necessary to ascertain the data consistency based on the data characteristics of an object for evidential purposes in the court of law.

II. LITERATURE REVIEW

The concept of collecting volatile memory data is still new to computer forensic study and evolving researches have been given to this area with a view to search for proper ways of investigation into this area. Recently, the analysis of volatile memory data becomes an item in live incident response on the notion that why an object may be evidence? There are a number of response toolkits being developed to address the needs [8]. The available toolkits are often automated programs that run on the live system to collect transient data in the memory [9]. However, if the response tool is run on a compromised system, the tool would heavily rely on the underlying operating system and may affect the reliability of the collected data [10]. Some of the response tools may even substantially alter the digital environment of the original system and causes an adverse impact to the dumped memory data. As a result, it is often required to study those changes to determine if those alterations will affect the acquired data [11].

Carrier and Grand pointed out the potential flaws in acquiring volatile data through application running at the original system and proposed a hardware-based procedure for making a copy of memory contents to avoid the collected data being compromised by any untrusted code of the operating system or its applications (Brian Carrier, 2005). According to [12], further discussed the problems when acquiring live data through a network-based model and suggested a forensically sound approach in using firmwaredevice to acquire memory data utilizing the Direct Memory Access (DMA) controller.

Notwithstanding, the aforementioned papers focus on methods and techniques that could be used for collecting reliable memory data, there are fewer analysis on the acquired memory data which contained transient and discrepant data. The inconsistency of memory violates computer forensic principles [13] because data in the memory are not consistently maintained during system operation. This issue poses challenge for computer forensics and need to be addressed before presenting the evidence to the court of law.

III. METHODOLOGY

We have observed that each memory process has its own allocated space at the system memory which may include both physical and virtual addresses. We have noted that a digital object is considered to have a characteristic or unique feature, based on their creator and function. For example, the characteristics of a hard disk sector will be different when it is used to store the contents of an ASCII text document versus a JPEG image mentioned above. We have examined the use of these characteristics to identify the data because, the state of an object is a value of its characteristics and if a character were changed in an ASCII text document, then the object corresponding to the file would have a new state.

However, a digital event is an occurrence that changes the state of one or more digital objects [14]. If the state of an object changes as a result of an event, then it is an effect of the event. Some types of objects have the ability to cause events and they are called causes. We have noted that because digital objects are stored in a physical form, then their state can be changed by both physical and digital events [15].

Furthermore, some types of objects in an event-based analysis have the ability to cause events and they can be called "causes". We have observed that because digital objects are stored in a physical form, then their state can be changed by both physical and digital events and the object is considered evidence of an event if the event changes the object's state. On this note, an object may be evidence of an event and this means that the object can be examined for information about the event that occurred.

Thus, future events could cause an object to no longer have information about past events but, every object is evidence of at least one event, because there had to be an event that created the object. Therefore, every object is evidence of at least one event, because there had to be an event that created the object. We are still investigating on some different scenarios of why an object may be evidence based on various data captured for further analysis on both Windows and Linux.

As we carry on with our investigation on both Linux and windows systems, we would be able to provide data describing the Forensic live response of data acquisition and data analysis on Linux and Windows systems. We have commenced further investigation on the techniques and process of event reconstruction of data analysis and we believe the memory captured on the system can be analyzed to determine an object in an event for evidential purposes and this can reconstructed based on the events that had previously occurred for further investigation on the purpose of data consistency for evidential use in the court of law [16].

With the case of volatile data, we have identified that once volatile data have been gathered and have moved into persistent data, it is compulsory to validate the images for object identification purposes of what caused the event to have occurred.

IV. FINDINGS

To develop and test hypotheses about the events that occurred before, during and after the incident, we need to determine what actually happened. The only proof that an event may have occurred is if evidence of the event exists. If the object whose state was changed by the event still exists, then we can examine it for information about the event and about other objects that were causes or effects of the event.

Therefore, we can make our previous evidence definition more specific and state that an object is evidence of an incident if its state was used to cause an event related to the incident or if its state was changed by an event that was related to the incident. Rynearson observed "Everything is evidence of some event and the key is to identify and then capture evidence relative to the incident in question [17]." For this framework, we have studied the following definitions of evidence, which are a little more general and do not focus on the cause and effect relationship. Physical evidence of an incident is any physical object that contains reliable information that supports or refutes a hypothesis about the incident and digital evidence of an incident is any digital data that contain reliable information that supports or refutes a hypothesis about the incident [18].

Based on the research studies, it is understood that an object has information about the incident because it was a cause or effect in an event related to the incident. We noted that because digital data has a physical form, then physical evidence can contain digital evidence. Using this definition, a hard disk is physical evidence and the sectors and files that contain information about the incident are digital evidence. However, the Electronic Crime Scene Investigation Guide describes the recognition and collection of a hard disk or other storage device as the collection of electronic, or digital, evidence [19].

We have studied this framework and that the collection of the hard disk is the collection of physical evidence and the collection of a digital object from the hard disk is the collection of digital evidence. Also we noted that the difference between physical and digital evidence is in their format and has nothing to do with the type of incident. Therefore, we can have digital evidence for a physical incident or crime. For example, a digital video camera will create a digital representation of a physical event and the resulting file will be digital evidence of the event. We can also have physical evidence for a digital crime and the object may be used as evidence in the law court.

It is no doubt that we require reliable tool and proper procedures to acquire memory data from live system to minimize any possible contamination to the collected data. Notwithstanding, due to the inconsistent nature of memory, the acquired memory data may raise challenge on its validity in the context of court proceedings. To overcome the problem, we discuss the component of memory and recommend the way of identifying consistent data that are contained within a memory process, such data are static in nature with its consistency is well-maintained.

However, this research is only done on analyzing consistent data within a logical memory process, more work should be conducted to derive a method of identifying same kind of consistent data within the whole memory. Volatile memory and live data collection are still green to the field of computer forensics and a substantial amount of researches still need to be conducted to secure the validity of the digital evidence collected from a live system. This is an on-going research as we have described it, 'Forensic live response and event reconstruction' and it becomes very important in today digital forensics because investigators must be able to defend their hypotheses about why an object may be evidence.

On the cause of our research study, we are contemplating to address all of these problems to ascertain why an object may be evidence for evidential purposes in the court of law. Some of the area of interest to consider are: incident response and live analysis; methods for interrupting the execution for live acquisition; methods for performing live analysis on systems without interrupting the execution sequence; methods in relation to the cause and effect of event reconstruction; abstract model of why an evidence exists; and the automated executable investigation analysis tools in event reconstruction of digital crime and digital investigations to generate 'data fact'.

V. CONCLUSION

Looking at the different methods of identifying data from the memory dumps, the general trend is that the less information we want to link to the analysis stage for example, process information or file name, the more stages can be identified, but not linked to other information in the memory dumps. By identifying the suspicious data in memory dumps and linking this information to process structures, we obtain information about the origin and usage of this suspicious data and this will reduce the amount of unknown data in memory dumps. From this scenario, an object may be discovered out of the origin of the data collected for evidence to further investigate the events of the incident for evidential purpose in the court of law.

REFERENCES

[36] Carrier, B. (2004). A Hardware-Based Memory Aquisition Procedure for Digital Investigations,. Journal of Digital Investigation , 90-101.

[37] Mandia, K. (2005). Incident Response and Computer Forensics. McGraw-Hill Osborne Media, 2 edition, , 61-119..

[38] Brian, C. (2006). Digital Forensic Examination Tools. Journal of Computer Crime , 28-62.

[39] Poque, C. (2007). Unix and Linux Forensic Analysis Forensic Science:. Master Linux and Unix File Systems for Digital Investigation , 21-45

[40] Carvey, H. (2006). Windows Forensics and Incident Recovery Process. Addison Wesley , 88-123.

[41] Walters, A. (2006). Volatools: Integrating Volatile Memory Forensics into the Digital Investigation Process. Digital Investigation , 21-71.

[42] Pepe, M. (2007). FireWire Memory Dump of Windows. The Digital Investigation Process , 76-90.

[43] Harlan, C. (2005). Forensics Analysis of an Event. Forensic Focus , 11-81.

[44] Shauw, L. (2007). Data Consistency: Computer Forensics Anaysis . Digital Forensics , 111-213.

[45] Carrier, B. (2005). Digital Investigation and Computer Crime Analysis. Journal of Security Incident, Law and Technology , 113-213.

[46] Petroni, W. (2006). Event Analysis and Automated Data Sequence. International Journal Digital Evidence , 21-76.

[47] Mantin, A. (2008). Next Generation Digital Forensics:Memory Dump Analysis of Windows . Digital Evidence , 12-112.

[48] Westbrook, Z. (2006). Eletronic Record Management. Journal of Information Science , 51-81

[49] Golden, G. (2006). Information Security and Forensic Society. Computer Forensics , 54-90.

[50] Garner, G. M. (2007). Live Forensics: Diagonising your system for evidence. Journals of Information Science , 45-64.

[51] Chris, P. (2008). Forensic Analysis of a Live System. Security Focus , 77-90.

[52] Rynearson, G. (2007). Hardware Memory Acquisition Procedure for Digital Investigation. Digital Investigation Journal , 14-19.

[53] Burdach, M. (2008). Finding Digital Evidence in Physical Memory. Journals of Forensic Science , 16-90

[54] Murdoch, G. (2007). Introduction to Windows Memory Forensic. International Journal of Digital Investigation , 28-76.

.

Guideline for Critical Information Infrastructure Protection in Nigeria

Ayo Rotibi
iSecure Consulting Ltd. (UK, NG, KQ).
arotibi@isecureconsulting.com

***Abstract*—In most nations, infrastructures for the provision of basic public services, socio-economic activities, safety, internal and external security, and governance are increasingly dependent on interconnected Information and Communication Technology (ICT). This dependency and interconnections are underpinned by the Internet which eliminates international borders and therefore makes real the threat of a "cyber-attack". Due to the magnitude and potential consequences of such cyber-attacks, nations are identifying these vulnerable critical services and making adequate provision for their protection. Part II of the Cybercrime Bill (2014) is dedicated to the "Protection of Critical National Information Infrastructure" in line with the global Critical Information Infrastructure Protection (CIIP) initiatives. This paper therefore reviews the processes adopted by various nations and thereafter propose an "Information Assurance Guideline for the Security and Protection of CII in Nigeria" It is hoped that the Guideline will assist Information Assurance Operators in the definition, identification and classification of threats to CII, impacts of such threats and best practice mitigations.**

Keywords—cybercrime; critical infrastruture; information assurance; cybercrime legislation;

I. INTRODUCTION

The revolution in information technology has changed the way governments and businesses operate, with most national economies and security becoming fully dependent upon information technology and its underlying information infrastructure. This infrastructure underpins the operation of all sectors of the economy and it exceeds the traditional national boundaries. They control not only physical objects such as radar, electric transformers, and pipeline pumps, but also the critical processes in governance, utilities, communications, banking and manufacturing. Often referred to as Critical Information Infrastructure (CII), this infrastructure is a spectrum of information system components and computer-based (control) communication systems, connecting together certain social-economic activities deemed to be vital for the security, governance and general wellbeing of a people. Information system components include, but are not limited to: operating systems, middleware, applications, servers (database, authentication, electronic mail and web, proxy, domain name, and network time), workstations and network components. Network components include such devices as firewalls, switches, routers, gateways, wireless access points, and network appliances. In the context of a nation, CII is a major component of the National Information Infrastructure; the massive computer databases and communications systems used by such sectors as government authorities, public utilities, telecommunication, health, banking and financial services, and transport. On the other hand, Critical Infrastructure (CI) is an assortment of physical structures/assets, processes and organisations, whose interdependence and interconnection are underpinned by the CII. This dependency and interconnection have made CI increasingly vulnerable to attacks by hackers and crackers who could launch remote attacks across networked computers and yet effectively obfuscate their identity, location, and intent. Sadly so, a serious disruption in the functioning of the CI could have cascading effect on the entire socio-economic activities and thereby undermine a nation, because a disruption in one critical infrastructure could adversely affect the others, which may invariably have a telling effect on human life, morale, governance, economy, defence and security. A fundamental goal of a nation therefore is to have an Infrastructure Protection Programme that will identify and protect infrastructures that are deemed critical in terms of governance, national and economic security, health and safety, and public confidence.

A. Critical Network Attacks And Protection

With increasing reliance upon digital technology and network infrastructure, the world is becoming increasingly vulnerable to cyber-attack. Protection of the Critical network is a global responsibility, with every nation expected to act responsibly to contribute to its protection. Nations must think globally, and act locally – a universal environmental protection slogan - because an incident in one nation may affect other nations.

The various virus attack incidences that originate in one corner of the world but spread to millions of computers around the world is the commonest form of global ripple effect. The rise in terrorism couple with the use of the computers makes the issue of asset protection more compelling; since terrorists are increasingly using the Internet to propagate their ideologies and claims, using the Internet to unleash terror. The Financial Times of London stated that:

"*Terrorists have long made use of the internet. But ISIS' (and Boko Haram's) approach is different in two important areas. Where al-Qaeda and its affiliates saw the internet as a place to disseminate material anonymously or meet in "dark spaces", ISIS (and BH) has embraced the web as a noisy channel in which to promote itself, intimidate people, and radicalise new recruits.*[1]"

More worrisome is the fact that cyber-attacks sophistication ranges from simple and unstructured, to complex and well-coordinated with the attacker's knowledge and skill-set dropping from "high" to "low", and attack tools advancing from manual password guessing to automated and intelligent codes.

B. The Act

The Cybercrime Act (2015) includes the designation of certain computer systems or networks as critical national information infrastructure. Specifically, Part II, Section 3 states thus

> The President may on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well being of its citizens, as constituting Critical National Information Infrastructure. in respect of:
>
> a) the protection or preservation of critical information infrastructure;
> b) the general management of critical information infrastructure;
> c) access to, transfer and control of data in any critical information infrastructure;
> d) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any critical national information infrastructure;
> e) the storage or archiving of data or information regarded critical national information infrastructure;
> f) recovery plans in the event of disaster or loss of the critical national information infrastructure or any part of it; and
> g) any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure.
>
> The Presidential Order made under section 3 of this Act may require the audit and inspection of any Critical National Information Infrastructure, from time to time, to evaluate compliance with the provisions of this Act.

This paper therefore seeks to:
Suggest an *Information Assurance Guideline* for the Security and Protection of designated *CII* in Nigeria. This Guideline will assist Information Assurance Operators in Nigeria to; **define, identify and classifythreats, impacts and mitigations**

II. NATIONAL SECURITY

There is a paradigm shift in 'National Security' with the term developing a whole new meaning and responsibility. The traditional national security apparatus and military strategies offer physical protection, but today's warfare is conducted in the borderless cyberspace of Information and Communication Technology (ICT) where political, geographical, ethnic, and religious divides is no barrier. Militaries use physical weapons to protect physical assets from attacks; which are by themselves are now under a different type of threats – these weaponry are now run by software which could be hacked unto, compromised, or corrupted – requiring a different type of security to protect the "weapons of protection". Cyberspace infrastructures (software and hardware) are common and global, so also are their vulnerabilities. Exploiting the weakest link from any location (in any nation), attack on the cyberspace could be swift, precise, widely distributed, continuous, and could leverage physical attack - the basic "weapon"; a computer system with Internet access. Jaeger quoted Collin [1] that "...this enemy attacks us with ones and zeros..." (2006:16)

While dealing with specific threats, nations must take proactive steps to identify and remedy critical information infrastructure vulnerabilities. The responsibility for this is no longer the exclusive purview of the military, but of all owners and custodians of critical information infrastructure – including government, business organizations, infrastructure owners, infrastructure operators, and information security experts. It also requires international cooperation since the exploitation of vulnerability in one nation could be used to attack another nation. Therefore informs nations to search for new ways to protect nations and her assets (including military assets) from attacks.

C. Cyber-Security

A nation's cyberspace border is defined by her information infrastructure, which must be protected from attacks targeted at, or utilising the infrastructures. Though a prerequisite for the development of the information society, cyber-security is not an end in itself; but a means to an end; not a destination; but a journey. Recognising the increasing need for cyber security due to the growing dependence of governments, businesses, and other users on information technologies, the United Nations (UN) General Assembly Resolution 57/239 [2] noted that increasing interconnectivity now exposes information systems and networks to "…a growing number and a wider variety of threats and vulnerabilities which raise new security issues for all…" and therefore resolved that "…effective cyber-security is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society…" (2003:1) The Resolution therefore identified nine elements for creating a global culture of security thus; Awareness, Responsibility, Response, Ethics, Democracy, Risk assessment, Security design and implementation, Security management, and Reassessment.

Way back 2005, IT-advanced/driven/dependent economies like the UK, the USA, Canada, Japan, Australia, Malaysia and Germany already have in place documented measures to protect Critical Infrastructures and Critical Information Infrastructures from cyber-attacks, with many more joining; including international organizations and institutions such as the World Bank, the United Nations (UN), the European Union (EU), the North Atlantic Treaty Organization (NATO) and

Organization for Economic Cooperation and Development (OECD).

D. Critical Infrastructure (CI)

A fluid term as it were, critical infrastructure could be explained as a collection of national socio-economic activities and services that are essential to: national security; government sustenance; provision of a safe living environment; maintenance of day-to-day business, and security of a prosperous economy. Because of the critical nature of these activities, any interruptions to them "…must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare [of the citizens]" [3]. The UK's National Information Security Control Centre (NISCC) defines Critical Infrastructure (CI) as:

…those assets, services and systems that support the economic, political and social life of the UK whose importance is such that any entire or partial loss or compromise could: cause large scale loss of life; have a serious impact on the national economy; have other grave social consequences for the community; be of immediate concern to the national government [4]

Similarly, the United State's USA PATRIOT Act of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) defines it as: …systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters [6].

In Australia, infrastructures which, "…if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on social or economic well-being or affect national security or defence…" [5] are classified as critical. In Germany, "…all elements of the infrastructure whose failure would result in supply shortages or other dramatic consequences for large parts of the population…" are defined as critical [7]. The composition of critical infrastructure is dependent on what services are considered critical, while U.K. and U.S. policy documents attempted a definition of CI, Germany and Australia classifies CI. However, a common element is that CI affects the very core of human existence, economy, and the ability of state (public) and businesses (private) to operate and function.

From the foregoing, the definition varies from one nation to another. For a clearer perspective, the European Union's Green Paper on a European Programme for Critical Infrastructure Protection [5] identified some critical sectors and their products and services as shown in Table 1 below.

Table 1: Indicative List of Critical Infrastructure Sectors [5].

	Sector	Product or Service
1	Energy	a. Oil and gas production, refining, treatment and storage, including pipelines b. Electricity generation c. Transmission of electricity, gas and oil d. Distribution of electricity, gas and oil
2	Information, Communication Technologies, ICT	a. Information system and network protection Instrumentation automation and control systems (SCADA etc.) b. Internet c. Provision of fixed telecommunications d. Provision of mobile telecommunications e. Radio communication and navigation f. Satellite communication g. Broadcasting
3	Water	a. Provision of drinking water b. Control of water quality c. Stemming and control of water quantity
4	Food	a. Provision of food and safeguarding food safety and security
5	Health	a. Medical and hospital care b. Medicines, serums, vaccines and pharmaceuticals c. Bio-laboratories and bio-agents

6	Financial	a. Payment services/payment structures (private) b. Government financial assignment
7	Public & Legal Order and Safety	a. Maintaining public & legal order, safety and security b. Administration of justice and detention
8	Civil administration	a. Government functions b. Armed forces c. Civil administration services d. Emergency services Postal and courier services
9	Transport	a. Road transport Rail transport Air traffic b. Inland waterways transport Ocean and short-sea shipping
10	Chemical and nuclear industry	a. Production and storage/processing of chemical and nuclear substance b. Pipelines of dangerous goods (chemical substances)
11	Space and Research	a. Space Research

It was however suggested in [8] that for an infrastructure to be judged critical, over time, it must be vital to one or more national functions of: national defence, economic security, public health and safety, and national morale, as shown in Table 2.

Table 2: What Constitutes Critical Infrastructure over Time.

Infrastructure	**Criteria for being considered critical. Vital to…**			
	national defence	**economic security**	**public health and safety**	**national morale**
Telecommunications information network	x	x		
Energy	x	x		
Banking and finance		x		
Transportation	x	x		
Water			x	
Emergency services			x	
Government			x	
Health services			x	
National defence	x			
Foreign intelligence	x			
Law enforcement			x	
Foreign affairs	x			
Nuclear facilities, in addition to power plants			x	
Special events				x
Food/agriculture			x	
Manufacturing	x			
Chemical		x	x	
Defence industry	x			
Postal/shipping			x	
National monuments icon				x

Reference [7] therefore proffer a definition as follows:

A critical infrastructure (CI) is an infrastructure or asset the incapacitation or destruction of which would have a debilitating impact on the national security and the economic and social welfare of a nation.

There is no official classification of Critical Infrastructure Sectors in Nigeria, but the “Indicative List of Critical

Infrastructure Sectors" in Table 1 and "What Constitutes Critical Infrastructure over Time" in Table 2, gives an idea of what can be classified as "critical". This is further discussed in this paper.

E. Critical Information Infrastructure (CII)

There is indeed a thin line of classification between CI and CII. CII is part of CI; the lubricant for real-time, efficient and reliable CI service delivery. It is the information systems for critical infrastructure. Reference [9] argued that information technology (IT) could be viewed as a golden thread that runs through all CI, rather than been considered as a separate sector. In its submission, the PCCIP (1997) noted that the nation (USA) was becoming increasingly dependent on the combination of electrical energy, communication, and computers, which are susceptible to physical and virtual threats. In the UK, CII is viewed as a subset of CI, with the responsibility for its protection vested on the Home Secretary (with National Infrastructure Security Coordination Centre [NISCC] acting as the lead coordinator.) The same view is shared by the Australian government; classifying "National Information Infrastructure" (a variant of CII) as a subset of CI. The German's National Plan for Information Infrastructure (NPIS) addresses the concerns in the nation's CII. Whereas the U.S.A. [3] calls for protection from natural and man-made events, implementation focused more on man-made events such as cyber attack through hacking of computers and computer networks. On the other hand, the Executive Order (EO-13231) of 2002 [10] focuses entirely on information systems (CII) stating that the three functions of business transactions, government operations and national defence now depend on an interdependent network of critical information infrastructures, and therefore must be secured. The Executive Order states that:

It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible... [10].

D. Interdependencies and Vulnerabilities

The nature of interdependencies and connectedness among critical infrastructures oftentimes become vulnerability in a situation where the failure of one infrastructure weakens others. The researchers in [11] identified cascading as the major category of interdependent failures and define cascading (in the context of infrastructure) to mean:

…when a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently causes a disruption in a second infrastructure. [11.

E. CII Ownership

The liberalisation and deregulation programme in many nations have transferred the ownership of many public monopolies from state to private hands [12] submits that between 80 and 90 per cent of German critical infrastructures is managed by private companies. The same percentage is claimed to be true in the United States [13]. This ownership percentage informed the choice of "sector" as a unit of analysis [7] and makes the private sector a major stakeholder in the national protection programme – a situation which raises the issue of Public-Private Partnership (PPP) in the CIIP implementation.

F. Threats and Vulnerabilities in Information Infrastructure

Threat is a circumstance or event that has the potential to cause harm, and vulnerability is some weakness of a system that could allow security to be breached; a weakness that can be exploited to accomplish unauthorized or illegitimate use of a network or system. In recent times, factors relating to vulnerability include: increase in the number of automated functions and the type of transactions conducted via the Internet; sophistication within the attacker's community, with sophisticated tools and web sites offering detailed description of hacking methodology; increase in architectural programming language and protocols complexity; political factors such as act of terrorism; and budget constraints, which force government and organizations to limit security activities to immediate functionality. Information Infrastructure allows for shared threats, vulnerabilities and risks, but it does not make provision for shared protection and defence. Indeed, Internet is at the core of the information infrastructure and most economy and national security are fully dependent upon it. Of particular concern is the connection of systems which control physical objects such as Supervisory Control and Data Acquisition (SCADA) systems, and Distributed Control Systems (DSC). Aware of such risks, NSSC argued that, though planning such an attack requires high technical sophistication, nations must not be too optimistic, but must be seen to protect such critical infrastructures from cyber attacks, stating that "the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving." NSSC therefore suggested proactive steps to identify and remedy vulnerabilities.

III. THE FRAMEWORK

Critical Information Infrastructure Protection (CIIP) is the security of cyberspace, a combination of actions and programmes that identify the information infrastructure (and its specific components of human, physical and cyber), assess their vulnerabilities, and take mitigative or protective measures to reduce vulnerabilities. CIIP concept is based on all the security concepts of confidentiality, integrity, availability, authentication, authorization, and non-repudiation.

The Dependability Development Support Initiative of the EU concludes that CIIP initiative is a political, economic and social issue, hence a need for synergy between nations, as well as between public and private stakeholders. Furthermore, the annexure to the United Nations (UN) General Assembly Resolution 57/239 outlines eleven elements for protecting CII covering issues such as: emergency warning; awareness and education; interdependencies; standards, crisis management and CERT; public-private partnership; data availability policies; training; international cooperation; and research. At a

meeting convened by ITU-WSIS on Cyber-security in 2005, it was concluded that the worst enemy of security is complexity and that the greatest challenges to information system protection are non-technical; they are the inability to understand the complexity of interdependency of information infrastructure, and comprehending potential magnitudes and consequences of disruptions. The framework for the CIIP therefore differs from nation to nation in terms of initiatives, policies, organization, and private sector involvement. However, the perception and goals are similar in all nations. Below is a review of CIIP approaches by some nations and international organizations;

1. United Kingdom

The British government is concerned with the reliability and availability of all information systems to protect the interests of her citizens, recognizing two major threats to Critical National Infrastructures: terrorist and electronic attacks; viewing the electronic attack as targeted at computers and communication infrastructures. In her desire to facilitate the achievement of secure and resilient information systems in all sectors (public, private and individuals), the government released the Information Assurance strategy document which recognizes the confidentiality, availability and integrity of all information systems and recognizes five key areas to concentrate efforts, namely: protection of information systems; combating hi-tech crime; creating awareness and education on information security; capacity building for professionals; and international cooperation.

2. United State of America

Reiterating the goals established in [3], the reference [10] which defines CIIP, makes a distinction between Executive Branch Information Systems Security and National Security Information Systems. The Executive Branch Information Systems Security, under the Director of the Office of Management and Budget (OMB) is concerned with the development and overseeing the implementation of government-wide policies, principles, standards, and guidelines for the security of information systems that support Federal departments and agencies, States, Local Governments, and private sector. However, where a department or agency is identified as custodian of national security information, then the Assistant to the President for National Security Affairs, the Secretary of Defense, the Director of Central Intelligence, and the affected departments and agencies, shall develop policies, principles, standards, and guidelines for the security of national security information systems that support the operations of such departments and agencies. Complementing the EO 13231 [10] is the National Strategy to Secure Cyberspace (NSSC) whose objectives include the prevention of cyber-attacks, reduction of vulnerability to such attacks and minimizing damage and recovery time [8]. The Strategy also empowers all Americans to secure the part of cyberspace they control. The Homeland Security Strategy identifies the government's role as setting and enforcing standards and protecting public interest. CII custodians are required to provide information about their current security to the Department of Homeland Security (DHS) for compilation. The United State Computer Emergency Readiness Team (US-CERT), in conjunction with the National Cyber Security Division (NCSD), maintains an early warning mechanism for computer incident reporting

3. European Union (EU)

EU views CII as cutting across all CI sectors, suggesting that CIIP activities be coordinated with CIP. The EPCIP defined CIIP programme as: the programmes and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of CII in case of failures, attacks or accidents above a defined minimum level of services and aim at minimizing the recovery and damage. (2005:19)

The EPCIP as a complementary initiative to individual national efforts, places more emphasis on collaborative research programmes. With the establishment of Critical Information Infrastructure Research Coordination (CI2RCO) to encourage Europe-wide approach for research, EU issues directives for the protection of CII. Also in the offering is the establishment of a Critical Infrastructure Warning Information Network (CIWIN), whose purpose is to harmonise the exchange of information on shared threats and vulnerabilities and appropriate counter-measures and strategies, among member states.

IV. IT SECURITY VERSUS CIIP

IT Security is concerned about safeguarding of processes and security of company infrastructures, mostly technical, and practice-oriented. At the maximum, its scope of coverage is from the IT asset (Platform Level) up to the corporate WAN with distributed nodes across the globe (Company Level). On the other hand, CIIP is concerned about security at the national level, a combination of IT management, Security management, and IT security management. It is technical, physical, physiological, and organizational; focusing on the identification and recognition of national security status, early warning and incident recording, supply security, interdependencies, political strategies and transnational cooperation. It is concept-oriented, and coverage scope is from the Company Level up to National Level. CIIP is mostly government-driven with significant input from the private sector; a network of trust on PPP relationship. The Trans-national Level is based on alliances and bi-lateral/multi-lateral agreements on issues such as Standards and Best practices and criminal prosecution. Figure 1 shows the relationship model between IT Security and CIIP.

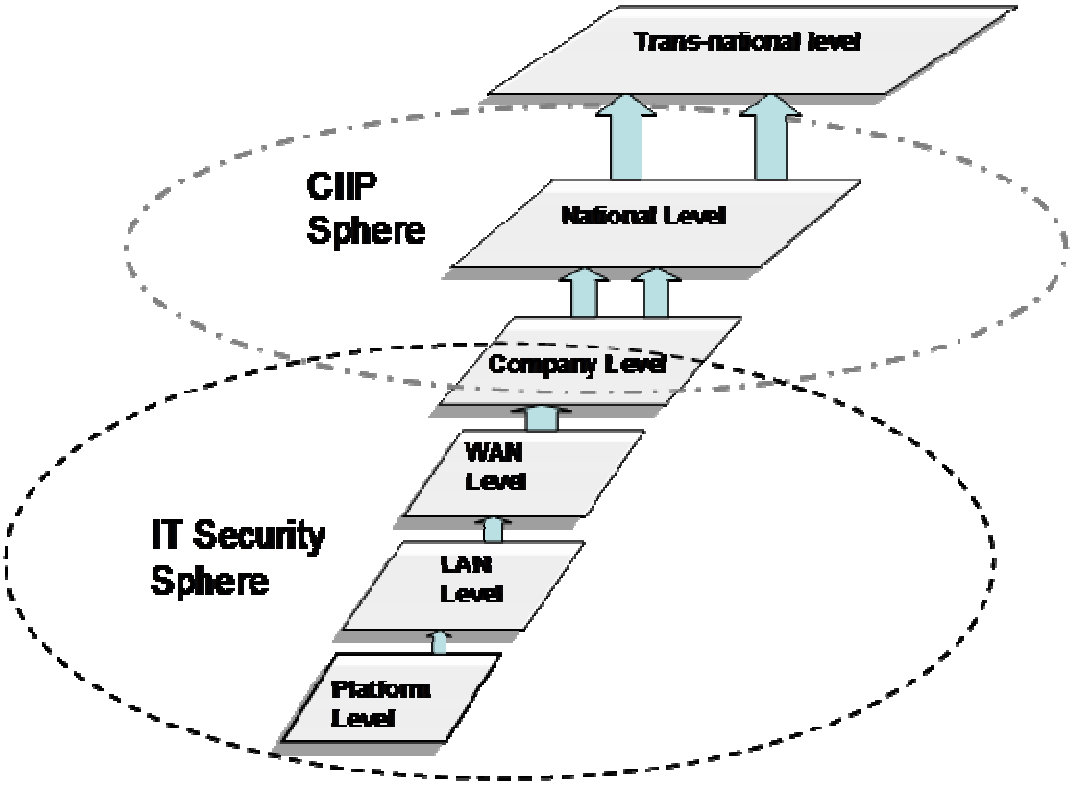


Figure 1: Relationship between IT Security and CIIPs.

F. CIIP Fundamentals

A common fundamental denominator to the CIIP concept is the understanding of the concept (in the context of individual nations), and the political and moral will to apply the concept. National security, crime prevention and law enforcement are the major reasons for all nations. In addition, counter-terrorism, business continuity and information assurance, economic growth, and State secrecy are other reasons. Generally speaking, CIIP concept helps to enforce (or suggest) some sort of standardisation and information assurance, since all participating actors will invariably conduct a risk analysis of their operationsand services.

G. Definition, Identification And Classification Of Critical Assets

This is the most fundamental of all. Based on the assumption that protection of citizens, national survival and economic safety are at the core of national interest, a nation must first define "criticality" in these terms and in consideration of issues raised above. For example, India and Japan consider IT as an essential component to their nation's quest for becoming an advanced IT society and technology superpower. Also, from national security perspective, the government determines the level of damage impact that is acceptable to the society. This definition then informs the identification of what assets and services are critical. This identification process requires the complex task of determining the criticality of an infrastructure and identification of CI. In general terms, this identification requires input from government, technocrats, experts and the private sector, whose diverse opinions are shaped by organizational background and subjective viewpoint. However, the EU Commission [7] suggests the following three factors as key considerations to the identification of critical assets and services: Scope (extent of loss in terms of geographical spread), Magnitude (the degree - ranging from "none", "minimal", "moderate", to "major"- of the impact on public health and safety, economic, interdependency, environmental, and political), and Time (ascertains time effect of impact - from immediate to infinity). Whatever is the tone of definition, CIIP will always be seen as comprising issues of national security, economics and law enforcement (cyber-crime); and rightly so. The popular unit of classification of assets is by "sector" (United States), based on services rendered.

H. Overview Of IT Security Situation

After identification, the state will need to ascertain if there are possibilities of threat and what indeed could be threatened. This could be factored from various perspectives including: government policy; ideology affinity; or business outsourcing. For example, support of the Spanish and British governments on the Iraq war raised the threat level to an all-time high. A general overview of the cyber threat, with a focus on the identification of national IT security situation and IT dependency and interdependency within the nation's cyberspace will be conducted.

I. Risk Analysis

At the completion of identification of critical assets and IT security situation, a comprehensive risk analysis of each sector will be conducted to analyse what threatens the assets (risk identification), the likelihood of the threat manifesting (risk quantification) and the consequences of the manifestation (risk measurement). Once established, it is necessary to establish what can be done to avert the incidence (risk evaluation), reduce the impact (risk acceptance) and risk management. Indeed, this is done by individual organizations (government establishments, operators and CII custodians) in each sector, and then summarised into a national Risk Management document.

J. Legal framework

For any programme to be successfully implemented and enforced, it must have some form of legal backing. CIIP related legislations address issues like data protection and privacy, cryptography and digital signatures, and minimum standards for information security. Both UK and USA have various policies and legislations in support of the CIIP programme.

K. Early Warning

Early warning system plays a major role to achieving efficient and effective CIIP. It is a system of analysing threats and vulnerabilities and disseminating early warning to those concerned. It enjoys support and patronage of government, industry and individuals. Perspectives of early warning system include: IT-technical which perceives CIIP as IT security; Prosecutor which perceives CIIP as the protection of society from cyber-crime; and Security-policy which perceives CIIP as a policy for combating IT incidents. Although many of the CIIP assets are operated privately, government is a major player in providing the legislation, intelligence services, and the lead role.

L. National Organization Structures

For an effective and successful implementation, the organizational structure is defined at the national level. A number of different agencies may deal with specific aspects of CIIP programme; however, there is a coordinating agency in every nation. In Nigeria, the office of the National Security Adviser (NSA) to the President is the coordinating agency in Nigeria.

V. THE GUIDELINE

The guideline highlights some of the management and technical details that guarantee the mitigation of risk (in the context of CII) to an acceptable level; maintaining that level, and ensuring that the CII continues to operate when under attack. This guideline will assist government, custodians and operators of Critical Information Infrastructure to: define; identify and classify threats, impacts and mitigation. The approach of the guideline is to place emphasis on the tasks/activities of a coordinating agency. However, such tasks/activities to be performed by CII organizations (custodians and operators) will be clearly indicated.

a) The Coordinating Agency

The Cybercrime Act (2015) invested the powers relating to Critical Infrastructure on the office of the National Security Adviser (NSA). This serves as a good starting point for policy formulation with NITDA and private operators providing the technical support.

b) Identification Of Critical Information Infrastructure (CII) Custodians, And Lead Agencies

The identification of CI/CII in Nigeria may follow in line with the "Indicative List of Critical Infrastructure Sectors" in Table 1 and "What Constitutes Critical Infrastructure over Time" in Table 2 above. In consideration therefore, the following assumptions could be made:

a The Federal Government is responsible for national security, economic security, and national public health.

b The Federal Government is responsible for the security of the nation's cyberspace.

c Operators are responsible for security of their IT.

d Both government and operators depend on secure IT.

e. Government is leading in cyber-security campaign and initiatives.

In consideration of the above an indicative list of Lead Agencies and their roles are listed in table 3 below:

Table 3: Lead Agencies and Roles.

AGENCY	ROLE
Office of the National Security Adviser (NSA) to the President	Overall Policy formulation, standards and initiatives.
Ministry of Defence	Guideline implementation on Command and Control (National Security) System
Nigeria Communications Commission (NCC)	Guideline implementation in the Telecommunication sector – Public and private telephone networks, SAT3, Satellite and VSAT deployments.
Central Bank of Nigeria	Guideline implementation in the Banking and Finance sector
Department of Petroleum Resources	Guideline implementation in the Gas and Oil sector

M. Point Of Contact (POC)

Every organization will be expected to identify an official who will be responsible for the overall coordination of the CIIP programme within the organization. Designated as the Chief Information Security Officer (CISO), she/he will be the POC for the organization; liaising with the national CIIP coordinating agency and her/his duties will include the development and implementation of security procedures such as:

a. Providing corporate leadership and overall management direction for the security and CIIP programme.
b. Directing the development and implementation of security procedures that comply with government requirements.
c. Performing common managerial accountabilities such as IT security budget.
d. Providing necessary resources for the administration of the corporate Information Security Programme
e. Developing overall corporate access control strategy and correcting leaks and vulnerabilities.
f. Coordinating information security awareness and training needs and activities.
g. Involvement in the formulation of Contingency plans and coordinating the implementation of the plans during an emergency.

D. Emergency Management - Contingency Plans

Each of the designated organizations will be required to develop contingency plans - processes that help organizations prepare for disruptive events. These plans will document procedures on what to do and how; guarantying organization's ability to keep rendering services. Depending on the size and scope of the establishment and the way it does business, the details will vary. The plans should address the following issues among others: objective of the plan; scope and applicability; assumptions; who is responsible for taking what action; list of Contingency Plan personnel; inventory listing (hardware and software); dependency agencies; offsite crisis meeting places; alternate means of communication; and partnerships with local emergency response groups. At the very least, the following Plans should be in place:

a. Business Continuity Plan (BCP): BCP is a document detailing how an organization will rapidly restore normalcy after a disaster or disruption of critical function. BCP is part of ISO/IEC 27001, and it based on risk assessment of the organization.
b. IT Contingency Plan (ITCP) and Disaster Recovery Plan (DRP): ITCP defines procedures for recovery of prioritized systems at the primary site. DRP on the other hand defines procedures for recovery of IT capabilities at an alternate site.

E. Improved Awareness And Skill

The human component is key to the success of any programme; CIIP inclusive. IT-security competence requires knowledge of its significance, as well as an understanding of the security level and one's own responsibilities. There is therefore need for deliberate advocacy and mobilisation by the Programme Coordinator to the CII custodians on the one hand; and by the organizations to their employees on the other hand. Also, in the long term, the Federal Government of Nigeria will make deliberate policy to train her citizens in the art of Information Assurance, Information Warfare, and Information Operations; similar to the North Korean's policy.

F. Corporate and Systems Characterization and Assurance Indicators

This task is to be performed at the organizational level, coordinated by the Lead Agencies and consolidated/summarised by the Programme Coordinator at the national level. The task identifies; functions or services that the organization provides, ownership, size and location, the underlying CII assets, Key Resources, and their criticality. It also identifies the information

infrastructures boundaries, system and organizational dependencies (such as telecommunication providers), network architecture and topologies, technical hardware and software protocols, block diagrams, management and operational controls (such as summary of how IT security is managed, security teams and contacts), current protection (if any), and backup procedures. Finally, it describes the impact of loss in terms of economic, social, political and life-threatening consequences. The output from this step is the description of the designated custodian of CII, its environment and delineation of its boundary.

G. *Corporate Assurance Indicators*

Assurance indicators are used to ascertain the level of preparedness of an organization towards the likelihood of manifestation of threat. All identified and designated CII custodians will undertake a high level IA Assessment to ascertain their level of compliance to the universal assurance indicators (NISCC Assurance Report, 2004) as explained below;

a. Management Commitment: This will indicate the support and understanding of the Management (preferably at Board level), of the concept of information security.

b. Information security policy: A document providing framework of overall corporate information security and protection.

c. Business Continuity (BCP) and Disaster Recovery (DRP) Plans: Two distinct documents. BCP is a documented predetermined set of procedures and/or instructions to be followed to guarantee the organization's functions during and after a significant disruption. DRP is a documented set of recovery procedures to be followed in the event of a disruption.

d. Penetration Testing: A comprehensive internal IT Security Checks (Audit) to measure compliance and check vulnerabilities by performing various reconnaissance scans against the organization's information security infrastructures.

e. ISO27001 (Information Security) Accreditation/Compliance: ISO27001 (Information Security) is the universal standard for information assurance. The organization may not necessarily be accredited but should, at least be compliant.

f. Use of CERT: This is the reporting of IT security incidents; to ascertain if the organization subscribes to any CERT.

g. Contact with External Security Experts: This is the outsourcing of elements of information security.

h. Recruitment Verification checks: This is the process of vetting key staff before employment and the inclusion of security responsibility and information disclosure procedure in the terms of employment.

These indicators are set out in a matrix grid of 4-level of assurance maturity from "No progress to best practice" to "Recommended best practice"(see Appendix A) Each of the designated organizations will be encouraged to work towards attaining the "Recommended best practice."

H. *Systems Assurance Indicators (for each system)*

Similar to the above task, assessment of all identified critical systems will be undertaken to ascertain assurance levels (whether the organization has a policy or practice in place) of each critical system or network, using the following systems assurance indicators [14] as follows;

a. Security policy: Does the organization have one for each system?

b. System Access Points: Has the organization identified and managed access points?

c. Network services protection: Is there a restriction on network services such as network scanning, pinging, SNMP, and Internet access?

d. Software Patches: What is the organization's procedure for patches implementation?

e Anti-virus Protection: Is Anti-virus protection managed centrally, on individual systems (clients), or not in place?

f. Password Policy: Is it adequate and of international standard?

g. IDS: Is it installed and adequate on the critical network under review?

h. Penetration testing and System Auditing: How regular and by whom (internally, or by external companies)? Are external companies approved?

i. System dependencies: Has the organization identified and managed the dependencies for each system?

j. Change control procedures: What are the procedures?

k. Information backup procedures: What are the procedures?

These indicators are set out in a matrix grid of 4-level of assurance maturity from "No progress to best practice" to "Recommended best practice" (see Appendix B) Each of the designated organizations will be encouraged to work towards attaining the "Recommended best practice."

VI. RISK MANAGEMENT PROCESS

This task is to be performed at the organizational level, coordinated by the Lead agencies and consolidated/summarised by the Programme Coordinator. Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence, a function of the likelihood of a threat agent exploiting a particular potential vulnerability. Risk Management is a continuous process of identifying risk, assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. All identified and designated CII custodians will therefore undertake a high level Risk Management process to access vulnerabilities and threats and the level of protection given to the CII assets in their custody. Vulnerabilities include those within and around the system or services and threats are those in a position to exploit those vulnerabilities. Every organization must

demonstrate that the risk management activities reduce the identified risks to an acceptable level – reducing the extent to which the vulnerabilities within or around the system are exposed to threat. Tasks include:

N. Risk Assessment

This is the process to determine the potential threat and the associated risk. Information on technical vulnerabilities can be derived from Common Vulnerabilities and Exposures, NIST ICAT [15] Vulnerability database, and SGI Vulnerability Database.

1. Vulnerability Assessment (Penetration Testing): Since vulnerabilities (weak links) exist throughout the information system process, this process identifies all the weakness that may be exploited, by examining the various attack techniques, possible avenues of attack and all known technical vulnerabilities. The output from this step includes categorization of attack techniques (including denial of service, network intrusion, malicious hardware, Trojan software and viruses), possible avenues of attack, and a list of specific systems vulnerabilities in the organization's hardware, software, networks and architecture. This task is best implemented by engaging the services of a Penetration tester.
2. Threat Assessment: Agents of threat could be natural, malicious or system issues. The assessment therefore examines the various threat sources and threat levels, with particular details to the capacity, motivation, amplifiers and inhibitors of the malicious agents. The output from this step is the threat statement containing a list of threat agents/sources and an estimation of the motivation, resources, and capabilities required for a successful attack.
3. Minimum Security Control Analysis: Security controls are prescribed countermeasures for the protection of CII to assure the confidentiality, integrity, and availability of the system - a proactive procedure to eliminate or reduce the impact of manifested threat. This process therefore ascertains the availability of these security controls, implementation of the selected controls; and the assurance that the implementations of the selected controls are effective. The output from this step is a list of existing controls and planned controls.
4. Likelihood Ratings: Based on the outputs from all the above, a Likelihood rating of the likelihood of manifestation is derived. The likelihood level could be any of:
   Low: The threat-agent lacks enough motivation and/or competence, and there are effective security controls in place to prevent, or inhibit manifestation.
   Medium: While the threat-agent has enough motivation and competence, there are sufficient security controls in place to impede manifestation.
   High: The security controls are ineffective and insufficient to prevent or hinder the highly motivated and sufficiently capable threat-agent.

O. Impact Analysis (Security Categorization):

Based on the services rendered and statutory function performed by designated organization, the security controls applicable to the CII in the organization should be commensurable with the potential impact, should there be a breach in security objectives of confidentiality, integrity, and availability. Based on the Risk Assessment of the organization, the impact could be categorized as low, moderate, or high. The potential impact values are the highest value from among the identified security categories of confidentiality, integrity, and availability. The NIST-800-30 (2004) [15] contains a generalized categorization format:

SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)},

(where the acceptable values for potential impact are Low, Moderate, or High.)

A low-impact system therefore, is a system in which all the three of the security objectives are low. A system is categorized as of moderate-impact if at least one of the security objectives is moderate and none is high. A high-impact system has at least one high security objective. The output is a qualitative magnitude of impact (high, medium, low) as shown in Table 4:

Table 4: Magnitude of Impact Definitions [15].

Level	Definition
Low	• May result in the loss of some tangible assets or resources or • May noticeably affect the nation's security, mission, reputation, or interest.
Medium	•May result in the costly loss of tangible assets or resources; •May violate, harm, or impede the nation's security, mission or interest; or •May result in human injury.
High	•May result in the **highly** costly loss of **major** tangible assets or resources; •May *significantly* violate, harm, or impede the nation's security, mission, reputation, or interest; or • May result in human death or serious injury.

P. Risk Level Determination:

The risk level to a system is a factor of the threat likelihood level and impact level. This is calculated by multiplying the weights of threat likelihood level and impact level (Tables 5) in a matrix. The weights assigned for each level of threat probability are: 1.0 for High; 0.5 for Medium; and 0.1 for Low. Likewise for the impact level; 100 for High, 50 for Medium, and 10 for Low (see Table 4 above). The result from matrix computation is either of Low Risk level, Medium Risk level, or High Risk level. Risk level to a system is a calculated weights of the threat likelihood level and impact level. This level could either be low, medium or high.

Table 5 Risk-Level Analysis.

Threat Likelihood	Impact		
	Low (10)	**Medium (50)**	**High (100)**
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

The final output of the Risk Assessment process is a Risk Determination Table, as shown in Appendix C

Q. Risk Mitigation Priorities

Since elimination of all risk is not feasible, this process seeks to prioritize, evaluate, and implement security controls (as recommended during the risk assessment process), so as to reduce risk to an acceptable or manageable level and minimal impact. High level risks should take priority over Medium, and Medium should take priority over Low. Risk mitigation is a function of Security Controls principles of: prevention; detection; recovery; and support, using any (or combination) of risk mitigation options: Risk Assumption; Risk Avoidance; Risk Limitation; Risk Planning; Research and Acknowledgement; and Risk Transference. The output of Risk Mitigation is an Action Plan which will contain information such as:

a. Risk Assessment Report; including all security controls, prioritized list of actions, and selected security controls for each action;

b. Resources required for implementation, including roles and responsibilities for management and staff;
c. Start and completion dates for implementation; and
d. Required maintenance.
Based on mitigation rules (see Table 6 below), the mitigation strategies will be implemented in form of Security Controls. The framework for Security Controls will be developed by the coordinating agency, while each organization will adapt it for their peculiar needs.

Table 6: Mitigation Strategies.

Threat condition: When….	Action
vulnerability to an attack exists	Apply administrative controls and assurance policies to reduce the likelihood of manifestation.
a vulnerability to an attack can manifest	Apply security controls and layered protections to reduce risk impact or prevent manifestation.
cost of attack is less than the potential gain	Apply security controls and layered protections to increase cost of attack.
loss to an attack is too great	Apply all technical and non-technical protections to reduce the *extent* of the attack.

Management Security Controls focus on the maintenance of standards and development of policies and guidelines, which outline acceptable and legitimate system use and clarify system abuse and deterrents. The following activities are part of the control:

a Authorization of risk assessment.
b Assigning security responsibility.
c Development and maintenance of system security plans.
d Implementation of security controls for personnel.
e Approval and coordination of security awareness training for end users.

Operational Security Controls focus on the establishment of guidelines for the proper and safe use of information systems, with emphasis on prevention from, and detection of attacks. Included in these controls are the following:

a Provision and control of physical and environmental security.
b Controlling of data media access, distribution and disposal.
c Virus software controls.
d Provision of backup capabilities, establishment of off-site storage procedure, and emergency power source.

Technical Security Controls This is the most elaborate part of the security controls, categorised into three broad areas of; support, prevent, and detect/recovery. The supporting technical control is the most basic, the foundation upon which other technical controls is built. It includes; identification, security administration, systems protections, and cryptographic key management. The preventive technical controls are those configured to stall violation of security policy. In this category are: authentication, authorization, access control enforcement, non-repudiation, protected communications and transaction privacy. The third category of technical control is the detection and recovery, which is put in place for early warning against violation and compromise to a system and restoration of lost resources. Included in this category are: audit, intrusion detection and containment,

restore secure state, and virus detection and eradication. This is addressed in detail below.

R. Technical Controls

Technical controls are Information Assurance (IA) technologies addressing issues that are mostly implemented on the physical network. However, the framework for these controls will be the responsibility of the programme coordinator who will ensure compliance. The CISO of each organization will ensure implementation. Three generations of IA technologies are identified; based on their goals. The goal of the first generation is to prevent intrusions by providing multiple levels of security, access control, physical security and cryptography. Second generation's goal is to

detect intrusions using firewalls, IDS and domain boundary controller. The third generation aims at survivability – ability to operate even when under attack. These generations covers the three basic concepts of Access control, Individual accountability, and Audit trails. These technical controls cover the basic practices under the three generations:

1. Prevention

Included in this; system administration, access control and authentication, and firewall. While the coordinating agency will propose policies on logs, password and auditing, and certify firewall devices, the CISO will ensure controlled and monitored access to the physical network, maintain user list, enforce password policy, apply encryptions, and manage firewalls. She/he will also ensure that all default passwords and configurations are disabled or deleted (where possible).

2. Detection

The main control here is the Intrusion Detection Systems (IDS). The implementation is at the organization level to ensure that IDS systems are in place, regularly updated, and frequently audited.

3. Survivability

This addresses issues such as data and systems backup, off-site and on-site activities, and recovery policy. Organizations with detailed recovery plans respond better to the attacks – with the ability to operate from a "hot site" within few hours/days after an attack. Survivability therefore starts with basic data and application backup policy of: how often is backup tested; who is responsible for backup; storage location for backup systems; and such similar issues.

S. Statement Of Commitment

"If it is not written down, it did not happen" so goes the popular saying. Although there are standards for compliances in some sectors, the present business settings and patronage in Nigeria do not make provision for compliance to international standards of information security. Particularly, ISO27001 outlines the code of practice for information security management (security techniques), which most businesses are requested to comply with. While the relevant legislations for such compliance are being promulgated, everyone of the CII custodians may be requested to have organizational commitment statement, signed by the CEO or Board Chairman, outlining their commitments to the IA process and verifying their responsibility for sustaining security measures on their individual network. A generic commitment statement - an adaptation from the GSi Code of connection - is contained in Appendix D

T. The Checklist

As a summary of all that has been discussed, a comprehensive list of all the security objectives and relevant activities was complied into The Checklist - an adaptation of the World Bank's Technology Risk Checklist (The World Bank, 2004). As its title, it will be used by the CIIP Coordinator to monitor maturity progress of all designated CII custodians. The Checklist covers nine areas of Organizational and Assets management; Policy management; Patch management; Access control and authentication; Firewalls; IDS; Virus management; Penetration testing; and Systems administration. A full detailed list is as contained in Appendix E

VII. CONCLUSION

Despite the variations between countries in terms of definitions of CIIP, the goal of the programme is universal: to protect; detect; respond to; and recover from cyber-attack, so as to guarantee availability; reliability; safety; confidentiality; integrity; and maintainability of critical services rendered to the citizens. However, this requires an understanding of the nature and magnitude of threats to the infrastructures. Nations therefore take a systematic and pragmatic approach to the implementation of the programme, in line with their varied concerns and interests. The guideline along with the accompany annexure covers issues fundamental to the CIIP programme from understanding the problem, to defining the goals and undertaking risk assessment. It also touched on best practices and includes a list of Security objectives (Checklist) to guide operators.

References

[55] Jaeger, C. (2006) 'Cyberterrorism and Information Security' in Bidgoli (ed) Handbook of Information Security (Vol 2) New Jersey: John Wiley, pp 16-39

[56] UN Resolution 57/239 (2003) Creation of Global Culture on Cybersecurity [online] Available from: http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf

[57] PDD-63 (1998) White Paper [online] Available from: http://www.usdoj.gov/criminal/cybercrime/white_pr.htm

[58] NISCC (nd) What is the Critical National Infrastructure [online] Available from: http://www.niscc.gov.uk/niscc/aboutCNI-en.html

[59] EPCIP (2005) Green Paper on a European Programme for Critical Infrastructure Protection [online] Available from http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf

[60] USA PATRIOT Act (2001) Critical Infrastructure Protection [online] Available from: http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107SZlxPX:e415432:

[61] Abele-Wigert, I and Dunn, M., (2006) International CIIP Handbook 2006, Vol 1, Zurich: Center for Security Studies

[62] NSSC (2003) The National Strategy to Secure Cyberspace [online] Available from: http://www.whitehouse.gov/pcipb/

[63] BCS (2006) The Cyber Structures That Matter Most [online]. Available from: http://www.bcs.org/server.php?show=ConWebDoc.5569

[64] EO-13231 (2002) Critical Infrastructure Protection in the Information Age [online] Available from: http://www.ncs.gov/library/policy_docs/eo_13231.pdf

[65] Zimmerman, R and Restrepo C.E (2006) 'The next step: Quantifying Infrastructure Interdependencies to improve security' in International Journal of Critical Infrastructures, 2(3):215-230G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (references)

[66] Helmbrecht, U. (2005) CIIP - A New Challenge for Governments [online] Available from: http://www.bsi.de/bsi/reden/210305Chatham_en.pdf

[67] Rak, A. (2002) 'Information Sharing in the Cyber Age: a Key to Critical Infrastructure Protection' Information Security Technical Report, Vol 7, No. 2 (2002) 50-56

[68] NISCC (2004) Assurance Report for "The CNI Organization" [online] Available from http://www.niscc.gov.uk/niscc/docs/re-20040601-00394.pdf

[69] NIST-800-30 Risk Management Guide for Information Technology Systems [online] Available from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

APPENDIX A: CORPORATE ASSURANCE INDICATORS

No	Assurance Indicator	Little or no progress to best practice	Some progress	Significant progress	Recommended best practice
1	**Information Security Policy**	No published policy document	Published policy document	Published policy document, available to all users responsible for security	Published policy document, approved by board, regularly reviewed, accepted by all users responsible for security
2	**Business Continuity Plan (BCP)**	No plans.	Plans being developed	Plans in place	Plans in place and tested regularly
3	**Penetration Testing (*Pen test*)**	No recent *Pen test*	Recent *Pen test* but no regular schedule	Regular *Pen test* – standard unknown	Regular standard
4	**Compliance with ISO17799 standard**	Unaware of standard	Aware of standard – compliance has been considered	Compliance with some aspect of standard	Certification/full compliance with standards
5	**Use of CERT**	Not involved in any CERT	Member of CERTs	CERT messages disseminated appropriately in organization	Contributing to CERT
6	**Contact with external Security experts**	No contacts	Occasional contact with one or more experts	Regular contact with limited range of experts	Regular contact with wide range of experts
7	**Contact with external security group**	No contacts	Some contact with relevant groups	Membership of a limited number of relevant groups	Membership of a wide range of relevant groups
8	**Recruitment verification check**	Little consideration of verification check	Developing verification checks for key staff	Has verification checks for key staff	Compliance with BS7858 or other similar standards

APPENDIX B: SYSTEMS ASSURANCE INDICATORS

No	Assurance Indicator	Little or no progress to best practice	Some progress	Significant progress	Recommended best practice
1	**Security Policy**	Policy not in place	System security policy being developed or inappropriate	Appropriate system security in place but implementation needs improvement	Appropriate system security policy implemented effectively
2	**Identification of System access point**	Little or no consideration of access point	Some access points identified/documented	Most access points identified/documented	All access points identified and documented
3	**Protection of networked services**	No protective measures in place	Few protective measures in place	Some protective measures – could be more effective	Appropriate protection in place
4	**Application of software patches**	No policy – patches not applied routinely	Policy under consideration	Policy on patches exists – implementation could be more effective	Policy of prompt application of software patches – implemented effectively
5	**Anti-virus protection**	No anti-virus protection	Anti-virus protection being considered	Some anti-virus measures – could be more effective	Appropriate anti-virus policy and effective implementation
6	**Password policy**	No password policy	Password policy in development or inappropriate	Appropriate password policy but little evidence of implementation.	Appropriate password policy implemented effectively
7	**Intrusion Detection procedures**	No intrusion detection procedures in place.	Intrusion detection procedures being considered	Some intrusion detection procedures – could be more effective.	Appropriate intrusion detection procedures in place
8	**Auditing of System**	No auditing of system	Auditing under consideration	Occasional auditing	System regularly audited
9	**Systems dependencies**	Dependency not identified	Some dependencies identified	Most critical dependencies identified	All critical dependencies identified

APPENDIX C: RISK DETERMINATION TABLE

System Name or Sequential Number	Function	Threat	Risk Description	Impact	Security Controls	Likelihood of Occurrence	Impact Severity	Risk Level

APPENDIX D
GENERIC STATEMENT OF COMMITMENT

On behalf of the organization listed below, I confirm that my organization is a custodian of a Critical Information Infrastructure and will therefore endeavour to uphold the Confidentiality, Integrity, and Availability of same.

Layers of Electronic Security	Security Objectives
1. Organizational and Assets Management	1. Board and Management are aware of Cyber-risk to the organization's operations.
	2. The organization's mission and philosophy includes provision for Cyber-risk.
	3. The organization's budget provides for enlightenment and training on Information security issue.
	4. There are clearly defined roles and responsibilities towards information security in the organization's core services.
	5. The organization has determined acceptable levels of cyber-risk.
	Organizational Management
	6. The organization has a Chief Information Security Officer-CISO (or such officer) with clearly defined roles and responsibilities.
	7. The security programme aligns with overall long term and short term plans of the organization.
	8. Security considerations are a routine part of normal business processes, systems designs and implementation.

	9. A protection strategy and risk mitigation plan is in place to support the organization's mission and priorities.
	10. A risk management framework for the identification and prioritization of information assets been performed.
	11. Framework for performance measurement of the security objectives is in place.
	12. There exists a designated officer who is responsible for keeping records of cyber intrusions, costs of remediation, response time, and documenting procedures and processes
	Asset Management
	13. There is a properly documented inventory of all access point to the organization's network, identifying potential points of vulnerabilities.
	14. The organization has an asset based threat profile.
	15. Risk assessment is conducted regularly with resulting action plan.
	16. There exists a network topology diagram, up-to-date and regularly updated
	17. Systems are properly configured according to designated architecture and the configuration is regularly reviewed.
	18. There exists a procedure for policy enforcement.
	19. The CEO and Board are abreast with organization's security level.
	20. The CISO authorizes all hardware and software acquisitions.
2 Policy Management	1. Board and personnel aware of their liabilities.
	2. There exists a comprehensive information policy and auditing process.
	3. There is a guideline for security auditing process.
	4. All security policy "owners" are qualified in their respective areas and are up-to-date on security issues.
	5. All new users receive detailed orientation on security policies and procedures and old users receive periodic security awareness training. All users have a copy of the policies and procedures and they have all signed to abide by them with penalties for non-compliant.
	6. All business associations, partners, contractors or customers that have access to the organization's computer systems are aware of the various security policies and procedures and have agreed to abide by them, with penalties for non-compliant
	7. All managers at each level of the organization understand their roles and responsibilities with respect to information security.
	8. The security policies address both internal and external access to the corporate network.
	9. There is a clearly defined role for each user in backing up the user data on their systems.
	10. There is a standard procedure for restoring a backup file.
	11. There exists a help-desk and/or points of contact (POC) at various levels to help resolve all IT-related issues.
	12. There exists a procedure to regularly review all VPN log files, system log files, firewall logs, IDS logs, etc by designated officers.

	13. All computer systems are regularly updated with critical patches and virus definitions.
	14. All hardware and software are standardized and properly licensed with manufacturers.
	15. Users are held accountable for the actions of their individual computer.
	16. No corporate sensitive and confidential data are available to remote users.
	17. Remote users have limited access and are restricted to certain log-on hour. Authentication process utilizes at least at a two-factor authentication system.
	18. All remote access computers utilize VPN and firewall software, and are certified for use by the CISO.
	Personnel Policy
	19. There is a standard procedure to conduct background checks on all personnel and contractors
	20. There is an employee "code of use" of E-mail, Internet, and Instant Messaging within the organization's network.
	21. All employees are trained on network security basics.
	22. All employees are made aware of their accountability for Internet activity associated with their individual user accounts
	Third Party Outsourcing Policy
	23. All outsourced personnel sign non-disclosure agreements and have received information security awareness training.
	24. All security controls outside the direct authority of the CISO (due to outsourcing) have been identified and documented
	25. The CISO has reviewed all relevant policies, procedures and standards that govern security requirements for outsourced service providers, customers, and business associates.
	26. Outsourcing contracts include clause requiring outsourced entities to notify the organization of major security incidents.
	Physical Security Policy
	27. Access to networked systems facilities is controlled and monitored.
	28. Systems facilities are securely locked at all times and equipped with alarms to notify of intrusion.
	29. There exists an officer who regularly checks audit trails of failed logs.
	30. Backup copies of software are safely secured on and off site.
	31. All sensitive areas are under constant surveillance watch and tapes are safely secured.
	32. Systems facilities work area (environment) is well conditioned and controlled.
	33. All IT assets are protected by automatic voltage regulators (AVR) and power backup systems.
3. Patch Management	1. The organization subscribes to CERT for regular patches updates.
	2. All patches are verified for integrity and tested on isolated system (test beds) before deployment.

	3. Systems are backed up before patches application.
	4. Patches updates are widely disseminated throughout the organization
4. Access Controls and Authentication	1. Authentication for System Administrators is more elaborate than ordinary user – may consider 2-factor authentication.
	2. User access is approved by senior managers and verified by the CISO.
	3. Standard and separate password policy exists and implemented. Users passwords are robust (long in length; mix of letters, numbers, and symbols), automated enforcement of password change, password reusability, unique user ID to each individual, and no shared ID.
	4. Regular checks of audit logs for failed logons, last logons and logon time stamps.
	5. Regular review of network users and groups list
	6. No root-level access request granted remotely. Request is only authorized by the CISO.
	7. Access controls of former employees are deactivated immediately.
5. Firewalls	1. The organization's firewalls are nationally certified and regularly tested updated.
	2. There is a comprehensive list allowed/disallowed traffic through the firewall.
	3. All network ports not required by applications on the organization's systems are blocked.
	4. All network protocols not in use by the organization are disallowed on the firewall.
	5. Rule sets are regularly backed up and tested.
	6. Firewalls configured to restrict web servers to accepting only inbound connections – no outbound connections.
	7. The organization uses port camouflaging.
	8. Standard ingress and egress filtering rules are applied thus: • All inbound packets do not have a source address of the organization's internal network. • All incoming packets have a destination address of the organization's internal network. • All outbound packets have a source address of the organization's internal network. • All outbound packets do not have a destination address of the organization's internal network. • All inbound and outbound packets do not have a source or destination address of a private address, loopback (127.0.0.0/8) or RFC1918 reserved IP address spaces • All DHCP auto-configuration reserved addresses are blocked.
	9. Firewall configuration explicitly restrict access by blocking unnecessary port such as 21/tcp, 22/tcp, 23/tcp, 139/tcp,
6. Intrusion Detection	1. The organization uses both or either of host-based and network-based Intrusion detection systems (IDS).

Systems (IDS)	2. IDS programmes are regularly updated.
	3. All system logins and intrusions are tracked and logs frequently reviewed.
	4. Log files are securely kept from any alteration or deletion.
	5. Frequent vulnerability testing is conducted against IDS systems.
	6. The organization subscribes to the National CERT for alerts on the latest threats and vulnerabilities.
	7. A profile of general characteristics for each server and IDS rule-sets are kept and protected from unauthorized persons.
7. Virus Management	1. The organization maintains a daily schedule of anti-virus signatures updates.
	2. All devices into the corporate network scanned for viruses – no exceptions.
	3. The organization subscribes to the National CERT for alerts on the latest virus threats and patches.
8. Penetration Testing	1. There exists a schedule for vulnerability testing (say, quarterly) and penetration testing (bi-annual) and reports from such tests are acted upon.
	2. Test includes the following: social engineering, password cracking, port-scanning, network survey, internal and external penetrations on firewall and IDS.
	3. Report from test includes: a. Description of threats in terms of who, how and when b. Classification of threats into classes. c. Determination of consequences of threat manifestation to business operations. d. Assessment of impact of the consequences as less low, medium or high.
9. Systems Administration	1. Network logs are audited daily
	2. Default software settings modified, disabled or deleted to guarantee a secure configuration?
	3. All unencrypted protocols such as SNMP, telnetd, ftpd, mail, rpc, rservices are disallowed from the network.
	4. Passwords are encrypted during transmission and storage.
	5. Instant Messaging is properly encrypted and controlled.

I will ensure that my organization complies with all relevant Information Assurance process
best practices, and attain to maturity on all Assurance Indicators as contained in the
guidelines. My organization will also fulfil all legal requirements pertaining to the CIIP
programme as contained in the relevant legislations.

I confirm that my organization briefs, trains or otherwise formally disseminates information
to staff about their secure use of the corporate and national network as laid down in the CIIP
Code of Practice and other materials as may be made available by CIIP Programme
Coordinator. This includes a user acceptance policy or personal commitment statement in
appropriate Personal Commitment.

I confirm that my organization has appointed a POC to liaise with the CIIP Programme Coordinator and that the Information assets list, along with the description of the network(s) and physical infrastructure of this organization are accurate and current at all times. A copy of this list and description are available at the office of the CIIP Programme Coordinator.

APPENDIX E: THE CHECKLIST

which the user agrees to comply with the security rules of the organization as well as those
within CIIP network.

I confirm that my organization maintains and regularly review access list and keeps accurate
records of all authorized users within the organization, and that such users signed the

I will ensure that my organization collaborate with the CIIP Programme Coordinator on all security issues report all security breaches (potential or real) immediately I become aware of it

Understanding Cyber-Criminology:

Techniques for Cybercrime Prevention and Detection

Zems, Mathias

maczems@gmail.com

***Abstract*—Our society has come to rely on the sheer size, technological power, and lightning fast speed of the internet to seek out immeasurable pages of information explore the unknown, and communicate with virtually anyone, anywhere, and at any time across the globe. Many traditional crimes are now being aided or abetted through the use of computers and networks, and wrongdoing previously never imagined has surfaced because of the incredible capabilities of information systems. Computer crimes are requiring police and law enforcement agencies in general and criminal investigators in particular to tailor an increase amount of their efforts toward successfully identifying, apprehending, and assisting in the successful prevention, detection, apprehension and prosecution of perpetrators. It is hoped that past knowledge can be assimilated with current observations of the computer-related criminality to inform and guide the science of police investigation in the future. Criminal investigation has been a topic of study for academics and practitioners alike, and is defined as the process of legally gathering evidence of a crime that has been or being committed. It seeks to identify the truths associated with how and why a crime occurred, and works toward building a case that may lead to the successful prosecution of the phishers (offenders). Though many research studies have sought to determine the best way in which the investigative process can be conducted and managed. The overarching goal of these studies has been to enable police and law enforcement agencies to reflect upon their own practices against the backdrop of the findings and then to implement salient positive changes which would improve the day- to-day operations of their organization. Practices of investigation have been modified and refined over the years, taking into account changes in social, political, economic, and scientific domains. These practices have infused science into an activity that was once primarily considered as an art and have consequently enhanced the investigative process.**

Keywords*—*Crime, Cybercrime, Cyber-security, Unlawful acts, Category of Phishers, Classifications of Cyber-terrorism & Cybercrime component; formatting; style; styling; insert (key words)

I. INTRODUCTION

It is pertinent to note that, Internet technology and the development of cyberspace have taken society to the next level of evolution. Cyberspace has defied the boundaries and has made geography (or place) irrelevant. Cyberspace presents myriad potential opportunities for society in the new millennium, of which a new era was ushered in, that Internet technology reigned supreme. However, the increase in the neatens has dwarfed the technology to a mere medium. Additionally, the perpetrators who attacked machines through machines have started attacking real humans through machines. This radical development led Criminologists to address the need for a discipline to study and analyze criminal behavior in cyberspace [1].

As far back as the early 1990s, the Internet was argued to be a unique medium showing the fastest speed of diffusion in human history[2,3]. Today, there are very few people whose lives are not affected beneficially and/or harmfully by the technology of the Internet era. On the positive side, the ability to share and exchange information instantaneously has provided unprecedented benefits in the areas of education, commerce, entertainment and social interaction. On the negative side, it has created increasing opportunities for the commission of crimes, information technology has enabled potential offenders to commit large-scale crimes with almost no monetary cost and much lesser risk of being caught. Compared to perpetrators of traditional economic-motivated crimes (such, burglaries, larcenies, bank robberies), online fraudsters are relatively free of worry from directly encountering law enforcement agency and witnesses.

II. DEFINITIONS, CONCEPTS AND ELEMENTS OF CYBERCRIME

Cyber: it could be understood to mean a prefix used to describe a person, thing, or idea as part of the computer and information age. It is also used in a growing number of terms to describe new things that are being made possible by the spread of computer. There is apparently no distinction between cyber and conventional crimes. However, on a deep introspection we may say that there exists a fine line of demarcation between the conventional and cyber-crime, which is appreciable. The demarcation lies in the involvement of the medium in cases of cyber-crime. The sine qua non for cyber-crime is that there should be an involvement, at any stage, of the virtual cyber medium. Before evaluating the concept of cyber-crime it is obvious that the concept of conventional crime and the points of similarity and deviance between both these forms may be discussed.

Therefore, conventional crime- is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction or punishment of the law. Crime or an offence is a legal wrong that can be followed by criminal proceeding which may result into punishment. The hallmark of criminality is that, it is breach of the criminal law. The criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences. Crime may be said to be any conduct accompanied by act or omission, prohibited law and consequential breach of which is visited by penal consequences [4, 5].

While, cyber-crime is an evil having its origin in the growing dependence on computers in modern life. A simple yet

sturdy definition of cyber-crime would be "unlawful acts wherein the computer is either a tool or a target or both". Defining cyber-crimes, as "acts that are punishable by the information Technology Act" would be unsuitable as the Nigerian Laws also covers many cyber-crimes, such as e-mail spoofing, cyber defamation etc. Cyber-crime is the latest and perhaps the most complicated problem in the cyber world [6]. "Cyber-crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime". While, the universal acceptable definition of cyber- crime may be "unlawful acts wherein the computer is either a tool or target and or both".

Cyber terrorism may be defined to be " the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." While, a terrorist means any person who indulges in wanton killing of persons or in violence or in disruption of services or means of communications essential to the community or in damaging property with the view to : putting the public or any section of the public in fear; or affecting adversely the harmony between different religious, racial, language or regional groups or communities; or coercing or overawing the government established by law; or endangering the sovereignty and integrity of the nation. And a cyber terrorist is the person who uses the computer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof is an act of cyber terrorism.

Cyber-criminology- it is a multidisciplinary field that encompasses researchers from various field such as criminology, victimology, sociology, Internet science, and computer. Cyber-criminology is defined as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space"

Cyber-security

In this age of technology and communication convergence, you cannot help but be impacted by technologies and innovations that center on computers, cell-phones and the Internet. But as we resolve our daily lives with these technologies, there are times that we set out to feel truly paranoid about our own safety [7]. May it be our physical safety or the security of our personal hardware and software. What is cyber security all about? It is in fact protecting your personal information or any form of digital asset stored in any computer or in any digital memory device. Cyber security involves protection of sensitive personal and business information through prevention, detection, and response to different online attacks. As mentioned interalia, because most important transactions are conducted across the Internet these days, there is a need to impose effective protection and measures to counter and repel cyber-crimes especially fraud, wired and other related cyberspace offences.

Understanding Cybercrime

It is imperative to note that, any criminal activity that uses a computer either as an instrumentality, target, tool or a means for perpetuating further crimes comes within the ambit of cyber-crime. Cybercrime is becoming an increasingly important area of criminology as more social activities take place online. This paper will provide you with cyber- criminological perspectives study of crime on the Internet (cybercrime), including its commission, motivations and patterns of occurrence, and techniques for management and prevention of cybercrime as a netizen or cyber-criminologist [5]. The range of technology enabled crime is always evolving, both as a function of technological change and in terms of social interaction with new technologies. It's worthy to note that there are three fundamental factors necessary for the commission of crime, be it scientific or conventional. There are as follows: a supply of motivated offenders, the availability of suitable opportunities and the absence of capable guardians [8, 9].

There are almost as many terms to describe cybercrime as there cybercrimes. Though, early descriptions included computer crime, computer-related crime or crime by computer. As digital technology become more pervasive, terms such as high-technology or information age, crime were added to the lexicon. The advent of the internet brought us cybercrime and internet or net crime. The other variants included digital electronic, virtual "IT' high-tech and technology-enabled crimes. If taken literally, each term suffers from one or more deficiencies. Those definitions that focus on computers may not incorporate networks. While others such as cybercrime or virtual crime may be seen as focusing exclusively on the Internet. Nonetheless, terms such as digital electronic or high-tech crime may be seen as so broad to be meaningless. For example, hi-tech crime may go beyond networked information technology and bioengineering. As such terms should not, however, be approached literally, but rather as broadly descriptive terms which emphasize the role of technology in the commission of crime [6].

As crimes have advanced with technology, the breadth of online services and the number of users have continued to increase. We have witnessed that the Internet has made users' lives easier and has begun to link together varied segregated services (e.g., telecommunications, banking, investing, pharmacy, social interaction, education, entertainment) and devices (e.g., computers, servers, smart phones, even electronic chips in individual household, air conditioning). The integration of such diverse technological applications coupled with the rapid growth of online users make fraudulent activities likely to rise further, if no intervention is proposed and implemented, as Nigerian will be again rated as the most notorious cybercrime netizens in the world [10]. Although, it is still the case that no one term has become truly pervasive, with many being used interchangeably, cybercrime has been adopted universally for a number of reasons:

- First, it is commonly used in the literature.
- Secondly, it has found its way into common usage.

- Thirdly, it emphasizes the importance of networked computers.
- Fourthly and most importantly, it is the term adopted in the Council of Europe Convention on Cybercrime.

III. WHY PEOPLE COMMIT CYBER CRIME

The concept of law has said that, 'human beings are vulnerable, so rule of law is required to protect them'. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber-crime. The reasons for the vulnerability of computers may be said to be:

a. Capacity to store data in comparatively small space- The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.

b. Easy to access- The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

c. Complex- The computers work on operating systems and these operating systems in turn are composed of millions of codes. In as much as human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

d. .Negligence- Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber-criminal to gain access and control over the computer system.

e. Loss of evidence- Loss of evidence is a very common and obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

Computer as a Tool and or Targets for unlawful act

Let us examine the acts wherein the computer which is a tool for an unlawful act, usually involves a modification of a conventional crime by the use of computer. While, some of the acts wherein the computer or computer network, is the target for an unlawful act, is usually out of the purview of the conventional criminal law, (Zems, 2011).

(1) Tools for an unlawful Acts

- Financial Claims: This would include cheating, credit card frauds, money laundering etc.
- Cyber Pornography: This would include pornographic websites; pornographic magazines produced using computer and the Internet (to down load and transmit pornographic pictures, photos, writings etc.).
- Sale of illegal articles: This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, bulletin boards or simply by using e-mail communications.
- Online gambling: There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.
- Intellectual Property Crimes: These include software piracy, copyright infringement, trademarks violations.
- E-Mail spoofing: A spoofed email is one that appears to originate from one source but actually has been sent from another source, can also be termed as E-Mail forging or forgery:
- Counterfeit currency notes, postage and revenue stamps, mark sheets etc., can be forged using sophisticated computers, printers and scanners.
- Cyber Defamation: This occurs when defamation takes place with the help of computers and or the Internet e.g. someone published defamatory matter about someone on a websites or sends e-mail containing defamatory information to all of that person's friends.
- Cyber Stalking: Cyber stalking involves following a person's movements across the Internet by posting messages on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim.

(2) Target for unlawful Acts

- Unauthorized access to computer system or network: This activity is commonly referred to as hacking.
- Theft of information contained in electronic from: This includes information stored in computer hard disks, removable storage media etc.
- E-Mail bombing: Email bombing refers to sending a large amount of e-mails to the victim resulting in the victims' e-mail account or mail servers.
- Data diddling: This kind of an attack involves altering the raw data just before it is processed by a computer programmer and then changing it back after the processing is completed.
- Salami attacks: Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers that deducts a small amount from the account of every customer.
- Denial of Service: This involves flooding computer resources with more requests than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.

- Virus/worm: Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses don not need the host to attach themselves to.

- Logic bombs: These are dependent programs. This implies that these programs are created to do something only when a certain event occurs, e.g. some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date.

- Trojan Horse: A Trojan as this program is aptly called is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

- Internet Time Theft: This connotes the usage by unauthorized persons of the Internet hours paid for by another person.

- Physically damaging a computer system: This crime is committed by physically damaging a computer or its peripherals.

IV. CLASSIFICATIONS OF CYBERCRIME

The subject of cyber crime refers to all activities done with criminal intent in cyberspace and may be broadly classified under the following three slots:

1(a)Against Individuals: i. Harassment via e-mails, ii. Cyber-stalking, iii. Dissemination of obscene material iv. Defamation. v. Unauthorized control/access over computer system, vi. Indecent exposure, vii. Email spoofing, viii. Cheating & Fraud.

(b) Against Individual/ Property: i. Computer vandalism, ii. Transmitting virus, iii. Trespass iv. Unauthorized control/access over computer system. v. Intellectual Property crimes, vi. Internet time thefts.

2. Against Organization: - . i. Unauthorized control/access over computer system, ii. Possession of unauthorized information. iii. Cyber terrorism against the government /organization. iv. Distribution of pirated software etc.

3. Against Society at large: - i. Pornography (basically child pornography). ii. Polluting the youth through indecent exposure. iii. Trafficking iv. Financial crimes v. Sale of illegal articles, vi. Online gambling, vii. Forgery.

Typology of Cyber phishers (offenders)

The cyber criminals constitute of various groups/ category. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber suspect:

a. Children and adolescents age- The simple reason for this type of delinquent behavior pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cogent reason may be to prove themselves to be outstanding amongst other children in their group, further the reasons may be psychological even.

b. Organized hackers- These kinds of hackers are mostly organized together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfil their political objectives.

c. Professional hackers / crackers – Their work is motivated by the color of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are even employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

d. Discontented employees- This group include those people who have been either sacked by their employer or are dissatisfied with their employer.

V. CYBERCRIME PREVENTION

A. Preventive Steps for Individuals

Children: Children should not give out identifying information such as Name, Home address, School Name or Telephone Number in a chat room. They should not give photographs to anyone on the Net without first checking or informing parents' guardians. They should not respond to messages, which are suggestive, obscene, belligerent or threatening, and not to arrange a face-to –face meeting without telling parents or guardians. They should remember that people online might not be who they seem.

Parents: Parent should use content filtering software on PC to protect children from pornography, gambling, hate speech, drugs and alcohol. There is also software to establish time controls for use of limpets (for example blocking usage after a particulars time) and allowing parents to see which site item children have visited. Use this software to keep track of the type of activities of children.

General Information: Don't delete harmful communications (emails, chats etc). They will provide vital information about system and address of the person behind these.

- Try not to panic.
- If you feel any immediate physical danger contact your local police.
- Avoid getting into huge arguments online during chat and discussions with other users.
- Remember that all other Internet users are strangers; you do not know who you are chatting with. So be careful.
- Be extremely careful about how you share personal information about yourself online.
- Choose your chatting nickname carefully so as others.
- Do not share personal information in public space online; do not give it to strangers.

- Be extremely cautious about meeting online introduced person. If you choose to meet, do so in a public place along with a friend.
- If a situation online becomes hostile, log off and if a situation places you in fear, contact local police.
- Save all communications for evidence. Do not edit it in any way. Also, keep a record of your contacts and inform Law Enforcement Officials.

B. Preventive Steps for Organizations and Government

- Physical Security: Physical security is most sensitive component, as prevention from cyber-crime. Computer network should be protected from the access of unauthorized persons.
- Access Control: Access Control system is generally implemented using firewalls, which provide a centralized point from which to permit or allow access. Firewalls allow only authorized communications between the internal and external network.
- Password: Proof of identity is an essential component to identify intruder. The use of passwords in the most common security for network system including servers, routers and firewalls. Mostly all the systems are programmed to ask for username and password for access to computer system. This provides the verification of user. Password should be charged with regular interval of time and it should be alpha numeric and should be difficult to judge.
- Finding the Holes in Network: System managers should track down the holes before the intruders do. Many networking product manufactures are not particularly aware with the information about security holes in their products. So organization should work hard to discover security holes, bugs and weaknesses and report their findings as they are confirmed.
- Using Network Scanning Programs: There is a security administration's tool called UNIX, which is freely available on Internet. This utility scans and gathers information about any host on a network, regardless of which operating system or services the hosts were running. It checks the known vulnerabilities include bugs, security weakness, inadequate password protection and so on. There is another product available called COPS (Computer Oracle and Password System). It scans for poor passwords, dangerous file permissions, and dates of key files compared to dates of CERT security advisories.
- Using Intrusion Alert Programs: As it is important to identify and close existing security holes, you also need to put some watchdogs into service. There are some intrusion programs, which identify suspicious activity and report so that necessary action is taken. They need to be operating constantly so that all unusual behavior on network is caught immediately.
- Using Encryption: - Encryption is able to transform data into a form that makes it almost impossible to read it without the right key. This key is used to allow controlled access to the information to selected people. The information can be passed on to anyone but only the people with the right key are able to see the information. Encryption allows sending confidential documents by E-mail or save confidential information on laptop computers without having to fear that if someone steals it the data will become public. With the right encryption/decryption software installed, it will hook up to mail program and encrypt/decrypt messages automatically without user interaction.

VI. CYBERCRIME DETECTION

Cyber-crime is the latest and perhaps the most specialized and dynamic field in cyber laws. Some of the Cyber Crimes like network Intrusion are difficult to detect and investigation even though most of crimes against individual like cyber stalking, cyber defamation and cyber pornography can be detected and investigated through following steps:

After receiving such type of mail

(1) Give command to computer to show full header of mail.

(2) In full header find out the IP number and time of delivery of number and this IP number always different for every mail. From this IP number we can know who was the Internet service provider for that system from which the mail had come.

(3) To know about Internet Service Provider from IP numbers take the service of search engine like nic.com, Com, apnic.com, arin.com.

(4) After opening the website of any of above mentioned search engine, feed the IP number and after some time name of ISP can be obtained.

(5) After getting the name of ISP we can get the information about the sender from the ISP by giving them the IP number, date and time of sender.

(6) ISP will provide the address and phone number of the system, which was used to send the mail with bad intention. After Knowing the address and phone number criminal can be apprehended by using conventional police methodology, investigation begins in a bid to detect for apprehension of the criminals.

VII. CONCLUSION

Police and other law enforcement agencies will have to expand their investigative practices to competently respond to the problem at hand, thankfully, they are not staring from square –one. So, the concept of cyber-crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules or laws and counterbalanced by the punishment or sanction of the state. It is not overstatement to add that, crime may be any conduct accompanied by act or omission, prohibited law and consequential breach of which is visited by penal consequences. Capacity of human mind is unfathomable. It is not possible to eliminate cyber-crime from the cyber space. Though, it is quite possible to check them, as history is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties (to report cybercrime as a collective duty towards its reduction in the society) and further

making the application of the laws more stringent to check cybercrime.

It is imperative to note that, one of the greatest lacunae in the field of Cyber Crime is the absence of comprehensive law particularly in Nigeria and the World at large. The problem is further aggravated due to disproportional growth ratio of Internet and cyber laws. Though a beginning has been made by the enactment of EFCC, Act as amended and Nigeria criminal law. Undoubtedly the Act is a historical step in the cyber world. Further all together do not deny that there is a need to bring changes in the Information Technology to make it more effective to combat cyber-crime. Nonetheless, identity theft and online frauds are contemporary crimes for profit. As the world market continues to progress toward transferring and managing money conveniently on the Internet, online frauds and scams are inescapable. As long as identity theft and online frauds are relatively easy paths to financial gain, the use of these fraudulent means will increase with the growth of the Internet.

Inasmuch as the movement of processing monetary transactions daily in Nigeria banks is holistically online, it is therefore, pertinent to note that online fraud has gradually transformed from a hybrid computer cybercrime to a true cybercrime. Collectively, cyberspace has become such an attractive place where suitable targets like personal information increase in value while effective guardians typically fall behind. Anti-fraud efforts must be accelerated and orchestrated proficiently to make online scams difficult for phishers (offenders).

REFERENCES

[70] Federal Trade Commission. (2009). Consumer Fraud and Identity Theft Complaint Data: January – December, 008. [online]. Available from: Federal Trade Commission. (2010).

[71] Nguyen, D, and Alexander, J. (1996). The coming cyberspace time and the end of polity. In R. Shields (Ed.), Cultures of Internet. London: Sage Publication.

[72] http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf [Accessed 02/09/2011].

[73] William, G. (1985) The definition of Crime and Current Legal, NY/

[74] Zems, M (2011) Understanding Crime: Analysis for Intelligence, Investigation and Security, Published in China

[75] Parker, BD. (2006) Understanding and Managing Cybercrime. Allyn and Bacon, NY.

[76] Parker, D. B. (1998). Fighting Computer Crime: A New Framework for Protecting Information. New York, NY: Wiley Computer Publishing. Poster, M. (2006).

[77] Information Please: Culture and Politics in the Age of Digital Machines. Durham: Duke University Press. RSA (2009). RSA Online Fraud Report. [online]. Availablefrom: http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_1208.pdf. [Accessed 16/08/2011]. [Accessed 01/09/2011].

[78] Zems, M. (2009) Crime is Normal, (laws are either made to be obeyed or be broken) Corpus Publishing and Printer, Nig LtdG. Eason, B. Noble, and I.N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)

[79] McQuade, S. C. (2006). Understanding and Managing Cybercrime. Upper Saddle River, NJ: Pearson Education Inc. National White Collar Crime Center. (2008). Internet Crime Report. Washington, DC: Bureau of Justice Assistance, [online].

Review and Evaluation of Cybersecurity Threats on Communication Networks

M. I OGBILE
Department of Electrical and Computer Engineering,
Ahmadu Bello University
Zaria, Nigeria
mwuohie@yahoo.com

P. U OKORIE
Department of Electrical and Computer Engineering,
Ahmadu Bello University
Zaria, Nigeria
puokorie@abu.edu.ng

***Abstract*—The analysis of risks associated with communications, and information security for a system-of-systems is a challenging endeavor. This difficulty is due to the complex interdependencies that exist in the communication and operational dimensions of the system-of-systems network. In light of the borderless nature of cyber-crime, international legislation and action are essential to combat the phenomenon. Current legal instruments, as well as continuing efforts of international organizations, provide a significant basis in this area. Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cyber security. Ensuring cyber security requires coordinated efforts throughout an information system. The goal of this research is to quantify the impact of attacks on communications, and information flows on the operability of the component systems. In this paper, we aim at classifying and evaluating the security threats on the communication networks, the possible vulnerabilities in communications and survey the current solutions on cyber security for communications.**

Keywords—Cyber-security, Information security, Network security, End-user education.

I. INTRODUCTION

One of the most problematic elements of cyber security is the quickly and constantly evolving nature of security risks. The traditional approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment. "The threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk. It's no longer possible to write a large white paper about the risk to a particular system. You would be rewriting the white paper constantly." [1]. To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach. The National Institute of Standards and Technology (NIST), for example, recently issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments.

The Internet and increased use of personal computer in recent years has provided a refuge for a multitude of computer-based crimes [2]. One of the most challenging computer related crimes to law enforcement and the economy has been intellectual property piracy. Personal computers and the Internet allow individuals to find, copy, and use intellectual property without providing any payment for it [3]. Digital piracy is one form of intellectual property piracy that has been increasing in recent years. [4] and others defined digital piracy as the illegal act of copying digital goods, software, digital documents, digital audio (including music and voice), and digital video for any reason other than to backup without explicit permission. The Internet facilitates digital piracy because it allows the crime to take place detached from the copyright holder [5]. This is especially true for digital music piracy that is committed through a multitude of modus operandi (e.g., CD burning, peer-top-peer networks, LAN file sharing, digital stream ripping, and mobile piracy. In turn, the perception of a victimless crime is created. However, music piracy is far from a victimless crime and has been described as "the greatest threat facing the music industry today" [5].

II. ANALYSIS OF THE SECURE NETWORK PROBLEM

New Vulnerabilities and New Threats

Control systems have been at the core of critical infrastructures and communication for many decades, and yet, there have been very few confirmed cases of cyber attacks. Control systems, however, are more vulnerable now than before to computer vulnerabilities for many reasons:

- Controllers are computers. Most of the original physical controls (traditionally conformed of logic of electromechanical relays) have been replaced by microprocessors and embedded operating systems. These controllers may provide many functionalities, such as flexible configuration via a web server, and digital communication capabilities that allow remote access and control. The increased complexity of the software base may also increase implementation flaws (software bugs).
- Networked. Control systems are not only remotely accessible, but increasingly -for efficiency reasons- they are being connected to corporate networks and the Internet. Even control systems designed to be closed may, in practice, not be

perfectly isolated: connectivity through uncontrolled connections can occur in many ways (e.g., via mobile devices). Similarly, Internet-connected embedded devices (including CPS) are expected to be the largest contributors to the growth of the Internet in future years [6], and are expected to have major technical, economic and societal impact. The security challenges of CPS will become more severe as the scale and scope of the Internet grows.

- Open design. Increasingly, even protocols that are unique to control systems are now more open and more accessible; therefore it is easier for an attacker to obtain the necessary knowledge to attack the system. This point is, however, controversial: security professionals generally argue that open design is preferable because they can find and fix bugs more easily. The debate between open design and closed design is an active one [7].

- Increasing size and functionality. Wireless sensor networks and actuators are allowing industrial control systems to instrument and monitor larger number of events and operations. Some infrastructures are also changing to provide new functionalities, such as the Smart Grid program [8]. It is a standard security concern that new functionalities may give rise to new vulnerabilities.

- Large and highly skilled IT global workforce. Larger groups of people can now find and generate attack vectors for computer-based systems.

- Cybercrime. Less computer-skilled people also have access to a number attack tools and cybercrime networks. A driving factor for the interest of cybercrime in control systems is extortion.

Consequences of an Attack

To our knowledge there has not been a publicly-available objective analysis of the possible consequences to attacks against critical infrastructures. In our view, while some of the reports on SCADA security might appear overly alarmist (safety safeguards in most control systems might prevent major catastrophes), the fact that a user is able to obtain unauthorized privileges in a control system should be taken seriously.

Efforts for securing control systems

Up to now, most of the effort for protecting control systems (and in particular SCADA) has focused on reliability (the protection of the system against random faults). There is, however, an urgent growing concern for protecting control systems against malicious cyber attacks [9, 10].

There are several industrial and government-led efforts to improve the security of control systems. Several sectors - including chemical, oil and gas, and water- are currently developing programs for securing their infrastructure. The electric sector is leading the way with the North American Electric Reliability Corporation (NERC) cyber security standards for control systems [11]. NERC is authorized to enforce compliance to these standards, and it is expected that all electric utilities are fully compliant with these standards by 2010.

NIST has also published a guideline for security best practices for general IT in Special Publication 800-53. Federal agencies must meet NIST SP800-53. To address the security of control systems, NIST has also published a Guide to Industrial Control System (ICS) Security [12]. Although these recommendations are not enforceable, they can provide guidance for analysing the security of most utility companies.

The Department of Energy has also led security efforts by establishing the national SCADA test bed program [13] and by developing a 10-year outline for securing control systems in the energy sector [14]. The report -released in January 2006- identifies four main goals: (1) measure current security, (2) develop and integrate protective measures, (3) detect intrusion and implement response strategies; and (4) sustain security improvements.

The use of wireless sensor networks in SCADA systems is becoming pervasive, and thus we also need to study their security. A number of companies have teamed up to bring sensor networks in the field of process control systems, and currently, there are two working groups to standardize their communications [15, 16]. Their wireless communication proposal has options to configure hop-by-hop and end-to-end confidentiality and integrity mechanisms. Similarly they provide the necessary protocols for access control and key management.

In order to control unwanted information and threats in the communication network, the following objective must be carried out and accomplished:

1) Create awareness of security issues with control systems,

2) Help control systems operators and IT security officers design a security policy, and

3) Recommend basic security mechanisms for prevention (authentication, access controls, etc), detection, and response to security breaches. These recommendations and standards have not considered technical details of the new research problems that arise when control systems are under attack.

III. CYBER SECURITY PLAN (CSP)

A. Application Environment factors in communication

In order to employ the wireless communication, firstly, the application environmental survey must be taken into consideration whether to apply low power of lesser wattage, or acceptance of wireless devices as a countermeasure for the electromagnetic interference (EMI). The following factors should be taken into consideration:

i. Communication type: Wi-Fi communication (IEEE 802.11) networks

ii. Transferring data type: audio (or video data)

iii. Usage area

iv. Connection status to critical digital asset (CDA)

- Voice and Video: no connection to existing systems and instrument and control (I&C) system through a separate network configuration

- Variable data: two-way communication to the variable server which separately configured, or one-way communication from non-safety system

v. The Safety system

B. The Criteria to be established for the Cyber Security Plan.

Criteria for the cyber security must be established and follows as to reflect the existing I & C systems cyber security program.

i. Communication type: reflect the security measures for the connection portion with the communications network to the I&C CSP

ii. Apply the latest technology with enhanced security features, such as authentication, encryption, WIPS (Wireless Intrusion Prevention System), etc.

iii. Derived to security measures, such as technical, management and operational control measures

iv. Create wireless CSP, taking into account the time factor.

IV. CYBER SECURITY PLAN (CSP)

Cyber Security Program and Regulation Analysis for the I&C Systems

As earlier detail in section 2.4 effort towards securing reliability of communication network several effort were been put further by agents and organization. The US billion dollars investments in cyber security are creating a securitisation of cyberspace. The argument is of threefold what has happened meanwhile in Europe related to cyber security threats. First, cyber threats were raised to the national threat level in Germany (2006), France (2008) and the UK (2008), but the justifications put forward for such an upgrade did not hold, as well as invested resources at that point in time. Second, cyber security strategy followed up this upgrade and designed a framework to tackle the threat that was found coherent with the assessment of the respective national security strategies. Third, cyber insecurity stemmed from criminals operating in cyberspace. Therefore, deterring criminals should have been at the core of tackling cyber insecurity but the defense strategies of France, Germany and the UK were instead focused on mitigating the effects of cyber attacks [17].

In the United States, March 2009, US Nuclear Regulation Commission (NRC) required a high level of cyber security for the safety, security and emergency preparedness (SSEP) functions by revising 10CFR73.54, January 2010, Reg. Guide 5.71 was issued. Since 2009, NEI has developed a guideline to meet the requirements of 10CFR73.54 and issued NEI 08-09 Rev.6, which was endorsed by US NRC in 2010 [18]. In Korea, KINS issued GT-N27, Reg. Guide 8.22 and has requested the cyber security activities [19]. Life-cycle of NPP consists of a variety of phases (e.g., concept, requirement, design, implementation, test, installation, operation and maintenance, retirement). I&C cyber security program consists of policy and plan documents and configured by management, operational, technical security controls, as shown in Figure 1

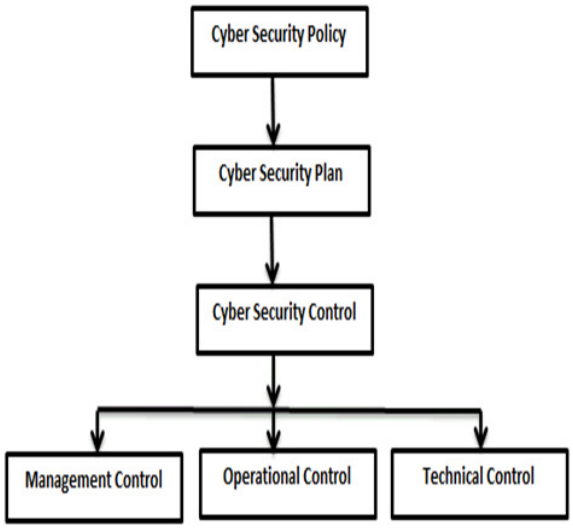


Figure 1: Architecture of Cyber Security Program.

Threat Analysis and Countermeasures of the Wireless Communication

The types of wireless threat are mainly attack to the internal network, authorized AP, outside AP by internal user, internal network by unauthorized outside user. Examples of internal network attack in the threat analysis are those of Rogue-AP, Soft-AP, Ad-Hoc Connection and mis-configured AP. The strategy which protect the connection with authorized AP by authorized user and control the connection with unauthorized, or authorized AP by unauthorized user, should be established, depending on the type of threat.

The countermeasures, which were reflected in the CSP, were configured by management, operational, technical security controls and those security controls were interconnected to employ defense-in-depth concept. For example, for the vulnerability of Service Set Identifier (SSID) broadcasting, technical controls (e.g. hidden SSID method, 802.1x authentication, Wireless Intrusion Prevention System (WIPS), operational controls (e.g., periodic scanning, AP stopping) can be considered.

V. CONCLUSION

he cyber security program is being developed not to affect inherent functions of I&C systems against the increase of cyber security threat and vulnerability due to application of digital technology. In order to take advantage of mobility and convenience by using wireless communication, cyber security evaluation is needed in terms of wireless communication itself and the connection portion with the wireless communications network to the I&C systems. Therefore, in this paper, we are establishing the wireless CSP through threat analysis, vulnerability analysis, countermeasures in the area of wireless communication to assess and manage the potential for adverse effects on safeguard and safety functions so as to provide high assurance that critical functions are properly protected cyber-attack.

VI. RECOMMENDATION

In addition to the three main objectives have been mentioned, information security has developed mature technologies and design principles (authentication, access control, message integrity, separation of privilege, etc.) that can help us prevent and react to attacks against control systems. However, research in computer security has focused traditionally on the protection of information but do not considered how attacks affect the estimation, control algorithms and physical world.

We therefore argue that while the current tools of information security can give necessary mechanisms for the security of control systems, these mechanisms alone are not sufficient for the defence-in-depth of control systems.

We believe that by understanding the interactions of the control system with the physical world, we should be able to

Better understand the consequences of an attack: so far there is no research on how an adversary would select an strategy once it has obtained unauthorized access to some control network devices.

Design novel attack-detection algorithms: by understanding how the physical process should behave based on our control commands and sensor measurements, we can identify if an attacker is tampering with the control or sensor data.

Design new attack-resilient algorithms and architectures: if we detect an attack we may be able to change the control commands to increase the resiliency of the system.

REFERENCES

[80] Adam Vincent, CTO-public sector at Layer 7 Technologies (a security services provider to federal agencies including Defense Department organizations).

[81] Adler & Adler, 2006; Hinduja, 2004; "Cyber Criminology" Expoloring Internet Crimes and Criminal Behavior; Intertional Journal of Cyber Criminology, vol. 2 , Issue 2.

[82] George E. Higgins, Scott E. Wolfe & Catherine D. Marcum- Music Piracy and Neutralization 2008 International Journal of Cyber Criminology.

[83] R.D. Gopal and Sulip Bhattacharjee; The effect of Dgital Sharing Technologies on Music Markets: A survival Analysis of Albums on Ranking Charts.

[84] J.S Chiou, C.Huang and H. Lee; The Antecedents of Music Piracy Attitutes and Intentions, vol.57, issue 2 pp161-174.

[85] JOHN H. MARBURGER, I., AND KVAMME, E. F. ; Leadership under challenge: Information technology R&D in a competitive world. An ssessment of the federal networking and information technology R&D program. Tech. rep., President's Council of Advisors on Science and Technology, August 2007.

[86] ANDERSON, R.; Security in open versus closed systems- the dance of Boltzmann, Coase and Moore. In Open Source Software Economics (2002).

[87] GAO. Information security. TVA needs to address weaknesses in control systems and newtworks. Tech. Rep. GAO-08-526, Report to Congressional Requesters, May 2008.

[88] TURK, R. J. Cyber incidents involving control systems. Tech. Rep. INL/EXT-05-00671, Idao National Laboratory, October 2005.

[89] BYRES, E., AND LOWE, J. The myths and facts behind cyber security risks for industrial control systems. In Proceedings of the VDE Congress, VDE Association for Electrical Electronic & Information Technologies (October 2004).

[90] NERC-CIP. Critical Infrastructure Protection. North American Electric Reliability Corporation, http://www.nerc.com/cip.html, 2008.

[91] STOUFFER, K., FALCO, J., AND KENT, K. Guide to supervisory control and data acquisition (scada) and industrial control systems security. Sp800-82, NIST, September 2006.

[92] INL. National SCADA Test Bed Program. Idaho National Laboratory, http://www.inl.gov/scada.

[93] EISENHAUER, J., DONNELLY, P., ELLIS, M., AND O'BRIEN, M. Roadmap to Secure Control Systems in the Energy Sector. Energetics Incorporated. Sponsored by the U.S. Department of Energy and the U.S. Department of Homeland Security, January 2006.

[94] HART. http://www.hartcomm2.org/frontpage/wirelesshart.html. WirelessHart whitepaper (2007).

[95] ISA. http://isa.org/isasp100. Wireless Systems for Automation (2007).

[96] Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK; VOL 22, ISS. 1, 2013.

[97] NEI 08-09 Rev.6, "Cyber Security Plan for Nuclear Power Reactor," NEI, 2010

[98] KINS Reg. Guide 8.22, "Cyber Security of Digital Instrumentation Control Systems in Nuclear Facilities," KINS, 2010G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)

Cybersecurity Threats and Potential Solutions

[1]Kenneth Sorle Nwizege, [2]Michael Mac Mammah
[3]Agbeb Nornu S.
[1,2,3,4&6]Dept. of Elect/Elect Engineering, School of Engineering, Ken Saro-Wiwa Polytechnic, Bori, Nigeria
[1]s.k.nwizege@ieee.org, [2]macmammahm@yahoo.com,
[3]agbeb_nornu@yahoo.co.m

[4]Irimiagha Paul Gibson, [5]Mmeah Shedrack,
[6]Harry, Inye, H.
[5]Dept. Of Computer Science, School of Applied sciences, Ken Saro-Wiwa Polytechnic, Bori, Nigeria
[4]mie4tammy@gmail.com, [5]shedrackmmeah@yahoo.com,
[6]ipadibi@yahoo.com

***Abstract* – Without strong password authentication, many devices and networks will remain vulnerable to attacks. Since cybercrime is on the increase daily, IT experts have to be up and doing in order to fight against this threat. Security consciousness and awareness will aid the fight for this dilemma. In order to stay secured, this work opines that devices such as computer, mobile phone, IPAD, networks should have strong password authentication. Hence, a viable and strong encryption algorithm was developed which could put cybercriminals to flight. It was recommended that effective security and network protocol analyzers be used at all times to reduce vulnerabilities. This paper analyses the threats and proposed possible solutions to reduce risk in various organizations and self acts.**

Keywords—computer security; cybersecurity; cybercrime; organization; threat

I. INTRODUCTION

Fundamentally, there is a relationship that exists between cybersecurity and computer security. This can be explained by the fact that the computer is one of the most commonly used devices in carrying out cybercrime activities.

Cyber crime includes any criminal act dealing with computer and networks (also, called hacking). It includes the traditional crimes conducted through the internet. For instance, hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet [1].

Cyber crimes against banks and other financial institutions certainly cost many hundreds of millions of dollars per year. These losses could just be the cost of doing business or they could be a major new risk for companies and nations as these illicit acquisitions damage global economic competitiveness and undermine technological advantage [2][3].

Conversely, computer security involves the protection of computing systems and the data that they store or access. Computer security allows an organisation to carry out its mission by:

- Enabling people to carry out their jobs, education, and research, etc.
- Protecting personal and sensitive information (data) [4].
- Supporting critical business process

However, a good security standards must follow the "90 / 10" rule which states that:

- 10% of security safeguards are technical.
- 90% of security safeguards rely on the computer user to adhere to good computing practices, reviews on the allocated spectrum available to their region of operation.

The lock on the door is the 10%, while a user remembering to lock the door, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90%. Both parts are need for effective security. This means that everyone who uses a computer or mobile device needs to understand how to keep their computer, device and data secure.

Now, cybersecurity is the protection of valuable intellectual property and business information in digital form against theft and misuse. It is an increasingly critical management issue. The US government has identified cybersecurity as one of the most serious economic and national security challenges they face as a nation. Institutions and companies must now fend off ever-present cyber attacks. This act is influenced by cybercriminals or even disgruntled employees releasing sensitive information, taking intellectual property to competitors, or engaging in online fraud. While sophisticated companies have recently endured highly public breaches to their technology environments, many incidents go unreported. Indeed, businesses are not eager to advertise that they have had to “pay ransom” to cybercriminals or to describe the vulnerabilities that the attack exposed.

Interestingly, to reduce security risk as much as possible, this work now outlines key principles to adopt at all times:

- Learn good computing security practices.
- Incorporating these practices into everyday routine.
- Encouraging others to do so as well.

- Report anything unusual –In this case, by notifying the appropriate contacts of a suspected security incident [5].

The rest of the paper is organized as follows. Section II presents a literature background of study, while Section III deals with security threats. Section IV presents a proposed security algorithm. Section V presents a potential solution to cyber threats and activities. The paper concludes in Section VI.

II. LITERTAURE REVIEW

Background on Cybersecurity

Cybersecurity is the protection of valuable intellectual property and business information in digital form against theft and misuse. Cybersecurity threats are criminals or even disgruntled employees who release sensitive information, taking intellectual property to competitors, or engaging in online fraud. With the rate of increase and complexity of the threats, organizations must adopt approaches to cybersecurity that will require much more engagement from the CEO and other senior executives to protect critical business information without constraining innovation and growth [6].

Why Cybersecurity

Large and reputable organizations have dramatically strengthened their cybersecurity capabilities over the past five years. Formal processes have been adopted to be implemented with priority. In the context of IT security risks, there have been developed strategies with hundreds of millions of dollars already committed in order to execute these strategies. Desktop environments are more vulnerable compared with how they were five years ago. This is because Universal Serial Bus (USB) ports and Web mail services are potential sources of invasion. Robust technologies and initiatives have been put in place to address attacks on the perimeter.

Cybersecurity is highly indispensible in this age. This is because; the cyberspace has become a new center stage for innovations, enterprises, social networking, criminality and warfare. However, the Cyberspace that offers numerous benefits also has risks at various levels.

Why Awarness

The US Executive Order (EO) 13636 initiated a dialogue to identify challenges and determine effective responses to cybercrime. One of the areas suggested to handle this alarming security threat is the use of forum for more awareness, training, and updates [7]. The CForum is one of those helpful avenues for handling cybersecurity issues. This can help identify critical resources that can save an organization's time. It applies the framework flexibility which is one of essential principles needed to achieve organizational cybersecurity goals. Apart from flexibility, other Framework's principles are: global impacts, risk management approaches, leverage on existing approaches, standards and best practice. It has guide that will help learn how different organizations use it in different ways with different tools to achieve Framework outcomes [8].

The American Water Works Association (AWWA) has developed Process Control System Security Guidance (PCSSG) for the water sector and a supporting Cybersecurity use-case tool [9]. The AWWA's cybersecurity resources are designed to provide actionable information for utility owner/operators based on their use of process control systems [10],[11].

III. CYBERCRIME THREATS

Cybersecurity threats is prone the following areas, Bank, schools, government sectors, and organization data base. The effect of these threats are really disastrous because it affect both financial and data management. In this section, emphasis is place on threat records. Afterwards, a proposal on a possible measure to handle security issues [12] is presented.

Who is vulnerable to threat?

The following are the identified sources of vulnerability, viz:

- The storage, network, etc media formats
- Mobile Phone Phone with PIN.
- Business competitors
- Electronic Blackmail
- Internal threats
- Governments Institutions/Agencies eg. Spy Agencies (National Security Agency and Government Communications Headquarters (NSA and GCHQ))

Basically, cyber attacks cover the above mentioned areas. The effect of these attacks can adversely affect an economy, information, and data management of any nation or organization. Most valuable resources and information are stolen via this criminal act.

Fig. 1 shows the trend of attack for a period of two years, Fig. 2 shows the daily attack encountered. Figure 3 shows the losses incurred as result of cyber attack on the economy [10][11]. Fig. 4 illustrates the brain behind cyber criminality. Fig. 5 shows the different types of cyber attacks.

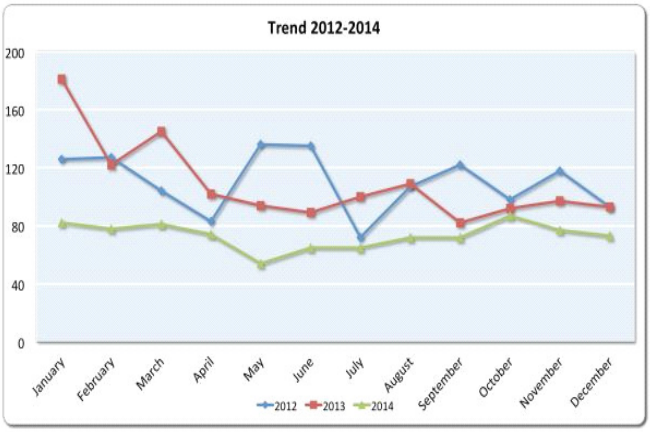


Fig.1.Trend of security threat [12].

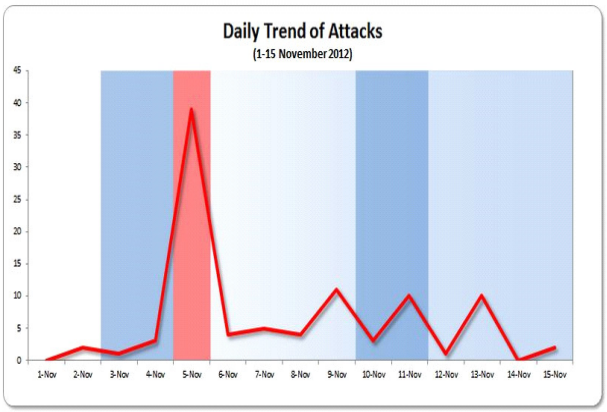


Fig.2. A trend plot of daily attacks [12].

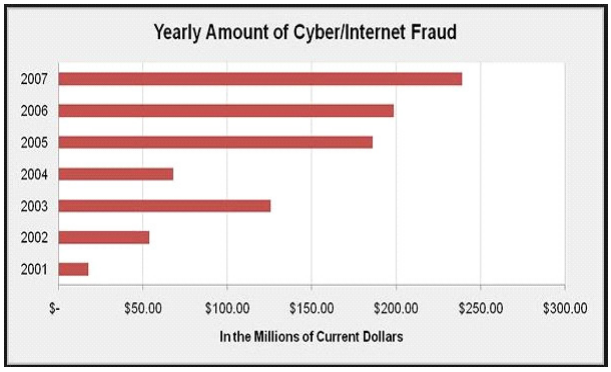


Fig.3. A plot of yearly looses due to cyber fraud [13].

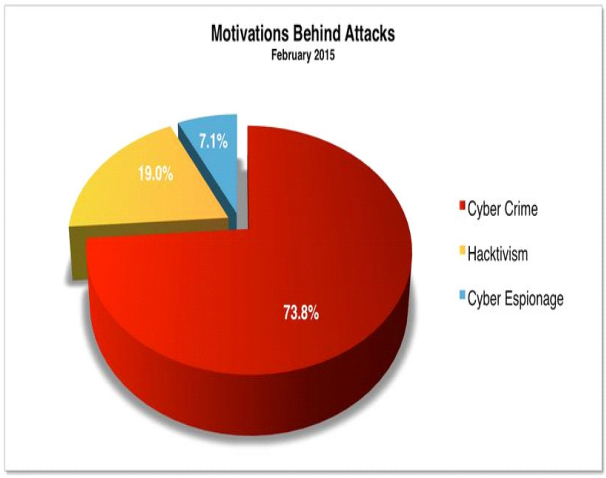


Fig. 4. The brain behind cyber attack [14],

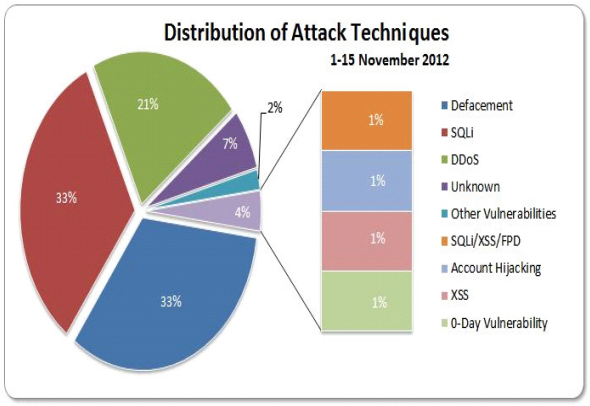


Fig.5. Types of Cyber attacks [12].

IV. PROPOSED ALGORITHM

Many IT experts have given lots of security tips to individuals and organization that will help to reduce the level of attack by cybercriminality. These tips were used to develop a security algorithms referred to as algorithm1 and 2 respectively.

Security tips

Some of these tips will really be of help once they are implemented and deployed by end users. These tips have been tested as functional and effective to be used as a security check. Some of these tips include:

- Protect Passwords
- Send passwords and restricted data securely
- Do not download unknown or unsolicited Programs or Files

- Protect information when using the Internet and email
- No open email relays or unauthorized proxy servers

Security Algorithms

Algorithm 1 gives a guide to security. Where ρ is password, ɗ is authentication, Ƭ is safe, ʉ is user access, ɱ is maxim retry.

Algorithm 1: Guide to security.

1: Input: (ʉ, ɗ)
2: Output:Ƭ
3: Require ʉ
4: Require ɱ
5: Authenticate user
6: Set ɱ = 3
7: If ʉ fail with ɗ
8: Deny access to ʉ
9: Repeat process ɱ
10: If ɱ > 3
11: Block ʉ
12: If ʉ = 1 and ɗ = 1, then
13: Ƭ=1, means system is safe

Algorithm 2 is called the DONTs' algorithm. This will aid security functionality.
Where ʉ is the user access, ρ is password entry, ɗ is authentication of user, ā is allow, δ is for DONT, ɱ is Maximum retry, known access is ŋ̀, and unknown access is ŋ Algorithm 2: The DONTs Algorithm for security.

1: Input (ʉ, ρ, ɗ, ā)
2 : Output (δ)
3: Require (ʉ)
4.:Set ɱ = 3
5: (ŋ̀)
6: (ŋ)
7: if ʉ = ŋ̀
8 : then input ā
9: else δ
10: Do until ɱ=3
11: for ɱ>3
12: Execute δ

V. POTENTIAL SOLUTIONS

This section will present possible tasks that should be adopted to enhance solution to security threats. In this regard, awareness is a key factor in cybersecurity implementation. From IT/security experts perspective, the leverage on the following solutions is highly recommended, viz:

- *Use of network protocol analyser*

A protocol analyzer helps in the examination of granular details of network traffic at the packet level. Some protocol analyzers, however, are either difficult to use or expensive.
Some of them are Microsoft network monitor, ethereal, nagios, OpenNMS, advanced IPScanner, Capsa Free, Fiddler, NetworkMner, PandoraFMS, Zenoss Core, The Dude, Slunk just to mention a few. These tools help to monitor traffic and give alert from hackers and intruders in customized network [16].

- *Password authentication*

Authentication is the process of verifying a claimed identity. In authentication, the person being authenticated would present a password to the authority requiring authentication. If the user were able to present the correct password, he or she would be authorized to gain access to something or to receive services.
Password authentication on the other hand can provide relatively strong security but in order to do so, certain assumptions must be true:

- The user must have some assurance that the authenticator is in fact the authority in question
- The communication channel between the user and the authenticator must itself be secure
- It must be highly unlikely that an attacker would be able to guess the password. Usually this is accomplished by limiting the number of wrong guesses
- If the user is a human being the password must be easy to remember , but not easy that it can be easily guessed

- *Wireless authentication*

Wireless networks are more prone to attacks than wired networks. Therefore, strong authentication is needed in wireless networks [15]. Wireless networks must provide mutual authentication, that is, the authenticator must authenticate the user, but he user must be able to authenticate the authenticator as well. Mutual authentication is particularly important over wireless networks because of the ease with which an attacker can set up a rogue access point. There are two possible attacks in this regard. First, the rogue is not connected to the target network and merely wishes to trick user into divulging authentication credentials. Second, the rogue is connected to the target network. The attacker may then ignore the credentials presented by the user and 'authorize' network access. The user' session may then be recorded in the data path.

- There must be self protection. It must protect itself from eavesdropping since the physical medium is not secure. The authentication must proceed in such a way that eavesdroppers cannot learn

anything useful that would allow them to impersonate the user later.

- The wireless network should be immune to dictionary Attacks. It must not be susceptible to online or offline dictionary attacks.

- An online attack is one of where the imposter must make repeated tries against the authenticator 'on line'. These can be thwarted by limiting the number of failed authentication attempts a user can have

- An offline attack is one where attackers can make repeated tries on their own computers, very rapidly, and without the knowledge of the authenticator. Simple challenge/response methods are susceptible to offline attacks because if attackers capture a single challenge/response pair, they can try al the passwords in the dictionary to see if one produces the desired response
- Produces Session Keys- It must produce session keys that can be used to provide message authentication, confidentiality, integrity, and protection for the session the user is seeking to establish. These keys will be passed to the user's device drivers to be used as Wired Equivalent Privacy (WEP) or Temporary key Integrity Protocol (TKIP) keys during the ensuring session.

VI. CONCLUSION

In this article, threats and vulnerabilities have been explored. It was shown that strong authentication, use of network protocol analyzers, would enhance more safety to in cyber enable device and networks. A strong authentication algorithm was proposed while offering several useful tips in the context of threats and its potential solution. In the future, this work will deal with each type of network protocol analyser, should the trend and the effectiveness of each type. This work will also consider all security solutions to mitigate cybercrime at large.

ACKNOWLEDGEMENT

This research was supported by Tertiary Education Trust Fund (TETFund) through the Ken Saro-Wiwa, Polytechnic, Nigeria.

REFERENCES

[1] http://www.webopedia.com/TERM/C/cyber_crime.html, [Accessed, 10/09/15].
[2] http://www.spiegel.de/international/world/0,1518,713478-6,00.html [Accessed, 10/09/15].
[3] http://www.dw-world.de/dw/article/0,,5645869,00.html, [Accessed, 10/09/15].
[4] http://www.forbes.com/sites/kurtmarko/2014/11/09/big-data-cyber-security/ [Accessed, 10/09/15].
[5] http://its.ucsc.edu/security/top10.html [Accessed,10/09/15].
[6] https://ics-cert.us-cert.gov/Assessments [Accessed,10/09/15].
[7] http://its.ucsc.edu/security/training/intro.html, [Accessed 10/09/15].
[8] Cyber.SecurityFramework.org [Accessed 10/09/15].
[9] http://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx [Accessed 10/09/15].
[10] http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ [Accessed, 10/09/15].
[11] https://www.us-cert.gov/ccubedvp [Accessed,10/09/15].
[12] http://www.forbes.com/sites/kurtmarto/2014/11/09/big-data-cyber [Accessed 10/09/15].
[13] https://prezi.com/6xolemrzxbys/cybercrime/ [Accessed 10/09/15].
[14] http://hackmageddon284.rssing.com/chan-15980644/all_p2.html
[15] J. R.Vacca, Guide to Wireless Network Security, pp. 247-275, Springer Science+ Business Media, LLC, USA, 2006.
[16] http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ [Accessed, 10/09/15].

Mitigating Social Engineering for Improved Cybersecurity

Osuagwu E. U. and Chukwudebe G. A, SMIEEE
Dept. of Electrical/ Electronic Engineering
Federal University of Technology Owerri, Nigeria
ernestfelix54@yahoo.com, gloria_chukwudebe@ieee.org

Salihu T., SMIEEE* and Chukwudebe V. N+.
*Abitus Computers, Port Harcourt, Nigeria.
+Melton Mowbray, Leicestershire, U. K.
tunde.s@ieee.org, debevictor@yahoo.com

***Abstract* - In this paper, Social Engineering threats and trends are investigated and mitigation strategies recommended. The national and economic security of countries now relies on the Cyberspace because virtually all businesses processes are using the Internet. Unfortunately, Cyber-criminality is increasing and rated the fastest growing crime worldwide. *Social engineering*, a technique whereby cybercriminals trick their victims into disclosing log-in information without using any technical gadget has been identified as one of the most dangerous threats of our time. Due to the fact that any identity theft or breach in an organization´s information system resulting in disclosure of sensitive information could have far-reaching consequences such as financial losses, disruption of services, damage to public image, or even bringing the organization or a nation to a complete standstill, this paper x-rayed most prevalent social engineering attacks, their typical tools and recommended mitigation strategies.**

***Keywords*—** social engineering; online security and safety; web threats; social media scams; targeted attacks; data breaches & malware.

I. INTRODUCTION

The availability of Internet has brought great improvement in e-commerce and e-business worldwide, consequently, virtually all human endeavors; financial, education, commerce, research, healthcare, transportation are using the Internet for offering online services. The ubiquity of the online services has reduced the world to a global village, people can access the Internet from anywhere, and thus, they can work from home, shop online and communicate using various media.

Information is one of the most valuable assets in organizations today, because organizations depend on information to operate and make the right decisions. As a result, if critical information is comprised, there is a problem. To protect sensitive information, many organizations follow standards and best practices such as ISO27001, ISO27002, COBIT, etc [1] & [2]. Although such measures help control access and keep information protected to some extent, information security breaches, hacking into organizations' computer networks/storage to steal information is continuing, this is because the processes are executed by people and people are the weakest link, when it comes to security in an organization [3], [4] & [5].

All survey results in recent times show an increase in hacking; this is probably because with the availability of online services, good people as well as criminals are using the Internet to improve their productivity [1] & [6]. There are various ways the cyber-criminals use the Internet, one of the prevalent strategies is to target emails to 'phish' for sensitive information, since email has become an important medium for business communications. This is done by asking the victim directly for his username and password. This has become one of the most dangerous threats of our time. Unfortunately, they succeed because of the natural human tendency for human beings to trust and provide as much help as possible. This technique has been tagged - *Social Engineering* [3].

According to [3], "Social Engineering involves manipulating or tricking people into giving out information or performing an action without using any technical gadget". There are various forms of social engineering and many more are evolving. They target individuals and organizations and many losses and data breaches have been recorded.

Any breach in an organization´s or a nation's information system, resulting in disclosure of sensitive information, could lead to disruption of services, damage to public image, financial losses or even bringing services to a complete standstill. In this paper, the most prevalent social engineering attacks are presented and mitigation strategies are recommended to ensure improved economic and national security.

II. LITERATURE REVIEW - CYBERSPACE THREATS

A. Information Security and Cyber-security

Information is the 'lifeblood' of organizations. Threats to information systems; such as Local Area Networks (LANs) and telecom systems have been around a long time. Some of the threats include: computer viruses, network and application attacks, industrial espionage, denial of service attacks, etc. Some of the threats are *External* while some are *Internal.* The External threats come from outside the organization; it could arise anywhere from one individual to a whole criminal organization. The Internal threats come from employees of the organization; they could be disgruntled employees or ignorant employees who may

sometimes disclose or destroy critical information unintentionally [1], [5], [6] & [7].

Over the years, Information Security has evolved as a discipline for protecting information from various threats because a breach in an organization´s information system, resulting in disclosure of sensitive information could have far-reaching consequences for individuals, the company or the country. Information Security officials are employed in organizations with the primary responsibility to use established standards and controls to ensure that confidentiality, integrity and availability of information is preserved while the information is transmitted or stored.

The **Information Security Controls** comprises of technical products, policies, best practices and education & training. A technology control could be a firewall, a thumbprint scanner, or any other desirable technical mechanism, which could enhance information security. Policies and practices prescribe the desired behaviour of the employees. While education and training ensure that the employees become aware and are trained for protecting information assets.

For many years now, standards and best practices on Information security have been established. There are International standards; (ISO27001, ISO27002), Control Objectives for Information and Related Technology (COBIT), the Sarbanes-Oxley Act, and national standards and guidelines for various countries. For example in Nigeria, there is the National Information Systems and Network Security Standards & Guidelines [1] & [2]. Although, some of the latest information security trends have made organizations safer, cybercrime is increasing rapidly, probably because of numerous advances in microelectronics and telecommunications which gave rise to smart phones, tablets, Internet services such as online banking, cloud data storage and social networking [6] & [7]. This is posing new challenges to established Information Security processes and standards.

Some stakeholders attribute the increasing threats to global economic crisis whereby some jobless people sought new means of financing themselves, some utilized their authorized access to acquire and sell valuable information, and others bought or developed sophisticated tools for creating unique malicious programs to steal valuable information. Such tools have made it possible for anyone to attack organizations or single individuals over the Internet. The number of malicious programs is increasing significantly in Cyberspace. Various countries of the world have scaled to Cybersecurity; which involves protecting information assets by preventing, detecting and responding to *online attacks*.

Cybersecurity has become of crucial importance to the world economy today because presently, many business and government processes rely on computers and the Internet; communication (email, cell phones), entertainment (digital cable, mp3), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment and medical records), etc. With the advances of Internet of Things (IoT), Cybersecurity will even become more crucial worldwide. The threat reports from Information security companies reveal increasing cyber-attacks with companies and individuals losing huge sums of money [6] – [10]. One of the most prevalent cyber-threats, *social engineering* will be discussed in the following section.

B. Social Engineering Threats and Trend

Many criminals have realized that it is sometimes easier to manipulate an employee into providing the password rather than spending excessive time attempting to crack it [3] & [4]. Manipulating an individual into providing sensitive information or performing an action is referred to as "social engineering". The term Social Engineering was made popular by ex-computer criminal Kevin Mitnick [3]. He confessed to illegally accessing private networks and in possession of forged documents. Although, this art of deception has been in existence for many years, for instance, in the 1980s, a man named Stanley Rifkin used a phone to deceive employees working at Security Pacific National Bank into wiring 10.2 million US Dollars into his account in Switzerland [4]. Kevin Mitnick has given several examples in his books on social engineering from the point of a hacker and a victim [4].

A social engineer manipulates or deceives people by using one, or many, social techniques that influence people's minds to alter their behaviour. Sometimes, they succeed by overloading a victim with new information, before previous information has been processed so as to confuse and reduce the victim's ability to think properly. Other times they take advantage of the fact that employees often bypass policies and procedures during emergencies; a social engineer may claim there is a fire in the server room, and that he needs an employee's password urgently to be able to save the employee's data.

Another way in which a social engineer could invoke fear in a victim could be by deceiving the victim into believing that critical data might be lost, if the victim does not follow the social engineer's instructions [3]. Another scenario is a situation whereby, a social engineer can distribute emails, claiming that the first 500 people to register at a web site will win a prize. When people register, the social engineer can get access to the employee's email accounts.

From the study, it was found that social engineers deceive their victims by triggering emotions, positive or negative. The positive emotional exploits include: helpfulness, reciprocation, building trust, integrity, legitimacy, authority, curiosity while negative emotional exploits include: overloading, urgency, fear and scarcity. The basic goals of social engineering are the same as hacking; to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage,

identity theft or simply to disrupt the system or network. Typical targets include: wealthy individuals, telephone companies, multinational corporations, financial institutions, military and government agencies. The social engineer's motives could be financial gain, personal interest, external pressure, intellectual challenge, personal grievance and politics.

The social engineers have well established global network. They have forums, codes of practice, and complex tools for their operation. When they extract information from the user´s email messages, they use the information to steal the user´s identity; search the user´s email box for user-names and passwords to services or websites where the user is registered. The cybercriminals have division of labour, for some, their role is to steal usernames and passwords and sell in their black market. Some others use the username and password to make purchases or transfer money illegally. While others just use the stolen log-in details to phish for sensitive or confidential information the user has sent or received. Some less serious criminals just 'Hijack' the user's account and use the account to distribute 'spam' [11] & [12].

C. Social Engineering Attacks

There are various forms of Social Engineering attacks. The mostly used is *"an email to update your account"*. Many people receive such emails every day. You only become a victim if you complete or click at a link in the email. The simplest example is that the victim's email account will be hijacked and used to send emails to all names in the address book with a pathetic story requesting for money to be sent to a bank account.

Another example is use of a malicious program called keystroke *logger*. The keystroke logger waits until the victim visits a banking website, and then records the victim´s account details and password. These credentials are then forwarded to the creator of the keystroke logger via the Internet. Subsequently, the malware creator may then use the stolen credentials to plunder the victim's bank account. Furthermore, once the malware has done its job, it may also delete itself – in order to avoid possible detection. Fig 1.0 summarizes a classification of various social engineering attacks:

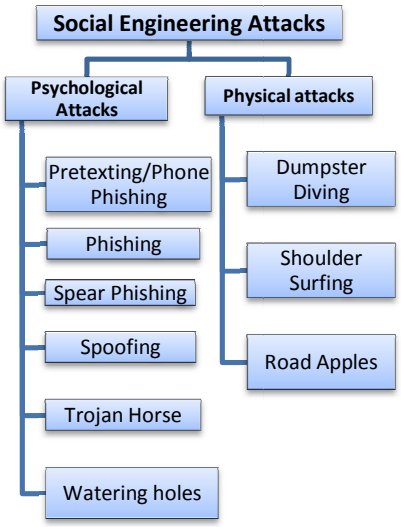


Fig 1.0: Social Engineering Attacks.

Psychological Attacks

Phone Social Engineering/Pretexting - Pretexting is the act of creating and using an invented situation in order to convince a target to release information or grant access to sensitive materials. Often this type of attack is usually implemented over the phone. By answering questions the victim will unknowingly provide the attacker with all the information the hacker needs to carry out the attack.

Phishing - The most common type of phishing involves completion of a fake online form. The attacker sends an email requesting the recipient to complete an online form with name, email address, password, postal address, etc. Using this technique, the social engineer will acquire all the information to get into his victim's email box. Once they highjack ones email they go through to harvest as much sensitive information as possible. Often many users use the same password for all their accounts such as: Yahoo, Gmail, Facebook, banking accounts, etc. So once an attacker has access to one account he/she has admittance to all of them [4].

Spear Phishing - Spear phishing is any highly targeted email or telephone scam, usually employed in a business environment. Spear phishers send email messages or make calls that appear genuine to all staff within a certain organization. Typically, the message looks like it comes from head of HR or from a colleague to everyone in the company. It might include requests for usernames or passwords [11].

Watering Holes - This is a type of social engineering attack in which cybercriminals will identify key web sites that are frequented by individuals or groups they would like to attack, such as mobile app developers. These targeted

Web sites are then infected with malware. An example of one such attack was an iOS mobile developers' forum that hosted malware targeted against Apple and Facebook [12].

Spoofing - Spoofing is the process of falsifying ones identity and masquerading as someone else. The social engineer develops a website that mirrors a trusted website, but can be used either for identity theft, typically by asking users to send login information for the duplicated website or to install malware onto the user's computer [11] & 12].

Trojan Horse - Some social engineers exploit peoples curiosity or greed to deliver "malware". The criminal sends an email with attachment posing as something free or urgent. The attachment could be labeled: tracking number for a courier parcel or a winning prize. Opening the attachment loads Trojan onto one's computer. The Trojan could be designed to track keystrokes, upload address book, or look for financial software files to modify [6], [7] & [11].

Physical attacks

Dumpster Diving - Dumpster diving is looking for information that could be used to carry out an attack on a computer network in someone else's trash (passwords written down on sticky notes, phone list, calendar, or organizational chart) [6], [7] & [11].

Shoulder Surfing - Shoulder surfing involves using direct observation techniques, such as looking over someone's shoulder at public places (airports, banks ATMs, public WiFi areas in hotels) to get his login and password [6] & [7].

Road Apples - refers to situations whereby the cybercriminal drops a physical media such as CD or USB Flash memory that is labeled to draw curiosity ("Executive Salary Survey", "HR Staff Reduction Plan", "Confidential Organizational Changes"). Once a staff picks the media and slots into a PC to view, the "autorun" feature will load Trojan or virus to track keystrokes and harvest IDs and passwords [6] & [7].

D. Related Work

There are many survey reports on breaches, threats and vulnerabilities conducted by researches and security companies. Symantec 2014 report has details of vulnerabilities, web threats, social media scams, targeted attacks, data breaches, e-crime & malware [11]. Madiant's threat report of 2014 revealed that organizations investigated made some gains but attackers still had a free rein in breached environments for a long time before being detected [10]. Further, the survey showed that retailers were found to be the top target because social engineers always devised new ways of stealing credit card numbers from Point-Of-Sale (POS) systems [10].

An Osterman research white paper published in April 2015 reported that malware infiltration was generally getting worse over time and email was identified as the leading source of malware infiltration into organizations [12]. The general observation from major security surveys revealed that the threat landscape is ever changing and that as security teams deploy new defenses, attackers evolve new tactics.

Symantec has the most comprehensive source of Internet threat data in the world through the Symantec™ Global Intelligence Network that monitors threat activity in over 157 countries using Symantec products and services such as Symantec DeepSight™ Intelligence, Symantec™ Managed Security Services, Norton™ consumer products, and other third-party data sources [6] & [11].

III. TYPICAL SOCIAL ENGINEERING SCENARIOS AND TOOLS

Social Engineering Scenarios

Individuals involved in cyber crime have their network and everyone has a service to render. They have different modes of operation and diversified areas of interest. Some are involved in getting details of people's credit cards or account details, some use dating sites to defraud their victims, some are good in writing viruses and attacking computers of big organizations e.g banks and other financial institutions etc. The mostly used are email and phone phishing. Scammers can send emails to more than 1000 people in a day using some of these Internet tools that do not have restrictions. Individuals get emails for password change, bank withdrawal confirmation, promo messages, job alerts etc. These messages are created in such a way as if they are being sent by some known big organization.

When people get such emails, maybe they have heard of a promo from the original firm, or they have withdrawn money, they tend to fall victims without making accurate enquiries. The links included in the emails are professionally cloned websites that are designed with the source codes of the original company website with variation in the extension. From the study, typical scenarios and some real life examples are presented in the following section.

i. Account deactivation/Suspicious log in

Account Deactivation - The scenarios in this category are phishing emails that instruct the receiver to click a link or complete an online form else his bank account will be deactivated or suspended for a stated very convincing reason. The web criminals (social engineers) exploit prevailing situations or events in a country to strategize and plan their crimes. For instance, the Central Bank of Nigeria (CBN) at the time of this study, requested all commercial banks to capture customers' biometrics and assign a unique identification number called Bank Verification Number (BVN). A BVN from one bank identifies a customer for all his other bank accounts. Since this exercise started, cybercriminals have been sending numerous phishing emails and unfortunately many people who become victims do not report. Fig 2.0 is a sample of an account deactivation alert with bank logos to deceive and confuse.

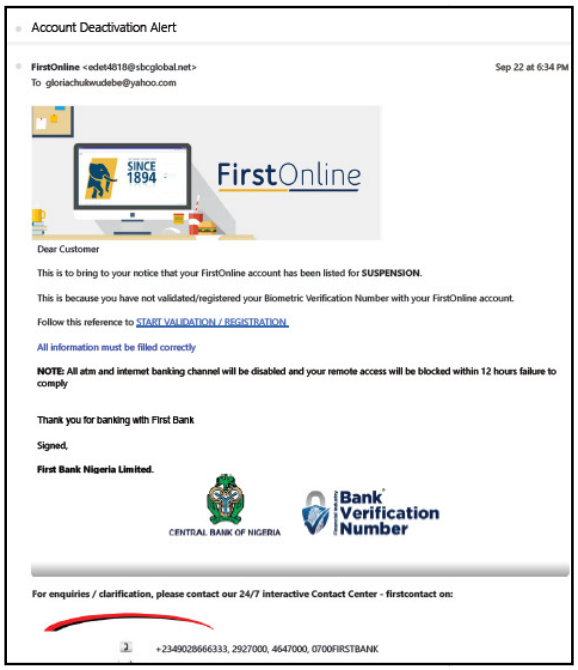


Fig 2.0: Account Deactivation Alert.

Suspicious log in - Many people who use certain types of smart phones have become victim of this type of Phishing email that warns about suspicious log in from another country. This is due to the fact that for some of the smart phones when you log on to your email you can get such a message. Another scenario is when one logs into one of the Nigerian banking platforms, the bank sends email so that you can make a report in case it was an intruder. Fig 3.0 is an example of a suspicious log in alert.

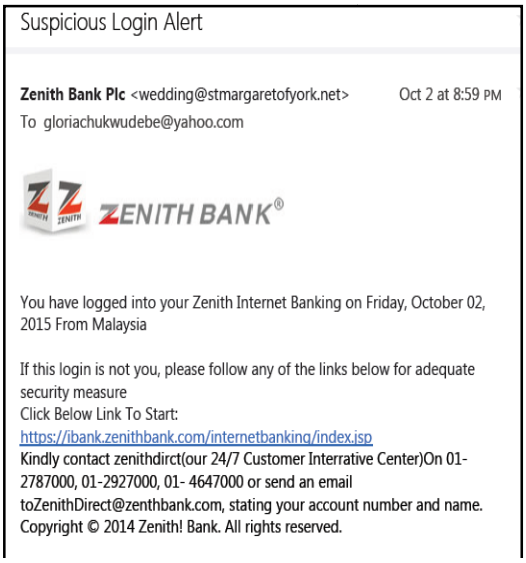


Fig 3.0: An example of a suspicious log in alert.

ii. Log in Details Update/Mail Support

Many have also fallen victims of phishing emails in the above category. Typical content of such emails are as follows: *"Due to the recent upgrade in our SSL server to serve you better, all users are mandated to update their login details in other to enjoy the new upgrade. You are required to update through the link below..."*. Some other emails inform the receiver that his email account has exceeded its limit and needs to be verified and updated, if not verified within 48 hours, the account will be suspended. Snap shots of such emails are shown in Fig 4.0 and Fig 5.0.

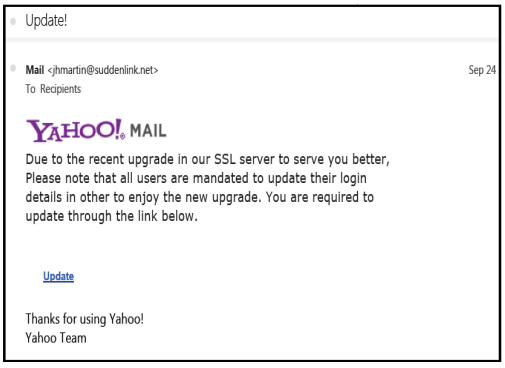


Fig 4.0: Mail Update.

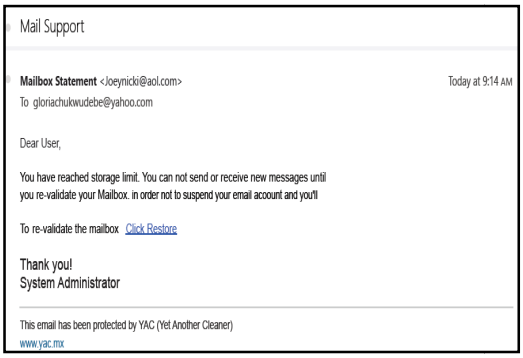


Fig 5.0: Mail box validation.

iii. Job Scam /Conference Invitation

At this period of unemployment, a lot of young people have fallen victim of job scams. The cybercriminals create fake job application portals where there victims pay processing fees online (Fig 6.0). The completed information of their victims are subsequently used for nefarious activities.

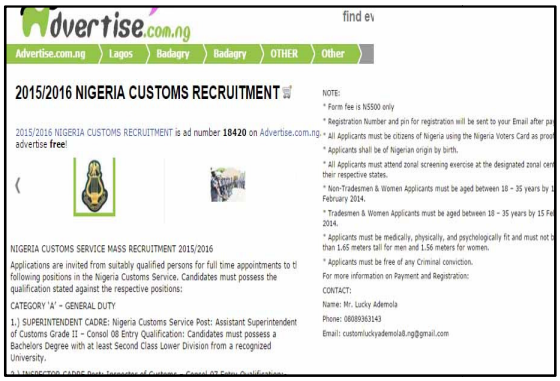


Fig 6.0: Job Scam.

Some phishing emails are invitation to fake conferences in USA or Dubai, they use choice countries people would want to travel to (Fig 7.0).

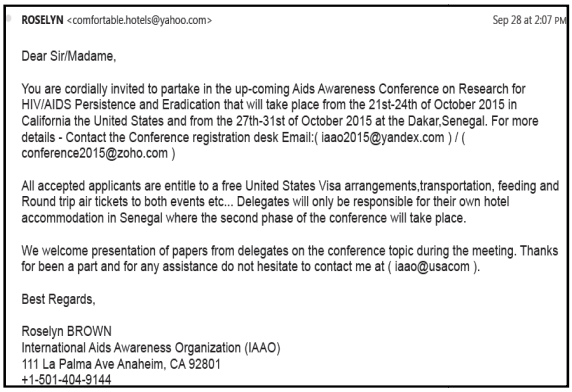


Fig 7.0: Fake Conference Invitation.

iv. Courier Parcel/Proforma Invoice/Award

Phishing emails in this category often contain Trojan horse as html or pdf attachment with the instruction for recipients to download. Real samples are shown in Fig 8.0, Fig 9.0 & Fig 10.0.

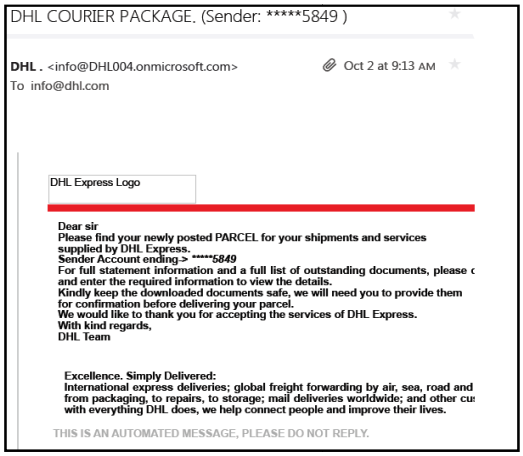


Fig 8.0: Phishing email with Malware (DHL courier).

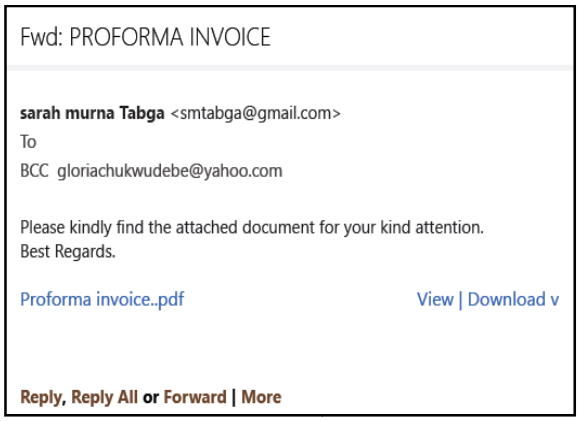


Fig 9.0: Phishing email with Malware (Proforma Invoice).

Fig 10.0: Phishing email with Malware (Award).

v. Password Change/Token advice

From time to time we change our passwords to an online banking account. Here is a real phishing email sent to exploit that scenario; *"Dear customer, this is a confirmation that your password has just been changed. If you did not request for a password change, kindly follow the reference link. If you made this password change kindly follow this link to review your account."*(Fig. 11.0). The email is so worded in such a way that one has a link to click whether you changed password or not.

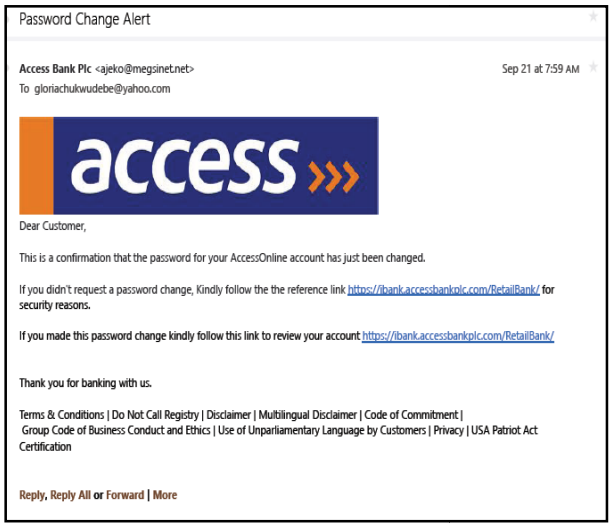


Fig 11.0: Phishing email with Password change alert.

With the introduction of tokens for second authentication, the cybercriminals have devised scam mails targeted at customers new to the use of token. An example phishing email on tokens is shown in Fig 12.0.

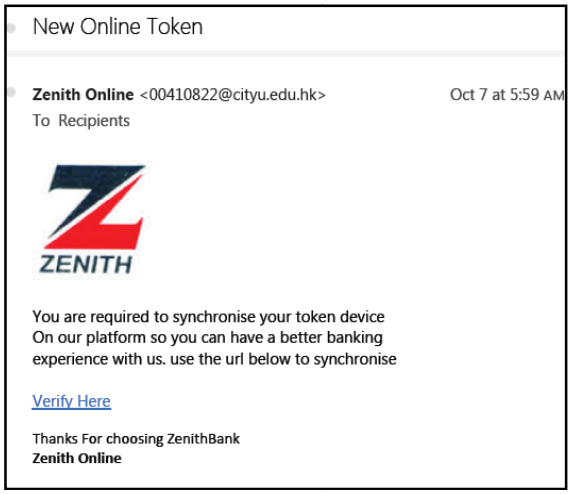


Fig 12.0: Phishing email on Token.

Cyber Attack Tools

i. Use of Internet Software Calls

These Cyber-criminals use Internet Software call facilities such as **Rynga**. With Rynga they can set foreign mobile numbers and use these numbers to call any one irrespective of your location (Fig 13.0). Many people fall victim because of seeing a foreign number display on their phone.

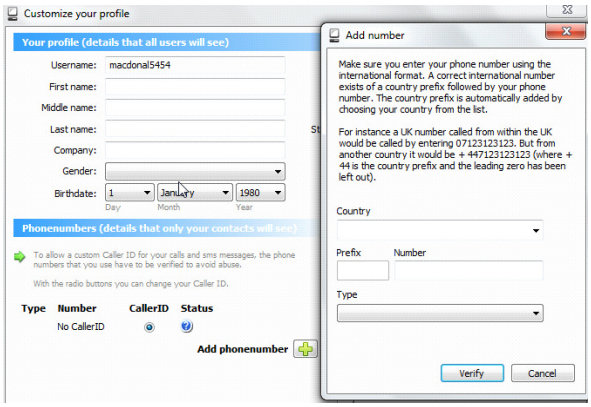


Fig 13.0: Rynga software.

ii. Cybergate

Cybergate is an advanced remote control solution designed for system administrators to control a large number of servers. Currently, Cybergate is being used for targeted attacks. An example is a big organization that are involved in selling machines for agriculture or road construction, they may receive emails with viral pictures of the needed machines, or viral links, once the firm opens

such pictures or links, their systems becomes vulnerable to attack. Fig 14.0 shows a screen shot of systems connected to Cybergate.

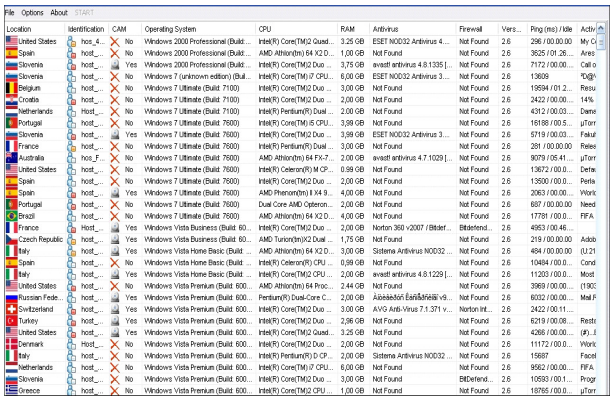


Fig 14.0: Cybergate with connected systems.

The most vital information of the connected systems is the key logger. With the key logger, information keyed in from the keyboard of the victimized systems are exposed to the intruder, who can get the company's email address and password, read and reply emails, divert any financial transaction.

In a similar scenario, there are cases of untargeted attacks, the Cybergate software searches and connects to random computers from different parts of the world. The intruder can gradually search for a system of interest and harvest vital information.

iii. Cain And Abel

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols. A screen shot of Cain and Abel is shown in Fig 15.0.

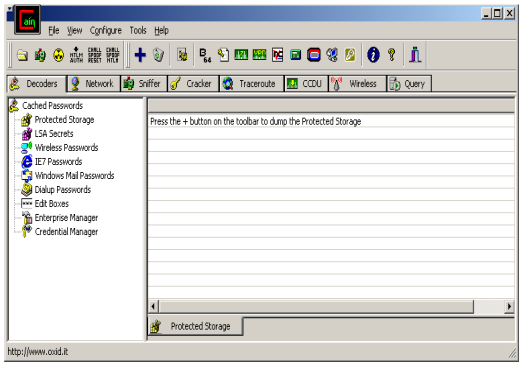


Fig 15.0: Cain and Abel software.

Some virus scanners and browsers detect Cain and Abel as malware but due to program advancement, latest versions of antivirus like Avast no longer sees it as a malware, thereby allowing its functionality. The latest version is faster and contains a lot of new features like APR (ARP Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks. The sniffer in this version can analyze encrypted protocols such as SSH-1 and HTTPS and capture credentials from a wide range of authentication mechanisms. The new version also ships routing protocols authentication monitors and routes extractors, dictionary and brute-force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, cryptanalysis attacks, password decoders etc.

iv. Metaspoilt

Metasploit is a huge database of exploits. There are thousands of exploit codes and payloads that can be used to attack web servers or any computer. It can be used to get root access to a remote computer and plant backdoors or do any other stuff.

Fig 16.0: Metasploit Screen Shot.

Metasploit runs on Unix and Windows. The Metasploit framework can be extended to use add-ons in multiple languages (Fig 16.0).

IV. DISCUSSION

The cybercrime of choice by majority of the criminals is social engineering. They use intelligently crafted phishing emails and phone calls to extract confidential information from naïve people. The success of phishing attempts varies based on the victim's gullibility, their training, their organization's security defenses and other factors.

Today's phishers are much more sophisticated than the "*Nigerian letter scam of the early 1990s popularly called a 419"*. Presently, the social engineers can now mimic legitimate sites much more effectively, making their malicious sites almost indistinguishable from the real thing. From the study, victims they have gotten their emails in the scam black market get up to 200 scam emails a week. Due to the fact that they are using automated tools, they keep sending without regard to whether one is responding or not. Those who are already aware, when they get such emails they either delete or mark it as spam.

As organiations are working hard to mitigate and control breaches, the hackers are developing new strategies and tools to help them to be one step ahead. From the study and reports of software security vendors, *Phishing and insider threats* will continue to be biggest cyber threat sources especially as world economy continue to recess[12], [13] and [14]. The risk grows even larger in social media such as Facebook, Twitter, Myspace etc.

V. RECOMMENDATIONS FOR MITIGATING SOCIAL ENGINEERING

For the world's economy to get full value from technological innovation, it must have a robust, coordinated approach to cybersecurity at organizational, national, regional and global levels because the Internet has turned the world to a global village. Many organizations in the advanced countries appreciate that ***mitigation*** is where enterprises need to start because prevention is significantly more effective and more cost efficient than remediation after an attack.

With the cybercriminals evolving numerous strategies all the time, there is no one single solution that can guarantee 100% security, consequently, all organizations with cyberspace presence should adopt established cybersecurity standards and best practices appropriate for their business process.

Organisations should have an Information/Cyber security policy that is annually updated, train their staff regularly on how to recognize a possible social engineering attack and how to deal with inquiries relating to passwords or other classified information. Most importantly, there is a need for a global action on legal regulations and compliance on cybersecurity especially with the emergence of Internet of things. Specifically, the following recommendations are proffered for Nigeria and developing economies:

a. Anti Phishing Tools

The use of **Anti Phishing Tools** that connect to a database of blacklisted phishing websites is recommended. Some of the examples include: Websense, McAfee's anti–phishing filter, Netcraft anti-phishing system and Microsoft Phishing Filter. This cannot provide 100% security since phishing sites are cheap, easy to build and their average lifetime is only a few days.

b. Increase of the population of Cybersecurity Professionals

There is shortage of Cybersecurity specialists in many developing countries, the ever-changing threat landscape and the need for 24/7 monitoring and response; demands the training of more professionals in this area.

c. Use of appropriate Internet Security Technologies

Businesses with online presence should ensure their Secure Sockets Layer (SSL) or the more robust version of the technology, Extended Validation (EV) SSL certificates are update and are from well known reputable providers; this is the only effective way to help protect customers and the company, from phishing attacks.

These are two crucial security measures that can help customers tell the difference between legitimate sites and fake sites designed to steal their information. Many online consumers now look for clear signs that a web site is legitimate, including small *padlock icons* and *https://* at the beginning of web site URLs.

d. Unique National Identification

Fake identification is still an issue in developing countries. The identities of some of these Cybercriminals cannot be traced. In some of these countries where mobile phone SIM registration is mandatory, these criminals register with untracable identity. To solve this problem, the telecommunication industry or network providers of Nigeria for instance, should devise a means of getting additional information in addition to accurate biometric data of citizens. There should be an integrated database for all telecommunication firms in the country in collaboration with the National Identity Card Management Commission (NIMC).

With database integration, individuals will only present their unique numbers during card registration and their information will be picked from the database.

e. Social Network Vulnerabilities

Individuals, the organized private sector and national governments use social media because of its innovation, convenience, and usability. To mitigate social media threats and vulnerabilities **Telecom and ICT regulatory bodies** of various countries must have a technical solution for control of social network abuse which may go viral and cause breakdown of law and order in a country.

For self protection, individuals should not add unknown persons to their network and also they should choose *Privacy Settings* on Social Networking sites that provide the greatest security and limit information shared with the social networking community.

f. Strong Passwords

Strong Password – Individuals should help themselves, by having a strong password and changing it regularly. Organizations should ensure compliance on office networks.

It is advisable not to have the same passwords for all accounts. Many people store vital information on phones, to avoid identity theft such phones should be passworded.

g. Physical Access

Physical access makes it easy to circumvent security measures. All personnel entering an establishment's ICT facilities should be checked and granted or denied access as appropriate. The data on the computer is just as valuable as the hardware. All machines on the network should be well protected by passwords and all magnetic media (hard drives, disks) should be erased before disposal. Similarly, papers should be shredded before disposal.

h. Ant-virus/malware

System Administrators and individuals should update computer software (operating system, anti-virus, anti-spyware, anti phishing, safe browsing and firewall) regularly. It is important to note that free anti-virus software has limited protection.

i. Staff training

Corporations make the mistake of only protecting themselves from the physical aspect leaving the psychological attacks that hackers commonly use. Many organizations put together education, training and awareness programs quickly in order to meet either an auditor's requirements, or to comply with legal requirement deadlines. Such training is seldom effective. Some do not evaluate the effectiveness of the education, training and awareness programs. Some CEOs frequently neglect to clearly support education, training and awareness programs. If the employees do not feel that their executive leaders support such programs, they may not be motivated to participate. Security education training/awareness program should be well planned, unique to the organization, and be evaluated and supported by the CEO.

VI. CONCLUSION

The national and economic security of countries now rely on the Cyberspace because virtually all business processes are using the Internet. Unfortunately, Cyber-criminality is increasing and rated the fastest growing crime worldwide. Criminal elements are exploiting the responsiveness, convenience and open cyberspace to perpetuate a diverse range of illegal activities that know no geographical boundaries.

Having realized that Email is an important medium for business communication; criminals use a technique tagged social engineering to get access to peoples' emails to 'phish' for sensitive information without using any technical gadget. From the study, this has become one of the most dangerous threats of our time, because of the natural human tendency to trust and provide as much help as possible.

Due to the fact that any identity theft, breach in an organization´s information system, resulting in disclosure of sensitive information, could have far-reaching consequences leading to financial losses, disruption of services, damage to public image, or even bringing the organization to a complete standstill, this paper presented the review of most prevalent social engineering attacks and recommended mitigation strategies.

REFERENCES

[1] G. Mark Hardy and Jaikumar Vijayan, "Risk, Loss and Security Spending in the Financial Sector: A SANS Survey," ©2015 SANS™ Institute, www.sans.org/reading-room/whitepapers/analyst/risk-loss-security-spending-financial-sector-survey-34690.

[2] National Information Systems And Network Security Standards & Guidelines, National Information Technology Development Agency (NITDA), January 2013, http://nitda.gov.ng/

[3] K. Mitnick with W. L. Simon, "Ghost In The Wires: My Adventures as the World's Most Wanted Hacker", August 2011.

[4] K. Mitnick with W. L. Simon, The Art of Intrusion: the Real Stories behind the Exploits of Hackers, Intruders and Deceivers, March 2005.

[5] James Kaplan, Shantnu Sharma, and Allen Weinberg, "Meeting the Cybersecurity Challenge", McKinsey & Company McKinsey Quarterly, June 2011.

[6] Tucker Bailey, Andrea Del Miglio, and Wolf Richter, "The Rising Strategic Risks of Cyberattack", 2015 Internet Security Threat Report, Symantec Corporation, www.symantec.com, April 2015.

[7] Gerhard Eschelbeck, New Platforms and Changing Threats, Security Threat Report 2013, SophosLabs and NakedSecurity.sophos.com.

[8] IBM X-Force Threat Intelligence Quarterly, 4Q 2014, ibm.com/security/xforce/

[9] Jaikumar Vijayan and G. Mark Hardy, "Security Spending and Preparedness in the Financial Sector: A SANS Survey", June 2015.

[10] A View From The Front Lines, Mandiant Threat Report, a FireEye company, M-Trends® 2015, www.mandiant.com.

[11] Tucker Bailey, Josh Brandley, and James Kaplan, "How good is your cyberincidentresponse plan?" McKinsey Quarterly, December 2013.

[12] Best Practices for Dealing with Phishing and Next-Generation Malware, An Osterman Research White Paper Published April 2015, www.ThreatTrackSecurity.com.

[13] Stop Phishing: A Guide to Protecting Your Web Site Against Phishing Scams, www.GeoTrust.com.

[14] The Ultimate Guide to Social Engineering From CSO Magazine and CSOonline.com

National Cyberspace: A Critical Point to Nigerian Economy

Ugwu, Joel N.; Daramola, Comfort Y.; Fagbuagun, Abayomi O.
Department of Computer Science,
Federal University, Oye-Ekiti,
Ekiti State, Nigeria.
{joel.ugwu;yetunde.daramola;abayomi.fagbuagun}@fuoye.edu.ng

Ogwueleka Francisca N.
Department of Computer Science, Federal University, Wukari,
Taraba State, Nigeria.
ogwuelekafn@fuwukari.edu.ng

***Abstract*—The security of National Cyberspace is important and strategic to national development as it is currently the base of national economy. The invention of internet technology has rapidly effected the overall aspect of human endeavor ranging from the methods of communication, banking and financial transactions, trades and businesses, manufacturing and advertising, food processing and supplies, electricity and water tariff control, healthcare and emergency services, energy distribution and transportation, news etc. The current clamor for total migration to e-economy is a testimony of an increasing dependability on the security and reliability of national cyberspace. It is against this background that this paper seeks to request for immediate cyber-security strategy draft by suggesting establishment of Nigerian National Initiative for Cyber-security Education (NNICE) to enhance the draft and champion awareness as a means of reducing cyber threats**

***Keywords*- cyber-security, cyber-wellness, threats, cybersafety, cyberfraudsters, awareness, and education**

I. INTRODUCTION

The journey of every nation into a digital electronic world cannot be complete without the measure of cyber wellness of their citizens. The cyber wellness of a nation is determined from the various factors that contributes towards the safety of cyberspace, which is a notional environment used to describe systems, software and services that are either directly or indirectly connected to internet, telecommunication and computer networks, supported by global distribution of information and communication technology, and network devices [1][2]. The cyber safety assurance should be seen as a national issue that desires a special agency saddled with the responsibility of overseeing the campaign against cyber related threats through the instrumentality of awareness about the prevalence and new threats, and as well as research on the newest discoveries of cyber threats and their remediation in other to advice the government and public on how to exhibit safe disposal. Such an agency has been used by some developed and developing nations like United States and India in other to entrench cyber-wellness of their citizens.

Ugwu and Ogwueleka [3] in their presentation at Cyber Secure Nigeria conference advocated the use of cyber security education as a means of protecting women and children from cybercrime. The dimension of cyber threats has gone beyond taking it as a private issue, one successful attack can create room for others and such is capable of bringing down the national treasury as well as critical national infrastructures. There is a saying that in crime investigation, "everybody is a suspect", in the cyber-world, there is no trusted party; hence the importance of cyber privacy and continued education should be the priority of a nation as it joins the rest of the world in harvesting the benefits of e-economy in the 21st century. But the question still remains, who has the responsibility of championing this awareness campaign?

It is no doubt that many nations have experienced cyber-attacks in the past such as Estonia, Georgia, and Kyrgyzstan [4], but are now using the instrumentality of awareness as a means of awakening the consciousness of the citizenry and streamlining their cyber security strategy against the misfortunes of cyber threat and attack. These go a long way in affirming the fact that one of the best ways of preventing crime is educating people about the crime and the strategies that the criminals use to perpetrate it, which will help people to quickly recognize those steps that might lead to such crime and avoid them.

One of the greatest challenges in curbing the existence of cybercrime is the dynamism of hackers, they can change their strategies with time, exploit, and/or environment. In fact, the issue of cybercrime is a borderless; it can occur within the range of impossible physical distance but at a click reach in the cyber world. When people were ignorant of the existence of cybercrime, simple strategies of deceit were used to exploit them, there was quick advancement in this and change of strategies as people no longer responded to deceitful emails. Nigeria as an economic giant of Africa should have a specialized agency to champion the course of this drive, rather than leaving it only in the hands of the private sector, this agency will coordinate the local campaign as well as research about the new strategies in other to adequately educate the citizens on the current trends of cyber-fraudsters as well as liaise with the international

community to ensure proper protection of the Nigerian image.

The national campaign and drives for safe cyber experience and awareness of the cyber threats should be an unceasing activity which should be championed by a special agency, Nigerian National Initiative for Cyber-security Education (NNICE) with the responsibility of drafting, coordinating, and assisting in the implementation of national cyber-security awareness programs and as well collaborate with other agencies to ensure that such campaign constitute an integral part of the national orientation program. This campaign should cut across all sectors, disciplines, departments, agencies, parastatals, and private sectors to ensure that the public is properly educated on the need to protect the national cyberspace.

II. LITERATURE REVIEW

As the cyberspace contains a mix of good and bad, the bad bring the migration of offline challenges of crime and aggression into the digital world, nations begin to take strategic steps to face off this challenge. Following the Australian Prime minister`s 2008 National Security statement to the parliament acknowledging that online threats has formed their top tier national security priorities, the Australian government in 2009 formed a cyber-security strategy draft. One of the core strategic priorities of the draft is the threat awareness and response campaign. They believed that through the instrumentality of awareness of cyber risks, the Australian people would take steps to protect their identities, privacy and finances online [5].

Reference [1] in his presentation titled ITU national cyber-security strategy guide, identified ten elements that constitute national cyber-security program. The seventh of these elements is cyber-security awareness and education, which he said shall constitute a national program to raise awareness about cyber threats, and help to shape the cultural change, furnishing them with information, which will educate and empower citizens with confidence and practical tools to protect them online.

As contained in the Indian government statement, they observed that cyberspace being a common pool for people of all races, nation, tribes and classes, is vulnerable to wide ranges of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purpose by both nations-states, and non-state actors, Thus formulating a cyber-security strategy draft that will enhance the cyber-wellness experience of their citizens. They observed that rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activities [2].

Observing that information and communication technology has caused major changes to the society over the past decades, as evidenced in the recorded significant improvements in individual and corporate businesses, including nation-states` by the Norwegian government. They maintained that the increasingly integration of ICT into all aspect of the society has improved human standard of living but also has brought a new phase of security challenge, pointing that it is the fact that infrastructures for these services have become critical for normal functioning of the society. It was on this note that they brought a cyber-security draft in 2012, sensitizing all stakeholders to be familiar with risks and secure their systems accordingly [6].

The national strategy for information security in the Slovak Republic, a lay down information security framework for the Slovak Republic was drafted following the 2006 EU strategy for a secure information society. It was captioned as dialogue, partnership, and empowerment, and other strategic document of the advanced information societies (US and Germany), aiming to be used as a means of achieving the cyber-wellness of the Slovak people. Their draft recognized that the security of information systems and networks should be compatible with essential values of a democratic society. Information availability being one of the core objectives of a democratic state is used to equip masses about the prevalence of cyber threats. Thus, formation of a specialized organization to combat computer crimes and ensure mutual cooperation, exchange of information and experience at the domestic level with links to a Europe-wide environment was targeted [7].

Pointing that the issue of cyber safety is a shared responsibility of both the government and the industry, the New Zealand`s government in 2011 brought a cyber-security strategic document which is aimed at building on the existing strategy and partnering with the industry and non-governmental organizations to deliver in the most effective way. One of the core strategies of their government known as `priority 1`, was increasing awareness on online security. These they ensured by providing support to Netsafe, an independent non-profit organization that champions the course of cyber-security education and awareness of cyber threat to their citizens [8].

Identifying the fact that cyberspace offers opportunities of anonymity and deniability for attacks on information systems and data, Turkish Government brought a national Cyber-security Strategy and 2013-2014 Action Plan as a measure to check the effect of these menace. They established a Cyber-security Council, chaired by one of their top government officials, Minister overseeing communication, to facilitate the plans, schedules, report, procedures, principles, and the prepared standard. They observed lack of national awareness on the issues of cyber threats, lack of coordination amongst the partner organizations at the national level in the field of cyber-security related matters, and the fact that most of the cyber-attacks went unreported due to fear of the damage it will bring to their reputation. They maintained that cyber-wellness is a responsibility of every citizens. They also suggested human resources education and awareness raising activities in the field of cyber-security in both short term and medium term as a means of creating proficient human resources [9].

The Swiss Federal Council for Information Society commissioned the national strategy aimed at the protection

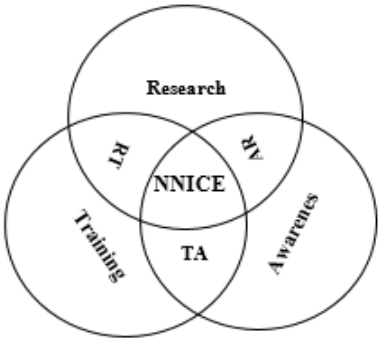
of information and communication infrastructure from cyber threat. Prior to this was the associated concept approved by the council back in 2010, a measure to raise the awareness of swizz population and businesses regarding security consciousness and legal compliant in the use of ICT [10].

In the central objectives of the Dutch national cyber security Strategy (NCSS) is the move from awareness to capacity which necessitated NCSS2, a document captioned with its subtitle as "From Awareness to Capability". Contained in the document is their effort for establishment of taskforce on cyber-security education that will mastermind advisory on the issues about cyber-security curriculum development for primary, secondary, technical and professional courses and proper integration of this as sought with their current initiatives regarding information sciences education and the Technology Pact 2020 [11].

The Spanish National Cyber-security Strategy, [12] was provided by their national Security Council to establish guidelines for secure use of Spanish cyberspace. They observed that the issue of cyber-security was dynamic and suggested coordinated approach within the public and private cooperation capable of ensuring the compatibility of initiatives and fostering of information sharing. They affirmed that the issues of cyber threats should be seen as a shared responsibility of every cyber actor.

III. METHODOLOGY

The general duties of NNICE shall revolve across three core functions which are interrelated to each other, these core duties are: Research, Training, and Awareness. The interrelationship between the core duties yields many other functions.



Fig

A.

NI in

or or

de to

avoid, respond, and/or withstand the occurrence of such attacks. The duty of research will help NNICE to remain updated about the most current of the cyber-criminal strategies. Assist the agency to know happening outside the shores of the country in other to domesticating some of the good strategies adopted by integrating them into the local cultures, norms and values of Nigerians. As the cybercriminals are dynamic, it is only through continuous research that NNICE will be able to discover new ways of combating their crafty strategies.

B. Training

Continuous training of experts in the field of cyber-security education is important and paramount to the overall realization of the cyber-wellness of a nation. NNICE as an agency championing the nation`s strides towards cyber safety shall have the responsibility of training and retraining of their experts and other government`s parastatals that interface with critical national infrastructures which are liable to cyber threats in order acquaint them with the latest findings on how to protect the national image. Training of the NNICE officials remains very important as they shall champion the training of other stake holders and create public awareness. Management of cyber threat is both capital and labor intensive; one of the methods by which it can be reduced is through the use of training as a means of equipping other stake holders. NNICE shall have the responsibility of developing a benchmark to assess public-private agencies and corporation, to ascertain the level of their defense strategy, support, and certify them as need be.

C. Awareness

The consciousness of the citizens about the existence, risk, and methods of control of cyber threats and means of achieving privacy in the use of ICT needs to be awakened. As have been adopted by many nations as one of the practical steps in reducing cyber risks and its related issue, Nigeria, as a nation needs to be a key player among African nations in this, by educating her masses about the need for a cyber safe experience. It is most important this time when the recent rebased GDP, and Foreign direct investment of so many developed nations have confirmed Nigeria as an economic giant of Africa. The motivations of the hacktivists are not public, their aim and actions are always destructive, it is high time that Nigerians come up with NNICE, an agency to champion the strategy draft and cyber threat information sharing campaign.

D. RT, TA, AR

These are the important interrelationships that exist among the NNICE core duties. These relationships are important as they form the basis for achieving the objectives of the agency. It expresses the combination of strengths of research and training, training and awareness and awareness and research respectively. The objectives of NNICE shall revolve around these formidable core duties and will be termed as the NNICE actions.

IV. AWARENESS AND STRATEGIC CYBER-SECURITY ACTIONS

The method of communicating to the public about the important of healthy cyber experience and the generality of securing cyberspace should form a part of early, secondary and tertiary curriculum as virtually all the activities of mankind strongly depend on the cyber network. As suggested by Maruf et al (2014), that the cyber security awareness programs should be integrated with the primary school curriculum. It is necessary to have early education on the existence of cybercrime and thus recommend that the

awareness should cut across all levels of education, including secondary and tertiary just as in Netherland`s NCSS, (2013). In other to ensure that people at all level always adhere to, and imbibe the culture of safe cyber disposal. From reviewed literatures, it was observed that some nations among the developed world created a special agency saddled with responsibility of championing cyber-security awareness. National Initiative for Cyber-security Education (NICE) in United States for instance, has the responsibility of coordinating a national effort focused on the awareness of cyber-security, education, training, and professional development. The two executive branches of the United States in 2008, and 2010 founded NICE (InfoSec, 2015c). The replication of such an agency within the nation to ensure that the security of cyberspace is not handled with levity is advocated. To this effect, there should be an agency called Nigerian National Initiative for Cyber-security Education (NNICE) to champion the course of the national cyber-security awareness across all levels of education and constitute an advisory board to the government on the issue of cyber-security strategic draft. This agency shall work in collaboration with the national orientation agency to ensure that the issue of cyber-security awareness becomes part of the nation's culture by implementing the suggested strategies below.

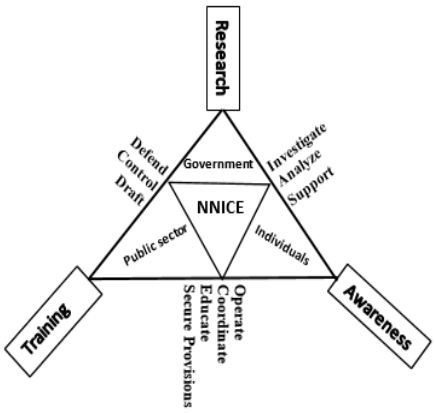


Fig. 2: NNICE Awareness Actors and their Actions

Through the instrumentality of research, Training, and awareness the major objectives of most nation`s cyber security strategy were realized, such objectives as indicated by the figure above include:

i. To defend
Protection of territorial integrity of every nation is trusted to their armed forces, but the territorial border of cyberspace is not physically bound. It is possible for a hacker to sit at the comfort of his home in far of Europe and take control of systems in nearby Africa. NNICE will have as one of its action plan, the duty to defend Nigeria cyberspace by the use of awareness and proper coordination of other cyberactors.

ii. To Control
Controlling the cyber-related activities of other public-private organization should be central to national cyber-security strategy to ensure compliance. NNICE shall also have the responsibility of assessing the awareness activities of the public-private sectors like banks and telecommunication industries to ensure consistency and award recommendations and sanctions when necessary.

iii. To investigate
Investigating the reported cases of cybercrime is important. NNICE a coordinating agency of the government shall be required to investigate any reported case of cybercrime together with other security operatives, in other to devise means of advising the public on how to counter such crimes in the future.

iv. To analyze
It is important that before NNICE submits any report to a supervisory ministry, the result of its investigation be analyzed by their experts. This will help to indicate appropriate actions taken or to be taken to determine and quantify the actual potential loss that was incurred or might be incurred as a result of the attack or realization of the threat. As well as the responses taken to ameliorate the effect of such threat or attack.

v. To support
Supporting other agencies of the government, and taxable public-private sector in terms of training and exchange of manpower should be one of the responsibilities of NNICE. As the coordinating eye of the government, NNICE should be saddled with the responsibility of providing informative support to all arms of government in other to enable them shape their activities and meet up with the cyber-safety demands. NNICE shall also support private sectors by providing current information about cyber threats and educate them on how to achieve safety.

vi. To operate
The NNICE shall operate in the Nigerian cyberspace in a manner that favors the three major cyber actors, the government, public-private organizations, and the individuals.

vii. To coordinate

Coordinating all government efforts on cyber related issues, such as international collaboration, public awareness programs, and certification of private companies based on compliance, research and investigation of attacks and threats` related matters, strategy draft, etc.

viii. To educate
The duty of educating the public about cyber-security is one of the primary responsibility of the NNICE, they shall enlighten the public about the effect of the cyber threats and attack, and also educate them on how to exhibit safe cyber disposal.

ix. Secure provision
The overall responsibility of NNICE is to provide security and protect Nigerian image at the international community. They shall provide security through their researches and education of public institutions and masses on how to protect their vital information and infrastructures.

There is no doubt that cyber-security issues are shared responsibility of every citizen, the government, public-private sectors, and individuals all have their share. NNICE shall be a central agency of the government that will coordinate the efforts of all cyber-security actors.

V. BENEFITS OF AWARENESS

Proper application of awareness shall effectively help to reduce the incessant occurrence of cybercrime in the country. It should be noted that issues about cyber-security is dynamic as the perpetrators often change their styles, awareness should be used as a means of educating the public about the outcome of research on this topic. Nigeria government, public-private institutions, and individuals shall benefit by:

i. Understanding the risk of not keeping to proper online-privacy guidelines.
ii. Learning how to create and manage personal passwords
iii. Learning about the existing cybercrimes
iv. Learning about government's punishments for cybercrimes
v. Learning updates on cybercrimes and safety controls.

VI. CONCLUSION

Issues about cybercrime is now a global challenge, government of every nation are sitting tight on all its matters of concern by drafting strategy and creating special agency to champion the education of their masses. Nigeria as a nation should not be left out in this campaign for safe cyber disposal. Nigeria National Initiative for Cyber-security Education (NNICE) should be created to champion the course of this national campaign.

REFERENCES

[1] F. Wamala, (2011) ITU National Cyber-security Strategy Guide, 2011
[2] Indian Cyber-security strategy, 2013. Notification on National Cyber-security Policy 2013 (NCSP-2013). *Federal Ministry of Information and Communication Technology, Department of Electronic and Information Technology. File No:2(35)/2011*-CERT-In
[3] J. N. Ugwu, F. N. Ogwueleka, Enhancing Cyber Security Awareness through Inter-Disciplinary Campaign: An Ideal for Protecting Women and Children from Cybercrime. *Cyber Secure Nigeria 2015 Conference Proceedings.* Pp 161 – 177.
[4] A. Kozlowski, Comparative Analysis of Cyber-attacks on Estonia, Georgia, Kyrgyzstan. *European Scientific Journal 2014/SPECIAL/edition vol. 3. Pp 237 - 245*
[5] Australia, Australian Government Cyber-security Strategy (2009), ISBN: 978-1-921241-99-4, © Commonwealth of Australia 2009
[6] Norwegian Ministries, Cyber Security Strategy for Norway. *Published by the Ministry of Government Administration, Reform and Church Affairs 2012.*
[7] Slovakia, National Strategy for Information security in the Slovak Republic, 2013.

Mobile Communications Legislation: A Panacea for Telephone Privacy Intrusions

John Funso-Adebayo
Huawei, Lagos, Nigeria
funso@ieee.org

Samuel A. Funso-Adebayo)
Rockseal, Lagos, Nigeria
samadey.fad@gmail.com

Abstract— **The advent of mobile communication technology made it possible for every mobile phone user to be reached, always, provided there is network coverage. However, the recent phone scams and unsolicited deliberate intrusions have shown that there is need for cyber laws and security which will govern the mobile communication sector, if users are to invest and pay more attention to the unlimited value added services rather than the incessant distractions. Good and unified mobile cyber laws and cyber security will give the entire citizenry a sense of ownership, which will in turn sustain the mobile sector investment on the long term.**

***Keywords*— Cyber Law; Mobile Communications.**

I. INTRODUCTION

It has been said that the world today is altogether different from the one of two decades ago and it promises to be even more different, difficult and complex as years go by.

The internet has become a human lifeline as well as the foundation for a large number of human activities and endeavors. Needless to say, the various criminal purposes and legal ramifications to which the internet is now susceptible could not have been envisaged by its founding fathers. Nonetheless, nearly two decades after the emergence of the World Wide Web, Cyber law and Cyber Crime are important topics for consideration by all stakeholders in the digital and mobile ecosystem.

Today, the world is concerned about the security and sovereignty of its computer resources and computer networks. Countries are particular about regulating their communications and access to data that is running on their domestic networks. Consequently, Countries have been looking in the direction of establishing country specific internets [ ].

On the national plane, Nigerian Cyberspace was previously without any legal rule, thereby enabling all sorts of cyber crime activities to continue unfettered. Nigeria's digital economy not having legal and institutional framework for cyber security accounted for the legal and transactional gap and the deficiencies in our law enforcement and national security systems, thus causing a major weakness in our digital economy value chain. Moreover, factors such as e-

government services, payment platforms for e-commerce, automated teller machines, electronic activities of government agencies, cashless Lagos (and soon Nigeria) etc, necessitated the emergence of laws which would cover existing cyber legal issues, regimes and challenges.

On the average about 60% of Nigerians own mobile communication devices [ ]. This gives a whole lot more than the entire population of South Africa.

This is good business for both investors and mobile users, having a major market with active users, it give a wider spread of businesses, projecting small enterprises to great corporations, at the speed of thought!

However, there are a few factors deterrent to this noble venture and investment. These factors have gradually played down the growth, security, and economic vitality of the mobile sector, in West Africa, and especially in Nigeria. The vices of these factors have made prospective customers vow never to own or invest in this 'strange air-based' business but rather stay unknown, and employ freelancers to act on their behalf, through managed and outsourced services, as spokesmen or representatives.

These spokesmen have taken over the airwaves and misguided the real customers, thereby creating avenues for phone scams, threats, and unsolicited intrusions through text messages, voice and video. This paper discusses ways of controlling such vices and offers recommendations on how achieving this may be made economically viable.

II. EASILY ACCESSIBLE MOBILE USERS

One of the key factors which encourage infiltration in the mobile network community is the easily accessible mobile users' database. This can be obtained directly from the licensed mobile operators or indirectly at events.

In the mobile network, the mobile identification number is assigned to a specific user which is supposed to be linked to the user's home or work address [ ]. This should aid tracing and monitoring the location of the user where necessary, but is not the case. Though the investors are apt in their operational duties, the miscreants have found ways around it.

Despite the various initiatives by mobile operators to encourage mobile users register and recharge for more benefits by specifying their work and home addresses, the registration process is still lagging behind, as it is not promoted and supported by all the operators.

While few mobile operators focus on constant network availability and wider coverage, others poach on the weak points of their competitors.

Whichever way, it is very necessary that the number portability as well as the Subscriber Identity Module (SIM) card registration initiatives of the Nigerian Communication Commission (NCC) be rejuvenated and sustained. Furthermore, the database of all mobile users (visitors, roaming or homed), should be inaccessible without the approval of the appropriate authority, for direct request while few cyber-laws can be put in place to protect the indirect requests.

In fairly developed countries, at large events and corporate visits, a biometric interface is now provided to authenticate attendees while Radio Frequency Identification (RFID) is used to confirm the mobile users, as against the regular attendance/visitors' lists [ ]. This has curbed a few attacks as well as leaving no trace of the vulnerable guests/mobile users in such locations. The protocol is automated, as well as every other detail regarding registration. Fig. 1 shows detail service and users on a mobile network.

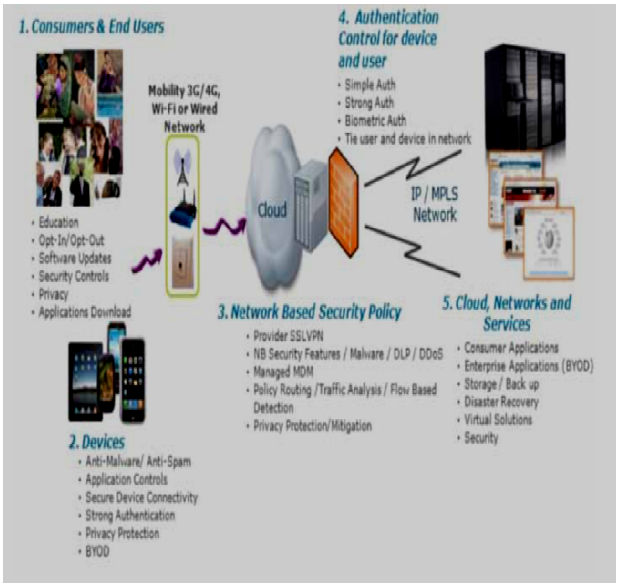


Fig. 1: Detail services/users on a Mobile Network [ ].

III. LACK OF CUSTOMER PREMISE INFRASTRUCTURE

Unlike other countries in the same category, the advent of the Global System for Mobile Communication (GSM) technology in Nigeria is unsustainable. The reason is not farfetched. It is due to lack of training infrastructure which is supposed to transfer knowledge to the customers, thereby giving the mobile users a sense of ownership and investment in the long term.

Looking back at the early years of making an International call in the then Nigerian Telecommunications (NITEL) phone users knew the implication of spending 1 minute on a long distance call, as well as how to do it.

Nowadays, the marketing and sales units of the mobile operators only focus on increase in the credit limits (local calls), and reduced tariffs (international calls) which is good and in order for their businesses. However, the common mobile user needs to be properly oriented on how such calls are placed. It looks a bit odd to engage in this but it will help out in the long term.

Most of the mobile network infrastructures are obsolete because they can no longer support the emerging technologies. These can be setup as training centres in small and remote villages to provide an affordable, if not free, mean of communication in that region, with little or no support (as standalone). Network infrastructures such as the legacy switches take time to install but they last better even in bad weathers, due to the switching modes and techniques incorporated (PTP connections). The modern devices in the power-line communications (broadband), and digital broadcasting (DTV), can be integrated into the available FOC on such equipment, for high delivery/traffic.

IV. HOW CYBER LAW CAN INCREASE INVESTMENT OPPORTUNITIES

There is a general saying, that, where there is no law, there is no crime~ [ ].

The present cyber law in Nigeria is on the waiting list and focuses more on the IT sector. Provided all validation processes are completed, a customer can buy and use a SIM legitimately. However, when a case of infiltration arises, the customer can approach the relevant customer friendship centre for help and be availed of the usual police report request. There can even be an automated IVR setup for this purpose, as against what is operational at present, recording the customers' voice for security purposes.

A win-win case not only ensures that receivers (operators of call centres) are protected, but also ensures customers are properly understood and well serviced until their requests are closed. A call back will be good as well to ensure the customer is well satisfied and willing to renew their subscription. A cyber law is the only instrument that will enlighten stakeholders of the proper implementation in this regard.

Fig. 2: Shows the meaning of the acronym cyber safety.

The Cyber Crimes (Prohibition, Prevention, etc) Act 2015 provisions can be summarized as follows:

Part I (sections 1 and 2) - provisions on the objectives and application of the Act.
Part II (sections 3 and 4) - provisions on the protection of critical national information infrastructure.
Part III (sections 5 to 36) - provisions on what amounts to offences under the Act and the penalties for such offences.
Part IV (sections 37 to 40) - provisions on the duties of financial institutions.
Part V (sections 41 to 44) - provisions on administration and enforcement.
Part VI (sections 45 to 49) - provisions on arrests, search, seizure and prosecution).
Part VII (sections 50 to 56) - provisions on jurisdiction and international co-operation.
Part VIII (sections 57 to 59) – Miscellaneous provisions.

V. CONCLUSION

The recently enacted CYBER CRIMES (PROHIBITION, PREVENTION, ETC) ACT 2015 provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cyber crimes in Nigeria. The Act also ensures the protection of critical national information infrastructure promotes cyber security, the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.
The Act is the only relevant statutory authority in Nigeria, having unified all other laws in relation to the protection of the Nigerian Cyber Space and it is hoped that its enactment will in turn adequately enable the development of the jurisprudence of law by Nigerian courts in the area of cyber security.

REFERENCES

[1] Legislation on Cyber Crime in Nigeria: Imperatives and Challenges, a presentation by T.G George Maria Tyendezwa
[2] Cyber law – Existing Cyber Legal Issues, Regimes & Challenges, a presentation by Pavan Duggal Advocate Supreme Court of India.
[3] Cyber Crimes (Prohibition, Prevention, Etc) Act 2015.
[4] Today's Cyber Security in Mobile Networks by CTIA, 2013

Cybersecurity Controls in Mobile Device Environment

Olileanya Ogbonna *PMP, R. Eng*
Project Management Dept, EYEJAY Trade & Services LTD
pc@eyejayts.com

***Abstract*–In recent years, there has been a sustained growth in the amount of information processing devices that are able to communicate with one another particularly small handheld devices. In addition, there has also been a great growth in the relationship that exist between the Nigerian populace and automated information systems. However, since large number of citizens uses mobile devices as the primary tools of engagement in the cyberspace, certain controls need to be in place to safeguard these users and their activities. Also, there is the need to ensure that the individuals are properly aware of the risks and the controls needed to be safe while online. This paper explores the issue of cybersecurity awareness and how certain controls can be applied to help increase user cybersecurity awareness and engagement. This will improve the ability of the average user of computer communication devices in managing potential threats to the Nigerian cyberspace.**

Keywords - Cybersecurity controls, cybersecurity awareness, incident reporting.

I. INTRODUCTION

In Nigeria today, there is an increase in the use of data processing, storage and communication devices by her citizens. There are private and public sector activities that involve massive utilization of computer based applications and infrastructure. At the heart of the system is data; how it is processed and managed across different transmitting routes and storage devices. The relevance of this data to the users and owners has made the infrastructure associated with it quite sensitive. The Nigerian government had sought to deal with the issues involved with data and data processing infrastructure. In 2015, an act was passed and signed into law.

The act among other things was designed to ensure the protection of critical national information infrastructure, promote cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights. The law enabled the President of Nigeria by the recommendation of the National Security Adviser, (having fulfilled other requirements) to designate certain computer systems and networks as "critical national information infrastructure" [1]. It is expected that such infrastructure would have the highest level of protection available assigned to it.

The users of different elements in the cyberspace 'ecosystem' have different levels of technical competence. This helps them to carry out their activities with minimal stress. There is need to discover if there is anything that can be done to enable these users, to be more cautious as well as involved in managing risks and threats to this system.

The 2014 Nigerian Cyber Threat Barometer Report had among other things suggested that Nigeria deploys its resources in three different areas namely: Training, Education and Awareness. Awareness is a very critical issue and involves awareness of information security requirements and awareness of individual participant responsibilities. It also involves awareness of risks, threats and potential responses. [2]

Cyberspace Ecosystem

The cyberspace or cyber ecosystem involves the following groups of equipment viz:

- Data input / processing devices
- Data storage devices
- Data networking devices

The vast amount of computers, smart phones and tablets form the first part of this ecosystem. These devices also have data storage capabilities but there are a distinct group of devices that are designed purely for data storage. A lot of these are found in large datacenters around the world. The interconnection between these devices is accomplished using wireline and wireless infrastructure.

With regards location specific information, the access terminals and data processing devices could be within Nigeria's physical environment, the massive data storage devices maybe in foreign countries and a small part of the interconnection framework may be resident locally, while the others are outside Nigerian national boundaries. This distribution of devices across different legal jurisdictions poses challenges in handling cyber crime.

User data or information is at the core of all manual and automated data systems.

Crimes that affect user data are the ones that attract the most attention from individual users of computers and associated devices.

The Nigerian cyber ecosystem has a large amount of mobile devices and to a lot of Nigerians the primary contact with telecommunications services is through mobile technologies. Fig.1 shows the April – July 2015 monthly subscriber data from Nigerian Communications Commission (NCC). According to the NCC reports, as at July 2015, Nigeria had over one hundred and fifty million (150, 741, 005) telephone subscriptions and a tele density of 107.67%. Of these subscriptions, about one hundred and forty-eight million (148,651,702) were full mobile telephone subscriptions accounting for about 99.87 % of the total subscriptions while fixed wire and fixed wireless subscriptions were about one hundred and eighty-eight thousand (188,281), accounting for 0.13% of the total subscriptions [3].

Monthly Subscriber Data Annual Subscriber Data

Months: May 2014 - July 2015

	Operator	Jul '15	Jun '15	May '15	Apr
Connected Lines	Mobile (GSM)	-	-	-	192,769,
	Mobile (CDMA)	-	-	-	3,799,
	Fixed Wired/Wireless	-	-	-	371,
	Total	-	-	-	196,941,
Active Lines	Mobile (GSM)	148,495,205	146,486,786	144,386,841	143,057,
	Mobile (CDMA)	2,057,519	2,105,981	1,993,278	2,234,
	Fixed Wired/Wireless	188,281	182,643	181,625	184,
	Total	150,741,005	148,775,410	146,561,744	145,476,
	Teledensity	107.67	106.27	104.69	103

1. Teledensity is calculated based on a national population of 140 million.
According 2006 Last Census Population Figures.

Fig.1: Monthly Subscriber Data in Nigeria, (Source:NCC Report ,2015).

Cybersecurity Awareness and Controls

Cybersecurity awareness will help in managing cyber threats and cyber crime. There are different bodies in different countries working on engaging the local populations on cybersecurity awareness and controls. Get Cyber Safe is a national public awareness campaign in Canada created to educate Canadians about Internet security and the different steps they can take to protect themselves online. The campaign's goal is to bring together all levels of government, the public and private sectors, and the international community, to help Canadians be safer online. [4]

In the financial sector, the Federal Financial Institutions Examination Council (FFIEC) members are also involved in raising the awareness of financial institutions and their critical third-party service providers with respect to cybersecurity risks and the need to identify, assess, and mitigate these risks. This is because of the rise in volume and sophistication of cyber threats [5].

The United States of America has October designated as National Cybersecurity Awareness Month. National Cybersecurity Awareness Month is designed to engage and educate public and private sector partners through events and initiatives aimed at raising awareness about cybersecurity and increasing the resiliency of the American nation in the event of a cyber incident. National Cybersecurity Awareness Month is sponsored by the Department of Homeland Security in cooperation with the National Cybersecurity Alliance and the Multi-State Information Sharing and Analysis Center[6].

The Nigerian National Information Technology Agency (NITDA) has put in place a Computer Emergency Readiness and Response Team (CERRT.ng). CERRT.ng is a team established to provide support in responding to cybersecurity incidents involving or affecting Nigerians. CERRT.ng will build national cybersecurity readiness through fostering the development of sectorial Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs). The CERRT.ng ecosystem will among other things:

- Identify existing and potential computer related threats
- Notify as appropriate
- Build capacities
- Coordinate requisite responses
- Build relationships
- Liaise as needed with similar incident response teams locally and worldwide as well as develop the requisite readiness processes [7].

To report an incident one can download a pdf form "Incident Reporting Form" on the CERRT.ng website and provide the necessary details of the incident. Not many Nigerians know about CERRT or its activities.

The Nigerian Communication Commission (NCC) also keeps incident reports of cybersecurity threats compiled from around the world. The reports can be downloaded from the NCC website.

There are also certain private sector initiatives. Cybersecurity Experts Association of Nigeria (CSEAN) is a "*STOP.THINK. CONNECT.*" Partner. "STOP. THINK. CONNECT" is a global cybersecurity awareness campaign to help all digital citizens stay safer and more secure online. [8]

On a global scale, there is an international government-industry effort to promote certain controls known as 'critical security controls' (CSCs) for computer and network security. The Council on CyberSecurity coordinates the development of these controls. There are twenty (20) controls. These controls (and sub-controls) focus on various technical measures and activities, aimed at helping organisations prioritise their efforts to defend against the current most common and damaging computer and network attacks. The Critical Security Controls for cyber defence are a

baseline of high-priority information security measures and controls that can be applied across an organization in order to improve its cyber defence [9].

Mobile Device Environment

There are two layers of mobile device activity. One is the operating system (OS) and the other is the application software or apps as they are generally referred to. The advantage with the mobile platform is that apps are usually downloaded from a centralized platform. Users can still obtain apps from third party platforms but on the average users utilize the app stores of the mobile operating system.

There are different operating systems for mobile devices. As shown in Table 1, in 2014, more than a billion smart phones were sold and global market share was 80.7% for Android, 15.4% for iOS, 2.8% for Windows Phone and remaining 1.1% for all other platforms.

TABLE 1. Operating System Market Share, (Source: Gartner (March 2015). [10].

Operating System	2014 Units	2014 Market Share (%)	2013 Units	2013 Market Share (%)
Android	1,004,675	80.7	761,288	78.5
iOS	191,426	15.4	150,786	15.5
Windows	35,133	2.8	30,714	3.2
BlackBerry	7,911	0.6	18,606	1.9
Other OS	5,745	0.5	8,327	0.9
Total	1,244,890	100.0	969,721	100.0

In Nigeria, there is a huge mobile device internet presence. The active internet subscriptions from mobile devices as at June 2015 are illustrated in Fig. 2 [11].

	Jun '15	May '15	Apr '15	Mar '15	Feb '15
Airtel	17,598,626	17,634,885	17,272,665	16,603,147	15,894,061
Etisalat	15,285,079	10,330,559	10,421,229	10,189,568	9,852,713
Globacom	19,330,549	19,340,990	19,690,526	18,617,607	18,184,587
MTN	40,485,670	40,830,146	39,520,285	39,904,772	39,278,019
Total	92,699,924	88,136,580	86,904,705	85,315,094	83,209,380

Fig. 2: Active Internet Subscriptions in Nigeria [11].

Apart from the subscriptions shown In Fig.2, there are other subscribers connected to companies providing broadband internet access. With a lot of activity being done on mobile devices, user must be involved in managing cyber threats. In this regard, cybersecurity will requires a lot of emphasis to be placed on the mobile device environment. In addition, government personnels use smart devices to exchange sensitive information. Therefore, any security awareness strategy that will have national significance must engage citizens at their point of primary activities on the cyberspace platform.

Vulnerabilities, Threats and Risks

Certain risks and threats are prevalent among mobile users. According to Eric Beehler in his article "Top five mobile application vulnerabilities", "devices are often blamed for insecurities, but mobile app vulnerabilities are insidious." He listed top five mobile application vulnerabilities viz [12]:

- Bad data storage practices
- Malware
- Unauthorized access
- Lack of encryption
- Data leaks from syncing

Essentially, mobile apps with such vulnerabilities ultimately pose great risks. Common Vulnerability Scoring System (CVSS) is a free, and open industry standard for assessing the severity of computer system security vulnerabilities. The Forum of Incident Response and Security Teams (FIRST) manage it. CVSS seeks to establish a measure of how much concern a vulnerability warrants, compared to other vulnerabilities, so efforts can be prioritized. The scores are based on a series of measurements (called metrics) based on expert assessment. The scores range from 0 to 10. Vulnerabilities with a base score in the range 7.0-10.0 are High, those in the range 4.0-6.9 as Medium, and 0-3.9 as Low [13]

The smartphone, tablet or laptop- contains significant information about individuals and their friends and family – contact numbers, photos, location and more. Mobile devices need to be protected [14].

In Nigerian environment, the major risks are associated with phishing and malwares threats.

Now, phishing is a technique used by identity thieves to steal personal information, usually passwords or financial information. Identity thieves try to lure unsuspecting individuals into giving up personal information by making what looks like a legitimate request from an organization one trusts. These might look like they are from a bank, credit card company, or even a University. Unfortunately, phishing scams can be highly effective [15]. If a user keeps a bank account and an email address, there is a very high probability of receiving an phishing email requesting such a user to update bank account details. Nigerians receive so many of such messages. Some of these request the recipient to follow some rogue web link that are illegitimate.

Malwares or malicious software constitutes another risk. A malware is any software used to interfere with computer normal operation, obtain sensitive information, or gain access to private computer systems. Malware has malicious intent, acting against the requirements of the computer user [16]. An advanced case, is mobile banking applications that do not come from the bank's authorised developers.

In cases where certain problems have been discovered on the software of any device, a patch can be deployed. Patches are useful in managing security breaches and flaws in apps and OS. A patch is a piece of software code that can be applied after the software program has been installed to correct an issue with that program [17]. One observation about patches is that they may not be enabled to automatically run once available and as such a user can have a device functioning without carrying out patch updates on software that require them.

User Involvement

People do not feed on information and communication technology devices, they simply use them as tools. Does knowing the location of a developer have any role to play in the cybersecurity issue? Maybe not. How many people install apps with little recourse to identifying the developers and their registered business locations? People need to understand their level of involvement in the cyberspace activities and its effect on their life.

There is need for a system that ensures the individual, (who is the most important agent in our ecosystem), is constantly aware of the risks, threats and implications of interactions with the cyber space.

With the aid of that awareness level, the user becomes a vital agent in managing security at different layers, the basic one being activities from user terminals and devices used by the individual. The user engagement and awareness improvement system can be deployedwith minimal interference with the individual's privacy and at relatively low cost to the individual. To be able to deploy any awareness building solution it is necessary to investigate the various activities carried out by users and how much of these activities the users pay attention to in any level of detail.

II. RESEARCH METHOD

In order to gauge the awareness level of the users on the challenges of being part of the cyberspace and security controls that could be applied, certain questions were posed to different people. The responses to these questions and the analysis form the remainder of this paper.

The survey was administered electronically using a web platform provided by *kwik surveys*. The link to the survey is http://kwiksurveys.com/s/o8toS0zw. Respondents cut across different age groups and academic background. Over 90% of them are resident in Africa.

The questions were structured with three different options; these are - Yes; No; Not Sure. Fifty-eight (58) respondents answered all the questions required for this study. Fifteen (15) other respondents did not complete all the required questions and their input was excluded in the analysis

III. SURVEY CONSIDERATIONS

In this paper, the investigation carried out considered the following issues viz:

- Awareness level at points of engagement: how aware are the individuals of their own cyberspace activities?
- Information sources – how and through whom do individuals obtain information on cybersecurity, cyber threats and general information security?
- Reporting/response platforms – what means are available to engage the user in providing information that can help deal with cyber threats and information security issues?

Awareness Level

Results obtained showed a certain degree of awareness with respect to certain issues but less on others. In this regard, the areas of concern are:

- Devices used
- OS: updates and security implications
- Apps on devices; Apps used regularly and Redundant apps
- Apps with access to sensitive information

Devices used

Most respondents (95%) were aware of the number of mobile data-enabled devices (smartphones, tablets, mobile phones) they possess or used regularly. 84% of the respondents were able to tell what information appeared first as soon as the devices they used were powered on.

OS: Updates and security implications

Operating system information is usually taken for granted. About 59% of the respondents were confident of the OS versions on their mobile devices. Only 28% kept track of how many OS updates were actually taking place. About 38% of the respondents bothered to know the reason for the updates.

With regards security, 40% of the respondents considered that the updates were done to address security concerns, 28% of the respondents felt that the OS with relatively frequent updates were more secure, however 29% felt that OS with more updates are relatively more prone to security breaches.

When dealing with the issue of device level tracking of updates, only 17% of the respondents think the OS has a way of telling the user how many OS updates have been done during a given year.

Apps on devices; Apps Used Regularly and Redundant Apps

In this regard, 22% of respondents could confidently say that they knew the number of apps on their mobile devices and 74% acknowledged that they carried out banking or financial transactions from the devices. 90% of the respondents were sure of which apps that they regularly used on their devices but the challenge came with knowing which companies developed these apps that they constantly used and the location of these software companies/developers.

Only 26% of respondents knew which companies manufactured the apps frequently used on their mobile devices and 19% could claim to know which countries these companies were located. Interestingly only 24% had ever read through the end user license agreement of the mobile device OS or any app being installed on their mobile devices.

A good number of the respondents (88%) knew where to locate the list of apps on the devices. Only 21% of the respondents felt that the volume of installed apps was too much to effectively keep track of these apps. This could imply that a number of people had redundant apps or apps that were rarely utilized. About 17% of the respondents had ever made attempts to keep a list of the apps on their devices.

Apps with access to sensitive information

When asked about knowing which apps on their devices that access personally identifiable information (where personally identifiable data include information about the device registered user/owner and could be any or all of the following: name, age, sex, nationality and location including current GPS location), only 41% of the respondents were aware of such apps. A further probe showed 71% of the respondents would love a situation where they could export a list of all those apps. An interesting observation is that 88% of the respondents would like the list of apps exported to include information on locations of companies that provide them and applicable data protection rights in their nations.

Summary on Awareness Level

The consciousness level was high on factors in Fig. 3 but low on factors in Fig. 4 and Fig. 5

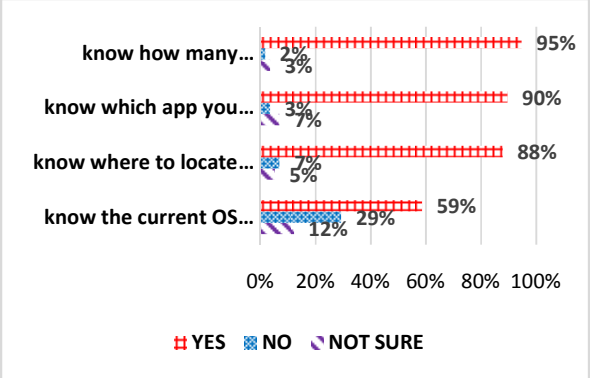


Fig.3. Awareness level Performance Prob 1.

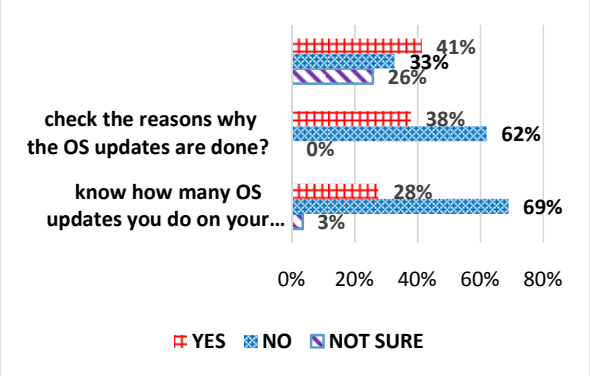


Fig.4. Awareness level Performance Prob 2.

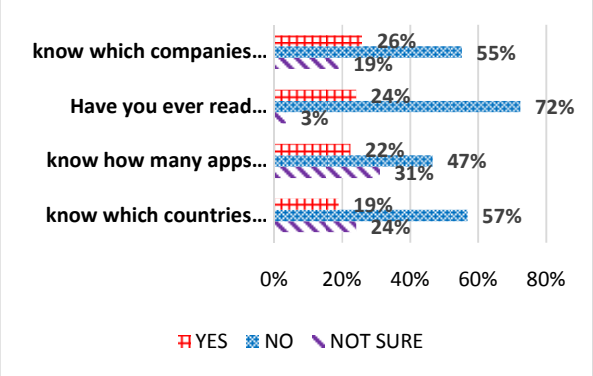


Fig.5. Awareness level Performance Prob 3.

Information Sources

Only 19% of the respondents had ever attended any information security or cybersecurity training. On the ease of obtaining information on cybersecurity only 34% of the respondents knew where to easily obtain reliable and accurate information on issues regarding cybersecurity. The distribution with respect to sources of information is given in Fig. 6

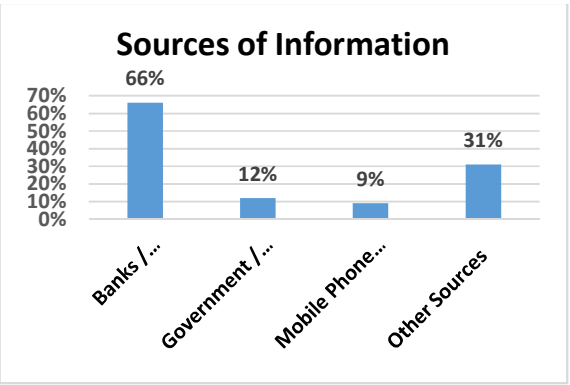


Fig. 6. Information Sources.

A larger number of respondents received information on cybersecurity from banks / financial institutions. The mobile phone companies featured least among the respondents as a source of information on cybersecurity. This is quite

disturbing considering that the mobile phone companies provide the platform for cyberspace activities in the nation. 31% of the respondents admitted to obtaining tips on cybersecurity from other sources. When asked if they felt they received enough information from these sources identified the response is given in Fig. 7

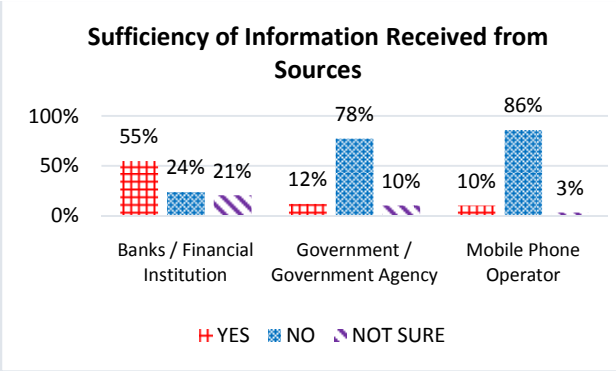


Fig.7. Sufficiency of Information Received.

More people (55%) perceived the banks and financial institutions as providing sufficient information to help handle cyber security risks and threats. 78% of the respondents felt the government was not providing enough information and 86% of the respondents felt the mobile phone companies were not providing enough information and safety tips on cyber security.

Concerning volume of messages sent on cyber security and cyber threats, 10% of the respondents felt the banks sent too many messages while 3% felt the government sent too many messages and 5% felt the mobile phone companies sent too many messages. Too many messages may not be considered as spam.

Reporting / Response Platforms

A major part of the survey was to ascertain the level of cooperation users would be able to offer in the cybersecurity issue. 62% of the respondents were willing to accept an alert on their device screen, during power on and once a day as a reminder to be cyber security conscious, with a link on how to obtain extra information and tips while 78% of the respondents were willing to utilize an application on their device to provide real-time information on possible threats to cybersecurity. Considering that the use of the app would involve data subscription costs, about 55% of the respondents were of the opinion that such an app should have free data access.

One major discovery is that only 10% of the respondents who live in Africa knew the local agency setup to handle cybersecurity issues.

IV. OBSERVATIONS AND DEDUCTIONS

From the results obtained, there were noticeable lapses in the sense of security required of the device users. It appeared most individuals assumed that devices were safe and were generally unaware of other issues associated with mobile device vulnerabilities and the role of regular OS updates to check that. It was also noticed that the respondents were not so conscious of ability of apps to request certain permissions to vital personal information and to transmit same.

The danger is that users could share information across apps and platforms without understanding the implications. The assumption is that if people cannot easily tell what activities they are involved in and with what applications they use, it would be difficult to get them to deal with breaches. It has been said that it is difficult to manage what cannot be measured how much more what is not being tracked. Considering that people hardly check where the developers of apps were located, one could assume that the users felt the cyber space is not one with geographic boundaries.

Banks, financial institutions, mobile phone companies, government agencies were among the sources sampled to check how conversant the users were of the activities of these bodies to keep them informed about cybersecurity threats and risks. There was a lack of visibility of the activities of government agencies and not many people had been part of any formal training on cybersecurity and information security.

It was observed that a lot of the information on cybersecurity came from the banks and financial institutions. However, certain people complained that the messages received were too much and this could imply that a number of these messages were discarded without completely reading through.

The banks had been compelled by the Central Bank of Nigeria to deploy ISO 27001 Information security standard. [18] The banks also pursued a policy to enlighten their clients on cybersecurity as well as general information security safeguards. This is accomplished through emails and short mobile messages (SMS).

The major objective of the information obtained is to design a system that could help in implementing certain controls and handle identified lapses. A full breakdown of the lapses and mode of remedying it will be described in the next section.

V. RECOMMENDATIONS

Distilled Requirements

Accomplishing certain controls can be integrated into a mobile device app. The requirements of this app and functions desired as gleaned from the survey respondents can be itemized below:

- Web link to national and international cyber attack response agencies
- Identification of a source for cybersecurity tips and information
- Daily notification of cybersecurity updates and tips.

- App developer and location of operation
- Incident report generation and transmission platform
- App usage tracker to tell which apps have not been in use for a long while. The user can configure this duration time.
- Export function of apps installed on device and permissions granted to those apps including app developer information
- Forced OS version update alert

Exporting the list of apps could take various forms but a more viable option would be to email the list of apps.

There are two platforms with the largest amount of devices. These are: android, and IOS. Mobile/Tablet Operating System Market Share (January, 2015 to August, 2015) is shown in Fig. 8 [19]

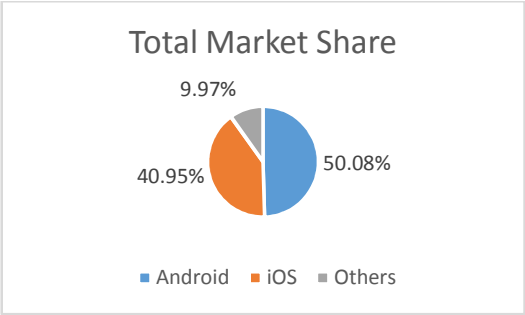


Fig.8. Mobile Tablet Operating System Market Share.

Any app development effort should first be targeted towards these platforms.

Table 2 looks at certain features that can be incorporated on the designed app and identifies if such features already exist in any form in the app market place or even embedded in the device OS.

TABLE 2: FEASIBLE FEATURES FOR APP DESIGNS.

Feature	Current Availability Status
OS Update Alert	Available on all platforms
Device Disability Function for delayed OS Update	Not Available (but certain corporate networks deny access to devices without updated software)
App Developer Location	Usually not specified
App list export function	Not available on any app
App Usage Tracker	Certain apps can
App permission (camera, gps etc)	Available at OS level
Tip provider and tutor function	Available on apps
Incident Reporting Features	Available on certain apps

There are certain applications on the app stores with ability to carryout certain of the functions named above but no one domesticated and with all the functionalities described.

There will also be the need to integrate the app with the CERRT platform deployed by NITDA or any body with such mandate. A number of the requirements specified for this application are already available on other computer platforms like laptops and desktops. The drive now is to have the same features available on handheld and smaller devices.

The major focus should be centered on apps that synchronise with online servers and provide personal information access across different platforms. A number of applications request access to address book and GPS location of activities of the user.

General Recommendations

A number of recommendations are given in this section. These recommendations can be implemented independent of the existence of the app described in the preceding section.

- *Operating System Level*

All devices should come with boot page caution information. Such information should be available in different languages. The idea is to create a sense of responsibility on mobile device users and also make them aware of their benefits in using such precautions. A screen flash of STOP, THINK, CONNECT is suggested. This can be displayed on screen shortly after device power on and at specified times of the day.

- Procedures for data breach compliance should be defined and incorporated in the machines.
- OS updates are extremely essential. All devices should be configured in such a way that 48 hours after an update is available, all other services are inhibited until the update is done on the mobile device to safe guard the user against threats. The major challenge is with data connection speeds and data costs. Such details can be worked out among service providers. Ultimately, if devices are shut off from mobile data environments these operators will still not make any revenue. Organisations have been able to carryout the precaution of disabling access by certain devices and apps to their networks effectively preventing any device without current patches and security updates to have access to their networks. Carrying this out on a large scale will involve the cooperation of the OS developers and app stores.

  The following quick activities are recommended in The Critical Security Controls (CSC) for Effective Cyber Defense Version 5.1 [20]

- Application whitelisting (found in CSC 2);
- Patch application software within 48 hours (found in CSC 4);

- Patch system software within 48 hours (found in CSC 4);
- App Level requirements

All applications should have the following information on their "About Page', VIZ:

i. App Version number and date
ii. Any applicable Certification Standard
iii. registered location of developer / firm
iv. Web link to Applicable data and Information security laws for the developer registered location.

- *Information Dissemination Platforms*

There is a great need to increase user awareness and compliance with essential controls. The first task is to establish the means of engaging the user. Users of mobile devices in developing countries such as Nigeria have little knowledge of all the essential precautions to take.

Mobile money, which is a product to incorporate user telephone lines into mainstream banking activity, runs almost completely on telephone platforms and as such, it is also possible to deploy training of users on the same platform that is used to solicit user participation and subscription to all sorts of products.

There should be well-defined guidelines on what constitutes cybercrime, security breach or security concern. This will aid in report gathering so that people do not make unnecessary reports. However, in the interim more reports are better than no activity reporting at all. Those tasked with monitoring the system can then sieve through.

Two entities have wide spread contact with the general Nigerian populace. These are the banks and the mobile phone companies. There are a lot of Nigerians with bank accounts. The telephone companies have so many subscribers on their network. An effective means of engaging the population will be by using these two agents. The banks are already at the fore front of providing information. Others should come on stream and the activities should be harmonised and integrated.

There is also need to increase the reach of the government agency set up to handle cybersecurity response CERRT. In the interim, CERRT should deploy incident-reporting apps that can be downloaded from the app stores of the different OS manufacturers. Considering that a lot of people in Nigeria do not have unlimited data subscriptions, it would be good to ensure that the incident reporting apps or apps utilized to aid cybersecurity operate like toll free emergency lines.

To aggressively pursue an awareness campaign, all mobile phone companies can be asked to provide slots of nationwide cell broadcast messages daily to CERRT to aid in nationwide awareness creation of cyber security activities of the agency and also enable the agency deliver information tips to aid the citizens be online safety conscious. This gesture will go a long way in helping the agency to engage the citizens and enlighten them on steps to take to be safe online. It can also be used to solicit their support in protecting critical information infrastructure.

VI. SUMMARY AND CONCLUSION

This paper has dealt with various issues resulting from cyber awareness and control survey. It was highlighted that in the cyberspace, with its associated activities, the following are visible, viz:

- Data
- Transactions
- Application Software (Apps)
- Operating systems (OS)
- Devices
- Connections
- Infrastructure

To improve user engagement and cooperation in cybersecurity, there is need to start by using what the user deals with often and then move towards what he may not notice often. This should be achieved without creating the impression that the user has become exposed to wild security agency surveillance systems that have little oversight control measures in place.The idea is to get the users' cooperation without getting users to be hysterical. The need for end user training, awareness, and education cannot be over emphasised but the ease of delivering same is the major challenge.

One interesting feature of commercial flights is the announcements. On board any flight is the pre-take off safety briefing. One may wonder if the safety briefing does have any real effect on the safety of the trip. However, with regards general transportation safety statistics, airlines have a good one. In 2013, the aviation accident rate was 0.24 out of 1 million departures. That means less than one accident for every 1 million flights [21]. The safety briefing on board planes is not given until the passenger has boarded the aircraft. In the same vein, the alerts on phishing, malware and other cyber controls should be deployed on the platform of usage, which is on the device.

Increased awareness of device activities can then be exploited to increase user awareness of cybersecurity measures. It is sad to admit, but it appears that if one wants to prevent people from reading any information, one good place to tuck it is in the End User License Agreement (EULA) of a software app. In summary, until mind reading apps become available, there are two ways for information to be kept ultimately safe. One way is to disclose the information to no one and have it only in one's mind; the other is to disclose the information to everyone (considering that there is real surprise effect in publicly available information). If one cannot do any of these. This work recommends using established information security standards and controls.

ACKNOWLEDGMENT

My thanks go to the numerous people who took out time to complete the survey associated with this paper, to kwik survey for providing the platform to administer the questionnaire and to the team involved in designing the app that should integrate the cybersecurity, safety and cyber control features described in this paper.

REFERENCES

[1] CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT, 2015

[2] "The **2014** Nigerian Cyber Threat Barometer Report", Wolfpack Information Risk. Johannesburg, South Africa. 2014, p.10

[3] NCC Nigeria. "*Subscriber Statistics,*"ncc.gov.ng. [Online]Available:http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:subscriber-statistics&catid=65:industry-information&Itemid=73. [Accessed 11 September 2015].

[4] About Get Cyber Safe. 2015. "*About Get Cyber Safe.*"[Online] Available: http://www.getcybersafe.gc.ca/cnt/bt/index-en.aspx. [Accessed 09 September 2015].

[5] FFIEC Cybersecurity Awareness. 2015. *FFIEC Cybersecurity Awareness*. [Online] Available: https://www.ffiec.gov/cybersecurity.htm. [Accessed 09 September 2015].

[6] National Cybersecurity Awareness Month. 2015 *National Cybersecurity Awareness Month. 2015* [Online]Available:http://www.dhs.gov/national-cyber-security-awareness-month [Accessed 09 September 2015].

[7] Cerrt.nG. 2015. *Cerrt.nG*. [Online] Available: http://cerrt.ng/. [Accessed 11 September 2015].

[8] STOP.THINK. CONNECT | CSEAN. 2015. *STOP.THINK. CONNECT | CSEAN*. [Online] Available: http://csean.org.ng/stop-think-connect/. [Accessed 11 September 2015].

[9] Critical Security Controls. 2015. *Critical Security Controls.*[Online] Available: http://www.cpni.gov.uk/advice/cyber/Critical-controls/. [Accessed 15 September 2015].

[10] Gartner, 2015. *Gartner Says Smartphone Sales Surpassed One Billion Units in 2014*. [Online]Available:http://www.gartner.com/newsroom/id/2996817. [Accessed 09 September 2015].

[11] Industry Overview. 2015. *Industry Overview*. [Online] Available: http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=68:industry-overview&catid=65:industry-information&Itemid=70. [Accessed 11 September 2015].

[12] E. Beehler,2015.*Top five mobile application vulnerabilities*. [Online] Available: http://searchmobilecomputing.techtarget.com/tip/Top-five-mobile-application-vulnerabilities. [Accessed 09 September 2015].

[13] Wikipedia. "*CVSS",*Wikipedia.org.[Online] Available: https://en.wikipedia.org/wiki/CVSS. [Accessed 13 September 2015].

[14] *SafetyTips for Your Mobile Devices,* 2015. p.1

[15] Phishing | Privacy and Information Security. 2015. *Phishing | Privacy and Information Security*. [Online] Available: https://security.illinois.edu/content/phishing. [Accessed 15 September 2015].

[16] Wikipedia. "*Malware",* Wikipedia.org.[Online]Available: https://en.wikipedia.org/wiki/Malware. [Accessed 13 September 2015].

[17] What is patch? 2015. *What is patch?*.[Online] Available at: http://www.computerhope.com/jargon/p/patch.htm. [Accessed 15 September 2015].

[18] *Nigeria Financial Services IT Standards Blueprint*, Central Bank of Nigeria, Abuja, FCT, May 2013, p. 63

[19] Operatingsystem market share. 2015. *Operating system market share*. [Online]Available:https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1&qpsp=2015&qpnp=1&qptimeframe=Y. [Accessed 09 September 2015].

[20] *The Critical Security Controls for Effective Cyber Defense Version 5.1*, Council on CyberSecurity, Arlington, VA, July 2014, p. 6

[21] Casey Tolan, Thom Patterson and Alicia Johnson(2014, July)*"Is2014 the deadliest year for flights? Not even close"*. CNN [Online]Available:http://edition.cnn.com/interactive/2014/07/travel/aviation-data/[Accessed 29 September 2015].

Modeling of RF Security System Using Smart Antennas

Ayodele S. Oluwole and Viranjay M. Srivastava
Department of Electronic Engineering,
Howard College, University of KwaZulu-Natal,
Durban-4041, South Africa.
asoluwole@gmail.com; viranjay@ieee.org

***Abstract*— This research work established a state of the art protective measure on how smart antennas can be used effectively to curtail the activities of hackers/intruders on radio frequency signals to scan confidential information/data belonging to organization, law enforcement, and even interception of radio frequencies signals to the public usage. In this paper, we use the two antenna elements array (i) The antenna elements that was used for the transmission / reception (transceiver) of radio frequency signal, transceiver for remotely transmitting information signal virtual to mobile station, (ii) The two antenna elements at the mobile station is being used as descrambler against any illegitimate activities. Some of the imperative securities challenges have been covered in this work are secrecy, authentication, privacy, and attacks. The IEEE standard 802.11 for wireless local area networks was maintained in the choice of frequency bandwidth for the transmission of signal.**

Keywords*— Antenna arrays; Internet of things; Network security; Radio frequency; Signals; Smart Antennas.

I. INTRODUCTION

Wireless networks transmit their data at any layer of the OSI protocol stack using radio frequency (RF) or optical wavelengths. Wireless local area networks (WLAN) has the complete transmission of data / signals through air as communications is wireless ubiquitously. Signal transmission through air offers opportunities for interlopers and hackers that come from any direction.

Attacks on radio frequency have become one of the major targets of hackers/intruders in wireless communications networks [1],[2]. A modern laptop / computer can listen to radio frequency in order to extract unlawful information to perpetrate their acts. Worse, attackers/hackers can invent innovative packets in the course of data transmission and influence wireless stations to accept their packets as legitimate. The IEEE 802.11 specifies hacking methods that attackers had used, this calls for and recommends various protective procedures in order to prevent hackers from having access to unlicensed information. It is not an indication of security structures suggested in IEEE 802.ll and does not reflect legal consequences or the intent behind such hacking, whether vindictive or humane [2],[3].

As antenna technology progresses, researchers had demonstrated that antenna can remotely steal data from devices using sound waves [3]. Smart antenna is a combination of multiple antenna arrays with a combination of spatial signal processing algorithms used to analyze the spatial signal parameters like direction of arrival (DOA) of signal, and use it to estimate beamforming vectors track and spot antenna beam on the target/signal.

A team of security researchers has developed a new hacking method called *Funtenna* that uses sound and radio waves to tap data from computers even without internet access [4]. According to *Angcui et.al* [5], the *Funtenna* radio signal hack has the prospective to crack internet linked devices (printer, washing machine and air conditioner) universally known as the *Internet of Things* into bugs that has the ability to transmit data out of a network with the aid of sound waves that cannot be perceived by a human ear. The hacker simply needs to install malware on a target's device such as a printer, office phone, or a computer. The malware overhauls the control of the electronic circuit of the device (general-purpose input/output circuits) and vibrates them at a frequency (which transmits radio signal) of the hacker's preference. A hacker then pick up these signals using an AM radio antenna popularly called Funtenna from a short distance away [4, 5]. The presence of network detection, firewalls, around our premises does not deter hackers from accessing unlicensed information because but this transmits data in a way that none of those things are being monitored. This primarily challenges how certain we can be of our network security said *Cui* [5]. Here, the hacked devices are themselves acting as transmitters. Therefore, the new Funtenna technique bypasses all conventional network security methodologies. *Hole et.al.* [6] has presented a process to hack machines and steal data, called the *Air Hopper* method using a smart phone capable of receiving FM signals.

The HackRF one provides an assessment equipment module for RF related experiments and measurements which covers a frequency range from 1 to 6,000 MHz. The system covers a wide frequency range from 1 to 6000 MHz, and covers many licensed and unlicensed as well as ham radio bands. Experiment/research needs new protective measures that totally reduce the adopted means of hacking [7].

A foremost problem to secure communication systems is the probability of unlicensed penetration. The unlicensed penetration of this kind is popularly known as hacking. Numerous techniques have been employed to overcome the problem of hacking. Firmly speaking, is commonly refers to a

person/software that breaks into or interrupts computer systems or networks to maneuver data or generate havoc by uploading malicious code. The Internet is the perfect medium for distributing wireless hacking software [8]. Encryption of transmitted data and authentication of communicators are some of the methods employed to make hacking more difficult.

This work introduces an analysis about how a radio frequency (RF) can be secured using smart antenna arrays. To receive radio signals an antenna must be used. However, since the antenna will pick up thousands of radio signals at a time, a radio tuner is necessary to tune into a particular frequency [9, 10].

The organization of the paper is as follows. In the section II we have described the smart antenna as transceiver that simultaneously performs transmission / reception of a signal. In the section III, we have provided the design of the antenna that prevents hackers from having access to licensed data / information. The section IV presents the analysis of the designed antenna. Finally, the section V concludes the work and recommends the future works.

II. SMART ANTENNA AS A TRANSCEIVER

Antenna arrays may be used in any wireless communication receiver or transmitter (or transceiver) at communication station that transmits or receives radio frequency signals using a single or multiple antennas [11]. The use of antenna arrays in such a communication station provides the performance improvements over the use of a single antenna element. These antenna improvements include directionality, signal to noise ratio, interference rejection for received signals, security, and reduced transmit power requirements for transmitted signals [12]. Antenna arrays may be used for signal reception, transmission or both.

The function of a transmitting antenna is to radiate the radio-frequency energy that is generated in the transmitter and guided to the antenna by the transmission line. In this capacity the antenna acts as an impedance matching of the device to match the impedance of the transmission line to that of free space [13]. In addition, the transmitting antenna should direct the most energy in desired directions and suppress the radiation in other directions where it is not wanted.

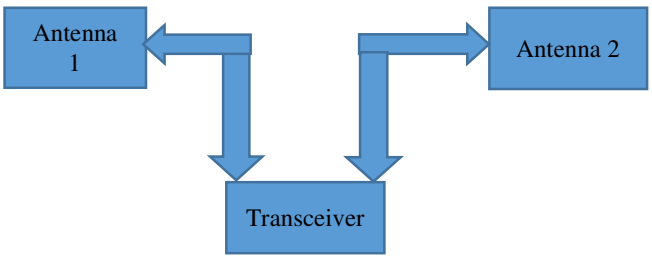


Fig. 1. Proposed RF smart antenna security.

The transceiver includes an array of transmit antenna elements. The array of this transmits antenna elements and the two other antennas connected to the main transceiver is used for the mode of the operation of this research work. Here in this research work, smart antenna is used for security purpose against any hackers on the RF transmission signals. The wireless transceiver antenna arrays is used for remotely transmitting information signal virtual to mobile station, while the two antennas at the mobile station is being used as descrambler against any criminal activities. The block diagram of the proposed smart antenna security is shown in Fig. 1.

Transceiver uses antenna array for communicating in a cellular communication system with a polarity of mobile stations. Therefore, the antenna array of the transceiver is used in this research work to design and communicate with antennas at the mobile stations. When there is an attack on the RF there will be transceiver for remotely transmitting alarm information relative to mobile station.

III. PROPOSED RF SECURITY ANTENNA DESIGN

Smart antenna is a combination of multiple antenna arrays with a combination of spatial signal processing algorithms used to analyze the spatial signal parameters like direction of arrival of signal, and use it to estimate beamforming vectors track and spot antenna beam on the target [14]. Antennas affect both Receive and Transmit range of radio frequency; frequently the easiest solution to a range problem is selection of the proper antenna and its location. Antennas design are preferred based on the following features: frequency of operation, gain, directionality pattern, impedance commonly referred to as voltage standing wave ratio, propagation path impairments, free space path loss, Fresnel zone clearance, constructional material attenuation, etc.

Most radio transceiver systems will have somewhat similar architectures and share common features and problems. All will require some form of: Antennas, RF Transmit Amplifiers and RF Receive Amplifiers, RF\Baseband Transmit Filters and RF\Baseband Receive Filters, Transmitter Modulation and Receiver Demodulation circuits and\or Digital Signal Processing (DSP), descrambler, Frequency synthesizers and clock generators (Often shared by both Receive and Transmit circuits), and DC Power Supplies. All these are coupled together in Fig. 2.

The hacking prevention system works through a descrambler in the RF board level in Fig. 1. This is an electronic device that decodes a scrambled transmission, typically a radio signal, into a signal that is intelligible to the receiving apparatus. This will make the radio or telephonic message incomprehensible to interceptors by systematically changing the transmission frequencies. A random number is generated in the descrambler. Using this random number, a key is calculated, which corresponds to the authorization packet corresponding to the generated random number [15]. This generated key and the offset value, which corresponds to the generated random number, are used to calculate the descrambling key.

The two antenna elements shown in Fig. 2 perform the function of sensor networks between the transceiver and the outside world. Whenever there is an attack on the RF, an alarm switch included in the transceiver will indicate the presence of intruder/hacker on the system.

The transceiver includes an array of transmit antenna elements. The method uses the remote transceiver for

receiving signals when the main transceiver transmits downlink calibration signals. When the main transceiver also has a receive antenna array, the remote transceiver can transmit uplink calibration signals to the main transceiver for determining an uplink signature/identity. The downlink and uplink signatures/identities are used to determine a calibration function to account for intruders/hackers in the chains that include the antenna elements of the arrays, and that enable downlink smart antenna processing identities to be determined from uplink smart antenna processing identities when the main transceiver includes means for smart antenna processing according to identities [16].

Smart antennas combines the antenna arrays elements of the transceiver and that of the antennas at the mobile station for the optimization of radiation beam pattern, with smart signal processing algorithms used to identify spatial signal signature/identity to track and identify whenever hacker wants to intrude on the transmitted signal. The antennas at the mobile stations communicate with each other using RFs between 1 and 7 GHz. Neighboring channels are can only receive signal at frequency below 1 GHz due to insecurity. If the neighboring channels receive signal at the specified/designed frequency and hacking is ON, there will be no alarm in the system.

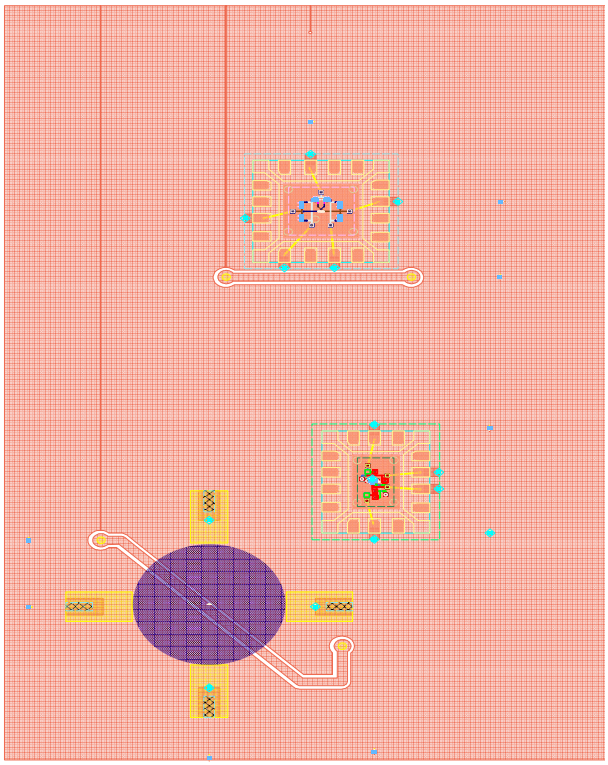


Fig. 2. RF board level smart antenna Transceiver system layout.

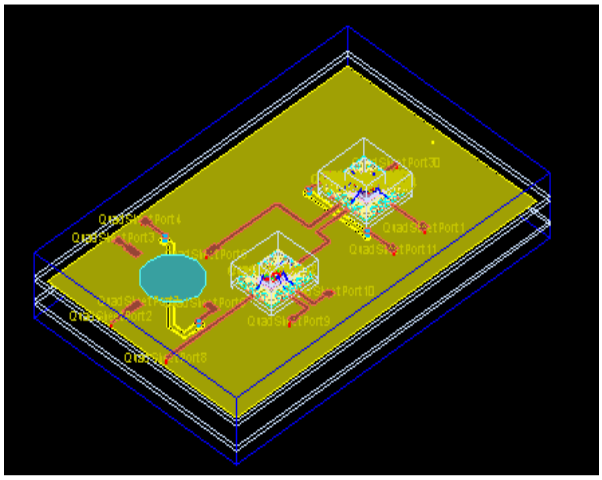


Fig. 3. Isometric 3 D EM Preview of the designed Antenna.

Hence hackers can steal data/information on the transmitted signal. At frequencies outside the working frequency, tracks and antenna elements do not behave as ideal elements. Fig. 2 shows the RF layout system for the paper work. The electronic antenna switch in the transceiver that connects the antenna to the transmitter or receiver based on the logic state of one or two control levels. This switch was used to switch on alarm system in the case of hackers/intruders. Immediately the alarm is on, the transmitting signal will be blocked. This is similar to the case of loading a credit card on the telephone or DSTV system. Whenever a wrong code is being sent twice, that line will be blocked. This will prevent theft/hacking on the system.

Fig. 3 shows the 3D EM preview of the designed shown in Fig. 2 before simulating using the EMDS simulator. This validated that the three dimensional design has been properly constructed.

IV. Analysis of Results and Discussions

Fig. 4 shows the simulated results for the designed antenna at a frequency range from 1 to 7 GHz. It has been shown in the graph that PAON (PA to antenna) is ON at an operating frequency of 5.07 GHz in the absence of no hacking, while the LNA OFF of the transceiver will be off whenever hackers want to hack any unlicensed information. The s-parameter was measured to check the stability of the transmitted signal/data. Due to its relative gain, since smart antenna is directional; there is no reflecting elements. This also made it possible for hackers to get access to information, since there is loss in the course transmitting signal/data.

Fig. 5 shows the simulated s-parameter data of the antenna network switches. For a radio transceiver to deliver power to the antennas at the mobile station, radio's impedance and transmission line must be well matched to the antenna's impedance. The transceiver gains frequency occurs at 5.1 GHz and 5.7 GHz.

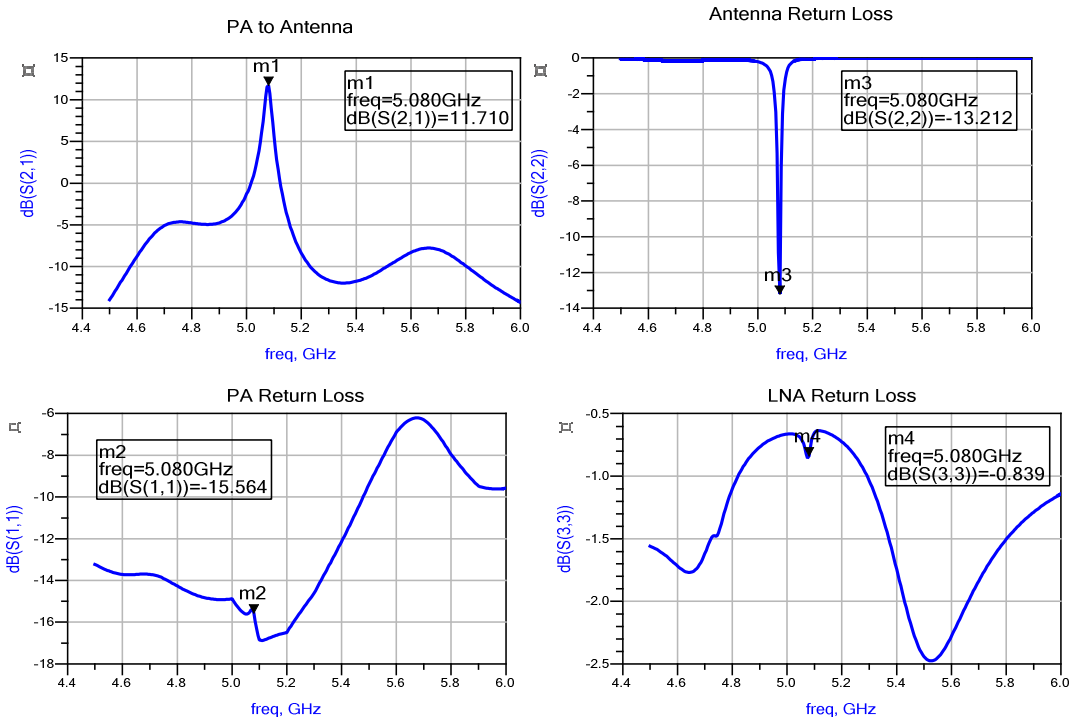


Fig. 4. Graph of RF transceiver antenna.

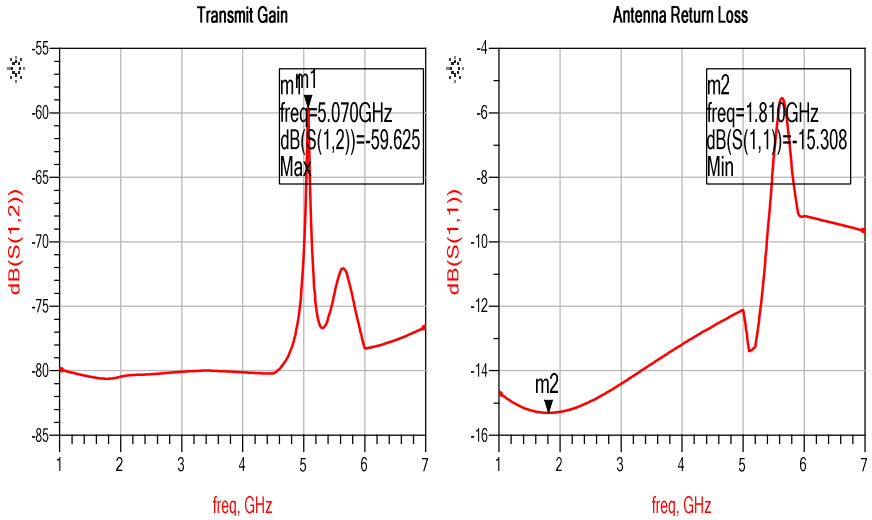


Fig. 5. Simulated S-Parameter data of the Network Switches.

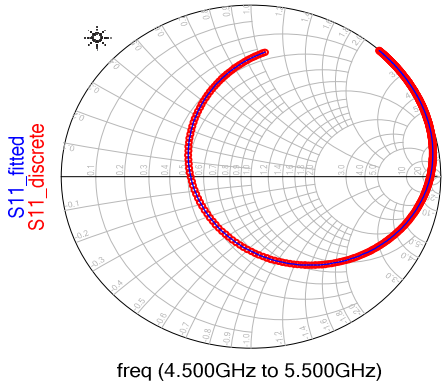


Fig. 6. Simulated Smith chart of the Network switches.

The simulated matching task was necessary in Fig. 6 for the ideal set of synthesizable impedances represented on the switches at frequency from 4.5 GHz to 5.5 GHz.

V. CONCLUSIONS AND FUTURE RECOMMENDATIONS

This paper work has demonstrated the effectiveness of smart antenna in a new dimension for security against attacks on RF. Many other problems also need further research. One is how to secure wireless communication links against eavesdropping, tampering, traffic analysis, and denial of service. There are a number of well-established RFID security and privacy threats. RFID, tracking, sniffing, spoofing, replay attacks. To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack. Consequently, security must pervade every aspect of system design [17-19].

REFERENCES

[5] H. Bidgol, "Hanbok of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management," *John Wiley and Sons Inc.*, vol. 3, 2006, pp. 210-222.

[6] S. Capkun and J. P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, Feb. 2006, pp. 221-232.

[7] D. R. Banbury, N. Fayyaz, S. S. Naeini, and Niknesham, "A CMOS 5.5/2.4 GHz dual-band smart-antenna transceiver with novel RF dual-band phase shifter for WLAN 802.11 a/b/g," *2004 IEEE Digest of Papers on Radio Frequency Integrated Circuits (RFIC) Symposium*, Forth Worth, TX, 6-8 June 2004, pp. 157-160.

[8] T. Chomsiri, "HTTPS hacking protection," *21st IEEE International Conference on Advanced Information Networking and Applications Workshops*, Niagara Falls, Ont., 21-23 May 2007, pp. 590-594.

[9] S. Capkun and J. P. Hubaux, "Secure positioning in wireless networks," *IEEE on Selected Areas in Communications,* vol. 24, issue 2, Feb. 2006, pp. 221-232.

[10] K. j. Hole, E. Dyrnes and P. Thorsheim, " Securing Wi-Fi networks," *IEEE Journals and Magazines*, vol. 38, no 7, Jul. 2005, pp. 28-34.

[11] K. Meena and A. P. Kabilan, "Modeling and simulation of microstrip patch array for smart antennas," *International Journal of Engineering*, vol. 3, issue 6, 2010, pp. 662-670.

[12] K. Kosher, and et al, "Experimental security analysis of a modern automobile," In *Proc. of the 31st IEEE Sysmposium on Security and Privacy,* Oakland, CA, USA, 16-19 May 2010, pp. 447-462.

[13] G. P. Hancke and M. G. Kuhn, "An RFID distance bounding protocol," In *SecureComm '05': Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, Wshighnton, DC, USA, 05-09 Sept. 2005, pp. 67-73.

[14] S. Slijepcevic, M. Potkonja, V. Tsiatsis, S. Zimbeck, and M. B. Srivastava, "On communication security in wireless Ad-Hoc sensor networks," *Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, Pittsburgh, PA, USA, IEEE Computer Society, 12 Jun. 2002, pp. 139-144.

[15] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad-hoc networks: challenges and solutions," *IEEE Journals and Magazines*, vol. 11, no. 1, Feb. 2004, pp. 38-47.

[16] M. R. Rieback, P. N. D. Simpson, B. Crispo, and A. S. Tanenbaum, "RFID malware: design principles and examples," *(ELSEVIER) Pervasive and mobile computing*, vol. 2, Oct. 2006, pp. 405-426.

[17] S. Ortiz, "How secure is RFID," *IEEE Journals and Magazines* vol. 39, issue 7, Jul. 2006, pp. 17-19.

[18] M. R. Rieback, B. Crispo and A. S. Tanenbaum, "Is your cat infected with a computer virus," *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, PISA, 13-17 Mar. 2006, pp. 170-179.

[19] X. Li and J. Hwu, "Using antenna array redundancy and channel diversity for secure wireless transmission," *Journal of Communications*, vol. 2, no. 3, May 2007, pp. 24-32.

[20] D. Welch and S. Lathrop, "Wireless security threat taxonomy," *IEEE Workshop on Information Assurance*, United States Military Academy, West Point, NY, 18-20 Jun. 2003, pp. 76-83.

[21] T. Tsegaye and S. Flowerday, "Controls for protecting critical information infrastructure from cyberattacks," *2014 IEEE World Congress on Internet Security*, London, 8-10 Dec. 2014, pp. 24-29.

[22] T. Chomsiri, "Sniffing packets on LAN without ARP spoofing," *Third IEEE International Conference on Convergence and Hybrid Information Technology*, Busan 11-13 Nov. 2008, pp. 472-477.

[23] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, Jun. 2004, pp. 53-57.

Security Challenges to Telecommunication Networks: An Overview of Threats and Preventive Strategies

Agubor C. K., Chukwudebe G. A. and Nosiri, O. C.
Department of Electrical and Electronic Engineering
Federal University of Technology
Owerri, Nigeria.
aguborcosy@yahoo.com

Abstract **-- Security challenges to telecommunication networks have been a matter of concern to the international community within the last two decades. Telecommunications infrastructure that provides the necessary backbone for information exchange such as voice, video, data, and internet connectivity have been found to be particularly vulnerable to various forms of attacks. Some of these attacks could lead to denial of service, loss of integrity and confidentiality of network services. Protecting these networks from attacks is thus an important aspect that cannot be ignored. This paper highlights some of the important security challenges to current telecommunication networks and recommends countermeasures that can be implemented to mitigate not only infrastructural insecurity but also the risk from cyber-attacks. One of which is security by default that aims at designing systems that can repair themselves when breaches are detected.**

Index Terms— cybersecurity, cyberattack, hacking, telecommunication infrastructure, cybercrime.

I. INTRODUCTION

Telecommunication network worldwide is a mix of Public Switched Telephone Network (PSTN) technology and mobile wireless network technology. The infrastructure of the former comprises of switches, telephone cables, optic fibre cables (surface and submarine), microwave transmission and communication satellite links. The PSTNis driven by circuit-switched technology primarily developed for voice signals. The inability to handle the demand for video and data services became the major limitation of this technology despite the introduction of such technologies like integrated service digital network (ISDN), digital subscriber line (DSL) and Dial-up(for internet services).

The advent of wireless mobile technologies which is a packet-based switching technology presented the type of network suitable for the transportation of all information and services such as voice, data and videos. The wireless mobile evolved from 2G for voice and SMS services to 3G systems with General Packet for Radio Service(GPRS), Enhance Data for Global Evolution (EDGE) and High Speed Packet Access(HSPA) designed for larger volume of data transmission and now to 4G. The 3G and 4G networks are based on the Internet Protocol (IP) and are expected to reshape the current structure of the telecommunication system[1].

Telecommunication networks are a combination of several technologies – PSTN, 2G, 3G and 4G with vital network components as access network, core network, Application and Management Network, Internal and External Network [2]. The interconnection interface of both fixed and wireless networks exposes the entire network to intruders and increases the potential for attacks caused by virus, worms and malicious software. Such attacks may be from either external or internal sources and may be targeted at any part of the telecommunication network, including the radio path of the access and core networks.

Attacks on one telecom operator's network could also spread to multiple networks over the interconnection interfaces [2].This highlights the possibility of intruders gaining access to their targets irrespective of the location of the remote terminal. In view of the increasing rate of attacks and the impact on the economy whenever it occurs, a review of the prevalent attacks and recommended mitigations for developing countries are presented in this paper.

II. CLASSIFICATION OF ATTACKS

All Threats connected with telecommunications assets and networks may be associated with the actions of various attackers and their intent. Attacks may be due to some players attempting to generate illegal profits. Attacks or threats on telecoms infrastructure can be classified as shown in Fig. 1.

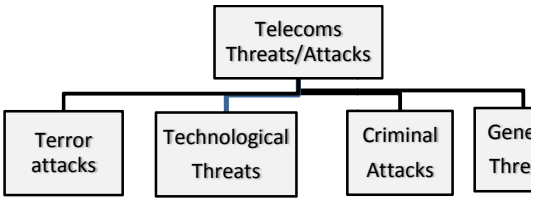


Fig. 1:Classification of threats/attacks on Telecoms assets.

A. *Terror Attacks*

One form of attack may be as a result of either civil or military conflict. Certain conflicts lead to the physical destruction of telecommunication installations assets by terrorists as a deliberate military strategy. This is true in regions that have or are still experiencing one form of military conflicts or the other. In [3], Nigeria, India, Iraq, Syria, Nepal and Columbia were mentioned as countries that have experienced telecoms infrastructural destruction due to insurgence or military conflicts. For example, in 2012 alone, Boko Haram in Nigeria destroyed or damaged some 530 base stations and killed staff, causing an estimated $132.5 million in damage—capital that could have been used to further develop networks in Africa's largest economy.

At least 300 telecom towers were targeted by the Taliban in Afghanistan between 2001 and 2013. In both cases, the decision to target infrastructure is probably based on the extent to which terrorists perceive the telecoms operators as undermining their security through call tracing. In Ranchi, India, a spate of Maoist attacks on telecom towers in recent years have forced mobile service providers to avoid setting up new ones in remote areas, plunging most parts of Bihar State and neighbouring areas into a 'zero-network.

In Iraq and Syria, telecoms towers and their guards have been regularly targeted by insurgents. During the ten-year civil war in Nepal (1999-2009) hundreds of towers were attacked by Maoists. In Colombia, FARC rebels have an extended history of destroying towers with explosives. It seems that certain conflicts lead to the physical destruction of telecoms assets as a deliberate strategy, often associated with their potential role in assisting states in tracking terrorist planning and movement[3].

B. ***Technological Threats***

Some telecommunication threats can be seen as technological threats. This involves threats ensuing from the technologies themselves and are mainly associated with the corporate clientele of telecommunications companies which can lead to large losses. An example is **a long non-disconnected call [4].**This threat is associated with private branch exchanges used by various companies and organizations. In some cases what can happen is that a subjectively terminated call is not disconnected by the private branch exchange properly, or is held without the participant's knowledge. Such a call may actually remain "connected" for a number of days. And in the event of an international call this could result in a major loss.

C. ***Criminal Threats***

This involves the use of various technological means for malicious intent. It has to do with threats associated with the activities of players to carryout traditional frauds by various manipulative means. These threats present a risk for telecommunications companies as well as for their customers. Criminal threats can be classified as shown in Fig. 2.

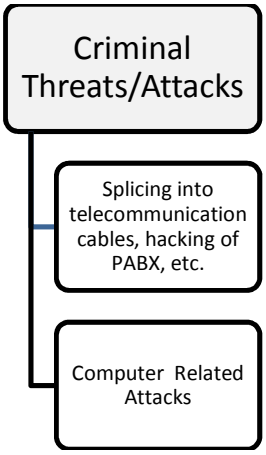


Fig. 2: Classification of criminal attacks.

Splicing into telecommunication cabling is an act of gaining access to telecommunication cabling for the purpose of making illegal connections. This is a problem encountered in regions where PSTN with fixed line network are still in use. Fixed line network contains hundreds of kilometers of copper cabling linking the telephone exchanges with the end users. Along this route is a number of telephone switchboards. It would be extremely costly and almost physically impossible to reliably secure these cables against third-party interference.

Due to its vulnerability to abuse, criminals mechanically splice into the cabling and are then able to make calls free of charge. Public telephones are becoming a frequent target of these attacks, in which case the telecommunications operator itself is at risk. In most cases, splicing into cabling can be with an intent to commit a more sophisticated criminal activity.

Hacking of private branch exchanges is a dangerous form of criminality. Modern branch

exchanges may be perceived as special communication equipment with a large number of functions. This equipment requires specially trained service personnel for its administration and allow for remote administrator access over the telephone network. This access for administrative purposes over the telephone is a stumbling block [4].

There are illegal operators who scan telephone number ranges and look for such access. After locating the access these operators then try to hack into this access, which is made easier by the fact that many administrators retain the original password pre-set by the supplier or use an inadequate password.Many branch exchanges can and do have administrator access via a data network. Then the act of taking control of such a branch exchange is a case of traditional computer hacking.

In computer-related attacks the telecoms infrastructure network be it fixed line or wireless network provides the platform for the perpetration of this form of attack or crime via computer links. These type of attacks are alternatively referred to as computer crime**,** cyber crime, e-crime, electronic crime, or hi-tech crime [4].

Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker; a hacker illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may have malicious intention to destroy or otherwise corrupt the computer or data files [5]. Examples of computer crimes are

- Child pornography or Exploitation - Making or distributing child pornography.
- Cyber terrorism – Hacking or Computer intrusion, threats, and blackmailing towards a business or person.
- cyberbully or cyberstalking - Harassing others online.
- Creating Malware - Writing, creating, or distributing malware (e.g. viruses and spyware)
- denial of service attack - Overloading a system with so many requests so that it cannot serve normal requests.
- Espionage - Spying on a person or business.
- Fraud - Manipulating data, e.g. changing banking records to transfer money to an account.
- Harvesting - Collecting accounts or other account related information ofother people.
- Identity theft - Pretending to be someone you are not.
- Intellectual property theft - Stealing another person's or companies intellectual property.
- Phishing- Deceiving individuals to gain private or personal information about that person.
- Salami slicing - Stealing tiny amounts of money from each transaction.
- Spamming - Distributed unsolicited e-mail to dozens or hundreds of different addresses.
- Spoofing - Deceiving a system into thinking you are someone you really are not.
- Unauthorized access - Gaining access to systems you have no permission to access.
- Wiretapping - Connecting a device to a phone line to listen to conversations.

D. General Threats/Attacks

These type of threats or attacks involve players like special government agencies. It is a form of hacktivism with nation-state sponsorship [6]. In [7] three different cases were used to illustrate the nature of such attacks:

Case No 1: Government agencies are increasingly attacking telecom operators' infrastructure and applications to establish covert surveillance. These sophisticated actors typically use very Advanced Persistent Threats (APT) that can operate undetected for long periods of time. Communication channels targeted for covert surveillance include everything from phone lines and online chat to mobile phone data. There have even been cases where one nation's cyber-attack prevented another nation's leaders from communicating on their mobile devices.

Case No 2: Given that telecom companies control critical infrastructure, any shutdown has great impact on the economy. For example, during severe petroleum product crisis in Nigeria mid-2015, the telecom companies were affected because they run on diesel generators, consequently, banks and various organizations could not sustain their regular services.

Case No 3: Customer data is another popular high impact target. Telecom organizations typically store personal information -- such as names, addresses and financial data – about all of their customers. This sensitive data is a compelling target for cyber-criminals or insiders looking to blackmail customers, conduct identity theft, steal money or launch further attacks.

Information can be lost in a variety of ways that may be as simple as a stolen laptop. Of course, laptops can be lost or stolen in any sector; however, the problem tends to be worse in telecom because

employees in this sector often serve customers as part of a call center or help desk function and may have large amounts of sensitive customer data stored on their laptops.

One critical threat unique to the telecommunications sector is the attack of leased infrastructure equipment, such as home routers from Internet Service Providers (ISPs). Once the equipment has been compromised, hackers can use it to steal data, launch other attacks anonymously, store infiltrated data, or access expensive services such as international phone calls. To avoid upsetting customers, telecom companies generally refund any charges associated with such attacks, often resulting in significant lost revenue.

These attacks lead to various forms of losses to the victims. Such attacks or threats and their likely outcomes are tabulated in Table 1.

Table 1: Threats and Likely Outcome [2].

Threat	Outcome
Unauthorised physical access to switching infrastructure, underground and local loop cable infrastructure and other critical telecom network equipment, for example, AuC, HLR and VLR.	Tampering, destruction or theft of information &equipment, illegal tapping and interception of the network traffic.
Interception of voice traffic or signalling system inPSTN networks due to absence of encryption for speech channels and inadequate authentication, integrity & confidentiality for the messages transmitted over the signalling system (which is based on the ITU-T SS7 specification.	Unauthorized access to telecom network traffic.
Use of modified mobile stations to exploit weaknesses in the authentication of messages received over the radio interface.	Spoofing of user de-registration and location update requests, leading to unreliable service/disruption.
Use of modified base stations to entice users to attach to it.	Denial of service, interception of traffic.
Misuse of the lawful interception mechanism.	Illegal tapping/interception of telecom network traffic
Compromise of the AuC or SIM used for storing the shared secret for the challenge-response mechanism.	Identity theft (intruders masquerading as legitimate users).
Deployment of malicious applications on devices with always-on capabilities like smart phones and Tablets.	Use of these compromised devices target the operator's network (for example, by setting up botnets to carry out DDoS attacks).
Intrusions into the operations networks.	Unauthorised changes to the users' service profiles, billing and routing systems, resulting in toll fraud and unreliable service.
Compromises of network databases containing customer information.	Unauthorised access to personal and confidential data.
Masquerading as authorised users, by gaining access to their credentials by means of malware, hacking tools, social engineering tools or other means.	Unauthorised access to the network systems, which can then be used to launch other attacks.

III. RECOMMENDATIONS

A. Telecommunications Network Security

The necessary technology must be put in place to safeguard critical telecoms infrastructure and assets. In regions where terrorist attacks are common, telecom outdoor infrastructure like towers, radio equipment and power generating sets should be sited on safer government-owned land to avoid physical destruction of telecoms assets by insurgents. It may also be necessary to have mutual agreement between government security agencies and network providers on modalities for providing security to key telecom installations.

B. Operations Security (OPSEC)

OPSEC is concerned with refining operational procedures and workflows to increase the security properties of an organization. Spam filtering and website blocking should be in place. For example a utility may restrict what employees post on their Facebook pages about the organization's procedures.

C. Security by default

A systematic method of preventing or fighting attacks should be in place and staff frequently trained and tested for compliance. Appropriate computer resources should be used to enforce security in a systematic way before they occur. This focuses on three themes [8]:

- Prevention or designing systems that are harder to hack.
- resilience, or designing systems that can offer secure transactions even after they have been compromised and
- regeneration or designing systems that can repair themselves when breaches are detected.

D. Criminalization of Cybercrime

In relation to cybercrime, the Cybercrime Convention of the Council of Europe called for eight offenses to be criminalized [9]:

- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Computer-related forgery
- Computer-related fraud
- Offenses related to child pornography,
- Offenses related to infringement of copyright and related rights.

Legislation should be given for all these offences where there are none so as to deter prospective criminals.

D. Restriction to sensitive areas.

Telecommunications spaces, pathways and equipment rooms should be treated as restricted zones. Access to these areas should be controlled and limited to authorized and properly security-cleared personnel only. Using appropriate methods, such as installation of electronic access controls, mechanical combination locksets or deadbolts, should be used to control access [10]. A list of persons authorized to access these sensitive areas or spaces should be maintained. The organization should also maintain a control log for security audit purposes.

E. Security infrastructure implementation

All policies and processes adopted by an organization should be supported by a security infrastructure that includes multiple security layers as in "Defense-in-Depth" approach [2]. This strategy ensures that the compromise of one security layer alone does not expose the network to attacks. Some of the security measures that can be deployed across the various layers are:

- Interference and tamper-proof cabling infrastructure
- Security guards and CCTV monitoring for operator premise perimeters
- Physical access control mechanisms like smartcard and biometricreaders
- Firewalls at the network perimeter for publicly accessible systems
- Host and network-based Intrusion Detection/Protection Systems (IDPS).
- Security Information and Event Management (SIEM) systems to handle security events and logs generated by multiple systems.
- Malware management by deployment of antivirus, antispyware technologies on internal systems and mail servers.
- Secure application development practices
- Security testing of the telecom equipment, perimeters, critical network components and applications
- Encryption and data masking techniques for both data at rest and transit
- Security awareness

IV. CONCLUSION

Telecommunications infrastructure is a big target for cyber-attacks. This is because they build, control and operate critical networks that are widely used to communicate and store large amounts of sensitive data. These networks which include fixed and mobile phone networks provide the traditional access for computer related crimes or cybercrimes e.g. phishing, hacking, spoofing, etc, to be perpetuated.

The attacks may cause damage such as sensitive information being leaked and security documents exposed which may put both individuals and the affected organizations

at risk. The paper has suggested some preventive measures that can be implemented as a way of fighting or preventing cybercrime.

REFERENCES

[1] Convergence and Next Generation Networks, Ministerial Background Report (OECD), 2007.

[2] Tata Consultancy Services Limited, 2012. Available from World Wide Web: http://www.tcs.com). Accessed 11th August, 2015.

[3] Williswire 2015, Available from World Wide Web:http:/www.willis.com/2014/10/threats-to-telecommunications-operators. Accessed 11th August, 2015.

[4] Available from World Wide Web: www.securtyrevue.com. Accessed 5th August,2015.

[5] Computer crime – Available from World Wide Web: www.computerhope.com. Accessed 10th August, 2015.

[6] Cyber in sight, Available from World Wide Web: www.surfacewatchlabs.com. Accessed 5th August, 2015.

[7] Telecoms Cyber intelligence centrehttp, Available from World Wide Web: www.cyberintelligencecentre.com/news/global-cyber-executive-briefing/telco.aspx. Accessed 5th August, 2015.

[8] Howard Shrobe, Available from World Wide Web: www.Cybersecurity@CSAIL). Accessed 5th August 2015.

[9] Buheita Fujiwara, Cyber Security "Threats and Countermeasures" Available from World Wide Web: http://www.gbd-e.org/ig/cs[Accessed 28th August, 2015].

[10] Security Implications of the Integrated Telecommunications Infrastructure, Available from World Wide Web: http://www.tpsgc-pwgsc.gc.ca Accessed 28th August, 2015.

A Particle Swarm Optimization Based Edge Detection Algorithm for Noisy Coloured Images in Multimedia Systems

Sadiq, B.O, Abubakar, A.S, Obi. E. Ochia, O.E
Department of Electrical and Computer Engineering
Ahmadu Bello University, Zaria
Kaduna State, Nigeria
bosadiq@abu.edu.ng, abubakaras@abu.edu.ng

***Abstract* - This paper presents an improved edge detection algorithm using particle swarm optimization (PSO) based on vector order statistics. The proposed algorithm was implemented using MATLAB 2013 script. The algorithm addressed the performance of edge detection in noisy coloured images, with a view to minimizing broken, false and thick edges whilst reducing the presence of noise. A collection scheme based on step and ramp edges was applied to the edge detection algorithm, which explores a larger area in the images in order to reduce false and broken edges. The efficiency of this algorithm was tested on two Berkeley benchmark images in noisy environments with a view to comparing results both visually and quantitatively with those obtained using proven edge detection algorithms such as the Sobel, Prewitt, Roberts, Laplacian and Canny edge detection algorithms. The Pratt Figure of Merit (PFOM) was used as a quantitative comparison between the proposed algorithm and the proven edge detection algorithms. The PFOM on the test images in noisy environment for the Sobel, Prewitt, Roberts, Laplacian, Canny and the proposed edge detection algorithms are 0.4191, 0.4191, 0.2807, 0.2811, 0.5606 and 0.8458 respectively. This showed that the developed algorithm will perform better than the existing edge detection algorithm in multimedia systems.**

Keywords - PSO, PFOM, Noisy coloured Images and Vector Order Statistics

I. INTRODUCTION

Detection of edges in images play a vital role in the areas of surveillance systems, biometrics, network security, vehicle detection and tracking, remote sensing amongst others. However, the images produced by digital cameras are often corrupted by noise due to dust particles, environmental factors etc. Noise is an unwanted, high frequency component, random variation of image intensity which are inherent in digital images. Noise in images occur during either the capturing stage or the transmission stage due to physics-like photon nature of light and thermal energy inside the sensors [1]. The presence of noise in digital images simply means that the pixels in the image show a different intensity value instead of the original pixels values.

In digital images, the number of corrupted pixels will show the quantification of noise present in the image [2]. There exist different types of noise in digital images, depending on the type of disturbance. These types of noise are as follows [1]: The impulsive noise (Salt & Pepper noise), amplifier noise (Gaussian noise), multiplicative noise (Speckle noise). The impulsive noise appears in form of black and white dots in an image. This type of noise occurs in the image due to sharp and sudden change in image signal. Dust particles during the image capturing stage or corrupted transmission channel are the major causes of this type of noise [3]. A Gaussian noise is a statistical noise having a probability density equal to that of the normal distribution. This type of noise occur during acquisition stage due to the environmental condition [4]. The multiplicative noise otherwise known as speckle noise is unwanted signal that worsen the resolution of the active radar and synthetic aperture radar (SAR) images. this type of noise originates due to coherent processing of back scatter signals from different distributed points [1]. An edge can be defined as a single pixel with local discontinuity in intensity [5]. Edges in images are also high frequency components which make it difficult to identify in noisy environment. Edge detection is a process of identifying these local discontinuities in images using an algorithm [6]. Particle swarm optimization algorithm was first introduced in 1995 by Eberhart and Kennedy [7]. The technique was a population based heuristic optimization problem solving algorithm, which was based on the idea of the social behaviour of bird flocking, fish schooling and swarm theory [8]. Particle swarm optimization has five basic parameters which are [Pariticle, velocity, fitness, P_{BEST}, and G_{BEST}9]. A number of researchers in [10],[11] and [12] presented edge detection algorithms in noisy environments.

The authors in [10] presented a colour edge detection algorithm in RGB colour space. The algorithm in the RGB colour space used a median filter to suppress the noise in the image, then a maximum directional difference of the sum of grey values when each component of the image taken separately were calculated for each pixel. However, in this procedure, there are lots of edges in the colour image that will not be detected due to the transformation technique used. Hence, missing edges exists in the generated output edge map. The authors in [11] presented an algorithm for edge detection

in RGB colour space. This algorithm used a Kuwahara filter to smoothen the original image before applying edge detection. An adaptive threshold selection method was applied to predict the optimal threshold value. An edge thinning algorithm was used to extract the edges considering each channel independently in RGB colour space. But with the application of the Kuwahara filter in smoothening process, edges are often displaced or removed due to the presence of noise in the image. The authors in [12] introduced an algorithm with a view to improving the canny edge detection algorithm to operate on colour images. The algorithm introduced the concept of Quaternion Weighted Average Filter (QWAF) and vector analysis to deal with the weakness of the traditional canny edge detection. The algorithm used QWAF with a sliding window of 9x9 to remove the Gaussian noise present in the image, and non-maximum suppression (NMS) based on interpolation for edge thinning. However, the performance of the algorithm highly depended on the size of the sliding window. This implies more blurring as well as detecting thicker edges. The outline of broken and false edges appears less using this algorithm, but the computation time is increased due to the sliding window.

In view of the shortcomings associated with the related works, there is need to introduce an effective noise filtering algorithm in order to minimize the effect of false and broken edges that exist in the generated output edge map.

II. PARTICLE SWARM OPTIMIZATION

The role of particle swarm optimization is to solve image enhancement problem by tuning the parameters with a view to obtaining the best combination according to an objective criterion that describes the contrast of the image. The swarm is initialized randomly, with a group of particles and it then searches for optima by updating through iterations. Two best values are used to update each particle in every iteration. The first one is the best solution of each particle achieved so far known as P_{BEST} and the other is the best solution tracked by any particle among all generations of the swarm known as G_{BEST} [7]. With respect to the two best values obtained, a particle updates its velocity and position with the help of the following Eq.(1a),(1b) [9] viz:

$$V_i^{t+1} = W^t V_i^t + C_1 R_1 .(Pbest_i^t - X_i^t) + C_2 R_2 .(Gbest_i^t - X_i^t) \quad (1a)$$

$$X_i^{t+1} = X_i^t + V_i^{t+1} \quad (1b)$$

Where: X_i^t and V_i^t denote the position and velocity of the i^{th} particle at time instance t W^t is the inertial weight at t^{th} instant of time C_1 and C_2 are positive acceleration constant R_1 and R_2 are random values generated in the range [0, 1], sampled from a uniform distribution.

The particle swarm optimization technique is initialized with a view to choosing candidates solution randomly within a search space. The algorithm uses the objective function to determine candidate's solution, thereby operating on the resultant fitness values [13]. The general process of implementing particle swarm optimization algorithm is described in [14].

The inertia weight w and the acceleration coefficient c_1 and c_2 are the particle swarm optimization parameters which are user supplied. The acceleration coefficient are positive constant within the range of [0 2] while the inertia weight is within the range of [0.8 1.2]. The inertia weight is responsible for keeping the particles moving in the same direction by either suppressing the particles inertia or accelerating the particle in its original ongoing direction [13]. This also controls the particle swarm optimization convergence rate. The values R_1 and R_2 are random values in the range of [0 1]. These values are generated for each velocity update [15].

Some of the advantages of using of Particle Swarm Optimization (PSO) are as follows [16]:

i. Fewer numbers of parameters: particle swarm optimization is easier to implement because it uses only one parameter which is the velocity calculation.
ii. Using particle swarm optimization algorithm to handle the edge detection in noisy images does not require any post-processing technique (such as a linking technique).

The acceleration coefficient C_1 and C_2 controls how far the particle will move in a single iteration and are usually a random number in the range [0 2]. To improve the performance of the algorithm, the acceleration coefficient C_1 and C_2 are set to equal integer values. Following [16] the values w = 0.81, C_1 = 1.4962 and C_2 = 1.4962 are used. The value w is the inertia weight that controls the convergence rate of the particle swarm optimization algorithm. The particle swarm optimization based on vector order statistics edge detection algorithm used a population size of 5 and maximum number of iterations of 10. These parameters are chosen with a view to reducing the computational time during edge detection. In order to measure the quality of a reconstructed image from a noisy environment, a mathematical model is required with a view to determining how much the image has been recovered. These mathematical models are the mean square error (MSE) and peak signal to noise ratio (PSNR) [17]. The mean square error is used as a signal fidelity measure to compare two signals by providing a quantitative score with a view to determining the level of error or distortion between them. The mean square error is calculated using (1c) [3].

$$MSE = \frac{\sum_{p,q} [I_1(p,q) - I_2(p,q)]^2}{p * q} \quad (1c)$$

Where; I_1 is the reconstructed image
I_2 is the noisy image
p * q is the dimension of the row to column.
The MSE is however usually expressed as the peak signal to noise ratio measure as in (2) [3]

$$\text{PSNR} = 10\log_{10}[\frac{T^2}{MSE}] \quad (2)$$

Where: T is the range of pixel intensities in an image. The value of T is calculated using (3) [17]

$$T = 2^N - 1 \quad (3)$$

For a unit8 image and unit16 type image of 8-bits and 16-bits respectively, the values of *T* are computed as:

$$T = 2^8 - 1 = 255 \text{ , } T = 2^{16} - 1 = 65535$$

Where N is the number of image bits.

III. METHODOLOGY

This work used the approach outlined below to derive the flowchart in Fig.1

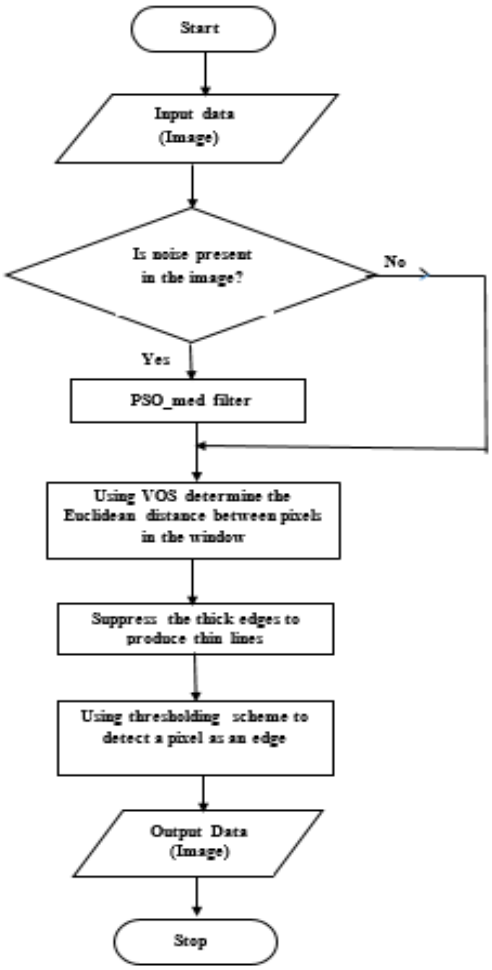


Fig. 1: Flowchart of the Proposed Edge Detection Algorithm.

A. Initializing the Algorithm

The vector order statistics was used to represent the reconstructed coloured images using the steps in [6]. The Minimum Vector Range (MVR) was employed with a view to further reducing the presence of noise in the images. The algorithm is described as follows:

i. Reconstruct the image from noisy environment to clean environment using the particle swarm optimization technique.
ii. Using Vector Order Statistics, generate a 3x3 window size pixel.
iii. Determine the Euclidean distance between each pixel in the window.
iv. Apply a pixel collection scheme to the reconstructed coloured images.
v. Use non maximum suppression to reduce thick edges.
vi. Determine which pixel is an edge or not using a threshold value. Thus generating the final output edge map.

The flow chart for the developed algorithm is shown in Fig.1.

1. Input the image.

The benchmark images are used as an input. The images are selected from the database of the computer system. The following program listing shows snippets of the

portion that extracts the image from the database. Fig.2 shows the extracted image from the computer database.

```
filename = uigetfile('*.jpg;*.tif;*.png');
data=im2double(imread(filename));
```

Fig. 2: Extracted Input Image form the Computer Database.

2. The program checks if noise is present in the input image. If there exists noise in the image, the particle swarm optimization median filter is initialized.
3. Initialize the position *x(t)* and velocity *v(t)* for the particle.
4. For every pixel in the population size, evaluate the fitness function.
5. Generate values for the weight, acceleration coefficient and the random values.
6. Update the position and velocity.
7. When f(present(t+1)) < f(Pbest(t)), update the Individual Best for i (particle), the set of weights that yields the (Best Fitness value) minimum MSE.
8. When f(Gbest(t)) < f(present(t+1))), update the Global Best, the set of weights that yields the minimum MSE in a global sense (i.e.,) Best of Individual Best's.
9. The algorithm is iterated until convergence is reached. This convergence yields Gbest (t), the optimal set of weights that minimizes the mean square error. With the set Gbest (t) as weights, the filter estimates the corrupted pixel.
10. Using the reconstructed image as an input image, generate a 3x3 pixel window from the image.
11. For each pixel in the window a vector of size 3 is used to describe the colour, this is written as $P_{p,q}$ RGB. The vector is the RGB values of that pixel.
12. A new set of scalars A_0 to A_8, is calculated for each pixel by determining the Euclidean distance between a given $P_{p,q}$ RGB and all other $P_{p,q}$ RGB in the window. The Euclidean distance between a pair of vector is the difference in each vector's R value squared added to the differences in G values squared added to the difference in B values squared and the sum in a square root. This result in a 9 distance which is A_0 to A_8.
13. This process is repeated for each pixel in the window, resulting in a single scalar for each pixel. So, the initial 3x3x3 matrix has been transformed into a 3x3x1.
14. The new 3x3x1 matrix is reshaped into a 9x1 array where the index corresponds to the pixel number.
15. The original 3x3x3 window is reshaped in a manner related to the reshaping of the 3x3x1 matrix to result in a 9x3 matrix where the first dimension corresponds the same pixel number as the 3x3x1 array index, and the second dimension is the RGB values for that pixel.
16. The 9x1 array is sorted into ascending order, and the same rearrangement of indices is applied to the first dimension of the 9x3 matrix.
17. The minimum vector range is then calculated by finding the Euclidian distance between the first pixel and the last pixel resulting from the ordering of the sort.
18. If the vector range is above a user set threshold then the window contains an edge, and the centre pixel of the window is set to 1 to represent an edge at that location. Fig. 3 shows the output result of the algorithm before edge suppression.

Fig.3: Output of the Vector Order Statistics.

19. Suppress the thick edges produced by the vector order statistics with a view to achieving thin and continuous edge lines.
The output result after suppressing the thick edges is depicted in Fig. 4.

Fig. 4: Output Result of the Suppressed Edges.

20. Calculate the Peak-Signal-Noise Ratio that determines the quality of the restored image by using (1) and (2)

IV. RESULTS AND DISCUSSION

Four images in the output result are displayed in Fig. 5 The first image represents the benchmark image before it was corrupted with noise, the second image represents the corrupted image, the third image represents the output of the vector order statistics and the fourth image represents the final output image obtained based on collection of pixels. The peak-

signal-noise ratio at different noise levels is shown in Table 1. The peak-signal-noise ratio at different noise levels is shown in Table 1 obtained using (1) and (2) as a measure of quality between the original image and the reconstructed image. The higher the peak signal-to- noise ratio, the better the quality of the reconstructed image

Fig. 5: Output Result of Test Image.

TABLE 1: NOISE LEVELS WITH THEIR RESPECTIVE PEAK SIGNAL-TO-NOISE RATIO.

Percentage pixel affected by noise (%)	PSNR (dB)
10	62.7104
20	59.8679
30	58.1529
40	56.9401
50	54.9414
60	54.1182
70	53.3830
80	53.7189
90	53.0920

The plot of peak-to-signal noise ratio is shown in Fig. 6 for the various noise levels. Fig 6 shows that, as the noise level in the images increases, the peak signal-to-noise ratio decreases. This implies that the quality of the reconstructed image decreases with increase in noise level.

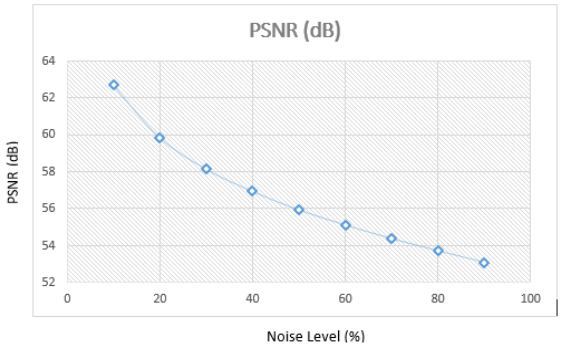


Fig. 6: Peak Signal to Noise Ratio for Various Noise Levels.

The computation time of the algorithm depends on the type of image to be processed (dimension of the image), the level of noise present in the images and the specification of the computer system running the program. It is also dependent on the number of iterations and population size in the particle swarm optimization algorithm. The specification of the system used to run the algorithm are as follows:

Processor: Intel ® Core ™ i3-2350M CPU @ 2.30GHz
RAM: 4GB
System type: x64-based processor

The Fig. 7(a)–7(f) are the output results in noisy environment of the traditional exsisting edge detection algorithms in comparison with the developed edge detection algorithm.

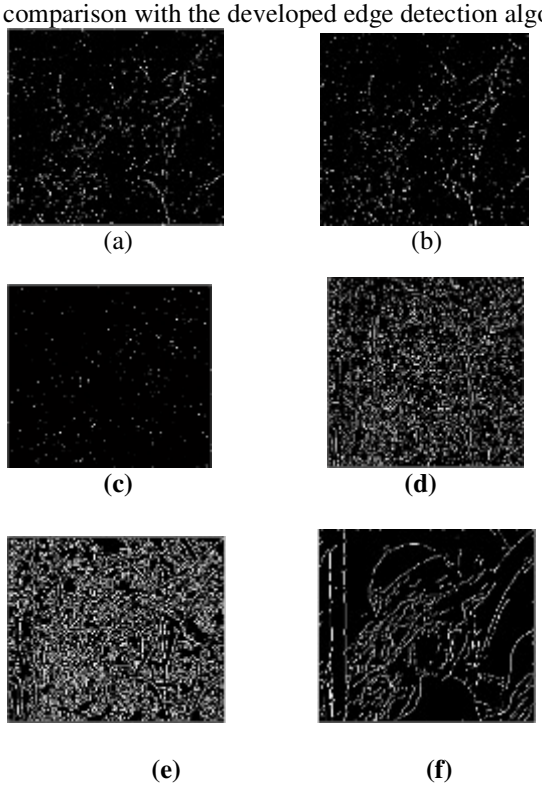


Fig.7.:Output Result of Existing Algorithms in Comparison with the Proposed Algorithm.

The output result (a) is the Sobel edge Detection, (b) Prewitt Edge Detection Algorithm, (c) Roberts Edge Detection Algorithm, (d) Laplacian Edge Detection Algorithm, (e) Canny Edge Detection Algorithm and (f) Proposed Edge Detection Algorithm

The Pratt Figure of Merit (PFOM) is a method used to provide a quantitative comparison between edge detection algorithms in image processing [5]. The PFOM is determined by a mathematical expression as in Equation (4). The PFOM measures the value of detected edges between 0 and 1. As the value get closer to 1, it shows better detected edge values.

$$R = \frac{1}{Max(N_I, N_A)} \sum_{k=1}^{N_A} \frac{1}{1 + md^2(k)} \quad (4)$$

Where: N_I is the number of actual edges
N_A is the number of detected edges

m is a scaling constant set to 1/9.
d (k) denotes the distance from the actual edge to the corresponding detected edge

The Pratt Figure of Merit is sensitive to different expected errors, it maximizes when the edge map is perfect and decreases as the error in the edge map increases. The Pratt Figure of Merit measures values between 0 and 1, depending on the quality of the edge detection algorithm used. As the values determine by the Pratt Figure of Merit moves towards 1, it shows best edge detection algorithm [18]. Table 2 shows the PFOM of various edge detection algorithms

TABLE 2: PFOM FOR VARIOUS EDGE DETECTION ALGORITHMS.

Edge detection algorithm	Image with noise
Sobel edge detection algorithm	0.4191
Prewitt edge detection algorithm	0.4191
Robert edge detection algorithm	0.2807
Laplacian edge detection algorithm	0.2811
Canny edge detection algorithm	0.5606
Proposed edge detection algorithm	0.8458

Fig. 8 shows the graphical representation of the Pratt Figure of Merit (PFOM) in comparison with the existing traditional edge detection algorithm such as

SEDA = Sobel Edge Detection Algorithm PEDA = Prewitt Edge Detection Algorithm
REDA = Roberts Edge Detection Algorithm LEDA = Laplacian Edge Detection Algorithm
CEDA = Canny Edge Detection Algorithm DEDA = Proposed Edge Detection Algorithm

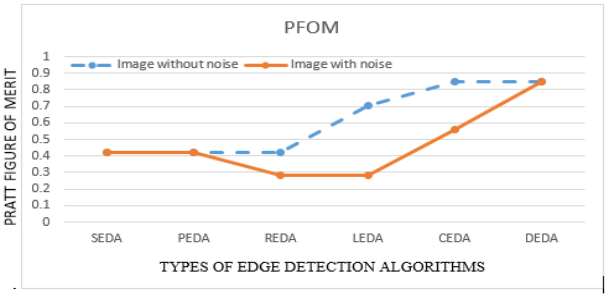


Fig .8: Quantitative Comparison Using Pratt Figure of Merit (PFOM).

The plot for the Pratt Figure of Merit (PFOM) showed that without noise present in the image, the value obtained are closer to the value 1 than the values obtained when noise is present in the image for the existing proven edge detection algorithms. The PFOM value obtained for the proposed edge detection algorithm in clean and noisy environment showed lesser margin than those of the existing proven edge detection algorithm. These results signify that the proposed algorithm performed better than the existing proven edge detection algorithms.

V. CONCLUSION

This research work presents an improved edge detection algorithm using particle swarm optimization based on vector order statistics. In order to address the shortcomings of the existing traditional edge detection algorithms that could not process coloured images directly unless been converted to grey scale, Vector Order Statistic technique was employed. The profile edge intensity was applied to generate a collection scheme. This collection scheme was obtained using set of pixels with respect to the step and roof edge profiles. The collection scheme was then applied as a mask in both vertical and horizontal directions to the images. An improved figure of 0.8458 was obtained in noisy environment using the PFOM. Further work should implement the algorithm on real physical systems in the areas of biometrics, vehicle detection and tracking, remote sensing amongst others.

REFERENCES

[1] Rohit Verma and Jahid Ali, "A Comparative Study of Various Types of Image Noise and Efficient Noise Removal Techniques," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3, pp. 617-622, 2013.

[2] Bijay Neupane, Zeyar Aung, and Wei Lee Woon, "A New Image Edge Detection Method Using Quality-Based Clustering," *Proceedings of the IASTED International Conference Visualization, Imaging and Image Processing,* vol. July 3-5, pp. pp.20-26, 2012.

[3] Amera Abdul and Wohid Funjan, "Denoising An Image Based On Particle Swarm Optimization (PSO) Algorithm," *journal of Babylon University/Pure and Applied Sciences,* vol. 21, pp. pp.1511-1518, 2013.

[4] Chris Solomon and Toby Breckon, "Fundermentals of Digital Image Processing A Practical Approach With Examples in MATLAB," First ed: John Wiley & Sons Ltd, 2011, pp. 1-109.

[5] B.O Sadiq , S.M Sani, and Garba.S, "Edge Detection: A Collection of Pixel based Approach for Colored Images," *International Journal of Computer Applications,* vol. 113, pp. 29-32, 2015.

[6] B O. Sadiq , S.M. Sani and S. Garba, "an approach to improving edge detection for facial and remotely sensed images using vector order statistics " *The International Journal of Multimedia & Its Applications (IJMA),* vol. 7, pp. 17-25, 2015.

[7] Venkata and Jagadeesh Babu, "Color Image Enhancement Using Praticle Swarm Optimization," *Internation Journal of Engineering Science and Technology (IJEST)* vol. 2, pp. pp.474-480, 2012.

[8] Monsoor Roomi and Jayanthi Rajee, "Speckle Removal in Ultrasound Images Using Particle Swarm Optimization Technique," *IEEE-international conference on recent trends in information technology,* Retrieved from www.ieeexplore.ieee.org on 21/03/2014, pp. pp.926-931, 2011.

[9] Amanpreet Kaur and M.D Singh, "An Overview of PSO-Based Approaches in Image Segmentation " *international journal of engineering and technology,* vol. 2, pp. pp.1349-1357, 2012.

[10] Soumya Dutta and Bidyut Chaudhuri, "A Color Edge Detection Algorithm in RGB Color Space," *IEEE-International Conference on Advances in Recent Technologies in Communication and Computing,* pp. pp.337-340, 2009.

[11] Xin Chen and Houjin Chen, "A Novel Color Edge Detection Algorithm in RGB Color Space " *Institute of Electrical and Electronics Engineers Transcations,* pp. pp.793-796, 2010.

[12] Geng Xin, Cgen Ke, and Hu Xiaoguag, "An improved Canny edge detection algorithm for color image," *Institute of Electrical and Electronics Engineers Transcations,* pp. pp.113-117, 2012.

[13] James Blondin, "Particle Swarm Optimization: A Tutorial," *retrieved from www.cs.armstrong.edu/saad/csci8100/pso_tutorial.pdf,* vol. on 23/11/2014, pp. pp.1-5, 2009.

[14] Russel Eberhart and Yahui Shi, "Particle Swarm Optimization: Developement, Applications and Resources " *Institute of Electrical and Electronics Engineers Transcations (IEEE),* vol. 3, pp. pp.81-86, 2001.

[15] Yahui Shi, "Particle Swarm Optimization," *institute of Electrical and Electronics Engineers Transcations (IEEE) Neural Network Society,* pp. pp.8-13, 2004.

[16] Mahdi Setayesh, Mengjie, and Mark Johnston, "A novel particle swarm optimization approach to detecting continuous, thin and smooth edges in noisy images," *Elsevier Inc.,* pp. pp.28-51, 2013.

[17] Peter Ndajah, Hisakazu Kikuchi, and Masahiro Yukawa, "An Investigation on The Quality of Denoised Images," *International Journal of Circuits, Systems and Signal Processing,* vol. 5, pp. pp.423-434, 2011.

[18] Karen Panetta and Eric J. Wharton, "Logarithmic Edge Detection with Applications " *Journal of Computers,* vol. 3, pp. pp.11-19, 2008.

Compressive Sensing: The Throughput Requirement for its Application in Energy Efficient M2M Communication Systems

[1]Sylvester Ajah, [2]TriantafyllosKanakis, [3]Chris Onyibe
[1]Computing, School of Science and Technology, University of Northampton, UK
[2]Computer Engineering Technology, Akanu – Ibiam Federal Polytechnic, Unwana, Afikpo, Nigeria
ajah.sylvester@gmail.com, triantafyllos.kanakis@northampton.ac.uk & chris912111@yahoo.com

***Abstract*– The energy efficiency of M2M communications devices remains a challenge that is partly addressed and must be solved in order to stimulate fast adoption of M2M communications paradigm. Compressed Sensing Technique (CST) efficiently acquire sparse signal and sample them at approximately information rate. This could be used for enhancing the energy efficiency of M2M communication devices. However, CS algorithm on the M2M devices increases their computational complexity, energy cost of their processing but reduces the energy cost of communications which on the battery life of the wireless devices. This trade-off between computation and communications energy costs in the wireless devices necessitate the need to determine the specific throughputs at which CS becomes energy efficient based on the devices' properties. This work proposes an energy efficient compressive sensing throughput model. This could provide an avenue through which the M2M/IoT communications experts and companies can use to determine the efficiency of compressive sensing algorithm on their devices. The proposed model has become handy for M2M/IoT communications experts to use in evaluating based on the throughput requirement of various M2M / IoT applications.**

***Keywords – Energy efficiency, M2M, Machine to Machine Communications, Compressive Sensing, Throughput,* EECST**

I. INTRODUCTION

The concept of M2M communications paradigm which is simply the autonomous communications between the electronics devices is no longer new, the applications across many sectors have already started. The year 2020 forecasted by Ericsson for the adoption of 50 billion connected devices is already close, hence some anticipated applications across all sectors are already in existence [1]. It is because of this reality and the need to have energy efficient M2M communication systems, the sparse nature of most digital signals which provided the basis for adopting CS algorithm in M2M communications paradigm and the variations in the throughput requirement of various M2M communications applications necessitate the need to ascertain the throughput at which the application of the CS algorithm on the node is energy efficient.

Compressive sensing (CS) is a signal processing strategy for efficient signal acquisitions and reconstructions, which sample the signals at approximately information rates. It can also be described as signal acquisition method that collects few sample of signal of interest and use optimization technique to reconstruct the original signal from incomplete measurement. The CS apply non-adaptive linear projection that retains the structure of the signal and the signal is reconstructed from these projections [2]. This technique has provided the window of opportunities for enhancing the energy efficiency of M2M communication systems. CS combines the signal sampling and compression into a single process, with low sensitivity to packet loss and graceful degradation of signal in the event of unusual sensor readings [3]. It also reduces the time spent on data acquisition by the nodes via intelligently picking the coefficients of the non-zero part of signals to be sensed, hence reducing the energy cost of sensing and communications. Furthermore, CS exploits the information rate with any signal, hence removes redundancy in the signal during sampling process, leading to lower effective sampling rate which reduces the energy cost of sampling in the nodes. Also, most computations take place in the base stations (sink) in CS, hence elongating the life span of M2M devices [3]. These enumerated points make CS an effective technique for enhancing the energy efficiency of M2M device.

This work is a novel idea that provides a model through which M2M communication experts can determine when it is optimal (energy efficient) to adopt CS algorithm on the M2M devices. This is based on the throughput requirements of their intended applications.

The rest of the work is organized as follows; section II discusses related works, section III discusses the theory of CS, part IV discusses the component parts of battery energy consumption in wireless devices, section V discusses the proposed Energy efficient Compressive Sensing Throughput (EECST) model, and section VI concludes the work.

II. RELATED WORKS

In the recent years, several research efforts have been made to tackle different challenges that affect different aspect of M2M communications paradigm. These challenges include spectra through which they will connect, the reliability of the communication system, energy efficiency of the wireless

devices that are expected to be used for M2M communications and cost. It is based on these challenges that Weightless SIG designed a specifications that uses white space for communication. The proposed weightless standard is expected to have the following features; support large number of M2M communication terminals because of large volume of the available spectrum in white space, long battery life for the M2M communications devices – over a decade lifespan for majority of M2M terminals, cheap M2M communication equipment, and mobility of M2M communication devices[4][5]. Sylvester A. et al [6] proposed the use of the available Sub 1 GHz Spectra for M2M communications, Weightless SIG later modify their specification to be able to communicate in Sub 1GHz ISM band[7]. Fig.1 and Table 1 show the available white space spectra and Sub 1GHz ISM bands respectively.

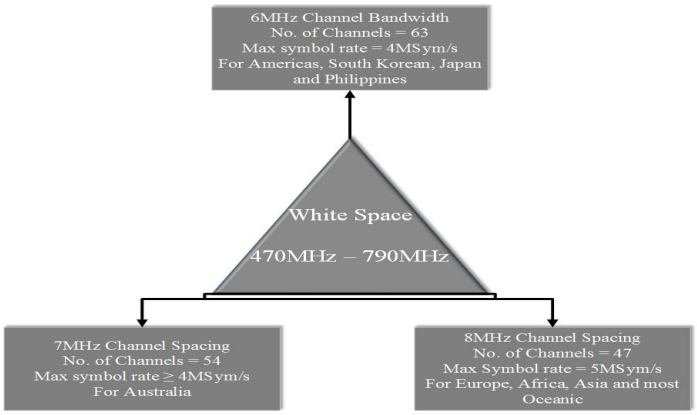


Fig. 1. The proposed white space bands, channels, bandwidth, symbol rate and regions for M2M communications [8].

Table 1: Allocation Of 1ghz Ism Bands, Bandwidth And Their Global Locations.

Bands (MHz)	Centre Frequency	Bandwidth (MHz)	Locations
902 - 928	915	26	US
433.05–434.79	433.92	1.74	Europe
863 - 870	868	7	Europe
950 - 958		8	Japan

The energy efficiency of the wireless devices which are supposed to be used for M2M communication have being a major issue since the emergence of wireless sensor networks (WSN). Sequel to the autonomous feature of M2M communication paradigm, the durability of the system is imperative, hence the need to have energy efficient wireless device. Sandra S. et al [9], stated that the power consumption in the wireless devices can be classified into device hardware, transmission, MAC and routing protocol. Hence, the energy efficiency of the wireless device is dependent on the energy efficiency of the various components in the wireless device. While Mark H. et al [10] stated that choosing the right energy efficient components and applying the right energy efficient technique in each component is the first step towards reducing the power consumption in sound electronic design.

Furthermore, many researchers and experts have tried to address various aspects of power consumption in wireless devices, Halkes, G. P. et al [11] stated that using a low-power listening aid effectively in reducing the energy cost of idle listening after comparing S-MAC and T-MAC. In which they observed that T-MAC with variable duty cycle that is suitable for variable applications is more energy efficient than S-MAC with fixed duty cycle irrespective of the applications.

One of the earliest work on the application of CS in wireless communication was done by Waheed, B. et al, in which they proposed a distributed matched channel communication scheme, which consider the trade-off between power, distortion and latency in the applications of CS in wireless sensor network (WSN) that communicates with a fusion centre (FC) [12]. This was followed by joint – channel communication architecture for energy efficient estimation of sensor field data at FC, which further analyse the relationship between power, distortion and latency at FC, couple with the impacts scaling behaviour with the number of sensor nodes on the above mentioned properties[13]. These research works and so many other ones have been published to address different challenges that mitigate the application of CS in wireless communications. But none of these works have explicitly discuss the throughput requirement based on applications for the applications CS algorithm in M2M communication.

III THEORY OF COMPRESSIVE SENSING

The basic principle of CS is to transform code the signal of interest x into the basis or frame that will provide the compressible and sparse representation of the signal [14]. Transform coding is done using Fourier transform (FT), fast Fourier transform (FFT), discrete cosine transform (DCT), wavelet transform (WT), etc. The sparse representation of the signal of length n, entails that it can be represented with k nonzero coefficients, where $k \ll n$. While the compressible representation of the signal entails that the signal can be well-approximated to those k none zeros part of the signal n. The CS algorithm can represent the signal of interest with high fidelity by preserving the k none zeros value of n and their locations.

This method is called sparse approximation, which is the foundation of the transform coding schemes that uses the signal sparsity and compressibility like JPEG, MPEG, MP3 and JPEG2000 standards[14]. The number of non-zeros coefficient of x is less than or equal to k. Heung – No, L [15] stated that CS comes down to two fundamental challenges; the design of good sensing matrix and the design of good recovery algorithm. While Keith, et al [16] stated that CS is dependent on the sparsity and incoherence of the signal of interest as shown by Eq.(1)

$$||x||_0 \leq k \quad (1)$$

The signal x is encoded into a smaller vector say b with the aid of a sensing matrix $A \in R^{m \times n}$, where $m < n$ and it is choosing independently of x [17]. The CS coded signal can be represented as given in (2). The CS approach involves directly acquiring the compressed samples without going via the intermediate stages and the compressive measurement through linear projections as given in (2) [15].

$$Ax = b \quad (2)$$

In the applications of CS in M2M communications, the encoding of x is not calculated by a computer or microcontroller, but obtained by certain electrical or electromagnetic, physical, or optical measuring means, depending on the application. Also, because of the condition in (3), b is the compression of x.

$$\begin{cases} k \leq m \\ m < n \end{cases} \quad (3)$$

Furthermore, on the application of this technique on M2M communications paradigm, b is recorded by the node and becomes digitally available to the decoder. Though equation (2) above is an underdetermined equation system and has infinite number of solutions, x is recovered from b by finding the sparsest solution of equation (2) by solving (4).

$$\min_x ||x||_0 \ subject\ to\ \boldsymbol{Ax = b} \quad (4)$$

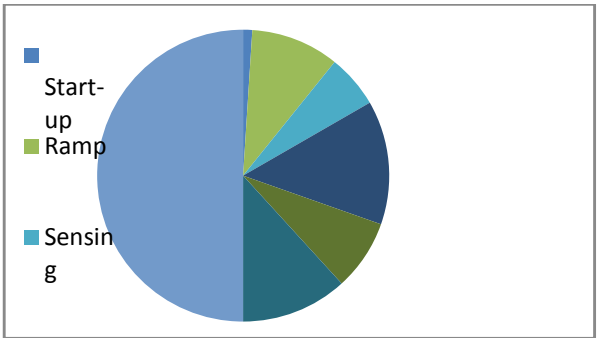


Fig. 2: Various operational energy costs in a Wireless node(s) [21].

Equation (4) above is called l_0 norm, and though the combinational equation of (4) is Non-deterministic Polynomial-time hard (NP Hard) [18], and the method of trying all the possible supports of cardinality k is computationally intractable [19]. To make it tractable, l_0 norm is replace by $l_1$norm as given in (5).

$$\min_x ||x||_1 \ subject\ to\ \boldsymbol{Ax = b} \quad (5)$$

Equation (5) above is a convex program and has several fast solvers than (4). In ideal case, we will like to recover x from (5) when m equals 2k, x is uniquely determined by k indices and k values of its non-zeros entries [19]. However, the whole processes of compressive sensing consist of the following stages; Signal sparse representation, Linear encoding measurement collection and sparse recovery.

IV. ENERGY CONSUMPTION IN WIRELESS M2M COMMUNICATIONS DEVICES

Equation (7) summarizes various energy costs associated with wireless communications and Fig. 4 gives the percentage of various operational energy costs within wireless devices. These energy costs are based on MAC protocol, because it has a major impact on the power consumption of the wireless devices and it is based on a single sampling period [20].

$$E_T = E_{start-up} + E_{ramp} + E_{sensing} + E_{logging} + E_{sampling} + E_{Computing} + E_{communication} \quad (6)$$

Where E_T is the total operational energy consumption costs in the wireless devices, $E_{start-up}$ is the sensor initial energy consumption during start-up, E_{ramp} is the energy cost of switching to different energy states for various nodes' operations, $E_{logging}$ is the energy cost of storing the data, $E_{sampling}$ is the data sampling energy cost, $E_{Computing}$ is the processing energy cost and $E_{communication}$ is the communications energy cost. Fig 4 illustrates the percentage of energy costs of various component operational energy costs in a wireless node(s).

Being that start-up energy cost associated with the wireless device is negligible (< 1%) as can be seen in Fig 2, its effect will not be considered further. The ramp energy cost in the micro-controller unit (MCU) of the wireless devices are negligible too, but the ramp energy cost in the radio is significant and it constitute 10% of the total energy cost in the wireless device[22][21]. Equation (7) below gives how to calculate the radio ramp energy cost.

$$E_{ramp} = \frac{|(I_{st2} - I_{st1})| \times T_{st12} \times V_{dc}}{2} \quad (7)$$

Where I_{st2} is consumed current in the state switched to, I_{st1} is the consumed current in the current state, T_{st12} is time used in switching from state 1 to state 2, and $V_{dc}$is the voltage consumed.

The sensing energy cost is about 6% of the total energy cost in the wireless device as can be seen in Fig 2, and the energy cost of sensing b bits of data can be calculated using Equ. (8).

$$E_{sensing} = b \times V_{dc} \times I_{Sensing} \times T_{sensing} \quad (8)$$

Where $I_{Sensing}\ and\ T_{sensing}$are the current consumed in sensing and the sensing time respectively.

The logging energy cost is the energy used by the wireless device for reading b bit packet data and writing it into the memory[23]. Eq. (9) shows how to evaluate the energy cost of logging d bits data size per cycle.

$$E_{logging}(b) = E_{read} + E_{write} = \frac{d \times V_{dc}}{8}(I_{read} \times T_{read} + I_{write} \times T_{write}) \quad (9)$$

The sampling energy cost $E_{sampling}$ is the energy the wireless device spent on sampling b bits of data. The $E_{sampling}$is hard to estimate because it greatly depend on the type of applications' data samples.

The energy cost of computing $E_{Computing}$ in a wireless communication device is a key constituent of total energy cost in a wireless device. The $E_{Computing}$ consistsof MCU's active and other modes. Equation (10) shows how to evaluate the $E_{computation}$ in two states (active and sleep).

$$E_{computation} = V_{dc} \times I_{active} \times T_{active} + V_{dc} \times I_{sleep} \times T_{sleep} \quad (10)$$

The communications energy costs consist of the energy cost ofdata transmission and the cost of data reception as given in (11)

$$E_{communication} = E_{tx} + E_{rx} \quad (11)$$

Where E_{tx} the energy is cost of transmission of packets of data, and E_{rx} is the energy cost of receiving data packets. Equ. (12) and (13) represents E_{tx} and E_{rx} respectively.

$$E_{tx} = V_{dc} \times I_{tx} \times B_{ltx} \times T_{btx} \quad (12)$$

$$E_{rx} = V_{dc} \times I_{rx} \times B_{lrx} \times T_{brx} \quad (13)$$

Where $I_{rx}\ and\ I_{tx}$are the current consumed in the reception and transmission mode respectively; $B_{ltx}\ and\ B_{lrx}$ is the bit length of the transmitted and received packets along with their preambles respectively; $T_{btx}\ and\ T_{brx}$ is the time for transmitting and receiving single bit of data. However in wireless communication devices, the energy costs of various operations are evaluated in terms of the number of clock cycles required to perform such operations [24]. To this end, the energy cost of performing various operations in wireless communication devices as given in (6) are evaluated in terms of the number of clock cycles required to perform such operations, which varies from one operation to another.

V. ENERGY EFFICIENT COMPRESSED SENSING THROUGHPUT (EECST) MODEL

Equation (14) gives the fundamental model through which any communication system follow, hence to have an energy efficient system, the effect of the energy cost of variables involved have to be considered.

$$y = H\boldsymbol{b} + n \quad (14)$$

Where y is the signal at the receiver, H is the channel properties, b is the signal transmitted l at the transmitter and n is the channel noise. From (14), the channel H is the part of the model that has most significant effect on the transmitted signal. The sensitivity of the receiver is the major determining factor in knowing the amount of power required to get a signal b from point A to B when the H properties have being ascertained using the appropriate models. The receiver's sensitivity which is the minimum input signal (S_{min}) required to produce a specific output signal with a specified signal-to-noise ratio (S/N) and is given in Equ. (15) [25].

$$S_m = (S/N)_{min} \times K \times T_o \times B \times (NF) \quad (15)$$

Where $(S/N)_{min}$ is the minimum signal-to-noise ratio needed to detect a signal, NF is the nose factor, K is Boltzmann's constant $=1.38 \times 10^{-23} Joule/°K$, T_o is the absolute temperature of the receiver input $(°Kelvin) = 290°K$ and B is the receiver bandwidth (Hz) [25]. A typical receiver's sensitivity is around -110dBm, though it is dependent on device type [26].

As stated in [6], that sub 1GHz spectrum provides the energy efficient medium through which M2M devices can be connected, let the communication frequency be Sub 1GHz ISM band (902 – 928) MHz with the centre frequency of 915MHz and bandwidth of 26MHz as given in Table 1. Now to determine the power required to transmit the signal from point A to point B say 4Km in a large city scenario, hence the path loss normally follows Rayleigh distribution. For this discussion, let assume that the value of n as contained in (14) is zero. Also, let the base station (BS) height be 40m, and mobile station height be 2m. Using Hata path loss model in path loss evaluation, using the above variables will result to a path loss of 144.55dB [27].

However, the channel losses between a transmitter and a receiver in wireless channel is given in Equ. (16).

$$Losses = Path\ loss + penetration\ loss + other\ losses \quad (16)$$

The path loss is already evaluated using Hata model as contained in [27]. The penetration loss can be evaluated using (17).

$$L_{pl}(\emptyset) = \sqrt{d - e(\emptyset - f)^2} \quad (17)$$

Where d, e, f are empirical parameters and $\emptyset$ is the angle of the signal inclination [28].

Now using the experimental results for the empirical parameters as contained in [28] for computation. The penetration loss at 60° signal reception angle, is 23.69dB. Also, other losses as contained in Equ. (16) is gotten by calculating 10% of the summation of the above losses. Therefore, other losses is 16.82dB. Hence, Total losses as given (16) is approximately 185dB.The power of the received signal at the receiverP_r is given in Equ. (18).

$$P_r = P_t + G_t - Losses \quad (18)$$

Where P_t is the transmit power at the transmitter and G_t is the total gains in both the transmitter and the receiver. Now using P_r as -110dBm, assuming that the total gains between the transmitter and receiver at 2dBm each is 4dB, then the required $P_t$is 71dBm. This value of P_t is the minimum required to get any signal across 4Km, assuming all the variables are right valued.

Given that there are numerous anticipated M2M applications across all sectors, the throughput requirement for each anticipated application also vary. Based on the trade-off between the energy gains from mainly communication energy cost and computing energy cost when CS algorithm is applied to the M2M communication devices. It is imperative to ascertain the throughput at which the applications of CS algorithm is energy efficient. The E_{tx}>E_{rx} for a typical wireless ad hoc network [29], and based on the fact that the wireless node to be used for M2M communications are expected to be dump in order to elongate the life span of the devices [8]. It can be deduced that most of the M2M communications devices will rarely receive packets except for updates in terms of the available spectra for communication. In forming this model, the following assumptions were made, as highlighted below.

a) M2M communication cellular structure as proposed by Weightless SIG hence, the major communication cost will be on transmitting the data packets to the base station, which do most processing and scheduling in the M2M communication paradigm as suggested by Weightless SIG in their specification [8].

b) The battery power of the nodes are very limited, hence the need to know the throughput at which the applications of CS algorithm is energy efficient.

c) The channels of communication are sub 1GHz spectra (902 – 928) MHz ISM Band, hence have limited bandwidths as proposed in [6].

d) The nodes are dump, hence does not process the sensed data.

e) Multipath fading does not exist

f) BPSK signal is used in the model

Let the amount of energy required to transmit a single bit of data be e_{tb}, which is equivalent to the number of clock cycles required to transmitted a single bit of data be n, and the energy cost per clock cycle be e_{cc}, to transmit x bit(s) of data without compression, the E_{tx} is evaluated as given in (19).

As mentioned above, the application of CS algorithm increases the energy cost of computing / processing. Let the number of clock cycle required to execute CS algorithm on the data sample beC_n, the E_{tx} when CS algorithm is applied is given in (21).

$$E_{tx} = x \times e_{tb} \equiv x \times n \times e_{cc} \quad (19)$$

For the benefit of the context of this discussion, it is imperative to split the total number of bits to be transmitted into the preamble which is assumed to be constant for both compressed and uncompressed signal. Let the number of bits in the preamble be x_1 and the remaining number of bits in the packet bex_2, putting the above assumptions in Equ. (19) will yield Equ.(20).

$$E_{tx1} = (x_1 + x_2) \times e_{tb} \equiv (x_1 + x_2) \times n \times e_{cc} \quad (20)$$

As earlier mentioned, the application of CS algorithm on the M2M Communication devices will increase the computing energy cost. To be able to evaluate E_{tx} when CS algorithm is implemented on the M2M communications device, let the number of clock cycle required to perform data compression using CS algorithm be n_c and the percentage of compression be ɳ, then the E_{tx} using CS algorithm is given as Equ. (21).

$$E_{tx2} = x_1 \times e_{tb} + \eta \times x_2 \times e_{tb} + n_c \times e_{cc} \equiv (x_1 + \eta \times x_2) + n_c \times e_{cc} \quad (21)$$

Eq. (20) and (21) above are suitable for single – input to single – output (SISO) form of communications. For multiple input multiple output (MIMO) form of communications, the above equations will not be suitable. This is as a result of the increase in circuit complexity which will increase the computing / processing energy cost, couple with ϰ number of bits are transmitted simultaneously. However, Zimran, R. et al [30] stated based on their analysis that using MIMO for data transmission is more energy efficient for transmission across long distance. While across short distance, $E_{computation}$ is more than E_{tx} as a result of the circuit complexity. In order to evaluate E_{tx} when MIMO is used, let the energy cost of transmitting ϰ bits of data using MIMO per transmission be $e_{\varkappa}$, and the number of clock cycles required by a MIMO circuit to

transmit x bits of data be $n_{\aleph}$ then the energy cost of transmitting x bits of data can be given as;

$$E_{tx3} = \left(\frac{x_1 + x_2}{\aleph}\right) \times e_{\aleph} \equiv \left(\frac{x_1 + x_2}{\aleph}\right) \times n_{\aleph} \times e_{cc} \quad (22)$$

Then the E_{tx} on the application of CS algorithm can be given as;

$$E_{tx4} = \left(\frac{(x_1 + \eta \times x_2)}{\aleph}\right) \times e_{\aleph} + n_{\aleph} \times e_{cc} \quad (23)$$

Considering SISO scenario as given in (11) and (12), let's take the energy cost of MSP 430 serial micro-processor in active state as the yardstick for evaluation, in which $e_{tb} = 230nj$ *and* $e_{cc} = 0.729nj$for a WSN with a range of 100 meters [24]. Also as mentioned earlier, the energy cost of processing CS algorithm in the node(s) is determined by the number of clock cycles required by the devices to perform the compression operations. Table 2 below shows the number of clock cycles required by MSP 430 micro-processor to perform certain floating point operations.

Table 2: Clock Cycles for Floating Point Operations [31].

Floating point operation(S)	Number of clock cycles
Addition	184
Subtraction	177
Multiplication	395
Division	405
Comparison	37

The type of the CS algorithm and the size of the sensing matrix will determine the number of clock cycle required by the micro-processor to perform the compression operation on the node.

For instance, a micro-processor with an impeded Sub-threshold (Sub-V_T) CS processor will require 8460 clock cycles to apply 50% compression on 512 samples of ECG data. The A in Equ.(2) is constructed by 12 random indices per column, and the sampling rate of the signal is 125Hz [32].

Also, assuming that the length of the MAC addresses for both the compress and un-compressed signal samples are same, then only x_2 in Equ. (20) and (21) is considered in the computation. Fig 7 below shows the data rates at which compression becomes energy efficient.

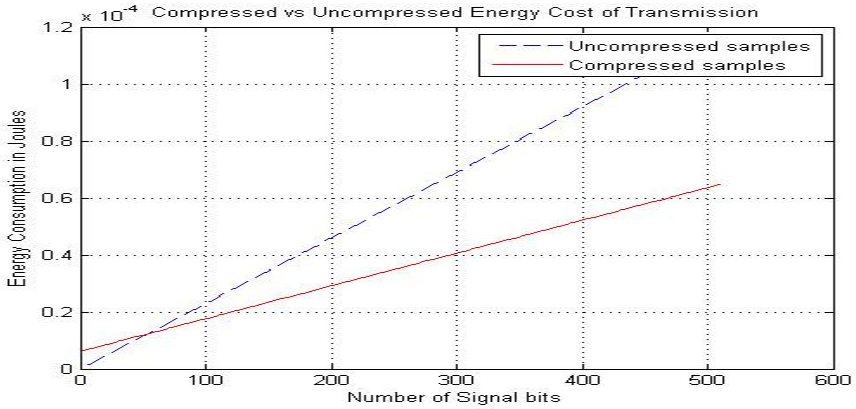


Fig 3: The CS compressed Vs uncompressed transmitted energy cost.

Based on the input variables above, the data rate at which compression becomes energy efficient is at 53.63 ≈ 54 bits. Though the number of clock cycles used for compression is based Sub-threshold (Sub-V_T) CS processor, the number of clock cycles required for performing CS compression algorithm varies from one micro-controller to another. Because of the variations in the inherent properties of various micro-controllers like speed, energy requirement per clock cycle, etc. and the variations on the various computation requirements of various CS algorithms.

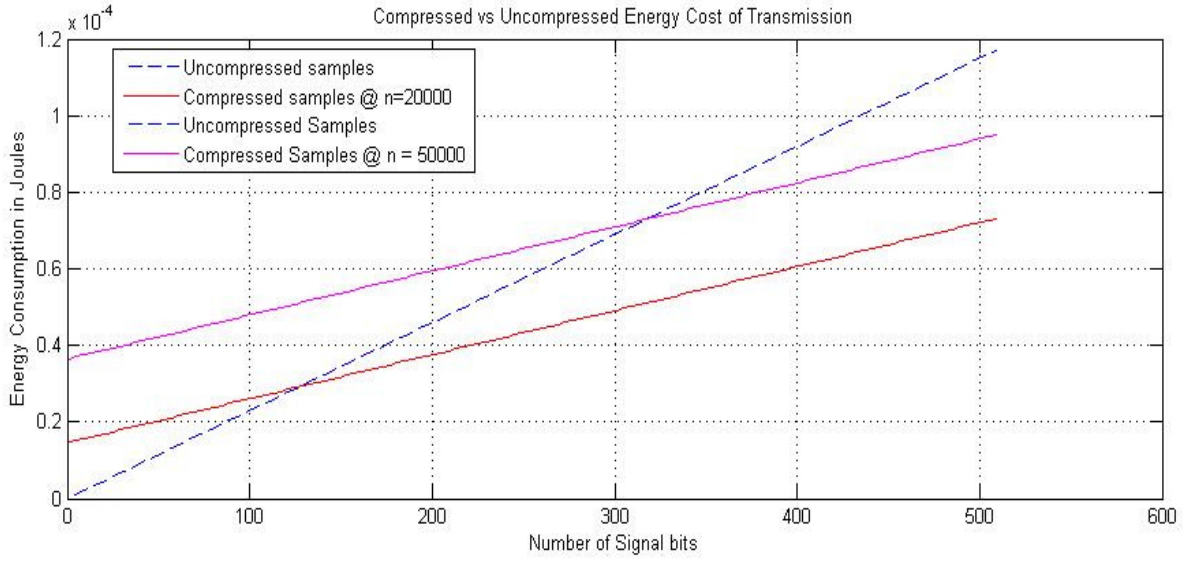


Fig 4: The CS compressed Vs uncompressed transmitted energy cost @ n = 20,000 and 50,000.

Consequent to the variations in the capabilities of different microprocessor and the number of clock cycles required to perform CS algorithms, Fig. 3 shows the minimum data rates required for the application of CS algorithm on M2M communications devices to be energy efficient. Fig. 2 and 3 are derived from Equ.(20) and (21) which can be used for evaluating the data rates in a BPSK scenario, while Equ.(22) and (23) can be used in evaluating the data rates at which the applications of CS algorithm on M2M communication devices become energy efficient in MIMO scenarios. As can be seen in the Fig 3, when the number of clock cycles is increased to 20000, the data rate at which compression becomes energy efficient is 127 bits and at 50000, the data rate becomes approximately 317.

VI. CONCLUSION

The proposed model has become handy for M2M/IoT communications experts to use in evaluating based on the throughput requirement of various M2M / IoT applications, the rates at which the application of the CS algorithm on the wireless devices becomes energy efficient. The higher the computational energy cost for executing CS algorithm on the wireless node, the higher the throughput at which the application of CS algorithm becomes energy efficient. The values used for $e_{tb}$is based on WSN with a range of 100m, the value is more in the range of 4Km. Though, it is imperative to note that the application of CS on any of the applications is subject to the recoverability error performance of such signal on the receiver.

REFERENCES

[1] Ericsson, "More than 50 Billion Connected Devices," Ericsson, 2011.

[2] G. B. Richard, "Compressive Sensing," IEEE Signal Processing Magazine, 2007.

[3] A. R. Mohammad and D. Simon, "Energy - Efficient Sensing in Wireless Sensor Networks Using Compressive Sensing," *Sensors,* vol. 14, no. 2, pp. 2822 - 2859, 2014.

[4] W. Webb, Understanding Weightless: Technology, Equipment, and Network Deployement for M2M Communications in White Space, Cambridge: Cambrige University Press, 2012.

[5] Weightless, "Weightless Core Specification V1.0," Weigtless SIG, Cambridge, 2013.

[6] S. Ajah, A. Al-Sherbaz, S. Turner and P. Picton, "Sub 1 GHz M2M Communication Standardization: The Advancement in White Space Utilization in Enhancing the Energy Efficiency," in *PGNET*, Liverpool, 2014.

[7] Weightless SIG, "New Weightless-N IoT Standard Launches," Weightless SIG, Cambridge, 2014.

[8] Weightless SIG, "Weightless Core Specification V1.0," Weightless SIG, Cambridge, 2013.

[9] S. Sandra, L. Jaime, G. Miguel and J. F. T., "Power saving and energy optimization techniques for Wireless Sensor Networks," *Journal of Comunications,* vol. 6, no. 6, pp. 439 - 458, 2011.

[10] H. Mark, J. L. Michael, B. David and W. Gu-Yeon, "Survey of Hardware Systems for Wireless Sensor Networks," *Journal of Low Power Electronics,* vol. 4, pp. 1 - 10, 2008.

[11] G. P. Halkes, T. Van-Dam and K. G. Langendoen, "Comparing energy-saving MAC protocols for wireless sensor networks," *ACM Journal on Mobile Networks and Applications,* vol. 10, no. 5, pp. 783 - 791, 2005.

[12] B. Waheed, H. Jarvis, S. Akbar and N. Robert, "Compressive Wireless Sensing," in *5th International Conference on Information Processing in Sensor Networks*, ACM, 2006.

[13] U. B. Waheed, D. H. Jarvis, M. S. Akbar and D. N. Robert, "Joint Source - Channel Communication for Distributed Estimation in Sensor Networks," *IEEE Transactions on Information Theory,* vol. 53, no. 10, pp. 3629 - 3653, 2007.

[14] A. D. Mark, F. D. Marco, Y. C. E. and K. Gitta, Introduction to Compressive Sensing, Stanford: Stanford.edu, 2011.

[15] L. Heung-No, Introduction to Compressed Sensing: With Coding Theoretic Perspective, GIST Korea, 2011.

[16] D. Keith, Z. Frank and S. Samuel, "Hardware Decompression for Compressive Sensing Applications," 2009.

[17] H. Zhu, L. Husheng and Y. Wotao, Compressive Sensing for Wireless

Networks, Cambridge: Cambridge University Press, 2013.

[18] B. K. Natarajan, "Sparse Approximate Solutions to Linear Systems," *Society for Industrial and Applied Mathematics,* vol. 24, no. 2, pp. 227 - 234, 1995.

[19] H. Zhu, L. Husheng and Y. Wotao, Compressive Sensing for Wireless Networks, Cambridge: Cambridge University Press, 2012.

[20] A. R. Mohammad and D. Simon, "Energy-Efficient Sensing in Wireless Sensor Networks Using Compressed Sensing," *Sensors,* vol. 14, pp. 2822 - 2859, 2014.

[21] M. N. Halgamuge, M. Zukerman and K. Ramamohanarao, "An Estimation of Sensor Energy Consumption," *Progress In Electromagnetic Research ,* vol. 12, no. B, pp. 259 - 295, 2009.

[22] J. Raha, G. R. Antonio and G. M. P. O'Hare, "Radio Sleep Mode Optimization in Wireless Sensor Networks," *IEEE Transactions on Mobile Computing,* vol. 9, no. 7, pp. 955 - 968, 2010.

[23] S. Stan, K. Saleem and M. Q. W. Halpem, "Wireless Sensor Networks," University of Melbourne Lecture Notes, Australia, 2005.

[24] Z. Davide, M. Borja, V. Ignasi and R. Michele, "To Compress or Not To Compress: Processing vs Transmission Tradeoffs for Energy Constrained Sensor Networking," *arXiv Ad Hoc Networks,* pp. 1 - 14, 2012.

[25] Department of Physics & Astronomy - University of Hawaii, "Receiver Sensitivity / Noise," Department of Physics & Astronomy - University of Hawaii at Manoa, Manoa.

[26] Cooper Crouse-Hinds, "Wireless Connectivity," Cooper Crouse-Hinds.

[27] N. Zia and I. A. Muhammad, "Pathloss Determination Using Okumura-Hata Model and Cubic Regression for Missing Data for Oman," in *International MultiConference of Engineers and Computer Scientists*, Hong Kong, 2011.

[28] H. Jaroslav and P. Pavel, "Penetration Loss Measurement and Modelling for HAP Mobile Systems in Urban Environment," *EURASIP Journal on Wireless Communications and Networking,* vol. 2008, no. 543290, pp. 1 - 7, 2008.

[29] L. M. Feeney and N. Martin, "Investigating the Energy Consumption of a Wireless Network Interface in Ad Hoc Networking Environment," 2001.

[30] R. Zimran, s. Boon-Chong and A. Al-Anbuky, "Perforamce Analysis of Cooperative Virtual MIMO Systems for Wireless Sensor Networks," *Sensors,* vol. 13, pp. 7033 - 7052, 2013.

[31] Z. Davide, M. Borja, V. Ignasi and R. Michele, "To Compress or Not To Compress: Processing vs Transmission Tradeoffs for Energy Constrained Sensor Networking," *arXiv Ad Hoc Networks,* pp. 1 - 14, 2012.

[32] C. Jeremy, D. Ahmed, A. Oskar and M. Pascal, "TamaRISC-CS: An Ultra-Low_Power Application-Specific Processor for Compressed Sensing," Santa Cruz, CA, 2012.

Terrain Effects on Path Loss Models

Kolawole Oluwaseun I
Department of Telecommunication Science
University of Ilorin
P.M.B. 1515 Ilorin, Kwara State, Nigeria
isaackolawole93@gmail.com

Nasir Faruk
Department of Telecommunication Science
University of Ilorin
P.M.B. 1515 Ilorin, Kwara State, Nigeria
faruk.n@unilorin.edu.ng

***Abstract*—In this paper, the effects of terrain on electromagnetic wave propagation in the VHF band was investigated using two transmitters both operating in the VHF frequencies. For each transmitter, five different routes were covered simultaneously within the metropolises. The measurement results were compared with the prediction of five propagation path loss models, a localized model called "Ilorin Model" was also tested. Furthermore, Digital Elevation Model (DEM) for the prediction errors for the models was developed. This was achieved through the use of Contour lines extracted from the Advanced Spaceborne Thermal Emissions Radiometer (ASTER) Image and Global Digital Elevation Model (GDEM) Datasets. The Contour lines extraction and DEM generation were developed using ArcGIS 3D Analyst Tools extension which exist within the ArcToolbox in ArcGIS, ArcMap and the visualization was achieved in ArcGIS ArcScene software environment. Simulation results and the DEM show that the terrain elevation have significant impacts on the errors.**

Keywords: Path loss, Terrain, ArcGIS, Elevation model.

V. INTRODUCTION

Path loss is the reduction in power density of an electromagnetic wave as it propagates through space. Some models include many details of the terrain profile, contours height, environment (urban or rural, vegetation and foliage) to estimate the propagation. Some uses carrier frequency, distance, antenna heights and other critical parameters. The transmission path between the transmitter and the receiver can vary from simple direct line of sight to one that is severely obstructed by buildings, foliage and the terrain. Many path loss models (e.g. COST 231 Model, EGLI model, Ericsson model, and HATA Model) are available to predict the propagation loss, the weaknesses of the existing path loss models is compatibility issues due to different in environment and terrain structure between where they were developed and others environment where they need to be utilized . Therefore it is very important to thoroughly understand the propagation characteristics and develop a channel model for the proposed wireless communication system before site-specific planning and deployment can be initiated. The main aim of this work is to investigate how terrain affects the performance of path loss models in the broadcast frequencies within Ilorin Metropolis.

VI. RELATED WORK

There are quite a lot of published research papers that worked on analyzing the efficacy of path loss models. In such cases, the authors often collect measurement data in an environment of interest and make an assessment of whether the models fit in. In [1], 30 propagation models considered. Large scale field measurement was taken in the rural and urban environments. In the end, it was established that no single path loss model was able to predict path loss consistently. In [2], a mobile propagation path loss studies was conducted in the VHF/UHF bands in Southern India. In the work, field strength was measured at 200, 400 and 450 MHz and the result shows that HATA'S prediction model gave better result in all cases. In [3] ten empirical path loss models were assessed in the UHF and VHF band in Ilorin, Nigeria. Also [4] provides a comparison of empirical propagation path loss models for fixed wireless access systems based on readings conducted in Cambridge, UK. It was found that, among all the models, ECC-33 model, Stanford University Interim (SUI) model, and COST-231 model are the most suitable and that the SUI model shows quite a large mean prediction error for the area.

VII. DATA COLLECTION

The propagation measurements were conducted in Ilorin (Longitude 4^o 36' 25"E, Latitude 8^o 25' 55''N) and some towns surrounding the city within Kwara State, Nigeria. Five different routes were covered during the measurement period. A dedicated Agilent N9342C 100 Hz-7 GHzspectrum analyzer having a GPS (Global Positioning System) device was placed inside a vehicle while the GPS device was attached to the roof on the vehicle and was driven at an average speed of 40 km/h along these routes, reading were taken during transmission time. Two transmitters were considered, NTA transmitting on 203.25 MHz and Harmony FM operating on 103.5MHz both in the VHF band.

A. Path loss models considered

Five models were considered in this work:

1) Hata Model

Hata Model [5] is a mathematical formulation of the graphical path loss data provided by Okumura but the model is valid between the range 150 MHz to 1500 MHz, the model transmission distance is less than or equal to 20 km. HATA

gave the propagation formula and provided correction factors. The propagation formula is given by:

$$L_{Hata} = 69.55 + 26.16 \log f_c - 13.82 \log h_t - a(h_r) + (44.9 - 6.55 \log h_t) \log d \quad (1)$$

Where; L_{Hata} is the path loss (in dB), f_c is the transmitting frequency (in MHz), h_t is the transmitter height in meters, h_r is the receiver height in meter and d is the distance between the transmitter and receiver (in km) and $a(h_r)$ is the correction factor for the receiver height given by:

$$a(h_r) = (1.1 \times \log f_c - 0.7)h_r - (1.56 \times \log f_c - 0.8)dB \quad (2)$$

2) Egli Model

In [6] measurement was performed between the frequency of 90 MHz to 1000 MHz over irregular terrain. It was decided that the median signal level in a small area follows the inverse fourth-power law. This attribute is similar to the plane earth propagation model but there was an excess loss over the plane earth model. Egli Path loss model is given as follows:

For $h_r \leq 10$

$$L_{(dB)} = 20 \log f_c + 40 \log d - 20 \log h_t + 76.3 - 10 \log h_r \quad (3)$$

For $h_r \geq 10$,

$$L_{(dB)} = 20 \log f_c + 40 \log d - 20 \log h_t + 85.9 - 10 \log h_r \quad (4)$$

Where; $L_{(dB)}$, f_c, h_t, h_r and d is as given in Hata Model

3) Cost 231 Model

The European co-operative for scientific and technical research formed the Cost 231 committee to develop an extended version of the Hata Model such that it can be used for frequency of up to 2 GHz. Path loss of this model is computed as:

$$L = 46.3 + 33.9 \log f_c - 13.82 \log h_r - a(h_r) + (44.9 - 6.55 \log h_r) \log d + C_m \quad (5)$$

C_m = 0 dB for medium sized city and suburban areas, and 3 dB for metropolitan centers, while $a(h_r)$ is defined as in "(2)" This combination is called "COST 231 Model" [7]

Where; $L_{(dB)}$, f_c, h_t, h_r and d is as given in Hata Model

4) Ecc-33 Model

ECC-33 model infers the original measurements data by Okumura and modifies the model factors to suit fixed wireless systems. The model gives correction factor for urban and medium cities. The model is considered more suitable for European cities and is as defined in [4] as.

$$L(dB) = A_{fs} + A_{bm} - G_b - G_r \quad (6)$$

$$A_{fs} = 92.4 + 20 \log f_c + 20 \log d \quad (7)$$

$$A_{bm} = 20.41 + 7.894 \log f_c + 9.83 \log d + 9.56 \quad (8)$$

$$G_b = \log(h_T/200)\{13.958 + 5.8 [\log d]^2\} \quad (9)$$

For medium size city

$$G_I = [42.7 + 13.7 \log f_c] \quad (10)$$

Where; A_{fs} is free space attenuation, $A_{bm}$is basic median path loss, G_b is BS height gain factor and G_r is receiver antenna height gain factor.

5) Ilorin Model

This is an extension and optimization model derived from Hata and Davidson model developed in the University of Ilorin, it was design to suit the Ilorin and Nigeria environment. Ilorin Model is given in [8] as:

$$L_{ILORIN}(dB) = 73.56 + 26.16 * 10 \log f_c - 13.82 * 10 \log h_t + 30.5 * 10 \log d + C \quad (11)$$

Where; $L_{(dB)}$, f_c, h_t, h_r and d is as given in Hata Model

C is the correction factor given in Hata-Davidson model as:

$$C = A(h_t, d_{km}) - S_1(d_{km}) - S_2(h_t, d_{km}) - S_3(f_{MHz}) - S_4(f_{MHz}, d_{km}) \quad (12)$$

For $d < 20km$

$A(h_t, d_{km}) = 0$; $S_1(d_{km})$=0

For $20km \leq d < 64.38km$

$S_1(d_{km})$=0;

$A(h_t, d_{km})$= $0.62317(d - 20)[0.5 + 0.15 \log(h_t/121.92)]$

For $64.38km \leq d < 64.38km$

$S_1(d_{km}) = 0.174(d - 64.38)$;

For $20km \leq d < 300km$

$A(h_t, d_{km})$= $0.62317(d - 20)[0.5 + 0.15 \log(h_t/121.92)]$

$for h_T < 300m$

$S_2(h_t, d_{km})$= $0.00784|\log(9.98/d)|h_t - 300$

$$S_3(f_{MHz}) = \frac{f}{250 * \log 1500/f}$$

$S_4(f_{MHz}, d_{km}) = [0.112 \log 1500/f](d - 64.38)$

$A(h_t, d_{km})$and$S_1(d_{km})$ are distance correction factors, $S_2(h_t, d_{km})$ is transmitter height correction factor, $S_3(f_{MHz})$ and $S_4(f_{MHz}, d_{km})$ are frequency correction factors.

B. Field Strength Measurements Considered

1) Received Signal Strength

In mobile and broadcast communication, received signal strength is a measurement of power present at the receiver or userend. Signal strength between transmit station and receiver must be greater than threshold value to sustaingood signal quality at the receiver end. During our field work the Received Signal Strength (RSS) were taken and recorded by the spectrum analyzer for the various transmit station used. Received Signal Level for the various path loss models were calculated as:

$$P_{rsl} = T_x - L_m \quad (13)$$

Where; $P_{rsl}$is Received signal Level in dB, T_x is transmitted power of the base station in dBm, L_m is total path loss in dB for the various model in dB.

2) Prediction Error

In mobile and broadcast communication, prediction error is calculated using path loss models to get the range of error that can occur between transmit station and receiver, which can be caused as a result of signal attenuation. The prediction error calculate the expected distance between what our predictions for specific value of the Received signal Level (RSL) and what the true value should be.

Also, Prediction error must not be too high, when too high it can cause the receiver receiving very weak signal.The prediction error for the various path loss were calculated as:

$$P_e = P_{rsl} - P_{rss} \quad (14)$$

Where; P_e is Prediction error in dB, $P_{rsl}$is Received signal Level in dB as in (13), P_{rss} is Received Signal Strength in dB.

C. Measurement equipment

Fig. 1. Measurement Experiment Set up.

TABLE 1
MEASUREMENT EQUIPMENT AND CONFIGURATION.

Spectrum Analyzer N9342C Agilent, 100 Hz- 7 GHz	
Displayed average noise level (DANL)	-164 dBm/Hz
Preamplifier	20 dB
Resolution bandwidth (RBW)	10 kHz
Receiver Antenna: Diamond RH 795	
Frequency range	70 MHz-1 GHz
Height	1.5 m
Gain	2.51 dB

D. Result with Practical Data

1)

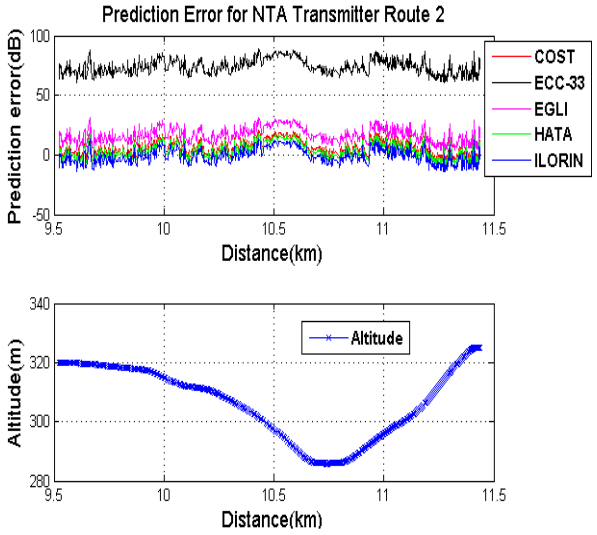


Fig. 2. Prediction Error against distance and Altitude against distance graph NTA Transmitter for Route 2

2)

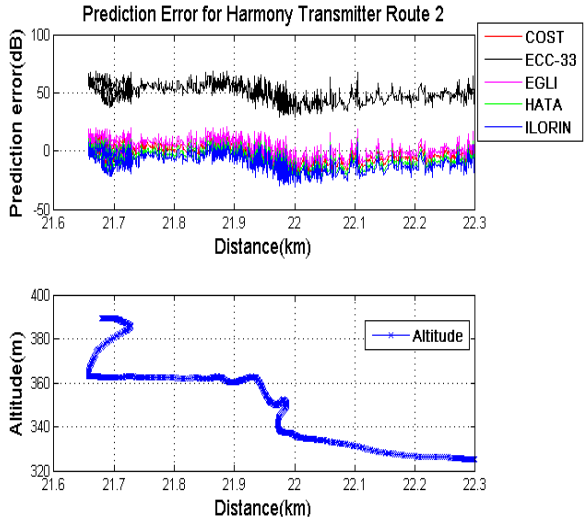


Fig. 3. Prediction Error against distance and Altitude against distance graph Harmony Transmitter for Route 2.

3)

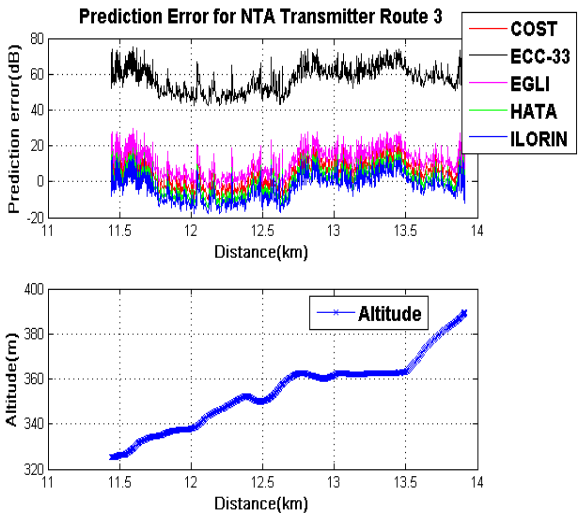


Fig. 4. Prediction Error against distance and Altitude against distance graph NTA Transmitter for Route 3.

4)

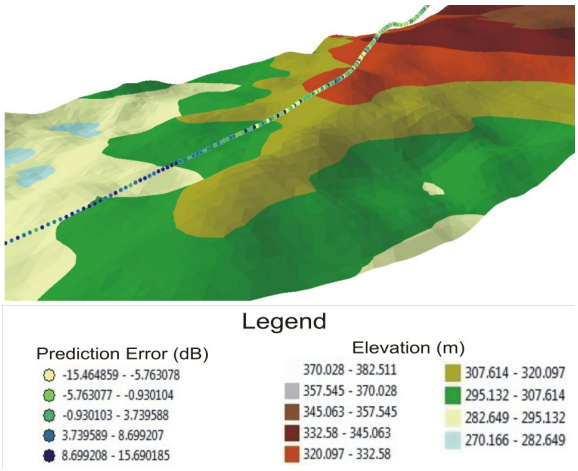


Fig 5. Prediction Error of Ilorin Model (Localized Model) for NTA Transmitter along route 4.

5)

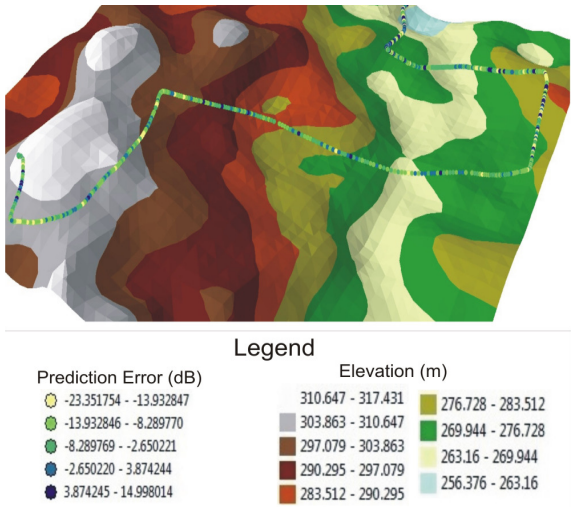


Fig 6. Prediction Error of Ilorin Model (Localized Model) for Harmony Transmitter along route 5.

E. Analysis

Fig. 3, 4 and 5 shows the prediction error against distance and Altitude against distance graph. It can be seen that the prediction Error follows the pattern of the Altitude.

Fig. 5 and 6shows the prediction error map and terrain elevation for routes 4 and 5 generated in 3D. This was developed by plotting the prediction error positions coordinates over the Digital Elevation Model (DEM). The DEM was developed from the Contour lines extracted from the Advanced Spaceborne Thermal Emissions Radiometer (ASTER) Image and Global Digital Elevation Model (GDEM) Datasets. The Contour lines extraction and DEM generation were developed using ArcGIS 3D Analyst Tools extension which exist within the ArcToolbox in ArcGIS ArcMap

Software package. This visualization was achieved in ArcGIS ArcScene software environment. Simulation results shows that the terrain elevation have significant impacts on the errors.

F. Conclusion

Results obtained shows that terrain has significant effects on the path loss models. However, ILORIN model gives the least prediction error in the environment covered.

ACKNOWLEDGMENT

This research is supported by the Communication and Network Research group (CNRG) of the department of Telecommunication Science, University of Ilorin, Nigeria.

REFERENCES

[1] Phillips C, Sicker, D and Grunwald, D., "Bounding the practical error of path loss models" International Journal of Antennas and Propagation Vol. 2012 (2012), Hindawi, pp 1-21, doi:10.1155/2012/754158.

[2] Fujitani. T., Tamisato. T., and Hata. M 'Experimental Study of Mobile Propagation Loss Correction Formula for a Slope Terrain Area', *in Proc. IEEE, Vehicular Technology Conference*, 72nd, p. 1-5 (2010).

[3] Faruk N., Ayeni A. A., and Adediran Y. A., "On the study of empirical path loss models for accurate prediction of TV signal for secondary users," Progress In Electromagnetics Research B, Vol. 49, 155 -176, 2013.

[4] Abhayawardhana., V.S, Wassell I.J, Crosbsy., D, Sellars M.P and Brown., M.G, "Comparison of empirical propagation path loss models for fixed wireless access systems" IEEE Vehicular Technology Conference, Vol. 1, pp 73-77, Spring. (2005).

[5] M. Hata, "Empirical formula for propagation loss in land mobile radio services," *IEEE Trans. Vehicular Technology.*, Vol. 29, No. 3, pp. 317–325, Aug. 1980.

[6] Egli, J.J., "Radio Propagation above 40 MHz over irregular terrain", *Proc IRE*, Vol. 45, No. 10, pp 1381-1391, (1957)

[7] COST 231,"Urban transmission loss models for mobile radio in the 900 and 1800 MHz bands (revision 2)." COST 231 TD (90) 119 *Rev*. 2, The Hague, the Netherlands. Sept, (1991).

[8] N .Faruk, A.A.Ayeni,Y.A. Adediran and N.T Surajudeen, " Improved Path Loss Model for Predicting DTV Coverage" *Int. J. Wireless and Mobile Computing, Vol. 7, No. 6, pp 565-576, 2014.*

Mobile Spamming in Nigeria: An Empirical Survey

Oluwafemi Osho*, Victor Legbo Yisa, Olasunkanmi Yusuf Ogunleke, and Shafi'i Muhammad Abdulhamid

Department of Cyber Security Science,
Federal University of Technology, Minna
*Corresponding Author: femi.osho@futminna.edu.ng

***Abstract*—Spamming has attained a global dimension and continued to maintain an upward trend, both in sophistication and frequency. And, so far, it has defied every effort, including technical and non-technical proposals, to curb it. This study seeks to investigate the prevalence of spam SMS, with focus on Nigeria. To quantify the prevalence, primary data was collected using questionnaire. Out of 270 surveyed, the responses of 191 mobile users were valid and analyzed. The study revealed that all mobile subscribers receive spam SMS, receiving an average of 2.45 spam SMS daily. This implies an average of 334,857,685 spam SMS received daily in Nigeria. However, most are for commercial purposes. Few mobile users report cases of fraudulent spam SMS, including those with SMShing intent, to network providers or security agencies. Most believe customers of mobile networks should reserve the right to determine the type of unsolicited SMS to be received, and unsolicited advertorial/promotional SMS should be regulated. Current guidelines and regulations need to be reviewed, to effectively manage spamming activities in Nigeria**

Keywords—Spam, SMS, Unsolicited, Mobile, Telecommunication, Spam Detection

I. INTRODUCTION

Since the turn of the century, there has been a drastic growth in the wireless communication industry, as there is a clear shift from the fixed telephone system to the more flexible but robust wireless mobile communication. An announcement made by the International Telecommunications Union (ITU) opined that the number of active cell phones would reach 7 billion by 2014 [1]. Nigeria, a developing country, has witnessed a much more agile development in the mobile industry. By 2012, it had over 110 million subscribers, and was ranked as the tenth country with the highest number of mobile telephony subscribers [2].

GSM growth in Nigeria has continued to maintain an upward trend. The number of subscribers, from 2007, just within a 7 year span, more than tripled [3]. Corresponding to the increase in mobile users in the country is increment in mobile users' activities which include, but not limited to, sending and receiving messages, making calls, sending and receiving emails, accessing the internet, and download applications. Because of its robustness, flexibility, and affordability, mobile communication in the country has attracted a whole lot of benefits. However, the country has had her share of setbacks associated with mobile telecommunication. One of these is sending unsolicited short messages (SMS) in bulk quantity to many mobile users, also known as SMS spamming.

There are varying definitions to spamming. Also, there is no agreed international definition for illegal spamming, as definitions from Australia differ from that of the European Union and United States. According to [4], spamming is an unsolicited electronic message which includes, but is not limited to, emails, short messaging service (SMS), Voice over IP (VoIP), instant messages from chats; usually, spam is sent in bulk for commercial or other purposes, and indiscriminately. Also, the messages sent are identical.

Spamming has become a gigantic problem to almost all sectors of the economy, causing loss of revenue to internet service providers (ISP), and users of these facilities generally. Due to its anonymous nature, spammers are often protected from being held responsible for their actions, as it is always difficult to identify them [5].

Many studies have focused on different aspects of mobile spamming, including detection and filtering [6], [7], [8], [9]; mitigation [10]; and spam laws and regulations [11], [12], [13]. Only very few have focused on quantitative and/or qualitative assessment of the state of mobile spamming [14]. As far as we know, only two studies have provided sparse information on the state of mobile spamming in Nigeria [3], [15]. In both surveys, spamming was not the primary focus. We therefore pose the following questions: how prevalent is SMS spam in Nigeria's mobile telecommunication sector? What categories of SMS spam are most prevalent? Have mobile users been experiencing SMS spam with fraudulent intentions? What are mobile users' perceptions on regulation of the sector?

The aim of this study is to investigate the prevalence and nature of SMS spam in Nigeria's mobile telecommunication sector. Khong [13] highlighted the fact that the issue of spam is not all about contents. The fact that spam is undesirable to its recipients, and could constitute considerable overheads for service providers, necessitates relevant studies to measure its prevalence. This could aid relevant regulatory bodies in developing appropriate containment measures.

Other sections of this paper are organized as follows: In section 2, we present a review of related literatures. In section 3, we describe the research methodology and then present the results in section 4. We discuss the preceding results in section 5 and then draw our conclusions in section 6.

II. LITERATURE REVIEW

G. Short Message Service (SMS)

Short Message Service (SMS) is a type of mobile communication system that utilizes the use of standardized protocols for exchange of text messages between mobile devices [16]. SMS is usually a maximum of 160 characters and is sent wirelessly to another mobile device user.

When a user sends a mobile SMS from his device, the message goes to the Short Message Service Centers (SMSC) [17]. The SMSC is usually maintained by the mobile network operator, and sends a message of maximum payload of 140 octet, thereby making the SMS maximum number of characters to be 160. Email-based SMS are directed to the SMS-gateway otherwise known as the SMSG. The SMSG on receiving the email-based SMS, routes it to the SMSC, which then sends it to the receiver device.

The SMSC operates either through a store and forward or a forward and forget method. It also utilizes Home Location Registry (HLR) to retrieve information about the receiving devise Message Service Centre (MSC), through which it delivers the message to the recipient.

Texting, otherwise known as Short message service (SMS), has become a popular means of mobile communication. Mobile subscribers send in excess of 200,000 SMS text messages every second [18]. For example, over 500 million SMS were sent to celebrate the New Year in France [19].

An increasing bandwidth for communication and a relatively low cost of sending SMS has been one of the major factors for its popularity [20]. According to Portio research, SMS usage was worth 200 billion dollars as at year 2011, and is estimated to surpass 300 billion United States dollars at the end of 2014 [16].

Another factor that has helped to increase SMS adoption is the relative level of trust and acceptance around the world that sending of SMS via mobile phones engenders. For instance, some financial institutions adopt its use even for payment authorization [21]. Many organizations have adopted using SMS for mobile advertising to inform its consumers of products and services appropriately. Unfortunately, spammers have been leveraging on these factors to exploit mobile users.

H. SMS Spam

Aside from being sent from mobile devices, spam SMS's have similar features with spam emails: they are unsolicited for by the receiver, sent for commercial or financial purposes and are sent indiscriminately in bulk form [17]. They could also be utilized for malicious purpose [10]. Due to the personal nature of mobile devices, SMS spam messages coming in will always draw the attention of the user, who is forced to open such messages, thereby intruding into such user's privacy. And the fact that some mobile telephone operators charge users for receiving messages only helps to compound the frustration experienced by users.

Generally, spam messages users receive on their mobile devices can be said to emanate from three major sources, viz. mobile network operators and groups that have paid the mobile network operator, groups that do not pay the mobile network operator yet send spam SMS, and user originated messages that are inconvenient to the receiver [20].

According to [21], based on the intention of the spammer, mobile messaging attack can be said to be of three major types: SMS spam, premium rate fraud, and SMShing.

SMS spam is such that unsolicited messages are indiscriminately sent to mobile subscribers for advertising hoax. In Nigeria, such SMS's encourage one to forward a message to all of his contacts, in order to get some airtime. For example,*"MTN national protocol is celebrating his birthday today. Send this message to 15 people and get N750 recharge card.sms is free."* Messages similar to this have also become very common on social media sites.

Premium rate frauds are spam messages that trick mobile network users to call some certain numbers where they could be defrauded, or are made to make expensive subscriptions that are billed from their account. An example of such fraudulent SMS received from an MTN Nigeria line reads:

> *LACASERA DRINK:congrats!you emerged winner of #300,000 from our 10th annual promotion code No MTN3).Call MR LARRY ON 08131921656 FOR CLAIMS.*

SMShing is the mobile form of phishing where baits are embedded in text messages to extract mobile users' personal information. This personal information is then used for purposes ranging from adverts to fraudulent activities. An example of a smishing *SMS: "MASTERCARD ALERT: Your CARD starting with 5110 has been DEACTIVATED. Please contact us at 361-400-xxxx."* A mobile device user that calls the number in the SMS is answered by an automated machine, which then extracts information from the user. Other types include links that directs the user to a website where personal information is requested.

I. SMS Spam in Nigerian and Other Countries

Cheaper SMS cost and increasing profit on spam messages has led to high rise in spam messages emanating from the United States. A research by [22] reports that 79% of Americans with a mobile phone send and receive SMS on their phones, and 69% of all mobile text senders claim that they receive unsolicited unwanted messages on their mobile device. An analysis of all the types of spam sent in the United States and United Kingdom is shown in Figure 1.

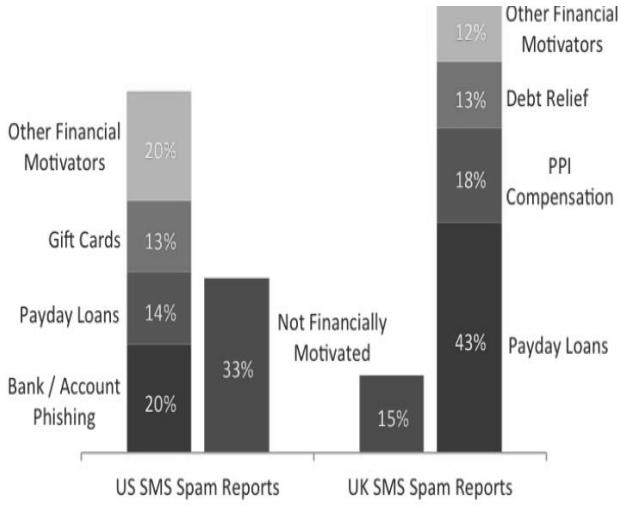


Figure 1: Categories of Spam Messages received in the UK and USA in 2013 (Source: [23])

About 67% of the spam messages received in the United States used money as their pitch with only 33% not financially motivated. Phishing forms the most observed motivation of attackers. On the other hand, in the UK, it was payday loans. Payday loans only accounted for 14% of SMS spam in the US.

A survey conducted on behalf of the Direct Marketing Association (DMA) in 2012 reported that about 9 million spam mobile messages are received every day in the UK [24], [25]. This implies that over 3.29 billion spam messages were sent in the year 2012 in the UK alone. The increasing nature of spam in the UK has reduced user trust in the security of their mobile devices. At least 19.1% of respondents in a survey admitted that SMS is less secure; a phenomenon attributed to the increase in SMS spam [26]. In most western countries, mobile subscribers view SMS spam as an intrusion to their privacy, thereby causing them to call the network operators for complaints.

The menace of SMS spam is becoming increasingly prevalent also in east countries, including China, Korea, and Japan. A Chinese mobile user, it was reported, experienced more than 8.3 SMS spam weekly [27]. Up to 30% of daily SMS received in Asia are spam [19].

With subscribers running over 120 million, spammers have been able to identify that they could reach more mobile targets in Nigeria. The rate at which Nigerian mobile subscribers have been receiving spam messages are on the increase. A consumer satisfaction survey suggests that 94% of mobile users use SMS in Nigeria, and 77% of the respondents claim to have been receiving SMS spam [28]. Mobile Subscribers in the country have been receiving barrage of different type of unsolicited SMS ranging from network operators' promotions adverts to unsolicited messages urging subscribers to subscribe to a particular type of service. A recent survey by the security firm Gemalto suggests that up to 80% of Nigerians are annoyed when they receive SMS spam on their mobile device [15]. Many Nigerian telecoms consumers have expressed discontent over the absence, in most of the spam messages, of option to opt out.

J. Guidelines, Regulations, and Legislation on Spam

The incessant spam SMS received by mobile network subscribers had led to the Nigerian Communication commission (NCC), the communication regulatory body of the country, to direct that all mobile network operators will have to comply with the commission's guidelines on bulk messaging. It warned it would not hesitate to wield the big stick on any erring mobile network provider [29]. Currently, there are no comprehensive guidelines or legislations solely developed for regulating spamming activities in Nigeria. However, there are guidelines and regulations, by Nigeria Communications Commission, that indirectly affect these activities. Examples include Guidelines on Advertisements and Promotions [30]; Competition Practices Regulations, 2007 [31]; Consumer Code of Practice Regulations, 2007 [32]; Guidelines on Short Code Operation in Nigeria [33]; and Quality of Service Regulations, 2012 [34]. Others include bills being drafted by the National Assembly, including Cyber Security and Data Protection Agency Bill, 2008 [35], and Cybersecurity Bill, 2011 [36].

A critical analysis of the documents reveals guidelines, regulations, and legislations that address aspects of mobile spamming, including identification of message sender, purpose of communication, pricing and charges, and penalties for offenders. For instance, the Guidelines on Short Code Operation in Nigeria [33] mandate that, for all advertisements, content provider must provide information displaying its name, telephone numbers and contact details. In addition, all terms and conditions, including pricing information; and whether service is or is not a subscription, must be clearly displayed. The Consumer Code of Practice Regulations [31] emphasizes that the purpose of the communication must equally be added at the beginning of the communication. The Guidelines on Advertisements and Promotions [30] emphasized the aspect of pricing and charges more clearly. This document, which specifies minimum standards and requirements for advertisements and applications for promotions stipulates an unambiguous communication of prices and financial implications, and "no hidden or disguised price adjustments, discounts, unrealistic price comparisons or exaggerated claims as to worth or value." In addition, as contained in Part II of the Consumer Code of Practice Regulations, 2007 [32], the service provider is expected to provide information regarding frequency of charges, and the subjectivity of such charges to change from time to time.

In recognition of mobile users' rights, the Commission mandates service providers to provide mechanisms for users to subscribe or discontinue subscription to their services. This regulation is contained in two of the documents. In [33], service providers are required to display consumer right to 'opt in' or 'opt out' of service, promotion, or programme regardless of whether such is subscription based or not. The equivalent regulation in [34] specifically addresses unsolicited messages. Service providers are mandated to provide option to recipients to 'opt out' of receiving unsolicited messages.

While the existing documents clearly relate to service providers within the country, it is not impossible for spammers to use external sources – means and providers outside the country. To mitigate spamming via external sources, NCC requires service providers to "make reasonable effort to identify and block or filter bulk, unsolicited and offensive messages from other sources" [34].

As a way of deterrent to potential offenders, some documents include penalties for erring service providers or communication sources. For instance, for advertisements, according to [30], non-provision of required information or provision of false or misleading information attracts a fine of ₦1,000,000 per violation. A fine of not less than ₦500,000 or imprisonment of not less than 3 years or both, for any person sending spam electronic mail messages to recipients with whom there is no prior commercial or transactional relationship is proposed in [35]. On the other hand, [36] recommends a minimum fine of ₦10,000,000 or a term of 5 years in prison or both fine and imprisonment, if the message is fraudulent.

Unfortunately, the level of compliance with these existing regulatory guidelines has been very low; senders of unsolicited SMS have continued to flout the provisions. For instance, NCC declared early in 2014 that mobile network operators should restrict sending of unsolicited messages on the networks to between 8.00 am and 8.00 pm [37]. However, this has not proved effective as mobile subscribers still receive unsolicited SMS even during these restricted periods. On June 8, 2015, one of the authors received a message from MTN (with the sender code 'MTNN'):

> *Hello, Oluwafemi, Esther has sent you a message on Facebook. Dial *510*55# to check Facebook messages without internet charges*

The first impression of the recipient, as a result of the clause "without internet charges," was that the service was free. However, upon dialing the supplied number, the network responded with the message:

> *Yello! You have successfully subscribed to Facebook Weekly. You have been charged N25.00 for 7 Days. To use the service dial *510#.*

The first message, obviously, falls short of the minimum standard set by most of the guidelines and regulations. Whilst displaying the purpose of communication, the message did not disclose, in clear terms, information on terms and conditions, including charges, frequency of charges; and did not provide any option for the recipient to 'opt out.'

The above scenario is an example of what has become typical of network operators and other service providers in Nigeria. They are generally indifferent to consumers' rights, and not much is being done to correct the menace. There have been instances where advertisers used flash SMS [10]. Once a recipient presses any key on the mobile device, such mobile user is automatically subscribed to the service being advertised.

It is evident that relevant regulating agency must awaken to their enforcement responsibility. Part of the recommendations contained in the Nigeria Consumer Satisfaction Survey Final Report (Part 1) [28] was directed to the NCC. The recommendations include encouraging operators to provide options to opt out from receiving SMS spam, and clearly publicize the procedures for opting out; show efforts being made to identify, block and filter spam messages; provide a platform for receiving unsolicited messages forwarded by mobile users; collaborate with each other to share best practices; and put mechanism in place to analyze the unwanted messages received, make every effort to identify the senders, and take appropriate action.

K. Theoretical Framework

This study is located around two inter-twined theoretical concepts: privacy and personal information as commodity. Privacy has been defined informally as the 'right to be let alone' [38]. Jerry [39] described privacy from the perspective of space, decision, and information. Leppaniemi & Karjaluoto [40] highlighted some six C's of privacy that every user should be entitled to: choice, control, constraint, customization, consideration, and confidentiality.

While some view privacy as a right, it is seen as commodity by others. Personal information privacy has even been viewed as a property right [41], [42]. For the privacy-as-commodity group, privacy is not the absolute right of anyone, but dependent on cost-benefit analysis and compromise [43]. For instance, while some countries view privacy as fundamental individual right, information privacy within the context of business to consumers was not captured under this fundamentality [44]. With advancements in information technology capabilities, information privacy right is deemed by some to already have vanished [45].

Applying the perspective of [39] in the study's context, in respect of space, privacy refers to a mobile user's cyber-domain, including the mobile device and all its resources, harbored from invasions by unwanted externalities. Viewed from a decision point of view, it connotes a user's individual right or freedom to make decision in the absence of encumbrances. The last concerns the right to mobile information privacy. This form of privacy puts the use of a mobile user's information, say, the mobile number, under his full control. Extending privacy-as-a-property-right model to decision privacy, a proprietor should have the exclusive right to exercise control over the use of the property; for example, determining the quantity and type of commercial messages that he wants to receive.

Some have argued spam as a violation of privacy rights [46]. It violates those entitlements described by [40]. Considering the fact that every mobile user has a right to his/her cyber-domain, spam can also be deemed to invade privacy. For instance, whenever a mobile user receives a spam SMS, such user is expected to open the SMS, with the expectation that it came from a sender acquainted with, and in many cases, read the message. Even if, upon discovering the content to be spam the user deletes immediately the SMS, some significant amount of time had already been expended.

Within the confines of legal norms of the community, spamming is unjustifiable [46]. The mere fact that it is

unsolicited makes it unacceptable. Spamming is coercive. It breaks users' autonomy over their personal cyberspace and cyber-possession, making them "captive audience to another's communication" [46]. Spammers invariably metamorphose mobile users' personal information into currency. In other words, spamming turns privacy into commodity [38].

III. METHODOLOGY

L. Participant

To obtain first hand information on mobile user's experience with spam SMS in Nigeria, primary data were collated. In order to collate data that are more representative of the country, it was necessary to consider population in multiple locations. Stratified cluster sampling was used. This method combines elements of stratification and clustering, combining the cost-saving benefit of clustering with the error reduction of stratification. The basis of clustering was the major geographical divisions of the country: north and south. This was necessitated due the fact that the country is majorly classified along these two regions, with each, in many ways, distinct from the other. Six strata of clusters were then formed based on six geopolitical zones in the country, with three in each of the two main clusters. The clusters in each stratum were states of the federation belonging to each geopolitical zone. Two of the strata were selected for the study, with one selected from each of the two main clusters. From each stratum, two states were picked. This gives a total of four states surveyed.

The research instrument used was questionnaire. 270 questionnaires were distributed. 265 were returned. Out of these, 191 were found to be valid. The invalid ones were due to respondents choosing multiple options where the questions required one option, or not responding appropriately to questions which depended on one or more preceding questions. Those who were not conversant with the term bulk or spam SMS were likewise considered invalid. A mobile user who does not understand what spam SMS is would not be able to complete appropriately the requested information in the questionnaire.

M. Measures

The questionnaire was divided into three parts. The first part covered demographic information, and networks subscribed to. The study essentially focused on users of the four major GSM operators in the country. The second part focuses on analyzing the prevalence and nature of mobile spamming. The last part deals with mobile users' expectations on determining the type of unsolicited advertorial/promotional SMS to be received, and regulation of these categories of SMS.

For the purpose of analysis, both descriptive and inferential statistics were applied on gathered data. The latter was used to identify relationships among the variables. Essentially, only those relationships with statistical significance are reported.

IV. RESULTS

N. Demographic of Mobile Users

62.3% of respondents were male, while the remaining 37.7% were female. Students accounted for more than half of the respondents, with only 7.9% unemployed.

TABLE 1: RESPONDENTS' SEX, OCCUPATION, AND SUBSCRIBED NETWORKS COMPOSITION

	Frequency	Percent
Sex		
Male	119	62.3
Female	72	37.7
Total	191	100.0
Occupation		
Student	114	59.7
Employed	62	32.5
Unemployed	15	7.9
Total	191	100.0
Subscribed Mobile Networks		
MTN	145	97.3
Glo	85	57.0
Airtel	90	60.4
Etisalat	70	47.0

MTN is the most subscribed to network. Average number of network subscription is 2.04 (SD = 0.9). 24.6% maintain subscription to a minimum of three network operators. 16 of the respondents (0.8%), presented in Figure 2, were found to be subscribed to all the four GSM operators in the country. 27.9% of respondents are subscribed to only one of the four networks.

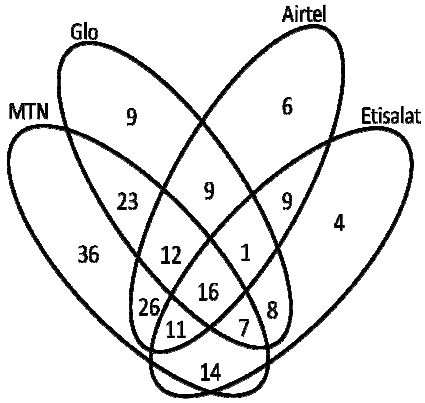


Figure 2: Venn diagram showing network subscriptions.

O. Mobile Users' Experiences with Spam SMS

All respondents reported they use their phones for sending or receiving text messages, and have also received at one time or the other spam SMS. The average amount of spam SMS received daily was found to be 2.45 (SD = 1.3). Most spam SMS are sent on MTN networks, with Airtel as the least used by spammers.

TABLE 2: EXPERIENCE OF MOBILE USERS WITH SPAM SMS.

Experience	Frequency	Percent
Number of bulk SMS received on average daily		
1	54	28.3
2	55	28.8
3	45	23.6
4	19	9.9
5	15	7.9
6	3	1.6
Total	191	100.0
Network on which spam SMS is most received		
MTN	109	57.1
Glo	33	17.3
Etisalat	30	15.7
Airtel	19	9.9
Total	191	100.0
Content of spam SMS most received		
Advertorial	74	38.7
Promotional	74	38.7
Invitational	17	8.9
Congratulatory	24	12.6
Fraudulent	2	1.0
Total	191	100.0
Respondents sending spam SMS		
Yes	83	43.5
No	108	56.5
Total	191	100.0

Spam SMS in Nigeria is mostly used for commercial purpose. Most respondents reported unsolicited mobile messages received are mostly either advertorial or promotional. Only 1% indicated the most dominant were fraudulent messages.

Most mobile users do not engage in sending spam SMS. The study found out being a spammer increases the likelihood of receiving a minimum of three spam SMS daily by 92.8% ($\chi^2(1) = 18.394,\ p = 0.002$). Specifically, 59% of mobile users who send spam SMS receive on average a minimum of three spam SMS daily. Only 30.6% of those who have never sent spam SMS reported getting this minimum daily.

TABLE 3: EXPERIENCE WITH ADVERTORIAL AND PROMOTIONAL SPAM SMS

Experience	Frequency	Percent
Unsolicited advertorial/promotional SMS from network provider		
Yes	175	91.6
No	16	8.4
Total	191	100.0
Unsolicited advertorial/promotional SMS from other sources		
Yes	145	75.9
No	46	24.1
Total	191	100.0

Most mobile users seem to receive unsolicited advertorial and promotional messages more from their network providers than other sources.

Being unemployed was found to significantly increase the likelihood of receiving unsolicited advertorial/promotional SMS from other sources than network providers ($\chi^2(1) = 6.563,\ p = 0.038$). Specifically, all the unemployed mobile users were found to have received this type of spam SMS, compared to 71.1% of those who were students, and 79.0% of employed mobile users.

Even though most respondents receive spam SMS on their MTN network, the study found out that the percentage of those who receive spam advertorial/promotional SMS from sources other than their network providers is most on Etisalat network ($\chi^2(1) = 9.549,\ p = 0.023$).

P. Mobile Users' Experiences with Spam SMS with Fraudulent Contents

Despite the fact that spam SMS are predominantly used for commercial purpose in Nigeria, most mobile users receive fraudulent messages. 78% reported they have received messages that were fraudulent. Among these, 69.1% disclosed the fraudulent messages requested for their personal details. Those involved in sending spam SMS were more likely to receive fraudulent messages by 16.8% ($\chi^2(1) = 4.112,\ p = 0.043$).

TABLE 4: EXPERIENCE WITH FRAUDULENT SPAM SMS.

Experience	Frequency	Percent
Received fraudulent SMS		
Yes	149	78.0
No	41	21.5
No response	1	0.5
Total	191	100.0
Fraudulent message requiring sending of personal details		
Yes	103	69.1
No	46	30.9
Total	149	100.0
Reported fraudulent message to network provider		
Yes	31	20.8
No	118	79.2
Total	149	100.0
Reported fraudulent message to security agency		
Yes	4	2.7
No	145	97.3
Total	149	100.0

Surprisingly, only 20.8% of those who received fraudulent message did make effort to report to network provider ($\chi^2(1) = 0.02,\ p < 0.001$). However, a little higher, 25.2%, of those whose received fraudulent message requested for their personal details, actually reported to network provider ($\chi^2(1) = 0.02,\ p < 0.001$).

While few users report fraudulent messages received on their mobile phones to their network provider, fewer users made effort to report to security agency.

Q. Mobile Users' Expectations

Majority of users believe mobile subscribers should be given the right to determine the type of unsolicited SMS they wish to receive. Almost the same percentage of respondents agrees on the need for regulation of unsolicited advertorial and

promotional SMS, and that the regulation should be undertaken by a monitoring body.

TABLE 5: USERS' EXPECTATIONS.

Expectation	Frequency	Percent
Need for customers' right to determine unsolicited SMS to be received		
Yes	170	89.0
No	21	11.0
Total	191	100.0
Need for regulation of unsolicited advertorial/promotional SMS		
Yes	169	88.5
No	21	11.0
No response	1	0.5
Total	191	100.0
Need for regulation to be undertaken by a monitoring body		
Yes	161	84.3
No	30	15.7
Total	191	100.0

V. DISCUSSION

This study sought to investigate the prevalence and nature of SMS spam in Nigeria's mobile telecommunication sector. From the study, an average mobile user is subscribed to a minimum of 2 networks. And most respondents use MTN network.

A crucial finding of this study is that all mobile subscribers in Nigeria receive SMS spam, either from network providers or other sources. This implies an increase of 29.9% compared to data obtained in 2012. As at 2012, only 77% were receiving the unsolicited mobile messages [28]. Most receive between one to three unsolicited SMS daily; with the average number of spam SMS received daily by mobile users from both network providers and other sources was found to be 2.45. The total number of subscribers on the four main GSM networks as at December 2014 was 136,676,606 [47]. Using this average per mobile user, the average number of spam SMS received daily in Nigeria is 334,857,685. This is higher than the average in UK [24], [25].

The study also reveals that MTN network is mostly used by spammers. Specifically, 57.1% of all spam SMS traverses this network. This is not surprising, considering the fact that, from the study, the network remains the most subscribed to in Nigeria. According to [47], as at December 2014, MTN has 59,893,093 subscribers. The other network operators, Glo, Etisalat, and Airtel, have 28,219,089; 21,103,749; and 27,556,544 respectively.

SMS spam is still mostly utilized for commercial purpose, specifically for advertorial and promotional purposes. Out of every ten spam SMS sent in Nigeria, approximately eight of them are either advertorial or promotional. Surprisingly, these categories of spam SMS come more from network providers than other sources. One possible reason for this development is the competition among the mobile network operators, to increase their subscriber base, and consequently their revenue. Two factors contribute to this completion. The first is decline in revenue. In Nigeria, the telecom industry Average Revenue Per User (ARPU) has been significantly declining [48]. For instance, from 2000 to 2012, there has been 44.4% drop, from ₦1,800 to ₦1,000 [49]. The other factor is the introduction of number portability in April, 2013. The effect of these is more products and services being developed by MNOs, to improve their revenues. Thus, subscribers' mobile devices are continuously barged with tons of information regarding existing and new products and services. These are in addition to those from other sources, including telemarketers and value-added service providers (VASPs). From observations, there are instances where a mobile user receives in quick succession two unsolicited SMS with exactly the same contents from a single source. Unfortunately, mobile users hardly have interest in these messages. Gonzalez [15] reported 65% of mobile users in Nigeria, in a survey, indicated they received promotional messages of no personal interest.

While all mobile users in Nigeria receive unsolicited SMS, most do not send spam. Only 43.5% indicated they send unsolicited messages. One interesting discovery in the study is the increase in likelihood by 92.8% of a mobile user receiving spam SMS if the user is a spammer, compared to when he is not. 59% of mobile users who send spam SMS receive daily more than the average spam SMS received in Nigeria. Only 30.6% who do not send spam fall into this category. While there are no studies that established the fact that sending spam increases the likelihood of receiving more spam, one possible explanation is that this type of occurrence could be location-specific. A cluster of population that sends spam SMS can be expected to receive more than those outside the cluster.

Compared to those who are students and employed, the study also reveals that unemployed mobile users receive advertorial and promotional spam SMS most. This can be adduced to the fact that most unemployed users, in search of jobs, usually submit their profiles, including phone numbers, to different job sites, recruitment agencies, and online fora. Based on the high availability of these mobile numbers online, spammers would easily harvest them.

It is evident that malicious spammers, though still in the minority, are also taking advantage of the growing mobile user base in the country. More than three-quarter, 78% to be precise, reported they have received fraudulent spam SMS. On March 4, 2015, one of the authors received an unsolicited SMS on his MTN network, purportedly sent from +2348110232119, with the content:

> *Congratulations!!! Your number is among the 15 lucky winners that won N500,000 from the ongoing GUNNESS CHOOSING NAIRA BET. Your Winning ticket number is (0103) Call Mr johnpaul on 08063999018 for claims….*

In 2014, the average percentage subscriber growth for the four main GSM operators was 3.06 [47]. The implication of this is that fraudulent spam SMS are bound to become more prevalent, as are the cases already in US and UK [23].

Unfortunately, less people are reporting cases of fraudulent messages to either network providers or security agencies. 79.2% did not report to their network providers, and almost all,

97.3%, to the security agencies. The study found out users were slightly more interested in reporting fraudulent messages with SMShing intent. Most mobile users are reluctant to report fraudulent messages to either network provider or security agencies, due to perceived waste of time and effort of such venture. For instance, in the 2012 Nigeria Consumer Satisfaction Survey Final Report (Part 2) [50], 64.0% reported they never made any complaint in the preceding year. 14.5% made complaint only once. When asked about the nature of last complaint, SMS-related complaints accounted for only 5.7% of total complaints. In Nigeria, consumer protection index is very low. When reports are made, most often, investigation by the agency concerned is never initiated. In cases where investigation is launched, they are hardly completed.

On the expectations of mobile users in respect of rights to determine type of spam SMS to be received and need for regulation of the sector, most agreed they should be given the right to determine the type of spam SMS they would love to receive. This finding agrees with that of [15], in which 86% of mobile users in Nigeria expect messages should be based on their interests and tastes.

Equally, most mobile users expressed the belief that unsolicited advertorial/promotional SMS should be regulated. Most indicated this should be done by a monitoring body apart from the mobile network operators. Current regulations and guidelines have not been adequately effective at regulating service providers who send spam SMS for commercial purpose. In addition, compliance with the guidelines and regulations has been very low. This low compliance with regulations is also experienced in Saudi Arabia [14]. One country, however, which has succeeded in this area of regulation, is India. There, the Telecom Commercial Communications Customer Preference Regulations helps in the regulation of commercial mobile communications [51]. While the regulation permits for sending of transactional messages, receiving of promotional messages are determined by the customers. These are categorized, and customers can register or deregister their preferences, via SMS or voice call. The regulation also specifies penalties that defaulters are liable to pay.

VI. CONCLUSION

SMS spam has attained a global dimension. And Nigeria is not left out of this reality. The issue of spam had been identified as one of the aspects of services requiring most attention from NCC [28]. Unfortunately, the county is yet to have a legislation or regulation that comprehensively addresses mobile spamming. This study is one of the first studies to provide some insight into the state of SMS spamming in Nigeria. The study revealed that all mobile users in Nigeria have received at one time or the other unsolicited mobile messages, receiving an average of 2.45 daily. In the country, spamming is utilized majorly for commercial purpose: advertorial and promotional messages accounting for most spam messages that traverse the national cyberspace. However, the study also found out that malicious spammers are also leveraging on the continual increase in mobile adoption in the country. Most mobile users, unfortunately, do not report receiving spam SMS to either network operators or security agencies. Most, however, indicated they would love to have the right to decide on the type of spam SMS they want to receive, and agreed on the need for more effective regulation of mobile messaging for marketing purpose. Current recommendations by the government are very limited in scope and potency. There are no guidelines on enforcement. Until more stringent regulations are put in place, MNOs, value added service providers, telemarketers, and other SMS spammers will continue to abuse mobile bulk messaging.

One major limitation of this study is the number of locations covered. In reality, stratified clustering sampling requires sampling from all the strata. However, the study considered only two of the six strata. Due to the fact that rate of spamming could differ from one location to another, sampling from the entire geopolitical zones would have portended higher representativeness of the country.

Providing a comprehensive framework for effectively managing mobile spamming is one research area that could be considered in future studies. There are other areas in respect of mobile spam experience that could further be investigated. It is necessary to know whether senders of spam SMS comply with guidelines set by NCC on actually providing options to opt out of receiving mobile messages, and not sending message before 8am and after 8pm. Another area worth exploring is mobile users' disposition to spam SMS.

REFERENCES

[1] International Telecommunication Union, "ICT facts and Figures," 2014, Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

[2] Central Intelligence Agency, "Country Comparison :: Telephones - Mobile Cellular," 2014, Retrieved from https://www.cia.gov/library/publications/the-world-factbook/rankorder/2151rank.html

[3] Nigerian Communication Commision, "Subscriber Statistics," 2014, Retrieved from http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:art-statistics-subscriber-data&catid=65:cat-web-statistics&Itemid=73

[4] International Telecommunication Union, " ITU Survey on Anti -spam Legislation Worldwide. Geneva: WSIS Thematic Meeting on Cybersecurity," 2005.

[5] J. M. Rao & D. H. Railey, "The Economics of Spam. Journal of Economic Perspectives," Vol. 26, No. 3, 2012, pp.87-110.

[6] I. Joe & H. Shim, "An SMS spam filtering system using support vector machine Future Generation Information Technology," 2010 (pp. 577-584): Springer.

[7] M. B. Junaid & M. Farooq, "Using evolutionary learning classifiers to do Mobile Spam (SMS) filtering," Proceedings of the 13th annual conference on Genetic and evolutionary computation, 2011, pp.1795-1802.

[8] T. M. Mahmoud & A. M. Mahfouz, "Sms spam filtering technique based on artificial immune system," International J. of Computer Science Issues, Vol. 9, Issue 2, No. 1, 2012, pp.589-597.

[9] A. K. Uysal, S. Gunal, S. Ergin & E. S. Gunal, "A novel framework for SMS spam filtering," Paper presented at the Innovations in Intelligent Systems and Applications (INISTA), 2012 International Symposium on, pp.1-4.

[10] O. Osho, O. Y. Ogunleke & A. A. Falaye, "Frameworks for Mitigating Identity Theft and Spamming through Bulk Messaging," Proceedings of

the IEEE 6th International Conference on Adaptive Science and Technology, Ota, Nigeria, 2014, pp.1 – 6.

[11] M. Y. Schaub, "Unsolicited email: Does Europe allow spam? The state of the art of the European legislation with regard to unsolicited commercial communications," Computer Law & Security Review, Vol. 18, No. 2, 2002, pp.99-105.

[12] M. Butler, "Spam – the meat of the problem," Computer Law & Security Review, Vol 19, No. 5, 2003, pp.388-391.

[13] D. W. Khong, "The problem of spam law: A comment on the Malaysian Communications and Multimedia Commission's discussion paper on regulating unsolicited commercial messages," Computer Law & Security Review, Vol. 20, No. 3, 2004, pp.206-212.

[14] M. A. Al-Kadhi, "Assessment of the status of spam in the Kingdom of Saudi Arabia," Journal of King Saud University-Computer and Information Sciences, Vol. 23, No. 2, 2011, pp.45-58.

[15] N. Gonzalez, "Are African mobile consumers ready for Mobile Marketing," November 2014, Retrieved from http://blog.gemalto.com/blog/2014/11/07/are-african-mobile-consumers-ready-for-mobile-marketing/

[16] A. Tiago, G. J. Hidalgo & S. P. Tiago, "Towards SMS Spam Filtering: Results under a New Dataset. International Journal of Information Security Science," Vol. 2, No. 1, 2013, pp.1-18.

[17] S. Dixit, S. Gupta, & C. V. Ravishankar, "LOHIT: An Online Detection and Control System for cellular SMS Span," Proceedings for the IASTED International Conference communication, Networks and Information Security. Phoenix, Arizona, 2005.

[18] Cloudmark Report, "Cloudmark 2013 Global Messaging Threat Report," San Francisco: Cloudmark Security, 2014.

[19] A. Lahmadi, L. Delosiere & O. Festor, "Hinky: Defending Against Text-based Message Spam on Smartphones," IEEE International Conference on Communications ICC2011, Kyoto, Japan, 2011.

[20] J. G. Hidalgo, G. C. Bringas & E. Sánz, "Content Based SMS Spam Filtering," Proceedings of the 2006 ACM symposium on Document engineering, New York: ACM, 2006, pp.107-114.

[21] GSMA Spam Reporting Service, "SMS Spam and Mobile Messaging Attacks Introduction, Trends and Examples. London: CloudMark, 2011.

[22] Pew Research centre, "Mobile Technology Fact sheet," 2014, Retrieved from http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/

[23] Cloudmark, "SMS Spam Overview - Preserving the Value of SMS Texting," 2014, Retrieved from https://www.cloudmark.com/en/s/resources/whitepapers/sms-spam-overview

[24] W. Johnson, "New service could stop nine million spam texts a day," December 2012, Retrieved from http://www.telegraph.co.uk/technology/internet-security/9761640/New-service-could-stop-nine-million-spam-texts-a-day.html

[25] S. Dakin, "MPs and the Text Pests: The Commons and the Campaign to Block the Spammers," November 2013, Retrieved from http://www.huffingtonpost.co.uk/dr-stephen-dakin/spam-phone-calls_b_3864737.html

[26] R. Cordon, "New mobile security statistics show consumers fearful of mobile spam," March 2012, Retrieved from http://www.computerweekly.com/news/2240146622/New-mobile-security-statistics-show-consumers-fearful-of-mobile-spam

[27] W. Ji, K. Hyoungshick & H. Jun, H, "Hybrid spam filtering for mobile communication," Computer and Security, Vol. 29, No. 4, 2010, pp.446-459.

[28] Nigeria Communications Commission, "Nigeria Consumer Satisfaction Survey Final Report Part 1: Overview," 2012, Retrieved from http://www.ncc.gov.ng/index.php?option=com_docman&task=doc_download&gid=369&Itemid=

[29] O. Olaleye, "NCC to sanction VAS providers for unsolicited SMS," November 2014, Retrieved from http://sunnewsonline.com/new/?p=91536

[30] Nigeria Communications Commission, "Guidelines on Advertisements and Promotions," Retrieved from http://www.ncc.gov.ng/index.php?option=com_content&view=category&id=66&Itemid=80

[31] Nigeria Communications Commission, "Competition Practices Regulations, 2007," Retrieved from http://www.ncc.gov.ng/index.php?option=com_content&view=category&id=66&Itemid=80

[32] Nigeria Communications Commission, "Consumer Code of Practice Regulations, 2007," Retrieved from http://ncc.gov.ng/archive/RegulatorFramework/Regulations-Consumer_Code_of_Practice.pdf

[33] Nigeria Communications Commission, "Guidelines on Short Code Operation in Nigeria," Retrieved from http://www.ncc.gov.ng/index.php?option=com_content&view=category&id=66&Itemid=80

[34] Nigeria Communications Commission, "Quality of Service Regulations, 2012," Retrieved from http://www.ncc.gov.ng/index.php?option=com_content&view=category&id=66&Itemid=80

[35] Cyber Security and Data Protection Agency Bill, 2008. Retrieved from http://www.gbengasesan.com/hb154.pdf

[36] Cybercrime Bill. Retrieved from http://www.nass.gov.ng/document/download/1365

[37] BusinessDay, "Telecoms operators, NCC and unsolicited text messages," January 2014, Retrieved from http://businessdayonline.com/2014/01/telecoms-operators-ncc-and-unsolicited-text-messages/

[38] Z. Papacharissi, "Privacy as a luxury commodity," First Monday, Vol. 15, No. 8, 2010.

[39] K. Jerry, "Information privacy in cyberspace transactions," Stanford Law Review, 1998, pp.1193-1294.

[40] M. Leppaniemi & H. Karjaluoto, "Factors influencing customers' willingness to accept mobile advertising: A conceptual framework," Int. J. Mobile Communications, Vol. 3, No. 3, 2005, pp.197-213.

[41] J. Litman, "Information privacy/information property," Stanford Law Review, 2000, pp.1283-1313.

[42] V. Bergelson, "It's personal but is it mine? Towards property rights in personal information," UC Davis Law Review, No. 37, pp.379-451.

[43] H. J. Smith, T. Dinev & H. Xu, "Information privacy research: an interdisciplinary review," MIS quarterly, Vol. 35, No. 4, 2011, pp. 989-1016.

[44] N. J. King & P. W. Jessen, "Profiling the mobile customer – Privacy concerns when behavioural advertisers target mobile phones – Part I," ComputerLaw and Security Review, Vol. 26, No. 6, 2010, pp.595-612.

[45] G. Barber, "Personal information in government records: protecting the public interest in privacy," Louis U. Pub. L. Rev. Vol. 25, 2006, pp. 63 – 122.

[46] R. A. Spinello, "Ethical reflections on the problem of spam," Ethics and Information Technology, Vol. 1, 1999, pp.185-191.

[47] Nigeria Communications Commission, "Operator Data," 2015, Retrieved from http://ncc.gov.ng/index.php?option=com_content&view=article&id=70:artstatisticsoperator&catid=65&Itemid=76

[48] T. Akinluyi, "The Changing Dynamics of the Telecommunications Industry," February 2015. Retrieved from http://www.proshareng.com/news/25921/TheChangingDynamicsoftheTelecommunicationsIndustryProshare

[49] MyFinancialIntelligence, "Opportunities in Telecoms: Operators Scavenging for More," Month Year, Retrieved from http://www.myfinancialintelligence.com/telecomsandit/opportunitiestelecomsoperatorsscavengingmore

[50] Nigeria Communications Commission, "Nigeria Consumer Satisfaction Survey Final Report Part 2: Data Analysis," 2012, Retrieved from http://www.ncc.gov.ng/index.php?option=com_docman&task=doc_download&gid=368&Itemid=

[51] Telecom Regulatory Authority of India, "The Telecom Commercial Communications Customer Preference Regulations," 2010, Retrieved from www.nccptrai.gov.in/nccpregistry/regu lation1diccndiv.pdf

An Enhanced Congestion Control System for Mobile Operation

[1]Egwali, A. O. and [2]Ukaoha, K. C.
Department of Computer Science. University of Benin, P.M.B. 1154. Benin City. Nigeria.
[1]egwali.annie@yahoo.com, [2]kingsley.ukaoha@uniben.edu

Abstract- The level of patronage being experienced in Global System for Mobile Communications (GSM) in Nigeria is increasingly overwhelming and presently, congestion is a major challenge both to the service providers as well as to subscribers. In this paper, a cell splitting technique was proposed to improve coverage area by applying Relay theory and Fixed Channel Allocation. Relay theory is integrated with Erlang B formula to calculate the call blocking probability of a cell, the current and target grade of service and to analyze the total number of channels to allocate to a cell based on the traffic of subscribers in the region. The fixed channel allocation scheme is used to assign the number of channels gotten from the Relay Theory to the new Micro cells developed. The results showed that cell splitting was efficient in freeing congested cells as it improves the coverage area signal.

Keywords: Service; GSM; Channel; Cells Splitting; Telecommunication; Network Decongestion.

I. INTRODUCTION

No modern economy can thrive without an integral information technology and telecommunication infrastructure. This is because ICT provide the veritable platform for development across the economic and other sectors if well harnessed. Nigeria has a population of nearly 140 million people and is being serviced by 60 phone Lines with a success rate of 45%. If 70% to 100% success rate is achieved, Nigeria would have many phone lines which can impressively improve the lives of the local people in as far as communication through telephone, cell phone and internet is concerned.

In the year 2013, the ratio stands at 1:3 implying that a Nigerian individual living in an urban center owns three communication lines in the sense that at work and home an individual will be serviced by telephone lines and a mobile cellular phone, to make it three gadgets of communication [1].

In Nigeria, there are five major GSM telecommunication operators: MTN, Airtel, GloMobile, Etisalat and MTEL. MTN enjoys the greatest patronage, with over 35.1 million subscribers [2]. It was predicted that between 2003 and 2006, Nigeria's GSM market would be Africa's fastest growing mobile market, and this prediction had long been fulfilled [3]. The competition is getting fiercer by the day as operators compete desperately for the same potential subscribers, consequently congestion is a problem all GSM service providers are facing and trying to resolve. The first issue that needs to be tackled by GSM operators is the provision of network coverage to the target population. Calls cannot be made or received in areas where there is no network, and where a network exists but has poor connectivity, calls may be difficult to make or receive. Poor connectivity of calls results from factors relating to handoff, dead-zone, damaged cell phone antenna, weather, outdated or corrupted cell phone roaming software and congestion [4].

This research work focused on congestion, which is usually associated with the network problem and not a user-side problem. In solving a network congestion problem, analysis of the traffic situation of a cell site is evaluated to determine the level of congestion. If the cell site is congested, then the splitting process is carried out by applying the Relay theory and using the Fixed Channel allocation scheme to assign frequency channel depending on the grade of service.

A. Congestion Problem of the GSM Network

Congestion is the unavailability of network to the subscriber at a time of making a call. Congestion arises when the number of calls emanating or terminating from a particular network is more than the capacity that the network is able to cater for at a particular time [5]. Other factors that could lead to congestion are: inadequate radio channels and infrastructure to support the vast number of subscribers on the network, redialing of subscribers when they experience blocking, too many users on the network, marketing strategies and pricing schemes also affect traffic behaviour since this would have increased the number of subscribers on the network and the use of old equipment facilities instead of new ones. These results in call signals queuing on the transmission channel and the unavailability of network to the subscriber at the time of making a call [2], consequently, the rate of transfer of voice signals is reduced or quality of signals received become distorted or both. At worse, the calls will not connect at all. On the network side four elements are related to congestion:

1. Traffic channels congestion (TCHC): Traffic channels (TCH) represent a voice channel and each call uses TCH. There are eight channels defined for each radio frequency carrier and most are used for traffic channels and some for control channels [6]. When there is no free voice channel (TCH), then, traffic channels congestion (TCHC) is obtained.
2. Dedicated control channel congestion (DCHC): Standalone dedicated control channel (SDCCH) is to

provide authentication to mobile station, location updating and assignments to voice channel (TCHs) during idle periods [6]. When making a call or responding to paging message for the allocation of an SDCCH for authentication, if there is no vacant SDCCH to use at that time, the call will be terminated. This failure is called the dedicated control channel congestion.

3. Common control channels congestion (CCCHC): Common control channel is a group of control channels that support the establishment and maintenance of communication links between the mobile stations and base stations [7]. It consists of random access channel (RACH), paging channels (PCH) and access grant channel (AGCH). RACH is used to make request for network assignment, PCH is used to alert the mobile station of incoming call and AGCH is used to assign mobile station to a specific DCCH or SDCCH for onward communication. When any of these three control channels is congested, there cannot be any call establishment between the sender and receiver, then, CCCH congestion is obtained.
4. Pulse code modulation congestion (PCMC): Pulse code modulation (PCM) or E1 is the link required to connect the base station (BS) and mobile-switching center (MSC) together. Each PCM can carry between 1 and 32 calls. When there is no free PCM to carry the call signals between the BS and MSC, then pulse code modulation congestion is obtained.

B. Existing Techniques to Address Congestion

Techniques to address congestion includes: micro cell, frequently recent call allocation, block time sharing, dynamic allocation without time slicing, dynamic allocation time slicing with signal sensing, SIM card priority allocation, cell splitting and multi band.

- Micro Cell technique is applicable in an environment where there is constant abnormal increase in the number of subscribers for some interval of days consistently like in an airport environment or stadium. The micro- cellular systems can be installed so as to take care of the sudden increase in the number of subscribers. The use of micro cells to cover hot-spots cell offload the macro cells, and help operators to avoid the cost of having to split cells. As traffic increases, the number of micro cells and indoor cells also continue to grow [2]. By adding more capacity to the micro cells, operators can achieve an extreme boost in capacity. However while this increases system capacity and reduce Hand-over (i.e. no call drop is experienced during roaming), its implementation is costly and it utilizes much power which can result in interference.

- Frequently-Recent-Call-Allocation technique give preference to some calls that were denied access but immediately redials within a specified time. What that means is that if there is any call that was among the one that came recently, the system will give a higher preference above the ones that are just appearing for the first time. This can be achieved by creating a small memory that will register the calls that were not given any service. So if any of these calls comes again, the system will first search the memory called cache if there is any of the call number has been registered in the cache before and if there is, the call will be served first. No call number should be allowed to stay more than a specified time interval like 1 minute in the cache so that some calls will not have undue privilege over the other. Also, higher preference will be given to numbers present in the cache. The memory should be created in the BSC as this is the gateway of every call to MSC. This memory will not affect the performance of BSC negatively since only a minimal number that will be here due to a purging mechanism that will be removing the calls that have exceeded their 1 minute duration time in the memory. Although this technique will not allow some calls to be starved for too long period of time, it often lead to waste of service time because there might be a need to check every call against the already registered call in the memory [8].

- Block Time Sharing technique requires a call to have full access according to the given time allocated to it. The call cannot be interrupted except the time interval has expired. But immediately the call time allocated is expired the call is disconnected to allow other calls. The merits of this technique are that it does not allow any call to a channel more than the allotted time, it gives access to the call without interruption from any other call within the time limit and it allows equal sharing among the call. However, it wastes service time.

- Dynamic-Allocation-Without-Time-Slicing allow calls to occupy the channel without given any time range. Any call that enters the channel will finish it work before allowing any other call to the channel. Also it allows any call that is ready to seize the channel without any consideration [9]. An advantage of this method is that it allows an initial call to end before any other call can be allowed into the channel, however, sometimes some calls occupies the channel unnecessarily thereby denying others from entering.

- Dynamic-Allocation-Time-Slicing-with-Signal-Sensing technique allows calls in a channel with a maximum time interval. It is done by the Carrier sending a signal to all available time slots to check if there is any call waiting and if there is, the signal will interrupt (preempt) any call that

has exhausted it time interval given to it but if no call is waiting at that time then the call continues to use the channel. Some merits of this technique are that it does not allow the system to be occupied unnecessarily and it allows the subscriber to continue calling as long as they wish provided there is no call waiting. However, it does not consider any call as important so essential calls are pre-empted without finishing the call and there is wastage of time for calls that do not finish their allotted time before they exit the channel.

- SIM card priority allocation technique allots a level of priority to calls. This priority initially has been integrated into the SIM card. So, anytime anybody buys a SIM card and activate it on the network, the priority level registered automatically. The priority level will be used throughout the period of subscription of the subscriber to the network. The level of priority will be determined by the nature of the user's service. This model will be able to take care of the executive essential duties officers like President, Governors, fire fighters, police and so on. In other words principles of arithmetic operation preferences will be used where the highest priority will gain access to the channel before the lower priority. Also, people of the same priority will follow any other model for managing equal priority. So this model is meant especially for essential duties officers. In this model, time interrupt preemption will not apply; their access to the network will not be terminated until they terminate it themselves. The Advantage of this Method is that it allow the essential duties calls to complete their calls without any interrupt and thereby forestalls casualties that might occur if they were not given attention. The disadvantage of this method is that so many calls will be denied access during the time when the essential duties are on. Also, some calls that may be very important to some subscribers might be dropped and immediate reconnection may not be possible easily.

Cell Splitting technique is applied as the number of subscribers increases in a particular cell site. If the present channels cannot carry all calls, the engineers may decide to increase the number of channels until the maximum number of channels per base station is exhausted. If this is exhausted, then the engineers can further improve the system by employing cell splitting. The advantage of this method is that users in different geographical areas (in different cells) may simultaneously use the same frequency. Nevertheless, there is the cost of implementation and interference that could arise as a problem.

Multiband technique involves accessing the spectrum in other frequency bands. For instance, in the situation where 900 GSM type is installed, the operator should be thinking of 1800 GSM. This phenomenon is referred to as multi-band system. That means, the 1800 GSM can be installed, so that 1800 bands will automatically handle some of the calls thereby relieving the 900 GSM type [10]. GSM-900 uses 890–915 MHz to send information from the mobile station to the base station (uplink) and 935–960 MHz for the other direction (downlink), providing 124 RF channels (channel numbers 1 to 124) spaced at 200 kHz. Duplex spacing of 45 MHz is used. Guard bands 100 kHz wide are placed at either end of the range of frequencies [4]. and GSM-1800 uses 1,710–1,785 MHz to send information from the mobile station to the base transceiver station (uplink) and 1,805–1,880 MHz for the other direction (downlink), providing 374 channels (channel numbers 512 to 885). Duplex spacing is 95 MHz GSM-1800 is also called Digital Cellular Service (DCS) in the United Kingdom, while being called PCS in Hong Kong– to avoid confusion with GSM-1900 which is commonly called PCS in the rest of the world. Mobile Communication Services on Aircraft (MCA) uses GSM1800. Generally, the GSM-1800 has more frequency channels than the GSM-900 so the switch could easily help in controlling or reducing the congestion level to a minimal point. This technique eases congestion on a particular cell but is very costly to implement on the side of the GSM operators and mobile phones which are not multi-band will not be supported on the network (Cell) that has a different band in that area.

II. RELATED WORKS

Over the years several models have been developed to manage and control congestion [11], proposed Micro cells system. The analysis of the is for time-division multiple access with frequency hopping, power control, and discontinuous transmission, and the radio channel is composed of an inverse fourth power path loss law with log-normal fading. A single microcell is introduced into a hexagonal cluster of macro-cells before considering clustered microcells. Both omnidirectional and sectorized cells are examined. Results show that high reuse factors are required when channel sharing is employed. When channel partitioning is used, no co-channel interference occurred between the microcells and the macro-cells, allowing them to be planned independently. This increases the number of channels per cell without an increase in co-channel interference. The co-channel interference problems of sharing frequencies between microcells and existing macro-cells was also investigated and based on the assumptions made, it was found that an isolated microcell could operate under a macro-cell layer of cluster size greater than 12.

The work by [1] proposed a technique for estimating the coverage of GSM system using variables like BS antenna height, transmitting antenna gain, output power of BS for propagation environment such as rural, sub-urban and urban case. MATLAB was used for simulation and

performance evaluation of the capacity and coverage in GSM system. Path loss for uplink and downlink was calculated using Link Calculator. Analysis reveals that coverage area improves significantly when the spectral efficiency, interference cell sectoring and cell splitting were considered.

The authors in [7] proposed a dynamic half rate technique which involves the process whereby only half of the normal data rate (full rate) is assigned to a user operating on a communication channel (typically a cellular). By reducing the data rate, the number of users that can share the radio communication channel is increased. Creating half rate doubles the radio channel's capacity. GSM is designed so that it can easily accommodate a half rate speech coder**.** The use of this higher data compression rates reduces the amount of data required per user and this increases the number of users that can share a radio channel. Considering the benefit to be gained by the operator (the subscribers number doubles and improved network is enjoyed by the subscribers).

The work by [8] proposed a frequently call allocation model that gives preference to calls that were denied access but immediately redial within a specified time. This was achieved by creating a small memory that registers the calls that were not given any service. Subsequently, if any of these calls comes again, the system first searches the memory cache if this incoming call number has been registered in the cache before and if there is, the call is served first. The system gives no call number undue privilege over the other by not allowing any call to stay more than a 1 minute in the cache. Nevertheless, higher preferences are given to numbers present in the cache and the memory is created in the BSC, the gateway of every call to MSC. This memory does not affect the performance of BSC negatively since at a point in time only a minimal call number is stored due to a purging mechanisms that removes calls that have exceeded their I minute duration time in the memory.

The work by [10] proposed a block time sharing scheme where each call is given a maximum block of time. When the actual time allocated to the given call expires, the call is dropped. He also proposed the Dynamic allocation without time slicing.

In [9], the authors proposed the process of simulating the network using the Erlang B formula traffic model. It explores the use of Erlang-B in determining the appropriate probability level for some range of subscribers. When a network is properly dimensioned, the channels will be used more efficiently and will produce greater user satisfaction. On the other side, poor modeling of traffic characteristics can actually affect system performance. When cells are under dimensioned, not enough radio channels are installed. This lead to congestion in the cell, and it also affect overall system performance. The network planning is built around three variables: servers (i.e. the channel that handles calls), traffic (i.e. radio channels) and grade of service (i.e. the probability that all servers will be busy when a call is attempted).

The work by [3] used Dijktra's routing algorithm to propose a congestion control mechanism. The Dijktra's algorithm is one of the standard algorithms that determine the shortest route between any two nodes, towns or villages in a Local Area network and road network respectively. It also determine the most efficient message route between each, two geographic area in a GSM network. The Dijktra's algorithm uses a special labeling convention to label the various nodes of the network. It begins by labeling the nodes temporary and proceeds until all the nodes have been labeled, permanent. The Dijkstra's algorithm terminates when you have labeled all the nodes as permanent labels, but it begins by labeling the source node with the permanent label, P[0,-]s, 0, in this label means that the distance from the source node to the node s, P, denotes a permanent label, while, -, means that there is no sequence node to the source node. Therefore, application of Dijkstra's routing algorithm model is needed to control congestion in GSM network by finding the shortest route path between the source and the destination. Dijkstra's routing algorithm models are in their simplicity and easy to use, which are very appropriate. The importance of the subscribers' retrials and redials cannot be overlay emphasized in the network planning since the GSM network operators charge users when the call set-up is successful, the blocking affect the revenues and leads to customers' dissatisfaction.

The work by [12] proposed a cell splitting technique which involves calculating the processing gain, number of subscribers requesting for service within each type of cell, user-transmitted in-band signal power to achieve desired SNR and the probability that a call attempt fails. Results were compared using MATLAB simulation software.

- *Generic Cell-Splitting Technique*

A cell is the area covered by a BTS and cell splitting is the process of subdividing a congested macro cell installed in a geography area into smaller cells each with its own base station and a corresponding reduction in antenna height and transmitter power, thereby increasing the capacity of the original cell because splitting increases the number of times the channels are reused for calls amongst smaller cells to cover that same area [13]. The advantage of these is that these new cells would each have its own independent channels assigned to it and there is room for frequency reuse. In addition, the power transmitted in the small cells is reduced compared to the power transmitted in the large cells as it would require much less power to cover the cell compared to the large cells [14]. The consequence of cell splitting is that the frequency is going to be assigned again, which affects neighboring cells.

As shown in Fig.1, cell splitting is achieved by splitting the macro cell by half of its radius R (i.e. R/2). In order to cover the whole service area with these smaller cells, about 4 times of the original cells are needed (i.e. if a circle C_1 with R is drawn, and another circle C_2 with R/2 is drawn inside C_1, it is obvious that C_2 covers an area 4 times as large as C_1).

Hexagonal geometry is used to represent a cell because its enables least number of cells to cover a geographic region and hexagon closely approximates a circular radiation pattern which would occur for an Omni-directional antenna and free space propagation.

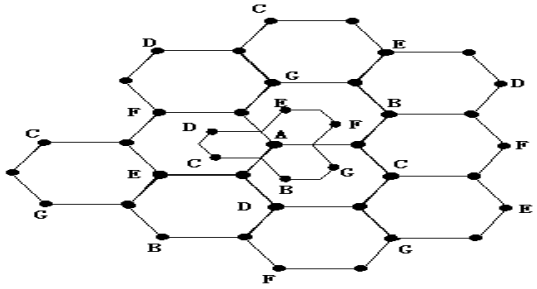


Fig.1. Cell splitting [13].

Suppose that the traffic in service area of the base station A is saturated, new BTSs will be needed to increase the number of channels in the area and reduce the coverage area of each single BTS. As shown in figure 1 the original BTS is surrounded by 6 new micro-cell BTSs added on the precondition that the frequency reuse plan of the system remains the same. The concept of frequency reuse is based on assigning to each cell a group of radio channels used within a small geographic area called cell. Cells are assigned a group of radio channels that is completely different from neighboring cells. The coverage area of cell is called the footprint. This footprint is limited by a boundary so that the same group of channels can be used in different cells that are far enough away from each other so that their frequencies do not interfere.

For the new cells to be smaller in size, the transmit power of these cells must be reduced. The transmit power of the new cells with radius half that of the original cells can be found by examining the received power P_r, at the new and old cell boundaries and setting them equal to each other. This is necessary to ensure that the frequency reuse plan for the new small cells (S_C) behaves exactly as for the original cells.

$$P_r(original\ cell)\ \alpha\ Pt_1(R)^{-n} \quad (1)$$

$$Pr(small\ cell)\ \alpha\ Pt_2(\frac{R}{2})^{-n} \quad (2)$$

where Pt_1 is the transmitter power of the original cell, Pt_2 is the transmitter power of small cell and n is the Path loss. Therefore, if n=4 and set the received power of Equ. 1 and 2 to be equal (assuming perfect power control),

$$\boldsymbol{Pt_2 = \frac{Pt1}{16}} \quad (3)$$

Thus the transmit power must be reduced by 12 dB in order to fill in the original coverage area with small cells (S_C), while maintaining the *S/I* requirement.

III. PROPOSED CELL SPLITTING SYSTEM

The proposed Cell splitting technique is achieved using the Erlang B formula by means of the Erlang B calculator, path loss, transmitter power, radius of cell, cell range for RF coverage planning and frequency reuse concept. Also the traffic data to be used is an assumption of the possibility of traffic scenarios, which employs the following choice of parameters:

A. *Channel Allocation*: There are two channel allocation schemes used to assign frequency channels to Cells in GSM: fixed channel allocation (FCA) and dynamic channel allocation (DCA). With FCA, a set of channels is permanently assigned to each cell, according to the allowed reuse distance. Each cell is given a predetermined set of frequency channels. FCA requires manual frequency planning, which is an arduous task in time-division multiple access (TDMA) and Frequency Division Multiplexing Access (FDMA) based systems since such systems are highly sensitive to co-channel interference from nearby cells that are reusing the same channel [15]. Demerits of this approach include the fact that there is a waste of resources during the non-busy hour since some of the channels might be left idle whereas somewhere along the cellular system a BTS is requesting for a channel. And since it is fixed, it cannot be removed automatically except the manual process is carried out again. Advantages of FCA includes the facts that after splitting cell, at any point in time there is always an available channel present to any subscriber that wishes to call, the waiting time or set up is almost negligible and also the numbers of channel remain constant irrespective of the number of customers in that cell. These merits override that of DCA and so it is the choice for this work.

The DCA are not assigned permanently to the cell; instead it is based on every call request base station request from MSC. The method of channel allocation of DCA requires that the MSC does the assignment of channels. The duties of the MSC is associated with the communication switching functions, such as call set-up, release and routing SMS, conference calls, fax, service billing as well as interfacing with other networks, such as the PSTN and also handles Handovers [16]. With the many duties of the MSC, it would be an overload to allow the MSC to be responsible for channels assignments to base stations

as this can also lead to delay, whereby a user might need a channel for communication.

B. Relay Theory: The cellular network system uses relay to meet the requirements of large-capacity subscribers when radio spectrum is limited, because relay makes it possible for a great many subscribers to share limited channel resources. Every subscriber, when originating a call, can occupy a channel via the relay network, and at the end of the call, the channel will be released and become available again for other subscribers. Relay network can be set up based on the statistics of subscriber status, so that a fixed number of channels or circuits will be able to bear a great deal of random subscriber requirements. The relay theory is dedicated to studying how to serve a great number of subscribers by limited service grade (Grade of Service, GOS) capability.

GOS is usually defined as the probability of call blocking or the probability when the call delay time is longer than a given queuing time. GOS is a measure of the subscriber's ability to enter the system when the system is the busiest. Busyness is based on the requirements of a customer in a week, a month or a year. GOS is used as the reference of the preset performance of a certain relay system. The work here is to estimate the maximum communications capacity (Channels) needed by GOS and allocate an appropriate number of channels. In a relay system with C channels, the traffic intensity *T* or call loss is defined as the number of calls that fails to complete in the request time due to congestion. It is calculated using the formula in Equ 4.

$T = N*M/3600$ (4)

where, *N* is number of call and M is the service time

C. Target Grade Of Service: To cater for the traffic intensity of 266.7, there is need to determine the number of channels the new cells will be having. Thus the aim is to achieve a Grade of Service of **4%** i.e. $\mathbf{Pr}_{[blocking]}$ should be **0.04**.

D. Cell Splitting Operational Steps

This work now outlines the steps used towards achieving the proposed congestion control

Step 1: *Check the congestion level of the original site*

Step 2: *If the traffic has been increased, calculate the blocking probability (using Erlang B calculator)*

Step 3: *If the call blocking probability has increased beyond an acceptable level Goto 4 ELSE Goto 10*

Step 4: *Then Begin the processes for the implementation of small cell (S_c) sites.*

Step 5: *Know the number of small cell sites needed in the site.*

Step 6: *Build the base stations (small cells) by reducing the Transmitter Power of the Macro cell radius.* The power of a transmitter determines the extent to which the diameter of a BTS covers an area. A low powered transmitter does not cover large area, but the extent a transmitter covers depends on the next adjacent BTS. This is so as to prevent interference with the frequency of the next cell (area covered by BTS). Transmitter power of this large cell in question is noted as Pt_1 and to get the radius of small cell, divide the radius *R* of the large cell by two (R/2) i.e. the Transmitter Power of large cell is divided in this $Pt_2 = Pt_1/16$.

Step 7: *Replacement of Large Cell with the Small Cells:* This process is achieved after reducing the transmitter power of the large cell and making sure the Radius is divided by 2 as stated above. The replacement is carried out by dividing the lager cell into the small cell by building base stations with their Transmitter power equal to what Pt_2 gives after the calculation, making each small base station to have the same value as Pt_2. The new cells will then be of the same size in radius.

Step 8: *Frequency channel Allocation (FCA)*: Frequency planning takes place after a successful setup. The cells are assigned fixed channels to cater for the traffic efficiencies using the FCA scheme.

Step 9: Repeats step 1-8 for subsequent implementation of small cells

Step 10: End

E. Cell Splitting Pseudo-code

In this work, the proposed cell splitting algorithm for congestion control is shown below.

Begin Cell-Splitting Process
\\ Check Traffic congestion status at the Original site
Int Maximum = 1, Minimum= 0.04, T=266.7, n=95
\\ If traffic increases unexpected .i.e when traffic grows beyond acceptable level.
Goto "EVALUATE" ELSE Goto END
EVALUATE Pr=\\ using Erlang B calculator
IF Pr EQUAL OR GREATER "maximum" then Goto START
ELSE Goto END
START
Goto EVALUATE
n++ UNTIL Pr EQUAL 0.047
\\ Cell splitting Processes start
GET Pt_2
EVALUATE Pt_2 =
\\ BuildingBase Stations(S_c)
Pt_2 EQUALS "R/2"
\\ Frequency planning processes Begin

Repeat BEGIN \\ Repeat for subsequent cell splitting processes
END

IV. EXPERIMENTATION

Table 1 results were evaluated using the Erlang B calculator. The values of call blocking probability against the resources (number of channels) are shown. The Probability of Delay (waiting time) reduces as the number of channels increases thus it is clearly seen that adding more channels to the cells helps reduces the delay of customers on the network. As the number of channels increases the offered load increases, indicating that the system can carry more load. The Probability of Delay (Pr [blocking]) in Table 1 reduces, it shows that as the number of channels increases, the delay is minimized to a point it tends to zero [17]. The delay probability gotten from the work of [17] is shown below.

TABLE 1 RELAY THEORY PARAMETERS CALCULATED

S/N	RESOURCES (Channels)	TRAFFIC INTENSITY	Blocking probability (Pr[blocking])	Delay probability (Pr[delay])	Offered load
1	95	266.7	0.645	0.579	91
2	112	266.7	0.582	0.527	107
3	122	266.7	0.546	0.50	117
4	135	266.7	0.498	0.49	129
5	160	266.7	0.405	0	160
6	178	266.7	0.340	0	178
7	187	266.7	0.307	0	187
8	230	266.7	0.156	0	230
9	250	266.7	0.092	0	250
10	267	266.7	0.047	0	267

The delay probability by [17] shows that as the number of channels increases the Delay probability reduces which means that there is a low level of call delay due to increase in the number of channels.

TABLE 2 DELAY PROBABILITIES AGAINST CHANNELS [17]

s/n	Pr [Delay]	channels
1	0.5954	12
2	0.0464	18
3	0.0013	21

It must be noted that cell-splitting increases the number of channels and also improves the signal strength of the coverage area, so it is a very important strategy to take to achieve great Quality of Service (QoS). Table 3 shows the use of the channels of Table 1 to simulate the offered traffic of [17] system. The comparison still shows that an increase in fixed channel capacity still reduces the Pr [blocking] of the system and also the delay probability still reduces as the channels increases until a point it becomes constant (Zero 0). The graph of Channels against *Pr* [blocking] of both the proposed system and [17] is plotted in Fig.2 the slopes shows the drop in blocking probability of the system. The comparison of the Probability of Delay (Pr [delay]) is shown in Figure 3.7.

TABLE 3 COMPARISONS OF PROPOSED SYSTEM CHANNELS WITH [17]

S/N	RESOURCES (Channels)	Proposed System Parameters [Relay Theory]						
		TRAFFIC INTENSITY	Blocking probability (Pr[blocking])	Delay probability (Pr[delay])	Offered load	Offered Traffic	Pr [blocking]	Pr [Delay]
1	95	266.7	0.645	0.579	91	500	0.81	0.770
2	112	266.7	0.582	0.527	107	500	0.777	0.692
3	122	266.7	0.546	0.50	117	500	0.757	0.757
4	135	266.7	0.498	0.49	129	500	0.731	0.716
5	160	266.7	0.405	0	160	500	0.681	0
6	178	266.7	0.340	0	178	500	0.645	0
7	187	266.7	0.307	0	187	500	0.627	0
8	230	266.7	0.156	0	230	500	0.542	0
9	250	266.7	0.092	0	250	500	0.502	0
10	267	266.7	0.047	0	267	500	0.463	0

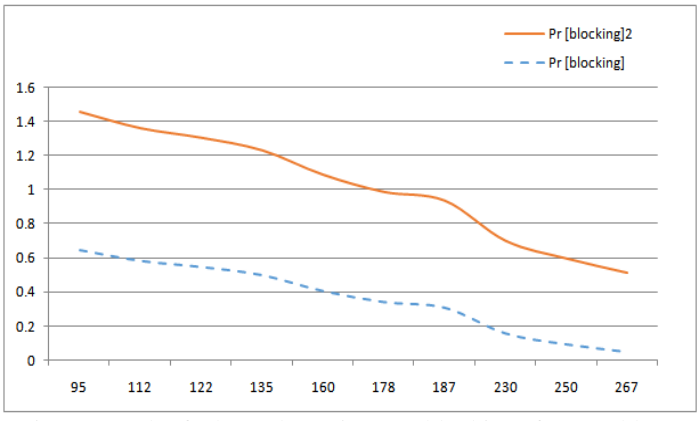


Fig. 2. Graph of Channels against Pr [blocking] from Table 3

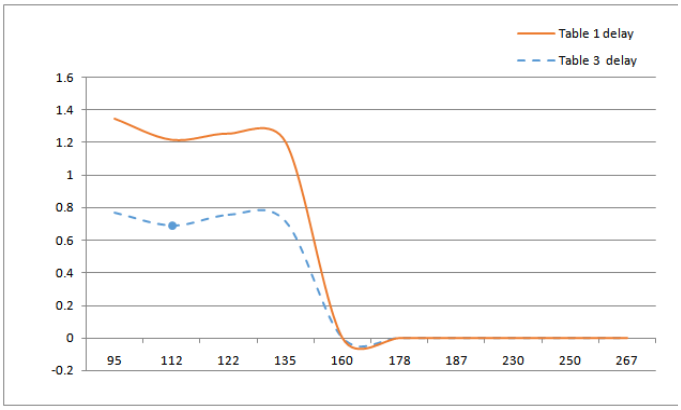


Fig.3. Graph of channels against Pr [delay] of Table 1 and Table 3

V. RESULTS AND DISCUSSION

The probability that a new call is blocked represented as Pr[blocked] is plotted against channel capacity in Fig. 2. The result shows that as the channel capacity increases, the call blocking probability Pr[blocking] reduces until a point when it becomes constant. Since the value of Grade of service is achieved, the number of channels that would be assigned to that cell is known. In this case the number channels is 267. In comparing of both systems, Fig. 2 shows the probability of blocking of both system, the slope of the proposed system (broken lines) and [17] have same slope steepness but the proposed slopes a quicker drop in blocking because the number of channels could easily cater for the traffic intensity (sometimes called Offered traffic), which at this case it is 266.7. This graph proves that both systems achieve a reduction the blocking probability of the network. Fig.3 shows the delay probability of both systems, the slope of the proposed system (broken lines) and [17] tends to zero quick when the number of channels is plotted against delay probability of both systems. This means the proposed system works adequately well enough to remove any trace of delay from the system, thus making the FCA system very efficient way to solving delay and blocking problems which causes congestion in the network.

VI. CONCLUSION

There are problems of congestion in Nigeria telecommunication industry with respect to GSM, such as difficulties in connecting subscribers and losing of resources by the service providers. While previous works used physical and mathematical model such as antenna heights, receiver sensitivity, spectral efficiency, Tabu search algorithm, processing gain, link budget calculations, etc. to achieve a very good coverage area capacity by improving the RF channels and signals, which results in improving capacity and increasing channels, this research work was based on the decongesting of network using cell splitting which was achieved by applying the Relay theory and the Fixed Channel allocation scheme to assign frequency channel.

The result gotten from calculating the Call Blocking Probability which was 0.645 shows that customarily 64.5% of calls in an area would be blocked at a time when all the traffic channels were occupied. This brings about a very low Quality of Service (QoS) from the operators. The approach used in this work is basically empirical. The data used for the analysis were taken from a statistical period of 3months and during the busiest hour of each day. From the number of traffic generated from this busy hour, a Grade of service of 0.04 was achieved showing that only 4% of the users are blocked, thus as the number of channels increases the blocking probability reduces indicating an increase in capacity until the Grade of service is achieved.

I. Future Work

The results show clearly that Cell splitting is very efficient in decongesting a congested cell because it improves the coverage area signal. By the FCA scheme each subscriber is assured of making call at any moment and knows the call would not be blocked and also a caller will not have to wait on the queue to get a timeslot to make a call. However, the cell splitting process should only be in well congested areas such as the urban settlements while the regular big base stations can be used in the rural areas. To avoid future congestion problems, data analysis should be carried out at the areas of likely congested situation like the cities and urban areas to determine the GOS in that area, so that the necessary steps toward splitting the cell (s) can be started.

For further researches, emphasis should be made on how to reduce the case of regular handover experienced by a user due to the multiple base stations in the area. Cell splitting brings about regular hand over which was suggested by [12], though they developed a process of how the macro base station should not be removed so as to handle the handover processes within the cell, more researches and works can be done to remove such case as regular handover to cause a call drop as in a case of a fast moving user (in a vehicle).

REFERENCES

[1] Afsana N. and Aditya S. K.. Performance Analysis of GSM Coverage considering Spectral Efficiency, Interference and Cell Sectoring. *International Journal of Engineering and Advanced Technology (IJEAT).* 2013, 2(4): 2249 – 8958.

[2] Kuboye B. M, "Optimization models for minimizing congestion in Global System for Mobile Communications (GSM) in Nigeria", Journal Media and Communication Studies, 2010 Vol. 2(5), pp. 122-126.

[3] Afolabi A.O. and Olabiyisi S.O, "Application of Routing Algorithm to Congestion Control in GSM Network", Proceedings of the World Congress on Engineering 2012 Vol II WCE 2012, July 4 - 6, 2012, London, U.K.

[4] Online Wikipedia (2014). International Telecommunication Union. Available at: www.wikipedia.org/wiki/International_Telecommunication_Union).

[5] Mughele.E. S. and Wole O. "Congestion Control Mechanisms and Patterns of Call Distribution in GSM Telecommunication Networks: The Case of MTN Nigeria", In Africa Regional

Center for Information Science (ARCIS). University of Ibadan. 2012, PP 27-31.

[6] Mehrotra A. "GSM System Engineering", Artech house, Inc., 1997, Pp: 70-73

[7] Harte L, Levine R, and Livingston G, "GSM Superphones", McGraw Hill, 1999, 71: 45-47.

[8] Konstain, "Radio Resource Management schemes for combines GSM /GPRS Mobile by stems", Wireless Communication Mobile Computing Journal; 2003, 357-384.

[9] Kuboye B. M, Alese B. K., Fajuyigbe O, and Adewale O. S, "Development of Models for Managing Network Congestion on Global System for Mobile Communication (GSM) in Nigeria", Department of Computer Science, Federal University of Technology, 2011

[10] Kuboye B. M.,"Development of a Framework for Managing of Congestion in GSM in Nigeria", Master's Thesis. 2006.

[11] Coombs R. and Steele R., "Introducing Microcells into Macrocellular Networks: A Case Study. Ieee Transactions On Communications", 1999, (47) 4: 1 – 9.

[12] Sohrab A., Ashish M., Mohd G. S., and Tauheed Q, "Capacity Improvement by Cell Splitting Technique in CDMA System over Telecommunication Network", International Refereed Journal of Engineering and Science (IRJES) Vol. 2, Issue 7, 2013, Pp.01-08.

[13] ZTE Corporation, "Training Material for GSM Mobile Communications System", 2003.

[14] Kumar A. and Verma V. "Study on Improving Coverage Area by Cell Splitting and Cell Sectoring Method in Cellular System", International Journal of Advanced Research in Computer Science and Software Engineering, 2014, Vol.4, Issue 2. Available online at: www.ijarcsse.com.

[15] Wikipedia (2013). GSM_frequency_bands . Available at: http://en.wikipedia.org/wiki/GSM_frequency_bands)

[16] Janssen C. "The Mobile Switching Center", Available on Technopedia: www.technopedia.com/8448/mobile-switching-center-mc, 2010.

[17] Ohaneme C. O.,Onoh G. N., Ifeagwu E. N., Eneh I. I., "Improving Channel Capacity Of A Cellular System Using Cell Splitting**.** International Journal of Scientific & Engineering Research, 2012, Vol. 3, Issue 5, May-2012 1 ISSN 2229-5518.

Source Code Defects - Case studies and Lessons Learnt

Mufutau Akuruyejo
Department of Electrical and Electronics Engineering
University of Lagos
Lagos, Nigeria
mufutau.akuruyejo@gmail.com

Stavros Moiras
Department of Computer Science and Technology University of Peloponnese
Peloponnese, Greece

***Abstract* — This paper takes a look at vulnerabilities in source codes and how to mitigate them. A common source of error in source codes written is programmers not checking for security flaws. It is very difficult to write codes that are completely secure especially if the code base is very large. Much of the effort in writing secure code can be reduced significantly if static code analyzers are used. Analyzers vary in performance and ease of use from the simple syntax checkers to enterprise level tools that requires a lot of configuration. This paper uses some of these tools. A brief background is provided. The authors present use cases of Rough Auditing Tool for Security RATS and FlawFinder. Also, manual code review of a C code is carried out and comparison of code review is made with static analysis. Recommendations to minimize occurrence of similar bugs then follow. Limitations and similar works are discussed after. In the end, conclusions and plans for future work are enumerated.**

Keywords — Software Vulnerabilities, Static Analysis, Code Review

I. INTRODUCTION

Vulnerability is a programming error that can be exploited by an attacker to subvert the functionality of the vulnerable software by feeding it malformed inputs (e.g., network packets or web form submissions that evade the program's error checks, allowing the attacker to execute arbitrary code on the host). In order to exploit vulnerability, an attacker must have an opportunity to exercise the vulnerable code, for instance by sending a message to a service listening on a network port. Such an opportunity is known as an attack vector. [1]

The vulnerabilities could range from buffer overflows, calls to vulnerable library functions to unguarded access to root privilege. These may lead to a lot of consequences which could be exploited by a hacker to access the system. Fortunately, there are a number of tools to help the programmer check for these errors. While it is impossible to be completely secure, it's possible to minimize these errors. This paper reviews some static code analyzers. Comparison can also be made between manual checking by the programmer and using automated tools.

Until recently, there was not much focus on the discipline of writing secure code. The efforts were directed towards writing codes that were functional and performed the intended tasks. Security was usually afterthoughts. Therefore, vulnerabilities could exist in software for a long time undetected. A number of instances would buttress this fact:

i. Shellshock, bash vulnerability existed since 1989 and went undetected for long. It was only announced September 2014, a 25-year interval. The number of unique attacks against systems vulnerable to Shellshock peaked at 20,753 [2]. Nevertheless, it would remain an issue for many months. This is because it takes some time for some system administrators to patch the system.

ii. goto fail bug: There are no universal or error-proof tactics that would result in totally bug-free code.

The previous vulnerabilities identified has plagued software developers for long. A good case in point is the Apple's "goto fail bug" [3]. The code that caused the bug is reproduced in Fig. 1:

```
1.  if ((err = SSLHashSHA1.update(&hashCtx,
        &clientRandom)) != 0)
2.   goto fail;
3.  if ((err = SSLHashSHA1.update(&hashCtx,
        &serverRandom)) != 0)
4.   goto fail;
5.  if ((err = SSLHashSHA1.update(&hashCtx,
        &signedParams)) != 0)
6.  goto fail;
7.  goto fail;
8.   if ((err = SSLHashSHA1.update(&hashCtx, &hashOut))
        != 0)
9.  goto fail;
10. err = sslRawVerify(ctx,
11.  ctx->peerPubKey,
12. dataToSign,
13. dataToSignLen,
14.  signature,
15. signatureLen);
16. if (err)  {
17.       ("SSLDecodeSignedServerKeyExchange:   "
18.       sslRawVerify   "returned %d\n", (int)err);
19.       goto fail
20.          }
21. fail:
22. SSLFreeBuffer(&signedHashes);
23. SSLFreeBuffer(&hashCtx);
24. return err;
```

Fig. 1: Goto fail bug code.

The 7th of the code would always be true as there is no associated conditional with it. Hence, fail would always be true, posing a security flaw.

II. RELATED WORK

Use of static analysis tools are relatively recent compared to most other branches of programming. This is both because the tools had to evolve to where they could be usable and also because security hasn't always been a front burner until recent. Majority of the static analysis tools are designed for C language families (including Java). In [4], the author analyzes a Java program that uses sockets. [5] discusses about Klocwork, a static analysis tool that works on C#, C++ and Java. Mention is also made in that paper of the common defects that could occur in software.

III. METHODOLOGY

Rough Auditing Tool For Security

Here, the vulnerable source code of Fig. 2 is analyze:

```
1 #include <stdio.h>
2 #include <string.h>
3 int main(void)
4 {
5     char buff[12];
6     int pass=0;
7     printf("Enter the password: \n");
8     gets(buff);
9     if(strcmp(buff, "thegeekstuff"))
10    {
11        printf ("Wrong Password! \n");
12    }
13    else
14    {
15        printf ("Correct Password \n");
16        pass = 1;
17    }
18    if(pass)
19    {
20       /* Now give access to the user */
21      printf ("\n Root privileges given to the user \n");
22   }
23  return 0;
24  }
```

Fig. 2: A C Code that validates user's password to give root access.

The source code analysis was done using Rough Auditing Tool for Security [RATS]. With RATS, manual analysis is still necessary but it shows a lot of great insight into the underlying code. One advantage of RATS is that it works for not only C/C++ but also Python and Perl. The code presented in Fig. 2 validates a user's password and it then gives root access if successful. The implementation is written in C. The problem lies in the function gets(), it does not check the length of the buff variable, any string given by the user that is longer than 12 bytes will cause a buffer overflow as shown in Fig. 3.

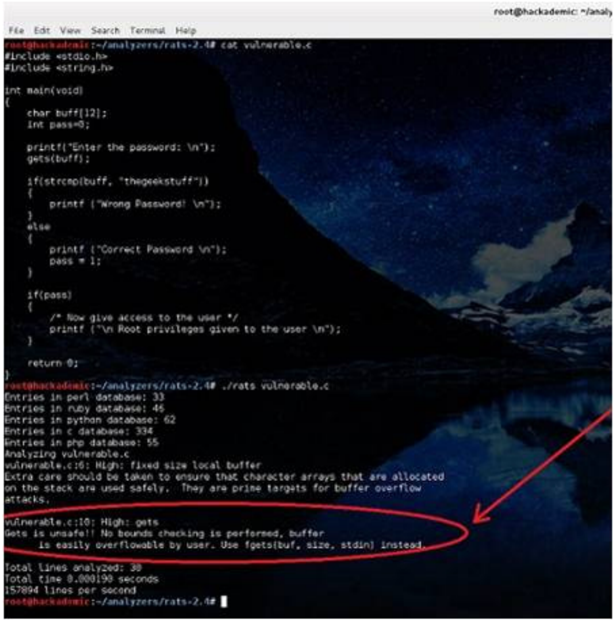


Fig 3: RATS analysis of a vulnerable code.

First, let's run the program with a string shorter than 12 bytes and see the output of the program as shown in Fig. 4. The source code has already been compiled to give an executable file.

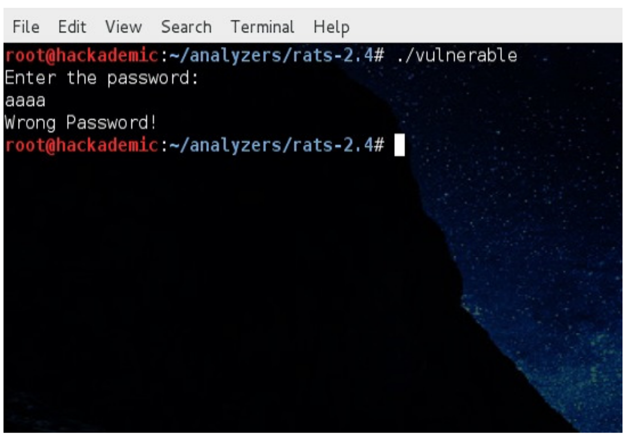


Fig 4: The code compiled and tested with the input aaaa.

In Fig. 4, the program behaves as expected. It reports back to the user wrong password. Let's now run this same program with another input as indicated in Fig. 5.

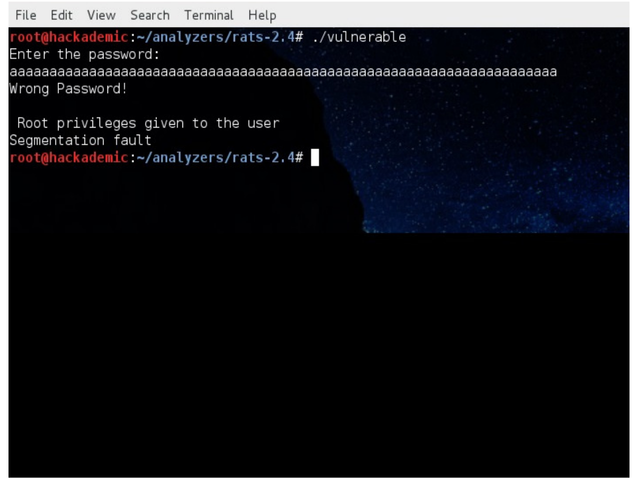


Fig 5: Bypassing the password protection.

In Fig. 5, the password protection was bypassed! What happened here? An input of length greater than what the buffer can hold (12 bytes) was supplied and the buffer overwrote the memory of integer "pass". The password was wrong but the value of "pass" became non zero and as a result root privileges were granted to the unauthorized user. And it can get even worse, the attacker can insert malicious shellcode in the buffer in order to take control of the victim's computer executing the program.

Important lessons that can be learnt are that: Treat all user input as potentially malicious. Always validate user input and check the length. Use fgets() instead of gets(). Use strncmp() instead of strcmp() and Use strncpy() instead of strcpy().

The FlawFinder Tool

Fig. 6 shows another vulnerable code written in C as well

```
#include  <stdio.h>
#include  <string.h>
#include  <stdlib.h>

int main (int argc, char **argv)
{
   char buffer [50];
   int x = 1;
   snprintf ( buffer, sizeof buffer, argv [1]);
   buffer [sizeof buffer -1] = 0;
   printf("Buffer size is: (%d) \nData input: %s \n",
        strlen(buffer), buffer);
   printf("X equals: %d/ in hex: %#x\nMemory address for x:
(%p)  \n", x, x, &x);
   return 0;
}
```

Fig. 6: C Code to be analyzed with FlawFinder.

FlawFinder is a static source code analyzer that is simple to use and runs very quickly. It has a low false positive rate. Also, it allows inline commenting to flag items that are not bugs [6]. If the Flawfinder is run against the vulnerable source code the report of Fig. 7 is generated:

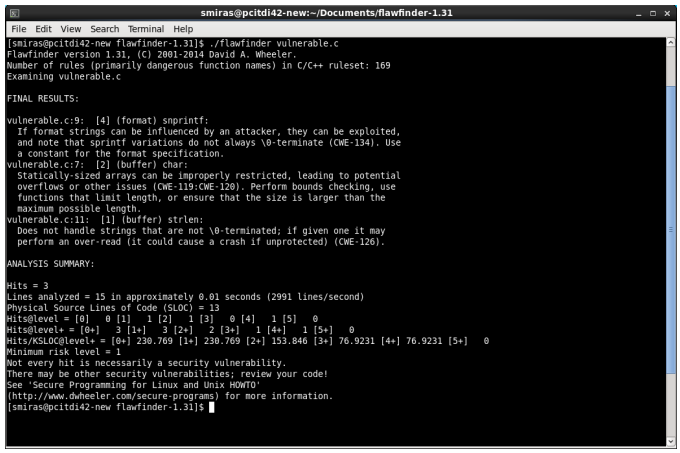


Fig. 7: FlawFinder analysis on the previous code.

As detected by FlawFinder, the program is vulnerable to a format string attack. But let us define what a format string attack really is. The format string attack happens when the submitted data is evaluated as a command instead of a string by the given application. In other words, the attacker can execute malicious code, read the contents of the memory and compromise the system [7].

If the program is run with the string "Steve" the expected name "Steve" is gotten back as input as shown in Fig. 8.

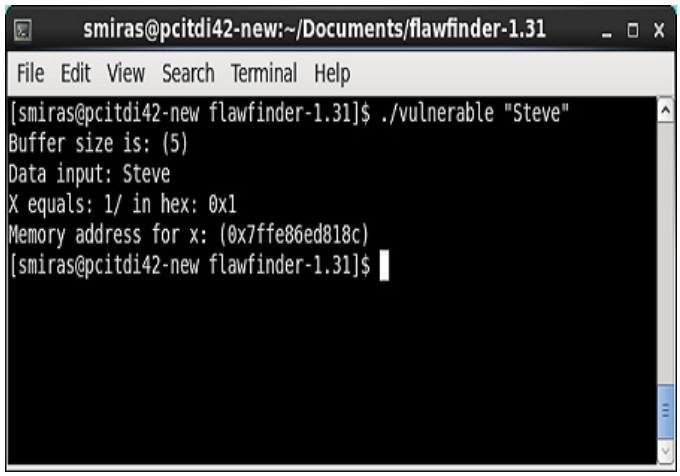


Fig. 8: The code with the user input – Steve.

But what if we supply format string parameters? For example the "%x" format parameter is used to read data from the memory as shown Fig. 9. This could be exploited by a malicious intent hacker over a network to access memory locations. If the format string parameters "%x %x" is inserted as an input then the format function evaluates the last arguments as code and the output will display "Steve" along with the contents of a memory address instead of just "%x %x" as shown in the screenshot of Fig. 8 below. Reading arbitrary data can be just as danger ous as executing arbitrary code. The attacker read a password, a cookie, etc. besides executing malicious code.

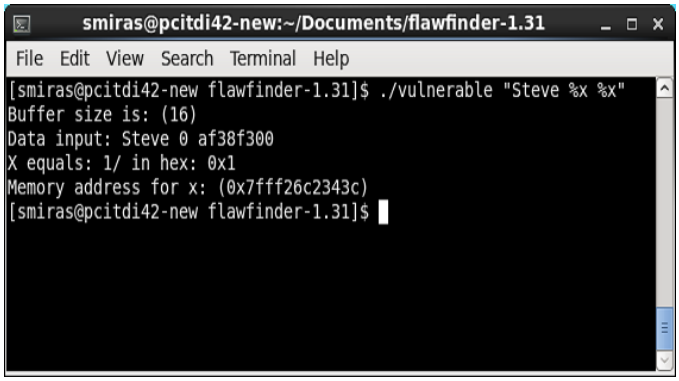


Fig. 9: Format string attack.

Lessons Learnt: Don't write mistakenly printf(buffer) instead of printf("%s", buffer). The first part evaluates the buffer as a format string, and gets any formatting code it may contain. The second part simply prints a string to the screen, as the programmer intended well.

Code Review on a C program fragment

The code listing of Fig. 10 is intended to run on ROOT framework, a framework and library used by physicists working in High Energy Physics to analyze collisions between particles. ROOT is heavily used by the European Organization for Nuclear Research (CERN), Geneva, Switzerland to carry out the analysis of the collisions that occur in the Large Hadron Collider (LHC).

```
0: int func(char* buf) {
1:    strcat(buf, “<default>”);
2:    int pos;
3:    if (buf[0] != ‘<’) {
4:       std::cout << “Number between 0 and 8:\n”;
5:       std::cin >> pos;
6:    }
7:    buf[pos] = 0;
8:    if (!buf) return -1;
9:    return pos;
10:   }
```

Fig. 10: C Code to be reviewed

In the least, 4 errors can be identified in the code fragment above:

i. [No parameter checking]: In the header, you receive a pointer pointing to an address [int func(char* buf)], but you never check whether the pointer received is valid or not. The pointer could be pointing to NULL. Hence pointers should be checked before being used.

ii. [No memory space checking]: The function strcat() appends the 2nd given string to the 1st one. The error here is that there might be some cases where the appending procedure will exceed the available memory pointed by the pointer *buf. This can either cause a crash (best out of the two options) or overwrite the following memory, without giving any error or warning message (effects of this can be disastrous and really hard to identify the source).

iii. [Usage of an uninitialized variable]: int pos; What happens if the if (*condition*) doesn't activate and we go on and execute buf[pos] = 0;? Some Integrated Development Environments (IDE), find these errors fairly easy but others don't and some just give a warning which is usually ignored by the programmer.

iv. [No user input validation]: Inside the if (!buf), you expect a number between 0 and 8, but you never check what you received. User input should be validated before they are used.

These and other errors could be spotted by having peer-reviews. This also poses some problems as it increases the time taken for development. Static analysis tools contain a collection of algorithms and techniques used to analyze source code in order to automatically find bugs. The idea is similar in spirit to compiler warnings (which can be useful for finding coding errors) but to take that idea a step further and find bugs that are traditionally found using run-time debugging techniques such as testing. Static analysis provide a good compromise as they are often fast and are quite versatile. Source Code analyzers can also be integrated into the development environment used. Hence, it could be part of Continuous Integrated Testing

IV. LIMITATIONS OF OUR APPROACH

Static Analyzers are very useful in finding bugs but the user has to bear in mind some things when using it. They are a work in progress and there are always a continuous work to update them. It is therefore the task of the programmer to get the latest versions. Although there are fundamental limitations to what static analysis can do, we have a very long way before we reach the limit and they remain a viable tool for ensuring of writing secure code.

Static Analyzers are meant to find security flaws without the need for compilations but a few are designed to only work when the source code is compiled. This poses a challenge as many times some libraries are not readily available for the developer to compile the code. Sometimes, this is necessary for the Analyzer to know the context of the code. Nevertheless, this could be improved upon. Although analyzers are designed to be faster than compilations, many times it takes longer when analyzing a source code than compiling it. This is because an analyzer evaluates all possible input values and branches. This could lead to exponential time in the worst case scenarios if unbounded. As an addition, they also report cases that rarely occur or very unlikely combinations. They test things that never happen. Many times, this leads to false positives.

V. CONCLUSION AND FUTURE WORK

With the recent increase in the attacks from hackers, it is more important than ever now to use automated tools to fix in-house the vulnerabilities associated with the software prior to its release and thus reduce the effort and time spent in fixing it when attackers gain access to the vulnerability. In this paper we review some source code analyzers otherwise known as static code analyzers. We evaluate various source code analyzers and their result. We also performed code review of a C Code. We then provided rationale for using automated tools and integrating it into the existing development environment.

As part of future work, we plan to analyze a framework written in Python – DBTest – a framework used at CERN to test performance and changes made to databases. It consists of different tests – called checks – that can be performed on databases. It is currently existing but a third check module is being added to it. The module to be added is the Oracle Real Application Testing (RAT). This third type of test allows the replay and analysis of workload captured from production environment before being replayed in a test environment. This is very useful if changes are to be made to the environment and hence the impact of the aforementioned changes could be anticipated before the changes to of the production environment is made. We also plan to conduct source code analysis on a system level administrative program developed in Ruby for Linux platform, and analyze their impacts and develop effective solutions to mitigate the effects as much as possible.

Even though the source codes analyzed here are in C, the solutions and methods derived here are general and could be in fact applied to other programming languages with appropriate modifications when needed.

REFERENCES

[1] K. Nayak, D., M. Petros Efstathopoulos and Tudor Dumitras, "Some Vulnerabilities Are Different Than Others Studying Vulnerabilities and

Attack Surfaces in the Wild", University of Maryland, College Park, pp. 5, 2014

[2] D. Paul, "Bored hackers flick Shellshock button to OFF as payloads shrink" The Register, 2014. Available: http://www.theregister.co.uk/2014/10/03/shellshock_bored_hackers_giving_up_droves//.

[3] H. A. Boyes, P Norris, I. Bryant, and T. Watson, "Trustworthy Software: lessons from 'goto fail' & Heartbleed bugs" pp. 2

[4] N. Maghanathan, "Source Code Analysis to remove security vulnerabilities in Java socket programs: A case study", International Journal of Network Security & Its App lications (IJNSA), vol.5, no.1, 2013

[5] W. Wang, H. Lilong, M. Yunxiu and B. He, "From Source Code Analysis to Static Software Testing", in IEEE Workshop in Advanced Research and Technology in Industry Applications (WARTIA), 2014, pp. 1280Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[6] CERN Computer Security (2015) FlawFinder Available: https://security.web.cern.ch/security/recommendations/en/codetools/flawfinder.shtml

[7] Web Application Security Consortium (2010) Format String Attack Available: http://projects.webappsec.org/w/page/13246926/Format%20String.

Current Survey of Computer Malwares Infestation and Inhibition

Akinde Olusola Kunle, Chukwuchekwa Nkwachukwu, Achumba Ifeanyi Eucharia
Electrical/Electronic Engineering Department,
Federal University of Technology Owerri
Imo State, Nigeria
nkwachukwu.ng.n@ieee.org

***Abstract*—Malware, also known as malicious code or malicious software,refers to a program that is inserted into asystem, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim. They are usually designed to perform these nefarious functions in such a way that users are unaware of them, at least initially.Malware infestations and inhibition before year 2000 centered on system attack, denial of service, and so on. However, beyond year 2000 till date, individuals, corporate bodies, and government of nations have been involved with malicious code design and propagation for distributed network breakdown, as well as, cyberwars. Shared ignorance about the nature of malware's development and propagation has resulted in colossal loss for both individuals and corporate organizations. With new malwares emerging daily to join the thousands in existence, it is evident that the virus issue will not go away any time soon. This paper details the history of malwares and their categories, obfuscation techniques, identification and recommendations for preventing malware incidents to all computer users.**

I. INTRODUCTION

In the 1980s, malware was occasionally a nuisance or inconvenience to individuals and organizations; but today, malware is the most significant external threat to most systems, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations. Malware intended to violate a user's privacy has also become a major concern to organizations. Although privacy-violating malware has been in use for many years, its use became much more widespread in 2003 and 2004, with spyware invading many systems to monitor personal activities and conduct financial fraud.

Shared ignorance about the nature of malware's development and propagation has resulted in the colossal loss for both individuals and corporate organization. With new malwares emerging daily to join the thousands in existence, it is evident that the virus issue will not go away any time soon. In fact, the Institute of Chartered Secretaries and Administrators(ICSA)annual surveys since 1995 suggest that

the problem has gotten worse. Over 99% of responding companies reported a virus incident in 2000, while nearly 67% experienced file problems and 40% suffered data losses from virus attacks. Most companies estimated annual losses from virus attacks between US$100,000 and US$1,000,000 [1].

II. OVERVIEW OF MALWARES

Malware is a generic term used to describe all of the hostile and intrusive program codes including viruses, spywares, Trojan, worms, or anything that is designed to perform any malicious operations on a computer [2]. The meaning of any of these words has changed over time. Some refer to how the malware infects your system, while others are used to describe what the malware does once it is active in a machine.

A. History of Malwares

The concept of the computer virus was actually formed in the early days of computing. The earliest created viruses appeared as benign pranks; it was written in the late 1970s with the aim of assisting in system maintenance. Malicious Malwares did not surface publicly until the early 1980s, when the most common form was compiled viruses, typical among these are boot sector viruses. At that time, virus writers also created several obfuscation techniques so that their viruses could avoid detection. In 1988, the infamous Morris worm was released, and it disrupted innumerable computer networks. Trojan horses equally surfaced in the mid-1980s.

At the early 1990s, the malware state remained largely unchanged, when compiled viruses continued to be the endemic form of malicious code. Nevertheless, in the latter half of the 1990s, quite a lot of changes in computing

produced new opportunities for malware. Virus writers began production of interpreted viruses and circulating them through e-mail, with developing independent worms with related potential.

Worms have been the common form of malware since 2000. Virus writers have preference for worms against viruses since worms multiply more rapidly. In 2001, Nimda was released and it became the first blended attack which caused prime disruptions. Nimda combined the attributes of viruses, worms, and malicious mobile code. Malicious mobile code attacks have recently become ever more common, chiefly due to the dominance of Web browsers and HTML-based e-mail; but, malicious mobile code is yet not as familiar as worms. A significant drift occurs with more of malware; including worms, Trojan horses, and malicious mobile code, present attacker tools, like rootkits, keystroke loggers, and backdoors, to infected computer systems [3]. As faster methods of files transfer became more popular, such as e-mail and file sharing software, attackers developed other types of malware that took advantage of these faster methods to spread rapidly.

Malware infestations and inhibition before year 2000 centered on system attack, denial of service, and so on. However, beyond year 2000 till date, individuals, corporate bodies, and government of nations have been involved with malicious code design and propagation for distributed network breakdown, as well as, cyberwars. Anonymous sources within the U.S. government of late revealed that the United States and Israel were indeed the authors of the Stuxnet worm and related malware, whose primary aim was to sabotage Iran's attempts to make weapons-grade nuclear material [4].

B. Obfuscation Techniques of Malware

To obfuscate is to deliberately make more confusing in order to conceal the truth. Most malwares are created using one or more obfuscation techniques outlined below. If a virus is hard to detect, it is likely to spread more widely and rapidly [5].

Self-Encryption and Self-Decryption: Some viruses can encrypt and decrypt their virus code bodies, concealing them from direct examination. Viruses that employ encryption might use multiple layers of encryption or random cryptographic keys, which make each instance of the virus, appear to be different, even though the underlying code is the same.

Polymorphism: Polymorphism is a particularly robust form of self-encryption. A polymorphic virus generally makes several changes to the default encryption settings, as well as altering the decryption code. In a polymorphic virus, the content of the underlying virus code body does not change; encryption alters its appearance only.

Metamorphism: The idea behind metamorphism is to alter the content of the virus itself, rather than hiding the content with encryption. The virus can be altered in several ways, for example, by adding unneeded code sequences to the source code or changing the sequence of pieces of the source code. The altered code is then recompiled to create a virus executable that looks fundamentally different from the original.

Stealth: A stealth virus uses various techniques to conceal the characteristics of an infection. For example, many stealth viruses interfere with OS file listings so that the reported file sizes reflect the original values and do not include the size of the virus added to each infected file.

Armoring: The intent of armoring is to write a virus so that it attempts to prevent antivirus software or human experts from analyzing the virus's functions through disassembly, traces, and other means.

Tunneling: A virus that employs tunneling inserts itself into a low level of the OS so that it can intercept low-level OS calls. By placing itself below the antivirus software, the virus attempts to manipulate the OS to prevent detection by antivirus software.

Antivirus software vendors design their products to attempt to compensate for the use of any combination of obfuscation techniques.

C. Malware Identification

A virus is a computer program that acts when an infected program is executed. Thus, only executable files can be infected. On MS-DOS systems, these files usually have the extensions .EXE, .COM, .BAT, or .SYS. Another class of files called overlay files can also be infected. These files often have the extension .OVL, although other extensions such as .OV1 are sometimes used.
Most of the cases viruses and worms change their file extensions from ".exe" to some other extensions like ".pif", ".scr" or ".jpeg" etc to trick its victim to download such files from internet or mails and execute it. Since, in most cases, these files are executables, they are executed once the user(s) click on them and infects the user's system.

III. CATEGORIES OF MALWARES

Some of the categories of malware include viruses, worms, Trojan horses, and malicious mobile code, as well as combinations of these, known as blended attacks. Malware also includes attacker tools such as backdoors, rootkits, keystroke loggers, and tracking cookies used as spyware. The discussion of each category explains how it affects systems.

A. Viruses

By definition, computer virus is a self-duplicating computer program that spreads from computer to computer, interfering with data and software. It is able to clone itself, so that it can multiply, constantly seeking new host environments. Just as biological viruses infect people, dispersing from person to person; computer viruses infect personal computers (PCs) and servers [6], [7]. Some viruses

are mere annoyances, but others can do serious damage. The virus payload contains the code for the virus's objective, which can range from the relatively benign. Viruses can delete or change files, steal important information, load and run unwanted applications, send documents via electronic mail (e-mail), or even cripple a machine's operating system (OS). Many viruses have a trigger, a condition that causes the payload to be executed, which usually involves user interaction (for instance, opening a file, running a program, clicking on an e-mail file attachment).

Virus programs, like the infectious microorganisms, are quite minute in size. Only a few lines of program code are required to write a simple virus. Once written, a virus can be conveyed over telephone lines or distributed systems via infected disks to other systems, where it can reproduce in microseconds to damage the biggest systems million miles away. These two facts made it virtually impossible to trace any virus back to the person who originates it. There are two major types of viruses; the compiled viruses, and the interpreted viruses. The two are expatiated briefly.

1. Compiled Viruses

A compiled virus is one that has had its source code converted by a compiler program into a format that can be directly executed by an OS. Compiled viruses typically fall into three categories:

File Infector: A file infector virus attaches itself to executable programs, such as word processors, spreadsheet applications, and computer games. When the virus has infected a program, it propagates to contaminate other programs on the system, as well as, other systems that use a shared infected program. Jerusalem and Cascade are two of the best known file infector viruses.

Boot Sector: A boot sector virus infiltrates the master boot record (MBR) or the boot sector of a hard drive or removable media, such as floppy diskettes. The boot sector is an area at the beginning of a drive or disk where information about the drive or disk structure is stored. Boot sectors contain boot programs that are run at host startup to boot the OS. Removable media, such as floppy disks, need not be bootable to infect the system. If an infected disk is in the drive when the computer boots, the virus could be executed. Boot sector viruses are easily concealed, have a high rate of success, and can harm a computer to the point of making it completely inoperable. Symptoms of boot sector virus infection on a computer include an error message during booting or the inability to boot. Form, Michelangelo, and Stoned are examples of boot sector viruses.

Multipartite: A multipartite virus uses multiple infection methods, typically infecting both files and boot sectors. Accordingly, multipartite viruses combine the characteristics of file infector and boot sector viruses. Examples of multipartite viruses include Flip and Invader. In addition to infecting files, compiled viruses can reside in the memory of infected systems so that each time a new program is executed, the virus infects the program.

2.*Interpreted Viruses*

Unlike compiled viruses, interpreted viruses are composed of source code that can be executed only by a particular application or service. Interpreted viruses have become very common because they are much easier to write and modify than other types of viruses. A relatively unskilled attacker can acquire an interpreted virus, review and modify its source code, and distribute it to others. The two major types of interpreted viruses are macro viruses and scripting viruses.

Macro viruses: These are the most prevalent and successful type of virus. These viruses attach themselves to application documents, such as word processing files and spreadsheets, and use the applications' macro programming language to execute and propagate. Macro viruses use the macro programming capabilities that many popular software packages, such as Microsoft Office, use to automate complex or repetitive tasks. These viruses tend to spread quickly because users frequently share documents from applications with macro capabilities. In addition, when a macro virus infection occurs, the virus infects the template that the program uses to create and open files. The Concept, Marker, and Melissa viruses are well-known examples of macro viruses.

Scripting viruses: are very similar to macro viruses. The primary difference is that a macro virus is written in a language understood by a particular application, such as a word processor, whereas a scripting virus is written in a language understood by a service run by the OS. Examples of well-known scripting viruses are First and Love Stages.

B. Worms

Worms are self-replicating programs that are completely self-contained, meaning that they do not require a host program to infect a victim. Worms also are self-propagating; unlike viruses, they can create fully functional copies and execute themselves without users' intervention. This has made worms increasingly popular with attackers, because a worm has the potential to infect many more systems in a short period of time than a virus. Although some worms are intended mainly to waste system and network resources, many worms damage systems by installing backdoors to perform distributed denial of service (DDoS) attacks against other hosts, or perform other malicious acts. The two primary categories of worms are network service worms and mass mailing worms.

1. Network Service Worms

Network service worms spread by exploiting vulnerability in a network service associated with an OS or an application. Once a worm infects a system, it typically uses that system to scan for other systems running the targeted service and then attempts to infect those systems as well. Because they act completely without human intervention,

network service worms can typically propagate more quickly than other forms of malware. Examples of network service worms are Sasser and Witty.

2. Mass Mailing Worms

Mass mailing worms are similar to e-mail borne viruses, with the primary difference being that mass mailing worms are self-contained instead of infecting an existing file as e-mail borne viruses do. Once a mass mailing worm has infected a system, it typically searches the system for e-mail addresses and then sends copies of itself to those addresses, using either the system's e-mail client or a self-contained mailer built into the worm itself. A mass mailing worm typically sends a single copy of itself to multiple recipients at once. Besides overwhelming e-mail servers and networks with massive volumes of e-mails, mass mailing worms often cause serious performance issues for infected systems. Examples of mass mailing worms are Beagle, Mydoom, and Netsky.

C. Trojan Horses

Named after the wooden horse from Greek mythology, Trojan horses are non-replicating programs that appear to be benign but actually have a hidden malicious purpose. Some Trojan horses are intended to replace existing files, such as system and application executable, with malicious versions; others add another application to systems instead of overwriting existing files. Trojan horses tend to conform to any of the following three models:

1. Continuing to perform the function of the original program and also performing separate, unrelated malicious activity (like, a game that also collects application passwords).
2. Continuing to perform the function of the original program but modifying the function to perform malicious activity (like, a Trojan horse version of a login program that collects passwords) or to disguise other malicious activity (e.g., a Trojan horse version of a process-listing program that does not display other malicious processes).
3. Performing a malicious function that completely replaces the function of the original program (e.g., a file that claims to be a game but actually just deletes all system files when it is run).

Trojan horses can be difficult to detect, because many are specifically designed to conceal their presence on systems and perform the original program's function properly.

The use of Trojan horses to distribute spyware programs has become increasingly common. Spyware is often bundled with software, such as certain peer-to-peer file sharing client programs; when the user installs the supposedly benign software, it then covertly installs spyware programs. Trojan horses also often deliver other types of attacker tools onto systems, which can provide unauthorized access to or usage of infected systems. These tools may be bundled with the Trojan horse or downloaded by the Trojan horse after it is placed onto a system and run. Some well-known Trojan horses are SubSeven, Back Orifice, and Optix Pro.

D Malicious Mobile Code

Mobile code is software that is transmitted from a remote system to be executed on a local system, typically without the user's explicit instruction. It has become a popular way of writing programs that can be used by many different operating systems and applications, such as Web browsers and e-mail clients. Although mobile code is typically benign, attackers have learned that malicious mobile code can be an effective way of attacking systems, as well as, a good mechanism for transmitting viruses, worms, and Trojan horses to users. Malicious mobile code differs significantly from viruses and worms in that it does not infect files or attempt to propagate itself. Instead of exploiting particular vulnerabilities, it often affects systems by taking advantage of the default privileges granted to mobile code. Popular languages for malicious mobile code include Java, ActiveX, JavaScript, and VBScript. One of the best-known examples of malicious mobile code is Nimda, which used JavaScript.

E. Blended Attack

A blended attack is an instance of malware that uses multiple infection or transmission methods. The well-known Nimda is actually an example of a blended attack. It uses four distribution methods:

E-mail: When a user on a vulnerable host opened an infected e-mail attachment, Nimda exploited vulnerability in the Web browser used to display HTML-based e-mail. After infecting the host, Nimda then looksfor an e-mail addresses on the host and then sends copies of itself to them.

Windows Shares: Nimda scans hosts for unsecured Windows file shares; it then uses NetBIOS as a transport mechanism to infect files on that host. If a user runs an infected file, this would activate Nimda on that host.

Web Servers: Nimda scans Web servers, looking for known vulnerabilities in Microsoft Internet Information Services (IIS). If it finds a vulnerable server, it attempts to transfer a copy of itself to the server and to infect the server and its files.

Web Clients: If a vulnerable Web client visits a Web server that has been infected by Nimda, the client's workstation would become infected.

In addition to using the methods described above, blended attacks can spread through such services as instant messaging and peer-to-peer file sharing. Nimda combines the characteristics of viruses, worms, and malicious mobile code.

Another example of a blended attack is Bugbear, which acted as both a mass mailing worm and a network service worm. Because blended attacks are more complex than single-method malware, they are considerably harder to create.

D. RootKits

A rootkit is a collection of files that is installed on a system to alter its standard functionality in a malicious and stealthy way. A rootkit typically makes many changes to a system to hide the rootkit's existence, making it very difficult to determine that the rootkit is present and to identify what the rootkit has changed.

E. Backdoors

A backdoor is a malicious program that eavesdrops for commands on a certain TCP or UDP port. Most backdoors allow an attacker to perform a certain set of actions on a system, such as acquiring passwords or executing arbitrary commands. Types of backdoors include zombies (also known as bots); these are installed on a system to cause it to attack other systems and remote administration tools. They are installed on a system to enable a remote attacker to gain access to the needed systems' functions and data.

The table below compares viruses, worms, Trojan horses, malicious mobile code, tracking cookies, and attacker tools on the basis of key characteristics. Because blended attacks may combine features of any combination of the other malware categories, their specific characteristics cannot be defined using these categories.

IV. PREVENTION AND OTHER INHIBITING OPERATION OF MALWARES

Policies addressing malware prevention must provide a basis for implementing preventive controls. Broad-spectrum malware awareness programs should be mounted for all computer users, as well as, specific awareness training for the IT staff directly involved in malware prevention. Expending effort on vulnerability mitigation can eliminate some possible attack vectors. Implementing a combination of threat mitigation techniques, as well as, tools like the use of antivirus software and firewalls, can help prevent threats from successfully attacking systems and networks [8].

When planning an approach to malware prevention, users should be mindful of the attack vectors that are most likely to be used currently and in the near future. They should also consider how well- controlled their systems are (e.g., managed environment, non-managed environment). Computer users should be aware that no matter how much effort they put into malware incident prevention, incidents will still occur (e.g., previously unknown types of threats, human error). For this reason, computer users and majorly organizations should have robust malware incident handling capabilities to limit the damage that malware can cause and restore data and services efficiently.

A. Policy

Malware prevention related policy should be as general as possible to provide flexibility in policy implementation and reduce the need for frequent policy updates. Common malware prevention related policy considerations include the following:

- Scanning of media from outside of the organization for malware before they can be used.
- E-mail file attachments, including compressed files (e.g., .zip files), be saved to local drives or media and scanned before they are opened.
- Forbidding the sending or receipt of certain types of files (e.g., .exe files) via e-mail and allowing certain additional file types to be blocked for a period of time in response to an impending malware threat.
- Restricting the use of administrator-level privileges by users;
- Requiring that systems be kept up-to-date with OS and application upgrades and patches.
- Restricting the use of removable media (e.g., floppy disks, compact discs (CD), Universal Serial Bus (USB) flash drives, particularly on systems that are at high risk of infection.
- Specifying which types of preventive software (e.g., antivirus software, spyware detection, and removal utilities) are required for each type of system (e.g., file server, e-mail server, and proxy server).
- Permitting access to other networks (including the Internet) only through organization-approved and secured mechanisms;
- Firewall configuration changes should be approved through a formal process;
- Specifying which types of mobile code may be used from various sources (e.g., internal Web servers, other organizations Web servers);
- Restricting the use of mobile devices on trusted networks.

Although all of these considerations are intended to help organizations prevent malware incidents, many of them could also be helpful in detecting or containing incidents.

B. Vulnerability Mitigation

Malware often attacks systems by exploiting vulnerabilities in operating systems, applications, and services. As such, mitigating vulnerabilities is very important to the deterrence of malware incidents, particularly when malware is released shortly after the announcement of a new vulnerability, or before vulnerability is publicly acknowledged. Vulnerability can frequently be mitigated by one or more methods, such as applying patches to update the software, or reconfiguring the software (e.g., disabling a vulnerable service). The under listed techniques could apply to securing nearly any system, but are particularly helpful for protecting against malware.

Patch Management: Patch management involves several steps, these includes assessing the criticality of the patches and the impact of applying or not applying them, testing the patches thoroughly, applying the patches in a controlled manner, and documenting the patch assessment and decision process. It is becoming increasingly challenging to deploy patches quickly enough to prevent incidents. Applying patches is one of the most effective ways of reducing the risk of malware incidents, and many instances of malware

have succeeded because systems were not patched in a timely manner. Patch management is also a key to incident handling.

Least Privilege: The principle of least privilege refers to configuring hosts to provide only the minimum rights to the appropriate users, processes, and hosts. Least privilege can be helpful in preventing malware incidents, because malware often requires administrator-level privileges to exploit vulnerabilities successfully. If an incident does occur, prior application of least privilege might minimize the amount of damage that the malware can cause. Least privilege is usually employed on an organization's servers and network devices, and is sometimes employed by users. Least privilege can be resource-intensive to implement and support; for example, users might not be able to install OS or application updates without administrative privileges.

Other Host Hardening Measurement: In addition to keeping hosts properly patched and following the principle of least privilege where appropriate, organizations should also consider implementing other host hardening measures that can further reduce the possibility of malware incidents. Examples of such measures are as follows:

- Disabling or removing unwanted services (particularly network services), which could contain vulnerabilities;
- Eliminate unsecured file shares, which are a common infection means for worms;
- Removal or changing default usernames and passwords for OSs and applications, which could be used by malware to gain unauthorized access to systems;
- Requiring authentication before allowing access to a network service;
- Disabling automatic execution of binaries and scripts.

Organizations should also perform periodic vulnerability assessments to identify unmitigated vulnerabilities on systems and develop plans for addressing the vulnerabilities. Periodic vulnerability assessments are still important even if all known vulnerabilities on a system have been addressed [9].

Threat Mitigation: In addition to vulnerability mitigation efforts, organizations should perform threat mitigation to detect and stop malware before attacking its targets. There are several types of security tools that can mitigate malware threats; antivirus software, spyware detection and removal utilities, intrusion prevention systems (IPS), and firewalls and routers. Each of these categories describes typical features, the types of malware and attack vectors the tools address, and the methods used to detect and stop malware.

C. Eradication of Malware

Although the primary goal of eradication is to remove malware from infected systems, eradication is typically more involving than that. If an infection was successful because of system vulnerability or other security weakness, such as an unsecured file share, then eradication includes the elimination or mitigation of that weakness, which should prevent the system from becoming re-infected or becoming infected by another instance of malware or a variant of the original threat. Eradication actions are often consolidated with containment efforts. For example, computer users might run a utility that identifies infected hosts, applies patches to remove vulnerabilities, and runs antivirus software that removes infections. Containment actions often limit eradication choices; for example, if an incident is contained by disconnecting infected systems from the primary network, the systems should either be connected to a separate VLAN so that they can be updated remotely, or patched and reconfigured manually. Because the hosts are disconnected from the primary network, the incident response team will be under pressure to perform eradication actions on the hosts as quickly as possible so that the users can regain full use of their systems.

Different situations oblige combinations of eradication techniques. The most common tools for eradication are **antivirus software**, **spyware detection**, and **removal utilities**. Automated eradication methods, such as triggering antivirus scans remotely, are much more efficient than manual methods. However, automated methods are not the best for all situations. For example, an infected host that is attempting to cause major damage to other systems or use large amounts of bandwidth should probably stay isolated from networks and be handled through manual actions.

In some malware incidents, it may be necessary to rebuild infected hosts as part of eradication efforts. Rebuilding includes the reinstallation and securing of the OS and applications, and the restoration of data from known good backups. Because rebuilding a host is typically more resource-intensive than other eradication methods, it should be performed only when no other eradication method or combination of methods is sufficient.

Eradication can be frustrating because of the number of systems to clean up and the tendency during major incidents of having additional infections and re-infections occurring for days, weeks, or months. Incident handlers should periodically perform identification activities to identify hosts that are still infected and estimate the success of the eradication. A reduction in the number of infected hosts would demonstrate that the incident response team was making progress and would help the team choose the best strategy for handling the remaining hosts and allocate sufficient time and resources.

D. Antivirus Software

Antivirus software is the most commonly used technical control for malware threat mitigation. For operating systems and applications that are frequently targeted by malware, antivirus software has become a necessity for preventing incidents. There are many brands of antivirus software, with

most providing similar protection through the following recommended capabilities:

- Scanning critical system components such as startup files and boot records;
- Watching real-time activities on systems to check for suspicious activity; a common example is scanning all e-mail attachments for known viruses as e-mails are sent and received. Antivirus software should be configured to perform real-time scans of each file as it is downloaded, opened, or executed, which is known as on-access scanning.
- It should monitor activity involving the applications most likely to be used to infect systems or spread malware to other systems (e.g. e-mail clients, Web browsers).
- Scanning files for known viruses. Antivirus software on systems should be configured to scan all hard drives regularly to identify any file system infections and, optionally, to scan other storage media as well. Users should also be able to launch a scan manually as needed, which is known as on-demand scanning.
- Identifying common types of malware; viruses, worms, Trojan horses, malicious mobile code, and blended threats, as well as, attacker tools such as keystroke loggers and backdoors.
- Disinfecting files; this refers to removing malware from within a file, and quarantining files, which means that files containing malware are stored in isolation for future disinfection or examination. Disinfecting a file is generally preferable to quarantining it because the malware is removed and the original file restored. But, many infected files cannot be disinfected. Accordingly, antivirus software should be configured to attempt to disinfect infected files and to either quarantine or delete files that cannot be disinfected.

E. Recovery from Malware Incidents

The two main aspects of recovery from malware incidents are restoring the functionality and data of infected systems and removing temporary containment measures. Additional actions to restore systems are not necessary for most malware incidents that cause limited system damage (for example, an infection that simply altered a few data files and was completely removable with antivirus software). Malware incidents that are far more damaging, such as Trojan horses, rootkits, or backdoors, corrupting thousands of system and data files, or wiping out hard drives, it is often best to first rebuild the system or to restore it from a known good backup, then secure the system so that it is no longer vulnerable to the malware threat.

Computer users should carefully consider possible worst-case scenarios, such as a new malware threat that wipes out the hard drives of a large percentage of the organization's workstations, and determine how the systems would be recovered in these cases. This should include identifying who would perform the recovery tasks, estimating how many hours of labor would be needed, and determining how the recovery efforts should be prioritized.

Determining when to remove temporary containment measures, such as suspended services (e.g., e-mail) or connectivity (e.g., Internet access, VPN for telecommuters), is often a difficult decision during major malware incidents. However, if nearly all systems have been patched and cleaned, the impact of a new malware infection should be minimal [10].

V. CONCLUSION

"Prevention is better than cure" is the aged adage. Malwares' infestation can be regularly inhibited or totally prevented through conscious ameliorative measures. There should be caution against accepting external drive(s); access to unauthorized users; opening of mail from sources. Routine check for any invasion via antivirus (AV) scanning is imperative; especially after intensive internet search or when a trace of malfunction is observed. While on network security, use of license software is highly recommended. Besides, regular update (auto-update box should be checked) is indispensable.

With all these in place, malwares crisis could be alleviated, while losses in terms of capitals could equally be curtailed.

REFERENCES

[8] Micro World Technologies Inc. "White Paper", www.mwti.net

[9] Eddy Willems, "VIRUS (COMPUTER)", Microsoft ® Encarta ® 2009. © 1993-2008 Microsoft Corporation

[10] Michael Smith (Veshengro): "the Way Out of the menace, by, © M Smith (Veshengro), April 2008

[11] Willie D. Jones "What the revelations about the U.S.-Israeli origin of Stuxnet mean for warfare" Tech Alert, ieee spectrum, August 2012.

[12] Micro World Technologies Inc. "HISTORY OF VIRUS 2", www.mwti.net

[13] Micro World Technologies Inc. "HISTORY OF VIRUS 3", www.mwti.net

[14] Microsoft® Encarta® 2009. © 1993-2008 Microsoft Corporation

[15] Robert Charette, "Spectacular Cyber Attack Gains Access to France's G20 Files", March 08, 2011
http://spectrum.ieee.org/riskfactor/telecom/internet/spectacular-cyber-attack-gains-access-to-frances-g20-files

[16] Robert Charette, "Smartphones Becoming Gateways to Identity Theft" Fri, February 24, 2012 http://spectrum.ieee.org/riskfactor/telecom/wireless/smartphones-becoming-gateways-to-identity-theft

[17] Computer Viruses : The Disease, the Detection, and the Prescription for Protection: Hearing ...by United States, Congress House Co. 2003
http://www.valorebooks.com/textbooks/computer-viruses-the-disease-the-detection-andtheprescription-hearing-before-the-subcommittee-on-telecommunications-and-the-internetofthe-committee-on-energy-and-commerce-hous/9780160715648

Metaheuristic Algorithm for Optimizing Green Computing Awareness for Environmental Sustainability and Economic Security as a Stochastic Optimization Problem in Sub-Saharan Africa

Emmanuel Okewu
Centre for Information Technology and Systems
University of Lagos
Lagos, Nigeria
okewue@unilag.edu.ng

Obey Haruna
Department of Geography
Nasarawa State University
Keffi, Nigeria
obbey@yahoo.com

***Abstract*— Using Nigeria as a test case, this paper gauges the green computing awareness level of Africans via sample survey. As part of effort to institutionalize green computing maturity model, we attempt to optimize the level of citizens awareness amid inherent uncertainties. The measure is to promote environmental friendly computing using web-based stakeholders interaction. Although there are alternative ways of promoting Green Computing education, a metaheuristic search indicated that an online real-time solution that not only drives but preserves timely conversations on electronic waste (e-Waste) management and energy saving techniques among the citizenry has cutting edge. Heightened focus on green computing is against the backdrop that Africa is feared to suffer most from the vulnerability of climate change and impact of environmental risk. Green Computing refers to the efficient utilization of computers and accessories such that they contribute minimally to environmental degradation. These devices are known to contain harmful chemicals and emit gaseous emissions when in use and out of use. It also encompasses efficient energy utilization. Given likely uncertainties posed by low bandwidth, poor network and erratic power to such a web-based effort to scale up users awareness in a typical emerging market such as Africa, we consider the problem to be a stochastic optimization problem and applied appropriate computational algorithm. The technology-based solution is a web-based multi-tier e-Green Computing system that educates computer users on innovative techniques of managing computers and accessories in an environment-friendly way. The authors therefore reviewed literature, gathered requirements, modeled the proposed solution using Universal Modelling Language (UML) and developed a prototype. An interactive forum such as a real-time web-based interaction has great potential for not only stimulating the interest of the common man in environmental-related issues of his use of ICT, but also creating awareness about the impact his computer-related activities have on mother earth. This way, he willing becomes part of the solution to environment degradation in his circle of influence.**

Keywords*— *Green Computing; Economic Security; Environmental Sustainability; Information Economy, Sub-Saharan Africa;

I. INTRODUCTION

In recent times, there has been unprecedented growth in Africa's cyberspace. This is particularly so as more original equipment manufacturing (OEM) companies are imbibing the philosophy of inclusive innovation, propelling them to development relatively cheap technologies that fit the purchasing power of users in developing economies. Hence, cheaper phones, computers, telecommunication equipment and other accessories purposely built for emerging markets are strengthening the vision of digital inclusion. However, associated with this development is the need to promote environmentally sustainable computing that limits the impact of global warming and environmental degradation. This is particularly concerning in that projected figures of Africa's vulnerability to climate change and environment risk by global environmental assessing bodies like IPDA, UN etc are quiet alarming. Already, flash flood, gully erosion, coastal erosion, and desert encroachment are threatening livelihood, posing economic insecurity challenges, and in extreme cases, culminating in humanitarian crisis.

Green computing is the study and practice of designing, manufacturing, using, and disposing of computers, servers, and associated subsystems — such as monitors, printers, storage devices, and networking and communications systems — efficiently and effectively with minimal or no impact on the environment [1]. Preliminary investigation revealed that despite the expansion of Africa computing community, there is low level of green computing awareness. The implication is that Africans continue to use ICT to support their with little concern for the adverse impact of computing on the environment. Meanwhile, computing by both corporate and individual users have been known to scale up global warming through carbon emission, degrade the environment through release of hazardous chemicals, and deplete energy availability. Many computing businesses depends on fuel generators for power supply in the absence of regular electricity from national grids. Carbon is present in every hydrocarbon fuel (coal, petroleum, and natural gas) and is released as carbon dioxide (CO_2) when they are burnt.

Conversely, non-combustion energy sources—wind, sunlight, hydropower, and nuclear—do not convert hydrocarbons to CO_2 which is a heat-trapping greenhouse gas [2,3]. Scientists have pointed to the effects on the climate system of releasing greenhouse gases (GHGs) into the atmosphere. Nonetheless, since cost-benefit analysis indicates that the benefits of ICT way outweighs its costs, measures have to be put in place for environmentally sustainable usage of ICT in Sub-Saharan Africa.

In this work, we proposed that one of such measures is stepping up green computing awareness in Africa's cyberspace. Educating computer users will empower them with the right information to be innovative and creative about the use of ICT facilities vis-a-vis the environment. An adequate green computing campaign can be launched in each African country in the fight against the adverse effect on climate change. Although a number of campaign initiatives are available, we concern ourselves basically with the solution option with maximum impact. Hence, we investigated an optimization problem. For the success of any green computing campaign nationally, support from government in terms of resources and enforcement systems are needed. It is therefore a source of concern that Africa's socio-economic landscape is characterised by deficient legal system, poor regulatory framework, weak institutions, infrastructure deficit, near non-existent standards, among others. The combined effect is a precarious climate that breeds corruption, mutual distrust and low productivity across all sectors, including the computing sector. This underscores the fact that the decision to optimize green computing awareness in a social-economic system with stochastic behaviour is a stochastic optimization problem.

Having classified the problem, we identified effective actions that could move the process from one state to another along the green computing awareness creation value chain as knowledge gap analysis, identification of suitable campaign initiative in socio-cultural context, application of preferred initiative and finally impact assessment of initiative on computer users behaviour. We then mathematically modelled the African green computing awareness decision environment as sequential decision making under uncertainty using stochastic finite automaton. Subsequently, the authors applied metaheuristic algorithm to the sequencing and selection process to ascertain the best-known awareness campaign initiative to be used. The outcome led to the design and development of a web-based e-Green Computing system using component-based software engineering (CBSE) approach. The proposed n-tier solution is aimed at promoting environmentally sustainable computing education for positive behavioural change towards the environment.

The remainder of this paper is made up of the following: Section 2 gives the background of study and related work; Section 3 presents the methodology and the selected case study; section 4 focuses on results and discussions; and finally, the paper is concluded in section 5.

II. BACKGROUND AND RELATED WORK

A. Electronic Waste

Electronic waste, or e-waste, is a term for electronic products that have become unwanted, discarded, non-working or obsolete, and have essentially reached the end of their useful life, but can be useful to some people or industry as raw material. Because technology advances at such a high rate, many electronic devices become "trash" after a few short years of use. In fact, whole categories of old electronic items contribute to e-waste such as VCRs being replaced by DVD players, and DVD players being replaced by blu-ray players. E-waste is created from anything electronic: computers, TVs, monitors, cell phones, PDAs, VCRs, CD players, fax machines, printers, etc.

B. Metaheuristic Algorithm for Optimal Green Computing Awareness

Our study assessed a number of potential initiatives for creating users awareness on green computing in the African context. The initiatives examined are:

- establishing functional regulatory bodies;
- use of traditional media awareness;
- use of web-based social media;
- organizing workshops and seminars;
- establishing waste collection and quantification systems; and
- organizing road walk campaign

An emerging market such as Africa is characterized uncertainties [4] predicated on constraints such as resource availability, literacy level, infrastructure deficit, epileptic power supply, weak institutions, among others. Hence, our decision to create optimal green computing education in a geo-political space with stochastic (probabilistic) behaviour exhibits trappings of stochastic finite automaton [5] as shown in Fig. 1.

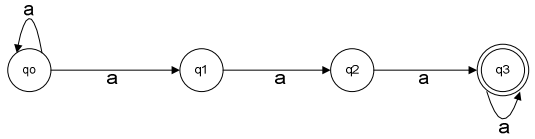


Fig. 1. Stochastic finite automaton for green computing awareness creation process

This is mathematically expressed as M* = (Q,A,q_0,∂, p, F) where

Q is a finite set of states;
A is a non empty set of actions;
$q_0 \in Q$ is the initial state;
F Q is the set of final states;
Q A Q is a finite set of transition between states; and
p is a function ∂ [0,1] such that all $q \in Q$ and for all a $\in$ A
$\sum p(q, a, q') = 1$

A finite state automaton is stochastic if the transition rules are defined by transition probabilities and initial and final states are defined by probability distributions [6]. In this instance, the inputs into the sequential decision making process of the green computing awareness campaign are:

a_0 = Knowledge gap analysis of computer end-users in Sub-Saharan Africa
a_1 = Identification of suitable campaign option for creating maximum awareness in the socio-cultural context of each African country
a_2 = Application of identified approach
a_3 = Evaluation of the impact of applied approach

The function P ($\partial \rightarrow [0,1]$) means that probability is assigned to the occurrence of the outcomes.

In any case, the research focus was to get the best way to execute the campaign, taking into cognizance each socio-cultural context. This means optimal decision has to be taken amid uncertainties that are hallmarks of developing economies in Africa. We therefore x-rayed each of the green computing awareness-creating initiative, focusing on capacity to engineer environmentally sustainable computing behavioural change measured by power of attraction, speed of message delivery, and message retention.

Since the solution space is populated with viable alternatives, with each having potential for delivery, the quest for the best-known solution took centre stage. The researchers thus applied Tabu Search - a metaheuristic algorithm as follows:

```
s ← s0
sBestInitiative ← s
awarenessTabuList ← null
 while (not awarenessSearchStoppingCondition())
    awarenessCandidateList ← null
    for(awarenessCandidate in searchNeighborhood)
        if(not containsTabuElements(awarenessCandidate,
        awarenessTabuList))
            awarenessCandidateList ← awarenessCandidateList
            + awarenessCandidate
        end
    end
    awarenessCandidate ←
    LocateBestAwarenessCandidate(awarenessCandidateList)
    s ← awarenessCandidate
    if(fitness(awarenessCandidate) > fitness(sBestAwareness))
      awarenessTabuList ←
      featureDifferences(awarenessCandidate,
      sBestAdmission)
      sBestAwareness ← awarenessCandidate
      while(size(awarenessTabuList) >
          maxAwarenessTabuListSize)
          ExpireFeatures(awarenessTabuList)
          s ← awarenessTabuLIstFirstElements
       end
   end
 end
 return(sBestAwareness)
```

Specific actions that are verifiable. It has profound negative implications. Think through several ways to ... A topic of conversation.

Using parameters likes power of attraction, speed of message delivery and message retention capability, the metaheuristic search indicated that of all the afore-mentioned green computing enlightenment strategies, a web-based social media platform would best serve the purpose of maximum green computing awareness. Hence, we applied design and software engineering skills to actualize an n-tier web-based e-Green Computing system. Specifically, component-based software engineering (CBSE) approach was applied

Meanwhile, mathematically, the optimization problem is:

Max
Green Computing awareness
Subject to
Availability of funds
Access to network infrastructure
Literacy level

C. Related Work

Some of the previous efforts that are related to the subject matter in the literature are presented as follows.

Saha [7] defined green computing as the practice and procedures of using computing resources in an environment friendly way while maintaining overall computing performance. The author carried out a survey of several important literature that focused on the field of green computing and stressed the importance of green computing for sustainable development. The study emphasized that the United Nations Framework Convention on Climate Change (UNFCCC) has been working assiduously to achieve its objective of preventing dangerous anthropogenic (human induced) climate change. Already, due to global warming consciousness, regulations and laws related to environmental norms are compelling manufacturers of ICT equipments to meet various energy requirements. The paper concluded that green computing is a well balanced and sustainable approach towards the achievement of a greener, healthier and safer environment without compromising technological needs of the current and future generations. Though the study highlighted efforts being made globally to promote environmentally tolerable behaviours, it did not state specifically state how to optimize green computing awareness in a emerging economy like Africa that is faced with uncertainties. This is the main motivation for our work.

Mittal and Kaur [8] conducted a survey to gauge the common man's understanding of issues related to green computing. A survey questionnaire incorporating major green computing was administered in the first instance as a pilot study before the actual survey. The paper opined that green computing is an effective approach aimed at energy efficient products. The authors are of the view that with the aid of green computing we can save lot of energy and protect our environment from the harmful impacts of computers and associated devices. While decrying the low-level of awareness about the harmful impacts of the use of computer on environment, the study stressed that most of the CO_2 emission is produced through the heat generated by computer and its devices. Another challenge posed to the environment by computing is energy consumption by various computing devices. Despite comprehensively highlighting factors related to green computing and measuring common man's awareness

level of the subject, the study stopped short of suggesting ways to scale up awareness level. Neither did it consider making nor implementing such a decision under uncertainty like this African study presents.

Shinde et al. [9] is an expository study on green computing also called green technology. The paper posited that it is the environmentally sustainable use of computers and related resources like - monitors, printer, storage devices, networking and communication systems - efficiently and effectively with minimal or no impact on the environment. The work stressed that its (green computing) goals are to reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste. The study observed that the upsurge in the use of computers for domestic, official and business purposes has led to unprecedented increase in the amount of electricity consumed by them which translates into increase in the carbon content of the atmosphere. Against this reality, measures are now being taken by people to minimize the power usage of computers as reduced energy usage from green computing techniques translates into lower carbon dioxide emissions, stemming from a reduction in the fossil fuel used in power plants and transportation. Conserving resources means less energy is required to produce, use, and dispose products just as energy and resources prudence saves money. The researchers concluded that green computing encompasses changing government policy to encourage recycling and lowering energy use by individuals and businesses. Though the authors mentioned that people are taken appropriate measures, they were not specific. In our study, we advocate a cohesive national programme for raising green computing awareness among teeming computer users.

Therese and Albert [6] worked on stochastic finite automata as a mathematical model for sequential decision making under uncertainty. They emphasized those decisions such as launching a comprehensive green computing campaign in an emerging economy can be complex in nature and may involve uncertainty to some extent. While a decision environment is collection of information, alternatives, values, and preferences available at the time of decision, a sequential decision problem comprises of n sequential states which may be independent or interdependent. Thus, action must be taken at each state and we need a sequence of actions to arrive at a solution. Decision made at one state owing to an action is passed on to next state and the overall decision depends on the decisions made at each state. The study reiterated that stochastic finite automata are suitable for the construction of mathematical models of complex systems having stochastic in a finite way. The authors concluded that a finite state automaton is classified as stochastic if the transition rules are defined by transition probabilities just as initial and final states are defined by probability distributions. Though the study did not specifically focus on the green computing awareness problem, it provided a framework for rightly classifying such an excercise in an emerging economy with trademark uncertainties and instabilities.

Silberholz and Golden [10] compared metaheuristics in terms of both solution quality and runtime. They opined that since metaheuristics were designed to give solutions of good quality in runtimes better than those of exact approaches, to be meaningful; they must give acceptable solutions within reasonable time. To compare two algorithms in terms of solution quality, a metric to represent the solution quality is needed and comparison should be done over same problem instances as comparison over different instances are weaker since they have different structures, optimal values and difficulties. Besides demonstrating good solution quality, another critical necessity is that they must have a fast runtime. Else, there would be no justification for choosing these approaches over exact algorithms. The authors stressed that runtime comparisons were some of the most difficult comparisons to make. This is aggravated by the difficulties in comparing runtimes of algorithms that compiled with different compilers and executed on different computers, potentially on different testbeds. Despite comparing and discussing how to secure greater value from optimization techniques, the work did not dwell on optimizing green computing awareness under uncertainty.

Glover [11] chronicled the creation of Tabu Search. It is a metaheuristic algorithm that can be used for solving stochastic optimization problems - problems where an optimal sequencing and selection of best-known solution is required under uncertainty. The author emphasized that local (neighbourhood) searches such as picking best-known green computing awareness creation strategy from a pool of strategies take a potential solution to a problem and check its immediate neighbours with a view to finding an improved solution. Since local search methods have a tendency to become stuck in suboptimal regions or on plateaus where many solutions are equally fit, Tabu Search pushes the limits by enhancing the performance of these techniques via memory structures that describe the visited solutions or user-provided sets of rules. In the event a potential solution has been previously visited within a certain short-term period or if it has violated a rule, it is marked as Tabu (forbidden) so that the algorithm does not consider that possibility repeatedly. Among other application areas, the author confirmed that it is also used in resource planning - this is key to mobilizing human and material resources towards environmentally sustainable computing. Though the study outlined the modus operandi of Tabu Search as a metaheuristic algorithm that could be used to tackle resource planning problem, it was silent on the impact of green computing awareness on environmental sustainability and economic security.

III. METHODOLOGY - THE E-GREEN COMPUTING SYSTEM

To identify the requirements for the e-Green Computing system and get an insight into current trend in cyberspace, relevant literature were consulted, interviews held, questionnaire administered and the Nigerian cyberspace observed as a reasonable representation of Sub-Saharan Africa.

Green computing process and procedures were modelled using the Universal Modeling Language; specifically we used use cases, collaboration diagrams, sequence diagrams, class diagram and deployment diagram.

The Microsoft SharePoint was then used as implementation platform for a prototype after designing and developing the proposed solution leveraging CBSE approach. The proof-of-technology was set up at the Centre for Information Technology and Systems (CITS), University of Lagos, Lagos, Nigeria and tested from Abuja and Lagos respectively. Microsoft SharePoint supports four major components namely: Document Library, Custom List, Task and Site. The tool was used because it supports the doctrine of component reusability with COM+ as its component model. It is also a web-based platform that supports distributed computing.

The researchers performed a number of controlled experiments using real-life and simulated data. The participants in the experiments had ample opportunity to interact with the system. Thereafter, they shared their insights on the potency of the proposed social-media application to drive online real-time conversations between green computing stakeholders, achieve the goal of promoting environmental friendly computing education and ultimately stimulate appropriate end-users behaviour. The authors then evaluated possible threats to research outcome.

We used Nigeria as a case study amid established concerns that it has one of the largest ICT users population on the African continent. Using the objective-methodology mapping in the Table 1, we embarked on the CBSE lifecycle activities to actualize the proposed e-Green Computing system as a measure for promoting environment-friendly computing behaviours in the African cyberspace and computing community.

TABLE 1. OBJECTIVE- METHODOLOGY MAPPING.

SN	Objective	Methodology
1.	To drive online real-time conversation on environmentally friendly computing in the African cyberspace	Design and implement an e-Green Computing system
2.	To ascertain proposed system can bring about desired end-users behaviour.	Verify and validate the e-Green Computing system

A. Requirements Analysis and Specification

In this section, we give a breakdown of the requirements for the e-Green Computing system. The requirements were gathered by interview, questionnaire and observation of the Nigerian cyberspace and computing community. The social functions required are *add information, access information, edit information, and delete information* (Table 2) while the non-functional requirements include quality requirements such as performance, security, usability, aesthetics, availability, reliability, scalability, fault tolerance, modifiability, portability and interoperability. The web-based n-tier e-Green Computing system incorporates mechanisms that respond to these requirements.

TABLE 2. FUNCTIONAL REQUIREMENTS.

Requirement ID	Requirement	Brief Description
R01	Add Information	The system shall allow computer users to add information on green computing techniques based on assigned rights and privileges
R02	Access Information	The system shall allow computer users to retrieve and view information on green computing practices within assigned rights and privileges
R03	Edit Information	The system shall allow computer users to edit information related to environmentally friendly computing in line with assigned rights and privileges
R04	Delete Information	The system shall allow users to delete information from the database based on allocated rights and privileges

Use Case modelling was used (Fig. 2) to consolidate requirements analysis in a bid to comprehend the core functionalities and usage scenarios associated with the proposed system's requirements. The researchers incorporated the Use Case diagram to capture the functional aspects of the e-Green Computing system by visually representing what transpires when an actor interacts with the system [12].

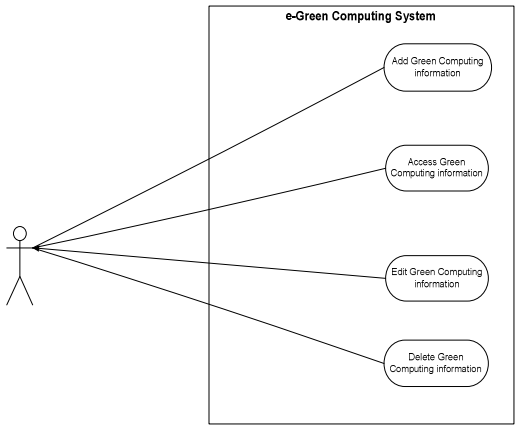


Fig. 2: Use Cases for e-Green Computing System.

The use cases empower the computing community to articulate and share information on global best practices on e-waste management, carbon emission and computer-related energy efficiency schemes. The end goal is to promote environmentally acceptable computing habits and behaviours.

B. System and Software Design

Component reusability and distributed computing are closely linked in an enterprise application such as e-Green Computing system. To leverage on this relationship, we designed the n-

tier enterprise architecture for the proposed solution incorporating mechanisms that respond to user requirements. The n-tier architecture is made up of presentation layer, logic layer and database layer. While corporate and individual ICT users operate at the presentation layer as end-users using devices like personal computers and phones to contribute or access information on environmentally tolerable practices, the logic layer made of clustered application servers process the information which is stored in the database layer. The essence of networking these layers is to make dialogue online real-time.

The interfaces between the respective e-Green Computing components are captured in the component diagram in Fig. 3. The role of component model (COM+) in this architecture is critical as it provides standards and support services to components though they are not represented physically in the software architecture in line with best practice [13]. The interdependence between *Add Information, Access Information, Edit Information and Delete Information* as graphically shown underpins the reality that conversations on green computing initiated by one party can be supported or debunked by another and it is expected that such healthy online social media debate will translate into enlightened computers users with responsibility for the environment. Hence, appropriate habits and behaviours towards the environment are cultivated. And this way, the green computing awareness campaign would have made significant impact on the environment.

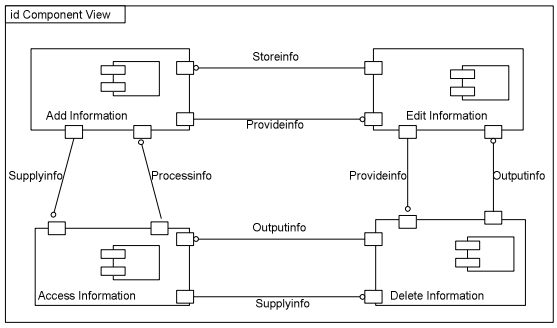


Fig. 3. e-Green Computing component diagram

The e-Green Computing reusable components (*Add Information, Access Information, Edit Information and Delete Information*) were subsequently built using Microsoft SharePoint standard components.

The class diagram for the e-Green Computing system is given in Fig. 4.

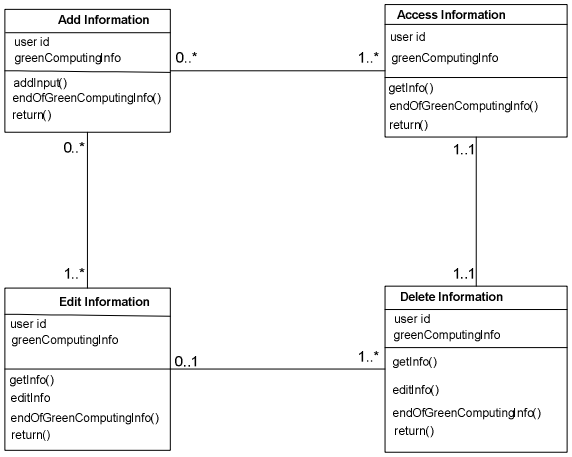


Fig. 4:. e-Green Computing class diagram.

Other design tools we used include collaboration diagram, sequence diagrams, class diagram, analysis class, design component and elaborated design class, class elaboration, algorithm, composite (appropriate) interfaces, and elaborated deployment diagram [14, 15].

The researchers used deployment diagram to represent the location of key packages or components of the e-Green system [14] . The study equally used class elaboration and algorithm to present abstraction details of the components and social functions of the proposed e-Green Computing system.

The e-Green Computing algorithm design is as follows:

```
Procedure addGreenComputingInfo()
  greenComputingInfo ← " "
  while (not endOfGreenComputingInfo())
  greenComputingInfo ← addInput()
return(greenComputingInfo)

Procedure accessGreenComputingInfo()
  while (not endOfGreenComputingInfo())
  getInfo(greenComputingInfo)
return

Procedure editGreenComputingInfo()
  while (not endOfGreenComputingInfo())
  getInfo(greenComputingInfo)
  editGreenComputingInfo()
return(greenComputingInfo)

Procedure deleteGreenComputingInfo()
  while (not endOfGreenComputingInfo())
  getInfo(greenComputingInfo)
  deleteGreenComputingInfo()
return(greenComputingInfo)
```

C. Implementation and Unit Testing

The study used Microsoft SharePoint as the development platform for the tailor-made e-Green Computing system. The testbed was set up at the Centre for Information Technology

and Systems (CITS), University of Lagos, Lagos, Nigeria. SharePoint is a web-based enterprise development tool that makes components available for reuse, the components are also called services. It uses Microsoft COM+ as the component model and provides an integrated development environment (IDE). Its core components include Document Library, Custom List and Tasks, which are not only independent but are distributed (Gorton, 2011). We developed the e-Green Computing system on an incremental basis. The minimal e-Green Computing system to start with was the *addInformation* module. Other modules were added subsequently. Since blackbox testing is more suitable for component-based systems, the authors used it [16].

D. System Integration

With *addInformation* as minimal e-Green Computing system, regression test was conducted as more modules were interfaced to ascertain that there were no interface errors. Else, if they existed, debugging took place before adding another module. In the final analysis, the *addInformation* function was the most tested component in the e-Green Computing system. It is the most referenced component in the proposed system. Test cases were developed and used to test the various components prior to integrating them. Then we used system test cases at the point of integration for regression tests. As expected of component-based systems, black-box testing was performed for all components [17]. Table 3 shows the function points.

TABLE 3. COMPONENT TESTING - FUNCTION POINTS

SN	Component	Function Points
1.	e-GreenComputing	addGreenComputingInfo(), accessGreenComputingInfo(), editGreenComputingInfo(), deleteGreenComputingInfo()

E. System Verification and Validation

The researchers verified and validated the process-correctness and requirements-compliance of the e-Green Computing architecture by assessing the various software representations - requirements documents, design documents and program code. We focused on ensuring that user requirements were well catered for in each software representation in the build-up process. We likewise ensured that the software product met both operational needs of users and emergent properties.

F. Operation Support and Maintenance

A compliment of technical personnel and end-users were trained to test-run the application. While the end-users operated the software, the technical staff provided sustained support.

IV. RESULTS AND DISCUSSION

The study extracted information and measured outcomes in two ways - software experiment and sample survey of computer users. We also evaluated possible threats to the research outcomes. Our evaluation mechanics are presented as follows:

A. Results of Software Experiment

The e-Green Computing site was created as a community site using Microsoft SharePoint enterprise development platform. As the name goes, it is a site where cyberspace members discuss topics that bother on environmentally friendly utilization of computers and accessories. The underlying message of this software engineering is that conscious and concerted efforts towards preventing computer-related environmental degradation can add mileage to ongoing global efforts to mitigate the adverse effect of climate change. This is to be achieved by leveraging online real-time discussion between cyberspace participants on new techniques of green computing. We set up an experimental design in University of Lagos, Nigeria precisely at the Centre for Information Technology and Systems (CITS) and test-run the system from near (Lagos environs) and remote location like Abuja, both in Nigeria. By this act, the researchers used a multi-tier web-based e-Green Computing system to mimic the sensation of sustained dialogue between African computing community members.

The simulation experiment affirmed that ICT could be instrumental to solving the problem e-waste and energy conservation management through sustained online real-time green computing conversations and education. The subjects who participated in the experiment concurred that the output of the experimental survey was a seamless and robust online real-time communication among cyberspace stakeholders on topical green computing services that geared toward the protection and management of the environment. The end game is that the e-Green Computing dialogue framework engendered a sense of users awareness on the role green computing plays in environmental sustainability and economic security. Though we experienced platform-dependent and hardware-dependent challenges particularly testing from remote location like and Abuja, this buttressed the fact that the problem is a stochastic optimization problem in which we attempted to maximize the gains of creating green computing awareness under uncertainty.

Figs. 5 - 7 are snapshots from the experiment.

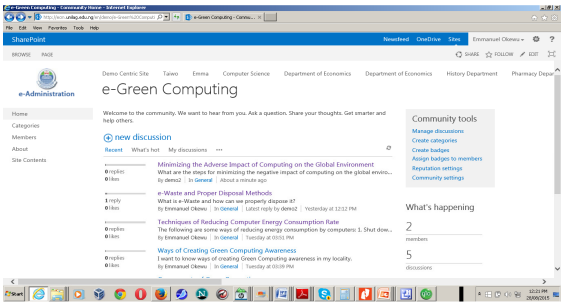


Fig. 5. The e-Green Computing site showing community discussion forum for computer users on environmental-friendly computing techniques.

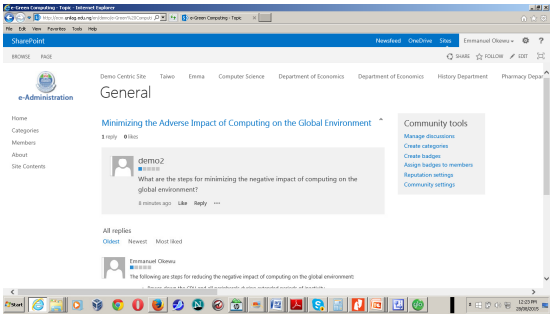


Fig. 6. Sample posting by a user seeking to know ways of minimizing the negative impact of computer usage on the environment.

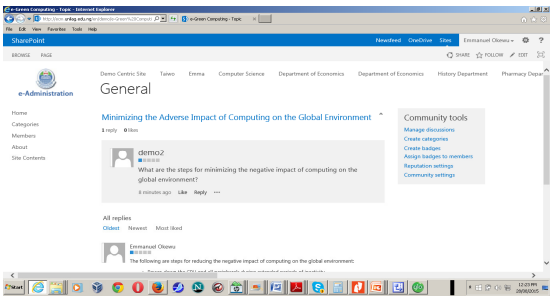


Fig. 7. A respondent outlines techniques for mitigating the adverse effects of computing on the environment.

B. Results of End-users Survey

We substantiated our assertion that there is low-level of green computing awareness in Africa by providing empirical data from survey conducted in University of Lagos. For sample survey, we targeted ICT professionals to gauge their level of green computing awareness. Of the total questionnaire administered, we retrieved 20. Their responses are tabulated in Table 4.

TABLE 4. SAMPLE SURVEY RESPONSES.

SN	Statement	Response			
		Yes	No	Abstained	Total
1.	Familiar with Green Computing?	3 (15%)	15 (75%)	2 (10%)	20 (100%)
2.	Green Computing is also referred to as environmentally sustainable computing?	4 (20%)	12 (60%)	4 (20%)	20 (100%)
3.	The goal of Green Computing is to reduce the hazardous material and save our environment	7 (35%)	11 (55%)	2 (10%)	20 (100%)

Fig. 8 presents graphical view of respondents' responses.

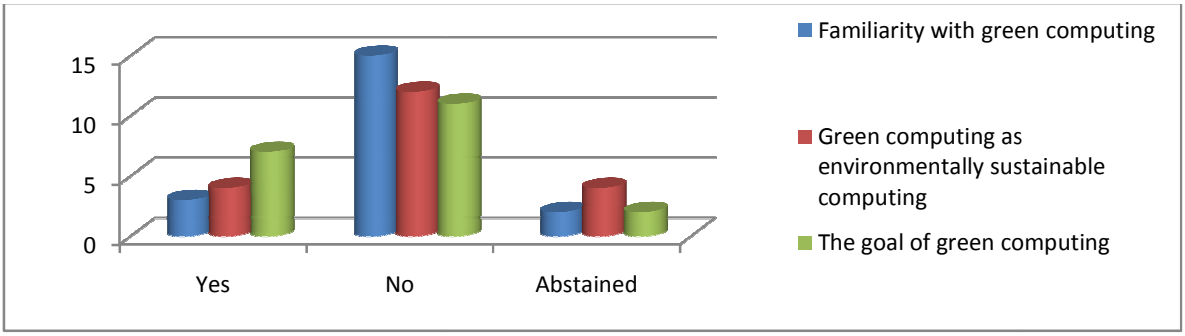


Fig. 8. Graphical view of respondents' responses.

From the above respondents' responses, a whooping 75% of the ICT professionals surveyed indicated they had no knowledge of green computing while a paltry 15% are in the affirmative and 10% refrained from answering. Using this as benchmark to measure the level of green computing awareness among the computer users in the African cyberspace, it is apparent that the continent is lagging behind in environmentally acceptable computing behaviours. Juxtaposing this with the continent's predicted disturbing figures for climate change vulnerability and environmental risk, there is clearly a problem to address as environmental destruction now results in decimation of livelihoods, economic insecurity and humanitarian crisis. Hence, this attempt to optimize green computing awareness even under uncertainties that are typical of an emerging socio-economic system like Africa's.

C. Evaluation Threats

There is the possibility that an elaborate evaluation of the different components of the e-Green system could unearth new perspective of things. In any case, the subjects (who are Nigerians) that participated in the application test run and sample survey have the required experiential knowledge of the Nigerian cyberspace. They equally had sufficient practical engagements with the e-Green system. This offered them good basis to make objective of the impact of the proposed solution on the green computing awareness campaign. Therefore, there is sufficient reason to take their views seriously [18, 19, 20, 21].

Equally important is the fact that only a select number of computer users where involved in the test run and sample survey, which could in a sense limit the statistical significance of the outcome [22, 23]. However, the outcome of the sample survey confirmed low-level green computing awareness in the Nigeria computing environment and underscored the need to upgrade efforts in this regard. Likewise, result of the prototype experiment clearly indicates that online real-time sharing of information on moderns steps to green computing could go a long way in achieving environmentally acceptable behaviours. This is considered to be a good result in that at this point in the project, the core objective is to gain a first impression of the degree of green computing awareness that can be created by the e-Green Computing system amid uncertainty characterising the Nigerian socio-economic terrain. So, inspite the constraint of using a limited number of evaluators, there is sufficient grounds to conclude that there is a positive and preferential disposition to the e-Green Computing system as a tool for promoting environmentally sustainable computing. It means even in the face of socio-economic uncertainties, optimizing green computing awareness via online real-time interactions is a reality. We can thus generalize that applying metaheuristic algorithm to the quest for optimal green computing education can enhance environmental sustainability and economic security in Sub-Saharan Africa.

V. CONCLUSION

The rapid growth of Africa's computing community means a cohesive programme of managing solid e-Waste, carbon emission, and conserving energy for other developmental purposes is required. This will ensure that Africa's contribution to global warming and environmental degradation is mitigated. Governmental regulation apart, there is need for self-discipline by computer users and this can be achieved to proper green computing education and awareness campaign. This study identified various ways national green computing campaigns can be carried out in Africa's socio-cultural context. The researchers considered that despite the emerging nature of African economies and associated stochastic behaviours, optimizing green computing awareness is a possibility though with probable outcomes. We applied metaheuristic algorithm to the stochastic optimization problem to search for best-known green computing awareness creation solution. Our experiment with Tabu Search indicated that an online real-time dialogue platform will serve the purpose best. Hence, we designed, developed and implemented an e-Green Computing system that proved effective. Component-based software engineering approach was used for re-usability of modules across African countries adapting the solution [24].

ACKNOWLEDGMENT

We thank the authorities of the University of Lagos, Nigeria for providing the platform for carrying out this research study.

REFERENCES

[1] S. Murugesan, “Harnessing Green IT: Principles and Practices,” IEEE IT Professional, January–February 2008, pp 24-33.
[2] P. Hoeller and M. Wallin, OECD Economic Studies No. 17, Autumn 1991. Energy Prices, Taxes and Carbon Dioxide Emissions (PDF). OECD website. p. 92. Retrieved 2010-04-23.
[3] Staudt, A. et al., "Understanding and Responding to Climate Change", U.S. National Academy of Sciences, 2008.
[4] E. Okewu, "Requirements Engineering in an Emerging Market", The 2015 International Conference on Computational Science and Its Applications (ICCSA 2015), Banff, Canada, Springer Publishers, 2015.
[5] K. Therese and J. Albert, "Stochastic Regular Language: A Mathematical Model for the Language of Sequential Actions for Decision Making under Uncertainty", International Journal of Mathematics and Computer Applications Research (IJMCAR), 3(1), pp. 1-8, 2013.
[6] K. Therese and J. Albert, "Stochastic Finite Automata: A Mathematical Model for Sequential Decision Making under Uncertainty", International Journal of Applied Mathematics and Modellling (IJM2M), Vol. 2, No. 3, pp 1-14, 2014.
[7] B. Saha, "Green Computing", International Journal of Computer Trends and Technology (IJCTT), Volume 14 number 2 – Aug 2014.
[8] P. Mittal and N. Kaur, "Green Computing – A Survey", International Journal of Computer Trends and Technology (IJCTT), Volume 4, Issue 4 –April 2013.
[9] S. Shinde, S. Nalawade, and A. Nalawade, "Green Computing: Go Green and Save Energy", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013 ISSN: 2277 128X
[10] J. Silberholz and B. Golden , "Comparison of Metaheuristics", 2010.
[11] F. Glover, "Tabu Search - Part 2", ORSA Journal on Computing, 2 (1): 4–32. doi:10.1287/ijoc.2.1.4, 1990.
[12] K.K. Aggarwal and Y. Singh, Software Engineering, New Age International Publishers, 2008.
[13] I. Gorton, " Essential Software Architecture", Second Edition, Springer, 2011.
[14] R.S. Pressman, "Software Engineering: A Practitioner’s Approach", 7th ed., 2009.
[15] R.C. Martin, UML Tutorial: Sequence Diagrams. Engineering Notebook Column , 1998.
[16] N. Sirohi and A. Parashar, "Component Based System and Testing Techniques", International Journal of Advanced Research in Computer and Communication Engineering, 2(6):33-42, 2013.
[17] S. Beydeda and V. Gruhn, "An Integrated Testing Technique for Component-Based Software, Computer Systems and Applications", ACS/IEEE International Conference, pp. 328 - 334, 2001.
[18] M. Host, B. Regnell, and C. Wohlin, "Using students as subjects - a comparative study of students and professionals in lead-time impact assessment", Empirical Software Engineering - an International Journal, 5(3):201-214, 2000.
[19] P. Runeson, "Using students as Experiment Subjects - An Analysis on Graduate and Freshmen Student Data", In: Linkman, S. (ed.) 7th

International Conference on Empirical Assessment & Evaluation in Software Engineering (EASE'03), pp. 95-102, 2003.

[20] J. Sauro and E. Kindlund, "A Method to Standardize Usability Metrics into a Single Score", ACM, CHI, 2005.

[21] M. Svahnberg, A. Aurum, and C. Wohlin, "Using students as Subjects -An Empirical Evaluation", Proc. 2nd International Symposium on Empirical Software Engineering and Management ACM, pp. 288-290, 2008.

[22] J. Nielsen, and T. Landauer, "A mathematical model of the finding of usability problems", Proceedings of ACM INTERCHI'93 Conference, 206-213, 1993.

[23] C.W. Turner, J.R. Lewis, and J. Nielsen, "Determining usability test sample size" In W. Karwowski (ed.), International Encyclopedia of Ergonomics and Human Factors (pp. 3084-3088). Boca Raton, FL: CRC Press, 2006.

[24] E. Okewu and O. Daramola, "Component-based Software Engineering Approach to Development of a University e-Administration System", IEEE 6th International Conference on Adaptive Science and Technology (ICAST). IEEE Explore Digital Library, 2014.

Spectrum Occupancy Measurements in the TV and CDMA Bands

[1]O.D. Babalola, [2]Emoseh Garba, [3]I.T. Oladimeji, [4]A.S. Bamiduro, [5]Nasir Faruk, [6]O.A. Sowande, [7]O.W. Bello, [8]A.A.Ayeni and [9]M.Y. Muhammad
[1, 2, 3, 4, 5, 6, 8,9]Department of Telecommunication Science, University of Ilorin, Ilorin, Nigeria
[7]Department of Information and Communication Science, University of Ilorin, Ilorin, Nigeria
Email: oluwolebabalola@gmail.com,emosehgarba@gmail.com,oladimejitemitope06@gmail.com
sundaybamiduro@gmail.com, faruk.n@unilorin.edu.ng, sowande.oa@unilorin.edu.ng, laibello@unilorin.edu.ng, aayeni@unilorin.edu.ng

Abstract: **Continuous demand, by end users, has become an issue with respect to the scarce resources of the radio frequency spectrum. In this paper we conducted a 24-hour outdoor measurement of spectrum occupancy, in both rural and urban areas in Kwara State, Nigeria, spanning across the frequency range of 48.5 MHz – 880 MHz. The results obtained show that the mean average duty cycle for TV bands 1-4 and CDMA band in rural and urban locations are 2.58 % and 12.02% and 0.25% and 3.13% respectively. Findings from this measurements show that there is ample opportunity for deployment of cognitive radio for a more efficient utilization of the spectrum.**

Index Terms**: Duty Cycle, VHF, UHF, CDMA.**

I. INTRODUCTION

The anxiety about providing services to the growing number of desirous users, even, with the realization of the finite and exhaustible nature of the radio spectrum is leading scholars, practitioners and other stakeholders to venture into new things and ideas.

Reuse of already allocated frequencies, by secondary users, though relatively novel, is becoming, particularly, attractive, in this direction. This is giving way to the idea of frequency utilization, spectrum efficiency and the duty cycle. For this use to be worthy, it should not lead to interference with the primary user and its resultant degradation in quality of service.

Many techniques are being experimented on, towards the realization of the goal of meeting continuously growing demands for spectral spaces in the face of finitely-limited spectral spaces. Prominent among these are the plethora of spectrum management/licensing regimes all designed to enhance efficient spectrum usage. Joseph Mitola [1]proposed the idea of *cognitive radio,*a software defined radio with capability to monitor the radio environment for the purpose of determining whether or not, they are occupied. Spectrum sensing is the process of detecting the presence of primary users in a licensed frequency band. There are broad categories spectrum sensing: cooperative sensing, non cooperative and interference based sensing.

Measurement of duty cycle gives valuable information on spectrum availability by frequency band, time and location; by extension it provides enough information to enable deployment of secondary user-devices. Duty cycle is a measure of the ratio of period of occupancy and period of observation, **t/T** where**, t** and **T** are, respectively, the period of usage and period of observation. In this paper we conducted a 24-hour outdoor measurement of spectrum occupancy, in both rural and urban areas in Kwara State, Nigeria, spanning across the frequency range of 48.5 MHz – 880 MHz.

II. RELATED WORKS

Several spectrum occupancy measurements and survey has been conducted globally, but minute research work has been conducted in Africa as most of the existing works were conducted in the USA, Europe and Asia. In [2]-[7] they made effort to conduct a field survey to protocols and model developments in improving spectrum utilization in VHF and UHF bands in Nigeria.

In [8], measurement and Analysis of Wideband spectrum utilization in Indoor and Outdoor environments was provided. In [9] they concluded that channel occupancy clearly varies on a 24 hour cycle. Mean time and frequency occupancy figures have shown that occupancy varies periodically, with a strong 24 hour cycle being visible. In [10] same energy detection (ED) threshold presented in [11] was used and measurement was conducted in Hull, United Kingdom between 180 MHz – 2700 MHz on top of a building and it measurement was taken within 24 hours. The frequency was sub-divided into six groups respectively. The average duty cycle for 180MHz – 850MHz was 10.18% and 880MHz –

960MHz was 32.19% which was the most utilized sub-band .But the mean spectrum occupancy of all the bands was 11.02% also it was observed that frequency 1.9GHz was the least underutilized.
In [11] they measured between 25 – 3400MHz with 14 different frequency groups. They took the measurement outside a top building. The average duty cycle for 25MHz – 230MHz was 28.44%, 230MHz – 400MHz was 11.09%, 400MHz – 470MHz was 18.37% ,470MHz – 766MHz was 40.02% and 766MHz – 880MHz was 12.30% .The mean occupancy was 12.19% which showed that the occupancy over the bands was pretty low but the most occupied group was between 880 -960 MHz which was 46.8% indicating that there were more users using the GSM band.[11]. In [12] they conducted an extensive spectrum occupancy measurement at the frequency range of 300MHz – 4900MHz, and generated a data for a period of more than 6 month in Bristol, UK. Their main objective was to discover which channel might be suitable for CR use on a time interleaved basis, and to discover how the availability of these channels varies according to the time of day and to find out more about the short-term temporal variability. In [13] an extensive measurement campaign to compare indoor and outdoor spectrum occupancy using energy detection sensing method. The measurement was carried out at Aachen, Germany and the frequency range considered was between 20MHz – 1520MHz, 1.52GHz to 3GHz and 3GHz up to 6GHz .The ED threshold used was 3dB above the measured noise floor and results was analyzed using amplitude probability distribution (APD) to observe primary user activity. In paper [14] he conducted his outdoor experiment on top of a building in Ohio, USA from frequency range 30MHz – 300MHz. He chose 7dB above noise level as ED threshold. Approximately 80% of the total spectrum measured showed that it was free and further explained that in a rural location the spectrum occupancy percentage will decrease because of lesser traffic.

III. METHODOLOGY

A. Measurement Set Up

The measurement setup and settings used are identical for the rural, urban and sub urban locations. The spectrum occupancy measurement setup consists of a spectrum analyzer and a data storage. Agilent N9342C Handheld Spectrum Analyser (HSA) capable of measuring from 100 KHz to 7GHz was used. The device uses energy detection to directly measures received signal level in dBm. It also has GPS (global positioning system) location features. A 32 Gigabyte Storage device was used to save the log files generated by spectrum analyzer in real-time. The measurement setup at the locations is shown in Fig 1.

Fig 1:Agilent N9342C Spectrum analyser and project vehicle.

The SA's parameters were configured according to the values shown in Table II. Analysis of the data was then post-processed offline in a powerful PC.

TABLE I: SPECTRUM ANALYZER CONFIGURATION

Parameter	*Value*
Resolution/ Video Bandwidth (RBW/VBW)	100 kHz/ 100 kHz (Automatically selected by SA)
Sweep time	34.10 ms (Automatically selected by SA)
Sweep Type	Continuous
Reference Level	-50 dBm
Number of points	461

B. Measurement Locations

The measurement was conducted outdoors at specific urban and rural locations in Kwara state, Nigeria to ascribe a wide view to our spectrum occupancy. Table 3 shows the measurement sites and type of environment considered, with their respective coordinates.

TABLE II: MEASUREMENT LOCATIONS

Location	*Type*	*Coordinate*	*Identifier*
Adio village, Oke Oyi	Rural	4°29'42" E; 8°46'40"N	LOC 1
Malete	Rural	4°29'42"E 8°22'34"N	LOC 2
Alamote	Rural	4°29'42"E 8°22'34"N	LOC 3
Odo Oke	Rural	4°31'55"E 8°17'09"N	LOC 4
Lagiki,	Rural	4°33'02"E 8°16'46"N	LOC 5
University Quarters, Ilorin	Urban	4°38'47"E 8°27'49"N	LOC 6
University of Ilorin, Ilorin	Urban	4°67'60" E 8.48'74"N	LOC 7
Pipe Line	Urban	4°35'07" E 8°27'57"N	LOC 8
Kwara Stadium, Ilorin	Urban	4°32'29"E 8°28'36" N	LOC 9

TABLE III: SERVICE BANDS CONSIDERED.

Service Bands	Frequency range	Bandwidth (Hz)
TV Band 1	48.5-92 MHz	43,000,000
TV Band 2	167-233 MHz	66,000,000
TV Band 3	470-566 MHz	96,000,000
TV Band 4	606-870 MHz	264,000,000
CDMA DL	870-880 MHz	10,000,000

C. Data Collection and Processing

The measurements were taken for 24 hours in the locations. All raw data was collected by the analyzer in a matrix form with elements of the received signal powers $P(f_i, t_i)$ (in dBm). Where f_i denotes the frequency or channel and t_j records the time slot with 461 as the number of time slots (N) measured per received frame. A total of 1500 frames were received into the Analyzer per band per location. Fifty frames 50 samples were randomly chosen from the raw data leaving a matrix *Y* of signal power (50, 461) to be processed in order to evaluate the occupancy statistics and to produce frequency-time occupancy plots.

The process of evaluating the occupancy statistics comprises of three steps- raw data input, setting of an adaptive threshold, and computing the average duty cycle of each channel. Raw data inputs are received power levels at the antenna output that have not been processed. Adaptive threshold setting is done as each channel has different noise power. In order to minimize false alarm, a threshold of 10 dB above the noise floor was used for this experiment. The average measured occupancy or Duty cycle indicates how often the signal is perceived during a sampled period of scanning a band. The duty cycle is delimited as the percentage of time a frequency band or channel is occupied over a given period as shown in the equation (1)

$$Duty\ \text{Cycle} = \frac{\text{Signal Occupation period (n)}}{\text{Total Observation period (m)}} \times 100\% \qquad (1)$$

When given a time series of channel power measurements the duty cycle can be calculated as:

$$Duty\ \ \text{Cycle}\ = \frac{nt}{m} \times 100\ \% \qquad (2)$$

Where n denotes number of time slots t, where the received signal level is above the decision threshold λ_j and *m* is the total number of time slots.

I.V RESULTS AND DISCUSSION

Figures 2 and 3 provide pie chart of the duty cycle for locations 2 and 3 which are all in the rural areas. In location 2, TV band 2 recorded the highest occupancy value of 2.47% while in location 3 TV band three has the highest occupancy of 14.19 %. In both locations, CDMA band was completely unoccupied with zero percent utilization. In the urban scenario, TV band 3 has the highest occupancy as shown in Figures 4 and 5. The average duty cycle for each of the bands was computed for the locations (i.e. LOC 1-9) the results are shown in Table IV. In Table IV, the average duty cycle of 0% for TV band 4 (606 – 870 MHz), was obtained for LOC 1, 3, 4 and 5which are all rural locations. Across all the locations, the average mean duty cycle for TV band 1 (48.5 – 92 MHz), TV band 2 (167 – 233 MHz), TV band 3 (470 - 566 MHz), TV band 4 (606 – 870 MHz) and CDMA band (870-880MHz) are 2.77 %, 4.64%, 16.56%, 3.12% and 1.53% respectively. In terms of mean occupancy across all the bands,LOC9 has the overall occupancy value of 13.39% followed by LOC 8 with 12.38 %and LOC 6 with 11.38% with all of these in urban areas. LOC 5 and LOC 3 in the rural areas have considerable occupancies.

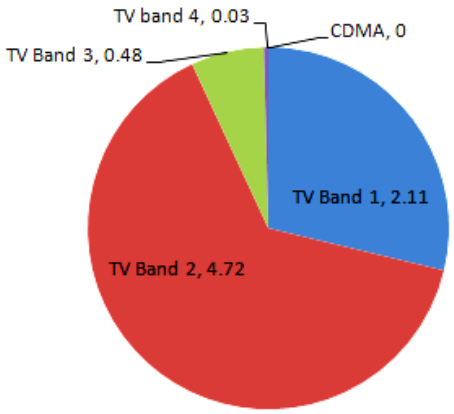


Fig . 2 Duty Cycle for TV and CDMA for LOC2

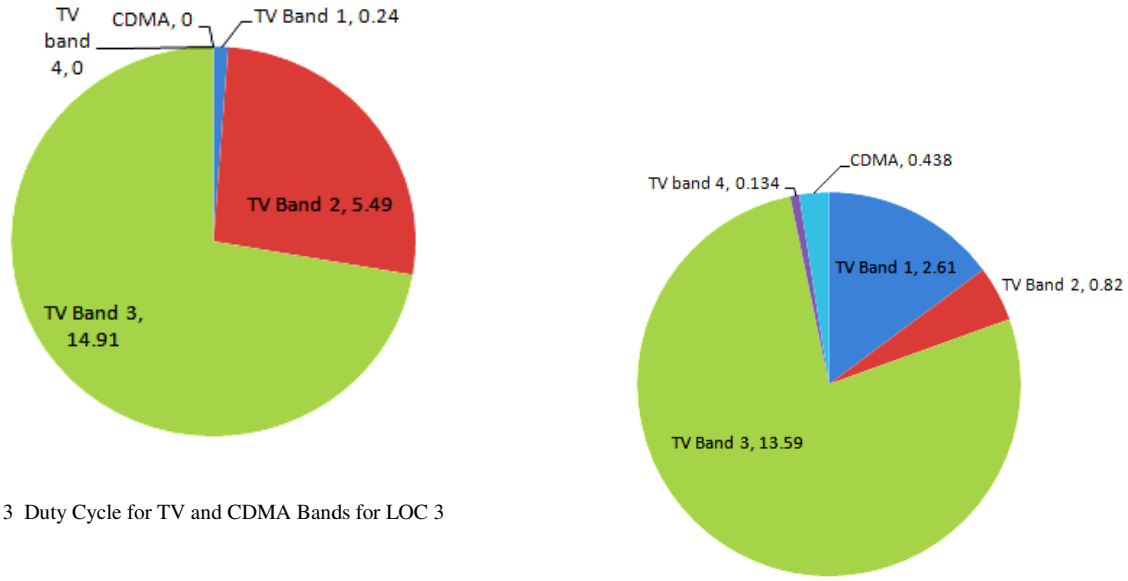


Fig. 3 Duty Cycle for TV and CDMA Bands for LOC 3

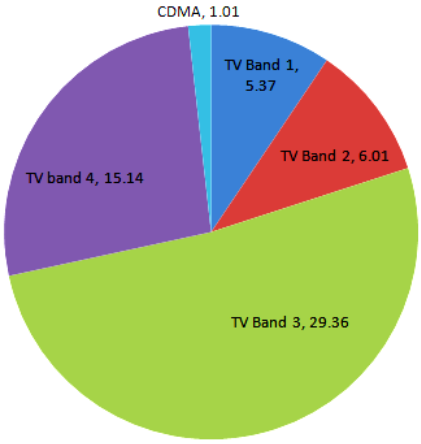


Fig . 4. Duty Cycle for TV and CDMA Bands for LOC 6.

TABLE IV. DUTY CYCLE (%) FOR LOCATIONS.

	TV Band 1	TV Band 2	TV Band 3	TV band 4	CDMA	Mean (%)
Loc1	0	0	0	0	0.65	0.13
Loc 2	2.11	4.72	0.48	0.03	0	1.46
Loc 3	0.24	5.49	14.91	0	0	4.12
Loc 4	0	0	0	0	0.2	0.04
Loc 5	0.92	2.45	20.26	0	0.41	4.81
Loc 6	5.37	6.01	29.36	15.14	1.01	11.38
Loc 7	2.61	0.82	13.59	0.134	0.44	3.52
Loc 8	6.42	11.49	37.27	6.42	0.3	12.38
Loc 9	7.23	10.84	33.21	6.38	10.8	13.69
Average	2.77	4.64	16.56	3.12	1.53	

V. CONCLUSION

Evidence, from the results of our 24-hr outdoor measurement, on spectrum occupancy,show that in both rural and urban areas,CDMA bands are less utilizedwhen compared with TV bands. However, the average occupancy of TV bands in the urban locations is still very low at 12.02%. Either of the bands is a good candidate for the deployment of *cognitive radio*.

VI. ACKNOWLEDGMENT

This research was conducted under the auspices of the Communication and Networking Research Group (CNRG) of University of Ilorin, Ilorin, Nigeria. The authors would like to express their sincere appreciation to the University of Ilorin for the purchase of a dedicated Agilent spectrum analyzer, used for this study.

REFERENCES

[1]Joseph Mitola III, *"Cognitive Radio an Integrated Agent Architecture for Software Defined Radio",* PhD Thesis, Royal Institute of Technology (KTH), pp 45-47, 2000.

[2] Y.A. Adediran, N. Faruk, A. A. Ayeni, O. Kolade, N.T.Surajudeen-Bakinde and O.W.Bello, "Geo-spatial Approach to Quantifying TV White Space in Nigeria in the UHF Band" *Submitted for review, Journal of Engineering Letters, November, 2014.*

[3] N .Faruk, N.T. Surajdeen, O. Kolade and A.A.Ayeni, and Y.A. Adediran, "DTV protection regions for spectrum sharing" *IET Journal of Enginnering, Institute of Engineering and Technology, 5th Sept, 2014.*

[4] N .Faruk, A.A.Ayeni,Y.A. Adediran and N.T Surajudeen, "Improved Path Loss Model for Predicting DTV Coverage for Secondary Access" *Int. J. Wireless and Mobile Computing, Vol. 7, No. 6, pp 565-576, 2014*

[5] N. Faruk, A.A.Ayeni and Y.A Adediran, " Impact of Path loss models on Spatial TV white space" *European Scientific Journal*, University of Azores, Portugal, Vol 4, pp 543-547, 2013.

[6] N. Faruk, Y.A. Adediran and A.A.Ayeni, "On the study of empirical path loss models for accurate prediction of TV signal for secondary users" *Progress in Electromagnetic Research (PIER) B,* USA, Vol. 49, pp 155- 176, 2013.

[7] N. Faruk, M. Gumel, A. Oloyode and A. Ayeni, "Performance Analysis of Hybrid MAC Protocol for Cognitive Radio Networks*," Int'l J. of Communications, Network and System Sciences*, Vol. 6 No. 1, 2013, pp. 18-28. doi: 10.4236/ijcns.2013.61003.

[8] K. A. Qaraqe, M. S. Alouini, A. El-Saigh, L. Abuhantashi, M. Al-Mulla, A. Jolo, A. Ahmed, "Measurement And Analysis of Wideband Spectrum Utilization in Indoor and Outdoor Environments,"*International conference on Communication Technologies (ICCT , 2010)* Riyadh, Saudi Arabia, Jan 2010.

[9] K. E. Nolan, "700MHz Band Spectrum-Usage Measurements from Denver to Washington Dc During November 2007 And Their Value In Helping Software-Defined Radio Enter The Mainstream"

[10] M. Mehdawi, *et al,*"Spectrum occupancy survey in HULL-UK for cognitive radio applications: measurement & analysis." *International Journal of Scientific & Technology Research* 2, no. 4,pp 231-236, 2013.

[11] A..Marţian, et *al*, "Evaluation of Spectrum Occupancy in an Urban Environment in a Cognitive Radio Context." *International Journal on Advances in Telecommunications* 3, no. 3,pp 172 -181,2010.

[12]T. J. Harold, R. A. Cepeda, M. A. Beach, " Long-Term Measurements of Spectrum Occupancy Characteristics", *New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on*. IEEE, 2011.

[13] M. Wellens, J. Wu, P. Mahonen, " Evaluation of Spectrum Occupancy in Indoor and Outdoor scenario in the Context of Cognitive Radio*", Proc. 2nd International Conference Cognitive Radio Oriented in Wireless Network Communication. CrownCom* 2007,Orlando,FL,USA 2007,pp 420 - 427.

[14] S. W. Ellingson, "Spectral occupancy at VHF: implications for frequency-agile cognitive radios," In *IEEE Vehicular Technology Conference*, vol. 62, no. 2, p. 1379. IEEE; 1999, 2005.

Short-Term Variation of Duty Cycle in the VHF and UHF Bands

[1]O.D. Babalola, [2]Emoseh Garba, [3]I.T. Oladimeji, [4]A.S. Bamiduro, [5]Nasir Faruk, [6]O.A. Sowande, [7]O.W. Bello, [8]A.A.Ayeni and [9]M.Y. Muhammad
[1, 2, 3, 4, 5, 6, 8,9]Department of Telecommunication Science, University of Ilorin, Ilorin, Nigeria
[7]Department of Information and Communication Science, University of Ilorin, Ilorin, Nigeria
Email: oluwolebabalola@gmail.com,emosehgarba@gmail.com,oladimejitemitope06@gmail.com sundaybamiduro@gmail.com, faruk.n@unilorin.edu.ng, sowande.oa@unilorin.edu.ng, laibello@unilorin.edu.ng, aayeni@unilorin.edu.ng

Abstract: **The continuing high demand, by end users, has become worrisome with respect to scarce resources of the radio spectrum. TV bands, spanning across has being in existence for quite a while now and much of the frequency bands, within these range, have been allocated to FM stations, TV stations and DTV stations in Nigeria. In this paper we conducted a 24-hours outdoor measurement of spectrum occupancy in both rural and urban locations in Kwara State, Nigeria, spanning across the frequency range of 48.5MHz – 870 MHz.The results obtained show that TV band 3 was the most occupied TV band in both rural and urban areas, with occupancy of up 20.26% and 37.27% respectively. Also the mean average of the duty cycle in the urban location is 12.02% compared to 2.58% in the rural locations.Findings from this measurements show that there is ample opportunity for deployment of software defined radio for a more efficient utilization of the spectrum.**
Index Terms: Short-Term, Duty Cycle, VHF, UHF

I. INTRODUCTION

Frequency utilization is fast becoming an issue in today's research activities, primarily, due to the realization that *demand* for frequency seems to be outgrowing *supply.*The reality, today, is that demand for space, in the wireless medium is increasing at a rate, sufficient to arouse questions about *availability* and, by extension, *frequency utilization*. This is due to the continuing emergence of wireless devices, on account of preferences for them as a means of information transmission. This has, over time, given rise to the ideas of *frequency reuse* and *cognitive radio.*

Cognitive radio is an intelligent radio which can be programmed and, dynamically, configured, to enable it use the best wireless channels in its vicinity. Such a radio, automatically, detects available channels in the wireless spectrum and changes its transmission or reception parameters, to allow more concurrent wireless communications in a given spectrum band, at a particular location. This process is a form of dynamic spectrum management.Frequency occupancy measurement enhances an estimation of *frequency utilization* and its related parameter*, duty cycle*, both of which, obviously, vary over time.

With the emergence of Wireless Local Area Networks (WLANs), in various environments, as well as proliferation of other wireless devices, the issue of frequency utilization is brought, further, to the fore. Considering that data is not transmitted on a continuous basis, the assumption of a continuous transmission, often made, is misleading as it overestimates frequency utilization, leading to underutilization of spectrum. Actual duty cycles of WLAN, as well as those of other wireless channels, are, thus, of importance, for purpose of frequency utilization determination and by extension cognitive radio deployment.

II. RELATED WORKS

Recently, there is growing spectrum occupancy measurements and survey due to global demand of more spectral spaces to accommodate increase in wireless data services. Some work, in this area, has been carried out in Africa, Malawi, South Africa but most of the existing works were conducted in the USA, Europe and Asia. However, research efforts have been made in [1]-[6] ranging from field survey to protocol and model developments, to improve on spectrum utilization, so that secondary use of radio spectrum in the VHF and UHF bands in Nigeria can be made feasible.

In [7] a bid to study the utilization of RF spectrum in indoor and outdoor environments simultaneously performed measurements in the 700-3000MHz frequency band, over three consecutive days, at an indoor and outdoor location simultaneously. Their findings show that there are striking and quantifiable differences in the spectrum utilization profiles between indoor and outdoor environments and bandwidth utilization differs for the different environments. With mean values of 1% and 15%, standard deviation of 0.2 and 0.5, for indoor and outdoor, respectively, the need for specifying the environment type is obvious whenever spectrum utilization is being measured. In [8] a measurement campaign covering a total of 4500 km along a route from Denver, Colorado to Washington DC in the band 698-806MHz, covering a variety of busy urban centers and quiet rural areas along the route. The aim was to evaluate the actual spectrum usage, in the 700MHz band, which was the subject of FCC auction 73.

In [9] same energy detection (ED) threshold presented in [10] was used and measurement was conducted in Hull, United Kingdom between 180 MHz – 2700 MHz on top of a building and it measurement was taken within 24 hours. The frequency was sub-divided into six groups respectively. It showed that the most utilized sub-band was 880MHz - 960MHz and the occupancy measured was 32.19%. But the mean spectrum occupancy of all the bands was 11.02% also it was observed that frequency 1.9GHz was underutilized. In [9] they recommended that frequency above 1GHz is the best and most under-utilized band which provides allowance for secondary user. In [11] they conducted an extensive spectrum occupancy measurement at the frequency range of 300MHz – 4900MHz, and generated a data for a period of more than 6 month in Bristol, UK. Their main objective was to discover which channel might be suitable for CR use on a time interleaved basis, and to discover how the availability of these channels varies according to the time of day and to find out more about the short-term temporal variability. In [8] they concluded that channel occupancy clearly varies on a 24 hour cycle. Mean time and frequency occupancy figures have shown that occupancy varies periodically, with a strong 24 hour cycle being visible.

In [12] an extensive measurement campaign to compare indoor and outdoor spectrum occupancy using energy detection sensing method. The measurement was carried out at Aachen, Germany and the frequency range considered was between 20MHz – 1520MHz, 1.52GHz to 3GHz and 3GHz up to 6GHz .The ED threshold used was 3dB above the measured noise floor and results was analyzed using amplitude probability distribution (APD) to observe primary user activity. In paper [13] he conducted his outdoor experiment on top of a building in Ohio, USA from frequency range 30 MHz – 300 MHz . He chose 7dB above noise level as ED threshold. Approximately 80% of the total spectrum measured showed that it was free and further explained that in a rural location the spectrum occupancy percentage will decrease because of lesser traffic.

III. METHODOLOGY

A. Measurement Set Up

The measurement setup and settings used are identical for the rural, urban and sub urban locations. The spectrum occupancy measurement setup consists of a spectrum analyzer, a data storage device, and data manipulation equipment (laptop). Agilent N9342C Handheld Spectrum Analyser (HSA) capable of measuring from 100 KHz to 7GHz (tuneable to 9 kHz) was used. The device uses energy detection to directly measures received signal level in dBm. It also capable of displaying the spectrograph of signals. It also has GPS (global positioning system) location features. A 32 Gigabyte Storage device was used to save the log files generated by spectrum analyzer in real-time to be worked on with a laptop. The measurement setup at the locations is shown in Fig 1.

Fig 1:Agilent N9342C Spectrum analyser and project vehicle.

The SA's parameters were configured according to the values shown in Table II. Analysis of the data was then post-processed offline in a powerful PC.

TABLE I: SPECTRUM ANALYZER CONFIGURATION

Parameter	*Value*
Resolution/ Video Bandwidth (RBW/VBW)	100 kHz/ 100 kHz (Automatically selected by SA)
Sweep time	34.10 ms (Automatically selected by SA)
Sweep Type	Continuous
Reference Level	-50 dBm
Number of points	461

.

B. Measurement Locations

The measurement was conducted outdoors at specific urban and rural locations in Kwara state, Nigeria to ascribe a wide view to our spectrum occupancy. Table 3 shows the measurement sites and type of environment considered, with their respective coordinates.

TABLE II: MEASUREMENT LOCATIONS

Location	*Type*	*Coordinate*	*Identifier*
Adio village, OkeOyi	Rural	4°29'42" E; 8°46'40"N	LOC 1
Malete	Rural	4°29'42"E 8°22'34"N	LOC 2
Alamote	Rural	4°29'42"E 8°22'34"N	LOC 3
OdoOke	Rural	4°31'55"E 8°17'09"N	LOC 4
Lagiki,	Rural	4°33'02"E 8°16'46"N	LOC 5
University Quarters, Ilorin	Urban	4°38'47"E 8°27'49"N	LOC 6
University of Ilorin, Ilorin	Urban	4°67'60" E 8.48'74"N	LOC 7
Pipe Line	Urban	4°35'07" E 8°27'57"N	LOC 8
Kwara Stadium, Ilorin	Urban	4°32'29"E 8°28'36" N	LOC 9

TABLE III: SERVICE BANDS CONSIDERED.

Service Bands	Frequency range	Bandwidth (Hz)
TV Band 1	48.5-92 MHz	43,000,000
TV Band 2	167-233 MHz	66,000,000
TV Band 3	470-566 MHz	96,000,000
TV Band 4	606-870 MHz	264,000,000

V. Data Collection and Processing

The measurements were taken for 24 hours in the locations. All raw data was collected by the analyzer in a matrix form with elements of the received signal powers $P(f_i, t_i)$ (in dBm). Where f_i denotes the frequency or channel and t_j records the time slot with 461 as the number of time slots (N) measured per received frame. A total of 1500 frames were received into the Analyzer per band per location. Fifty frames 50 samples were randomly chosen from the raw data leaving a matrix *Y* of signal power (50, 461) to be processed in order to evaluate the occupancy statistics and to produce frequency-time occupancy plots.

The process of evaluating the occupancy statistics comprises of three steps- raw data input, setting of an adaptive threshold, and computing the average duty cycle of each channel. Raw data inputs are received power levels at the antenna output that have not been processed. Adaptive threshold setting is done as each channel has different noise power. In order to minimize false alarm, a threshold of 10 dB above the noise floor was used for this experiment. The average measured occupancy or Duty cycle indicates how often the signal is perceived during a sampled period of scanning a band. The duty cycle is delimited as the percentage of time a frequency band or channel is occupied over a given period as shown in the equation (1)

$$Duty\ \text{Cycle} = \frac{\text{Signal Occupation period (n)}}{\text{Total Observation period (m)}} \times 100\% \qquad (1)$$

When given a time series of channel power measurements the duty cycle can be calculated as:

$$Duty\ \ \text{Cycle} = \frac{nt}{m} \times 100\ \% \qquad (2)$$

Where n denotes number of time slots t, where the received signal level is above the decision threshold λ_j and m is the total number of time slots.

IV RESULTS AND DISCUSSION

TV broadcasting frequencies is categorized into four bands i.e.band 1, band 2, 3 and band 4. Table III provides details of the frequency range for each band. The average duty cycle for each of the bands was computed for locations 1-9. In table IV, the average duty cycle of 0% was obtained for locations 1 and 4 across all the bands. For TV band 1 (48.5 – 92 MHz), loc 9 has the highest occupancy of 7.23 %. For TV band 2 (167 – 233 MHz) and TV band 3 (470 - 566 MHz) loc 8 has the highest occupancy of 11.49%. and 37.37% respectively. However for TV band 4 (606 – 870 MHz), loc 6 has the highest occupancy value of 15.14%. In terms of mean occupancy, loc 8 has the overall occupancy value of 15.4% followed by loc 9 14.41% and loc 6 with 13.97% with all of these in urban areas. TV band 1 recorded the least occupancy across all the locations when compared with other bands this is because only one active transmitter (i.e. Unilorin FM radio, operating on 89.3 MHz frequency) in the VHF channels is allotted for FM radio broadcasting. Therefore, no significant activity was captured, although the experiment did not cover other bands, in which other radio transmitters such as royal FM transmitting on 95.1 MHz, harmony FM operating 103.5 MHz and midland FM 105.3MHz are operating. TV band 3recorded the highest occupancy value asup to 40% of the band is occupied during the period of the measurements. This value is expected to vary depending on time and usage. There was no much activity in the TV band 4 as only about 15% of the band is occupied and considering the frequency band of 606 – 870MHz which is UHF band, this would be suitable for secondary network deployment with high capacity. However, the duty cycle for Location 7 was 2.61% in TV band 1 which is very low compared to other urban locations in spite of its closeness to the Radio transmitter of about 100m. The observed low duty cycle is accounted for, by the phenomenon of near field effects.

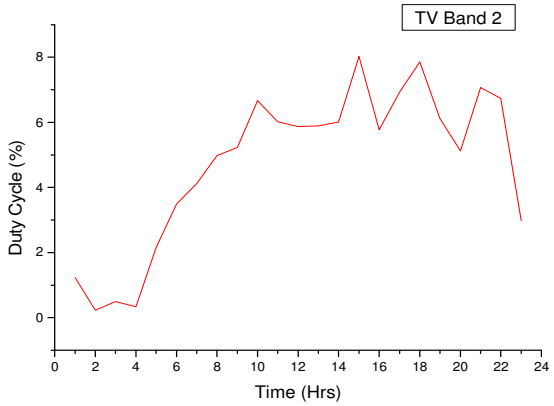


Fig . 2 Variation f Duty Cycle for TV Band 2.

TABLE IV. DUTY CYCLE FOR LOCATIONS 1-9

Locations	Location Type	TV band 1 (48.5 – 92 MHz)	TV band 2 (167 – 233 MHz)	TV band 3 (470 – 566 MHz)	TV band 4 (606 – 870 MHz)	Mean (%)	Mean Average (%)
Loc 1	Rural	0	0	0	0	0	2.58
Loc 2	Rural	2.11	4.72	0.48	0.03	1.83	
Loc 3	Rural	0.24	5.49	14.91	0	5.16	
Loc 4	Rural	0	0	0	0	0	
Loc 5	Rural	0.92	2.45	20.26	0	5.91	
Loc 6	Urban	5.37	6.01	29.36	15.14	13.97	12.02
Loc 7	Urban	2.61	0.82	13.59	0.134	4.29	
Loc 8	Urban	6.42	11.49	37.27	6.42	15.4	
Loc 9	Urban	7.23	10.84	33.21	6.38	14.41	

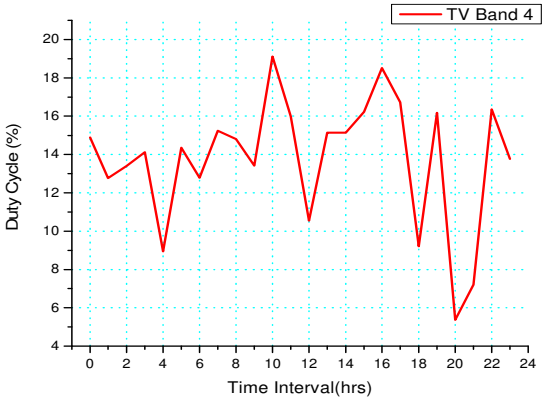


Fig .3 Variation f Duty Cycle for TV Band 3.

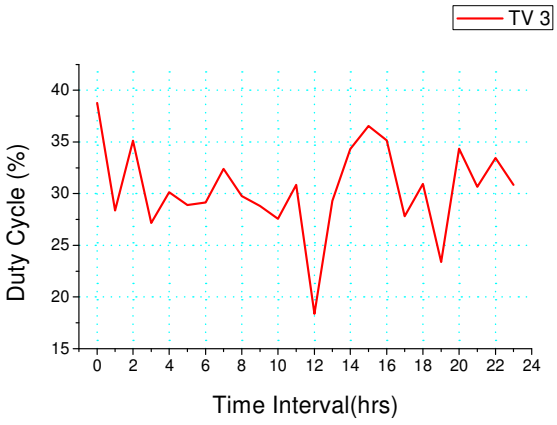


Fig . 4 Variation of Duty Cycle for TV Band 4.

Figures 2-4 show the temporal variation of duty cycle for TV bands 2,3 and 4 for location 6. Short term temporal variation of from duty cycle is the hourly variation of the occupancy. The occupancy of the channels for every hour of the day was measured for the period of 24 hours in LOC 6. The meanof the hourly occupancy is calculated in order to establish which channels' occupancy stays constant or steady and which of the channel have a more unpredictable occupancy (regarded by higher deviation from the mean occupancy from a statistical viewpoint). The average duty cycle for each measured frequency point was computed at 1 hour periods through 24 hours, thus obtaining the time variation of the duty cycle for different frequencies. In Fig 3, at around 0-4 (hrs), the duty cycle was very low, close to zero. The duty cycle however increase with time and drops at around 24 hrs. These sudden drops were as the result of OFF periods for NTA transmitter which operates on channel 5, 203.25 MHz. NTA's transmission schedules are from 06:00 hrs to 23:59 hrs.

V. CONCLUSION

In this paper, a 24-hr outdoor measurement, on spectrum occupancy,in both rural and urban areas, ofKwara State, Nigeria, spanning across the frequency range of 48.5 MHz – 870 MHz was undertaken. Measurements obtained show that the TV bands are underutilized and, in future, might be a very good band for the deployment of*software defined radio* SDR. Similarly further experiment will be conducted in various geopolitical zones in Nigeria to ascertain the level of spectrum occupancy at this frequency range.

VI. ACKNOWLEDGMENT

This research was conducted under the auspices of the Communication and Networking Research Group (CNRG) of University of Ilorin, Ilorin, Nigeria. The authors would like to express their sincere appreciation to the University of Ilorin for the purchase of a dedicated Agilent spectrum analyzer, used for this study.

REFERENCES

[1] Y.A. Adediran, N. Faruk, A. A. Ayeni, O. Kolade, N.T.Surajudeen-Bakinde and O.W.Bello, "Geo-spatial Approach to Quantifying TV White Space in Nigeria in the UHF Band" *Submitted for review, Journal of Engineering Letters, November, 2014.*

[2] N .Faruk, N.T. Surajdeen, O. Kolade and A.A.Ayeni, and Y.A. Adediran, "DTV protection regions for spectrum sharing" *IET Journal of Enginnering, Institute of Engineering and Technology, 5th Sept, 2014.*

[3] N .Faruk, A.A.Ayeni,Y.A. Adediran and N.T Surajudeen, "Improved Path Loss Model for Predicting DTV Coverage for Secondary Access" *Int. J. Wireless and Mobile Computing, Vol. 7, No. 6, pp 565-576, 2014*

[4] N. Faruk, A.A.Ayeni and Y.A Adediran, " Impact of Path loss models on Spatial TV white space" *European Scientific Journal*, University of Azores, Portugal, Vol 4, pp 543-547, 2013.

[5] N. Faruk, Y.A. Adediran and A.A.Ayeni, "On the study of empirical path loss models for accurate prediction of TV signal for secondary users" *Progress in Electromagnetic Research (PIER) B,* USA, Vol. 49, pp 155- 176, 2013.

[6] N. Faruk, M. Gumel, A. Oloyode and A. Ayeni, (2013)"Performance Analysis of Hybrid MAC Protocol for Cognitive Radio Networks*," Int'l J. of Communications, Network and System Sciences*, Vol. 6 No. 1, 2013, pp. 18-28. doi: 10.4236/ijcns.2013.61003.

[7] K. A. Qaraqe, M. S. Alouini, A. El-Saigh, L. Abuhantashi, M. Al-Mulla, A. Jolo, A. Ahmed, "Measurement And Analysis of Wideband Spectrum Utilization in Indoor and Outdoor Environments,"*International conference on Communication Technologies (ICCT , 2010)* Riyadh, Saudi Arabia, Jan 2010.

[8] K. E. Nolan, "700MHz Band Spectrum-Usage Measurements from Denver to Washington Dc During November 2007 And Their Value In Helping Software-Defined Radio Enter The Mainstream"

[9] M. Mehdawi, *et al,*"Spectrum occupancy survey in HULL-UK for cognitive radio applications: measurement & analysis." *International Journal of Scientific & Technology Research* 2, no. 4,pp 231-236, 2013.

[10] A..Marţian, et *al*, "Evaluation of Spectrum Occupancy in an Urban Environment in a Cognitive Radio Context."*International Journal on Advances in Telecommunications* 3, no. 3,pp 172 -181,2010.

[11]T. J. Harold, R. A. Cepeda, M. A. Beach, " Long-Term Measurements of Spectrum Occupancy Characteristics", *New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on*. IEEE, 2011.

[12] M. Wellens, J. Wu, P. Mahonen, " Evaluation of Spectrum Occupancy in Indoor and Outdoor scenario in the Context of Cognitive Radio*", Proc. 2nd International Conference Cognitive Radio Oriented in Wireless Network Communication. CrownCom*2007,Orlando,FL,USA 2007,pp 420 - 427.

[13] S. W. Ellingson, "Spectral occupancy at VHF: implications for frequency-agile cognitive radios," In *IEEE Vehicular Technology Conference*, vol. 62, no. 2, p. 1379. IEEE; 1999, 2005.

E-Voting in Nigeria: A Survey of Voters' Perception of Security and Other Trust Factors

Oluwafemi Osho*, Victor Legbo Yisa, Olawale Joshua Jebutu
Department of Cyber Security Science,
Federal University of Technology, Minna
*Corresponding Author: femi.osho@futminna.edu.ng

***Abstract*—In March and April, 2015, for the first time in the history of Nigeria, elections were conducted, using partial electronic voting means. Specifically, smart card readers were utilized for accreditation of prospective voters. While the 2015 election exercise was adjudged the best ever in the history of the country, it was not without challenges. One of these was the failure, in many instances, of the readers to authenticate eligible voters. This study is aimed at collating the perception by voters of security and four other factors capable of influencing their trust the use e-voting system. Using questionnaire, the data collated from 306 participants were analyzed. Majority of the participants were male (63.7%), students (40.8%), within the ages of 18 and 24 years (39.5%), and intermediate in their IT proficiency level (50.3%). The study reveals that the proposed factors enhance voters' trust. Demographic differences were also found to affect the perception of the proposed factors. If the country plans to deploy full-fledged e-voting mechanism for future elections, voter education, with emphasis on voters with low IT literacy and the elderly, must be given due attention.**

Keywords—election, e-voting, smart card reader, INEC, trust

I. INTRODUCTION

The advancement and application of information and communication technology in all facets of life have provided several potential benefits including improved efficiency, convenience, with reduced costs and productivity. Most countries and institutions all around the world are using ICT to improve services for its citizenry, a trend popularly known as e-governance [1]. An example of this is the application of ICT in the conduction of elections, a phenomenon known as electronic voting or e-voting.

Electronic voting is a general term which is connected here to allude to all parts of electoral voting that includes some component of casting or tallying of votes using electronic means [2][3]. Adoption of electronic voting during elections could solve problems, usually associated with manual voting, such as long queues, invalid votes, fraudulent votes, and help ensure transparency [4].

Many countries are at different stages of e-voting adoption. Countries like Australia, Canada, France, and Japan, have implemented legally binding e-voting and legally binding remote e-voting systems. While most countries are still holding pilots and trials, other countries, including Germany, Ireland, and Netherlands have stopped using e-voting for elections, due to the conclusion that further developments are needed in the fields [5].

Prior to 2015, elections in Nigeria had been conducted using traditional (manual) method of voting. Not surprisingly, each election had always been plagued by irregularities, rigging, and other forms of malpractices, malfeasances, and electoral fraud, which often lead to loss of lives and property [6], [7], [8], [9], [10]. Transparency, freeness, and fairness – which are all requirements of a voting system – have always been lacking. Mass ballot paper thumb printing, exemption of valid voters from the voters list, intimidation, errors due to miscomputation and forged results, snatching of ballot boxes, impersonation, and inflation of election results, to mention but few, were commonplace [11], [12]. The situation got so critical that some authors labeled elections in Nigeria as inseparable from violence [13], and synonymous with rigging [10]. Consequent upon these, [14] concluded that the manual method of conducting elections in Nigeria had been "bought over and corrupted;" thus highlighting the need for new ideas and methods of voting.

Attempts, in the past, to adopt the use of e-voting system by the Independent National Electoral Commission (INEC) in Nigeria were resisted, even by the legislature [6]. Sections 53(2) of the Electoral Act, 2006 [14], and 52 of the Electoral Act, 2010 [15], for instance, prohibited the use of an e-voting system. This resistance was borne out of the fact that past projects in the country had failed. And there was no guarantee that embarking on the use of e-voting system would fare better. In other words, the government could not be trusted in such critical area. Trust (or distrust) is easily transferable [16]. Having earned citizens' distrust in one area, it would be difficult for the government to be trusted in others.

However, over the years, the country has made significant progress in the adoption of technology. An instance is the adoption trend of mobile technology and internet, which have continually maintained an upward surge. From 2000 to 2013, the percentage of individuals using the internet rose from 0.06 to 38.00 [17], while the

number of mobile subscribers have moved from 0.02 to 67.68 per 100 inhabitants, within a period of 12 years, from year 2000 [18]. Having experienced the benefits that information technology affords, the realization that more and more processes manually being handled could be automated has continued to grow stronger and wider. This explains the yearnings and calls, from different sectors, for the adoption of e-voting system for the conduction of elections [12], [14], [15],[19], [20], [21]. And, considering the fact that even developing countries, like India and Brazil have successfully implemented e-voting for the conduction of their respective elections[12], [16], Nigeria cannot afford to continue with the traditional method.

In March and April, 2015, during the general elections, Nigerians witnessed the partial use of e-voting system to complement the manual method. By taking this stride, the country joined the league of low- and middle-income countries that have utilized biometric identification systems for voter identification. Up to 34 of these countries, including Ghana, Senegal, Cameroun, Zambia, Kenya, Malawi, Mali, Mauritania, Sierra Leone, and Rwanda had implemented, for one election or the other, this partial adoption of e-voting system [15].Essentially, the decision to adopt the use of information and communication technology tools was the result of part of the recommendations of the Registration and Election Review Committee, a committee of experts on electoral issues inaugurated by INEC in 2011 [10].

During the 2015 general elections, e-voting mechanism was deployed to ease accreditation process. Smart card readers (SCRs), a low power consumption technological device running on the android operating system, were utilized for accreditation of voters, via authenticating and confirming voters' Permanent Voter's Cards (PVCs) [10], [15], [22]. The permanent voter's card has a chip embedded into it to verify and authenticate prospective voters by comparing the biometrics earlier obtained and stored in the database during registration with that of the voter on the spot.

Before the elections, INEC test-ran the SCRs in 12 states of the Federation [23]. Unfortunately, most of the problems encountered during the test run were still experienced during the elections. For instance, some of the card readers broke down and were not able to perform its intended purpose. Others showed blank screens, while others had Subscriber Identification Module (SIM) issues [24]. Even where the card readers worked, and were able to correctly display voter's information from the PVC, verifying voters using their biometrics was very difficult [24], [25]. Yet, in spite of the shortcomings recorded, the use of the SCRs boosted voters' confidence in the electoral processes. Hence, it was not surprising that the number of elections petitions substantially dropped after the elections [15].

Electronic voting, over the years, has attracted vast amount of studies, spanning across many disciplines. However, most of these studies have concentrated on the technical aspect. These include e-voting design requirements [5], [26]; development [27], [28], [29], [30]; security [31], [32];and implementation issues [33]. Quantitative studies have been mainly focused on investigating perceptions on requirements or factors that influence trust of, readiness to accept, and adoption of e-voting systems. Kimbi & Zlotnikova [16] investigated readiness factors, considering Tanzanian voters. Nu'man [34] developed a trust model to ascertain what trust requirements are applicable to voters in Jordan. Yao and Murphy [35] sampled potential voters in US, exploring their perceptions about e-voting requirements capable of influencing intention to use the systems.

Few studies have attempted exploring adoption models in the context of Nigeria. Studies by [12] and [36] focused on exploring factors that affect e-voting adoption from the perspective of managerial and operational staff of INEC– the nation's Election Management Body (EMB).

It has already been established that Nigerians are in support of the adoption of e-voting for elections in the country [21].Yet, some pertinent questions need to be answered: Are all categories of voters similar in their opinion of e-voting system? Do voters prefer e-voting system to the traditional manual system? Which e-voting mechanism is most preferred by voters? What factors would enhance voters' trust in the adoption of e-voting system? This study seeks to identify some trust requirements capable of influencing, and investigate the level of influence of these requirements on, voters to trust the adoption of e-voting technology in Nigeria.

The rest of the study is organized as follows: section 2 discusses the theoretical foundations on which our model is based, and presents the research model. The methodology used in the study is described in section 3. Section 4 presents the results, while discussions on the results are presented in section 5.

II. THEORETICAL FOUNDATION

In this research, the proposed model of trust requirements is hinged on two research areas: information technology adoption and e-voting system (EVS) design. These are discussed below.

Information Techn ology Adoption

Different theoretical models have been developed to explain user acceptance or adoption of technology, with varying capacity to explain the variance in the intention by individuals to use technology [37]. Some of these models include the Technology Adoption Model (TAM) [38],Technology-Organization-Environment (TOE) [39], Diffusions on Innovation (DOI) [40], and that proposed by [41].Attempts have also been made to develop adoption model with specific focus on e-voting [12], [36].

One model, however, that encapsulates the conceptual and empirical frameworks of eight of these commonly used models, is the Unified Theory of Acceptance and Use of Technology (UTAUT), developed by [37]. This model has been demonstrated to be highly effective at explaining variance in user acceptance and usage behavior.

UTAUT is composed of four constructs: performance expectancy, effort expectancy, social influence, and

facilitating conditions. Performance expectancy connotes the measure of perceived usefulness of a system towards achieving 'gains in job performance.' Effort expectancy refers to the measure of ease of use of the system. Social influence describes the perceived social approval to use the new system, while facilitating conditions are the measure of perceived availability of the system's supporting organizational and technical infrastructure.

Extending this model to e-voting, three of the constructs, with the exception of social influence, can be applied to understand e-voting acceptance. These constructs capture specific requirements of e-voting systems. Performance expectancy directly relates with requirements such as security, privacy, and reliability. Effort expectancy is synonymous with ease of use of the e-voting system. Facilitating conditions, on the other hand, captures availability of the system.

E-Voting System Design

In reality, developing a perfect e-voting system is essentially an impossible task, given the current architecture of the internet and the PC [42], [43]. Notwithstanding, designing an EVS is a complex task. Zissis [5] explained that the complexity involved in this system is due to a host of multidisciplinary requirements that must be satisfied. Beyond technological considerations are legal, political, and societal influences [5].

Every EVS must satisfy some requirements. These have been categorized under legal, functional, operational, and security requirements. Some of these include [5], [35], [44]: availability, authenticity, freedom, eligibility, practicability, robustness, security, uniqueness, verifiability, fairness, democracy, privacy, ease of use, accuracy, integrity, and uncoercibility. These requirements affect the likelihood, and potentially the rate, of acceptance of any EVS. In other words, if an EVS would be accepted by users, there must be evidence that such system possesses most of the aforementioned characteristics.

A critical look at the requirements reveals that there are five major requirements, namely availability, security, privacy, ease of use, and reliability. Every other requirement is directly or indirectly related to one of these requirements. This work defined these primary requirements in respect of e-voting and list other related requirements:

Availability: the property of a system to be accessible to authorized users whenever needed. This is closely linked with mobility and accessibility. With respect to e-voting, valid voters are provided with the means to cast their vote. Satisfying this requirement entails protecting the system against primarily network attacks capable of making the system unavailable to access. These attacks include distributed denial of service, traffic redirection, connection flooding, hardware-based attack [5], and jamming attack.

Security: the property of an EVS to ensure voters and voting integrity. It encapsulates security of e-voting components: hardware, software, communications information [45] against different attacks. These attacks include insider (programmer), phishing, DNS, spoofing, denial of service, distributed denial of service, automated vote buying, and malware attacks [42], [26], [43], [46].A secure e-voting system guarantees every vote is tamper-proof [29]. E-voting systems arguably require the highest possible level of security [34], exceeding that required for e-commerce [5], [43]. Security ensures other requirements like integrity, freedom, secrecy, equality, generality, fairness of elections [5], and authenticity.

Privacy: this is a system's capability that ensures that a particular vote cannot be linked to a voter [29], [34], [35]; any traceability between a vote and its voter is basically removed [47]. An e-voting system that guarantees privacy ensures voters' votes are not revealed by the system. Based on this description, privacy is related with anonymity, confidentiality, uncoercibility, and secrecy.

Ease of use: the property of an EVS that makes voters able to use it with little or no assistance. An e-voting system that is easy to use is especially beneficial to those with low computer literacy. One other requirement in the same category is practicability.

Reliability: this is synonymous with dependability. It connotes a system's capacity to function as required. Such a system performs exactly as expected. A reliable system ensures that the voting outcome is the absolute consequence of the votes cast [26]. For instance, a reliable e-voting system must ensure no valid vote is rejected, and no invalid vote is accepted [34]. A reliable system is also capable of ensuring eligibility, robustness, accuracy, fairness, and democracy.

III. RESEARCH MODEL

Acceptance of new system always correlates with trust in such systems. The achievement of public trust has always been one of the cardinal objectives for implementing e-voting system [5]. This trust is enhanced when such system proves its dependability [34], and closely knit with this property of reliability is security.

The Council of Europe, in their guidelines on transparency of e-enabled elections [48] emphasized that "… trust should not be taken for granted and states need to do their utmost in order to ensure that it is preserved. All the more so because once trust and public confidence is diminished, it is exceedingly challenging to regain it."

Our trust model, represented in Figure 1, suggests that these five main requirements independently affect voters' trust. Based on this, the following hypotheses were proposed:

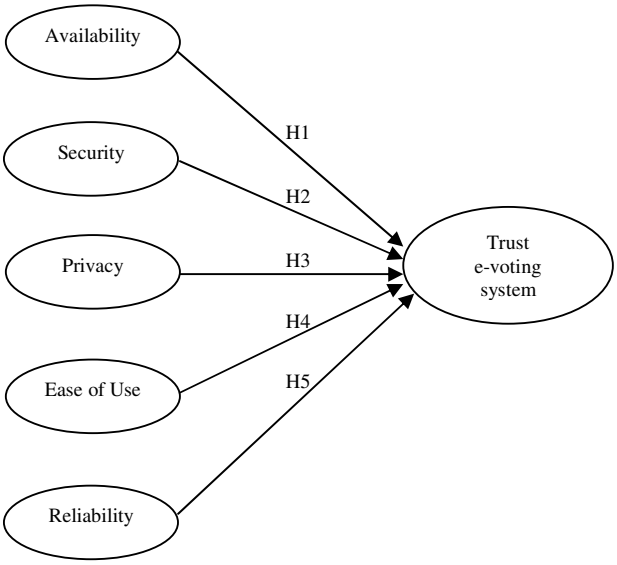
H1: higher availability will influence voters' trust, and consequently participating, in the use of the electronic voting system.

H2: higher security of the system will influence voters' trust, and consequently participating, in the use of the electronic voting system.

H3: higher privacy of the system will influence voters' trust, and consequently participating, in the use of the electronic voting system.

H4: higher ease of use of the system will influence voters'trust, and consequently participating, in the use of the electronic voting system.

H5: higher reliability of the system will influence voters'trust, and consequently participating, in the use of the electronic voting system.



Proposed model of trust factors

IV. METHODOLOGY

Survey Research Technique

In this research, to collate data, a survey was conducted between October and November, 2014 in one of the northern states in Nigeria. A combination of purposive and stratified random sampling techniques were employed in the selection of participants. Based on the fact that the minimum age requirement to be eligible to vote is 18 years, it was ensured that only participants eligible to vote were considered. This work then divided the above-18-years population into three groups: students, employed, and Non-employed. Participants from each group were sampled randomly.

The research instrument used was questionnaire. In total, 350 questionnaires were distributed. Out of these, 306 were valid, and consequently used in the analysis. The participants consist of 195(63.7%) males and 111(36.3%) females. Majority were students (40.8%), within the ages of 18 and 24 years (39.5%). Most (50.3%) classified their IT proficiency level as intermediate. The sample characteristics of the respondents are presented in Table 1.

Procedures and Data Analysis

The questionnaire (see Appendix F) used was composed of three sections. The first section contains definition of terms related to electronic voting used in the construction of the scale items. General questions pertaining to respondents' characteristics, and order of preference among the three main mechanisms of deploying electronic voting constituted the second section. The last section presents the measurement scales, each with 3 items. Level of agreement was indicated on a 5-point Likert scale, ranging from 1 = Strongly Disagree to 5 = Strongly Agree.

A pilot test was performed involving 28 respondents including IT faculty members and professionals, students, employed and unemployed personnel participated in a pilot test. Various comments were considered in revising the questionnaire, to improve its validity.

A candid assessment of the 10 IT faculty members and professionals who participated in the pilot test was sought. They were requested to rate the general layout, complexity, and relevance of the questions under each factor, using a scale of 1 to 5, where 1 stands for lowest score and 5 for the highest score. A minimum of 70% rated the general layout of the questionnaire, and each proposed factor, 4 and above. On the other hand, in terms of complexity, 70% scored the questionnaire 3 and below.

The internal consistency of the factors was measured with Cronbach's alpha coefficient. The overall internal consistency of the 15 items was 0.92, which indicate high reliability of the items. Each of the scales also indicated high reliability. The mean, standard deviation, and internal consistency of the 5 factors are presented in Table 2.

For the analysis of the data, SPSS 16.0 was used for descriptive analysis of the sample characteristics, and Amos 22 for confirmatory factor analysis of the constructs. For assessing model adequacy, Goodness-of-fit index (GFI), comparative fit index (CFI), both of which must be above 0.9 to have a good fit [35], [49];the root mean square error of approximation (RMSEA), with value between 0.05 and 0.08 considered acceptable; and the normed chi-square (χ^2/df), where value less than 3 implies a good fit[50].

V. RESULT

Preferred E-Voting Mechanism

From this study, Table 1 shows the sample characteristics of the used respondents while Table 2 shows their level of consistency. Table 3 shows the rank of the E-voting system.

TABLE 1. SAMPLE CHARACTERISTICS OF RESPONDENTS

	Frequency	Percent
Sex		
Male	195	63.7
Female	111	36.3
Age		
18 – 24	121	39.5
25 – 34	96	31.4
35 – 44	62	20.3
45 – 54	22	7.2

55 – 64	4	1.3
Above 64	1	0.3
Occupation		
Student	125	40.8
Employed	95	31.0
Unemployed	86	28.1
IT Proficiency Level		
Novice	35	11.4
Intermediate	154	50.3
Advanced	90	29.4
Expert	19	6.2
Missing Values	8	2.6
Participated in Voting		
Yes	196	64.1
No	110	35.9
Preferred Voting System		
Manual Voting	75	24.5
E-Voting	225	73.5
Missing Values	6	2.0
Study Total	306	100.0

TABLE 2. MEAN, SD AND INTERNAL CONSISTENCY OF MODEL FACTORS

Factor	No. of Item	Mean	SD	Cronbach's alpha
Availability	3	4.41	0.83	0.70
Security	3	4.38	0.86	0.82
Privacy	3	4.29	0.82	0.77
Ease of Use	3	4.46	0.77	0.83
Reliability	3	4.50	0.79	0.81

When asked of the preferred voting method, 73.5% of participants reported they prefer electronic form of voting to the manual method. The study found out that in the category of participants who are novice in their level of IT proficiency, majority (72.7% v 27.3%) preferred manual voting. This contrasted sharply with other IT proficiency categories. In these categories, e-voting was preferred, with increasing percentage of majority from the intermediate to the expert category: intermediate (21.7% v 78.3%), advanced (16.9% v 83.1%), and expert (11.1% v 88.9%). The finding was highly significant ($\chi^2 = 45.54,\ p < 0.001$).

They were also requested to rank the 3 different electronic voting deployment platforms, in order of their preferences, from 1 = most preferred to 3 = least preferred. To identify if participants have different preferences for the e-voting mechanisms the Friedman test was used. The mean ranks of the mechanisms are presented in Table 3. Web-based e-voting system has the least mean rank.This implies it is the most preferredform of e-voting system.However, the finding was not significant ($\chi^2(1) = 3.66,\ \mathrm{p} = 0.16$). It therefore cannot be concluded that voters do have different preferences for all the e-voting mechanisms.

TABLE 3. MEAN RANK OF E-VOTING MECHANISM

E-Voting Mechanism	Mean Rank
Polling booth/Kiosk voting system	2.09
Web-based EVS	1.94
Mobile-based EVS	1.97

Measurement Model results

The results of the measurement model and confirmatory factor analysis of security and other trust factors are presented in Table 4 and Figure 2 respectively. The obtained model fit indices were GFI = 0.90, CFI = 0.93, RMSEA = 0.08, $\chi^2/df = 2.87$, and p < 0.001. The factor loading of each latent variable was high, with range from 0.54 – 0.86.The same can be observed with the scales. Each factor loading was also high, with values between 0.76 and 0.92.

Some post hoc analyses were performed to see if there are differences in perception based on the individual factors. The focus was on perception by sex, age, occupation, IT proficiency level, and voting experience. In the perception by sex (see Appendix A), male participants had higher perception scores for three of the characteristics: security, privacy, and ease of use. Both sexes had similar perception for availability and reliability.

Considering perception by age (Appendix B), in all the characteristics, except security, the perception scores by the age group 55 – 64 were lower than the rest of the groups. Based on occupation (Appendix C), the study reveals those who were unemployed rated all the characteristics lower, when compared to the scores by those in other occupation categories. One interesting finding is the perception by IT proficiency level (Appendix D).

In all the characteristics, with increasing level of proficiency, there was increase in perception score. The same as discovered when the perceptions by voting experience was considered (Appendix E). Those who possessed voting experience scored all the characteristics higher.

VI. DISCUSSION

This study aimed to explore the perception of voters on security and four other trust factors, to influence participation in the use of e-voting system for elections in Nigeria. The construction of the factors was based primarily on e-voting system characteristics. The scale items indicated high internal consistency. Data used for testing the measurement model were collated using survey method. Majority of the participants were male, students, within the ages of 18 and 24 years, and intermediate in terms of IT proficiency. Majority of the participants had participated in one or more elections in the past.

The study found out that majority of voters would prefer the use of e-voting system, rather than continue with the manual method primarily in use. This is consistent with the finding of [21]. However, voters who deem themselves novice in their IT proficiency level prefer the country continue to utilize manual voting during elections. Kimbi and Zlotnikova[16]had identified low IT literacy as an impediment to acceptance of e-voting system. Much effort

would no doubt be required to convince this category to accept the use of e-voting system. Equally to increase such voters' trust, the electronic voting system must be developed to guarantee maximum ease of use. This finding also highlights the need for government to develop necessary measures to bridge the digital divide.

Another finding is the lack of significant evidence to conclude that voters prefer one e-voting method to another. One explanation is that voters in Nigeria are generally not used to the use of electronic method of voting. An e-voting system was used, partially, for the first time in the last 2015 general elections. Until there is full adoption, voters will not be able ascertain which mechanism is most preferable.

TABLE 4. MEASUREMENT MODELRESULT

Factor	Item	Loading
Availability	Be deployable via mobile and web platforms, and/or a polling station	0.54
	Have facilities for all eligible citizens, including disabled and old citizens, to be able to vote.	0.71
	Be accessible right from the time voting starts and all through the period of voting.	0.77
Security	Ensure only eligible voters can access the e-voting system.	0.66
	Ensure a cast vote cannot be altered by unauthorized person or system.	0.86
	Be secure against session hijacking, malware, and other forms of attack.	0.83
Privacy	Ensure voters' identification data are secure against unauthorized disclosure and alteration.	0.76
	Ensure no vote can be traced to a particular voter.	0.63
	Ensure no attacker can successfully eavesdrop on a voter during voting process.	0.83
Ease of Use	Be easy to learn to use.	0.82
	Be simple to operate.	0.86
	Provide help facility readily available to voters in the event of problems with voting procedures.	0.71
Reliability	Ensure no voter can successfully cast more than one vote.	0.82
	Be able to acquire votes correctly, i.e., any vote cast is rightly recorded.	0.78
	Not reject valid votes nor accept invalid votes.	0.70

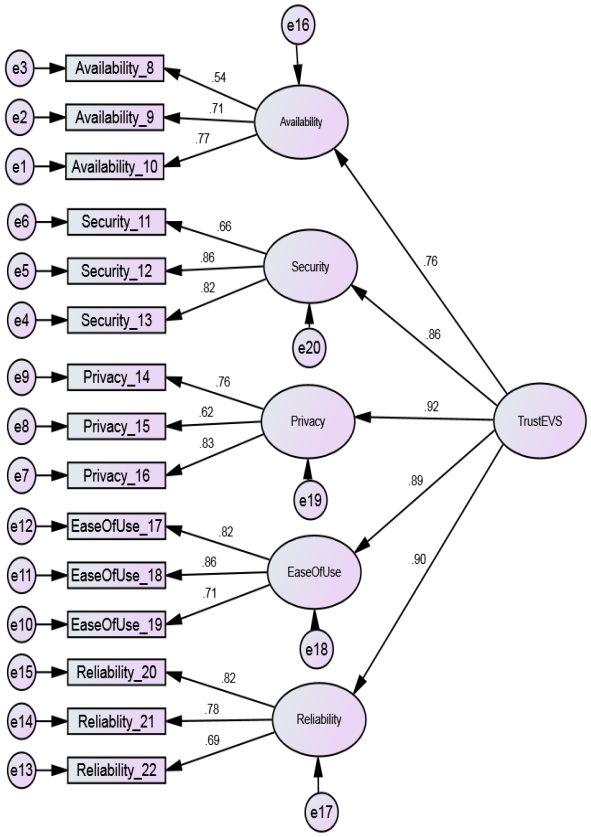


Fig 2. Confirmatory factor analysis of security and other trust factors.

As expected, all five factors – privacy, reliability, ease of use, security, and availability – are capable of enhancing voters' trust in the acceptance of e-voting system for elections. A similar result was recorded in [16], where majority of voters in Tanzania have concerns over security, reliability, and privacy of e-voting, though they prefer the system to the existing manual system. The authors cautioned that absence of security, reliability, and privacy would pose serious threats to acceptance of e-voting. Thus, an EVS that would earn voters' trust, and consequently determine their acceptance and participation, must satisfy all these requirements.

Surprisingly, security was rated only ahead of availability. Privacy was placed in the first position. When privacy is related with anonymity, confidentiality, uncoercibility, and secrecy, it becomes clearer while this is most paramount to Nigerian voters. The use of coercion, either physically or subtly, from informal observations, is not new in the country. For instance, during the last general elections, one of the authors witnessed prospective voters in a particular polling booth being promised monetary rewards once they voted for a particular candidate. While a voter cast vote, the agent of the candidate was close by to ensure such

voter voted as instructed. It is obvious that any system that would guarantee the privacy of voters would be welcomed.

Closely tied to privacy was reliability. The smart card readers used during the 2015 general elections were not reliable. If one views this characteristic in connection with eligibility, accuracy, fairness, and democracy, it can be said unequivocally that if electronic form of voting would be used for future elections, the government must ensure these related characteristics are given due attention in the e-system design. During the elections, many eligible voters were not authenticated by the readers. The voters' registration sheets had to be completely resorted for accreditation of voters.

Ease of use is another important factor to influence trust in an e-voting system. Any system that is difficult to use, regardless of the amount of functionalities it possesses, would not be easily acceptable by users. Most voters would prefer to cast their votes with little or no help, even if they have to use an electronic system.

It has been cautioned that replacing manual, paper-based, voting with e-voting could exclude a sizeable number of voters from participating [51], most of which would likely be old voters and those with low computer literacy. Studies have ascertained the fact that age provides a bias towards e-voting, with young voters having most bias for the system[16], [35], [51]. Providing an easy to use e-voting system would inevitably contribute substantially to alleviating this potential challenge. Zissis [5] advised that to make e-voting as equivalent to manual voting, ease of use and accessibility must be guaranteed.

An e-voting system that aims to gain its users' trust must guarantee security, as deduced from the study. This covers security of voting data and channels. Voter and voting integrity are essential for any essential election. To ensure security of e-voting system, [16] warns that it must not be perceived only from a technical point of view. Issues relating to security are often local, specific to individual country. The government and EMB will do well to identify the local threats, and put necessary mechanisms in place to address them.

The least scored factor was availability. However, the rating is high enough to affect voters' trust. Voters definitely would appreciate a voting system that is easily accessible; and deployable via different platforms, including mobile platform. Mobile penetration is Nigeria has continued to maintain upward trend. This technology could be leveraged on for election purpose.

One other interesting findings in this study is the need for due attention to be paid to demographic differences. Those who had ever voted in Nigeria gave higher considerations to the proposed trust factors. Also, the level of rating was influenced by level of IT proficiency. Considering the fact that majority of voters with low computer literacy prefer manual to electronic voting system, simply explains why they rated all the trust factors less than voters in other IT proficiency category. The implication is that the government needs to massively improve existing methods employed for voter education.

This study also agrees with [37] in the moderation of performance expectancy by age. Using the UTAUT, it was noted that the influence of performance expectancy is stronger for men. From the study, while both men and women rated reliability equally, the men were more disposed to security and privacy. The study also reveals that men also tend to value ease of use, as a trust factor, more than women. This contradicts the finding of [35].

VII. CONCLUSION

The Independent National Electoral Commission (INEC) has been urged to utilize electronic voting mechanism for future elections [19], [20]. One important summary of this study is that any e-voting system the Commission hopes to deploy must give due considerations to characteristics that a typical e-voting system must possess. Essentially, privacy, reliability, ease of use, security, and availability are critical to enhancing voters' trust in the system.Also, voter education, with emphasis on voters with low IT skills and adult voters, would be indispensible.

Having recorded some significant gains upon the partial adoption of e-voting during the 2015 general elections, it is evident that embracing e-voting fully can only improve election processes in Nigeria. The country must therefore take decisive steps towards full implementation of electronic voting. Evidently, the electoral reforms will be gradual. The starting point could be establishing necessary legislative framework. An example is Kenya, which, in a bid to reform her electoral processes, established a new electoral body. One of the mandates given to the Commission was "the use of appropriate technology and approaches in the performance of its functions" [52]. However, considering the consequences Nigerians have experienced in past elections as a result of the perversion of the manual methods, it is evident that the country cannot afford to get it wrong, when she decides to fully implement electronic voting system.

While this study has exposed some important findings in respect of the adoption of electronic voting systems for future elections in Nigeria, there are limitations. The fact that data was collected within one state of the country imposes a constraint to generalizing the result of the study as being representative of the entire country. While it may be argued that experience by voters during elections, which potentially could affect their disposition to a new system of voting, are similar across the nation, further studies, covering preferably all the geopolitical zones of the country,are required before accurate generalization can be made.

Another limitation is the lack of consideration of the relationships among the different factors. Essentially, all the factors are inter-connected. An e-voting system that cannot guarantee security would invariably not ensure privacy. These inter-relationships could also be explored in further studies for the construction of the measure model.

REFERENCES

[1] O M Olaniyi, D O Adewumi, E A Oluwatosin, O T Arulogun, and M A Bashorun, "Framework for Multilingual Mobile E-Voting Service Infrastructure for Democratic Governance," *African Journal of*

Computing and ICT Nigeria Computer, vol. 4, no. 3, pp. 23 – 32, 2011.

[2] S. A. Adeshina & O. Adegboyega, "Design Imperatives for Evoting as a Socio-technical System," in Electronics, Computer and Computation (ICECCO), 2014 11th International Conference on, 2014, pp. 1-4.

[3] Tsun-Shao Chen. (2003, July) https://files.nyu.edu/tsc223/public/ElectronicVoting.pdf

[4] Murshadul M Hoque, "A Simplified Electronic Voting Machine System," international Journal of Advanced Science and Technology, vol. 62, pp. 97-102, 2014

[5] D. Zissis, "Methodologies and technologies for designing secure electronic voting information systems," Unpublished.

[6] C. Ayo, A. A. Adebiyi, & A. B. Sofoluwe, "E-Voting Implementation in Nigeria: The Success Factors," in Curbing Political Violence in Nigeria: The Role of Security Profession, R. I. Salawu, A. Akinade, & S. O. Adetona, Eds., 2008, pp.50-60.

[7] J. Iteshi, "Audio-visual voting method, Theonly way to build genuine democracy in Nigeria," 2006, Retrieved from http://www.gamji.com/article6000/NEWS6205.htm

[8] L. Anyanya, "Assessment of 2011 elections in view of recommendations from the 2010 workshop," in Election Security in Nigeria: Matters Arising, L. Olurode, Eds. Abuja: Friedrich-Ebert-Stiftung, 2013, pp. 19-30.

[9] M. Igini, "Election security in theory and practice: Perspective of a resident electoral commissioner," in Election Security in Nigeria: Matters Arising, L. Olurode, Eds. Abuja: Friedrich-Ebert-Stiftung, 2013, pp. 43-62.

[10] k. Bolaji, "Toward institutionalizing credible elections in Nigeria: A review of reform measures by the Independent National Electoral Commission" in Improving Electoral Practices: Case Studies and Practical Approaches, Stockholm: Institute for Democracy and Electoral Assistance, 2015, pp. 49-82.

[11] F. N. Okafor, "Electoral Violence and The 2015 General Elections in Nigeria: The Implication Perspective," *Afro Asian Journal of Social Sciences*, vol. VI, no. 1, pp. 1-14, 2015.

[12] S. R. Ishaq, W. R. S. Osman, A. J. K. Shittu & R. G. Jimoh, "Adoption of e-voting system in Nigeria: A conceptual framework, " International Journal of Applied Information Systems, vol. 5, no. 5, 2013, pp.8-14.

[13] L. Olurode & M. K. Hammanga, "Deployment of security personnel in elections: Challenges and lessons from the field," in Election Security in Nigeria: Matters Arising, L. Olurode, Eds. Abuja: Friedrich-Ebert-Stiftung, 2013, pp. 63-85.

[14] F. Okoye, "Nigeria: Civil Society Groups and Electronic Voting Systems, the Challenges," Vanguard, January 2010, Retrieved from http://www.vanguardngr.com/2010/01/civil-society-groups-and-electronic-voting-systems-the-challenges/

[15] C. Nwangwu, "Biometric Voting Technology and the 2015 General Elections in Nigeria," Conference on The 2015 General Elections in Nigeria: The Real Issues, July 2015. Retrieved from http://www.inecnigeria.org/wp-content/uploads/2015/07/Conference-Paper-by-Chikodiri-Nwangwu.pdf

[16] S. Kimbi & I. Zlotnikova, "Citizens' readiness for remote electronic voting in Tanzania," Advances in Computer Science: an International Journal, vol. 3, issue 2, no. 8, 2014, pp.150-159.

[17] ITU, "Individuals Internet: 2000-2013," Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls

[18] ITU, "Mobile_cellular_2000-2012," Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Mobile_cellular_2000-2012.xls

[19] S. Daniel, "2015: As Buhari's victory covers INEC flaws…," Vanguard, May 2015, Retrieved from http://www.vanguardngr.com/2015/05/2015asbuharisvictorycoversinecflaws/

[20] C. Okeke, "Implement electronic voting in 2019, CSO tell INEC," Leadership, June 2015, Retrieved from http://leadership.ng/news/440398/implementelectronicvotingin2019csostellinec

[21] C. Ayo, A. Adeniyi, & I. Fatudimu, " E- Democracy: A Requirement for a Successful E-Voting and E-Government Implementation in Nigeria," International Journal of Natural and Applied Sciences, 4(3), 2008, pp. 310-318.

[22] INEC. (2015) www.inecnigeria.org. [Online]. www.inecnigeria.org/wp./FactSheet-on-PVC-and-Card-Readers.docx

[23] A. Hassan. (2015, March) Premium Times. [Online]. http://www.premiumtimesng.com/news/headlines/178264-inec-says-card-reader-test-successful-admits-41-fingerprints-verification-failure.html

[24] Vanguard. (2015, march) Vanguard Nigeria. [Online]. http://www.vanguardngr.com/2015/03/after-initial-card-reader-failure-nigerians-persevere-vote-in-peaceful-elections/

[25] N. Ibeh. (2015, March) Premium Times. [Online]. http://www.premiumtimesng.com/news/top-news/179447-3-card-readers-fail-to-accredit-jonathan.html

[26] D. A. Gritzalis, "Principles and requirements for a secure e-voting system," Computers & Security, vol. 21, no. 6, 2002, pp. 539-556.

[27] M. Malkawi, M. Khasawneh, O. Al-Jarrah, & L. Barakat, "Modeling and simulation of a robust e-voting system," Communications of the IBIMA, vol. 8, 2009, pp. 198-206.

[28] R. Alaguvel & G. Gnanavel, "Offline and online e-voting system with embedded security for real time application," International Journal of Engineering Research, vol. 2, no. 2, 2013, pp. 76-82.

[29] G. Z. Qadah & R. Taha, "Electronic voting systems: Requirements, design, and implementation," Computer Standards & Interfaces, vol. 29, 2007, pp. 376-386.

[30] L. O. Osho, "Development of a hybrid e-voting system using cloud architecture," Unpublished.

[31] I. Ray, I. Ray& N. Narasimhamurthi, "An anonymous electronic voting protocol for voting over the internet," Proceedings of the Third International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems, WECWIS, 2001, pp. 188-190.

[32] A. Juels, D. Catalano & M. Jacobsson, "Coercion-Resistant Electronic Elections," Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005, pp. 61-70.

[33] R. kofler, R. krimmer & A. Prosser, "Electronic voting: algorithmic and implementation issues," Proceedings of the 36th Hawaii International Conference on System Sciences, 2003, pp.1-7.

[34] A. Nu'man, "A framework for adopting e-voting in Jordan," Electronic Journal of e-Government, Vol. 2, Issue 2, 2012, pp.133-146.

[35] Y. Yao & L. Murphy, "Remote electronic voting systems: an exploration of voters' perceptions and intention to use," European Journal of Information Systems, Vol. 16, 2007, pp.106-120.

[36] S. R. Ishaq, R. G. Jimoh, W. R. S. Osman, & A. J. K. Shittu, "Adoption of e-voting systems: A case study of Independent National Electoral Commission (INEC), Nigeria: A Preliminary study," Knowledge Management International Conference (KMICe), Malaysia, pp.304-308, July 2012.

[37] V. Venkatesh, M. G. Morris, G. B. Davis & F. D. Davis, "User acceptance of information technology: Toward a unified view," MIS Quarterly, vol. 27, no. 3, 2003, pp. 425-478.

[38] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS Quarterly vol. 13, no. 3, 1989, pp.319–339.

[39] L. Tornatzky, & M. Fleischer, The Process of Technology Innovation, Lexington, MA: Lexington Books, 1990.

[40] E. M. Rodgers, Diffusion of Innovations, 4th ed. New York: Free Press, 1995.

[41] C. L. Iacovou, I. Benbasat, & A. S. Dexter," Electronic Data Interchange and small Organizations: Adoption and Impact of Technology," MIS Quarterly, 19(4), pp. 465- 485.

[42] D. Jefferson, A. Rubin& B. Simons, "A comment on the May 2007 DoD report on Voting Technologies for UOCAVA Citizens" Retrieved from https://www.verifiedvoting.org/wp-content/uploads/2014/10/serve_dod_comment_2007.pdf

[43] D. Jefferson, A. D. Rubin, B. Simons & D. Wagner, "A security analysis of the Secure Electronic Registration and Voting Experiment (SERVE)," 2004, Retrieved from http://requiem.googlecode.com/files/paper.pdf

[44] A. Al-Ameen & S. A. Talab, "E-voting System Vulnerabilities," in Information Science and Digital Content Technology (ICIDT), 2012 8th International Conference, 2012, pp. 67-73.

[45] E. Onyekpere, "Election security finance," in Election Security in Nigeria: Matters Arising, L. Olurode, Eds. Abuja: Friedrich-Ebert-Stiftung, 2013, pp. 87-101.

[46] S. S. Chaeikar, M. Jafari, H. Taherdoost & N. S. C. Kar, "Definitions and criteria of CIA security triangle in electronic voting system," International Journal of Advanced Computer Science and Information Technology, vol. 1, no. 1, 2012, pp. 14-24.

[47] K. Sampigethaya & R. Poovendran, "A framework and taxonomy for comparison of electronic voting schemes," Computers & Security, vol. 25, 2006, pp. 137-153.

[48] Council of Europe, "Guidelines on transparency of e-enabled elections," 2011, Retrieved from Retrieved from http://www.coe.int/t/DEMOCRACY/ELECTORAL-ASSISTANCE/themes/evoting/CoEenabledElections_en.pdf

[49] J. F. Hair, R. E. Anderson, R. L. Tatham & W. C. Black, Multivariate Data Analysis, 5th ed., New Jersey: Prentice-Hall, 1998.

[50] L. W. Vilca & M. Vallejos, "Construction of the Risk of Addition to Social Networks Scale (Cr.A.R.S)," Computers in Human Behavior, Vol. 48, 2015, pp.190-198.

[51] A. Oostveen & P. V. D. Besselaar, "Users' experiences with e-voting: A comparative case study," International Journal of Electronic Governance, vol. 2, no. 4, 2009, pp. 357-377.

[52] L. Mahiri-Zaja, "New security challenges of election management in Kenya," in Election Security in Nigeria: Matters Arising, L. Olurode, Eds. Abuja: Friedrich-Ebert-Stiftung, 2013, pp. 115-121.

Appendices

Appendix A: Perception by Sex

Level	Availability	Security	Privacy	Ease of Use	Reliability
Male	4.41	4.39	4.30	4.49	4.50
Female	4.41	4.35	4.28	4.43	4.50

Appendix B: Perception by Age

Level	Availability	Security	Privacy	Ease of Use	Reliability
18 – 24	4.45	4.40	4.33	4.49	4.50
25 – 34	4.35	4.39	4.23	4.47	4.50
35 – 44	4.43	4.35	4.26	4.47	4.52
45 – 54	4.38	4.27	4.42	4.36	4.49
55 – 64	4.25	4.33	4.17	4.17	4.42

Appendix C: Perception by Occupation

Level	Availability	Security	Privacy	Ease of Use	Reliability
Student	4.45	4.44	4.33	4.50	4.51
Employed	4.47	4.39	4.33	4.51	4.58
Non-employed	4.27	4.27	4.18	4.36	4.38

Appendix D: Perception by IT Proficiency Level

Level	Availability	Security	Privacy	Ease of Use	Reliability
Novice	4.13	4.03	3.92	4.15	4.21
Intermediate	4.42	4.35	4.25	4.45	4.48
Advanced	4.46	4.50	4.44	4.56	4.57
Expert	4.60	4.70	4.49	4.70	4.63

Appendix E: Perception by Voting Experience

Voting Experience	Availability	Security	Privacy	Ease of Use	Reliability
Yes	4.44	4.40	4.36	4.47	4.53
No	4.36	4.33	4.17	4.46	4.44

Scale from 1 = Strongly Disagree to 5 = Strongly Agree

Appendix F: Questionnaire Item

E-Voting Adoption in Nigeria: A Survey of Voters' Perception of Security and Other Considerations

Dear Ma/Sir, the aim of this survey is to explore the degree of influence of security and other factors among voters to trust the adoption of e-voting technology in Nigeria. We therefore solicit your sincere response. Your utmost privacy is guaranteed. Thanking you for your usual cooperation.

Definitions

- **E-Voting**: (also known as electronic voting) system is an automated system of voting via electronic means. Often votes are cast and tallied electronically.
- **Session Hijacking (**mentioned in question 13**):** occurs when a hacker takes over an authenticated user's session.
- **Malware (**mentioned in question 13**):** a software or program created to cause a computer system to malfunction. Example of malware is a virus program.
- **Eavesdrop (**mentioned in question 16**):** unauthorized capturing of data packets during transmission between systems.

General Questions

1. Sex: **[ ]** Male **[ ]** Female.
2. Occupation: **[ ]** Student **[ ]** Employed **[ ]** Non-Employed.
3. Age: **[ ]** 18-24 **[ ]** 25-34 **[ ]** 35-44 **[ ]** 45-54 **[ ]** 55-64 **[ ]** Above 64.
4. Level of IT skills proficiency: **[ ]** Novice **[ ]** Intermediate **[ ]** Advanced **[ ]** Expert.

> **Novice:** requires frequent guidance in the use of computer, its applications and tools.
> **Intermediate:** requires occasional guidance in the use of computer, its applications and tools.
> **Advanced:** generally require little or no guidance.
> **Expert:** serves as key resource and advises others.

5. Have you ever participated in any voting (either at the local government, state, or national level) before? **[ ]** Yes **[ ]** No.
6. For an election, which system of voting would you prefer? **[ ]** Manual (traditional) voting **[ ]** e-voting.
7. Assuming the following three e-voting mechanisms were all available in an election, rank them according to your preference. Write '1' for your most preferred, '2' for the next preferred, and '3' for the least preferred.
   [ ] Polling booth/Kiosk e-voting system
   [ ] Web-based (Computer-based) e-voting system
   [ ] Mobile-based e-voting system

For the following statements please indicate (by ticking) your agreement using the scale:
5 = Strongly agree 4 = Agree 3 = Neutral 2 = Disagree 1 = Strongly Disagree

		5	4	3	2	1
Availability – An e-voting system should:						
8.	Be deployable via mobile and web platforms, and/or a polling station					
9.	Have facilities for all eligible citizens, including disabled and old citizens, to be able to vote.					
10.	Be accessible right from the time voting starts and all through the period of voting.					
Security – An e-voting system should:						
11.	Ensure only eligible voters can access the e-voting system.					
12.	Ensure a cast vote cannot be altered by unauthorized person or system.					
13.	Be secure against session hijacking, malware, and other forms of attack.					
Privacy – An e-voting system should:						
14.	Ensure voters' identification data are secure against unauthorized disclosure and alteration.					
15.	Ensure no vote can be traced to a particular voter.					
16.	Ensure no attacker can successfully eavesdrop on a voter during voting process.					
Ease of Use – An e-voting system should:						
17.	Be easy to learn to use.					
18.	Be simple to operate.					
19.	Provide help facility readily available to voters in the event of problems with voting procedures.					
Reliability – An e-voting system should:						
20.	Ensure no voter can successfully cast more than one vote.					
21.	Be able to acquire votes correctly, i.e., any vote cast is rightly recorded.					
22.	Not reject valid votes nor accept invalid votes.					

A Review of the Impact of Cybercrime on Nations' Economy

[1]Kenneth Sorle Nwizege, [2]Michael Mac Mammah
[3]Agbeb Nornu S.
[1,2,3,4&6]Dept. of Elect/Elect Engineering, School of Engineering, Ken Saro-Wiwa Polytechnic, Bori, Nigeria
[1]s.k.nwizege@ieee.org, [2]macmammahm@yahoo.com,
[3]agbeb_nornu@yahoo.com

[4]Irimiagha Paul Gibson, [5]Mmeah Shedrack,
[6]Harry, Inye, H.
[5]Dept. Of Computer Science, School of Applied sciences, Ken Saro-Wiwa Polytechnic, Bori, Nigeria
[4]mie4tammy@gmail.com, [5]shedrackmmeah@yahoo.com,
[6]ipadibi@yahoo.com

***Abstract*— in the modern times, a so-called smart way to perform criminal act is getting involved in cybercriminal act. This act is perpetuated by both highly learned and those that just learn computer for the purpose of implementing this atrocity. It is indeed a very ugly act that must be fought against, just like any other crimes. This observed that are daily occurrences of theft through various means such as internet/mobile banking, online transactions etc. In this paper, a review on the impact and trends of cybercrime was carried out. This was done so as to create awareness and stimulate a more security consciousness especially in the top 20 countries identified in this paper. The work emphasized on security consciousness and the need to take cybersecurity seriously. The goal is to create more security awareness in cybercrime, cybercsecurity issues and related acts.**

Keywords—computer security; cybersecurity; cybercrime; organization; threat.

I. INTRODUCTION

Cyber crime is any criminal act that deals with computers and networks. Hence, it is used to generally describe criminal activities in computer networks and internet. It is a term for any illegal activity that uses a computer as its primary means of commission. It includes traditional crimes conducted through the internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet [1].

Cyber crimes against banks and other financial institutions probably cost many hundreds of millions of dollars every year. Besides, there is cyber theft of intellectual property and businesses. These losses could just be the cost of doing business or they could be a major new risk for companies and nations as these illicit acquisitions damage global economic competitiveness and undermine technological advantage [2],[3].

Conversely, computer security involves the protection of computing systems and the data that they store or access. Computer security allows an organisation to carry out its mission by:

- Enabling people to carry out their jobs, education, and research, etc.
- Protecting personal and sensitive information (data) [4].
- Supporting critical business process

However, a good security standards must follow the "90 / 10" rule which states that:

- 10% of security safeguards are technical.
- 90% of security safeguards rely on the computer user to adhere to good computing practices, reviews on the allocated spectrum available to their region of operation.

The lock on the door is the 10%, while a user remembering to lock the door, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90%. Both parts are need for effective security. This means that everyone who uses a computer or mobile device needs to understand how to keep their computer, device and data secure.

Now, cybersecurity is the protection of valuable intellectual property and business information in digital form against theft and misuse. It is an increasingly critical management issue. The US government has identified cybersecurity as one of the most serious economic and national security challenges they face as a nation. Institutions and companies must now fend off ever-present cyber attacks. This act is influenced by cybercriminals or even disgruntled employees releasing sensitive information, taking intellectual property to competitors, or engaging in online fraud. While sophisticated companies have recently endured highly public breaches to their technology environments, many incidents go unreported. Indeed, businesses are not eager to advertise that they have had to "pay ransom" to cybercriminals or to describe the vulnerabilities that the attack exposed.

Interestingly, to reduce security risk as much as possible, this work now outlines key principles to adopt at all times:

- Learn good computing security practices.
- Incorporating these practices into everyday routine.

- Encouraging others to do so as well.
- Report anything unusual –In this case, by notifying the appropriate contacts of a suspected security incident [5].

This paper seeks to offer customized review on the impact of cyber security on a nation's economy.

The rest of the paper is organized as follows. Section II presents a literature background of study, while Section III deals with cybercrime threat. Section IV deals with the impact of cybercrime. Section IV presents the analysis of cybercrime activities. The paper concludes in Section IV.

II. LITERTAURE REVIEW

Background on Cybersecurity

Cybersecurity is the protection of valuable intellectual property and business information in digital form against theft and misuse. It is a critical issue with an alarming rate of increase. The US government has identified cybersecurity as one of the most serious economic and national security challenges [6]. With the rate of increase and complexity of the threats, organizations must adopt approaches to cybersecurity that will require much more engagement from the CEO and other senior executives to protect critical business information without constraining innovation and growth [7].

Why Cybersecurity

Large and reputable organizations have dramatically strengthened their cybersecurity capabilities over the past five years. Formal processes have been adopted to be implemented with priority. In the context of IT security risks, there have been developed strategies with hundreds of millions of dollars already committed in order to execute these strategies. Desktop environments are more vulnerable compared with how they were five years ago. This is because Universal Serial Bus (USB) ports and Web mail services are potential sources of invasion. Cybersecurity is highly indispensible in this age. This is because; the cyberspace has become a new center stage for innovations, enterprises, social networking, criminality and warfare. However, the Cyberspace that offers numerous benefits also has risks at various levels.

Why Awarness

The US Executive Order (EO) 13636 initiated a dialogue to identify challenges and determine effective responses to cybercrime. One of the areas suggested to handle this alarming security threat is the use of forum for more awareness, training, and updates [6]. The CForum is one of those helpful avenues for handling cybersecurity issues [8][9]. This can help identify critical resources that can save an organization's time. It applies the framework flexibility which is one of essential principles needed to achieve organizational cybersecurity goals. Apart from flexibility, other Framework's principles are: global impacts, risk management approaches, leverage existing approaches, standards and best practice. It has guide that will help learn how different organizations use it in different ways with different tools to achieve Framework outcomes [9].

The American Water Works Association (AWWA) has developed Process Control System Security Guidance (PCSSG) for the water sector and a supporting Cybersecurity use-case tool. The AWWA's cybersecurity resources are designed to provide actionable information for utility owner/operators based on their use of process control systems [10][11].

III. CYBERCRIME THREATS

In this review paper, the following constitute threat to IT systems, viz:

- Automated non-targeted viruses
- Script Kiddies
- Hackers
- Spammers
- Organized Crime
- The media
- Business competitors
- Insider employees
- Governments
- Data management

In order to efficiently manage data in various sections, data control is a crucial issue that has to be taken seriously. The goal of every cyber-attack attempt is to steal sensitive information or cause damage, so having control over data is an essential component to a successful defence. Also, numerous insider security breaches are the result of an employee downloading valuable data intellectual property (such as source code).

To protect sensitive data, an organization should protect and control data in various states such as:

- Data at-access. Sensitive information attempting to be accessed by an individual in an inappropriate role using a local workstation or laptop.
- Data in-motion. Sensitive information communicated over the network.
- Data at-rest**.** Sensitive information stored in repositories such as databases, fileservers or collaboration systems.

To achieve this, organizations must define policies to enforce control if inappropriate access or usage of the data is detected. Once a policy violation occurs, (such as attempting to access intellectual property, copying the information to a USB drive or attempting to email it), the solution should mitigate the compromise while generating an alert.

IV. IMPACT OF CYBERCRIME

The alarming increase in the rate of Cybercrime on the economy of nations and impact of cybercrime cannot be over-emphasized. This is because, it is a daily occurrence in

various geographical locations, and has become a normal routine. The impact is so severe that it affects sensitive aspects of a nation's economy such as bank, government, schools, research, military, corporate sector, and others. In this section, this paper will deal with attack issues and effective control measures

Area of Attacks

With mobile platforms being so popular and with its increase in data storage, the future is mostly likely going more crime disposed. There will be availability of tools focusing on these devices explicitly. This trend may also come to fruition for other platforms in the Internet of Things (IoT) space as these devices proliferate around us.

- Mobile payment systems
- Internet banking
- Mobile devices
- Company data base Networks [12].

How to Stay Secured

Security threats will always be available so long as crime rate increases geometrically and does not decrease. The tip is that everybody should be security conscious at all times and adopt some security measures proposed by computer security experts. The computers, networks and other devices are always at risk to cybercriminals. It is the end user's responsibility to always stay secured. Some proposed measures of security to be adopted include [6]:

- Install Operating System and Software Updates
- Use Malicious Software Protection (e.g. Anti-Virus)
- Turn On the computer's firewall
- Protect passwords
- Send passwords and restricted data securely
- Lock the computer screen
- Turn Off unnecessary Services
- Don not open email relays or unauthorized proxy servers
- Recycle phased out devices

Proposed Solutions

Some of the recommended practices (solutions) will reduce the level of risks and guide an unsuspecting user stay secured. They are either instructions to be adhered to, or actions that could be implemented [6]. These include:

- If it is not feasible to verify the legitimacy of a link or attachment, it is not advisable to click on it or open it. This includes links online, in texts, tiny Uniform Resource Locators (URLs), etc.
- Do not open, respond to or forward spam email.
- Be suspicious of any unsolicited phone call, email, Instant Messages (IM), text, facebook post, etc. asking you for your password, financial account information, social security number, Bank Verification Number (BVN), or other personal or private information, even if it seems to be from a company or person you are familiar with.
- Do not download unfamiliar software or plug-ins from the Internet.

Key Indicators for an Illigitimate e-mail

In order to escape the snare of cybercriminals, these are red-flags that must be looked out for, viz:

- If a user is asked for his/her password, money or financial account information.
- If it hints the user that there is a problem with his/her account and has a suggested link where he/she can go to fix things.
- If it is unsolicited/unexpected and has an attachment or link for the user to click.
- If an unsolicited mail is not addressed to a user personally
- The sender is not specified, is not a person the user knows or whose identity does not match the "from" address.
- If it has spelling or grammatical errors.
- If it has a link that doesn't seem match where the email says the link will take you to.

  To all of these, it is advisable not proceed with instructions or transactions. In this regard, stop and seek help from an expert in order not to be a victim

V. ANALYSIS OF CYBERCRIME ACTIVITIES

This section will analyze some of the trends in cyber crimes in order to expose its adverse effects with respect to various countries of the world.

Country Threat

Statistics is able to reveal to us the trend of cyber crime for various nations yearly. It also provides information on the economic impact of cybercrimes. This statistics is a guide and creates more awareness for affected countries and also for the other countries to be conscious of its spread.

Other countries which are not among the top 20s can at any time be even the top in Cybercrime, knowing that it is a global issue and effect is on the increase progressively. Table 1 show top 20 countries in cybercrime activities. Figure 1 shows yearly trend of cybercrime activities [13] [14].

TABLE 1. TOP 20 COUNTRIES FOR CYBERCRIME ACTIVITIES [15]

S/NO	Countries	Cybercrime act					
		Malicious computer act (%)	Malicious code rank	Spam zombies rank	Phishing web site rank	Bot rank	Attack origin rank
1	USA	23	1	3	1	2	1
2	China	9	2	4	6	1	2
3	Germany	6	12	2	2	4	4
4	Britain	5	4	10	5	9	3
5	Brazil	4	16	1	16	5	9
6	Spain	4	10	8	13	3	6
7	Italy	3	11	6	4	6	8
8	France	3	8	14	9	10	5
9	Turkey	3	15	5	24	8	12
10	Poland	3	23	9	8	7	17
11	India	3	3	11	22	20	19
12	Russia	2	18	7	7	17	14
13	Canada	2	5	40	3	14	10
14	South Korea	2	21	19	4	15	7
15	Taiwan	2	11	21	12	11	15
16	Japan	2	7	29	11	22	11
17	Mexico	2	6	18	31	21	16
18	Argentina	1	14	12	20	12	18
19	Australia	1	14	37	17	27	13
20	Israel	1	40	16	15	15	22

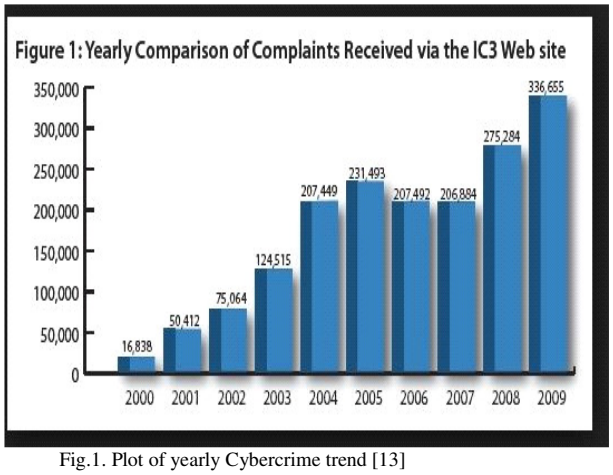


Fig.1. Plot of yearly Cybercrime trend [13]

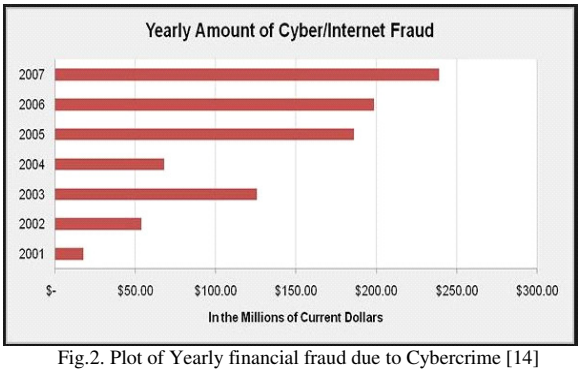


Fig.2. Plot of Yearly financial fraud due to Cybercrime [14]

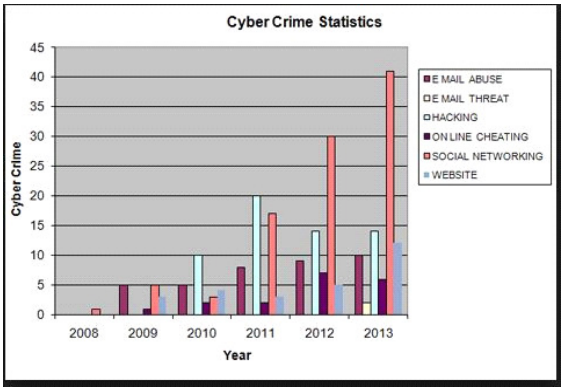


Fig.3. Plot of Cybercrime statistics [14]

India is one of the top countries for cybercrime activities. Its statistical analysis is shown in figure 4.

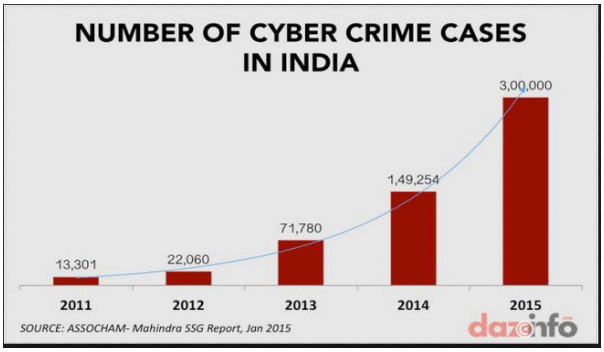


Fig. 4. Cybercrime analysis in India [14].

Why Attack

There are numerous reasons why cyber criminals engage in cyber attacks. Essentially, the same motive for performing any other type of crime is behind cybercrime activities. The primary motive is for financial gain. This definitely leads to damage and looses when implemented. Some other reasons for cybercrime attacks include:

- Political motivation- just to show they can, practice their skills

- Money- Any system that stores personal details is a source of potential revenue for a criminal!
- Hobby, ie using one's systems to attack others. For instance, the recent use of compromised corporate twitter accounts to spread viruses, fake news, and links to scam web pages.
- National security

Assessing Attacks

Table 1 illustrates some acts in cybercrime that were used in assessing the attacks of various countries for cybercrime activities. This paper used the 3-axis and the aAdvanced Persistent Threats (APTs) methods in assessing attacks.

For 3 axis, they are:

- Motivation
- Skill
- Funding

While for Advanced Persistent Threats (APTs). They include:

- Advanced attackers
- Usually highly skilled, motivated and funded
- Often governments

TABLE 2. ATTACK MATRIX

3axis	Script Kiddie	Motivated Individual	Hacker Collective	Organised Crime	APT (Government)
Motivation	Low	Medium to High	High	High	High
Skill	Low to Medium	High	High	High	High
Funding	Low	Low	Low	Medium	High
Number	High	Medium	Low	Medium	Very Low

VI. CONCLUSION

This work has discussed various cybersecurity issues and will summary with some of these key recommendations:

- Use good, cryptic passwords that can't be easily guessed and keep your passwords secret
- Make sure that the computer's operating system and applications are protected with all necessary security patches and updates.
- Make sure that the computer is protected with up-to-date antivirus and anti-spyware software
- Do not click on unknown or unsolicited links or attachments, and do not download unknown files or programs.
- Remember that information and passwords sent via standard, unencrypted wireless are especially easy for hackers to intercept.

It is worthy to note that the effects of a single, successful cyber attack can have far-reaching implications including financial losses, theft of intellectual property, and loss of consumer confidence and trust.

This paper concludes by re-stating that cybersecurity issue is every ones responsibility. Everybody must rise up and fight against it in every measure. In the future, this work will focus on identifying the trend of spread of cybersecurity in Africa with Nigeria as a case study. This will help stakeholders to identify the rate at which everyone may be exposed or vulnerable to this act at large.

ACKNOWLEDGEMENT

This research was supported by Tertiary Education Trust Fund (TETFund) through the Ken Saro-Wiwa, Polytechnic, Nigeria.

REFERENCES

[1] http://www.webopedia.com/TERM/C/cyber_crime.html [Accessed 10/09/15].
[2] http://www.spiegel.de/international/world/0,1518,713478-6,00.html [Accessed 10/09/15].
[3] http://www.dw-world.de/dw/article/0,,5645869,00.html [Accessed 10/09/15].
[4] http://www.forbes.com/sites/kurtmarko/2014/11/09/big-data-cyber-security/[Accessed , 10/09/15].
[5] http://its.ucsc.edu/security/top10.html [Accessed, 10/09/15].
[6] http://its.ucsc.edu/security/training/intro.html,[Accessed 10/09/15].
[7] https://ics-cert.us-cert.gov/Assessments[Accessed,10/09/15].
[8] http://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx,[Accessed 10/09/15].
[9] Cyber.SecurityFramework.org [Accessed 10/09/15].
[10] http://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx,[Accessed 10/09/15].
[11] https://www.us-cert.gov/ccubedvp [Accessed, 10/09/15].
[12] J. R.Vacca, Guide to Wireless Network Security, pp. 247-275, Springer Science+ Business Media, LLC, USA, 2006
[13] http://www.blog.thehigheredcio.com, [Accessed, 10/09/15].
[14] https://prezi.com/6xolemrzxbys/cybercrime,[Accessed 10/09/15].
[15] http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ [Accessed, 10/09/15].

A Datacentric Model for Mitigating Smartphone Vulnerabilities and Threats

C. C. Duru
Dept. of Electrical/Electronic Engineering
Imo State University, Nigeria
emisykes2000@yahoo.com

G. A. Chukwudebe and I. E. Achumba
Dept. of Electrical/Electronic Engineering
Federal University of Technology Owerri, Nigeria
ifeyinwaeucharia@yahoo.com

***Abstract*— In this paper, an investigation of the vulnerabilities of the Android OS platforms and reported attacks on it such as Inter Process Communication and Root related exploits are presented. An analysis of current mitigation methods against some known Smartphone exploits, the drawbacks and benefits are evaluated. From the study, a data-centric model for securing the Android operating system is developed. The proposed model will preserve privacy, integrity and more especially availability of native smartphone applications to only authorized parties. Integrating the proposed model with anti-malware software is recommended for future work to enhance the security of mobile devices even more. In this way, data stored in malware databases can be classified and changes made to data by mobile device users can be monitored to ensure unauthorized modification does not occur.**

Keywords*— Smartphone Operating Systems; Exploits; Malware; Inter-process communication; Phone threats and vulnerabilities.

I. INTRODUCTION

As the popularity of Smartphone usage worldwide is increasing because of its mobility, convenience and enormous processing power, cybercrimes targeted at Smartphones is also evolving at an alarming rate. Almost all, if not more malicious programs for desktop computers are also being launched for the Smartphone[1], [2] & [3]. The vulnerability level of the Smartphone is even higher than that of the personal computer because the Smartphone is an always-online device. Thus presently, cybercrime pose a huge threat to Smartphone owners who use it for mobile banking and other e-commerce activities.

A greater part of the developing world access the Internet via mobile phone's GSM facilities. Most of these individuals are totally unaware of the security vulnerability of these devices. Of recent, the Federal Government of Nigeria introduced the cashless policy encouraging the use of different e-channels such as Point of Sale services (POS) and Mobile banking for commercial transactions [4]. Consequently, it has become important to study the implications of the use of these security sensitive applications because the trend is just bound to continue with more supported applications to be introduced in the near future.

For this work, the mostly used Android operating system has been studied. Android owned by Google Inc., is a Linux-based, open-source operating system designed for use on cell phones, e-readers, tablet PCs, and other mobile devices. Android provides easy access to social networking sites like Facebook, Twitter, and YouTube. In addition it has smooth integration with Google products like Gmail, Google Maps, and Google Calendar. Android's facility in supporting screen-based interfaces has also made it the OS of choice for a number of blue-chip manufacturers such as Motorola, Samsung, HTC and Sony Ericsson. The expanding assortment of applications available on this platform suggests that Android-based phones will continue to be strong competitors in the smart-phone market.

Google allows software developers to create applications for Android mobile devices in Java and list them in Android Market, consequently there is a huge number of Android applications available to users. As at July 2013, the Google Play store had over one million Android applications ("apps") published, and over 50 billion applications downloaded [4]. An April–May 2013 survey of mobile application developers found that 71% of them create applications for Android. Another 2015 survey, found that 40% of full-time professional developers see Android as the "priority" target platform, which is more than iOS (37%) or other platforms [4] & [5].

However, Android applications may pose some privacy or security concerns because, unlike Apple, Google does not oversee or approve third-party Android apps before they go to market. For example, in a joint study by Duke University, Penn State University, and Intel, researchers studied a random selection of free Android applications and found that half of them sent private information including GPS coordinates and phone numbers to remote servers without seeking permission or notifying the owners [6] & [7].

In view of the increasing rate of cybercrime; some targeted at Smart phone users, the primary aim of this research is to analyze different exploits and security shortcomings of the

Android Operating System and develop a model for improved security.

II. AN OVERVIEW OF ANDROID

Android Operating System Architecture

The Android operating system has its software stack built on the Linux kernel. This kernel provides the following functionalities: Process management, Memory Management, Device Management (i.e device drivers for display, keypad, Bluetooth, Wi-Fi, camera, audio, power, etc) [6].

On top of the Linux Kernel there is a layer containing native C-library, SQL database engine, 2D and 3D graphic libraries, native web browser engine (WebKit) and Android runtime and virtual machine [6]. This layer enables the device to handle different types of data. All the libraries are written in C or C++language and are called through Java interface.

The next layer is the **Application Framework**, it provides many higher-level services or major APIs to applications in the form of Java classes. Application developers are allowed to make use of these services in their applications [6]. The Important blocks of Application framework are: Activity Manager, Content Providers, Telephony Manager and Location Manager.

The **Applications Layer** is the top layer in the Android architecture (i.e. on top of the Application framework layer). Some applications come preinstalled with every device, such as: SMS client app, Telephone, Web Browser, Calendar, Camera, Clock, Albums and Contact Manager. A developer can write his own application and can replace it with the existing application [6].

Security Features of Android OS

Over the years because Linux is open source many researchers have worked and improved its stability and resilience. As a result, several Linux security mechanisms are implemented on Android Trusted Computing Base (TCB) to ensure the security of users, user's data, applications, the device, and the network. To achieve the security of these components Android provides some of these key security features [6].

i. Security at the Operating System level through the Linux kernel

A user-based permissions model whereby each file and directories has three user based permissions: owner, group, and other users. This permission model ensures that proper security is maintained while accessing android files.

ii. Sandboxing Technology

Google has implemented the sandboxing technology for Android. A sandbox is a security mechanism for separating running programs and limiting the resources of the device to application. It is often used to execute untested code or programs from untrusted users and untrusted websites. By using sandboxing technique, limited access to device resources is given.

iii. Secure Inter-process Communication

The Android operating system assigns a unique user ID (UID) to each Android application and runs it as a separate process. But android operating system also provides new mechanism for IPC such as Binder, Services, Intents and Content Providers. All these mechanisms allow developers to verify the identity of an application and also use it to set the security policies [7].

iv. Application Signing

In order to install and run applications on Android OS they must be digitally signed. With this mechanism Android OS identifies the author of an application. This feature is also used to establishing trust relationship between applications. If an application is not signed properly then it cannot be installed on the emulator.

Some of the protected APIs in Android include: Camera functions, Location data (GPS), Bluetooth functions, Telephony functions, SMS/MMS functions and Network or data connections. These resources are accessed only through the operating system [9] & [10].

Despite all the above security mechanisms the cybercriminals are head in discovering vulnerabilities. In view of the fact that Google does not have a very good control over Android apps available to users, the next section will present a survey carried out on Android Exploits and vulnerabilities.

III. STUDY OF ANDROID EXPLOITS AND VULNERABILITIES

This research on Android Operating System is done from vulnerability perspective having in mind the different stakeholder's requirement for private data: *Confidentiality, Integrity and Availability*. These stakeholders includes: the manufacturer, service provider, application developer, and the user. Emphasis will be made on some important exploits/threats on the Android operating systems and current efforts made towards its mitigation will be evaluated in this section.

Exploits on the Android Smartphone operating system can be classified into two major categories thus: Inter Process Communication (IPC) and Root Exploits[11].

Inter-Process Communication

If communication between high priority applications is hijacked maliciously, the information being sent can be intercepted and re-coded with malicious code that can compromise the overall system. Android's IPC (Inter Process Communication) is useful for developers [12]. IPC exploits can be further divided into the following:

- Internet without permission related exploits
- Application interaction related exploits

Root Exploits

Root exploits take advantage of bugs (flaws) in the codes that make up the kernel to elevate their privileges to root. Once they get root privileges they can cause unimaginable damage to the Smartphone[11] & [12]. Exploits in this category are as follows:

- Linux kernel related exploits
- Exploits using device files
- Android software exploits

Nigerians Root their Android Smartphones for more application installation flexibility. This nullifies the original ROMs (with a locked bootloader so that no other ROM can be installed). With these original ROMs, there is no SU (Switch User) binary that allows the user to gain root rights. For the user to get access to functions that need root, or install a different ROM, the phone need to be rooted. Linux kernel related exploits.

Tables 1 and 2 show the different categories of Smartphone Exploits. The current mitigations against these exploits are analysed to show how effective each mitigation measure is. The shortcomings of these mitigation measures are the main drive towards the policies and models proposed for securing Smartphone Operating Systems and its unique applications.

Table 1.0:Inter-Process Communication.

		Instance	Mitigation	Benefits	Drawbacks
1	Internet without Permissions	none	Virtualization	High resilience and Privacy	Limited apps and tools available
2	Application Interaction	none	Dual Boot	Medium resilience and privacy	Complicated approach and low. Probability of introducing more attack vectors

Table 2.0: Root Exploits.

		Instance	Mitigation	Benefits	Drawbacks
1	Linux kernel related exploits	Exploid, Gingerbreak, Mempodroid, Wunderbar.	Kernel Hardening	High resilience and Privacy	Limited apps and tools available
2	Exploits using device files	Leviator, Exynos-Abuse	SE for Android	Very high resilience and low loss in Usability	Very complicated and can't prevent vulnerabilities allowed by the inbuilt security policies.
3	Android Software exploits	Psneuter/Killing in the NameOf, Rage Against the Cage, Zimperlich, ZergRush	**K**ernel Hardening	Less complication. Prevents the use of su binary in the Android kernel for altering UIDs an GIDs.	Not effective on Rage Against the Cage and Zimperlich.

Current Mitigation against IPC Exploits/Threats

From Table 1.0, the current mitigation against IPC (Inter Process Communication) Exploits are **Virtualization** and **Dual Boot.** They are discussed in further detail in the following section.

Virtualization – One goal of virtualization is the "Isolation of one application from another to enhance security of the environment". There are *In-App virtualization* and *System virtualization.*

Dual Boot - In dual boot, several independent Android operating systems are stored on the device. Those systems are called containers. When the device is started, the kernel is loaded and one of the different containers is booted. Containers come with pre-installed apps and are allotted limited system resources for operations. Most apps in a container do not have the same feel like normal Android applications.

Current Mitigation against Root Exploits/Threats

Kernel hardening and Security Enhancements (SE) for Android are some of the approaches developed lately to mitigate against Root exploits.

Kernel hardening- Hardening the Android system against root exploits has to be done on kernel layer as the attacks target the kernel. Kernel hardening prevents bugs in the Android software from being used for privilege escalation. With this mitigation technique, if a malicious application gains toot privilege, the damage that can be done with these privileges must be kept as low as possible [14].

SE for Android- Security Enhancements for Android (SE for Android) is a project and reference implementation by the National Security Agency (NSA) to increase security of the Android system. SE Linux implements a MAC system, each subject and object is assigned an SE Linux user ID, one or more roles and an access type [15]. This information helps in resource allocation based on security of the assigned ID and role.

IV. PROPOSED DATA-CENTRIC MODEL FOR IMPROVED ANDROID OPERATING SYSTEM SECURITY

The Smartphone and all its components needs to be secured from confidentiality, integrity, availability and privacy viewpoints, also the information flow on the device needs to be monitored. A Smartphone should have explicitly stated security requirements, which are statements about what and how it should function. These requirements would be a collection of well-defined, consistent, and implementable rules that are clearly and unambiguously expressed. From the investigation of exploits and current mitigations, a data-centric model is proposed based on the following assumptions and requirements:

a. The trusted computing base (which consists of the operating system, application framework and core device application) is a protected entity.
b. All the proposed security policies in this work are implemented and the manufacturer has correctly handled secure boot-loading and firmware security.
c. There is a secure storage on the device for storing property files for all objects loaded on the Smartphone.
d. The installer must read and display the privacy policy for any application prior to installation.
e. The user should have the choice of agreeing to a subset of privacy rights that the application is seeking.
f. An independent tamper-proof security monitor must be provided whose actions should be atomic.
g. Every access is made to be communicated down to the security monitor.
h. Data access process must adhere to the principle of fail-safe defaults; all accesses are denied unless approved on every access basis by the monitor.

This model builds upon the basic concept of Datacentric security system [8]. Rather than protecting a device hardware or platform as the case maybe, a data centric model focuses on the device data, it groups them into security levels, the higher the level the more stringent and strict the authentication becomes. To better understand this concept, in a platform centric security model, once a user gains access to the Smartphone, using a single user authentication factor like username and password, he automatically gains unrestricted access to the entire file system of the Smartphone, this is why user space hacks are very brutal and rampant.

The Datacentric model is described using a UML sequence diagram (Figure 1.0). It shows authentication requirements that must be met by a Smartphone user when accessing the three levels of data. For the proposed Datacentric model (Fig 1.0), a user gains access to the Smartphone by providing a username and password. This access only allows him to access **level 1** protected data like pictures, music libraries, contacts, saved documents, etc. If this same user tries to access **level 2** confidential data, then a second factor authentication such as a one-time token generated random set of numbers (to be provided by the hardware maker will be required). This token data expires after a length of time (session) and would require the user to provide another set of random token numbers if he wishes to continue access. Level 2 confidential data includes; financial data from Electronic wallet, location database from GPS, etc.

Level 3 data include; System configuration files, operating system files, Core Device application private files, installer permission files, etc. Modification access rights to this level of data should be denied for all mobile devices. This choice is made owing to the fact that most Denial-Of-Service attacks affecting a cellular network is done through Smartphones. Also, jailbreaking is possible by deceiving the Smartphone manufacturers' device specific data with false data and permanently placing the Smartphone in device update mode to be able to load an unsigned kernel. It is worthy to note that the

fake data must be uploaded to the manufactures database through the Smartphone as it is Smartphone dependent. By denying access to all level 3 data to mobile devices, these category of hacks can be drastically reduced.

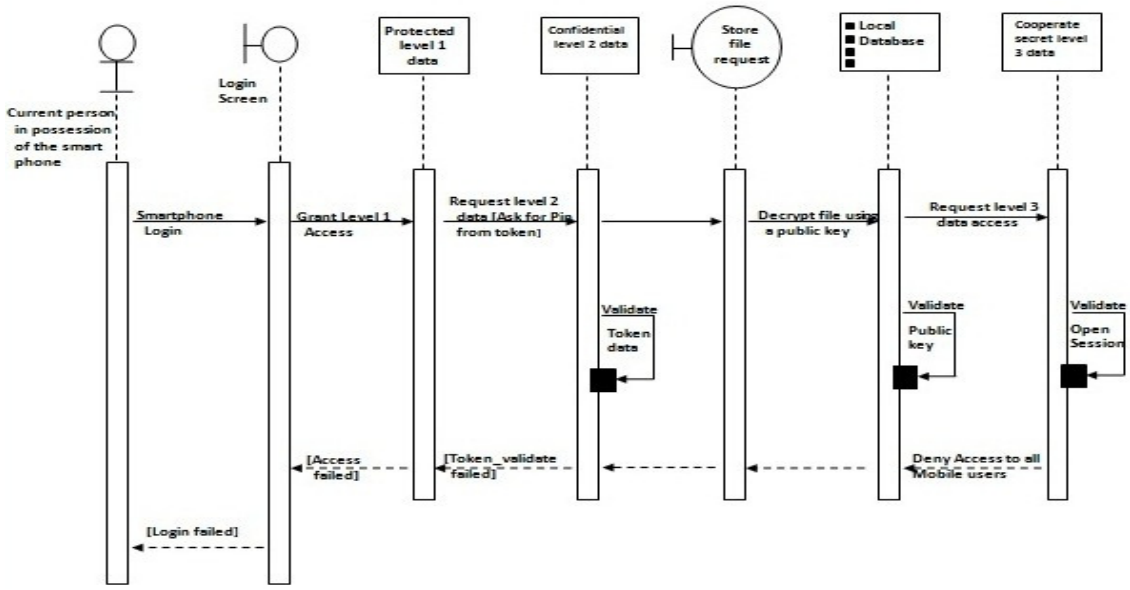


Figure 1.0: Datacentric Model for improved Smartphone Operating System security.

V. RESULTS AND DISCUSSION

The sequence diagram specifically denied all mobile devices access to Level 3 data to cub user space Smartphone hacks and botnet injections via a Smartphone. Since most of these attacks like jailbreaking and mobile botnets are launched from the device to the manufacturers Smartphone unique database.

All access to level 2 data is paired with a physical hardware like token. A token is a hardware device that generates a random set of numbers to be authenticated by a remote system to be able to allow access to any user. Access to level 2 data will not be allowed until token information is authenticated. Once access is gained, a session is created. The user gets logged out once this session elapses and must require another token data to be able to continue access. By creating a session, even if the system is compromised, it doesn't last for a long time before re-authentication is requested.

Level 1 data is made to require a onetime username and password from the user before access is granted.

Both Level 1 and Level 2 access control work in the Trusted Computing Base, which is part of the kernel and the regular Smartphone user cannot disable this feature. This way, malware activities and deception with false data is drastically reduced.

Dual boot and SE for Linux were employed to test the efficiency of the proposed model. These two mitigation techniques were carefully combined in CynogenMode 10.1 (a research based Android OS) to avoid making access to some important system resource more difficult to access than usual.Also, to prevent making some core system data and resource too open to the level of jeopardizing their confidentiality and integrity requirements.

To allow the device to run SELinux in enforcing mode, the following were implemented:

- Creation of labels for files specific for the test phone
- Relabeling of special files after their creation in the boot process
- Implementation of stated models and policies to allow different subjects access to several objects.

Figure 2.0 shows the effect is a major Root Exploit (Exynos-Abuse) on a custom Android OS with custom

ROM. Figure3.0 shows the effect of the same exploit after the proposed model and mitigation techniques has been implemented.

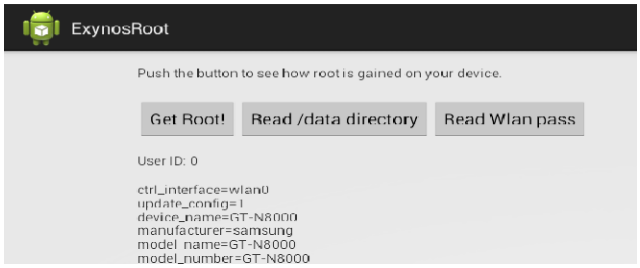


Figure 2.0: The Exploit App reading sensitive WLAN configuration files.

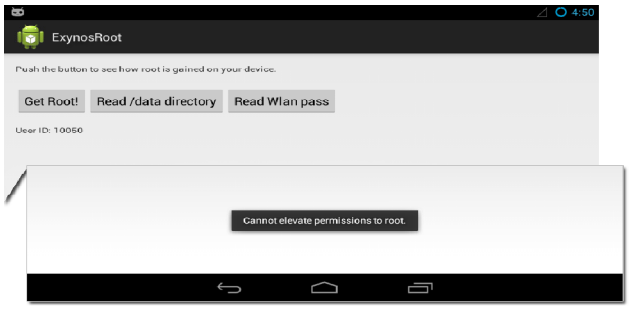


Figure 3.0: Malicious App denied privilege elevation.

Mitigation against Root Exploits will not only prevent kernel level related exploits but also prevent container escape exploits (a major flaw for Android container apps). Exynos-Abuse is a major Android vulnerability that is used in rooting most Android Smartphones. This compromises security and opens the whole system to new attacks.

VI. CONCLUSIONS AND RECOMMENDATIONS

This work has succeeded in analyzing different threats and exploits to the Android Smartphone Operating System and provided a model to circumvent them. The growing popularity and changing trends in Smartphone applications is specifically emphasized, necessitating the need for higher security requirements. How the Android Smartphone addresses security on their devices was discussed.

Datacentric model is proposed for securing different levels of private and confidential data available in the Smartphone. Grouping of these data into levels was done based on confidentiality, integrity and availability levels of these data in the Smartphone.

Further testing of the model can be done in other to expand on the scope of verification of the model. Also, integrating data-centric platform security with anti malware software can be considered as future work to enhance the security of mobile devices even more. In this way, data stored in malware databases can be classified and changes made to data by mobile device users can be monitored as well to ensure unauthorized modification does not occur.

REFERENCES

[1] Paul Ruggiero and Jon Foote, Cyber Threats to Mobile Phones https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

[2] The Shifting Threat Landscape, 2014 Global Threat Intelligence Report, (accessed September 2015), https://www.dimensiondata.com.

[3] 2015 Mobile threat Report, Published by the Pulse Secure Mobile Threat Center (MTC) ,www.pulsesecure.net

[4] Payments System Transformation: Cash-less Nigeria Implementation, (accessed September 2015), http://www.cenbank.org/cashless/

[5] Adam Koueider, Play Store hits 1 million apps, July 2013, http://www.androidauthority.com/play-store-1-million-tablets-70-million-248068/

[6] An Overview of Android Operating System and Its Security Features, Rajinder Singh, Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 2(Version 1), February 2014, pp.519-521

[7] Sumedh P. Ingale1, Sunil R. Gupta, Security in Android Based Smartphone, International Journal of Application or Innovation in Engineering & Management , Volume 3, Issue 3, March 2014.

[8] Monica Rozenfeld, Mobile Devices Remain Vulnerable to Attacks, (accessed September2015), http://theinstitute.ieee.org/technology-focus/technology-topic/mobile-devices-remain-vulnerable-to-attacks, March 2015

[9] Application Functionality on Smartphones. In: Proceedings of the 12th Workshop on Mobile Computing Systems and Applications (HotMobile).

[10] Au, K., Zhou, B., Huang, Z., Gill, P., Lie, D. (2011). Short Paper: A Look at SmartPhone Permission Models. In: Proceedings of the ACMWorkshop on Security and Privacy in Mobile Devices (SPSM).

[11] Bickford J., Hare R. O, Baliga A, Ganapathy V, and ftode L.I. (2010). Rootkits on smart phones: attacks, implications and opportunities, in Eleventh Workshop on Mobile Computing Systems & Applications, pp. 49.

[12] Bickford J., Hare R. O, Baliga A, Ganapathy V, and ftode L.I. Rootkits on smart phones: attacks, implications and opportunities, in Eleventh Workshop on Mobile Computing Systems & Applications. (2010).

[13] Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D. (2011). A Survey of Mobile Malware in the Wild. In: Proceedings of the ACM Workshop on Security and Privacy in Mobile Devices (SPSM).

[14] Barrera B.and Van Oorschot P.(2011, May). Secure Software Installation on Smartphones. Retrieved from Security Privacy, IEEE, vol. 9, pp. 42.

[15] Shabtai, A., Fledel, Y., Elovici, Y. (May/June 2010). Securing Android-Powered Mobile Devices Using SELinux. IEEE Security and Privacy Magazine.

Plausible Approach to Mitigate Security Challenges in Cloud Computing

Agbaeze E.[1], Nwokorie E. C.[2], Uzoh, O. F.[3]
Department of Computer Science
Federal University of Technology, Owerri, Nigeria
ejem.agbaeze@futo.edu.ng[1], euphemia.nwokorie@futo.edu.ng[2], contactofuzoh@gmail.com[3]

***Abstract*—Cloud Computing is a flexible, cost-effective and proven delivery platform for providing business or consumer Information Technology (IT) services over the Internet. However, Cloud Computing is growing rapidly and bringing up numerous security challenges for today's world. Some of the security challenges include, but not limited to, security and confidentiality of user data in terms of its location, relocation, availability etc. There are various opinions on the security of cloud computing which deal with the advantages and disadvantages of it. This paper presents plausible approaches to these security challenges in cloud computing using an extensive secondary research methodology. Information was collected and analyzed from acknowledged texts, standard documents, industry periodicals, white papers and analysts' report. The approaches tackle the problem of protecting data-in motion, in process, and at rest. They also deal with securing a cloud platform, extending trust across federated clouds, choosing the right service provider, etc. It was found out that using these approaches counteract the security challenges in cloud computing to a great extent.**

Keywords— Cloud Computing; Security Challenges; Internet; encryption; Data protection

I. INTRODUCTION

The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

According to Rosado, et al [1] and Zhao, et al [2], Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing.

Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters. As Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing [1]. That uncertainty has consistently led information executives to state that security is their number one concern with cloud computing [13].

II. RELATED LITERATURE

Cloud Computing

Cloud computing is the latest extension of an evolution in distributed computing that takes advantage of technology advances. The cloud's roots date back to early mainframe processing, when users connected to a shared computing resource through terminals to solve their computing needs. The advent of faster and cheaper microprocessors, random access memory (RAM) and storage brought computing into the client-server model, which grouped sets of users into networks sharing computing power on decentralized commodity servers. These networks interconnected to form the internet as bandwidth became more ubiquitous, faster, and less costly. Information Technology (IT) departments did typically provision their datacenters in house, and hence are protected inside a firewall. Eventually, enterprises took advantage of higher throughputs to reexamine the need for monolithic onsite datacenters. Accessing servers virtually through a browser window present substantial advantages in software and hardware maintenance. Software vendors began capitalizing on the concept that a scaled datacenter could also deliver remote content to customers almost immediately at a reduced cost, giving rise to on-demand Software-as-as-Service (SaaS). Today's mature virtualization platforms enable contemporary cloud computing: a new model of rapid, on-demand, low-cost, al-a-carte computing. Like its predecessors, present-day cloud computing features a multitude of users connected to remote computing resources over the Internet. Cloud computing delivers software and services over networked connections, relying on a steady flow of throughput to and from the virtualized datacenter in order to maintain high service levels. Kresimir and Zeljko [4] discussed high level security concerns in the cloud computing model such as data integrity, payment and privacy of sensitive information. Subashini and Kavitha [5] discuss the security challenges of

the cloud service delivery model, focusing on the SaaS model. A recent survey by Cloud Security Alliance (CSA) and IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security is needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing growth. According to Kevin et al [6], there are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. The main issues they considered include storage security, middleware security, data security, network security and application security. The main goal is to securely store and manage data that is not controlled by the owner of the data. Several studies have been carried out on security issues in cloud computing but this work presents a detailed survey of the plausible approaches to counteract cloud computing security issues and challenges. Fig. 1 below depicts cloud computing components.

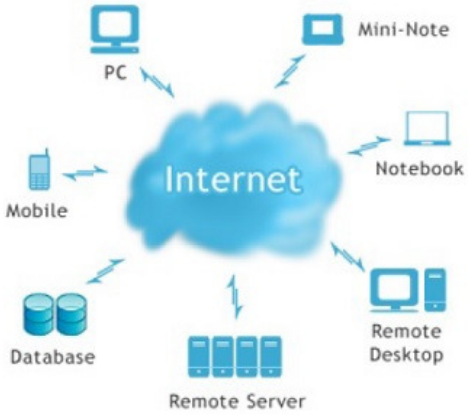


Fig. 1: Cloud Computing [7].

Types of Cloud Computing

Private Cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific private cloud [8].

Public Cloud

A public cloud is built over the Internet, which can be accessed by any user who has paid for the service [9]. Public clouds are owned by service providers and are accessed by subscription. Many companies have built public clouds, namely Google App Engine, Amazon AWS, Microsoft Azure, IBM Blue Cloud, and Sales Force Force.com. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

Hybrid Cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems.

A hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets, for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter [8]. Fig. 2 shows the different types of clouds and how they can be deployed.

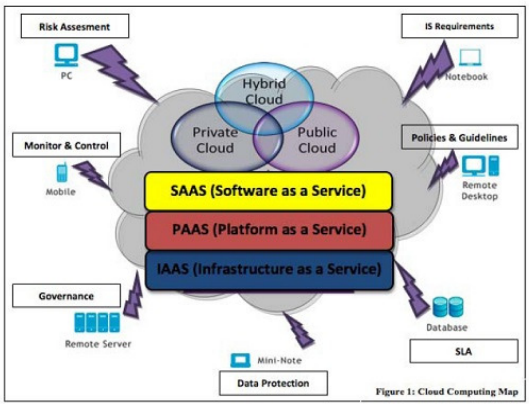


Fig. 2: Cloud Deployment Model [10].

Services of Cloud Computing

There are three service models for cloud computing [11] which enables how computing resources or power are being provisioned and consumed as a utility based on the earlier outlined characteristics. The service models are:

*Software as a Service (SaaS)***:** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Examples of SaaS are customer relationship management (CRM), human resources (HR) or Accounting applications.

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations, e.g. Microsoft Azure, Sales Force and Amazon Web Service.

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host, firewalls). Examples of IaaS providers are Rackspace Hosting, Network Solution and Go-daddy Hosting. Fig. 3 below shows how the various cloud computing models and services compare in terms of their levels of abstraction, control and governance capabilities, flexibility of purpose and economies of scale.

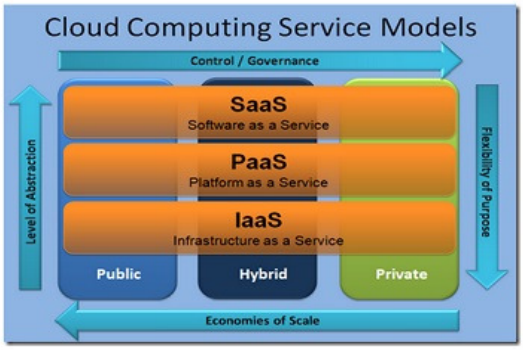


Fig. 3: Cloud computing service models [11].

III. SECURITY CHALLENGES IN CLOUD COMPUTING

In traditional data centers, IT managers put procedures and controls in place to build a hardened perimeter around the infrastructure and data they want to secure. This configuration is relatively easy to manage, since organizations have control of their servers' location and utilize the physical hardware entirely for themselves. In the private and public cloud, however, perimeter boundaries blur and control over security diminishes as applications move dynamically and organizations share the same remotely located physical hardware with strangers [12].

Multi-Tenancy

Cloud computing users share physical resources with others through common software virtualization layers. These shared environments introduce unique risks into a user's resource stack. For example, the cloud consumer is completely unaware of a neighbor's identity, security profile or intentions. The virtual machine running next to the consumer's environment could be malicious, looking to attack the other hypervisor tenants or sniff communications moving throughout the system. Because the cloud consumer's data sits on common storage hardware, it could become compromised through lax access management or malicious attack.

Multi-Location of the Private Data

It is rather dangerous, if the business stores its private data in the third party's device. In this sense, the businesses' private data are stored in an external computer, and in an external facility. Then, many things can go wrong. Firstly, the cloud service provider may go out of business. Secondly, the cloud service provider may decide to hold the data as hostage if there is a dispute. Furthermore, it is important for a company to know in which country its data will be hosted [13].

Cookie Poisoning

It involves changing or modifying the contents of a cookie to have unauthorized access to an application or to a webpage. Cookies basically contain the user's identity related credentials and once these cookies are accessible, the content of these cookies can be forged to impersonate an authorized user. Fig. 4 illustrates this kind of attack.

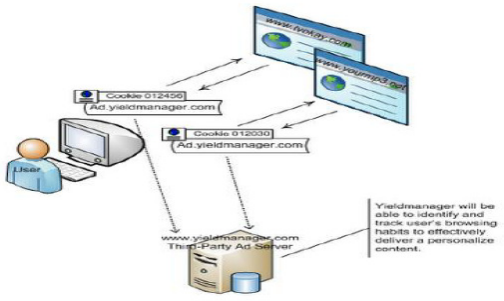


Fig. 4: Cookie poisoning [14].

Data Privacy

The public nature of cloud computing has significant implications on data privacy and confidentiality. Cloud data is often stored in plain text, and few companies have an absolute understanding of the sensitivity levels their data stores hold. Data breaches are embarrassing and costly. In fact, a recent report by the Cloud Security Alliance lists data loss and leakage as one of top security concerns in the cloud. Recent laws, regulations and compliance frameworks compound the risks; offending companies can be held responsible for the loss of sensitive data and may face heavy fines over data breaches. Business impact aside, loose data security practices also cause harm on a personal level. Lost or stolen medical records, credit card numbers or bank information may cause emotional and financial ruin, the repercussions of which could take years to repair. Sensitive data stored within cloud environments must be safeguarded to protect its owners and subjects alike.

IV. APPROACHES TO MITIGATE SECURITY CHALLENGES IN THE CLOUD

A. Protect Data- In Motion, In Process, and At Rest

Encryption is an effective, well-established way to protect sensitive data. It is widely regarded as best practice to use encryption on any sensitive data that might be at risk of loss of physical control, for example, many companies have policies that data on laptops must be encrypted. It is critically important in cloud environments, especially in hybrid or public cloud models, where data may move outside the traditional IT environment, but also in internal private clouds, where data can be exposed on shared compute resources.

Certain industries, such as healthcare and financial services, require organizations to meet certain regulations and standards for the way they protect data. Increasingly, these and other regulations are encouraging, and specifying, encryption in certain usage scenarios, including cloud computing. The penalties for noncompliance are stiffer than ever. However, data encryption is often not used broadly due to the performance impact. With user expectations for the cloud to provide instant access to resources, it can be a tough sell as an IT manager to justify the trade-off in performance with the requirement for secure data.

When to Encrypt Data

Typically data do not stay in one place in a network, and this is especially true of data in the cloud. Encrypt data wherever it is in the cloud: at rest, in process, or in motion.

Data in Motion

- Data in flight over networks (Internet, e-commerce, mobile devices, automated teller machines, and so on).
- Data that use protocols such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Internet Protocol Security (IPsec), Hypertext Transfer Protocol Secure (HTTPS), File Transfer Protocol (FTP), and Secure Shell (SSH).

Data in Process

- Transactional data in real time or sensitive personal financial data stored as encrypted fields, records, rows, or column data in a database.

Data at Rest

- Files on computers, servers, and removable media.
- Data stored using full disk encryption (FDE) and application-level models.

B. Secure the Platform

Rootkit and other low-level malware attacks are increasing. They are difficult to detect with traditional antivirus products and use various methods to remain undetected. Rootkit attacks infect system components such as hypervisors, basic input/output system (BIOS), and operating systems, and can hide malware that operates in the background and spreads throughout a cloud environment, causing increasing damage over time.

With sophisticated threats and malware an ongoing and growing threat, securing both client and server platforms provides an additional enforcement point that builds trust between servers and between servers and clients.

The best way to enable a trusted foundation is to start with a hardware-based root of trust and extend the chain of trust through the critical controlling software layers, including firmware, BIOS, and hypervisor virtualization layers. A root of trust hardens the platform against attack and is extremely difficult to defeat or subvert. It substantially reduces the security risks of using remote or virtualized infrastructure and enables a more secure platform for adding tenants and workloads. Essentially one builds protection into one's hardware to better protect one's software. A root of trust helps ensure system integrity within each system. Integrity checking is considered a key capability for software, platform and infrastructure security [15].

C. Extend Trust across Federated Clouds

As cloud computing evolves, the vision of federated cloud relationships—across which users, data, and services can move easily within and across several cloud infrastructures—adds another layer of complexity to the security equation. Trusted access to the cloud and across clouds are based on managing identities and access-management policies, including standards-based single sign-on (SSO), strong authentication, account provisioning, application programme interface (API) security, and audit capabilities. For cloud security, simple user names and passwords are no longer adequate because they can be easily compromised. Secure SSO based on strong second-factor authentication is essential in federated cloud environments, where the cloud service provider is relying on the authentication performed by the enterprise to grant access to applications.

D. Choose the Right Cloud Service Provider

Choosing a cloud service provider is complicated on many levels—from the cloud delivery model and architecture to

specific applications. To complicate matters, some companies offer not only software, but also hardware and services. Nevertheless, one must be vigilant about making sure the security one needs to protect one's data and platform are part of the offering. At the highest level, one needs to know if the cloud provider can provide evidence of data and platform protection for the services they provide. Once the criteria have been met, one can then establish measurable, enforceable service level agreements (SLAs) to provide ongoing verification.

A list of additional security considerations to think about when choosing a cloud service provider is shown in Table 1 [16].

Table 1: Cloud service security considerations.

.Security Selection Criteria	Considerations
Data centre risk management and security practices	• What are the patch management policies and procedures? • How does technology, architecture and infrastructure impact the cloud service provider's ability to meet SLAs?
Hardware-based security	• Can the cloud service provider offer trusted pools for your most sensitive workloads? • Is encryption a software-only solution?
Technology segmentation	• How are systems, data, networks, management, provisioning and personnel segmented? • Are the controls segregating each layer of the infrastructure properly integrated so they do not interfere with each other? For example, investigate whether the storage compartmentalization can easily be bypassed by management tools or poor key management. • What cloud access and identity protocols are used?
Identity and access management	• How is identity managed and authenticated? • Is two-factor authentication utilized?
Attack response and recovery	• How are attacks monitored and documented? • How quickly can the cloud service provider respond? • What recovery methods are used?
System availability and performance	• How does the cloud service provider handle resource democratization and dynamism to best predict proper levels of system availability and performance through normal business fluctuations? • How does the cloud service provider measure performance?
Vendor financial stability	• Is the cloud service provider financially stable? • How long has the vendor been in business? What is their current financial standing?
Product long-term strategy	•What is the vision for the service provider's cloud offering? • Does the cloud service provider have a product roadmap for their offering? Cloud service providers seeking to provide mission-critical services should embrace the ISO/IEC 27001 standard for information security management systems. If the provider has not achieved ISO/IEC 27001 certification, they should demonstrate alignment with ISO 27002 practices.
Limits of responsibility	• What is the limit of the cloud service provider's responsibility for security? • What security responsibilities are expected of the enterprise? • What is the legal accountability in a breach?
Compliance capabilities	• Does the cloud service provider have the ability to comply with regulatory requirements that you face? • Is the cloud service provider able to provide you with full visibility into compliance-related activities? • Can you perform your own audit?

V. CONCLUSION

Without doubt, putting data and running software on someone else's hard disk using someone else's CPU appears daunting to many. This paper has looked at the security challenges facing cloud computing and plausible approaches to counteract them. Security issues in resource multi-tenancy, private data multi-location, cookie poisoning and privacy of data has been discussed. With various encryption techniques, platform security measures, extending trust across federated clouds and choosing the right cloud service provider these problems are grossly minimized. As no computer system can provide absolute security under all conditions more research is needed to investigate ways of curbing these security threats inherent in cloud computing.

REFERENCES

[1] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469–487

[2] Zha G., Liu J., Tang Y., Sun W., Zhang F., Ye X., Tang N., (2009), Cloud Computing: A statistics aspect of users, First International conference on cloud computing (Cloudcom), Beijing, China, Springer Berlin, Heidelberg, pp 347-358

[3] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA

[4] Kresimir P. and Zeljko H. "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.

[5] Subashini S. and Kavitha V. (2010) "A survey on security issues in service delivery models of cloud computing." J Network Comput Appldoi:10.1016/j.jnca.2010.07.006, Jul., 2010.

[6] Kevin Hamlen, Murat Kuntarciogh, Latifur Khan, Bhavani Thuraisingham (2010),"Security Issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2),39-51, April-June. University of Texas at Dallas,USA.

[7] Srinivasa Rao V., Nageswara Rao N. K., E Kusuma Kumari," Cloud Computing: An Overview", Journal of Theoretical and Applied Information Technology © 2005 - 2009 www.jatit.org

[8] Arnold S. (2009, Jul.). "Cloud computing and the issue of privacy" *KM World*, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[9] Kuyoro S. O., Ibikunle F. & Awodele O., "Cloud computing security issues and challenges", International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[10] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." *Platform Computing*, pp6, 2010.

[11] Toyin Ogunmefun's Space (2011)," Effective Data Protection for Cloud Computing and its Relevance in the Nigeria Economy". Available: http://toyinogunmefun.wordpress.com [June 18, 2015]

[12] Drue Reeves (2009),"Cloud Computing:Transforming IT", December 3rd,2009. Available at: http://net.educause.edu/ir/library/pdf/ECRC0901.pdf [June 18, 2015]

[13] Vahid Ashktorab, Seyed Reza Taghizadeh," Security Threats and Countermeasures in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM) Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com,volume 1, Issue 2, October 2012

[14] Albert B Jeng, Chien Chen Tseng, Der-Feng Tseng, Jiunn-Chin Wang, "A Study of CAPTCHA and its Application to User Authentication", Proc. Of 2nd Intl. Conference on Computational Collective Intelligence: Technologies and Applications, 2010.

[15] IntelITCenter(2012),"cloud computing security planning guide", available from Intel.com/ITCENTER [Accessed 26th September, 2013]

[16] Adapted and expanded from *How to Choose a Cloud Computing Vendor*. Inc.com (November 29, 2010). inc.com/guides/2010/11/how-to-choose-a-cloud-computing-vendor.html

Social Media Applications: Are the youth Addicted?

Dr. Shivani Arora
ShaheedBhagat Singh College, University of Delhi, New Delhi, India

Dr. Daniel Okunbor
Fayetteville State University, Fayetteville, North Carolina, USA, Visiting Fulbright Scholar at the University of Abuja, Abuja, Nigeria

***Abstract*--Social media (SM) has seen an exponential growth since its inception on the web, making it an interesting and unexplored area of research. The positives and the novelty of the SM sites have resulted in its integration to our daily lives. Unfortunately, there are repercussions to its adoption, including but not limited to uncontrollable daily dedicated hours; loneliness creating the need to use it and causing more loneliness as the end product; addiction arising out of pleasure, etc. This paper aims to study the SM usage pattern of a sample of students from United States and India, and gauge the pattern and relate the same as symptoms of addiction.**

***Keywords*--Social media, Addiction, Usage, Facebook**

I. INTRODUCTION

This paper involves the study of social media sites (SMS) in the context of two countries (India and the United States of America) in two different continents (Western Asia and North America). The authors believed that comparing the behaviors of users of SMS from two countries will shed some lights on this important subject and spur further research. This research is in two parts, namely, the impact analysis of SMS in general and a more focused impact analysis on Facebook. The first part will be represented in this paper.

The pervasiveness of the social media (SM) into mainstream culture and its integration into every life of people in all nations of the world has made it an active research. The advent of the Internet has brought about the ubiquitous nature of SM. Research in social media, which is often called social media analysis, has its root in social sciences, particularly, sociology, psychology and anthropology. While there are many variants in the definition of social media analysis in the literature, we would adopt one that defines it as the mapping and measuring of relationships and flows between people, groups, organizations, computers, and other connected information/knowledge entities. Social media analysis represents a complex mathematical modeling of connectivity and relationships. Our research will be focusing on the social media occurring on the Internet. Although, this research utilizes some aspects of social media analysis, relating to the behavioral analysis of social media users, the bulk of the analysis is on the usage of SM websites. We investigate the manner in which users access SM sites, the impact analysis will include an examination of the addictive nature of the SM sites.

This paper is organized as follows: first, we will provide a historical background of the five SMS addressed in this paper. Second, we will discuss the current research on SMS and their impact analysis. Third, we would address the methodology used in this research along with the research questions. Fourth, the results and findings will be presented. We would discuss impact analysis on the basis on addiction. Lastly, we would be followed by concluding remarks.

II. HISTORICAL PERSPECTIVE OF SM SITES

Social media sites, social media application and social media service are used interchangeably in the literature. Although, social media is used in many other contexts, it is becoming increasingly synonymous with building relationships via the World Wide Web. Following the argument presented in [1], we would prefer the use the term “social media,” which they claimed connotes “looking to meet new people or initiating relationship.” According to them, many large SMS users do not necessarily engage in “networking.” They define SMS as web-based services that allow individual to construct personal profiles for public or semi-public consumption; articulate “friends” to share connections with; and surf information of other notable users within the confines of the systems.

III. REVIEW OF LITERATURE

In this section, the review of studies related to social media and various aspects related to it, have been considered. The review of empirical studies has been undertaken to observe which areas have been explored and which need further investigation, in order to formulate the objectives and undertake productive research. The review has also been undertaken to earmark the problem areas related to social

media. Besides, these studies would provide an insight into the various efforts directed towards better understanding of the complexities of the social media.

The recent report by Ofcom, an independent regulator and competition authority for the United Kingdom communication industries described their qualitative and quantitative analysis research to gauge social media sites in the wider media literacy, online and communication contexts; to profile peoples' use and understanding of networking sites; and to understand the associated privacy and safety concerns of social media sites [2]. According to Ofcom, social media sites are most popular with teenagers and young adults just over one fifth (22%) of adult internet users aged 16+ and almost half (49%) of children aged 8-17 internet users. It was also reported that some under-13s are by-passing the age restrictions on social media site with 27% of 8-11 year olds who are aware of social media sites say that they have a profile on a site. The same report indicated that the average adult social mediaer has profiles on 1.6 sites, and most users check their profile at least every other day.

The EDUCAUSE Center for Analysis and Research (ECAR) in its Research Study on Social media Sites supported the findings by Ofcom as indicated above (ECAR 2008). According to ECAR, the extent of social media sites use has increased dramatically with considerably 95.1% of users aged 18 and 19 years using social media as opposed to 37% users aged 30 and older. Other findings of ECAR included: Facebook has the most users with 89.3%; majority of the users (55.8%) spend 5 hours or less on social media sites and 26.9% between 6 and 10 hours; half of the users utilize social media sites to communicate with classmates about course-related topics; fewer than one-third of users are very concerned or extremely concerned about the misuse of their information, security problems, cyberbullying or cyberstalking, or leaving a history that could cause them problems.

The study "Facebook Addiction:Factors Influencing an Individuals Addiction", in [3] suggests that though internet addiction has been studied but social media addiction has not been researched. The study investigates how factors such as personality, gender, procrastination, boredom and ones values may affect amount of time they spend on facebook. It further concludes that they are either overly possessive about the usage thereof or not. The research conducted was a combination of qualitative and quantitative techniques, using scholarly articles that focused on personality types and Internet addiction. Based on the results from the qualitative study, quantitative survey instrument was devised, which includes likert-style statements that test personality type, values, boredom and procrastination.

The article titled, "3 Reasons You Should Quit Social Media in 2013" discusses the UK study which proves that over 50% of social media users evaluated their participation in Social media websites as having a negative effect on their lives. Comparing themselves to others (family, friends, peers) was a blow to their self-esteem. And stalking by ex or his/her husband/wife is considered worse.

Psychologist Dr.MichaelFenichel describes FAD as a situation in which Facebook usage "overtakes" daily activities like waking up, getting dressed, using telephone or email checking. According to Joanna Lipari, a clinical psychologist at University of California, LA, discusses some signs of Facebook addiction as:

i) Losing sleep over FB. Staying logged in throughout the night and eventually getting too tired for the next day;
ii) As a bench mark spending one hour or more on FB is too much;
iii) Being obsessed with exes who reconnect on FB;
iv) Ignoring work for FB;
v) The thought of getting off FB leaving the user in cold sweat;

In article [4] "Status update: Facebook Addiction Disorder", opines that the user is suffering from FAD, a disease referred to by psychologists, if he/she has more online friends than real life friendships. Also, if the user checks the FB more than 5 times a day (spending hours updating the status) or if checking the facebook account is the first thing that he/she does in the morning.

The study, "Facebook a more powerful addiction than alcohol [5], reveals that the pull of checking one's facebook page can be more powerful than addiction to alcohol or cigarettes. As in 2012, scientists claim that 350 million people suffer from this condition.

The reason cited by FB addicts have been:

i) The urge of human interaction and the ease of it through FB/twitter;
ii) Getting a message on FB/twitter is exciting since it feels like someone is interested in "me".

To check this urge to be on FB page, a web application can be used, which shuts off the computer after the user has spent a pre-determined amount of time. (NEwsChannel9WSYR, 2012, "Study: Facebook a more powerful addiction than alcohol, cigarettes")

A medical study titled , "Microstructure Abnormalities in Adolescents with Internet Addiction Disorder" by Kai Yuan, Wei Qin, Guihong Wang, Xuejuan Yang, Peng Liu, Jixin Liu, Jinbo Sun, Karen M. von Deneen, JieTian reveals that long-term internet addiction would result in brain structural

alterations, which probably contributed to chronic dysfunction in subjects with IAD. The study sheds further light on the potential brain effects of IAD. The areas that were affected in the people who were diagnosed with IAD are thought to govern emotional processing, executive thinking skills and attention, and cognitive control. What's more, the brain changes found in this study are thought to be similar to those involved in other kinds of addictions like alcohol and drugs.

A study by University of Chicago Booth School of Business states the desire to frequently check your social media sites, such as Facebook and Twitter, among other social media sites, can lead to a stronger addiction than those who are addicted to alcohol or cigarettes.

The study was done by giving 205 adults, ages 18-85, Blackberries and sending them tweets seven times over 14 hours a day for seven days. The study quotes that "Texting and checking Facebook and Twitter come in just below sex and sleep on impossible to resist urges,

Ellison, N.B., Steinfield, C., & Lampe, C in their study "The Benefits of FB "friends": Social Capital and college students use of online social media sites" provide the scale items to judge the addiction of Social media, viz.,

i. Facebook is a part of my everyday activity
ii. I am proud to tell people, I am on Facebook
iii. FB has become a part of my daily routine.
iv. I feel out of touch when I haven't logged onto FB for a while.
v. I feel I am a part of FB community.
vi. I would be sorry if FB shut down.
vii. Approximately how many FB friends do you have?
viii. In the past week, on average, how much time Per Day have you spent actively using FB?

Foremski Tom in his article, "Facebook 'Likes' can reveal your sexuality, ethnicity, politics and your parent's divorce", discusses the study which included researchers from Cambridge's Psychometric Centre and Microsoft Research Cambridge Researchers. The researchers analyzed a dataset of over 58,000 US facebook users and developed a model that could predict whether a man was homosexual 88% of the time, and 75% of the time for women; ethnic origin (95%), gender (93%), religion (82%), political affiliation (85%), if they use addictive substances (75%) and relationship status (67%).

Also, Frank Agyemang, in his article, "Infected with Facebook Addiction Disorder?", refers to a study by Cambridge University suggests that contrary to the belief, it aids in people to be more sociable giving people more choice as to how and with whom they conduct their relationship.

Haisha Lisa in her article "Is your Facebook Addiction a sign of loneliness? discusses a unique aspect of Facebook Addiction which differentiates it from the other types if addictions. Unlike addiction to drugs, alcoholism, and sex, where the guilt is a major factor, the Facebook addict feels that they have reasons to be addicted, since they claim to be doing business. Some are self-employed professionals looking for clients, some are job seekers trying to network for a new job, and some are corporate employees trying to extending their company's message. Their time on Facebook is actually escapism disguised as working. Also, most of the people are addicted to their past-reconnecting with their friends, old classmates, former lovers, etc.

In another research on social media [6], focused on students' performance in an online course offered at the National Cheng-Chi University in Taiwan. They found that social media that serve advising roles have positive impact on students' performance and that networks that are adversarial have negative impact.

The review of the available literature reveals that studies have included various aspects of Social media Addiction (with special reference to Facebook) including-its symptoms; positives of Usage, also its negatives; implications and impact of Social media Addiction. The studies listed here, also included are the professional opinions of the psychiatrists and psychologists regarding the influx of SM cases especially FAD cases.

IV. RESEARCH METHODOLOGY

Purpose of the Study

The research study will investigate the daily usage of social media and how people interact with social media sites on a daily basis. The focus will be on how often people use this tool to converse with or keep current with their friend's social or personal lives. The significance of the study is to examine the impact of social media has on its users and the merits and demerits of social media, particularly, the aspect that pertains to dysfunctional behaviors. Research questions include:

1. What is the threshold for social media usage to be classified as dysfunctional, such as causing addiction disorder?
2. What are the differences in social media usage in geographical context? In this case, we would compare usage in Western Asia (India), North America (United States).

The research design that will be used in this study is based on the mixed research model. This model is chosen in order to achieve full potential, including benefits of mixed methodology and to provide a comprehensive

investigation of the research questions. These benefits include: 1) the ability to engage in both inductive and deductive reasoning, 2) allows qualitative approach to complement the results of the quantitative approach and vice-versa, 3) maximizes the advantages of quantitative and qualitative methodologies and minimizes the demerits, 4) applies both objective and subjective points of view, 5) allows researchers to choose explanations that best produce desired outcomes, 6) researchers' values play a large role in the interpretation of results and 7) mixed model is pragmatic and more realistic and serves as the middle ground for the positivist and constructivist theories [7]. These benefits of mixed model are of great importance to this study. The open-ended questions are intended to complement the closed-ended questions and vice-versa to help produce stronger analyses and desired outcomes.

The qualitative approach of this research study will utilize content analysis based on open-ended questions of the survey questionnaire. Content analysis is chosen for this research because it is well suited to the study of the methodical and description of the content of recorded human communication. Babbie [8] defines content analysis as "any technique for making inferences by objectively and systematically identifying specified characteristics of messages."

Judgment sampling was used to study 151 Under-graduate students from Delhi University and 120 from Fayetteville State University, Fayetteville, North Carolina, USA. The questionnaire was sent to 1000 respondents but as a limitation, only 151 and 120 respondents respectively filled it up. The quantitative portion of this research study will involve a cross-sectional approach for data collection. This data analysis will utilize statistical package provided by Google Docs. The percentage of the total agreement has been taken by adding the strongly agree and agree percentages, and same for disagreement level. The simplicity of the method, combined with the qualitative discussions, would give us the real crux of the comparison. To keep it simple, the agreement level of the two set of respondents is compared and conclusions drawn accordingly. For this study, we will be using Google Forms' spreadsheet that keeps the responses.

V. FINDINGS AND ANALYSIS

The purview of the paper is to study the various aspects of Social media affecting the respondents from the United States (U would be prefixed with the code) and India(I, would be prefixed). The Coding for various aspects is

1. Tsp Time spent on SMS
2. FTM First thing in the morning
3. LTN Last thing at Night

4 A.SWL Social media is the way of life.

4 B. SMA Social media is Addictive

5 A. HPH spending too much time online is Harmful to Physical Health

5 B. HMH spending too much time online is Harmful to Mental Health

Symptom I

The Time Spent (TSp)

One of the most important symptoms of Social media Addiction is the amount of time spent online. Psychologists suggest that if more than an hour is being spent on SM websites, the chances of being affected are high.

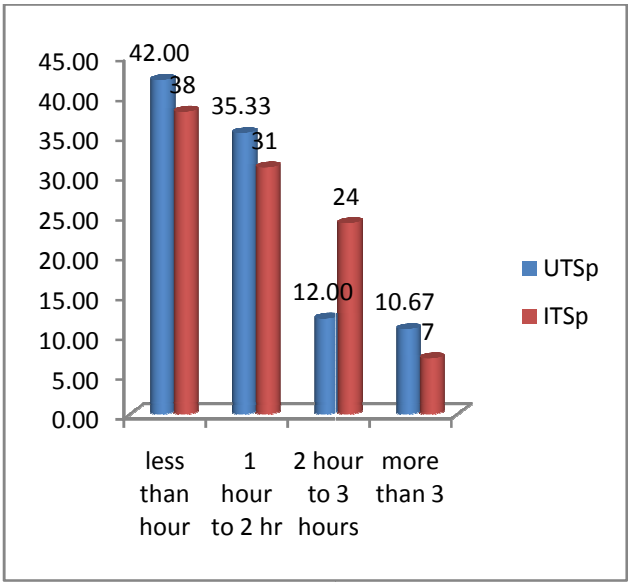


Fig 1: Time spent by respondents from US and India

The two set of respondents, I (Indian) and U (United States of America), are analyzed and compared.

ITSp- 62% of users spend more than an hour on SM websites, every day.

UTSp- 58% of respondents from US spend more than an hour daily.

Both set of users fall in the danger area of being addicted, since they are using it for more than an hour. An hour and more from the day, that is otherwise packed with very important activities.

Also, when discussed informally with some of the respondents a very interesting observation has been made. The respondents shared that since all popular social media sites had developed their "Apps" for their smart phones, which were far more convenient than logging on to the website, they access them numerous time in the day. At the same time, they shared that since they had their smart phone with them all the time, it was impossible for them to ascertain the time spent on these websites. Though not possible in quantitative terms but qualitatively it can be laid down that most of the respondents have been spending more than an hour and hence a

problematic for their psyche and at the same time a potential for the brands to promote themselves.

Symptom 2

FTM First thing in the morning

The basic reason for the inclusion of this symptom is that something of immense importance or something that you slept over would a respondent do the first thing in the morning. Hence, in case the respondents access their social media accounts first thing in the morning, it emphasizes the paramount importance of SM sites to them.

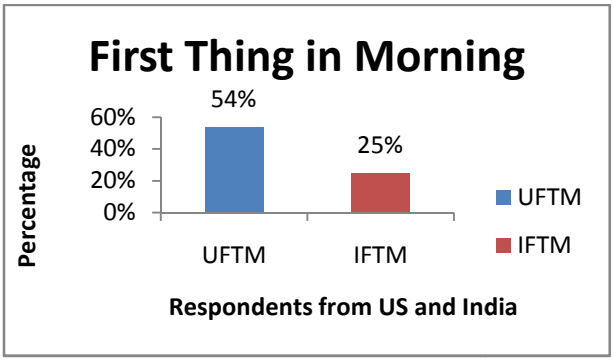


Fig 2: Accessing SMS first thing in the Morning (FTM).

The analysis reveals an interesting aspect that only 25 percent of Indian respondents access social media websites FTM as compared to more than half (54%) of the respondents from US. This symptom is more pronounced in US respondents as compared to Indian respondents.

Symptom 3

LTN Last Thing at night

This symptom is extremely important not only to establish whether the addiction exists or it doesn't but also to infer that it is not healthy. The scriptures of many religions and also the psychological health groups emphasize that the last thing we do before sleeping off determines to an extent how well we sleep at night, which in turn affects our mental health.

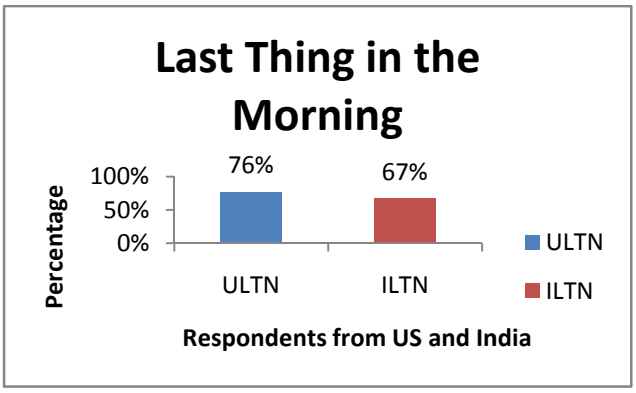


Fig 3: Accessing SMS last thing at night (LTN).

The practice of logging into the social media websites last thing before going to sleep is prevelant in both set of respondents, more than half are indulging in it. If compared more respondents from the US(76%) as compared to Indian respondents(67%) are in the habit of checking their social netwroking accounts before going to sleep.

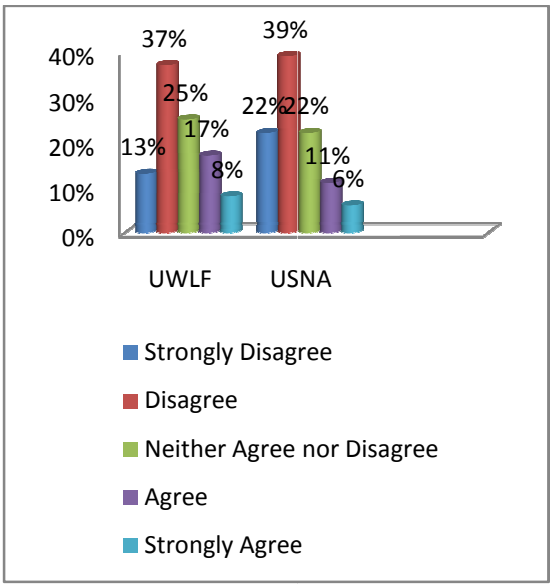
The psychological interpretation for the same cant be good. Religion tells you to chant before going off to sleep, psychiatrists tell you to either read good books or think of all the good things you did in the day. Basic reason is to make the mind calm before going to sleep. In today's busy life, getting a good night sleep is the only respite our brain gets. Logging on the various SM websites would mean, either viweing other people's lives (Facebook), getting more career advise and connections (linkedin), getting advice from novices or peeping into the lufe of celebrities (twitter), etc. None of which can have calming affect on the mind of the user.

Symptom 4

4A WLF Social media is the way of life.

4B SMA Social media is Addictive

This parameter was important to study since the acknowledgement of this statement can be construed as a positive sign, which can lead to the acceptance and then of course responsible use.



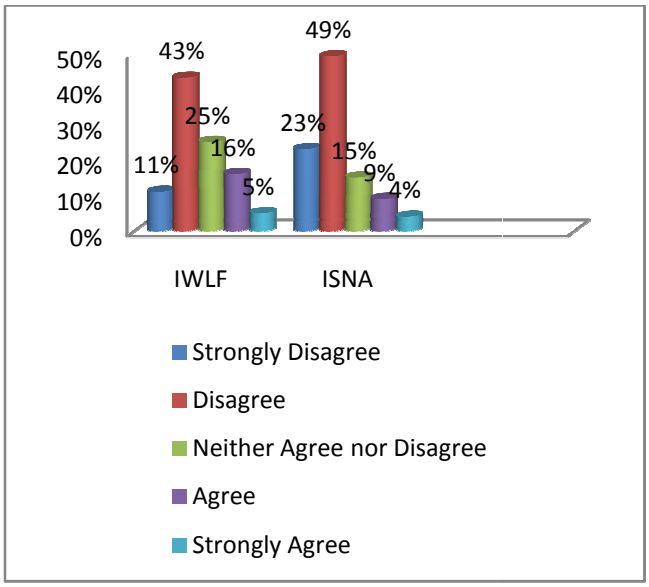


Fig 4 A and 4 B: SM is the way of life and Social media is addictive.

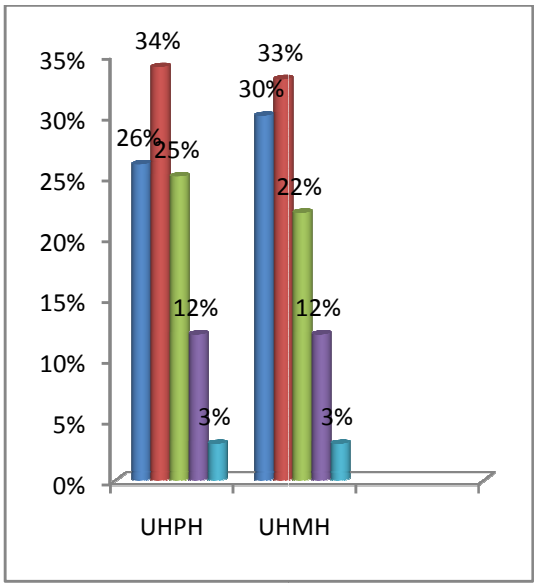
4A "Social media is the way of life" (WLF) is a statement that studies the comfort and dependance of respondents on the medium. The graphs above depict that the in case of US respondents, 37% agree (13% Strongly agree) with the statement, that SM is the way of life for them. Similar pattern is followed by Indian respondents, 43% agreeing with the statement (11% srongly agree). All this implies that it's a ritual of daily lives and not a one off thing that they might indulge in occasionally. It can be construed as a signal towards SM to be used as a marketing medium as well.

4 B "Social media is addictive". The analysis of the statement yields a very encouraging finding. 72% Indian Users and 61% US respondents acknowledge the fact that they feel SM medium is addictive. The fact that they are open to the idea of it being addictive is remarkable and since the above discussed symptoms point at them being addicted, the chances of them accepting it and hence using it judiciously increase.

Symptom 5

5 A HPH spending too much time on Social media is harmful to Physical Health

5 B HMH spending too much time Social media is harmful to Mental Health



.

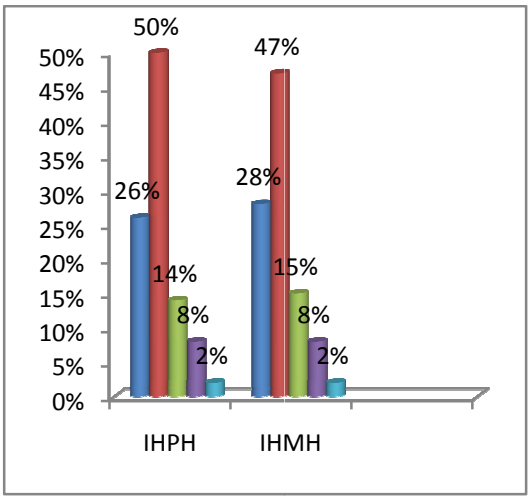


Fig 5 A and 5 B: SM is Harmful to physical and mental health.

5 A "Spending too much time on Social media is harmful to Physical Health"

Substantial number of respondents agree/Strongly agree with the statement that spending too much time on SM is harmful to physical health of a person. The time spent on SM keeps people away from physical activities. Being glued to the social media for hours through laptops, tablets, smartphones harms physical health.

The agreement level (26% SA; 34% of US respondents agree and 26% SA; 50% of Indian respondents Agree) is again a very promising finding, which implies that the respondents are aware of the perils associated with it in terms of physical health.

5B "Spending too much time on Social media is harmful to Mental Health"

The studies have revealed that the "need to belong" increases the use of Social media websites. "Loneliness" causes excessive use of SM websites like Facebook but at the same time mental health is adversely affected by its increased use. Again 63% of respondents from US and 75% from India agree with the statement that using too much of SM is harmful to mental health, implying their understanding that the excess use needs to be avoided.

VI. CONCLUSION

The comparative analysis of the respondents from the United States of America and India has been made and it reveals that Social media (SM) being a global phenomena, the behavior of the two set of respondents is similar, though more profound in some areas and lesser in the other.

- Majority of both the group of respondents spend more than an hour on Social media websites (which isn't encouraging). The symptom recognized by many psychologists as an indicator of SM Addiction.
- FTM and LTN, both are important to determine the addictiveness of the respondents. Lesser number of respondents are using it the first thing in the morning as compare to the Last thing at night. More number of respondents from the United States of America are hooked on SM websites as compared to the Indian respondents but both are bordering the addiction pattern, which is in no way comforting.
- The encouraging finding is that both the set of respondents agree that SM is addictive and it's the way of life. The recognition and acknowledgement that they have expressed reveals that they are aware that the path they are treading, is addictive. It is a positive sign and hence we see them making use of the positives of social media websites to their advantage, without being sucked into it and feeling trapped in times to come.
- Again there is a unified agreement by both the set of respondents that spending too much time on SM is harmful to physical and mental health.

  Cyber-bulling, Pseudo self-image, Body Dysmorphic syndrome are some of the psychological manifestations of excessive social media.

  It can be concluded that SM has become an integral part of respondents' life. It justifies being a global phenomenon since the opinion/usage pattern all fall within the same range. The gen-next seems to be bordering on the symptoms of SM Addiction (using it for more than an hour or probably more, first thing in the morning , last thing at night) but they seem to be weary of it being addictive, harmful to physical and mental health.

The analysis reveals that if made aware of Social media addiction symptoms, problems, and ways of de-addiction, they might in all probability stay clear of it or get de-addicted.

REFERENCES

[1]. Babbie, E. (2002). *The basics of social research.* Belmont, CA: Wardsworth Group.

[2]. Ofcom. (2008.) Social media A Quantitative and Qualitative Research Report.http://www.innpdf.com/ebookreview/social-networking-a-quantitative-and-qualitative-research-report.html

[3]. Sherman, E. (2011). Facebook Addiction: Factors Influencing an Individual's Addiction. Massachutes: Erica Sherman.

[4]. Shaw, E. (2013, January 29). Status Update: Facebook Addiction Disorder. Retrieved from The Glen Echo: http://theglenecho.com/2013/01/29/status-update facebook-addiction-disorder

[5] Calderon, J. (2012, February 21). Facebook Addiction Disorder in Malaysia, Newsweek (Japan). Retrieved from Transcending Culture Shock: http://justincalderon.wordpress.com/2012/02/21/facebook-addiction-disorder-in-malaysia-newsweek-japan/

[6]. Yang, H., & Tang, J. H. (2003). Effects of social media on students' performance: a web-based forum study in Taiwan. Journal of Asynchronous Learning Networks, 7(3), 93-107

[7]. Tashakkori, A. &Teddlie, C., (1998). Mixed methodology: Combining qualitative and quantitative approaches. Thousand Oaks, California: SAGE Publications, Inc.

[8]. Henderson, J. M. (2012). 3 Reasons You Should Quit Social Media In 2013. *Forbes* Retrieved from Forbes: http://www.forbes.com/sites/jmaureenhenderson/2012/12/29/3 reasons-you-should-quit-social-media-in-2013

Password Authentication and Encryption in Wireless and Telecommunications Security

K. S.Nwizege, M.MacMammah, N.S. Agbeb, P. G. Irimiagha, I.H.Harry,
Elect/Elect Engineering Dept
Ken Saro-Wiwa Polytechnic
Bori, Nigeria
s.k.nwizege@ieee.org, macmammahm@yahoo.com, agbeb_nornu@yahoo.com, mie4tammy@gmail.com, ipadibi@yahoo.com
Mmeah Shedrack
Computer Science Dept
Ken Saro-Wiwa Polytechnic, Bori, Nigeria
shedrackmmeah@yahoo.com

***Abstract* – Password is a secret identification chosen by an individual that when required and provided correctly will grant access to a device or network. In order to stay safe on network and devices, a strong password is needed so that it is not easily broken by hackers and intruders. A good practice to computer and network security is by chosen a password with alphabets, numbers, special characters, and case-sensitivity. Authentication on the other hand, is to verify a user before granting access to device on network.Wi-Fi Protected Access (WPA) is an interim standard adopted by the Wi-Fi Alliance to provide more secure encryption and data integrity. This is because, it uses dynamic key encryption. In this paper, we have dealt with password and authentication issues as relate to wireless security. We have also proposed some solutions and techniques to combat insecurity issues in wireless and telecommunications systems.**

Keywords –IEEE 802.11; wireless security; computer security; cybersecurity; authentication

I. INTRODUCTION

IEEE 802.11 standard include various wireless standards. Its standard is used based on application that best suit each standard. Wireless network is a technology that enables the communication between devices without the use of wires or cables.

With the nature and weak status of wireless networks unlike wired, they are susceptible to attacks than their wired counterparts. This means that more tasks is needed to ensure the security of wireless networks than wired. This makes wireless and computer securities a very important task in wireless and telecommunications systems.

The increased threat posed by information insecurity has in no small major way affected the productivity and sustainability of many firms today. One of the most affected is the bank followed by other financial institutions. Several reports of financial crimes are received on a daily bases, especially that of cybertheft. This is where confidentiality of information management is most needed.

Cyber crimes against banks and other financial institutions probably cost many hundreds of millions of dollars every year. Cybertheft of intellectual property and business. Confidential information has costs developed economies billions of dollars, how many billions is an open question. These losses could just be the cost of doing business or they could be a major new risk for companies and nations as these illicit acquisitions damage global economic competitiveness and undermine technological advantage [1] - [4].

Cybersecurity is the protection of valuable intellectual property and business information in digital form against theft [5] and misuse. It is an increasingly critical management issue. The US government has identified cybersecurity as one of the most serious economic and national security challenges. These acts take place in wireless and telecommunications systems, hence, need for them to be strongly secured.

II. BACKGROUND OF STUDIES

Since the early 1990s, there have been remarkable changes and challenges in the area of wireless and mobile communication. The development of semi-conductors and integrated circuits is the basis of the working principle of mobile communication [6]. In the late 1990s, this area experienced a rapid growth and interest with the existence of 2G, 3G, and 4G cellular networks. Due to the flexibility and portability of this technology. Many researchers have being motivated , having interest in researching into the field of Information and Communication Technology (ICT) with telecommunication engineers interested in how to employ the capabilities of this technology. The last few years, has witnessed a dramatic growth in the wireless industry which has created a lot of employment as well as financial revolution in the wireless industry.

Since the introduction of this technology, there has been a tremendous shift away from landlines telephones which were very effective since their introduction in 1979 to mobile cellular telephony in 1980.
The Advanced Mobile Phone System (AMPS) was launched in 1982 in the United States due to the growth of mobile communications in order to deploy mobile services to people. The system was allocated a 40 MHz bandwidth within the 800-900 MHz frequency range by the Federal Communications Commission (FCC) for AMPS. An additional 10 MHz bandwidth called Expanded Spectrum (ES), was allocated to AMPS in 1988 [6].
The importance of wireless technology is ubiquitous in that everyone can feel the impact of this technology, since it is deployed both at home, schools, coffee shops, hospitals, cafe, and many other places. Life became easier than before when wireless and mobile technology and devices such as Personal Digital Assistant (PDA), laptops, IPADs, and mobile phones were deployed. [6].

- *Why cybersecurity?*

Large and reputable organisations have dramatically strengthened their cybersecurity capabilities over the past five years. Formal processes have been adopted to be implemented with priority. IT security experts have developed mitigation strategies, and hundreds of millions of dollars have been dedicated in order to execute these strategies. Desktop environments are far less “wide open” than they were even five years ago, as Universal Serial Bus (USB) ports have been disabled and Web mail services blocked. Robust technologies and initiatives have been put in place to address attacks on the perimeter.

- *Why awareness?*

U.S. Executive Order (EO) 13636 initiated a dialogue to identify challenges and determine effective responses to cybercrime. One of the areas suggested to handle this alarming security threat is the use of forum for more awareness, training, and updates [7]. The CForum is one of those helpful avenues for handling cybersecurity issues.
CForum can help identify others’ examples of use that can save your organization time. It applies the Framework’s flexibility to achieve organizational cybersecurity goals. It has guide that will help learn how different organizations use it in different ways with different tools to achieve Framework outcomes [8].

American Water Works Association has developed Process Control System Security Guidance for the Water Sector and a supporting Cybersecurity Use-Case Tool [9]. The AWWA’s cybersecurity resources are designed to provide actionable information for utility owner/operators based on their use of process control systems [10] & [11].

III. COMPUTER SECURITY

Computer Security is the protection of computing systems and the data that they store or access. Companies must now fend off ever-present cyber-attacks. This act is influenced by cybercriminals or even disgruntled employees releasing sensitive information, taking intellectual property to competitors, or engaging in online fraud. While sophisticated companies have recently endured highly public breaches to their technological environment, many incidents go unreported. Indeed, business owners are not eager to advertisepayment of ransom to cybercriminals or to describe the vulnerabilities that the attack exposed [12].

To reduce security risk as much as possible, it will be good to adopt the following principles at all times:

- Learn **"good computing security practices."**
- Incorporate these practices into your everyday routine. Encourage others to do so as well.
- Report anything unusual - Notify the appropriate contacts if you become aware of a suspected security incident [13].

Computer Security allows an organisation to carry out its mission by:

- Enabling people to carry out their jobs, education, and research
- Protecting personal and sensitive information (data) [14].
- Supporting critical business process
- **Data in-motion.** Sensitive information communicated over the network.
- **Data at-rest.** Sensitive information stored in repositories such as databases, fileservers or collaboration systems.

To achieve this, organizations must define policies to enforce control if inappropriate access or usage of the data is detected. Once a policy violation occurs (such as attempting to access intellectual property, copying the information to a USB drive or attempting to email it) the solution should mitigate the compromise while generating an alert. To secure our computer and network, strong password is needed.

- *Passwords*

When storing passwords, hashes of passwords should be stored instead. If an attacker steals the password file detecting the passwords is difficult. To convert them back to passwords every possible hashed password will be tried until its detected. Any system which can reveal a password isn't hashing it.

- *Problems with Passwords*

- Finding written passwords
    - Post –It Notes
- Guessing passwords/pin
    - Dog/kid's name/Birthday
- Shoulder surfing
- Keystroke logging
    - Can be resolved with mouse based entry
- Screen scraping (with keystroke logging)
- Brute force password crackers.

- *Problem with hashed passwords*
    - Use ofcommon password
    - dictionary of hashed common passwords or dictionary words have been built (passwords from other password breaches)
- Do not re-use passwords from one system to another!

IV. NETWORK SECURITY

The alarming increase and impact of cybercrime cannot be over-emphasised. This is because, it is a daily occurrence in various geographical locations, and has become a normal routine. The impact is so severe that it affects sensitive aspects of a nation's economy such as Bank, Government, Schools, others.

Network security, wireless security, use of network protocol analyser, and cloud computing as control/ solutions to cybersecurity, network or computer attacks are discussed.

- *Wireless network*

Wireless network or connection enable nodes or devices to communication with each other without the use of wire or cable as shown in figure1.

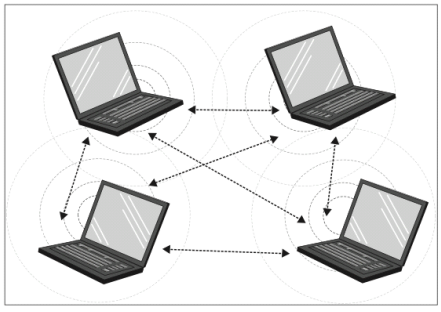


Figure 1: Wireless configuration.

There are many Wireless Local Area Networks (WLANs) with no or inadequate securities, one in every three WLANs in various locations are unsecured. Some of the reasons behind it may be carelessness, lack of IT knowledge, laziness, and ignorance. The IEEE 802.11 standards addresses security issues by supporting wireless technology used for security of wireless networks.

New types of malicious code have been written that force wireless devices to make phone calls, because of the telephony capabilities present. With the availability of wireless networks everywhere, sniffing is an inherent problem in wireless networks. Sniffers need have access to the physical parts of the network before a wired network can be broken, unlike in wireless network where sniffers do not even need to be in the network but somewhere nearby with a transmitter and the network can be accessed [15].

Wi-Fi Protected Access (WPA) is an interim standard adopted by the Wi-Fi Alliance to provide more secure encryption and data integrity, while the IEEE 802.11 standard was being ratified. Its more secure than Wired Equivalent Privacy (WEP).

WPA is the first generation of advanced wireless security, providing enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Some the characteristics of this technology are: strong encryption, strong access controls, strong user authentication.

WPA uses dynamic key encryption, which means the key to constantly changing and making breaking into a wireless network more difficult than WEP. WPA is regarded as one of the highest levels of wireless security for a network and is recommended if the devices support this type of encryption.

- *Temporary Key Integrity Protocol(TKIP)*

Temporal Key Integrity Protocol (TKIP) is a protocol used to create dynamic key encryption and mutual authentication. It is the heart of soul of WPA security. TKIP replaces the WEP encryption and provides the security features that fix the limitations of WEP as the keys are always changing. It provides a very high level of security for networks. WPA 'Personal' mode is the most likely choice for homes and small offices.

Furthermore, TKIP encryption algorithm is stronger than the one used by WEP but works by using the same hardware-based calculation mechanisms WEP uses. Some of the functions of TKIP are: It determines which encryption keys will be used and verifies the client's security configuration, It is responsible for changing the unicast encryption key for each frame, It sets a unique starting key for each authenticated client that is using a preshared key.

- *Network protocol analyser*

A protocol analyzer examines the granular details of network traffic at the packet level. Some protocol analyzers, however, are either difficult to use or expensive. Ethereal bucks the trend in both cases.

Some of them are Microsoft network monitor, ethereal, nagios, OpenNMS, advanced IPScanner, Capsa Free,

Fiddler, NetworkMner, PandoraFMS, Zenoss Core, The Dude, Slunk just to mention a few.
These tools help to monitor traffic and are alert to hackers and intruders on a network [16].

- *Cloud computing*

This is another technology that helps to secure data/information to some extent. Cloud computing allows users to migrate and from anywhere to access their data. It has the following characteristics: reliability, agility, Application Programming Interface (API), cost, location independence, device, maintenance, multitenancy, performance, productivity, scalability, elasticity, and security [17]- [19].

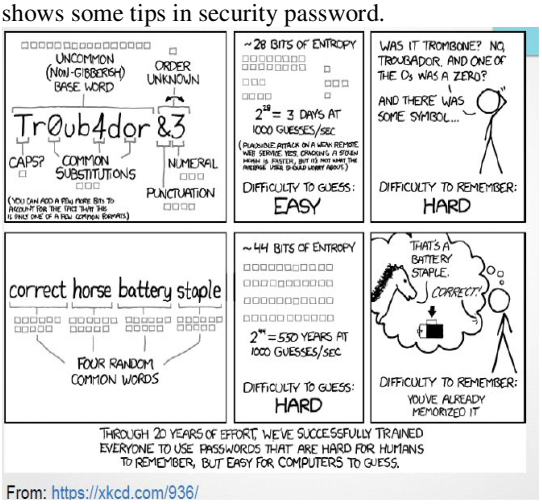
Cloud services can be private, hybrid, and public. With private services, the clients can install hardware and software required to use only, this is in contrast of a public offer where the user does not give any guarantees about the hardware on which their applications are running and it cannot be used by other users. While hybrid cloud computing uses a mixture of both private and public cloud services.

V. AUTHENTICATION AND ENCRYPTION

Authentication and encryption processes that control attacks on wireless and telecommunication systems are discussed.

- *Password authentication*

Password authentication is very necessary in order to verify a user before granting access. Password that can NOT be easily broken or hacked is very vital. Figure 2 shows some tips in security password.



F igure 2: Password tips.

Password authentication can provide relatively strong security but in order to do so, certain assumptions must be true:

- The user must have some assurance that the authenticator is in fact the authority in question
- The communication channel between the user and the authenticator must itself be secure
- It must be highly unlikely that an attacker would be able to guess the password. Usually this is accomplished by limiting the number of wrong guesses
- If the user is a human being the password must be easy to remember , but not easy that it can be easily guessed

- *Requirement for Wireless authentication*

- **Mutual**- It must provide mutual authentication , that is , the authenticator must authenticate the user , but he user must be able to authenticate the authenticator as well
- Mutual authentication is particularly important over wireless networks because of the ease with which an attacker can set up a rogue access point

There are two possible attacks:

- The rogue is not connected to the target network divulging authentication credentials

  The rogue is connected to the target network. The attacker may then ignore the credentials presented by the user and 'authorize' network access. The user' session may then be recorded in the data path.
- **Self protecting-** It must protect itself from eavesdropping since the physical medium is not secure. The authentication must proceed in such a way that eavesdroppers cannot learn anything useful that would allow the user to be impersonated later.
- **Immune to Dictionary Attacks-** It must not be susceptible to online or offline dictionary attacks.

An online attack is one of where the imposter must make repeated tries against the authenticator 'on line'. These can be thwarted by limiting the number of failed authentication attempts a user can have.
An offline attack is one where attackers can make repeated tries on their own computers, very rapidly, and without the knowledge of the authenticator. Simple challenge/response methods are susceptible to offline attacks because if attackers capture a single challenge/response pair, they can try all the passwords in the dictionary to see if one produces the desired response

- **Produces Session Keys**- It must produce session keys that can be used to provide message authentication, confidentiality, and integrity and protection for the session

the user is seeking to establish. These keys will be passed to the user's device drivers to be used as WEP or TKIP keys during the ensuring session.

- *Encryption*

Encryption is a way of representing information or encoding it in such a way that only the individual can read. Encryption does not present interception, which means the hacker could intercept the network or device, but will deny the message content to the interceptor.

In cryptography, Secure Sockets Layer (SSL) is used for encryption. SSL was developed by Netscape in 1990s to create confidence in e-commerce. It also known as Transaction Layer Security (TLS) .It is used by Secure HTTP (HTTPS).

Some of the roles of SSL are:Encrypts all data exchange with a symmetric cipher. It ensures that the server being communicatingwith, is the actual server by using secure message authentication and public keys. And also detects "man in the middle attacks" with secure hashes.

Banks and most websites were payment schedules are handled use this encryption.

For this reason, banks obtain the SSL certificate and their domain name bears https before it. If such certificate is not possessed, an organization's domain name is exposed to security threats especially if itprovides payment transaction facility.

- *Wireless encryption*

WPA is considered as one of the highest levels of wireless security for a network and is recommended if the devices support this type of encryption. The WPA data is encrypted using the RC4 stream cipher with a 128-bit key and a 48 –bit Initialization Vector (IV).

One great improvement in WPA over WEP is the TKIP , which dynamically changes keys as the system is used. When combined with the much larger IV, this defeats the well-known key recovery attacks on WEP. Table 1 shows the types of encryptions vendor type, cost, and also level of security. It also shows the effectiveness of security type as WEP is the weakest of all encryption types.

TABLE 1: WIRELESS ENCRYPTION.

Types	Desktop control Needed	Cost to implement	Difficult to Message	Vendor Support Problem	Vulnerable to Attack
none	Low	Low	Low	Low	High
WEP	Medium	Low	High	low	Medium
WPA TKIP	High	High	High	Medium	Low
802.11AES	High	High	High	High	None
VPN	High	High	Medium	Low	none

VI. CONCLUSION AND FUTURE WORKS

This paper, identified security threats in wireless and telecommunications systems, and proffers measures to mitigate these attacks. Strong password and authentication will alleviate to protect devices and networks. Network protocol analyzers and cloud computing technology canhelp in securing data and network.

In the future, SSL certificate is recommended for reliable authentication of organizations that deal with payment and financial issues, sincetheyarethe major targets of attackers and hackers.

ACKNOWLEDGEMENT

This research was supported by Tertiary Education Trust Fund (TETFund) through the Ken Saro-Wiwa, Polytechnic, Nigeria.

REFERENCES

[24] http://www.spiegel.de/international/world/0,1518,713478-6,00.html [Accessed 10/09/15].

[25] http://www.dw-world.de/dw/article/0,,5645869,00.html[Accessed 10/09/15].

[26] http://www.blog.thehigheredcio.com [Accessed 10/09/15].

[27] https://prezi.com/6xolemrzxbys/cybercrime [Accessed 10/09/15].

[28] http://www.webopedia.com/TERM/C/cyber_crime.html [Accessed 10/09/15].

[29] K. S Nwizege. Adaptive Data Transfer for Dedicated Short Range Communications (DSRC)-Based Vehicle Networks, PhD thesis, Swansea University, UK, pp. 3.4, 2014.

[30] http://its.ucsc.edu/security/training/intro.html [Accessed 10/09/15].

[31] Cyber.SecurityFramework.org [Accessed 10/09/15].

[32] http://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx [Accessed 10/09/15].

[33] http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ [Accessed 10/09/15].

[34] https://www.us-cert.gov/ccubedvp[Accessed 10/09/15].

[35] https://ics-cert.us-cert.gov/Assessments[Accessed 10/09/15].

[36] http://its.ucsc.edu/security/top10.html[Accessed 10/09/15].

[37] http://www.forbes.com/sites/kurtmarko/2014/11/09/big-data-cyber-security/ [Accessed 10/09/15].

[38] J. R.Vacca, Guide to Wireless Network Security, pp. 4-7, Springer Science+ Business Media, LLC, USA, 2006

[39] http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/[Accessed 10/09/15].

[40] Contracts of Cloud: Comparison and Analysis of the Terms and Conditions of Cloud Computing Service, Queen Mary School of Law Legal Studies Research Paper No. 63/2010, 2010

[41] Lamia Youseff, Maria Butrico, Dilma Da Silva, Toward a Unified Ontology of Cloud Computing, Grid Computing Environments Workshop, 2008. GCE '08 New York, pp. 1-10, Nov. 2008.

[42] Radu Prodan and Simon Osterman, A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers, Grid Computing, 2009 10th IEEE/ACM.

Security QoS Profiling Against Cyber Terrorism in Airport Network Systems

F.N.Ugwoke[1], K.C.Okafor[2], V.C.Chijindu[3]
[1]Dept. of Computer Science, Michael Okpara University of Agriculture, Umudike, Umuahia, Nigeria
[2]Dept. of Electrical Electronic Engineering, Federal University of Technology, Owerri, FUTO, Nigeria
[3]Dept. of Electronic Engineering, University of Nigeria, Nsukka, Nigeria
[1]ndidi.ugwoke@gmail.com, [2]kennedy.okafor@futo.edu.ng, vincent.chijindu@unn.edu.ng

***Abstract*—Attacks on airport information network services in the form of Denial of Service (DoS), Distributed DoS (DDoS), and hijacking are the most effective schemes mostly explored by cyber terrorists in the aviation industry running Mission Critical Services (MCSs).This work presentsa case for Airport Information Resource Management Systems(AIRMS) which is a cloud based platform proposed for the Nigerian aviation industry. Granting that AIRMS is susceptible to DoS attacks, there is needed to develop a robust counter security network model aimed at pre-empting such attacks and subsequently mitigating the vulnerability in such network. Existing works in literature regarding cyber security DoS and other schemes have not explored embedded Stateful Packet Inspection (SPI) based on OpenFlow Application Centric Infrastructure (OACI) for securing critical network assets. As such, SPI-OACI was proposed to address the challenge of Vulnerability Bandwidth DepletionDDoS Attacks (VBDDA). A characterization of the Cisco 9000 router firewall as an embedded network device with support for Virtual DDoS protection was carried out in the AIRMS threat mitigation design. Afterwards, the mitigation procedure and the initial phase of the design with Riverbed modeller software realized. For the security Quality of Service (QoS) profiling, the system response metrics (i.e.SPI-OACI delay, throughput and utilization) in cloud based network were analysed only for normal traffic flows. The work concludes by offering practical suggestion for securing similar enterprise management systems running on cloud infrastructure against cyber terrorists.**

Keywords—Attacks; Cloud Datacenters; DoS; DDoS; Vulnerabilities; AIRMS; Mitigation Techniques; Aviation Industry)

II. INTRODUCTION

As the human population grows, malicious cyber-criminals grow in a proportional status. These entities tend to launch attacks for various reasons yet to be justified. With respect to post September 9/11 attack, the United States aviation security Transportation Security Administration (TSA) has placed focus on security checkpoints and unearthing potential threats through bomb-sniffing technology, terrorist watch lists, increased use of in-flight security officers, full-body-scanners, behavioral detection officers, positive baggage matching, and hardened cockpit doors [1], [2]. More so, a variety of airport security techniques are currently available, and more are at the developmental stage. The most popular security schemes on aviation systems architectures includes: Intruder Detection Systems (IDS), Biometrics, Enhanced Body Scanners (EBS), X-ray technologies, Smart Phone Applications (SPAs), blackholing, router filtering, and firewalls.Because sophisticated DDoS attacks are defined byanomalous behaviour at layers 3 and 4, existing approaches are not optimized for DDoS detection or mitigation as they are not reliable, cost effective, and scalable.

Again, the technological components of aviation security systems such as biometrics and access control, flight tracking and information display systems (FIDS), Air Traffic Control (ATC), passenger screening, baggage tracking and inspection, networks and web Services and radio communication [3] have gained strong advocacy in the past with still various degree of inefficiencies. Since airport information systems infrastructures could be complex and are derived from a seemingly untraceable number of sources, by developing an intelligent cloud based network infrastructure, a mitigating technique for dealing with DoS attack will ensure that the AIRMS is undisrupted.

Hence, this work adopted Application Centric Infrastructure (ACI) which supports OpenFlow paradigms, Network Address Translation (NAT), Quality of Service (QoS), IP Security (IPSec), Secure Sockets Layer (SSL) VPN, and an embedded DDoS thereby improving end-to-end network security infrastructure. This research is still ongoing, but the intended contributions are as follows:

i. To use SPI-OACI for the AIRMS cloud based network while carrying out the security QoS profiling using selected metrics.
ii. To develop the vulnerability bandwidth and memory attack model for the cloud based AIRMS network.

This paper will only address the above while providing the roadmap for future work. The rest of the paper is organized as follows. Section II; focus on threat dimensions, and airport security models/architectures. In Section III; a description of the airport network model was made. Also, characterization of Vulnerability Bandwidth Depletion DDoS Attack (VBDDA), SPI-OACI security architectural components, and SPI-OACI DDoS mitigation procedure were presented. Section IV presented the system design detailing the experimental setup and results analysis. Section V; presents the conclusions, recommendations and future work.

III. RELATED WORKS

A. *Threats Dimensions*

Globally, threats such as nuclear, biological and chemical attacks exist [4]. However; these physical threats are not the only security challenges facing the Nigeria. At large, everybody is concerned with the emerging technological threats to critical cyberspace infrastructures. With the globalization incidence, the Nigerian government is now tending towards the use of e-governance i.e. using interconnected computer systems to manage public services such as smart cities, smart grid energy systems, coordinate public transportation logistics, e-payment systems, and leverage similar technologies for a variety of services that will promote economic growth for the huge populace.

However, a state-sponsored attack could be launched to either deny certain services, steal information, or to take control and hijack such system. In the aviation context, this is referred to as cyber terrorism. For Instance, on June 22, 2015, hackers forced polish airline to cancel flights and this adversely affected the 1400 passengers [5]. Similarly, for the past two years, a team of Iranian hackers has compromised computers and networks belonging to more than 50 organizations from 16 countries, including airlines, defense contractors, universities, military installations, and hospitals. The hackers used common SQL injection, spear phishing or watering hole attacks to gain initial access to one or more computers of a targeted organization. They then used privilege escalation exploits and other tools to compromise additional systems and move deeper inside its network [6]. The aviation network systems if not well secured will suffer from emerging attacks and threats.

The author in [7] outlined the cyber security threats facing airports and revealed the potential vectors that might be used in an attack as well as the tactics for securing known vulnerabilities. It was noted that several threats could be focused on external airport operations, such as external airport or airline websites, concession point-of-sale, credit card transaction information, and passenger's wireless devices. However, the overall impact of cyber attacks on systems external to airport operations is little when compared to attacks on systems required to perform internal airport operations.

In this context, the potential targets within an airport internal network include: access control and perimeter intrusion systems, e-Enabled aircraft systems, radar systems, wireless and wired network systems, and network-enabled baggage systems [7].Unfortunately, a variety of vulnerabilities occur within cyberspace because of humans, hardware, software, and connection points that provide access to such systems. The United States Computer Emergency Readiness Team (US-CERT) [8] has provided a high level overview of cyber vulnerabilities for control systems. These include the following vulnerabilities: wireless access points, network access points, unsecured SQL databases, poorly configured firewalls, interconnected peer networks with weak security, and several others.

Similarly, the National Institute of Standards and Technology (NIST) [9] has published a guide called Risk Management Guide for Information Technology Systems which shows a multi-step system analysis which network experts can use to assess network vulnerabilities, measure the potential of each vulnerability occurring with respect to the threat's source, motivation, and actions, whilst developing recommendations and documentation to counteract the vulnerabilities found within the assessment. In their report, vulnerabilities from the perspective of the potential consequence(s) of an exploited vulnerability is presented in three folds: loss of integrity, loss of availability, and loss of confidentiality. Loss of integrity occurs when access is gained and one can no longer guarantee that data has not been modified. Loss of availability occurs when a system is no longer operational or loses effectiveness.

Finally, loss of confidentiality "refers to the protection of information from authorized disclosure. Furthermore, NIST provides three levels to measure vulnerabilities: high, medium, and low. Ultimately, the assessment in [7] which is similar in nature to [8] and [9], settles on four components within an airport that are vulnerable to cyber attack. They include: the network, the device, the application, and the back-end system. Each of these requires a different approach to security. But by focusing on process, culture, staffing, and training, security of such systems can be guaranteed [10].

B. *Related Research Efforts*

Various works in the context of threats and attacks in airport security are reviewed in this section. The intent is to ascertain the extent of security research in AIRMS as well as the computing networks.

- *Airport Security Models/Architecture*

A selected highlight of works on Airport Transport management systems, security, frameworks and models is presented below. In [11], the authors presented a risk-based Airport model that consists of 5A's (Accounting, Authorization, Authentication, Auditing and Administration). Case study approach was used while an application method of the risk-based Airport model to the cyber security environment. This paper in [12] focused on key Airside Management Information Systems (AMIS) which could be used to facilitate the airport and airline operations. These are required to process aircraft, passengers, and air cargo. They involve the ticketing of air travelers, ground movement of aircraft and vehicles, flight procedures of aircraft within airport airspace, and scheduling and managing of boarding and gate equipment, and weather updates. Their AMIS proposal covered include: Gate Management System, Aircraft Fuelling System, Air Traffic Control (ATC) System, Weather Monitoring System, Airfield Lighting System, and Automatic Vehicle Identification (AVI) System. This study used naturalistic inquiry to elicit data related to the classification and use of AMIS. In [13], the author proposed a violation and vulnerability diagram of a cyber-exercise scenario based on Air Traffic Management infrastructures (ATM) incidents and showed how Vulnerability and Violation (V2) diagrams can identify interactions between malware and degraded modes of operation. Their initial results revealed the underlying

vulnerabilities that exist across safety-critical transportation infrastructures.

In [14], the authors discussed the US FAA's National Airspace System (NAS) model, and summarize the need, background, ongoing developments and research efforts on cyber-security standards and best practices at U.S. airports with special emphasis on cyber security education and literacy.Cyber Threats to Internal Airport Operations and related vulnerabilities were also presented.

The whitepaper in [15] presented an introduction to cyber security in air traffic management, including the cyber threats and risks and motives of threat actors, as well as some considerations to managing cyber risks and implementing a cyber security programme. In addition, the ATM information standards, framework for cyber security, and some practical guidance to conducting a cyber risk assessment and managing the cyber security risks to systems, assets, data and capabilities in ATM were detailed.

- *Existing DoS Attack Models*

In this section, a concise explanation of DDoS is given with the review on various research efforts. A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet. It is aimed at disrupting the normal function of a *specific* website or service. In context, DDoS attacker attempts to prevent legitimate administrators from accessing information or services. By targeting the AIRMS (computers and its network connection), an attacker may be able to prevent access from the airport application services that rely on the affected computer network. It is planned and coordinated with the goal of ensuring that an entire web service is unavailable to the valid users. In a DDoS attack, by taking advantage of security vulnerabilities an attacker could take control of the entire network system by using multiple systems to launch the attack. This forces a vulnerable system to send huge amounts of data to the entire network making the web service to be unavailable to the valid users.

The work in [16] proposed self-aware networks and a defense against denial of service attacks. The work presented an overview of the existing proposals on both detection of such attacks and defense against them. Also, a generic framework of DoS protection based on the dropping of probable illegitimate traffic, witha mathematical model which can measure the impact of both attack and defense on the performance of a network were presented. The work was validated with simulation results and experimental measurements in a SAN environment.

In [17], Internet scale DoS attack with a survey on its theoretical underpinnings and experimental applications was carried out. A comparison on the different types of DoS attacks were discussed as shown in figure 1. The work detailed the classifications as well as the application domain. In [18], the authors proposed a mathematical model for a low-rate DoS attacks against application servers (LoRDAS) attack. Their model was used to evaluate the performance LoRDAS by relating it to the configuration parameters of the attack and the dynamics of network and victim. The model is validated by comparing the performance values given against those obtained from a simulated environment.

In [19], secure overlay services (SOS) architecture was proposed to provide reliable communication betweenclients and a target under DoS attacks. The SOS architecture employs a set of overlay nodes arranged in three hierarchical layers that controls access to the target. Their proposed SOS architecture that proactively prevents denial of service (DoS) attacks, which works toward supporting emergency services. Their goalwas is to allow communication between a confirmed user and a target.

Similarly, the work in [20] proposed a composite DoS attack model that combines bandwidth exhaustion, filtering and memory depletion models for a more real representation of similar cyber-attacks. On the basis of their introduced model, different experiments were done. They showed the main dependencies of the influence of attacker and victim's properties on the success probability of denial of service attack. The concept of the composite model was explained were an incoming traffic is blocked because of insufficient bandwidth. In this case, the remaining part of traffic can be blocked by its filtering system. This is efficiently carried out using the proposed SPI OACI. This will also block anything left after filtering by creating an insufficient place in the buffer devoted to store open connections for the cyber attackers.

Apart from the generalized DoS classification given in Fig1, a comprehensive cyber-based threat to Air Traffic Management is shown in Fig 2. The Possible DDoS traffic types include: HTTP Header, HTTP POST Flood, HTTP POST Request, HTTPS Post Flood, HTTPS POST Request, HTTPS GET Flood, HTTPS GET Request, HTTP GET Flood, HTTP GET Request SYN Flood (TCP/SYN), UDP Flood, ICMP Flood, MAC Flood.

However, there two identified mitigation approaches for any large scale DoS/DDoS attacks, viz:

- Using firewall device at layer 4 and 7. This can be optimized for flow and deep inspections. In this case, the DoS protections include: Screen, session limits, and SynCookie.
- Using Router device at layer 3 and 4. This can be optimized for packet inspection and flow inspection. In this case, the DoS protections include: Line-rate ACLs, and Tare Limits.

This work combines the effectiveness of both approaches to offer an efficient security solution for AIRMS. By addressing the above attacks, bandwidth depletion and memory exhaustion in the network infrastructure is eradicated.

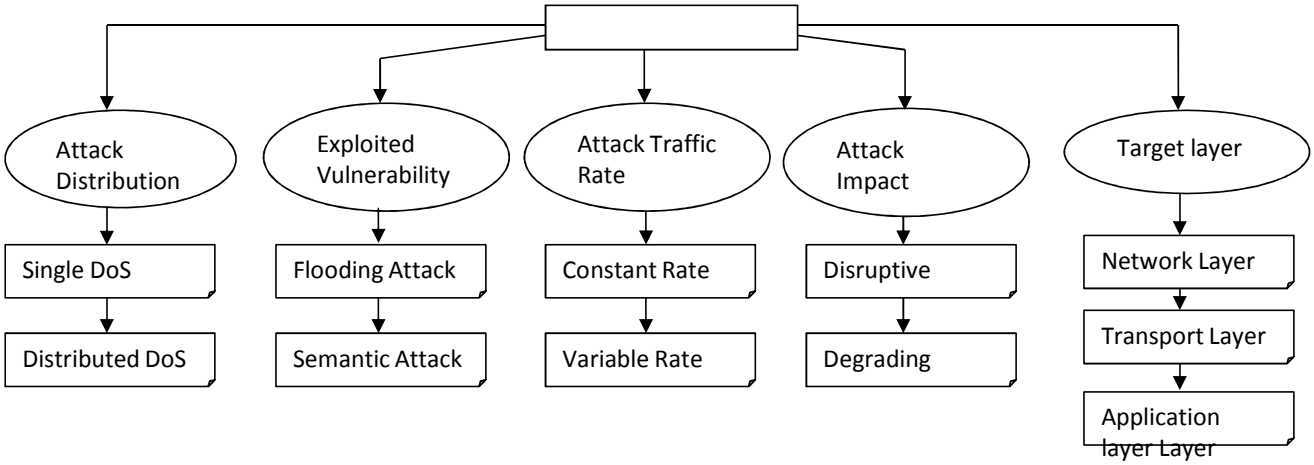


Fig. 1: DoS Attack Classification [17]

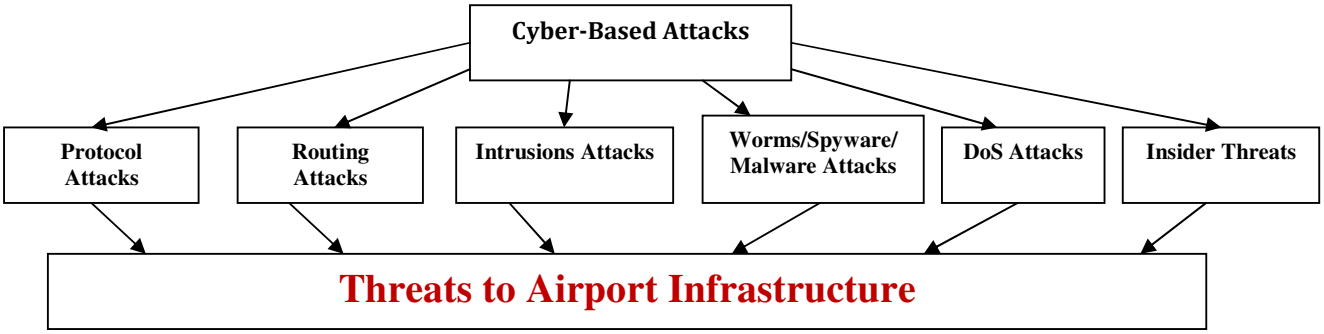


Fig. 2: Cyber-Based threats to Airports [21]

Other works on threats and attacks with emphasis on evaluation analysis of DoS traffic have been studied in [22],[23]. Existing works in literature regarding cyber security DoS and other schemes have not explored embedded Stateful Packet Inspection (SPI) based on OpenFlow Application Centric Infrastructure (OACI) for securing critical network architecture. This work seeks to address this research gap.

IV. Proposed AIRMS Network Model

Generally, many security algorithm computations exhibit a trade off between execution time and quality of service. For example, a firewall SPI OACI encoder can often track packets more quickly if proper configuration is made to drop only illegitimate traffic. This is generally summarized as Deep Packet Flow Inspection (DPFI) shown in Fig 3. All the network traffic inputs into the SPI-OACI processing are mapped into a clean vector $A_{gm.}$

This ensures that the monitoring servers are well secured.

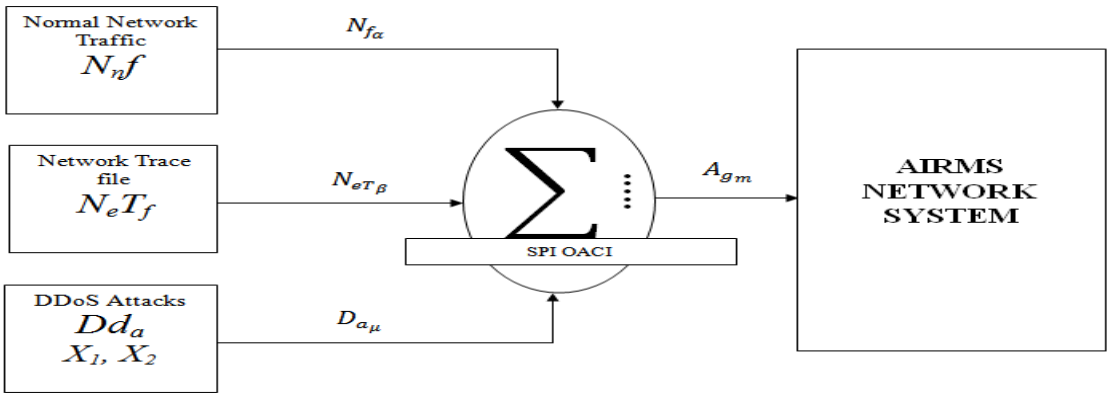


Fig. 3: Proposed System Architecture of cloud based Airport System

Fig 3 shows the proposed airport management system with information flowing between interacting systems via an SPI-OACI firewall. The management system runs on a cloud environment. The infrastructures and platforms supporting the AIRMS are interfaced on the cloud. The use of airport backend servers and high end monitoring servers via the airport fixed wireless infrastructure is shown in the proposed architecture. Also, maintenance services inside and outside the airport systems are enabled via e-devices. The security enforcement must find optimizations that appropriately balance quality of service and performance of the cloud network.

It must be stated that theproposed system architecture of cloud based airport system as shown in Fig 3 evolved from an initial work carried out in Distributed Cloud Computing Network (DCCN) [24]. The major issue investigated in context is the security layout of traffic flow into the AIRMS perimeter of defencewhere malicious attackers seek to hijack the AIRMS via DDoS attacks.This paper will present Vulnerability Bandwidth Depletion DoS Attack (VBDDA) characterizations that will facilitate QoS profiling with ease. This will help security designers and network architect to identify promising optimization benchmarks in such networks.

Interestingly, cyber terrorists represented by the attackers (see Fig 3) have the sole aim of exploiting the AIRMS via the backend servers. In this regard, an introduction of optimal allocation usingstateful Packet Inspection implemented in Cisco IOS firewall [25] will suffice. Some of the functions of the SPI include:

i. It provides a per-application control mechanism across network perimeters,as well as within networks through the Transparent Firewall capability. The SPI sets precedence for Context-Based Access Control (CBAC) which improves Access Control List (ACL) immensely.

ii. It enhances security for TCP and UDP applications by scrutinizing several attributes of data connection. The inspection enginetracks the state and context of network connections to secure traffic flow.

iii. It protects against packet-injection attacks by checking several components of TCP and UDP sessions. Source and destination IP address and port numbers must match, as well as TCP sequence number. Other attributes are checked as well, such as TCP window size, reducing the likelihood of buffer overrun attacks.

iv. It provides support for several complex, advanced services such as streaming protocols, IP voice, and other complex services that require detailed scrutiny to support additional data and media channels.

v. It provides DoS detection and prevention against some popular attack modes, such as SYN (synchronize/start) flooding, portscans, and packet injection.

From Fig. 3, when the SPI firewall detects unusually high rates of new connections, it issues an alert message, and resets excessive half open TCP connections to prevent system resource depletion. It tracks connections by destination address and port pairs to control undesired activity and reduce impact on hosts on the protected network that are under attack from malicious activity originating outside the firewall. Essentially, the SPI monitors several attributes in TCP connections, UDP sessions,

and Internet Control Message Protocol (ICMP) dialogue to ensure that the only traffic allowed through a firewall ACL is the return traffic for dialogue that was originated on the private side of the firewall. The OpenFlow ACI [26] is now the state of art for large scale configurations. This work opines that DoS and DDoS attacks just as in [20] can be modeled at the session rather than at the package level. Using Poisson process with arrival rate to characterize this scenario gives a better platform to study DoS types and their mitigation approach.

A. *Characterization of Vulnerability Bandwidth Depletion DoS Attack (VBDDA)*

Now, a Vulnerability Bandwidth DepletionDDoS Attack (VBDDA) could occur when an attacker $X_n$consumes all available bandwidth in Fig 3by generating a large number of packets directed to the cloud based network. ICMP ECHO packets or disruptive malware could be used. This could also result from an attacker comprising any vulnerable system and using it to launch an attack to the compute server center.

The properties of an attack could be used to ascertain its effect on QoS. While the work in [20] presented a mathematical expression of calculating the success of DoS attack using theknown data on the attacks, normal flow and other properties of the victim this work models the security QoS metrics using the SPI OACI approach. When a DDoS resource depletion attacks occurs, this will facilitate an attacker sending packets that misuse network protocol communications or sending malformed packets that tie up network resources sothat none are left for legitimate users or the server backend at large. Active memory is usually exhausted, and thus no new queries can be stored and served in the intervening devices or nodes. It has been observed that memory depletion DDoS attacks are the most common because of noticeable effect on an operational networks. For memory depletion DDoS attacks models, using the simplified Engest loss model G(N)/G/m(0) [27], this helps to estimate the success of the SYN flooding attackwhen average attack flow, the average storage time of open-state connections and buffer size areknown. This work considered a bandwidth exhaustion and memory depletion contexts which basically allows fractional analysis of every DoS or DDoSattack.

Considering Fig. 3, when analyzing a DDoS attack, vulnerability bandwidth and memory depletion DDoS models as well as for the SPI OACI filtering properties of the system are very vital. Incoming illegitimate traffic can be blocked because of insufficient bandwidth configured in SPI OACI while correctly filtering a legitimate packet. Anything left after filtering can be blocked by an insufficient place in the buffer devoted to store open connections. Let SPI OACI bandwidth exhaustion probability be given as B_p,the probability of filtering legitimate traffic as Fn_P and memory depletion probability as M_P. A stateful attack probability S_P can be calculated as the probability of blocking legitimate traffic at least in one of these three device variables, viz: bandwidth exhaustion, filtering or memory depletion [20]:

$$Sp=\sum_{i=0}^{n}\langle 1-(1-B_p)*(1-F_{np})*(1-M_p)\rangle \quad (1)$$

For estimating bandwidth exhaustion probability Bb_P in SPI OACI, the use of stochastic bandwidth exhaustion model was adopted [28] which is given by

$$Bbp = \left(\frac{\rho^k}{k!}\right) \Big/ \sum_{i=0}^{k}\left(\frac{\rho^i}{i!}\right) \quad (2)$$

Where

$\rho = (S_{Ba} + S_{Bn})/T$. This is also given by

$$\rho = (I_a * \lambda_{Ba} + I_n * \lambda_{Bn})/T$$

$K = Numberofopenchannels$

$S_{Ba} = Attacktraffic\ (bps)$

$S_{Bn} = Normaltraffic\ (bps)$

$T = Channelbandwidth(bps)$

$I_a = AverageQuerySizeoftheAttack\ (b)$

$I_n = AverageQuerySizeofthelegitimateusers\ (b)$

λ_{Ba}= *Average arrival rate attack queries (qps);*

λ_{Bn}= *Arrival rate of legitimate user queries (qps).*

It was assumed that the SPI OACI filtering system has two properties: the probability of filtering and dispatching legitimate traffic $\boldsymbol{Fn_P}$andthe probability of filtering and dropping attack traffic $\boldsymbol{Fa_P}$**.** These properties show the part of legitimate and attack traffics that are blocked on average using filters.

To estimate incoming traffic, these properties were considered in Fig 3 to address attack probabilities and memory depletion. Considering the bandwidth exhaustion model, this work assumed that both legitimate and attack traffic has the same distribution in time as the overall incoming data. After passing the bandwidth exhaustion model, the rate of incoming traffic will be reduced to λFa and λFnsuch that Equ 3 and 4 holds

$$\lambda_{Fa} = \lambda_{Ba}.(1 - B_p) \quad (3)$$

$$\lambda_{Fn} = \lambda_{Bn}.(1 - B_p) \quad (4)$$

Now, the SPI OACI filtering system must block traffic equally at every instant of time. It is reasonable to say that incoming legitimate traffic λ_n and attack traffic λ_a could change in size only but not in its distribution as perceived by the SPI OACI firewall. The extent to which traffic size will be reduced depends on filtering properties abnormal or illegitimate traffic probability and normal or legitimate traffic probabilities given in Equ 5 and 6.

$$\lambda_{\text{Mn}} = \lambda_{Bn}.(1 - P_{Fn}) \quad (5)$$

$$\lambda_{\text{Ma}} = \lambda_{Ba}.(1 - P_{Fa}) \quad (6)$$

In the AIRMS, another identified type of DDoS attack model is the memory depletion model. To represent this kind of the DDoS attack, this work leveraged the SYN flooding attack model [29] which can serve as a more general DDoS attack types. This model is given by Equ 7.

$$P_m = \left[\frac{\sigma^M}{M!}\right] \Big/ \sum_{i=0}^{M} \frac{\sigma^i}{i!} \quad (7)$$

Where

$$\sigma = \lambda M_a * t_a + \lambda M_n * t_n$$

t_a = $Averageprocessing\ time\ of\ the\ attack\ query\ (s)$; $M = Buffer\ size\ of\ the\ SPI\ firewall$

t_n = $Averageprocessing\ time\ of\ the\ legitimate\ query\ (s)$.

Equation 2 can be used to model a typical ping of death traffic where an illegitimate attack with about 250GBps traffic flow hijacks a network. A case based scenario was found in [30]. This was an online context illustrating a typical DDoS attack which represented a 250GBps DDoS attack designed to crash the web based service. This can be eradicated with SPI OACI.

B. SPI-OACI Security Architectural Components

This work will use the SPI-OACI security model for securing the AIRMS against VBDDA. The major device is adopted for the implementation is the Cisco ASR 9000 firewall [31] which is network embedded, and has a virtual DDoS protection capacity. There are two distinct components in the SPI-OACI security model viz:

The Traffic Anomaly Detector (TAD) and the Guard alert trigger. Both of these works together to deliver complete DDoS protection for virtually any environment. An in-depth discussion is presented below.

- SPI-OACI Traffic Anomaly Detector (STAD): This acts as an early warning system. It provides in-depth analysis of the most complex DDoS attacks and passively monitors network traffic while looking for any deviation from normal or baseline behaviour that indicates a DDoS attack.
- SPI-OACI Guard (SG): When an attack is identified, the STAD alerts the SG, providing detailed reports as well as specific alerts to quickly react to the threat. For instance, the model can examine and deduce that the rate of UDP packets from a single source IP is out of range, even if overall thresholds are not exceeded. The SG is the heart beat of AIRMS cloud network DDoS detection. It represents a high-performance DDoS attack-mitigation device that could be deployed upstream at either the cloudservice provider data center or at the perimeter of the AIRMS to protect both the network and data center resources.

When the SG is notified that a network link or device is under DDoS attack traffic destined for the target is diverted to active treatment and possible packet discard as shown in Fig 7. In this case, the traffic is then subjected to a concurrent five-stage analysis and filtering process designed to remove all malicious traffic whileallowing legitimate packets to get to the AIRMS backend servers without any interruption.

Considering Fig. 3, the architectural components of the SPI OACI (see Fig 4) comprises the following, viz: verification, analysis, and enforcement techniques. This was used to identify and separate malicious traffic from legitimate traffic (See section III). This purification process consists of five modules or steps:

- Filtering: This block includes both static and dynamic DDoS filters. Static filters block the non-essential traffic from reaching the backend servers under attack. They are user-configurable, and come with preset default values. Dynamic filters are inserted by the other modules based on observed behaviour and detailed analysis of traffic flows, delivering real-time updates that either increase the level of verification applied to suspicious flows or block sources and flows that have been verified as malicious.
- Active verification: This block verifies that packets entering the system have

not been compromised. The SG uses numerous unique, patent-pending source-authentication mechanisms to stop spoofed packets from reaching the backend servers. The active verification module also has several mechanisms to help ensure proper identification of legitimate traffic, virtually eliminating the risk of valid packets being discarded.

- Anomaly recognition: This block monitors all traffic that was not stopped by the filter or the active verification modules and compares it to baseline behaviour recorded over time, looking for deviations that would identify the source of malicious packets. The basic principle behind the operation of this module is that the pattern of traffic originating from an attacker daemon residing at a source differs dramatically from the pattern generated by legitimate sources during normal operation. This principle is used to identify the attack source and type, as well as to provide guidelines for blocking traffic or performing more detailed analysis of the suspected data.
- Protocol analysis: This block processes flows that anomaly recognition finds suspicious in order to identify application-specific attacks, such as HTTP error attacks. It then detects any misbehaving protocol transactions, including incomplete transactions or errors.
- Rate limiting: This block provides another enforcement option and prevents misbehaving flows from overwhelming the target while more detailed monitoring is taking place. The module performs per-flow traffic shaping, penalizing sources that consume too many resources (for example, bandwidth or connections) for too long a period.

In context, between any DDoS attacks, the SG will be in learning mode, passively monitoring traffic patterns and flow for each of the different resources it protects to understand normal behavior and establish a baseline profile. This information is later used to fine-tune policies for recognizing and filtering both known and unknown attacks in real-time network activity.

C. SPI OACI DDoS Mitigation Procedure

An outline of the cloud security counter DDoS flowchart was detailed while showing the initial phase of the design with Riverbed OpenFlow software in this work. By enabling the SPI OACI firewall, the following were monitored in the AIRMS cloud network viz: link consumption of computational resources, disruption of configuration information, disruption of state information, disruption of physical network, disruption of the communication media between the firewall and its back end servers. The flow chart in Fig 4offers a complete DDoS protection solution based on the principles of detection, diversion, verification, and forwarding to help ensure total protection and mitigation. When a DDoS attack is launched against the AIRMS firewall, the cluster server network is protected by the flow as shown in Fig 4thereby maintaining business continuity. Some of the technical highlights of the SPI OACI firewall include:

- Provision of a granular firewall engine
- Provision for authentication proxy which offers a per-host access control mechanism
- Its application Inspection features additional protocol conformance while checking the network policy controls
- Greater deployment flexibility, reduce implementation timelines

It is known that common single-connection services such as Point of Presence, Telnet, Microsoft Remote Procedure Call, and other simple protocols are usually inspected by the generic capability of TCP, UDP, and ICMP inspection. However, using these inspection capabilities is simple to implement, but can limit Stateful Packet Inspection's granularity (i.e any traffic that was allowed to leave through a firewall was allowed to return because inspection created an Access Control List (ACL) can bypass entry for that traffic). However, the recursive SPI OACI can allow the creation of specific ACL bypass for only the desired traffic, as defined by an inspection list consisting of only the protocols that are explicitly permitted by an organization's network security access policy.

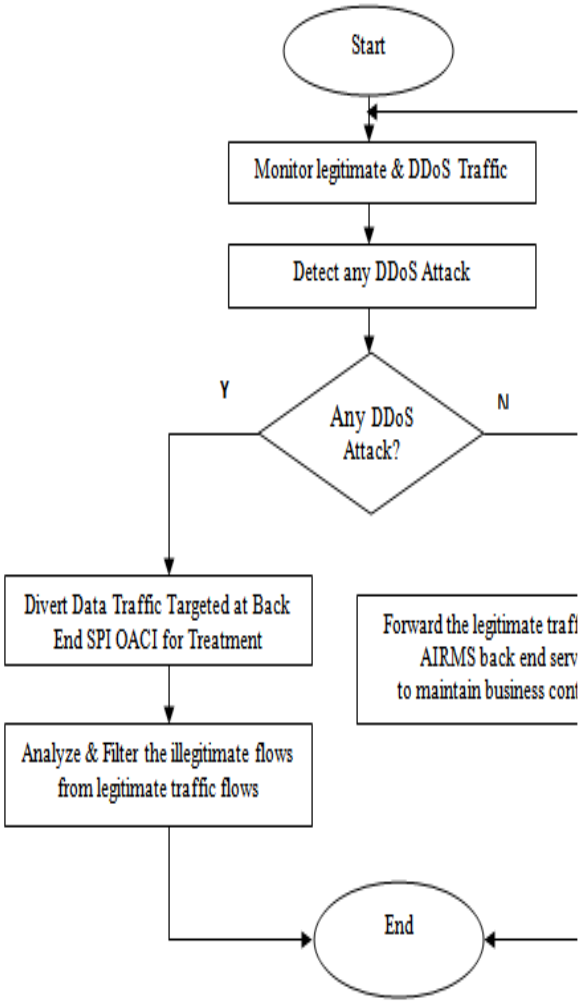


Fig. 4: A Proposed Recursive SPI OACI flow model

By analysing and filtering the illegitimate traffic flows from the legal traffic flows packets, this will prevent malicious traffic from impacting QoS performance while allowing legitimate transactions to complete appropriately.

D. Recursive SPI OACI Advantages

The SPI OACI solution shown in Fig 4 provides complete protection against all types of DDoS attacks including VBDDA as discussed in section III. The advantages include:

i. Growth: Scalability to network growth in respect of computing infrastructures. The solution offers a scalable option that eliminates any single points of failure and does not impact the performance or reliability of the existing network components
ii. Intelligence: Active mitigation capabilities that rapidly detect attacks and separate malicious traffic from legitimate traffic.
iii. Latency: It delivers a rapid DDoS response that is measured in seconds.
iv. Deployment ease: It can be easily deployed adjacent to critical routers and switches.

V. SYSTEM DESIGN

A. Experimental Design

In this paper, the core of the threat mitigation proposal is the SPI OACI device. The foundation devices of SPI-OACI are the Cisco Application Policy Infrastructure Controller (Cisco APIC) and Cisco Nexus 9000 Series multilayer Switches configured for firewalling the AIRMS servers. A characterization of the Cisco 9000 router firewall as an embedded network device with support for Virtual DDoS protection was considered in the AIRMS threat mitigation proposal. Considering Fig 3, the SPI OACI was placed adjacent to a switch on a separate VLAN network interface, helping enable on-demand protection on the backend monitoring server systems. This was positioned so as to concurrently protect multiple potential LAN server network cluster and WAN bandwidth.

For the security QoS profiling, the system response metrics (i.e. SPI-OACI delay, throughput and utilization) in cloud based network will be analysed. Using the models outlined above for the composite DDoS attack, different situations were examined. The purpose of the QoS profiling via a DDOS experiments was to distinguish the influence of different attack properties on the success of the DDoS attack and how the SPI firewall can normalize the attack scenario and protect the AIRMS. For the analysis of simulation experiments, standard situation parameters were chosen as detailed below [20] while implementing the system using Riverbed Modeller version 17.5 [32]. Table 1 shows the security cloud network design parameters.

Table 1: Experimental design Parameters

SN	Parameters	Specifications
1	Normal Traffic	20 Mbps normal traffic (100 queries per second by 200 bits in each).
2	Attack Traffic	10 Mbps attack traffic (50000 queries per second by 200 bits in each).
3	Bandwidth	2 Channels with 100 Mbps bandwidth each;
4	SPI firewall Filter	Uses filters that filter 20% of the attack and 2% of legitimate user's queries.
5	Query Time	Legitimate query takes 200 ms to execute

6	Attack Query	Execution takes 2000 ms.
7	Firewall Type	Cisco 9000 router firewall
8	SPI firewall buffer capacity	2500 and can hold information of 50 connections.

The modeler software served as the tool for predicting, measuring, modeling, and analyzing the system performance. In the work, the performance of the AIRMS cloud network was determined by network attributes that are affectedby the various components such as network media, nodes, clients, servers, server applications. From Table 1, the analysis of the network leveraged the following phases:

i. Capture packet traces when the AIRMS http service is running normally to build a baseline for QoS study. These traces are captured using the application characterization environment in riverbed modeller.
ii. Importing the capture files to create a representation of the application's transactions called an application task for further analysis.
iii. After creating the application task, the following operations are carried out over the captured traffic traces:

- Viewing and editing the captured packet traces on different windows.
- Performing application level analysis by measuring the components of the QoS metrics in terms of throughput, delay and utilization.

B. *Analysis of Results*

This study focused only on the security QoS profiling under normal traffic flow via the SPI OACI firewall device. The intent is to form an initial baseline for a comparative study in a future research. After proposing the model, some selected network QoS metrics were evaluated to ascertain the applicability of the SPI OACI. However, the difficulty of carrying out an exhaustive set of experiments in real environments, involving production AIRMS servers and real traffic must be noted at this point. This fact, together with the exhibited performance by current simulation tool, gives way to accepting this kind of software tool as valid framework for experimentation. The metrics for security QoS profiles is presented next.

- *Security QoS Profile 1: Point-to-Point Throughput*

In context, this is defined as the probability for a legitimate user to acquire a free position in the service queue during an observation period. It is related to the amount of time during which at least one free position in the service queue is available. It can serve as a measure of the efficiency considering the valid traffic pattern into the server. With the pseudo traffic generation event tool, normal traffic was generated by the configuration manager considering a typical http request on the AIRMS servers via the SPI OACI. The variable request speed not exceeding 25requests/secs was used.

Fig. 5 shows the throughput verification results. A scan be seen from the figure, the actual measured values follow a linear response for all the legitimate requests made to the server via the firewall device. The maximum value is about 8700packets/sec representing 96.66% of correctly delivered packets with respect to the trace back time which is determined by the maximum hop count between the sever and the firewall. The implication is that reliability is guaranteed besides securing the server clusters from cyber attacks.

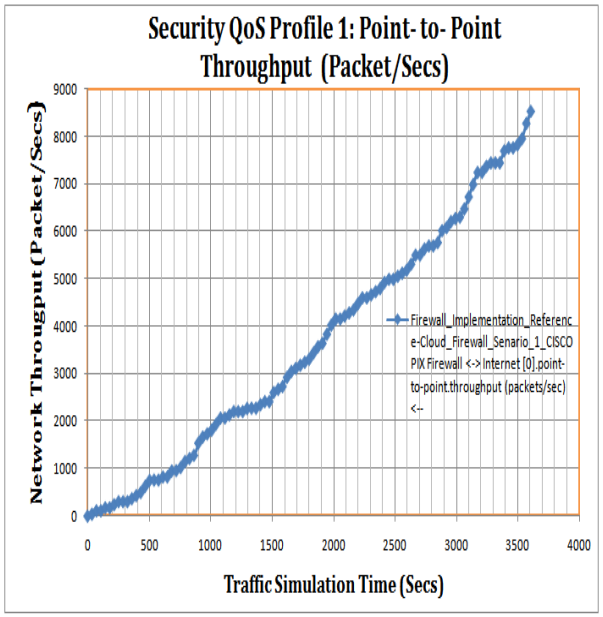


Fig. 5: Normal Traffic flow throughput (Packets/sec)

- *Security QoS Profile 2: Point-to-Point Resource Utilization*

Network utilization is the ratio of current network traffic to the maximum traffic that the port can handle [33]. It indicates the bandwidth use in the network. While high network utilization indicates the network is busy, low network utilization indicates the network is idle or less busy. When network utilization exceeds the threshold under normal condition, it will cause low transmission speed, intermittence, request delay and so on. It is know that

networks of different architectures have different theoretical peaks under general conditions. Ensuring that there is no packet loss when network utilization reaches a certain value is a basic concern.

For most networks 50% network utilization can be considered as high efficiency. By monitoring network utilization, this can aid understand whether the network is idle, normal or busy. It also helps us to set proper benchmark and troubleshoot network failures. In this research, utilization is the reciprocal of resource availability (which is the ratio between the number of legitimate user requests served by the server, and the total number of requests sent by these users). The aim of the DDoS attack is to minimize the availability of the service by increasing resource utilization beyond some specified thresholds. This task can be achieved by minimizing the client success probability, which reduces the probability of a legitimate user acquiring a position in the queue. Fig. 6 shows a 15% resource utilization response from the AIRMS network. An interesting behavior was observed by disabling the SPI OACI device. A 70% differential in the resource utilization was evidenced. In this case, the sudden transition from 15% to over 85% utilization response shows the influence of a possible Synflood DDoS attack which will normally lead to very high link bandwidth, memory and CPU utilization cycles. Fig 6 shows the measurement results in this regard. As can be seen from the figure, it shown that over a prolonger DDoS attack, the network can come to a halt.

However, by re-enabling the firewall device, the effective resource utilization was restored.

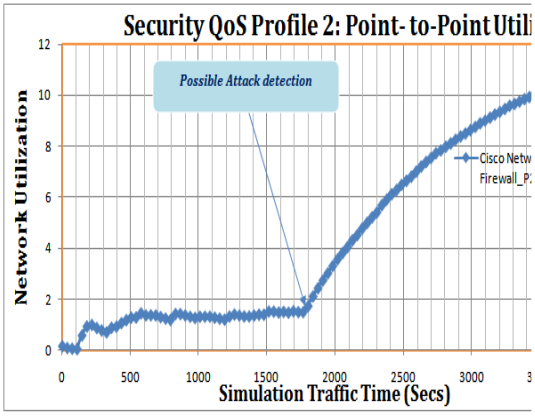


Fig. 6: Biased normal traffic flow Utilization Response

- Security QoS Profile 3: Point-to-Point Delay

This work used delay interchangeably with latency. The delay of the network specifies how long it takes for a bit or byte of data to transverse across the network from point *A* to point *B*. It is typically measured in multiples or fractions of seconds. As shown in Fig 7, the latency of the firewall device including the network delay during the normal traffic flow is about 87.5% (0.875secs). The effect is basically negligible in the context of AIRMS. However, the concern in network latencies is on how to reduce it to the barest minimum.

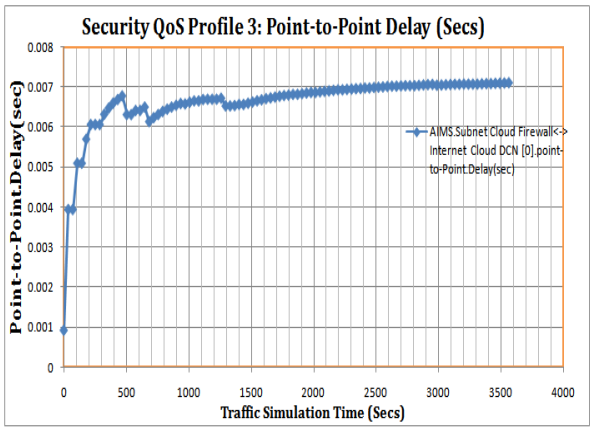


Figure 7: Normal Traffic flow delay response

Another security QoS profile deduced from the work is the effect of resource utilization on the network throughput. Essentially, an increase in utilization leads to higher throughput response. However, beyond a certain utilization threshold, the network throughput becomes very unstable leading to TCP incast collapse. The congestion caused by DDoS Incast has the effect of increasing the latency observed by the application and its users. The detrimental effect on TCP throughput caused by network congestion via incast communication patterns makes its imperative to guard against DDoS traffic at all times. All the observations made in tis phase of the work only depict the scenario for normal traffic flow via the SPI OACI device.

VI. CONCLUSION AND FUTURE WORK

This paper has dealt with security QoS metrics for legitimate traffic flow in an AIRMS cloud network system. Bandwidth exhaustion, memory depletion, CPU power drain and application crashing are the identified DDoS strategies used by cyber terrorist. In the Proposed AIRMS, Stateful Packet Inspection based on OpenFlow Application Configuration Infrastructure firewall scheme was presented as a comprehensive solution. Mathematical characterization of the VBDDA and DDoS mitigation procedure were discussed. Using Cisco 9000 router firewall as an embedded network device and the design parameters in table 1, the security QoS metrics under normal traffic flow was analyzed. It was concluded that

the absence of a robust security firewall technology can adversely affect the network QoS and expose the network to various forms of DoS attacks. R&D is currently underway on the use of SPI OACI traceback device to track down the sources ofDDoS attacks on Enterprise cloud based services like EETACP, AIRMS, etc. The roadmap for future works involves: i) Completing the design phase of AIRMS for production use, ii) applying the proposed SPI-OACI approach in DCCN smart portal [24] against various forms of DoS attacks and iii) comparing various mitigation models with the proposed SPI-OACI proposal.

In practical context, the mitigation model of the AIRMS cloud network can be enhanced by using these preventive steps as recommended for SPI-OACI based deployment. These are stated below.

- Employing SPI rate-limiting in OpenFlow firewalls which encompasses the routers, load balancers and other network perimeter devices.
- Enabling TCP SYN cookie protection.
- Testingdeployed applications and the network architecture for DoS vulnerabilities and fix them.
- Conduct regular configuration audits on the perimeter devices.
- Using updated software/firmware
- Employing updated Anti-virus and regularly checks for malware, bots on existing physical machines.
- Employing multiple hybrid cloud providers for redundancy.
- Maintaining a smart backup site for quick switch over.
- Installing and configuring network SPI-OACI monitoring systems which can use its SG to trigger an alert any time any DDoS hits the network.
- Engaging network security experts to manage the network professionally

ACKNOWLEDGEMENTS

This research was carried out as an extended work on Security of Distributed Cloud Computing Network for SGEMS EETACP project commissioned by the Department of Electronic Engineering, University of Nigeria Nsukka. We would like to express our gratitude to Engr. Prof. O.U.Oparaku for his guidance and support.

References

[1] C. C. Mann, "Smoke screening", *Vanity Fair*. (2011, December 20). Retrieved from http://www.vanityfair.com/culture/features/2011/12/tsa-insanity-201112.

[2] R. W. Poole, Jr., "Toward risk-based aviation security policy", *International Transport Forum*. (2008, December 11), Retrieved from http://www.internationaltransportforum.org/jtrc/discussionpapers/DP200823.pdf

[3] https://researchedsolution.wordpress.com/2012/02/27/protecting-airport-information-systems-against-cyber-attacks/

[4] P. K. Kerr, "Nuclear, biological, and chemical weapons and missiles: Status and trends", *Congressional Research Service. The Library of Congress* (CRS Report for Congress), (2008, February 20). Retrieved from http://www.fas.org/sgp/crs/nuke/RL30699.pdf

[5] http://www.cbsnews.com/news/hackers-force-poland-lot-airlines-to-cancel-and-delay-flights/June 22, 2015, retrieved on August 1st, 2015

[6] https://www.google.com/search?q=ranian+hackers+compromised+airlines%2C+airports%2C+critical+infrastructure+firms&ie=utf-8&oe=utf-8-IDG News Servicel Dec 2, 2014, retrieved on August 1st, 2015

[7] D. Nessi, "Are you exposed? The perils of a connected world", *Airports Council International – North America*, (2011, October 17). Retrieved from http://www.aci-na.org/sites/default/files/nessi-areyouexposed-bit.pdf

[8] Overview of cyber vulnerabilities. (n.d.). US-CERT (United State Computer Emergency Readiness Team). Retrieved from http://www.us-cert.gov/control_systems/csvuls.html

[9] G. Stoneburner, A. Goguen, and F. Alexis, "Risk management guide for information technology systems", *National Institute of Standards and Technology* (NIST), , (2002, July). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[10] D. Swan, "Assessing Primary Cyber Threats to an International Airport's Critical Information Systems", University of Maryland University College.

[11] Yong-Suk Kang, Yang-Ha Chun, Yong-Tae Shin and Jong-Bae Kim, "A Study of the Airport Model Based on Security Risk", International Journal of Software Engineering and Its Applications Vol. 8, No. 11, 2014, Pp. 67-74 http://dx.doi.org/10.14257/ijseia.2014.8.11.06.

[12] A. Marks and K. Rietsema, "Airport Information Systems—Airside Management Information Systems", In Intelligent Information Management", vol. 6, may 2014, pp. 149-156 in SciRes. http://www.scirp.org/journal/iimhttp://dx.doi.org/10.4236/iim.2014.63016

[13] C. W. Johnson, "Preparing for Cyber-Attacks On Air Traffic Management Infrastructures: Cyber-Safety Scenario Generation",

[14] K.Gopalakrishnan1, M.Govindarasu, Doug W. Jacobson, and B. M. Phares, "Cyber Security For Airports", International Journal for Traffic and Transport Engineering, vol. 3, no. 4, 2013, pp. 365 – 376,DOI: http://dx.doi.org/10.7708/ijtte.2013.3(4).02.

[15] Whitepaper- CANSO Cyber Security and Risk Assessment Guide,CANSO civil air navigation services organisation, June 2014.

[16] G. Loukas, "Defence Against Denial of Service in Self-Aware Networks", PhD thesis, Intelligent Systems and Networks Group Dept. of Electrical

& Electronic Engineering Imperial College London.

[17] B. Kurar , R. Tahboub, "Internet Scale DoS Attacks", In International Journal of Applied Mathematics, Electronics and Computers, IJAMEC, vol 3, no. 2, 2015, pp.83–89.

[18] G. M. Fernández, J. E. Díaz-Verdejo, and P. G. Teodoro, "Mathematical Model for Low-Rate DoS Attacks Against Application Servers", IEEE Transactions On Information Forensics And Security, vol. 4, no. 3, September 2009, Pp.519-529. DOI: 10.1109/TIFS.2009.2024719 · Source: *IEEE Xplore*

[19] S.S. Chowriwar, M. S. Mool, P. P. Sabale, S. S. Parpelli, N. Sambhe, "Mitigating Denial-of-Service Attacks Using Secure Service Overlay Model", *International Journal of Engineering Trends and Technology (IJETT),* vol. 8, no. 9, Feb 2014.

[20] S. Ramanauskaitė, A. Čenys, "Composite Dos Attack Model", System Engineering, Computer Technology, vol. 4, no. 1, 2012, pp. 20–26 doi:10.3846/mla.2011.05 Pp.20126

[21] M. Montanari, R. H. Campbell, K. Sampigethaya, and M. Li, "A security policy framework for eEnabled fleets and airports", *Systems Software Research Group at University of Illinois at Urbana-Champaign*. 2011, Retrieved from http://srg.cs.uiuc.edu/srg/sites/default/files/montanari_ieeeaerospace_2011.pdf.

[22] Y. Jiang, K. Zheng, Y. Yang, S.Luo, "Evaluation Model for DoS Attack Effect in Softswitch Network", Communications and Intelligence Information Security (ICCIIS), 2010 International Conference on 13-14 Oct. 2010, pp. 88 – 91

[23] A. Aissani, "Queueing Analysis for Networks Under DoS Attack", Computational Science and Its Applications – ICCSA 2008Lecture Notes in Computer Science Volume 5073, 2008, pp 500-513 .

[24] K. C. Okafor "A Model for Smart Green Energy Management Using Distributed Cloud Computing Network", Ph.D. Thesis, Department of Electrical Electronic Engineering, University of Nigeria Nsukka, *2015*

[25] Cisco IOS Firewall Design Guide, 2005, Cisco Systems Inc

[26] Cisco Application Centric Infrastructure May 2014Cisco Systems Inc.

[27] Q. Huang, H. Kobayashi, B. Liu, "Analysis of a new form of distributed denial of service attack", in *Proceedings of Conference of Information Science and Systems*. The Johns Hopkins University, 2003, March 12–14.

[28] S. M. Specht, and R. B, Lee, "Distributed denial of service: Taxonomies of attacks, tools and countermeasures", in *Proceedings of International Conference Parallel and Distributed Computing Dydtems*. San Francisco, 2004, pp. 15–17.

[29] S. Ramanauskaitė, "Modeling of SYN flooding attacks", *Jaunųjųmoks lininkųdarbai,* vol 26, no. 1, Pp. 331–335.

[30] Online: https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html

[31] Online: http://www.arbornetworks.com/.

[32] Riverbed Modeler Academic Edition release17.5 PL6.https://splash.riverbed.com/.../riverbed-modeller academic- edition-release, June 11, 2014.

[33] http://www.colasoft.com/capsa/network_bandwidth_analyzer.php. Retrieved, 9th August,2015

Economic Viability of Commercial Wireless Network in Nigeria– Prospective of IEEE 802.16

Giadom, Vigale Leelanubari
Department of Computer Science,
University of Port Harcourt,
Rivers State,
Nigeria.
vigalegiadom@yahoo.com

E.E Williams
Department of Computer Science,
University of Calabar,
Cross River State,
Nigeria.
edemwilliam@yahoo.com

***Abstract*—the growing use of hand held devices has necessitated a research into optimized ways of utilizing wireless technology to benefit the growing population of electronics devices users in nigeria. therefore the need to research into viable ways of implementing commercial wireless network that is efficient, effective and cost-advantageous without compromising profitability on the operators and regulators alike cannot be overemphasized.although commercial internet connections in nigeria is usually through the use of cdma/gsm (sim cards), this research shall dive into developing and deploying commercial wireless internet network that shall not be affected by mobility, hence a user in a high moving vehicle shall not be disconnected from the network.**

Keywords-hand held devices; optimized; CDMA/GSM, commercial; wireless network; mobility; (key words)

I. INTRODUCTION

The daily and increasing use of wireless capable devices such as smartphones, tablets, laptops, wireless enabled desktops, etc in our everyday life means a lot for the economic growth of commercial wireless network in Nigeria. Wireless Networks today are faster and the technology is more affordable with its attendant improvement in users' satisfaction, increased productivity, flexibility and accessibility. Ranging from educational environment to business places and to personal use, wireless technology enhances work anywhere, and anytime, making data review, note taking, sending and receiving emails and on the spot research convenient. This work will begin by looking at the Metropolitan Area Wide Area Network, (MAWN).

II. METROPOLITAN AREA WIRELESS NETWORK

At the heart of commercial wireless network is the IEEE 802.16 and IEEE 802.20. Metropolitan wireless Network is a set of wireless data networks that provides wireless coverage for townships, exurbs, countries, states and even nations. It is primarily advantageous to build wireless MANs for data access as opposed to building cabled network infrastructure due to cost [9]. The cost of installing and maintaining imposes a lot of overhead particularly in Nigeria where road construction is done constantly and as a result fibre cables buried along the right of ways are being tampered with thereby disrupting network connection.

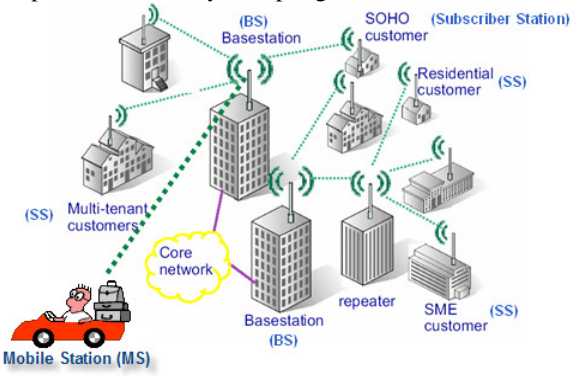


Fig. 1. IEEE 802.16 Standard WIMAX network architecture.

IEEE 802.16 is an emerging wireless family aim to provide high rate connectivity for the masses. Through the Wireless Metropolitan Area Network, IEEE 802.16 technology family is intended to provide broadband access network with a wider coverage spanning many miles [4]. It is highly expected and anticipated and it is being looked at as the next generation of wireless network technology.

Scholars foresee it as a threat to the viability of existing wireless networks like IEEE 802.11, broadband residential technologies like DSL and cable network, 3G cellular technologies etc. It has been claimed that IEEE 802.16 will be deployed with very high capacity ranging from tens to hundreds of megabytes per second (Mbps) with a long range

of coverage spanning tens of miles having strong quality of service (QoS) and supports mobility such that a user in a high moving vehicle will not be disconnected from the network. It is emerging as a very powerful tool geared towards addressing a lot of issues surrounding the problems of space spectrum.

Table 1: IEEE 802.16 Specifications.

Specification	Certifi-cation year	Description
IEEE 802.16	2001	Original specification with PHY and MAC definition for fixed broadband wireless access in the frequency of 10 – 66-Ghz frequency band
IEEE 802.16a	2003	Includes additional PHY definition for the 2 – 11 Ghz frequency band with mesh network mode of operations
IEEE 802.16c	2002	Contains system profile for 10 – 66 Ghz frequency bands
IEEE 802.16d	2004	Base for IEEE 802.16 specification combining MAC enhancement for IEEE 802.16, a and d.
IEEE 802.16e	2005	Provides support for mobility as an enhancement to IEEE 802.16d
IEEE 802.16f	2005	Manages information base for IEEE 802.16 specification

Based on table 1 specification above, vendors have developed wireless technologies particularly proprietary products adopting a variant of these specification like fixed WIMAX technology which is based on IEEE 802.16d, Mobile WIMAX base on 802.16e and proprietary PRE-MAX base on IEEE 802.16a.

III. REVIEW OF COUNTRIES ADOPTION OF IEEE 802.16 TECHNOLOGY.

Some countries have signed up to this emerging technology haven foreseen its economic viability, foremost in this regard is South Korea. South Korea has developed a country proprietary product call WIBRO, although there is no specific date of its ratification, this Korean broadband technology has been incorporated into the IEEE 802.16e standard.WIBRO (Wireless Broadband) as a product adopts TDD for duplexing, Orthogonal Frequency Division Multiple Access for multiple access and 8.75/10.00mHz as a channel bandwidth. This enables it to overcome the limitations of mobile phones with CDMA 1x and to allow for mobility to internet access. Two Korean Telecommunications companies launched a commercial service in June 2006 and the tariff was around US $30. It offers base stations aggregation of data with a throughput of 30 to 50 mbits/per carrier and cover a radius of 1-5km allowing for the use of portable devices on the internet, it provides mobility for moving devices up to 120km/h (74.5mi/h) compared to wireless LAN having mobility up to walking speed and mobile phone technologies having mobility of 250km/h.

In 2005, Germany subscribed to WIMAX with a leading telecommunication company Deutsche Breitband licensed by its Government to set up WIMAX first in Munich. It now provides services to major cities and rural areas in Germany. In Africa, AccessKenya is one of the major WIMAX network provider in Kenya, they provide wireless broadband for residential use in the cities of Nairobi and Mombase in Kenya. Similarly, in Nigeria, it is acclaimed that Galaxy wireless communications has been licensed to launch the first mobile broadband services based on IEEE 802.16e with XS broadband being a major contributor to the installation of WIMAX and currently holds license in 24 out of the 36 states in Nigeria. There are also indications that suburban telecom the largest supplier of wholesale internet solutions to Nigeria's GSM and StarTech Telecoms have begun deploying Alvarine BreezeMax 3500 a proprietary product of WIMAX in Abuja and Lagos in Nigeria.

IV. DESIGN OF WIMAX PROPRIETARY PRODUCT

Just as in the standard specification of IEEE 802.16 specification, any design of a proprietary product will follow the standard set. In the process, two aspects of the air interface are essential. These are the physical layer (PHY) and the Media Access Control (MAC) layer [4]:

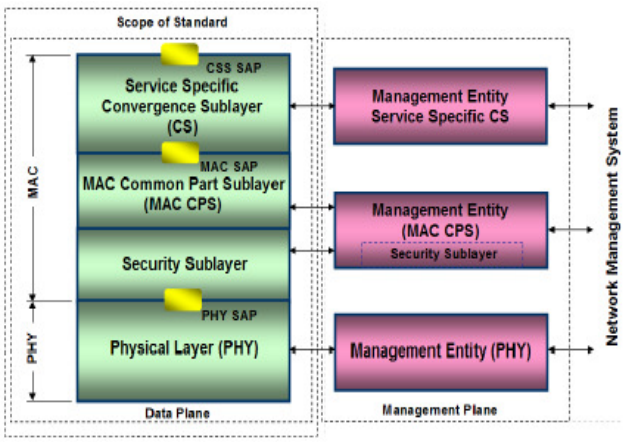


Fig. 2: Logical Architecture of IEEE 802.16

A. *PHYSICAL LAYER (PHY)*

IEEE 802.16 makes use of scalable OFDMA to carry data, support channel bandwidths ranging from 1.25MHz to 20MHz with up to 2048 subcarriers. In the event of good signal, an efficient 64 QAM coding scheme is adopted hence its support for adaptive modulation and coding, on the other hand, in the event of poorer signal, a more robust BPSK coding method is used whereas in between good and poor signal, 16 QAM and QPSK can be used. The Physical Layer (PHY) also supports features such as Multiple-Input Multiple-Output (MIMO) antennas in order to provide good Non-Line-Of-Sight propagation (NLOS) characteristics or higher bandwidth and Hybrid automatic repeat request (HARQ) for good error correction performance. It is worthy of note that IEEE 802.16 standard permits operation in bandwidth between 2 -66 GHz, best practice in mobile operation functions optimally in lower bands which are also the most crowded and expensive.

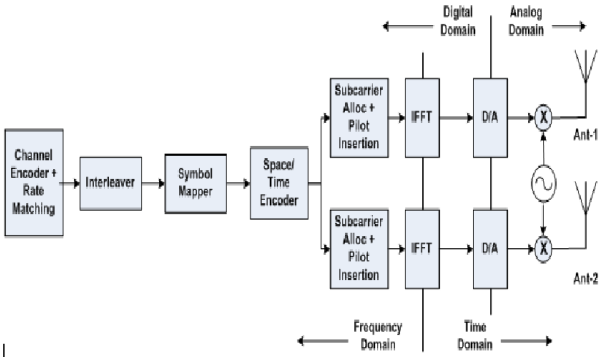


Fig. 3 Physical layer (PHY) diagram

B. Media Access Control (MAC)

In MAC design, the aim is to establish Point to Multipoint broadcast wireless access applications with the views of establishing an interface between higher transport layer and the physical layer in TCP/OSI model. Packets are transported from the upper layer to other layers. These packets known as MAC Service Data Units (MSDUs) organizes into MAC Protocol Data Units (MPDUs) for air/space transmission. The reverse is achieved in the case of data reception. IEEE 802.16 standards on my design incorporates a convergence sublayer. This layer interfaces with the other higher layer protocols like ATM TDM voice, Ethernet, IP and any future compatible protocol. It is based on the Collision Sense Multiple Access with Collision Avoidance (CSMA/CA) design for point to multipoint (PMP) applications. IEEE MAC incorporates the following features that are suitable for a range of applications and users' devices mobility.

i. Extensible Authentication Protocol (EAP) which incorporated in Privacy Key Management (PKM) for MAC layer security.
ii. Support for broadcast and multicast
iii. Primitive management
iv. Primitive higher speed handover and mobility management
v. Power management in three modes – normal operation, sleep, idle.
vi. Efficient use of spectrum through the process of header suppression, packing and fragmentation.
vii. Support for Unsolicited Grant Services (UGS), Extended Real-Time Variable Rate (ERT-VR) service, Real Time Polling Service (RTPs), Non Real Time Polling Service (NRTPs) and best effort.

These features in addition to scalable OFDMA make IEEE 802.16 suitable for high speed data bursting IP multimedia application. A fundamental aspect of WIMAX is its support for Quality of Service. This strong QoS controls work by using connection – oriented MAC architecture where all downlink and uplink connections are controlled by a sensing Base Station (BS).

The MAC sub-layer is further divided into three parts as shown in fig. 2:

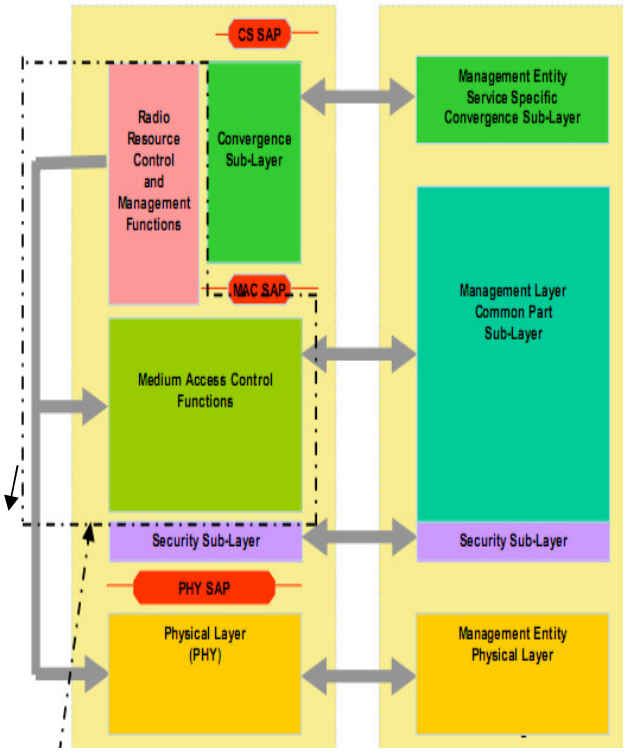
- Convergence Sub-layer (CS)
- Common Part Sub-layer (CPS)
- Security Sub-layer

The convergence sub-layer is aimed at enabling IEEE 802.16 to better accommodate higher layer protocols placed above the MAC. The IEEE 802.16 specification assumes two predominant traffic transported across the network viz: ATM, Ethernet. Therefore CS associates data received from higher layers with particular connections. By this it can perform additional process like Payload and Header Compression (PHC). The CS is separate from the other IEEE 802.16 MAC protocols enabling vendors to support developed proprietary and specialized CSs.

Central to IEEE 802.16 is a process of connection – service flow. Traffic flows are associated with connections An SS has potential multiple connections with BS where each is delineated by a Connection ID (CID). CID is 16 bits in length and allows connection totaling 64000 within each uplink and downlink channel. Associating traffic with CID depends on the classifier which is a rule set within the CS.

The Common Part Sub-layer is the central piece of IEEE 802.16 standard MAC which provides functions like duplexing, network entry and initialization, framing, QoS and channel access.

Security Sub-Layer is also referred to as the privacy sub-layer with the primary goal of providing subscribers with privacy across the wireless network and also provide operators with strong protection from theft of service.



B.

1) *Fig. 4: IEEE 802.16 MAC Reference Model*
2)
3)

V. JOINING THE IEEE 802.18 NETWORK

The following steps will be taken before an SS can join an IEEE 802.16 network:

A. Acquisition- In this case, the acquisition of downlink signal involves the SS using the last known valid operational parameters to join the network. If the signal is not found, the SS searches across the downlink channels to join.The SS need to obtain a valid uplink parameters from the UL-MAP message through:

i. The ranging process that allows stations to calibrate the performance of their PHY based on current PHY channel conditions.
ii. Optimal timing, power settings and frequency synchronization.
iii. Network entry request
iv. Authorization and encryption of the key exchange through the process of authentication and cryptography
v. Obtaining an IP configuration through DHCP.

B. The sub-channel network entry procedure may also be used to join the network through:

i. The SS choice of a particular sub-channel and sends specialized messages to the BS
ii. The sub-channelized network mitigate large contention that can take place for initial ranging and logon.

This procedure of joining the network is shown in fig. 5

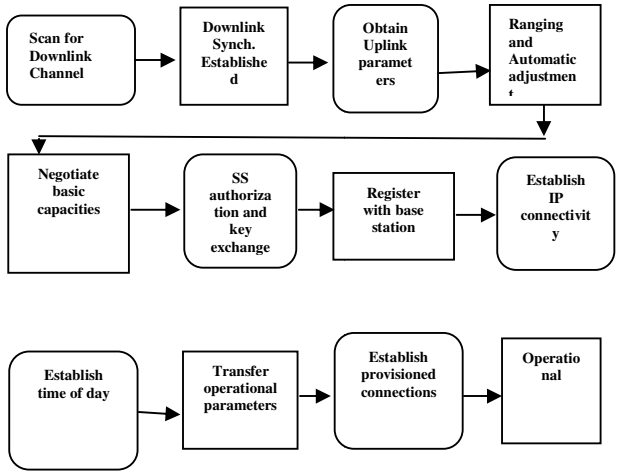


Fig. 5: Procedure for joining IEEE 802.16 network

VI. IMPLEMENTATION OF IEEE 802.16 TECHNOLOGY IN NIGERIA.

In Nigeria, it is the responsibility of the Nigerian Communication Commission to facilitate the investment into the Nigerian market for the provision and supply of communication services, equipment and facilities. This entails granting of operating licenses to interested investors in implementing proprietary IEEE 802.16 technology in the country.

First there is the need for a legal framework creating an enabling environment for IEEE 802.16 standard investors to operate, thereafter Nigeria need to be part of the IEEE 802.16 WIMAX Forum in order to benefit from its certification of proprietary products which guarantee compliance, interoperability and compatibility with other wireless broadband products. An announcement of auctioning of IEEE 802.16 standard in the relevant frequency spectrum should follow which will then attract competent vendors to key into this which in turn will yield enormous economic gains for the country.

VII. ECONOMIC VALUE OF IMPLEMENTING IEEE 802.11 TECHNOLOGY IN NIGERIA

The following benefits can be derived from the implementation of WIMAX technology in Nigera.

i. Enhancement of industrialization: The implementation of IEEE 802.16 technologies in Nigeria will in no small measure attract

industries as most industries operate with high speed internet needs.

ii. Revenue generation: By adopting IEEE 802.16 standards in implementing proprietary WIMAX products, a huge income can be generated accruing from the operators and customers alike. This will contribute to the Gross Domestic Product of Nigeria.

iii. Source of employment: The adoption of the standard will be a way of creating job opportunity for the growing number of unemployed citizens of Nigeria, as the activities of operating this standard will provide jobs.

iv. The deployment of IEEE Standard product can be an added enhancement to solving specific internal issues in the country, as the standard supports QoS multimedia. This can be used in networking surveillance cameras to fight crude oil theft and terrorism.

v. By operating WIMAX, operators will save a lot as a single station can serve hundreds of users thereby reducing the cost of multiple installation.

vi. WIMAX deployment enables faster deployment of new users as compared to wired networks.

vii. Provides a speed of 10mbps at 10 kilometres line of site. As it is standardized, the same frequency equipment should work together.

viii. Knowledge transfer: In the process of deploying IEEE 802.16 products a lot of knowledge on developing related technology shall be gain from experts from other the shores of the country thereby developing local capacity in technological advancement.

Indeed the benefit derivable in considering the deployment of IEEE 802.16 products into the Nigeria Tele-Networking space cannot be overemphasized, hence the need for the government and other stakeholders to look into this emerging area and attract its overall benefit into the country.

REFERENCES

[1] J. Burbank, “Commercial Wireless Networking Explained” APL, 2009

[2] J. Vizcaino, A. Rantala, “WIMAX: 802.16” Tampere Polytechnic, Telecommunications Engineering, 2008

[3] M. Hassan, “Performance Evaluation of WIMAX/IEEE 802.16 OFDM Physical Layer” Helsinki University of Technology, Department of Electrical and Communications Engineering, Communications Laboratory, 2007

[4] M. Seyedzadegan, and M. Othman, “IEEE 802.16: WIMAX Overview, WIMAX Architecture”, International Journal of Computer Theory and Engineering, Vol. 5, No. 5, Pgs 784 – 787, October 2013.

[5] R. Marks. “The IEEE 802.16 WirelessMAN Standard for Broadband Wirelee Metropolitan Area Networks” (US) National

[6] Institute of Standards and Technology Boulder, Colorado, USA, April 2003

[7] R. Wu, “WIMAX in China” GoingWimax, China, 2010

[8] S. Hamiti, “The Draft IEEE 802.16M System Description Document” IEEE 802.16 Broadband Wireless Access Working Group Session #55, 2008.

[9] T. Smura, “Competitive Potential of WIMAX in the Broadband Access Market: A Techno Economic Analysis” Helsinki University of Technology. Networking Laboratory, Finland, 2015

[10] O. Marcel, A. Rayolla, and C. Palanisamy, “The WIMAX PHY Layer” Digital Communication, ISBN: 978-953-51-0215-1, Intech, South Africa.

Cybersecurity Issues on Web-Based Systems in Nigeria: M-Learning Case Study

S. S. Oyelere
Dept. of Computer Science
Modibbo Adama Univ. of Tech.
Yola, Adamawa State, Nigeria
Solomon.oyelere@mautech.edu.ng

D. I. Sajoh
Dept. of Computer Science
Modibbo Adama Univ. of Tech.
Yola, Adamawa State, Nigeria
disajoh@mautech.edu.ng

Y. M. Malgwi
Dept. of Computer Science
Modibbo Adama Univ. of Tech.
Yola, Adamawa State, Nigeria
yumalgwi@yahoo.com

L. S. Oyelere
Windows Click Computers
Modibbo Adama Univ. of Tech.
Yola, Adamawa State, Nigeria
lydialuggu2005@gmail.com

***Abstract*—There is a rapid growth of the application of mobile devices as a learning aid especially in developing countries such as Nigeria largely due to affordability, interest and availability of mobile handheld devices. Though web-based learning systems such as m-learning are used nowadays to support several learning activities and learners are generally willing to use the devices for learning, cybersecurity negligence poses a huge threat to this beneficial system. This work used questionnaires and interviews survey approaches to obtain lecturers and students opinion and standpoints on the harmful effects of cybersecurity negligence on m-learning as well as possible solutions to the menace of cybersecurity threats. The results of this study identified harmful effects of cybersecurity negligence in m-learning. Also, mitigating approaches were proposed to counter cybersecurity issues on m-learning. It was recommended that appropriate plan and implementation of systems applied in web-based learning must have sufficient cybersecurity administration for m-learning platforms. This must be considered for enhanced learning, efficiency, satisfactoriness and acceptability of m-learning solutions.**

Keywords—m-learning, mobile learning, mobile device, mobile device security, m-learning security, cybersecurity, developing African country, Nigeria

INTRODUCTION

The dawn of mobile technologies such as Wireless network and mobile devices has encouraged advancement in the education sector owing to the introduction of mobile learning (m-learning). Novel digital learning platforms are designed to support the advances in mobile technologies so as to make learning ubiquitous, engaging and flexible. M-learning is richly supported by the convergence of internet and cyber technologies into a single entity called the internet-of-things. This shows the huge strength and potential of m-learning. M-learning offers the opportunity for teachers and students to communicate effectively, share learning contents and experiences anywhere, anytime by anyone. According to [1], m-learning broaden learning far beyond classrooms and help to support the 21st century learning environment. M-learning is the facilitation of learning process and access to educational resources through the use of mobile handheld devices [2]. There are numerous advantages of m-learning including supporting communication, collaboration, and increasing learner-learner, learner-teacher interactions [3]. M-learning is supporting learning in Nigeria but there are several concerns regarding the application of wireless mobile technology for education purposes that may impede its overall adoption. Most of these issues have been enumerated in several researches [4], [5], [6]. One crucial issue with m-learning is the security challenge and vulnerability of mobile devices especially cybersecurity risk. Mobile devices are vulnerable to security threats such as software attacks: virus, service denial, worms macros; hardware attacks: theft, espionage; and intellectual property attacks: copyright, piracy infringement [7]. The cyber space is the key front of most threats faced by m-learning system. Due to common use, handy and portable nature of mobile devices, they tend to be prone to software, hardware attacks and cyber attacks. The apprehension regarding cybersecurity risks and confidentiality problem in m-learning systems seems quite soaring among educators especially in developing country context such as Nigeria with enormous cybercrime, fraud, theft, copyright and internet security threat [8].

Consequently, it is expedient to investigate m-learning stakeholders' concerns regarding cybersecurity challenges. This research seeks to elicit answers to the following research questions:

i. Are there harmful effects of cybersecurity negligence to m-learning stakeholders?
ii. What are the tactical approaches to improve the cybersecurity threats facing m-learning?

The contribution of this paper is dual in nature. First, it identifies detrimental effects of the negligence of cybersecurity threats to m-learning especially in a developing country such as Nigeria. Obviously, several of these harmful situations can be identified for e-systems in general, but here effort was geared toward examining them solely under the m-learning prism. Subsequently, several strategic actions were enumerated to ameliorate the identified threats from cybersecurity. This research paper opens up a new issue with regards to the security aspect of m-learning implementation. The next section of this article review existing and related researches about cyber security and m-learning.

The rest of the work is organized as follows. Section II summarized the systematic review of research publications on m-learning security as a whole and appraised the recommendations provided in existing works. Section III presents the research methodology, highlighting the procedure of this research. Results obtained concerning harmful effects and tactical approaches to cybersecurity in m-learning were analyzed and presented in section IV. Section V presented a detailed discussion of the research outcome and offered recommendations to overcoming the ills of cybersecurity facing m-learning.

SUMMARY OF PREVIOUS RESEARCH

Cybersecurity is basically the process of ensuring the safety of cyberspace from known and unknown threats. The International Telecommunication Union states that cybersecurity is used to "summarize various activities such as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" [9]. Cybersecurity involved the malicious application of information and communication technology (ICT) either as a target or as a device by several malicious actors. Cybersecurity could also refer to the security of internet, computer networks, electronic systems and other devices [10].

According to [11], [12], [13] and [14], some activities that define cybersecurity include information confidentiality, systems integrity and computer network survivability, online contents filtering, wiretapping, call logging, and protection against cyberspace abuse.

Cybersecurity is up-and-coming but also a key concern for institutions including management information systems, information and communication systems, communication systems, health systems, essential infrastructural systems and engineering systems. M-learning, which is a sub-system to these systems is gaining tremendous popularity among educational stakeholders especially in developing countries such as Nigeria [4]. According to Oyelere, Suhonen, and Sutinen [4], "m-learning is the study and practice of using mobile devices, such as smart phones, mobile phones, tablets, PDAs, MP3s and pocket PCs in order to support learning for anyone, anytime and anywhere". The application of mobile technology makes learning ubiquitous, collaborative and flexible. Unfortunately, this learning system is vulnerable to cyber attacks. Such that one malware or virus can infect and damage an entire system and infect the other systems connected to the network [15], [16]. M-learning systems are multifaceted based on their diverse, simplicity, and pervasive possibilities. In these systems, the threat is increased, and the security concern turns out to be huge. This work is interested in beaming a spotlight on the security of m-learning platforms especially since the users of this systems are using the cyberspace. Moreover, successful learning can only take place in an environment safe from security challenges. As long as mobile devices have potentials to stimulate contemporary learning, the security challenges inbuilt in mobile devices are also found on m-learning. Even though mobile devices are to a great extent used than computers, they comprise various loopholes for attack by external forces. The essential security necessities to safeguard m-learning systems are privacy, validity, availability, data reliability, and control [6]. A broad research review and classification of relevant security and privacy issues in m-learning platforms were presented in [17]. Additionally, [17] classified security issues on m-learning systems as were taken up from e-learning systems are: security and privacy of data, avoidance of offensive activities, cloud data protection, mobile devices data protection, content filtering, and protection of copyright. The author argued that the test is about securing m-learning platforms and installing appropriate security policies and measures to identify and prevent attacks while guaranteeing data privacy, integrity, and confidentiality. Though the author presented several approaches on m-learning cybersecurity, these are applicable under European context e-learning scenario, but this research article is focused on cybersecurity threats on m-learning systems in Nigeria. The authors in [4] discovered that Nigeria possess the required infrastructure to implement m-learning, converses benefits and challenges of m-learning implementations, assessed the required features of m-learning platform and level of readiness and suitability of m-learning in Nigeria. In addition, their research proposed a cloud-based framework for m-learning. Of course security is an important dilemma to every cloud infrastructure. M-learning security issues were measured as the major impediment to its implementation in Nigeria [5]. About 70% of education stakeholders interviewed confirmed the concerned of emergent threats posed by cyber threats to data security. Though, this research is contextually relevant to this article but particular emphasis was not placed on cybersecurity threats to m-learning in Nigeria which is the major concern.

This research article will therefore, underpin cybersecurity issues as its pertain m-learning systems in Nigeria. The study will scrutinize stakeholders' concern on m-learning cybersecurity, especially, its harmful effects and proffer strategic approaches to improving the situation

RESEARCH DESIGN

In this research work, survey approach was used to obtain data from sample population of lecturers and students in computer science department and information and management technology department of Modibbo Adama University of Technology, Yola. Questionnaire was administered to both lecturers and undergraduate students. In all, 200 set of questionnaires were randomly distributed to the students and 14 questionnaires were distributed to the lecturers to obtain their opinions and standpoints on the harmful effects of cybersecurity negligence on m-learning and possible solutions to the menace of cybersecurity threats. Apart from the questionnaires, interviews were conducted random to

obtain data about the tactical solution to the identified issues. The responses from both lecturers and students that participated in the data collection process are held in total confidentiality. The respondents were assured anonymity throughout the research process. Ethical consent for conducting this research was obtained from the universities management. The data collected were analyzed and presented using frequency distributions and bar charts. Replies from the questionnaire were entered on a five-point Likert-scale: Strongly disagree, Disagree, Unsure, Agree, Strongly agree.

IV. RESULTS

The results of this research work are organized into two sections so as to present answers to the research questions:

Research question 1

Are there harmful effects of cybersecurity negligence to m-learning stakeholders?

This section identifies the harmful effects of cybersecurity negligence to the important stakeholders (lecturers and students) of m-learning systems. The questionnaire administered identified nine (9) important harmful effects of cybersecurity inattention: loss of data, loss of privacy, psychological issues, loss of confidentiality, loss of trust on education, piracy and copyright infringement, examination malpractices, poor performance, and loss of study time. Results from students response were presented in Fig. 1 while results from lecturers response were presented in Fig. 2.

Research question 2

What are the tactical approach to improve the cybersecurity threats facing m-learning?

Several interviews were conducted on both students and lecturers at random to obtain data on their opinion on the approach to improve the issues caused as a result of cybersecurity negligence. The summary of themes obtained from these interviews are summarized below:

a. Installation of anti-malware, anti-phishing, anti-virus, and firewalls on m-learning systems: most of the respondents proposed the installation of these security features to safeguard m-learning systems against cybersecurity threats. This tactical approach conforms with the study and proposal in [19].
b. Employment of trained security experts to man m-learning systems: this is one important approach noted by interviewees. They are of the opinion that though there are shortage of highly skilled ICT experts in developing countries, there is need to search and ensure that only highly skilled security experts are recruited to manage m-learning systems, servers, clouds and other infrastructures. Employment of highly trained personnel was suggested in [5].
c. Regular data and systems backup: data backup was suggested by most students and lecturers interviewed. They opined that in order to minimize the unbearable effect of cybersecurity negligence threats posed on m-learning platforms. Servers, systems and other infrastructure used for m-learning should be regularly backed-up to avoid loss of stored data and users credentials. The approach of data backup is in line with the proposal put forward in [20].
d. Data encryption and biometric protection: respondents are of the view that they are not only confronted with cybersecurity issues but other security issues such as mobile devices theft and hardware failure. They suggested data encryption to secure their communication and sensitive information on m-learning systems. Biometric protection using techniques such as facial recognition, fingerprint recognition, and digital signatures can be applied to protect m-learning platforms. This tactical approach is in position with the study in [18].
e. Cybersecurity awareness: most of the interviewed respondents also proposed that there should be broad awareness regarding cybersecurity threats posed to m-learning. They opined that awareness to m-learning stakeholders is important especially in developing country such as Nigeria to enlighten them about the dangerous risks of cybersecurity.

V. DISCUSSIONS

It is of great importance for the stakeholders especially the students and lecturers to identify the harmful effects of the negligence of cybersecurity in an m-learning systems because this will aid in ensuring optimal protection of m-learning infrastructure and efficient learning outcome.

From the results obtained, almost 93% of lecturers are of the opinion that loss of data is a foremost issue faced as a result of cybersecurity negligence while more than 78% of students share the same view. Another harmful effect of cybersecurity negligence is loss of privacy, almost 79% of lecturers are concerned about loss of their privacy due to cybersecurity whereas 68% of students identified the same issue as pertinent. Most of the respondents agreed that they are likely to experience psychological disturbance as a result of leakage of personal information through m-learning. The effect of cybersecurity issues on m-learning platform is vital to both lecturers and students. 93% of lecturers that participated in this study were of the opinion that they are affected psychologically because of m-learning cybersecurity attacks while only 63% of students share the same opinion. This study result is consistent with the results obtained in [18]. An additional side effects of cybersecurity on m-learning is the loss of confidentiality by both lecturers and students alike. 78% of the two important stakeholders believed that loss of their confidential information is a major cybersecurity consequence of m-learning. The outcome of this aspect of the

study is consistent with the work in [17] who affirmed that the trouncing of confidential information is one of the fears of lecturers in m-learning and that their confidentiality should be certain at all times. Likewise, lecturers would prefer that their identities remained confidential to avoid being victimized by unsuspected criminals who can assume lecturers' identity to accomplish nasty acts.

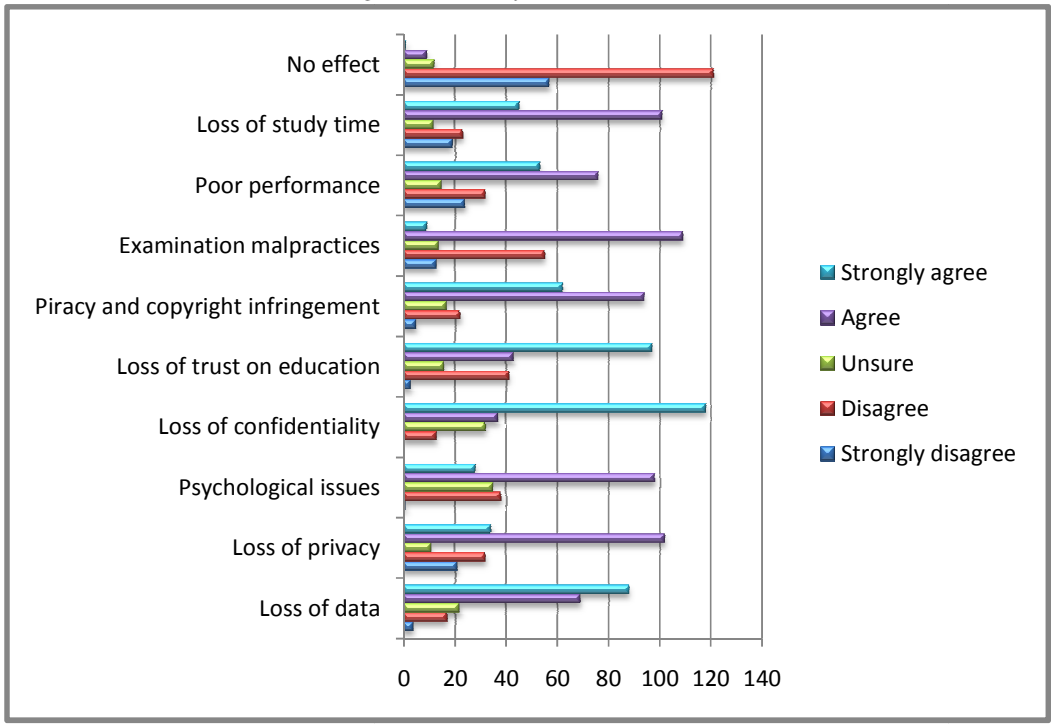


Fig. 1. Students perspectives on identified harmful effects of cybersecurity negligence in m-learning

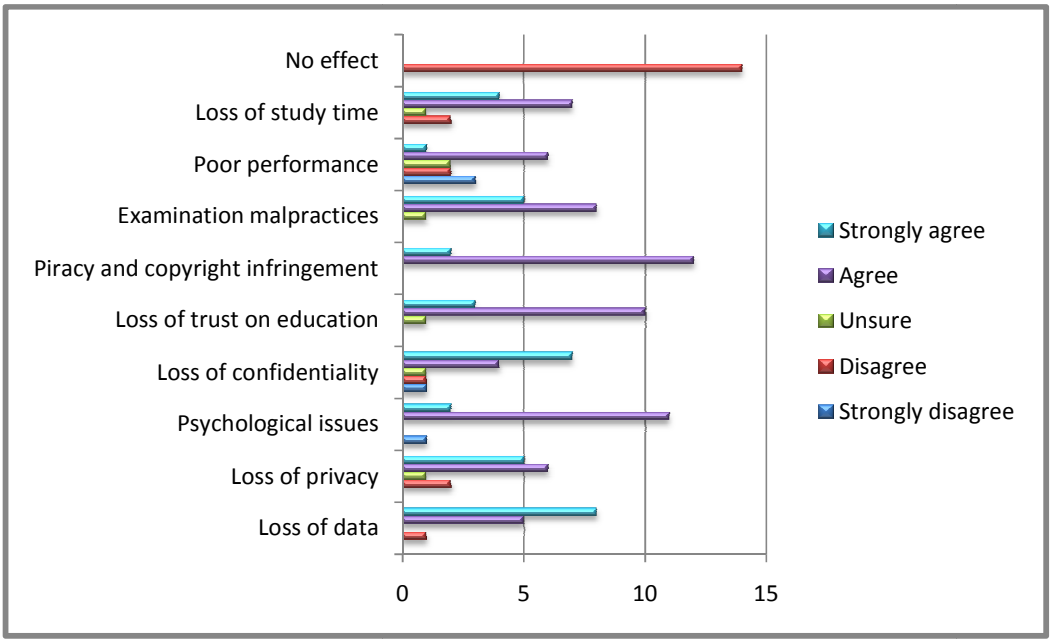


Fig. 2. Lecturers perspectives on identified harmful effects of cybersecurity negligence in m-learning

Students and lecturers agreed that they will lose trust in the education system due to cybersecurity threat on m-learning. In all, 93% of teaching staff and 70% of students have opined this view. Similarly, 100% of the academic staff have indicated that piracy and copyright infringement is a serious issue with m-learning cybersecurity threat while 78% students supported this same notion. The respondents also considered examination malpractices as one of the effects of cybersecurity on m-learning. 93% of the lecturers indicated that they lose control mainly during computer-based-test especially when exam contents have been altered leading to examination malpractices. Only 59% of learners share similar views. This result is likewise consistent with the study earlier conducted in [5], where the educators supposed that m-learning will ease examination malpractices. Once more, the findings agree with that of the work in [18] which revealed that computer-based-test done in an unsupervised or semi-supervised way is one of the intricate issues for m-learning. Another identified cybersecurity issue with m-learning is poor performance, in which 65% of students and 50% lecturers share the same opinion. Finally, loss of study time can be caused due to cybersecurity issues on m-learning system. More than 70% of both lecturers and students agreed that they lose a lot of important time on cybersecurity threats from m-learning. However, 0% of the lecturers believed that cybersecurity negligence on m-learning does not poses any harmful effect to them while only 5% students share this same opinion. The summary of themes obtained through interviews conducted are exhaustive tactical approaches that would be required to overcome negligence of cybersecurity threats facing m-learning.

VI. RECOMMENDATION

As the use of computers and as the technologies associated with computing become more powerful and ubiquitous, there is a strong possibility that cybersecurity issues will become more common. Cybersecurity must be addressed seriously as it is affecting the image of the country in the outside world. Since cybersecurity issues have discussed, especially in the context of web-based systems such as m-learning, this paper have discussed the harmful effects of cybersecurity negligence to m-learning, and presented several the tactical approaches to improve the cybersecurity pressure facing m-learning. The followings are recommendations to further alleviate the issues with cybersecurity. There is need for a combination of sound technical measures tailored to the deterrent of cybersecurity crimes, in conjunction with legal policy framework to give developing countries like Nigeria a clear stand on cybersecurity. Information attacks can be launched by anyone, from anywhere, and these attackers can operate without detection for years and can remain hidden from any counter measures unless the government and other stakeholders in the education sector agree to work together to address cybersecurity threats. This indeed emphasizes the need for the government security agencies to note that there is need to keep up with technological and security advancements. It will always be a losing battle if security professionals are miles behind the cyber criminals. Fighting cybersecurity requires an holistic approach to combat this menace in all ramifications. There is need to create a security aware culture involving the students, teachers, government, public, internet service providers, cybercafés, security agencies and other web users. Also with regards to strategy, it is crucial to thoroughly address issues relating to enforcement.

VII. CONCLUSION

This research work has been applied to recognize various threats caused on m-learning by cybersecurity negligence by stakeholders directly involved in the use of m-learning. It is certain that the students and lecturers are interested in adopting m-learning in their colleges [4].

In this study, several harmful effects of cybersecurity negligence in m-learning have been identified. Both lecturers and students expressed their view on these issues: loss of data, privacy loss, psychological disturbance, loss of confidentiality and trust on education, copyright infringement and piracy, examination malpractices, reduction in academic performance and loss of study time. These issues need to be well attended to in order to sustain the benefits of m-learning. Furthermore, since both student and lecturers are willing to adopt m-learning, it has become imperative that cybersurity must be maintained to thwart threats and attacks on learning process [18].

Some of the approaches proposed by stakeholders to reduce cybersecurity threat on m-learning are installation of cybersecurity mechanisms such as anti-malware, anti-phishing, anti-virus, and firewalls, employment of highly trained security experts to manage m-learning systems, backing-up of data and m-learning systems, installation of data encryption and biometric protection and embarking on public awareness about cybersecurity issues. Though educational stakeholders were not really concerned about cybersecurity threats posed on m-learning, but recently, these issues are importantly considered high threats especially in developing African countries. Currently,

cybersecurity in educational setting is gradually more imperative because web-based learning infrastructure and applications have become widespread. Therefore, stakeholders, most especially the lecturers and students now consider cybersecurity negligence a threat in learning systems as component of the general learning and business strategy of their establishment. Appropriate plan and implementation of systems applied in web-based learning and sufficient cybersecurity administration for m-learning platforms will transform into better learning, efficiency, satisfactoriness and acceptability of m-learning.

REFERENCES

[43] J. Sitthiworachart, and M.S. Joy. "Is Mobile Learning a Substitute for Electronic Learning?" In proceeding of: IADIS International Conference e-Learning 2008, Amsterdam. pp.451 – 458.

[44] A. Litchfield, L. E. Dyson, E. Lawrence, and A. Zmijewska, "Directions for m-learning research to enhance active learning," Proc. of the Australian Society for Computers in Learning in Tertiary Education (ASCILITE '07) - ICT: Providing choices for learners and learning, Singapore, pp. 587-596, 2007.

[45] N.Y. Asabere, "Benefits and Challenges of M-learning Implementation: Story of Developing Nations," International Journal of Computer Applications, vol. 73 no. 1, pp. 0975–8887, 2013.

[46] S.S. Oyelere, J. Suhonen, E. Sutinen, "M-Learning: A New Paradigm of Learning ICT in Nigeria," International Journal of Mobile and Interactive Learning, iJIM., in press.

[47] F. B. Osang, J. Ngole, and C. Tsuma, "Prospects and Challenges of M-learning Implementation In Nigeria: Case Study National Open University Of Nigeria (NOUN)," International Conference on ICT for Africa, February 20 -23, 2013.

[48] S.A. Shonola and M.S. Joy. "Security of M-learning System: A Collective Responsibility," International Journal of Mobile and Interactive Learning, iJIM – Volume 9, Issue 3, 2015.

[49] N.H. MohdAlwi, and I.S. Fan, "E-Learning and Information Security Management," International Journal of Digit Society (IJDS),. Vol. 1, No. 2, 2010.

[50] The Punch Newspaper. Nigeria ranked sixth in Internet security threat. [Online] Available from http://www.punchng.com/business/business-economy/internet-threat-nigeria-ranked-sixth-in-africa/ [Accessed on 18-September-2015].

[51] International Telecommunication Union (2004), "Understanding Cybercrime: A Guide for Developing Country." Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

[52] O. J. Olayemi "A socio-technological analysis of cybercrime and Cyber security in Nigeria," International Journal of Sociology and Anthropology, Vol. 6, No. 3, pp. 116-125, March, 2014.

[53] Magutu, P.A., Ondimu, G.M., and Ipu, C.J. "Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic Deployment in Kenya," Journal of Information Assurance & Cybersecurity, 2011. DOI: 10.5171/2011.618585.

[54] Nojeim, G.T. "Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace" Statement Before the Senate Committee on the Judiciary, Subcommittee on Terrorism and Homeland Security, 2009.

[55] Cybercrime Law, "Peace, Justice and Security in Cyberspace." Retrieved from http://www.cybercrimelaw.net/Cybercrimelaw.html.

[56] J. O. Odumesi. "Combating the menace of cybercrime: The Nigerian Approach" (Project), Department of Sociology, University of Abuja, Nigeria, 2006.

[57] N.H. MohdAlwi, and I.S. Fan, "E-Learning and Information Security Management," International Journal of Digit Society (IJDS), Vol. 1 No. 2, 2010.

[58] S.S. Oyelere, L.S. Oyelere. "Users' Perception of the Effects of Viruses on Computer Systems – An Empirical Research," African Journal of Computing & ICT, Vol 8. No. 1 – March, 2015.

[59] G. Kambourakis, "Security and Privacy in m-Learning and Beyond: Challenges and Stateof-the-art. International Journal of u- and e-Service, Science and Technology, Vol. 6, No. 3, pp.67-84, 2013.

[60] S.A. Shonola and M.S. Joy. "Mobile learning security issues from lecturers' perspectives (Nigerian universities case study)," Proceedings of EDULEARN'14 Conference 7th-9th July 2014, pp. 7081 – 7088, Barcelona, Spain.

[61] F.C. Obodoeze, F.A Okoye, C.N Mba, S.C. Asogwa and F.E. Ozioko. "A Holistic Mobile Security Framework for Nigeria," International Journal of Innovative Technology an Exploring Engineering (IJITEE), Vol.2 , No.3, pp.1-11.

[62] Z. F. Zamzuri, M. Manaf, Y. Yunus and A. Ahmad "Student perception on security requirement of e-learning services" 6th international conference on University Learning and Teaching, Procedia Social and Behavioural Sciences, Vol.90, pp.923-930, October, 2013.

A Cleanroom Software Engineering Approach to Development of an e-Environment System for Socio-economic Sustainability and National Security

Emmanuel Okewu
Centre for Information Technology and Systems
University of Lagos
Lagos, Nigeria
eokewu@unilag.edu.ng

Obey Haruna
Department of Geography
Nasarawa State University
Keffi, Nigeria
obbey@yahoo.com

***Abstract*—Despite ample legal instruments and institutional frameworks for the protection of the environment in Sub-Saharan Africa, the much anticipated impact on the development and conservation (protection) of the environment is still a mirage. This assertion is substantiated by the reality that inspite of these regulatory frameworks, the environment is largely degraded with negative ramifications for the twin goals of attaining sustainable socio-economic development and realization of the right to environment. Such degradation is apparent from the findings of various regional and national state of environment (SoE) reports. It is worthy of mention that almost all African countries have ratified and domesticated the various regional and subregional environmental agreement. Efforts to solve the puzzle have revealed that corruption and environmental degradation in Sub-Saharan Africa are closely linked. Financial impropriety in ecological funds management, poorly equipped environmental protection institutions, and inadequate citizens' environmental management awareness campaigns are some of the consequences of public sector corruption. Since corruption thrives in the absence of transparency and accountability, this study proposes a cutting-edge technology-based solution that promotes participatory environmental accountability using an e-Environment system. The web-based multi-tier e-Environment system will empower both citizens and government officials to deliberate online real-time on environmental policies, programmes and projects to be embarked upon. Both parties will equally put forward proposals on the use of tax payers money in the environment sector while monitoring discrepancies between amount budgeted, amount released and actual amount spent. We applied design and software engineering skills to actualise the proposed solution. Using Nigeria as case study, our research methodology comprised literature review, requirements gathering, designof proposed solution using universal modelling language (UML) and development/implementation on the Microsoft SharePoint platform. In view of our determination to evolve a zero-defect software, we applied cleanroom software engineering techniques. The outcome obtained so far has proved that the model supports our expectations. The system is not only practical, but ecologically sound. It is anticipated that the full-scale implementation of such an enterprise e-Environment system will stem the current tide of corruption in the environment sector, mitigate environmental degradation and by extension, reduce social-economic tensions and guarantee national security.**

Keywords*—*Cleanroom Software Engineering;Corruption; e-Environment;Environmental Degradation;Socio-economic Sustainability; National Security

I. INTRODUCTION

Amid concerns that climate change is the defining threat of the century, measures are being put in place globally to mitigate its effect. In Africa, humanitarian crisis linked to environmental challenges such as flash flood, desert encroachment, coastal erosion, oil spillage and gully erosion continues to be a threat to national security[1,2]. The reason not far-fetched: economic livelihoods are threatened by these ecological distortions.

The environment is of strategic imperative to Africa's quest for sustainable development. The New Partnership for Africa's Development (NEPAD) in its Environmental Initiative has acknowledged that a healthy and productive environment is a sine qua non for NEPAD in that it is critical to creating the social and ecological base upon which the partnership can thrive. Before the inception of NEPAD, African leaders had acknowledged the relevance of the environment and its resources to the continent's development and had put measures in place for its protection and conservation as confirmed by the adoption of the African Convention on the Conservation of Nature and Natural Resources in 1968 at the Algiers Convention[3]. Since then, other regional and subregional environmental agreements such as the BamakoConvention on the Ban of the Import into Africa and the Control of Trans-boundary Movement and Management of Hazardous Wastes within Africa, the Nairobi Convention for the Protection, Management and Development of Marine and Coastal Environment of the Eastern Africa Region, and Convention for Cooperation in the Protection and Development of the Marine and Coastal Environment of the West and Central African Region.

Equally at the national level, there has been actions - many environmental instruments have been adopted to protect the environment and enhance socio-economic development. Moreover, various human rights instruments in Africa have sufficiently made provision for the right to environment that ensures positive contribution to the promotion of socioeconomic development in the region as contained in article 24 of the African Charter on Human and Peoples' Rights which states people shall posses the right to a general satisfactory environment favourable to their development.

It is worthy of mention that almost all African countries have ratified and domesticated these charters. For example, section 24 of the South African Constitutions provides that everyone has the right to an environment that is not harmful to their health or wellbeing as well as have the environment protected for the benefit of present and future generations through reasonable and secure ecologically sustainable development and use of natural resources while promoting justifiable economic and social development.

Despite these legal instruments and institutional frameworks for the protection of the environment, the expected impact on the conservation or protection of the environment in Sub-Saharan Africa has not been felt as evidenced by the fact that even in with the presence of these regulatory frameworks, the environment is hugely degraded with negative repercussions for both the attainment of sustainable development and realisation of the right to environment. Empirical evidences of monumental degradation are found in various regional and national state of environment (SoE) reports such as the 2003 Kenyan SoE, and the 2006 South African SoE.

Since it has been established that the problem of environmental degradation and associated non-realization of the right to environment in Africa is not as a result of absence of regulatory frameworks, we therefore beamed our searchlight somewhere else. As alluded to in the literature by some authors, corruption exists in Africa [4] and it has continued to aggravate environmental degradation in Africa [1].Mismanagement of ecological funds, poorly equipped environmental protection institutions, inadequate citizens' environmental management awareness campaigns are some of the consequences of public sector corruption. Bribes and backroom deals don't just steal resources from the public coffers, they undermine environmental justice and economic development, and provide grounds for social tension and national insecurity. Based on expert opinion from around the world, Transparency International, the global coalition against corruption, in its 2014 Corruption Perceptions Index measured the perceived levels of public sector corruption worldwide and came up with an alarming picture of African countries. Though globally, not one single country got a perfect score and more than two-thirds scored below 50, on a scale from 0 (highly corrupt) to 100 (very clean), the fact that 92% of African countries scored below 50 is a pointer to the phenomenal corruption in the region[5]. Corruption is a problem for all countries. A poor score is a sign of widespread bribery, lack of punishment for corruption and public institutions that don't respond to citizens' needs. While countries at the bottom of the index need to adopt radical anti-corruption measures in favour of their people, countries at the top of the index should make sure they don't export corrupt practices to developing countries [5].

This article aims to proffer a technology-based approach to tackle the problem of corruption-induced environmental degradation in order to enhance environmental sustainability and national security in Sub-Saharan African countries. Our strategy is to provide participatory environmental accountability forum through an online real-time e-Environment system that is web-based. This is against the background that corruption thrives in the absence of transparency and accountability[4]. The solution empowers the citizenry and government to engage in constructive discussions on how public finance for the environment sector is utilised. It is a confluence for all environment stakeholders to cross-fertilise ideas on appropriate policies, programmes and services that would best serve the ecological governance of their country. With e-Environment, financial prudence in the public sector is promoted, fiscal discipline entrenched, corruption levels are checked and resources freed up to cater adequately for the protection of the environment and realisation of the right to environment.

Typically, countries in Africa share alot in common in terms of environmental structure, practices and operations, but still have their peculiarities. This scenario implies that a reuse-based approach to modelling and developing software that will be relevant to several countrieswith minimal errors would yield considerable benefits. Cleanroom software engineering (CSE) is a virtual error-free model of developing software where processes and environments are thoroughly scrutinized, controlled and monitored for possible defects[6,7].In the event a defect is found, it is classified to ascertain which process failed and how the failure can be prevented. The faulty process is amended and rerun while the original product is discarded. In CSE, unit testing is not required [8] and this implies reusable components from tested and trusted vendor products that engenders users and developers confidence are used[9,10].

This article reports a study of the use of CSE for developing an e-Environment system for Africa using Nigeria as test bed. It empirically investigates the link between corruption, environmental sustainability and national security that some authors have alluded to in the literature [11, 2,.3]. However, not many reports on empirical application of CSE in industrial settings have been found in the literature. Kaur [12] and Selby et al.[13] argue that the cleanroom software engineering research community is in need of more industrial experiences and empirical studies. In addition, the calls for papers of the foremost International conferences in the area of cleanroom software development such as the International Conference on Software Engineering Practices, and the European Industrial Symposium on Cleanroom Software Engineering have in recent memory, advocated the need for more case studies in CSE. Thus, as a contribution, this work seeks to enrich the existing body of knowledge in cleanroom software engineering by reporting on a unique industrial experience of CSE from Nigerian. This is particularly

significant in that rarely does one come across reports of empirical studies of application of technically sophisticated software engineering concept like CSE that originates from the African region.

The remainder of this paper is made up of the following: Section 2 gives the background of study and related work; Section 3 presents the methodology and the selected case study; section 4 focuses on results and discussions; and finally, the paper is concluded in section 5.

II. BACKGROUND AND RELATED WORK

A. Climate Change in Africa

Climate change in Africa refers to aspects of climate change within the continent of Africa. Contributing, Schneider et al. [14] stressed that Africa is likely to be the continent most vulnerable to climate change. The same sentiment was shared by Boko et al. [15]who forecasted that in many African countries and regions, agricultural production, food security and water stress would likely be severely compromised by climate change and climate variability.

In East Africa, the worst drought in many years was experienced in 2011 owing to interrupted seasonal rains for two seasons in a row. Overtime in many areas within the region, the precipitation rate during the rainy season has dwindled considerably with less than 30% of the average rainfall for the time period 1995 - 2010. In 2012, researchers found a connect between the region's low rainfall and changes in the sea surface temperature of the tropical Pacific Ocean, which they explained was mainly responsible for the disruption of the long rains. This unique discovery is already aiding improved forecasts and emergency preparedness.

The Sahel region is also suffering from climate change vulnerabilities and environmental risks. It is reported that 15 per cent of Sahel region population experienced a temperature increase of more than 1°C from 1970 to 2010. Equally, the mean seasonal rainfall is also below the long-term average, and flooding has increased in frequency and severity. Since 1985, 54 per cent of the population has been affected by five or more floods in the 17 Sahel region countries. Just in 2012, severe drought conditions in the region were reported. Regional governments responded swiftly, launching strategies to address the environmental challenge.

B. Corruption Incidence and Measurement in Africa

As observed by Okewu and Okewu [4], in order to manage corruption successfully in Africa, there is need to understand its depth and breadth. The menace is real and of monumental threat to the socio-political and socio-economic development of the continent. Against the backdrop that measuring corruption will enable us to manage it more effectively and efficiently in the context of environmental justice, we measured corruption incidence in Africa for a period of 3 years (2012 - 2014) relying on data from the global corruption perception index by the global corruption watchdog, Transparency International. Our findings indicate that Africa is the poster child for corruption and poor governance. Of the 175 countries measured for the 3-year period, data clearly indicates that vast majority of African countries were at the bottom of the table, a segment classified as highly corrupt. Table 1 is a summary of the corruption perceptions index 2014 by region measured on a scale of 0 (highly corrupt) to 100 (very clean).

TABLE 1. CORRUPTION PERCEPTIONS INDEX 2014 RESULTS BY REGION

Region	Average score	Top (Cleanest country)	Bottom (most corrupt country	% of countries that scored below 50
Americas	45	Canada (83)	Haiti, Venezuela (19)	68%
EU and Western Europe	66	Denmark (92)	Greece, Italy, Romania (43)	16%
Sub-Saharan Africa	33	Botswana (63)	Somalia (8)	92%
Eastern Europe and Central Asia	33	Georgia (52)	Turkmenistan (17)	95%
Middle East and North Africa	38	United Arab Emirates (70)	Sudan (11)	84%
Asia Pacific	43	New Zealand (91)	North Korea (8)	64%

Source: Transparency International Corruption Perception Index 2014

As shown above (Table 1), there is ample statistical evidence that Sub-Saharan Africa is among the most corrupt regions in the world, having tied with the Eastern Europe and Central Asia region on average score of 33 with 92% of its countries scoring below 50. Even then, one of the most corrupt nations, Somalia, is in Sub-Saharan Africa tying with only North Korea at a corruption score of 8. Of the 175 countries gauged in 2014, Denmark emerged the cleanest with score of 92.

To corroborate these statistics and global perspective with ground-level perspective, virtually all institutions in Africa ranging from legislature to judiciary are under the yoke of corruption and mismanagement of public resources [4]. A case in point: despite the pervasive poverty in African countries like Nigeria and Kenya, the cost of governance is high. In a comparative study, Tom and Attai [16] provided statistical evidence as shown in Table 2, comparing the emoluments of legislators and their minimum wages in six countries, Nigeria and Kenya inclusive.

TABLE 2. COMPARISON OF LEGISLATORS' PAY IN SIX COUNTRIES

Country	Legislators' pay monthly	Legislators' pay annually	Minimum wage monthly	Minimum wage annually	% of legislators' pay that is minimum wage
Nigeria	Senate N15.2m Reps N10.6m ($69,533)	Senate N182m Reps N127m ($834,402)	N18,000 ($118.15)	N234,000 ($1,536) inclusive of 13th month salary	0.13% 0.18%
India	N305,058 ($1,999)	N3.7m ($23,988)	Varies from state to state, sector to sector	-	-
US	N2.2m ($14,500)	N26.5m ($174,000)	N191,667 ($1,257)	N2.3m ($15,080)	8.6%
UK	N1.3m ($8,686)	N15.9m ($104,228)	N283,333 ($1,883)	N3.4m ($22,597)	21.68%
Sweden	N1.2m	N14.1m	Set by annual collective bargaining deal	-	-
France	N1.02m ($6,754)	N12.3m ($81,951)	N275,433 ($1,805)	N3.3m ($21,664)	26.73%
Kenya	N2.2m ($14,543)	N26.7m ($175,000)	N10,534 ($6,917)	N126,413 ($830)	0.4%

It is disturbing, if the excerpt above is anything to go by, that politicians in Africa (Nigeria and Kenya) compared to their counterparts in developed societies have positioned themselves to get stinkingly rich while the masses get impoverished by poverty. It is instructive to note that only 0.47% and 0.13% (0.18%) of legislators' pay constitute minimum wage in Kenya and Nigeria respectively while it is 8.6%, 21.68% and 26.73% in US, UK and France respectively. Juxtaposing these statistics with those of Transparency International in 2014 corruption index, we observed that Nigeria and Kenya respectively occupy distant 136 and 145 out of the 175 countries measured. Since, these legislature pay structures don't reflect the economic realities of these African countries, it is safe to say that politics in Africa favours political officials to the detriment of the masses. Little wonder then that would-be political office holders would do anything, including corrupt practices, to secure position at all cost. And once there, they explore and exploit public sector finance, including ecological funds, for personal aggrandizements. An inclusive dialogue platform such as the e-Environment system that empowers the masses to air their concerns on environmental budgets, policies, programmes and services will certainly checkmate these fiscal excesses.

To substantiate the sentiment in some quarters that corruption has assumed the status of a culture in Africa, both the highly and lowly placed citizens engage in the practice with impunity. Overtime, the weakening of institutions has made things worse as prosecution of offenders is now a mirage. Nonetheless, the judicial system, home and abroad, has been instrumental in bringing to book some high profile corruption cases in Africa. This situation calls for urgent measures to get Africa out of the woods. One of such measures we proposed in this study is the technology approach (e-Environment) which provides a technique of enhancing participatory environmental accountability in ecological governance.

C. Cleanroom Software Engineering

One of the doctrines of cleanroom software engineering (CSE) is ensure virtual error-free software by eliminating unit testing as much as possible [6,17,18]. Hence, six-sigma (highly quality) software could be achieved by focuing on design and coding. One practical way to achieve this is to use tested and trusted components from established vendors [9] such as embedded in Microsoft SharePoint [10].Cleanroom software engineering is a metaphor derived from integrated circuit manufacturing. Large-scale integrated circuits must be manufactured in an environment that is free from dust, flecks

of skin, amoebas, among other things. The processes and environment are carefully controlled and the results are constantly monitored. When defect occur, they are considered to be defects in the process and not in the product. These defects are characterized to determine the process failure that produced them. They are corrected and rerun. The product is regenerated. The original defective product is not fixed, but discarded[7, 17].

The cleanroom software engineering philosophy is similar to the integrated circuit manufacturing cleanroom process. Processes and environments are meticulously controlled and are monitored for defect. Any defects found are considered to be defect in one or more of the processes. For instance, the defect could be in the specification process, the design methodology, or the inspection techniques used. Defects are not considered to be in the source file or the code module that was generated. Each defect is classified to determine which process failed and how the failure be prevented. The failing process is corrected and rerun. The original product is then discarded. As a result, the life cycle of a cleanroom project differs from the traditional life cycle. The traditional 40-20-40 postinvestigation life cycle consist of 40% design, 20% code, and 40% unit testing[8]. The product then goes to integration testing. But cleanroom uses an 80-20 life cycle (80% for designing 20% for coding). The unexecuted and untested product is then presented to the integration testing and is expected to work. If it doesn't work, the defects are examined to determine how the process should improve. The defective product is then discarded and regenerated using the improved process. Hence, unit testing is conspicuously absent in cleanroom software engineering [9].

D.Innovative System and Inclusive Environmental Protection and Development

Sustainable protection and development of the African ecosystem should be collective responsibility of government and the citizenry alike. In this light, a major consideration is a platform that drives real-time dialogue between leaders and the led such that public expenditure on proposals and implementations of environmental initiatives should be well scrutinized for fiscal discipline in the environment sector. Our proposal of a web-based online real-time e-Environment system is part of efforts to deploy innovative system for inclusive environmental protection and development. It is anticipated that e-Environment will empower government ministries, departments and agencies (MDAs) on one hand and the citizenry on the other hand to have fruitful deliberations on how environmental budgets such as ecological funds should be spent. Besides the conversation, it will provide a monitoring and compliance scheme such that citizens able to monitor discrepancies between amount budgeted, amount released and actual amount spent on environmental management programmes. This way, endemic corruption in the sector can be mitigated if not eliminated.

C. Related Work

Some of the previous efforts that are related to corruption and environmental management in Africa in the literature are presented as follows.

Ewharieme and Cocodia [1] x-rayed urban development in Nigeria vis-a-vis ecological governance with particular focus on the Niger Delta region reputed for its environmental degradation struggles. The authors noted that owing to the centrality of oil in thepolitical economy of Nigeria's Niger Deltaover the years, there has been so much emphasis on issues of environmental degradation relating to oil. But they observed that besides oil, corruption has aggravated the situation, wrecking havoc on the environment and making the oil-induced environmental assaults worse.The paper also examined how issues such as ecological menaces are being handled and the role corruption plays in leaving them unaddressed.Despite providing linkages between corruption and worsening environmental degradation in Nigeria, the study fell short of suggesting how ICT could be used to tackle environmental challenges in a bid to guarantee national security. This is the chief motivation for our study.

Vuuren [19] studied the nature and degree of corruption in South Africa. Though South Africa has successfully developed laws and institutions that have formulated a response to instances of corruption at a national level, the law is applied inconsistently and corruption fuels already high levels of economic inequality. The study observed that levels of corruption are peaking and elite networks within government and business are deeply compromised. The author posited that South Africa is a state with a functioning democracy but with elements of the political elite that have anti-democratic tendencies. These elements do not launch a direct attack on democratic institutions, but rather seek to undermine them by ensuring that the rule of law is applied inconsistently and a climate of uncertainty exists within management of public institutions.It is not only the state that has been complicit in corruption; recent revelations of collusion and cartel behaviour suggest that the problem is equally acute in the private sphere of the economy. Despite the lack of leadership in tackling corruption within the public and private sector, civil society organizations employ different methods to tackle corruption, such as using the courts (benefitting from an independent judiciary), public advocacy, and protest. The answers to South Africa's problems do not lie in institutions alone—they can only succeed if society remains open, and if corrupted elite networks are challenged. Failure to do so will only serve to deepen inequality and allow anti-democratic tendencies to prosper. It is worth mentioning that our proposal for an e-Environment solution is to drive open and online real-time conversations between citizens and government officials on how public finance is utilized with particular reference to the environment sector.

Kakonge [11] focused on the challenges confronting the internalization and institutionalization of Environmental Impact Assessment (EIA)process.Amid concerns that environmental planning is yet to gain ground in Sub-Saharan Africa, the author stressed that SSA countries are to adapt and benefitfrom the Environmental Impact Assessment (EIA)process. A number of issues that have hindered full utilization of the EIAprocess were outlined as limited public participation, lack of national expertise andexperience in EIA, unreliable and inadequate data, limited impact coverage, defectiveenvironmental legislation, and weak enforcement. Measures to correct the situation were highlighted as expanding ownership of EIA, ensuring compliance with international agreements, improving funding of EIA studiesfor government funded-projects,

encouraging public sensitization to demystify the EIAprocess, reducing corruption, and enhancing good governance. In conclusion, the researcher advised that greater efforts andmore resources would be required to integrate EIA at all levels of the developmentplanning process, so that full benefits can be realized. Though the study did not highlight the role of ICT in environmental planning, the author agreed that corruption impacts on environmental impact assessment.

Amechi [3] approached the subject from a legal point of view, emphasizing the link between the environment and sustainable development.The article proffered a holistic or integratedapproach to tackle the problem of environmentaldegradation in a bid to enhance realization of the rightto environment and overall sustainable development in Sub-Saharan Africa. Factors responsible for environmental degradationin the region were outlined and some recommendations made on how theinternational community can help Sub-Saharan Africancountries in protecting their environment and enhancingthe realization of the right to environment in the region. The author was motivated by the fact that despite Africa's many legal instruments as wellas institutional frameworks for the protection of theenvironment, the desired effects on the conservation or protection of the environment in sub-Saharan

Africa has not been felt. This is evident by the fact that Africa's environment is heavily degraded as apparent from the findings ofvarious regional and national state of environment (SoE) such as the 2003 Kenyan SoE, and the 2006 South African SoE. Although the study did not suggest a technological solution for dealing with environmental degradation, it drew a link between ecological governance, economic sustainability and national security.

Akokpari [2] opined that human insecurity has reach high levels in Africa, especially Sub-Saharan Africa.Apart from having large portion of its population living below poverty line, the continent is bedevilled with conflict and instability. In addition, Africa has high disease burden even as food and nutritional inadequacies have reached phenomenal proportions. The continent remains vulnerable to drought, even as environmental degradation is on the increase as typified by deforestation, desertification, soil erosion, oil spillage, pollution, and depleting fish and game stocks. The paper added that ecological problems in Africa are made worse by inability of African governments to establish credible environmental regimes coupled with their willingness to trade the environment for scarce foreign exchange. The combination of all these factors presents Sub-Saharan Africa as an indisputable region for human insecurity. The study sufficiently drew a connect between environmental injustice and national (human) security even though it was silent of role of ICT in entrenching ecological governance.

Head [6] shared practical experience from the application of cleanroom software engineering (CSE) at Hewlett-Packard (HP). The paper confirmed that CSE has demonstrated ability to produce software in which the user finds no defects and its application in a typical HP environment achieved remarkable results. The author emphasized that CSE is possibly the easiest methodology and most repeatable technique of all software development methodologies to produce six-sigma (high quality) software. CSE was developed at IBM Corporation's Federal Systems Division in early 1980's. Although the six-sigma measure was initially applied only to hardware reliability and manufacturing processes, it has been realized it could be applicable to software quality. The six-sigma value is put at 3.4 parts per million (3.4 ppm) defective and the philosophy is that long-term reliability requires more robust design so that the emergent product can endure the stress of use without failing. Despite sharing industrial experience of using CSE, it was not applied in an African context to tackle the problem of ecological degradation, socio-economic sustainability and national security.

In a nutshell, none of the reviewed literature focused on applying CSE to resolving corruption-driven environmental degradation for socio-economic sustainability and national security . We therefore instituted a study in this regard.

III.METHODOLOGY - CLEANROOM SOFTWARE ENGINEERING FOR THE E-ENVIRONMENT SYSTEM

The study used Nigeria as a test bed since environmental degradation is real in Nigeria, particularly in the Niger Delta region [1] and its nature and scale are a microcosm of Africa's ecological challenges.It is on record that by the establishment of the Federal Environmental Protection Agency (FEPA) in 1988, Nigeria became the first African country to establish a national institutional mechanism for environmental protection.Prior to the dumping of toxic waste in Koko village, in Delta State, in 1987, Nigeria was ill-equipped to manage serious environmental crisis, as there were no institutional arrangements or mechanisms for environmental protection and enforcement of environmental laws and regulations in the country.
In the aftermath of the Koko toxic waste scam, the Federal Government promulgated the Harmful Waste Decree 42 of 1988, which facilitated the establishment of the Federal Environmental Protection Agency (FEPA) through Decree 58 of 1988 and 59 (amended) of 1992.
FEPA was then saddled with the responsibility for environmental management and protection. FEPA has since metamorphosed into National Environmental Standards and Regulations Enforcement Agency (NESREA), a parastatal of the Federal Ministry of Environment.
With the understanding that Nigeria's environmental experience could represent in microcosm the African ecological experience, we used the country as case study and industrial experience. We developed the e-Environment system and tested it.The proof of technology was done using Microsoft SharePoint while the underlying theoretical framework was cleanroom software engineering (CSE) with real-life environmental data from Nigeria to enhance confidence in our work [8,9]. Guided by the CSE life cycle activities (specification, development and certification), the study progressed. We reviewed literature, gathered

requirements, designed the proposed solution using universal modelling language[20], developed and implemented it on the Microsoft SharePoint platform. We then verified and validated the solution and discussed our findings . Fig. 1 is the visual version of our research methodology.

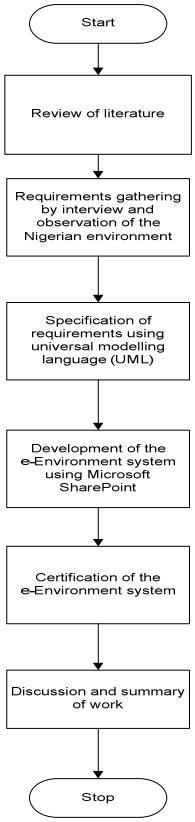


Fig. 1. Visual version of the research methodology.

A. Specification

Requirements gathered, analyzed and system modeled using universal modelling language (UML).The researchers gathered requirements and summarized the cross-cutting functional requirements of the proposed solution in Table 3.

TABLE 3. CROSS-CUTTING FUNCTIONAL REQUIREMENTS.

Req. ID	Requirement	Brief Description
R01	Add environmental information	The system shall allow authorized users to add environmental information to the database depending on assigned rights and privileges.
R02	Access environmental information	The system shall allow authorized users to access environmental information from the database in accordance with assigned rights and privileges.
R03	Edit environmental information	The system shall allow authorized users to edit environmental information on the database in line with assigned rights and privileges.
R04	Delete environmental information	The system shall allow authorized users to delete environmental information from the database contingent upon rights and privileges assigned.

The deployment diagram for the proposed e-Environment solution is shown in Fig. 2. Users can view outcome on personal computer (PC) and third party tool such as phone.

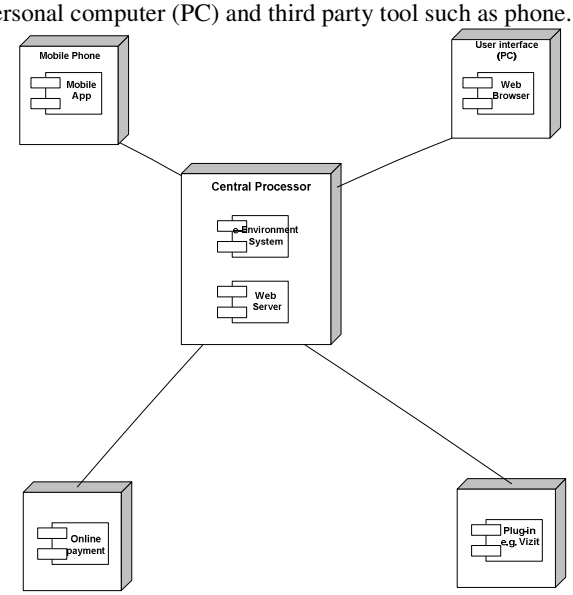


Fig.2.e-Environment deployment diagram.

It is anticipated that inspite of environmental awareness campaign and government regulation and enforcement system, some citizens may default and would be sanctioned by way of paying fines. We therefore included an online payment component as shown above. This way, defaulters can make payment online real-time directly to appropriate and authorized accounts operated by environmental agencies like NESREA.

B. Development

Microsoft SharePoint was used as the development platform. This against the backdrop that reusable components from an established vendor product that is well tested and trusted promotes confidence of users and developers [9,10] that the proposed solution would be virtually error-free in tandem with the ideology of cleanroom software engineering [12, 17]. Fault eradication apart, integrating reusable components in the development effort fast-tracks software development. Also, the web-based multi-tier clustered architecture of Microsoft SharePoint supports quality requirements and emergent properties of the e-Environment system - usability,

availability, reliability, fault tolerance, maintainability, among others [8].
Ahead of development and implementation on the web-based n-tier Microsoft SharePoint development platform, we evolved an algorithm for the proposed system.The e-Environment algorithm is as follows:

```
Procedure addEnvironmentServicesInfo()
environmentServicesInfo ← " "
  while (not endOfEnvironmentServicesInfo())
environmentServicesInfo ← addInput()
return(environmentServicesInfo)

Procedure accessEnvironmentServicesInfo()
  while (not endOfEnvironmentServicesInfo ())
  getInfo(environmentServicesInfo)
return

Procedure editEnvironmentServicesInfo()
  while (not endOfEnvironmentServicesInfo ())
  getInfo(environmentServicesInfo)
  editEnvironmentServicesInfo()
return(environmentServicesInfo)

Procedure deleteEnvironmentServicesInfo()
  while (not endOfEnvironmentServicesInfo())
  getInfo(environmentServicesInfo)
  deleteEnvironmentServicesInfo()
return(environmentServicesInfo)
```

The e-Environment software architecture pattern is presented as n-tier architecture and the visual overview is shown in Fig.3.

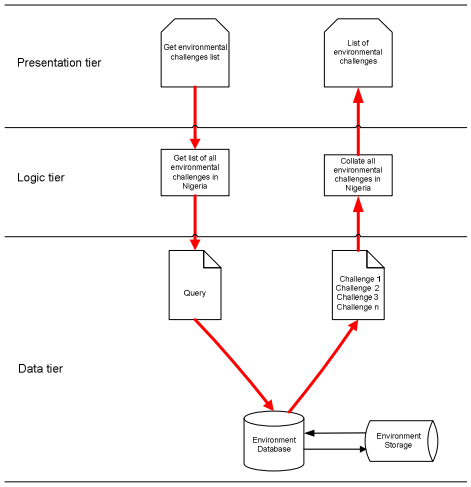


Fig.3. Visual overview of the 3-tiered e-Environment architecture

In consonance with the requirements of six-sigma and CSE for robust design so that product can endure stress of use without failing [6] , the e-Environment architecture is a clustered architecture with clustered application servers and clustered database servers. In this instance of the e-Environment architecture, they are three layers, hence n = 3 and we have a 3-tier architecture as explained in the Table 4 below.

TABLE 4. E-ENVIRONMENT ARCHITECTURE EXPLAINED.

SN	Tier	Explanation
1.	Presentation tier	The top-most layer of the application is the user interface. Its key function is to translate tasks and results to something environment stakeholders can understand.
2.	Logic tier	This layer articulates the application, processes commands, take logical decisions and evaluations, and performs calculations. It equally moves and processes data between the two surrounding layers.
3.	Data tier	At this level, information is stored and retrieved from an environment database or file system. The information is then passed back to the logic tier for processing, and then ultimately back to the user.

C. Certification

To verify and validate the e-Environment architecture, a prototype was developed using Community Site component of Microsoft SharePoint. The web-based solution was then tested using real-life interactive sessions between stakeholders. As the name implies, the Community Site component facilitated online real-time conversationsamong environment stakeholders. Test scenarios were presented where service users (requesters) sought for information from the service providers housed in the service registry. To underscore the dynamic collaboration philosophy of the e-Environment system which encourages real-time exchange between information users and providers, the prototype ensured that information was provided on real-time basis. This confirmed that e-Environment is a not only web-based, but also service-oriented. Put in another fashion, service users were able to access service providers warehoused in the service registry of the e-Environment system [21].

IV. RESULTS AND DISCUSSION

Concerned about the impact an innovative system such as e-Environment could make in the effort to entrench fiscal discipline in public expenditure on environmental management initiatives, conducted a test run and assessed the outcomes. The researchers evaluated possible threats to results obtained.

A. Results of Software Experiment

The e-Environment system was built as a community site on Microsoft SharePoint enterprise development platform using cleanroom software engineering techniques. True to its name, the web-based multi-tier enterprise application allows members of the environmental management community - comprising citizens and government officials - to deliberate on topical environment protection and development issues. Underling this software engineering is the environmental message that in the absence of

participatory social accountability and transparency in the application of environmental funds, corruption will thrive and the already dilapidated environment would be worse for it [4]. We set up an experimental design in University of Lagos, Nigeria precisely at the Centre for Information Technology and Systems and test-run the system from near (Lagos environs) and remote location (from Nigeria's capital, Abuja) as visually presented by broken arrow in Fig. 4 below. Online postings and responses were made from both Lagos and Abuja in real-time.

Fig.4. e-Environment experimental corridor - Lagos and Abuja

Going by the reliability standards of cleanroom software engineering approach for design and development, real-life operational data on environmental issues in Nigeria were used [12,13]. The experiment confirmed that ICTs could bridge the gap between stakeholders in the environment sector and more importantly entrench transparency and accountability in environmental protection and development. The participants in the experiment agreed that the outcome of the experimental study was seamless and robust online real-time communication among environment stakeholders on topical public policies, programmes, projects and services that are result-oriented. Ultimately, the e-Environment dialogue ignited a sense of transparency procedure capable of promoting participatory environmental accountability for sustainable environment, and by extension national security. Though we experienced platform-dependent and hardware-dependent challenges at the initial stage testing from remote location (Abuja), this suggests that more robust infrastructure is needed for wide-scale implementation in the future.

Figs. 5 to 7 shows snapshots of experiments with the e-Environment system.

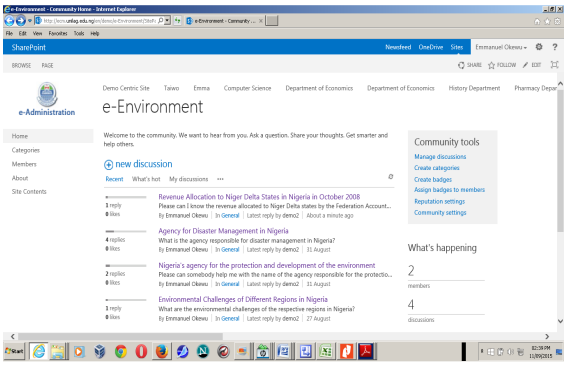


Fig. 5. The e-Environment home page showing conversation topics on public sector financing and evironmental management for government and citizens to deliberate on in the spirit of participatory environmental accountability.

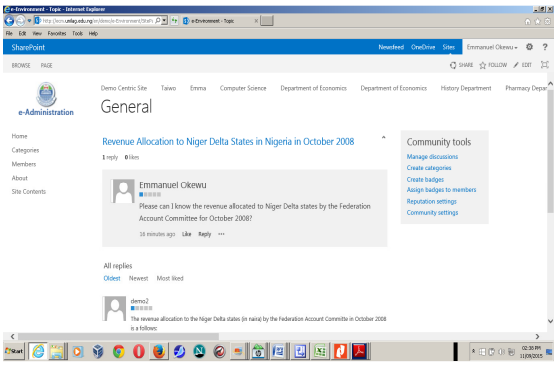


Fig. 6. A citizen posted requesting to know the revenue allocation to Niger Delta states in Nigeria by the Federation Account Committee for October 2008.

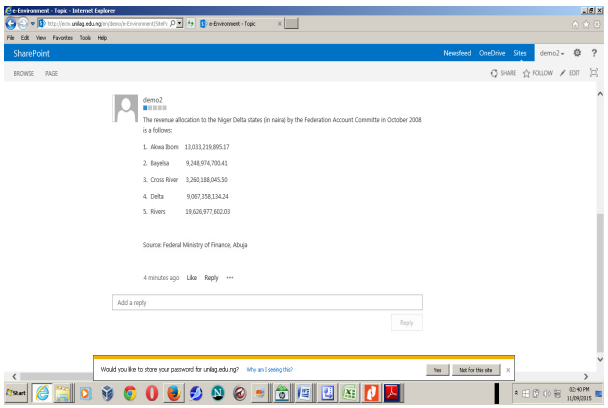


Fig. 7. Another stakeholder responded by providing real-life data for October 208 from the Federal Ministry of Finance on exact amount allocated to the Niger Delta States reputed for environmental degradation as a result of unguarded oil exploration activities.

4.2 Evaluation Threats

It is possible that a broader evaluation of the different components of the e-Environment system could throw up new perspective of things. Nonetheless, those who participated in the test run have the required experiential knowledge of the challenges confronting environmental governance in Nigerian - corruption, weak ecological infrastructure, oil spillage in Niger Delta, coastal erosion in South-West region, gully erosion in South East, desert encroachment in Northern Nigeria, among others. They also had sufficient practical engagements with the e-Environment system. This offered them good basis to make objective assessment of the impact of the proposed solution on environmental justice by ensuring judicious utilisation of public funds meant for ecological renewal, improved livelihood and national security. Thus, there is sufficient reason to take their views seriously [22, 23, 24, 25].

Also of note is the small number of participants involved in the evaluation which could in a sense limit the statistical significance of the outcome [26, 27]. However, the outcome of the experiment shows that every aspect of possible stakeholder interactions within the ecological space was adequately covered and robust online real-time conversation ensued. This is considered to be a good result because at this juncture in the project, the core objective is to have a sense of how the e-Environment system could inject transparency and accountability into environmental governance. Hence, regardless of the constraint of using a limited number of evaluators, there is sufficient grounds to conclude that there is a positive and preferential disposition to the e-Environment system as a tool for enhancing participatory environmental accountability for sustained economic livelihood and national security. It means optimal utilization of state resources such as ecological funds as a consequence of transparency will translate into wellbeing of the citizenry, mitigating social tension and insecurity . We can thus generalize that the CSE developed e-Environment system is effective for enhancing environmental sustainability, economic stability and national security.

V.CONCLUSION

So far, we have addressed the problem of environmental injustice perpetuated by financial impropriety in the environment sector. Though a number of measures have been advanced before now to stem the tide of corruption militating against environmental protection and development efforts, we unveiled an innovative system approach. The ICT solution, e-Environment system, empowers environment stakeholders to put forward proposals as well as monitor how budgets on environmental management are spent. This way, excesses of government officials reputed for diverting ecological funds are checked. With state resources judiciously utilised, environmentaldegradation is checked, socio-economic livelihood improved and national security guaranteed. Apart from solving a problem using cleanroom software engineering approach, the study presents a case study and an industrial experience from the African context as an addition to the body of knowledge of the cleanroom software engineering community. Finally, the e-Environment system is practical and ecologically sound.

ACKNOWLEDGMENT

We thank the authorities of the University of Lagos, Nigeria for providing the platform for carrying out this research study.

REFERENCES

[1] W. Ewharieme and J. Cocodia,"Corruption and Environmental Degradation in Nigeria and Its Niger Delta", Journal of Alternative Perspectives in the Social Sciences (2011) Vol. 3, No 3, 446-468, 2011.

[2] J. Akokpari, "The Political Economy of Human Insecurity in Sub-Saharan Africa", Institute of Developing Economies, Japan External Trade Organization, VRF Series, No. 437, Oct. 2007.

[3] E. P. Amechi, "Poverty, Socio-Political Factors and Degradation of the Environment in Sub-Saharan Africa: The Need for a Holistic Approach to the Protection of the Environment and Realisation of the Right to Environment", Law, Environment and Development Journal, Vol. 5 No. 2 p. 107, 2009.

[4] E. Okewu and J. Okewu, "e-Government, e-Governance, and e-Administration: A Typology of Corruption Management Using ICTs", 15th European Conference on eGovernment, University of Portsmouth, Portsmouth, UK, 2015.

[5] Transparency International Corruption Perceptions Index 2014

[6] G. E. Head, "Six-Sigma Software Using Cleanroom Software Engineering Techniques", June 1994 Hewlett-Packard Journal.

[7] H.D. Mills, M. Dyer, and R.C. Linger (1987), "Cleanroom Software Engineering", IEEE Software, Vol. 4 No. 5, September 1987, pp. 19 - 25.

[8] R.S. Pressman, "Software Engineering: A Practitioner's Approach", 7th ed., 2009.

[9] I. Sommerville, "Software Engineering", Ninth edition, 2011.

[10] E. Okewu and O. Daramola, "Component-based Software Engineering Approach to Development of a University e-Administration System", IEEE 6th International Conference on Adaptive Science and Technology (ICAST), IEEE Explore Digital Library, 2014.

[11] J. O. Kakonge, "Environmental Planning in Sub-Saharan Africa: Environmental Impact Assessment at the Crossroads", Yale Publishing Services Center, 2006.

[12] K. Kaur, "Cleanroom Software Engineering: Towards High-Reliability Software" IJCST Vol. 2 Issue 4, Oct- November, 2011.

[13] R.W. Selby, V. R. Basili, and F. T. Baker, "Cleanroom Software Development: An Empirical Evaluation", IEEE Transactions on Software Engineering Vol. SE-13, No. 9, September 1987.

[14] S.H. Schneider et al., (2007). "Regional vulnerabilities". In Parry, M.L., et al. (eds.). Chapter 19: Assessing Key Vulnerabilities and the Risk from Climate Change. Climate change 2007: impacts, adaptation and vulnerability: contribution of Working Group II to the fourth assessment report of the Intergovernmental Panel on Climate Change (IPCC). Cambridge University Press (CUP): Cambridge, UK: Print version: CUP. This version: IPCC website. ISBN 0-521-88010-6, 2007.

[15] M. Boko et al., "Executive summary". In Parry, M.L., et al. (eds.). Chapter 9: Africa. Climate change 2007: impacts,. Cambridge University Press (CUP): Cambridge, UK: Print version: CUP. This version: IPCC website. ISBN 0-521-88010-6, 2007.

[16] E.J. Tom and A.J. Attai, "The Legislature And National Development: The Nigerian Experience" Global Journal of Arts Humanities and Social Sciences Vol.2,No.9, pp. 63-78, November 2014 Published by European Centre for Research Training and Development UK.

[17] R. C. Linger, "Cleanroom Software Engineering for Zero-defect Software", Proceedings of the 15th International Conference on Software Engineering, ACM Digital Library, 1993.

[18] R. C. Linger and C. J. Tramell, "Cleanroom Software Engineering Reference Model", Version 1.0, Technical Report, CMU/SEI-96-TR-022, ESC-TR-96-022, November 1996.

[19] H. V. Vuuren, "South Africa: Democracy, Corruption and Conflict Management", Democracy Works Conference Paper, 2014, Legatum Institute/Centre for Development and Enterprise.

[20] R.C. Martin, "UML Tutorial: Sequence Diagrams", Engineering Notebook Column, pp. 1-5, 1998.

[21] E. Okewu, "Enhancing Small and Medium Enterprises (SMEs) in Africa through Service Oriented Software Engineering

(SOSE)", 2nd Covenant University International Conference on African Development Issues (CU-ICADI), 2015.

[22] M. Host, B. Regnell, and C. Wohlin, " Using students as subjects - a comparativestudy of students and professionals in lead-time impact assessment", Empirical SoftwareEngineering - an International Journal, 5(3):201-214, 2000.

[23] P. Runeson, "Using students as Experiment Subjects - An Analysis on Graduate and Freshmen Student Data", In: Linkman, S. (ed.) 7th International Conference on Empirical Assessment & Evaluation in Software Engineering (EASE'03), (2003), pp. 95-102.

[24] J. Sauro, and E. Kindlund, "A Method to Standardize Usability Metrics into a Single Score", ACM, CHI, 2005.

[25] M. Svahnberg, A. Aurum, and C. Wohlin, "Using students as Subjects -An Empirical Evaluation" Proc. 2nd International Symposium on Empirical SoftwareEngineering and Management ACM, pp. 288-290, 2008.

[26] J. Nielsen, and T. Landauer, "A mathematical modelof the finding of usability problems",Proceedings of ACM INTERCHI'93 Conference, (1993), 206-213, 1993.

[27] C.W. Turner, J.R. Lewis, and J. Nielsen, "Determining usability test sample size". In W. Karwowski (ed.), International

[28] Encyclopedia of Ergonomics and Human Factors (pp. 3084-3088), Boca Raton, FL: CRC, Press, 2006.