Academic Community Cyber Cafés –A Perpetration Point for Cyber Crimes in Nigeria

Article · January 2011

5 authors, including:

Haruna Chiroma
University of Hafr Al Batin
174 PUBLICATIONS   **1,924** CITATIONS

SEE PROFILE

Shafi'i Muhammad Abdulhamid
Federal University of Technology Minna
110 PUBLICATIONS   **1,503** CITATIONS

SEE PROFILE

Abdulsalam Ya'u Gital
Association for Computing Machinery
32 PUBLICATIONS   **238** CITATIONS

SEE PROFILE

Ali Muhammad Usman
Universiti Sains Malaysia
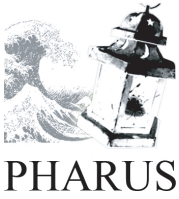**16** PUBLICATIONS   **57** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

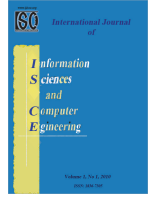The state of the art of cuckoo Inspired algorithms View project

Recent Advances in Mobile Touch Screen Security Authentication Methods: A Systematic Literature Review View project

Academic Community Cyber Cafés - A Perpetration Point for Cyber Crimes in Nigeria

Haruna Chiroma[1,*], Shafi'i Muhammad Abdulhamid[2], Abdulsalam Ya'u Gital[3], Ali Muhammad Usman[1], Timothy Umar Maigari[1]

[1]*Computer Science Department, School of Science, Federal College of Education (Technical), PMB 60, Gombe, Nigeria*

[2]*School of Information Technology, Cyber and Security Science, Federal University of Technology, PMB 65, Minna, Niger State, Nigeria*

[3]*Computer Science Department, School of Science, Abubakar Tafawa Balewa University, Bauchi, Bauchi State, Nigeria*

Abstract– **This research work investigates the contribution of academic community cyber cafés in perpetrating cyber crime. Four hundred (400) questionnaires were distributed among academic staffs, non teaching staffs and students in four (4) higher institutions of learning in Gombe state, located in north – eastern part of Nigeria. Three hundred and seventy eighty (378) were retrieved successfully, three hundred and forty (340) were properly responded. The data collected was presented on graph and table. It was analyzed using one way ANOVA and two way ANOVA. The results obtained shows there is significance difference in perception of academic staff, non – teaching staff and students in perpetrating cyber crimes in academic community cyber cafés. The perception of the three variables on perpetrating phishing, credit card fraud, cyber piracy, virus dissemination, hacking and cyber plagiarism are equal. It was concluded in the paper that academic community cyber cafés are hub for cyber crimes perpetration.**

Keyword: *Academic community , Academic staffs ,Cyber crimes ,perpetration, Nigeria, Non teaching staff, students.*

1. Introduction

Cyber crimes committed in Nigeria is more than any other country in Africa, the crime discourages investors from investing in Nigeria economy and it also poses a great danger to national security and development activities [1]. World ranking in cyber crime indicate that Nigeria is on top of the list after US and Britain but first in Sub – Saharan Africa (Adomi, 2008; Boateng et al, 2010) cited in [2]. The advent of fixed wireless access has change the pattern of cyber crime, The perpetrators who can afford to subscribe for the service are now using the wireless access to perpetrate cybercrimes at home comfortably without going to internet cafés. There are internet cafés in Nigeria that reserved special computers only for cyber criminals. Others share their bandwidth for home use to perpetrate cyber crimes [3]. Law enforcement agencies in Nigeria have not done much to arrest and prosecute perpetrators of cyber crimes due to lack of necessary legislature on cybercrime so they operate freely without fair of

being arrest and prosecuted. Internet policy is lacking in Nigeria police force so also digital forensic leaving the police handicap, Normally police in Nigeria raid suspected internet cafés mainly to collect bribes from operators of such cafés and allow them to continuo with their criminality [4]. Nigeria cyber crime working group vested with the responsibility of dealing with cyber crime to reduce it to the lowest level is not successful due to insufficient fund that will allow them formulate policies and strategies for dealing with this ugly menace. The huge losses encountered lack authentic data to back it up and reveal the real extend of damage what is available is mainly complain from individuals and organizations [5]. There is no existing law to address cyber crime in Nigeria, a bill title "*Cybersecurity And Critical Infrastructure Bill*" was submitted to National Assembly since 2005 but unfortunately the bill is not pass into law. The bill adequately captured Europe Cyber crime Convention 2001 (Budapest convention) which is enough to have legal stand in a court of law [6]. Massive transfer of data across network is the paradigm of communication between applications and this makes paperless society possible relegating paper transaction to the background. The data is converted into 0's and 1's and stored in a databases across network therefore retrieval of digital information becomes easier but the most unfortunate scenario is the existence of cyber criminals in the virtual world across the network hunting for victim to defraud [7]. Central Bank of Nigeria place cash withdrawal ceiling at N150, 000:00 ($980:39), N1, 000,000:00 ($6535.95) for individuals and organizations respectively with effect from 1st of Jun 2012 but the policy is to be pilot tested in Lagos state of Nigeria in December 2011, This is aimed at cashless society where transactions are to be done through electronics means in line with global practice [8]. In 2009 complains received for attempted or successful financial crime in Nigeria banking sector spring up but losses significantly reduced. 3,852 fraud cases were recorded involving N33.3 Billion, US$1,009.00, £2,800.00, 11,000.00. 1590 out of 3852 fraud incidence causing the banks to loss N4.1 Billion, US$328,201.00, £2,800 and 3,795.00. Seventy percent of the frauds were cyber crime [9]. The CBN policy will force depositors and investors (local and foreign) into electronic transaction while Nigeria is a hub of cybercrimes and no

*Corresponding author:
E-mail: freedonchi@yahoo.com, Ph: +23 48035955858

legislature to fight the crime, this indicate that depositors and investors are in a high degree of danger. Therefore this research to justify on exposing perpetration points of such criminal activities to the world since having access to a single network will give access to other networks across the globe and this paper expose the types of cyber crimes perpetrated in academic community cyber cafés. It was concluded that cafés in academic community are cyber crimes perpetration point.

1.1. Research questions

What is the perception of academic staff, non – teaching staff and students on perpetrating cybercrimes in academic community cyber cafés?

How do credit card fraud, phishing, hacking, virus dissemination, cyber piracy and cyber plagiarism differ based on perception of academic staff, non – teaching staff and students in academic community cyber cafés ?

1.2. Hypothesis

H_{01}: There is no significant difference on perception of academic staffs, non teaching staffs and students in perpetrating cyber crime in academic community cyber cafés.

H_{02}: There is no significant difference among credit card fraud, phishing, hacking, virus dissemination, cyber piracy and cyber plagiarism in respect of academic staffs, non teaching staffs and students perceptions.

2. Related Work

2.1. Definition of cyber crime

Cyber crime is a word that is use each day, The obstacle in determining the extend of cyber crime is that there is no worldwide accepted definition of cyber crime but British police defined cyber crime as offence committed with the aid of computer network [10]. In [11] cyber crime is defined as offence committed due to advancement in computer technology, [11] further admitted that various definitions of cyber crime are in existence. In [12] there is no consensus on definition of cyber crime but Canadian law enforcement agency defined cyber crime as crime committed via computer or part of the crime is committed using a computer as a tool. Based on the given definition, cyber crime is divided into two classes as using computer to commit crime already in existence in the physical world using computer and committing of a crime via computers and networks. Literature in existence shows there is conceded definition of cyber crime but base on explanations given in [10, 12] a crime committed using computer and networks is referred to as cyber crime.

Cyber crime is divided into four groups [11] as follows:

Economic Crime: comprising of hacking, computer sabotage and virus dissemination, computer espionage, computer forgery, computer fraud and computer manipulations.

Contend related offences: comprising of dissemination of child pornography and racial attack statement through the internet.

Intellectual property offences: comprising of violation of copyright and related rights and cyber squatting.

Privacy offences: comprising of illegal collection, storage, modification and disclosure of information.

Internet crime complain center (IC3) was established on May 8, 2000 with collaboration between NW3C/BJA and FBI with the aim of fight in against cyber crime . IC3 received 2 million complaints from inception and 303, 809 complaints about cyber crime in 2010 alone. IC3 create public awareness on how to avoid cyber criminals. Table 1 shows top 10 cyber crime complaints received in 2010, Figure 1 indicate the pattern of complaints received from the public on cyber crime from 2000 to 2010, Figure 2 shows dollars lost due to cyber crime over a period of eight years, the most reported cyber crime was non delivery payment/merchandise [13]
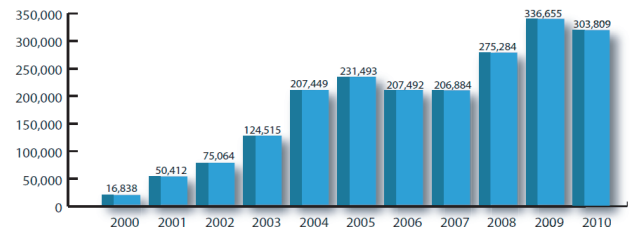

Fig. 1. Yearly comparison of Complaints Received via the IC3 Web Site.
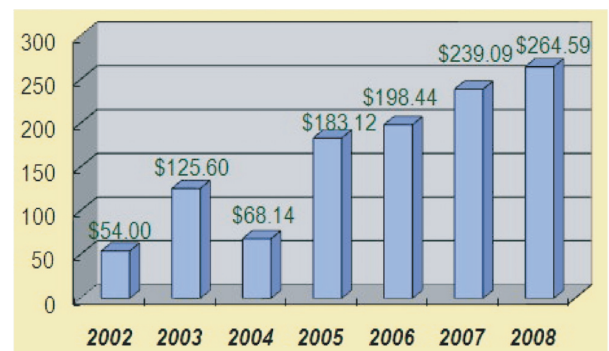

Fig. 2. Dollar lost from 2002 – 2008.

Administration, businesses and entire society put their confidence on efficiency and cyber security of ICT facilities [11] but these huge amount losses to cyber crime may frighten the general public from dealing with electronic transaction systems because the confidence will no longer be here.

Table 1. Top 10 Crime Type.

Type	Percent
1. Non-delivery Payment/Merchandise	14.4%
2. FBI-Related Scams	13.2%
3. Identity Theft	9.8%
4. Computer Crimes	9.1%
5. Miscellaneous Fraud	8.6%
6. Advance Fee Fraud	7.6%
7. Spam	6.9%
8. Auction Fraud	5.9%
9. Credit Card Fraud	5.3%
10. Overpayment Fraud	5.3%

Study conducted in [14] reveals new threats and damages incurred by these threats which include:

i. Every year $202 million is lost by organizations in US due to cyber crimes.

ii. Most cyber crime financial lost (over 50%) are internal.

iii. Over 400, 000 web pages have network intrusion tool in one form or the other.

iv. It is estimated that every 20 seconds enterprises experiences cyber crime attacks.

Table 2 adopted from [10] indicated financial losses due to cyber crime in different forms in US in 2003

Table 2. High Cost of Computer Crime.

Type of Cyber Crime	Cost in Millions
Theft of proprietary information	US$ 70.1
Financial fraud	US$ 10.2
Networked Data sabotage	US$ 5.1
Virus	US$ 27.4
Insider Network Abuse	US$ 65.6
System penetration by outsiders	US$ 2.8
Others (laptop theft, telecommunication fraud, wire tapping, insider access)	US$ 9.4
Total	US$ 202.4

2.2. Cyber Crimes in Nigeria

Penetration of ICT in sub Saharan Africa is relatively successful and this open up space for cyber crimes which posses great danger to economic growth of the region, image of the region is also dented due to cyber crimes [15] the statement about ICT penetration in Africa is depicted in Figure 3 and Nigeria top on the penetration chart as shown in Figure 4 both charts are sourced from [16].

In [1] cyber crime in Nigeria are characterize by:

i. Perpetrators of cyber crimes in Nigeria are unemployed youths who are knowledgeable in computer skills.

ii. They connived with insider within financial institutions and Nigerians abroad to perpetrate their criminal activities.

iii. Cyber criminals in Nigeria have migrated to other African countries with weak enforcement agencies to perpetrate their dangerous activities.

iv. They enjoy the fact that there are no adequate cyber crime laws to deal with this ugly menace.

v. Nigerian cyber criminals utilizes reshippers mechanism in Dubai, UK and west African way stations.

Different categories of crimes are committed each day through internet access point with Nigerians toping the scene by deceiving their victims with fraudulent financial proposals [3]

A study conducted in [3] reveals that there was consensus among respondents that cyber cafés offer facilities for perpetrating cyber crime and the study further inferred that internet access point, home networks, private organizations and government offices in Nigeria respectively are cyber crimes perpetration points.

3. Research Methodology

A detail research questionnaire design and developed by [17] was adopted and modified a little bit to suit the study. The questionnaire consist of four sections, introduction, demography, definition of cyber crime terms and questions related to cyber crimes perpetrations in the last section "Yes or No" question with 'Yes' 2 points and 'No' 1 point. A pilot test was conducted on 20 respondents to ascertain content validity and reliability of the instrument. We employ and trained 8 students of computer science as research assistance that were trained on how to administer and give detail explanation on how to correctly respond to the questionnaire. The study was conducted in Gombe state, located in north eastern part of Nigeria. Population of the study was all Academic staff, Non – teaching staffs and students of all higher institutions located across the state which are 7 in number, 4 were selected for the study because of their large size, population and existence of functional cyber cafés which attract higher patronage from the academic community. 400 questionnaires were distributed by the researchers and research assistance by visiting each institution cyber café, offices, classes and hostels to randomly select individual and administered the questionnaire, out of 400 distributed questionnaires 378 were retrieved successfully and 340 were properly filled while 38 do not capture relevant information required for this research. Data collected was presented on graph, table and analyzed using one way Analysis of Variance (ANOVA), two way ANOVA as shown in Table 4 and Table 5.

4. Result Analysis and Discussion

Figure 5 is a plot of data collected from the field among academic staffs, Non – Teaching staffs and students. Horizontal axis is the number of questionnnaires properly responded and vertical axis is the stack point for each responded questionnnaire and total number of the questionnnaires was 340. One way and two ANOVA was use to analyse the data of Figure 5 and Table 4 using SPSS for windows version 17[18] and result is shown in Table 3, Figure 6 and Table 5 respectively.

From Table 3 F > F- Tabulated at 5% level of significance therefore H_{01} is rejected and conclude that there is significance difference among academic staff, non teaching staff and students on their perception in perpetrating cyber crime in academic community cyber cafés .

Figure 6 is a plot of mean of the variables, the variables are on horizontal axis where 1.00 represent academic staff, 2.00 non – teaching staff and 3.00 students respectively while the vertical axis is the mean of the variables, the graph further confirmed rejection of the null hypothesis (H_{01}) since the means are approximately not on the same level

Table 4 shows cyber crime type that are most active in cyber cafés located in academic community with their corresponding points for each of the variables (academic staffs, non – teaching staffs and students), result of analysis of Table 4 is shown in Table 5.

In Table 5 cyber crime type shows that F < F – Tabulated at 5% level of significance which indicate that H_{02} was accepted and conclude that there is no significance difference among cyber crime types (credit card fraud, phishing, hacking, virus dessimination, cyber piracy and cyber plagiarism) in respect of academic
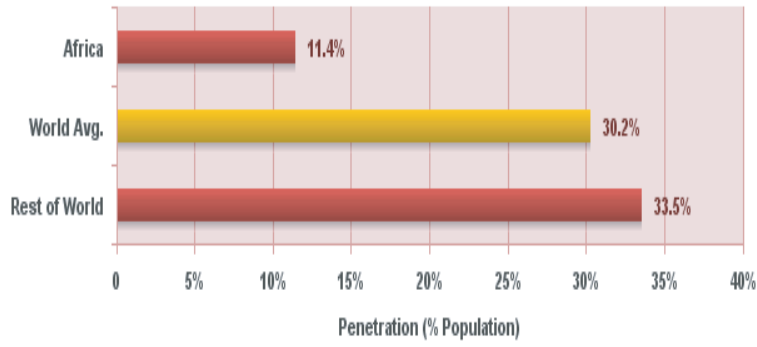
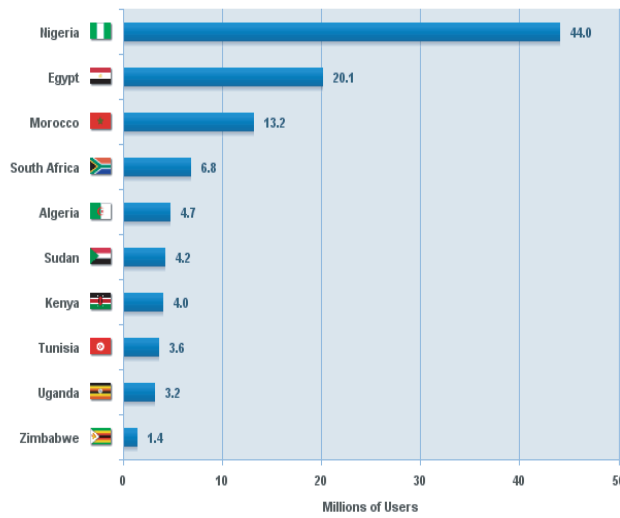**Fig. 3.** Internet penetration in Africa as at March 31, 2011.

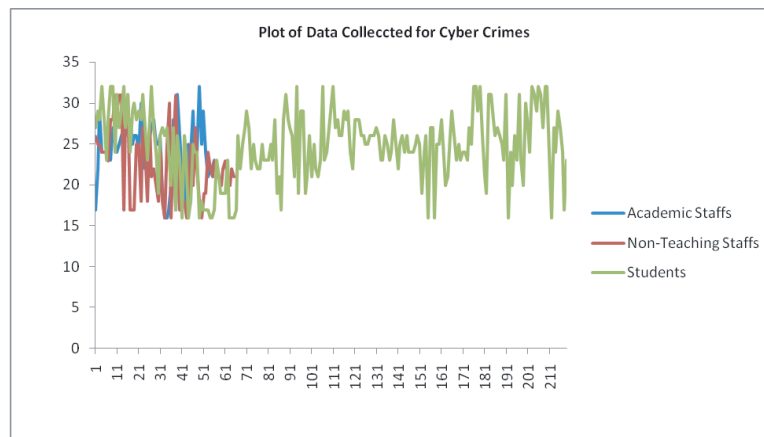**Fig. 4.** Africa top internet countries as at 31 March, 2011.

Fig. 5. Plot of Raw Data Collected.

Table 3. One way ANOVA.

	Sum of Squares	Df	Mean Square	F	F-Tabulated
Between Groups	293.645	2	146.822	8.302	3.000
Within Groups	5960.049	337	17.686		
Total	6253.694	339			

staff, non - teaching staff and students. Indicating that the cyber crimes type are of equal papetration. Analysis in table 5 further rejected H_{01} since variable F > F - Tabulated at 5% level significance.
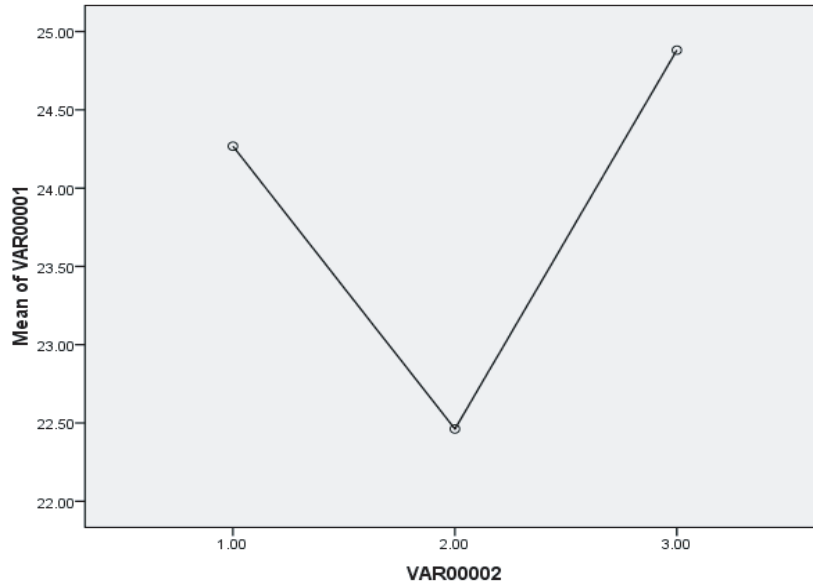
Fig. 6. Plot of Mean Vs Variables.

Table 4. Active Cyber Crimes in academic community cyber cafés.

Cyber crime Types	Academic Staffs	Non-Teaching Staffs	Students
Credit Card Fraud	85	86	337
Phishing	78	91	300
Hacking	91	97	369
Virus Dissemination	98	111	388
Cyber Piracy	93	96	377
Cyber plagiarism	91	100	369

Table 5. Two way ANOVA.

Source	DF	SS	MS	F	F-Tabulated
Variable	2	278073	139037	344	3.81
Cyber Crime Type	2	654	327	0.81	3.81
Error	13	5248	404		
Total	17	283975			

5. Discussion of Results

The perception of members of academic staff, non-teaching staffs and students on perpetrating cyber crime using academic community cyber cafés differs but they all conceded that cyber crimes are perpetrated through the cafés, this result was suspected because similar research conducted at different locations in Nigeria agreed with the results of this research work for instance in [15, 3, 17] but differs in magnitude of cyber crimes and types. H_{02} was accepted signifying that the rate at which phishing, credit card fraud, hacking, virus dissemination, cyber piracy and cyber plagiarism are perpetrated are equal based on perception of academic staffs, non – teaching staffs and students. Phishing and credit card fraud are serious source of concern as they negatively affect economic development directly, CBN policy of cashless society is seem to be threaten by cyber crime both local and foreign investors may shy away from using transactions systems in Nigeria there by making it difficult to attract international investors into the country if urgent and radical action is not taken. This research work have added to other research works conducted on cyber crimes in different parts of Nigeria and the entire world.

6. Suggested frameworks to combat cybercrime in Nigeria

If the stake holders presented in Figure 7 will put hands on desk and exchange ideas there will be a legislature and policies that will capture effective cyber crime laws that can stand technological advancement and compete globally. Results of researches adopted and properly use can give a brilliant finish to the legislature there by putting cyber crime perpetrators at a serious re – think of their activities [2] this research work added pressure from international community onto the conceptual model because government in Nigeria have respect for international community, their voice speed up legislation, policies and practice.

7. Conclusion and further research

Result emanated from this research triggered the conclusion that the active types of cyber crimes are phishing, credit card
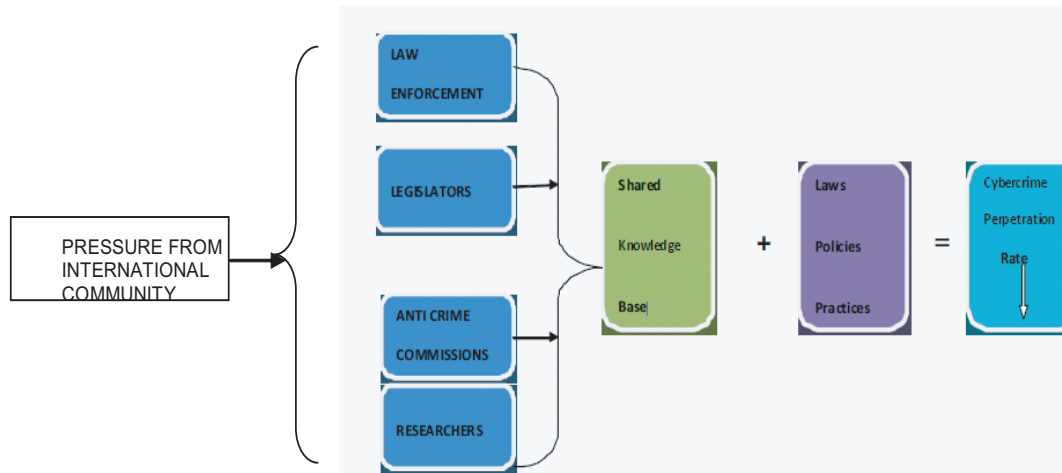
Fig. 7. Conceptual Model adopted in [2] and modified

fraud, hacking, virus dissemination, cyber piracy and cyber plagiarism therefore urgent and drastic action is needed from law enforcement agency, legislatures, researchers and international community to combat this menace to tolerance level. Cyber cafés located in academic community are hubs for perpetrating cyber crimes in Nigeria. Similar empirical research are recommended to be replicated in other part of Nigeria, Africa and the world to expose cyber crime perpetration points.

Acknowledgements

References

[1] N. Ribadu, "Cybercrime and commercial fraud: A nigerian perspective," in *Modern law for global Commerce Congress to celebrate the fortieth annual session of United Nation Commission on International Trade Law*, (Vienna, Austria), pp. 2–3, 2007.

[2] E. A. Akuta, I. M. Ongoa, and C. R. Jones, "Combating cybercrime in sub saharan africa: A discourse on law, policy and practice," *Journal Of Peace, Gender And Development Studies*, vol. 1, no. 4, pp. 129–137, 2011.

[3] O. B. Longe and S. C. Chiemeke, "Cybercrime and criminality in nigeria -what roles are internet access points in playing?," *European Journal of Social Sciences*, vol. 6, no. 4, pp. 132–139, 2008.

[4] O. E. Robert and A. Bola, "Cyber crime in nigeria," *Business intelligence journal*, vol. 3, no. 1, pp. 93–98, 2010.

[5] O. Ajuogu, "Running head: burden of cyber crime to e-commerce in nigeria." Internet and Society: Technologies and Politics of Control, 2011. http://cyber.law.harvard.edu/is2011/sites/is2011/images/Internet_Society_Final_Project.pdf.

[6] N. N. Ajikanle, "Lack of law to address cybercrime is dangerous." Daily Trust Newspaper online edition, 2011. http://allafrica.com/stories/201107040174.html.

[7] H. Chu, W. D. Lin, and K. H. Chang, "Digital forensics core curriculum design in higher education in ubiquitous computing era," *Tamkang Journal of Science and Engineering*, vol. 13, no. 1, pp. 89–97, 2010.

[8] "CBN annual report and statement of accounts for the year ended 31stdecember,2009," tech. rep., Central Bank of Nigeria, 2009. http://www.cenbank.org/out/2010/publications/.

[9] "Questions and answers on the cbn policy on cash withdrawal/lodgment limit," tech. rep., Central Bank of Nigeria, 2011. http://www.cbn.gov.ng/Out/2011/pressrelease/gvd/R evised.

[10] S. Fafinski, "Uk cybercrime report," tech. rep. http://www.garlik.com/press/Garlik_UK_Cybercri me_Report.pdf.

[11] S. K. Mercado, "Cracking down on cybercrime global response: The cyber crime convention," *Communication of the International Information Management Agency*, vol. 5, no. 1, pp. 59–66, 2005.

[12] K. Melanie, "Issues, data sources and feasibility of collecting police reported statistics," *Canadian Centre for justice statistics*, p. 6, 2002. http://dsp- psd.pwgsc.gc.ca/Collection/Statcan/85-558-X/85- 558-XIE2002001.pdf.

[13] "Internet crime report," tech. rep., Internet Crime Complain Center, 2010. http://ic3report.nw3c.org/docs/2010_IC3_Repo rt_02_10_11_low_res.pdf.

[14] "Cisco integrated network security in higher education institutions," tech. rep., Cisco Systems, 2004. http://www.cisco.com/web/strategy/docs/highe r_security.pdf.

[15] O. Longe, O. Ngwa, F. Wada, and V. Mbarika, "Criminal uses of information technologies in sub – saharan africa: Trends, concerns and perspectives," *Journal of Information Technology Impact*, vol. 9, no. 3, pp. 156 – 172, 2009.

[16] "Internet usage in africa," tech. rep., Internet World Statistics, 2011. http://www.internetworldstats.com/stats1.htm.

[17] M. A. Shafi'i, H. Chiroma, and A. Abubakar, "Cybercrimes and the nigerian academic institutions networks," *The IUP Journal of Information Technology*, vol. VII, no. 1, pp. 47– 57, 2011.

[18] "Spss version 17 for windows." SPSS Inc, 2007.

Haruna Chiroma is a lecturer at Computer Science Department of Federal College of Education (Technical) Gombe. Nigeria. Haruna has obtained MSc in Computer Science at Bayero University Kano, Nigeria, 2009. First degree in Computer Science from Abubakar Tafawa Balewa University Bauchi, Nigeria, 2004. Post Graduate Diploma in Education (Mathematics) in 2007 from Usman Danfodio University Sokoto. Member Nigeria Computer Society , member International Association of Engineers and Member Teachers Registration Council of Nigeria. Have numerous journal publications both in Nigeria and out side. His research interests are; Artificial Neural Network, Computer Forensic, Software Engineering, and Computer Networking and Security.

Shafi'i Muhammad Abdulhamid holds M.Sc. degree in Computer Science from Bayero University Kano, Nigeria (2011) and B.Tech. degree in Mathematics/Computer Science from the Federal University of Technology Minna, Nigeria (2004). His current research interests are in Software Engineering, Cyber Security, Computational Intelligence and Operating Systems. He has published many academic papers in reputable journals within Nigeria and Internationally. He is a member of International Association of Computer Science and Information Technology (IACSIT), International Association of Engineers (IAENG), The Internet Society (ISOC) and a member of Nigerian Computer Society (NCS). Presently he is a lecturer at the Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.

Abdulsalam Ya'u Gital is a lecturer at Mathematical Science Department, Abubakar Tafawa Balewa University Bauchi, Nigeria. Presently a PhD research scholar at University of Technology, Malaysia. MSC Computer Science from Abubakar Tafawa Balewa University, 2008. B .Tech, Computer Science from the same University in 2003. Area of research interest: Software Engineering, Neural Network, Network security and intelligent machines.

Ali Muhammad Usman is a Lecturer at Computer Science Department, Federal College of Education (Technical),Gombe, Nigera. First degree in Computer Science from Abubakar Tafawa Balewa University, Bauchi, Nigeria in 2005. Post Graduate Diploma in Education (Mathematics) from Usman Danfodio University Sokoto. Member of Nigeria Computer Society and have many journal publications within Nigeria. His research interests are; Database Management System, Computer programming, Artificial Neural Network, Cyber security science.

Timothy Umar Maigari is with Adamawa State University (2010/2011) - MSc in View. Attended Abubakar Tafawa Balewa University, Bauchi, Nigeria from 1998- 2003 and obtained B. Tech Computer Science. Post Graduate Diploma in Education was obtained from National Teachers Institute, Nigeria in 2008. Currently a member of Nigeria Computer Society and Lecturer at Federal College of Education (Technical), Gombe, Nigeria at the Computer Science Department. Research interest includes programming, cyber security, data modeling, software engineering and intelligent machines.