Network System Design for Combating Cybercrime in Nigeria

Abstract. This research work is to bring to light, the danger posed by Cyber Crime in the world generally and Nigeria in particular with the hope that policy makers will work with the recommendations and practical combating framework design of this research work. In order to achieve this, the following approaches were adopted; survey of some common Cybercrime in Nigeria with the frequency of occurrence and design of a frame work system to combat the crime. The system design controls and track cyber criminals on the Nigerian cyber space. The paper proposes the establishment of National Cybercrime Control Center (NCCC) to effect this system. The Security Agents could obtain tracked information from NCCC as evidence to arrest and prosecute cybercriminals.

Keywords: Network, Cybercrime, Framework, Combating

1 Introduction

Generally, crime means "a legal wrong that can be followed by criminal proceedings which may result into punishment" whereas Cyber Crime may be "unlawful acts wherein the computer is either a tool or target or both" [13].

Nigeria is adjudged as the most populous black nation in the world and by the figures of the last population census, Nigeria's population has grown slightly above 140 million [10]. This has no doubt increase commercial activities and hence attracted more providers of services locally and internationally, one of these services is the computer and internet revolution that has rapidly increased over the years. Cyberspace is already woven in to the fabric of our society. Our security and economy can no longer do without the cyberspace and online access is the most dominant part of the cyberspace, it is already viewed by many as the 'fourth utility', a right rather than a privilege [6]. In less than 11years, the number of global web users has exploded by more than a hundred-fold, from 16 million in 2003 to more than 1.7 billion presently [9].

While cyberspace provides Nigeria with massive opportunities, the dangers associated from our increasing dependence on it are huge in the last 10 years. There have been more interconnected devices than ever; everything from mobile phones, computers, cars and surveillance systems, are networked across homes, offices and classrooms across the geopolitical zones of the country [9].

The advancement of man in terms of Information Technology which surpasses any previous generation has usher in a new dimension in crime. The Cyber space has become a fertile land where various crimes are being committed per second.

Cyber Crime is a computer-based crime which involves all criminal activities that are carried out in the Cyber-Space [13]. The Internet revolution formed the backbone for this crime as it merged the Universe into a global village. This crime could be committed against individual, businesses and governments.

In the era of cyber world as the usage of computers has became more widely deployed, with the advancement in supporting technology devices as well. The term 'Cyber' became more familiar. The rapid growth of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analysis, with the use of high technology. Due to increase in the number of users, misuse of technology in the cyberspace was clutching up which gave birth to cyber crimes at the domestic and international level as well [10].

Cyber Crimes Actually Means: It could be hackers attacking your site and trying to gain undue privilege to your information, with the use of internet. It can also include 'denial of services' and virus attacks preventing regular traffic from hitting your site. These crimes are not committed by outsiders unless in case of viruses and with respect to security related cyber crimes that is usually committed by the employees of particular company who can easily access the password and data storage of the company for selfish gain [13]. Cyber crimes also includes criminal activities done with the use of computers like plagiarism, online advanced fee frauds, pornography, online gambling, piracy and other cyber crimes.

Problem statement of this work is the fact that Impact of Cybercrime on National image and Security cannot be over-emphasized. Any Nation, be it developed or developing like Nigeria depend on interaction with other countries of the world. The integrity of data and communication at the private, business and official level forms the bedrock for any meaningful development in terms of policy formation, security, education, economy, social tribes.

Therefore, any false modification of data and fraudulent activities on the nation's cyber space may spell doom on such country. For an example, if someone gained access into the data storage of a certification of competency to fly a plane, if cyber criminals succeeded in defrauding intending investors in the country of all their money, the consequences both on safety, economic downfall and the country's image can be imagined.

This problem is increasing globally and in Nigeria; hence this designed frame work as proposed by this paper shall reduced this problem drastically and as a deterrent to cyber criminals.

.

The research is aimed at combating cybercrime using centralized control system with the objectives to;

- Identify the various cyber crimes in Nigeria and measure the frequency of their occurrences.
- Design a system to combat cyber crimes by way of monitoring and controlling users.
- Sum all registered users in a control centre with a mathematical model
- Be able to track and apprehend criminals on the Nigerian cyber space.

This research work is significant in the sense that it serves as an automated system to control and checkmate cyber criminals' activities in Nigeria and the world at large. Therefore, the author(s) of this paper shall be willing to partner and make this frame-work available to partner the security agencies of government to be able to make right policy that will curb the menace of Cyber Crime and by so doing improve the security of the nation's cyber space.

The scope of the work is to cover some common Cybercrimes that poses serious threat to the financial and material Security and Nigeria image as a whole. The proposed system design recognizes any IP addressable devices on the cyber space under consideration but can only produce full detail logs of only the screen-based devices since the imagery part of the logs is the most important evidence of cyber crime.

Although so many things could be integrated on the proposed frame work design, but for the purpose of this very work, the system is limited to control only screen-based and camera embedded devices used on the Nigerian cyber space.

Since it is required that the network installs the auto imagery controller in user's device in a matter of seconds, the complex programs to synchronize the imagery capturing devices with the logs recorder at the control center can still be perfected further to be able to discriminate users with obscure face or any form of shades to prevent recognition.

2 Review of Existing Framework for Combating Cybercrime

Researchers in the IT profession has been working seriously to come up with frame work to combat cybercrime globally and locally, but various frame work has always been with its own limitations in the fight to combat cyber crime.

Legislative approaches, administrative measures and Technical measures were the solutions suggested by [7]. Technical measures which are of interest to the authors of this paper, was theoretical and advisory as the author could not provide practical implementation of such technical measures. Curriculum should include courses on cyber-management, crime and its prevention. Education is a most vital weapon, as inculcating the right culture will create a high level of awareness among all stakeholders, seminars and workshop should be organized from time to time with emphasis on cyber safety so that the individuals will learn to keep their personal information safe and flee cybercrime. Some youths are misguided and misdirected by peers and uncensored films; unless they are guided they may not realize the inherent danger in the act. In the work of [2], the authors suggested building of database of phone numbers and faxes of fraudsters relying on Criminal Act Section 419 of the Nigeria Criminal code Capp 777 of 1990 that prohibits advance fee fraud. This is to allow the authority to shut down the phone numbers and cafes in case of criminal activities. Considering the argument of the author [5], maintains that "Fighting cybercrime requires not just IT knowledge but IT intelligence on the part of the security agencies. After all, in [1] the authors said a little stringent measure on individual's internet activities can assist in reducing cybercrime.

Cyber crime is information and intelligence based. Curiously, the criminals have the technological advantage which the fighters lack sometimes. To outsmart the criminal, having the necessary skills and intelligence are sine qua non. Nigeria government should do more than just enactment of laws and to start prosecuting offenders. [11], according to the author, fighting cybercrimes goes beyond bill boards at strategic places as warnings to cybercriminals in Nigeria without any serious government policy to deal with cybercrime offenders. The effort of the Nigeria Cyber Working Group (NCNG) formed by the Federal Government of Nigeria in 2004 has also not yielded any positive fruit. In another work [4], the authors came up with a frame work using packet attestation which can establish whether or not a given packet is sent by a particular subscriber. This has the capability of allowing network operator to verify the source of malicious traffic and it will also help to validate complaints. However, the limitation of this frame work bothers on the availability and credibility of the packet attestation itself. The availability and credibility depends on the ISPs of the originating messages or packets. Again, this system cannot trace a multi stage attacks by itself back to the source.

The impact of cyber crimes on Nigerian economy is the focus of [12] in which survey and statistical analysis are used as a methodology for accessing how prevalent the cyber crime menace is, and to sensitive the Nigerian masses against risks that are evident in the cyberspace. The drawback of this study is the inability to define and suggest a framework for fighting cybercrime in our cyberspace.

Accessing Cyber Crime and E-banking in Nigeria uses Social Theories as a methodology for proffering policy modulation in combating cybercrime in electronic banking services in Nigeria [15]. It is limited with the fact that banks in Nigeria have implemented bank verification numbers, a policy that adds captured biometrics details of individual bank customer means cyber security solutions have gone beyond social theories to a more practical approach and model.

In [3], the causes, effects and way out of cybercrimes in Nigeria were suggested. The methodology lies on policy definition, it lacks a specific technically model for achieving security in the cyberspace.

However, the review of [16] reveals that it is the same as [15] but with a different title with same authors and contents.

Models from technological innovation with public health, law of sea, aviation law automotive regulation and coordinated ecosystem change were part of the frame work designed to combat cybercrime [14]. The work dealt mostly on laws and regulations of various sector that concerns cyber space, but the limitation of this framework lie in the fact that practical solutions are not achievable where those laws and regulations are not implemented or where cyber criminals can cleverly by pass laws and regulations.

In [8], authors proposed the risk-based approach which work on the principle of assumption that unauthorized user can gain access to the system and compromised data. The design responses based on the data that could be compromised. This approach is meant to prioritize risks and Categorizing the most valuable data. The paper also proposes the approach of developing actionable cyber threat intelligence with a model of cyber intelligence acquisition and analysis.

This frame work has the limitation of not being able to apprehend the cyber criminals in most cases. The prioritizing of data may have some consequence because, a less important data taken from a place can be very useful to compromise more important data somewhere and thereby used to commit serious cyber crime.

In summary, all existing framework reviewed lacked little or no system designs that can could ensure practical implementation leading to monitoring, arrest or prosecution of cyber criminals. This paper seeks to bridge that gap.

3 Proposed System Design to Combat Cybercrime

This is a system design where all devices that uses internet can be monitored. Transactions, communications and information can be traced to the originator of such transactions and communication with the clear image of the perpetuator for arrest and prosecution.

3.1 Methodology of the Research

The survey and system design model was used in this research. The survey was used to identify the common cyber crimes and the frequency of their occurrence in Nigeria; then the proposed system model was designed to reduce the frequency of the cyber crime to the barest minimum and to serve as practical control and preventive mechanism against cybercrime as well as evidence to arrest cyber crime perpetuators. Also, a mathematical model for summing up all registered user is included, bearing in mind that is important to know the number of people using the network with their individual bio data saved in the database. This research is proposing the establishment of NCCC that will be the custodian of the implementation of this framework design. Several Network security technologies and configurations shall be implemented under very strict network security policy. The model was designed and simulated with a network design tool (packet tracer).

3.1.1 Survey of Cybercrimes in Nigeria

The study identified some common cyber crime in Nigeria such as: Online Advance-fee fraud, pornography, software piracy, software cracking, ATM fraud, spam e-mail, website hacking, and personal identification theft (PIT). A total of two hundred experience respondents were selected to give the general rating of cyber crimes mentioned as either L – Low, H – High or VH – Very High. The results were presented in tables below

Table 1. Cybercrimes Rating

Cybercrime	Rating	Outcomes	%
1. Online Advance-fee fraud	L	20	10

2. Pornography 3. Software piracy, 4. software cracking, 5. ATM fraud 6. spam e-mail, 7. website hacking 8. Personal identification theft (PIT).	H	40	20
	VH	140	70
	Total	200	100

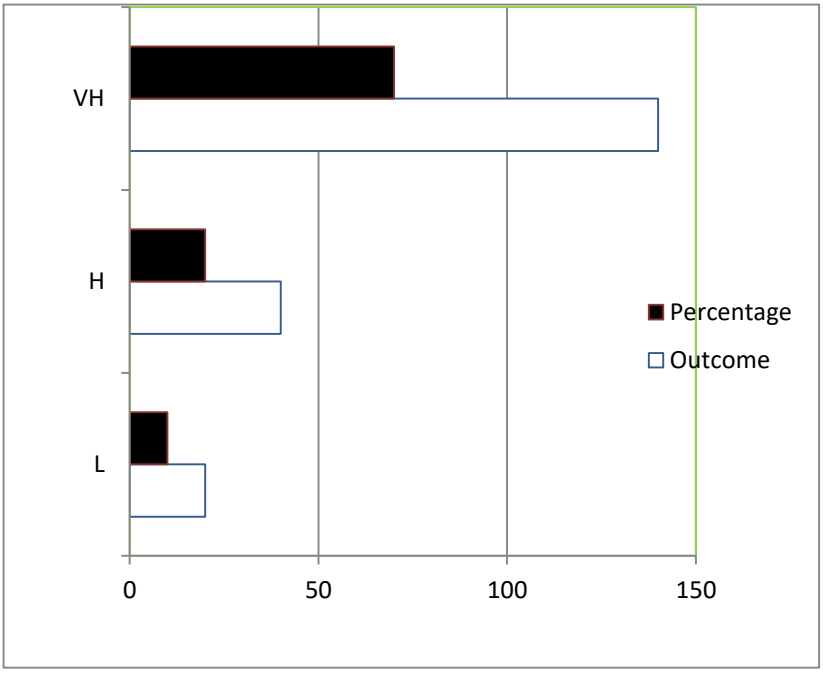

Fig. 1 Occurrence chart representing the table.

From Table 1 above, it clearly shows that all the identified cybercrimes in Nigeria has had a sharp rise going by the percentage of respondents in terms of the very high (VH) rating parameter. While the least of respondents on the table are 2, that rated cyber crime occurrences low and that are just 2%, this shows that most enlightened Nigerians understands the negative effect of various cybercrime in the country. The high rise in online Advance-fee fraud and other cybercrimes as enumerated above could be seen through a lot of social media such as Facebook and free e-mail services such as Yahoo mail. Most Nigerians now have access to the internet through their

phones via the GSM service provider. Figure 1 above shows the occurrence chat from the table.

3.1.2 Designed Model for the Proposed System

Figure 2 below shows the proposed design system model. An anonymous user can login from any location in the Nigerian cyber space and start surfing and other activities without being aware of all the complex processes that are going on within the network system via the NCCC. This shall be explained later in the paper.

The control center also needs to login and perform several actions to establish connections with the anonymous user via the State nodes or direct to the user's devices.

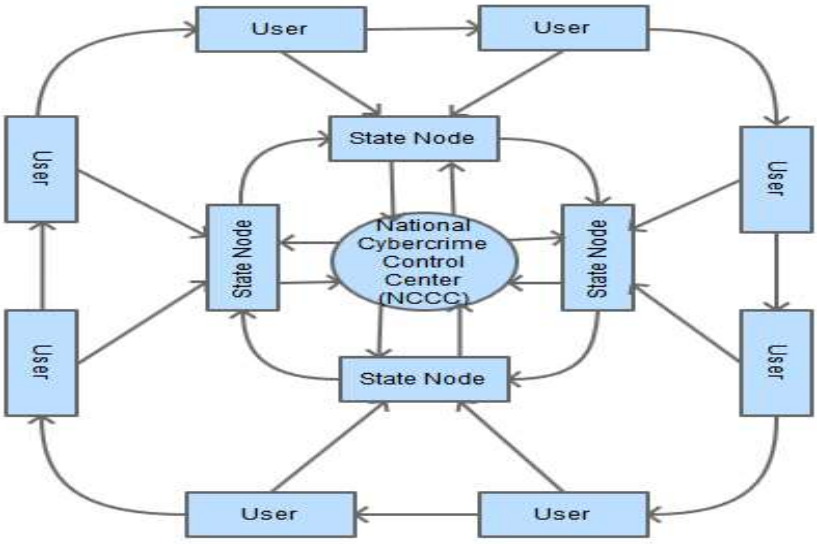

Fig. 2 Model of the Proposed National Cybercrime Control Center

3.1.3 Mathematical Model for the System

Given Users (U) is a function of individually registered X users, using personal computing devices.

$$U = (X_1, X_2, X_3 \ldots X_{n-3}, X_{n-2}, X_{n-1}, X_n) \quad (1)$$

At the State level (S), the system calculate the sum of anonymous users to access the internet. This shown mathematically as;

$$s = \sum_{ci=1}^{n} U(Xi) \quad (2)$$

Finally, at the National Cybercrime Control Centre (N), the sum of anonymous users in the country's cyberspace is calculated by adding users in all the states as follow;

$$N = \sum_{i=1}^{37} S(\sum_{i=1}^{n} U\ (Xci) \qquad (3)$$

3.2 The System Algorithm

The system algorithm is from the perspective of the two main actors that will be interacting with the system; that is, the user who in this case, the targeted cyber criminal and the control personnel(s) at the NCCC. The algorithm below explains the process involved in setting up the NCCC.

Start

Step1: Assign one router each to all the 36 states (Nodes) plus FCT in the country with IP addresses

Step2: Use one of the routers to serve as admin server router linked to a database

Step3: At the state level, all anonymous user X is routed to the state nodes with its router IP.

Step4: anonymous user X's facial image is automatically captured by the network controlled web cam and saved to the National Cybercrime Control Center database.

Step5: An IP Address for internet access is assigned to the anonymous user's device else access is automatically denied if Step3 and Step4 are skipped.

Step6: the Control Center monitors internet uses and trace a user X details in the event of cybercrime.

Stop

- The system algorithm is from the perspective of the two main actors that will be interacting with the system; that is, the user who in this case, the targeted cyber criminals and the control personnel at the NCCC.

USER

- Login
- Networks controlled -auto-Imagery program activated
- Profile created
- Access network

NCCC

- Login
- Access active nodes

- View logs at the nodes
- View user's logs at the node
- Display or print user's logs

3.3 Flow Chat for the Proposed System Design

The figure 4 below presents the system flow chart for the proposed National Cybercrime Control System. Several anonymous users can attempt to login to internet on the Nigeria cyberspace from any of the state nodes. The auto-imagery program from the NCCC activates the camera on the users' devices via the state node

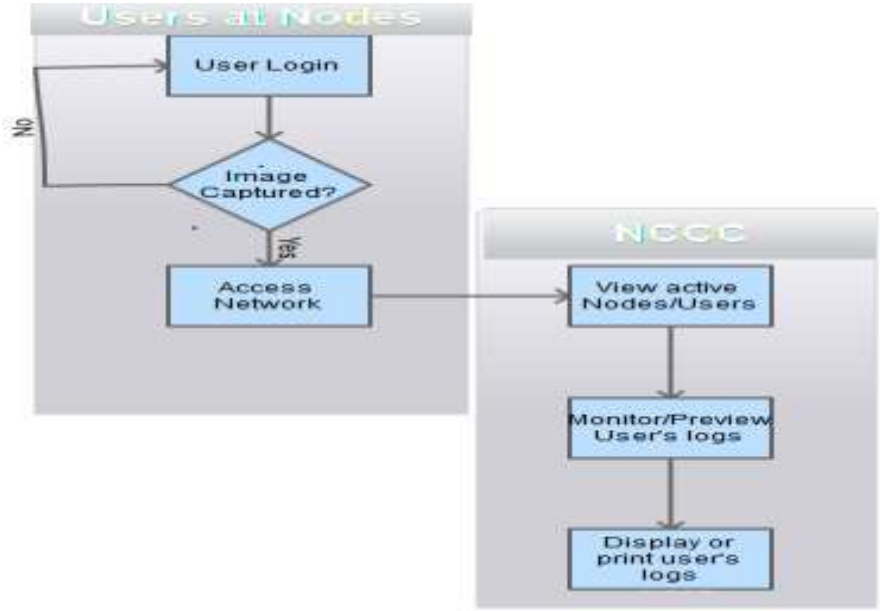

Fig. 3 Flow Chart of the System

3.4 The Network Design Concept for the System

This paper execute the idea of Internet Protocol (IP) location based system steering framework where IP version4 (IPV4) or IP version 6(IPV6) can be used; in light of the fact that IPV4 and IPV6 has turned out to be a vigorous and adaptable convention for Internet directing. IPV4 utilizes 32-bit IP address, and with 32 bits, the number of IP locations can reach 4,294,967,296. This is more than four billion. But the Ipv6 shall also be considered in the implementation of this system design in view of the foreseen geometrical increase of devices on the Internet, or the requirement for more IP locations than IPV4 could supply. The system design work on the supposition that

each electronic gadgets connected to the internet must have an IP for Identification. In this system design, we are considering only the screen -based devices like the desktop, Portable Computer, PDAs, and convenient telephone gadgets.

IPV6 is utilizing 128 bits which gives a hypothetical location space of $3.4 * 10^{38}$ locations. This is 3.4 trailed by 38 zeros, or 3,400,000,000,000,000,000,000,000,000,000,000,000,0

By this, we are convinced that the number of possible ip addresses will be enough to be assigned to any number of the computer devices in Nigeria for a very long time to come.

With the table below showing the IP address blocks already allocated to the Nigerian cyber space, it will be very convenient for the propose system to work effectively

Table 2. Major IP Address Blocks for Nigeria

From IP	To IP	Total IPs
41.58.0.0	41.58.255.255	65536
41.67.128.0	41.67.191.255	16384
41.71.128.0	41.71.255.255	32768
41.73.0.0	41.73.31.255	8192
41.73.128.0	41.73.159.255	8192
41.73.224.0	41.73.255.255	8192
41.75.16.0	41.75.31.255	4096
41.75.80.0	41.75.95.255	4096
41.75.192.0	41.75.207.255	4096
41.84.160.0	41.84.191.255	8192
41.86.128.0	41.86.159.255	8192
41.87.64.0	41.87.95.255	8192
41.138.160.0	41.138.191.255	8192
41.139.64.0	41.139.127.255	16384
41.155.0.0	41.155.127.255	32768
41.184.0.0	41.184.255.255	65536
41.189.0.0	41.189.31.255	8192
41.190.0.0	41.190.31.255	8192
41.203.64.0	41.203.95.255	8192
41.203.96.0	41.203.127.255	8192
41.204.224.0	41.204.255.255	8192
41.205.160.0	41.205.191.255	8192
41.206.0.0	41.206.31.255	8192
41.206.224.0	41.206.255.255	8192
41.211.192.0	41.211.255.255	16384
41.216.160.0	41.216.175.255	4096
41.217.0.0	41.217.127.255	32768
41.219.128.0	41.219.191.255	16384

41.219.192.0	41.219.255.255	16384
41.220.64.0	41.220.79.255	4096
41.221.112.0	41.221.127.255	4096
41.221.160.0	41.221.175.255	4096
62.173.32.0	62.173.63.255	8192
62.193.160.0	62.193.191.255	8192
80.248.0.0	80.248.15.255	4096
80.250.32.0	80.250.47.255	4096
82.128.0.0	82.128.127.255	32768
105.196.0.0	105.199.255.255	262144
105.235.192.0	105.235.207.255	4096
193.189.0.0	193.189.63.255	16384
195.166.224.0	195.166.255.255	8192
196.1.176.0	196.1.191.255	4096
196.27.128.0	196.27.255.255	32768
196.29.208.0	196.29.223.255	4096
196.40.192.0	196.40.255.255	16384
196.45.48.0	196.45.63.255	4096
196.200.64.0	196.200.79.255	4096
196.200.112.0	196.200.127.255	4096
196.207.0.0	196.207.15.255	4096
196.220.0.0	196.220.31.255	8192
196.220.64.0	196.220.95.255	8192
196.220.192.0	196.220.207.255	4096
196.220.224.0	196.220.239.255	4096
196.220.240.0	196.220.255.255	4096
196.222.0.0	196.222.255.255	65536
197.149.64.0	197.149.127.255	16384
197.156.192.0	197.156.255.255	16384
197.159.64.0	197.159.79.255	4096
197.210.0.0	197.210.255.255	65536
197.211.32.0	197.211.63.255	8192
197.214.96.0	197.214.111.255	4096
197.240.0.0	197.240.255.255	65536
197.242.96.0	197.242.127.255	8192
197.242.240.0	197.242.255.255	4096
197.244.0.0	197.244.255.255	65536
197.253.0.0	197.253.63.255	16384
197.255.0.0	197.255.63.255	16384
197.255.160.0	197.255.175.255	4096
197.255.208.0	197.255.223.255	4096
212.100.64.0	212.100.95.255	8192

217.14.80.0	217.14.95.255	4096
217.117.0.0	217.117.15.255	4096

3.4.1 Network Design for the System and Working Principle

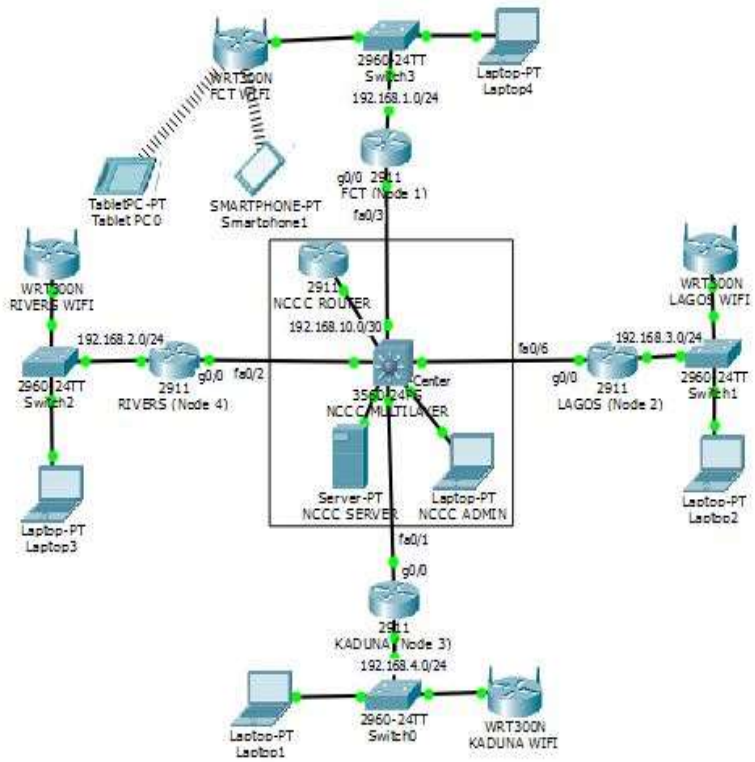

Fig. 4 Network design and configuration for the proposed system

From figure 4 above, the design entails complex configurations from the NCCC to all the state nodes. The network and devices shown on the Federal Capital Territory node (node 1) is same for all the remaining 36 nodes. All user devices like desktops, laptops, and other screen–based PDAs connected to any node via the node switch are anonymous. The NCCC can ping any node or any device; the green LED indicators shows successful communications when tested.

3.5 Proposed National Cybercrime Control System Interactive Interfaces

3.5.1 The Users

The graphical user interface of the proposed system is shown in the figure 5 below. The anonymous user login and the system sends request to control server at the NCCC via the core node of the network where the user is connected.

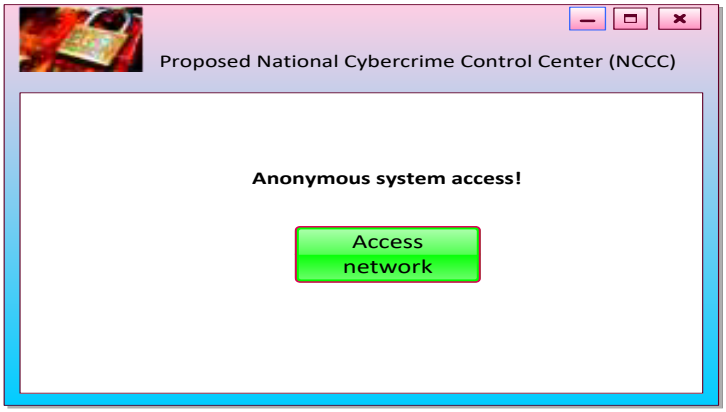

Fig. 5 Anonymous system login

Figure 6 below is the anonymous system access where the request of the user to access the network is granted upon the capture of the user's clear imagery. The system shall deny access upon obscured imagery. The clocking circuit is also activated.

Fig. 6 Anonymous system access

3.5.2 The Control Center

The control center oversees the activities of users in the national cyber space. So like earlier explained, they can track users' foot prints in the network.

Figure 7 below shows the node access interface at the NCCC. The control center login and can access all the nodes at a glance, a particular node could also be access for view, for example, the NCCC may want to view the Lagos node only. The detail log on that node could also be accessed.

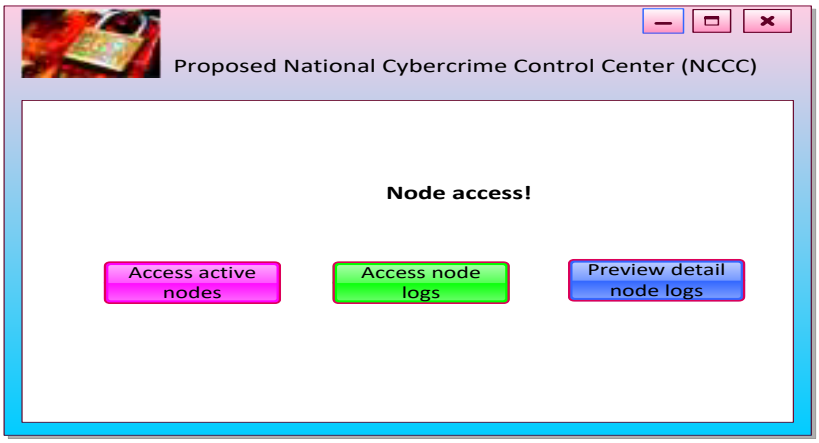

Fig. 7 Node access

Figure 8 below shows the users access interface at the control center. The NCCC could by pass any node to access any user on that particular node, access the logs and preview detail logs of the user.

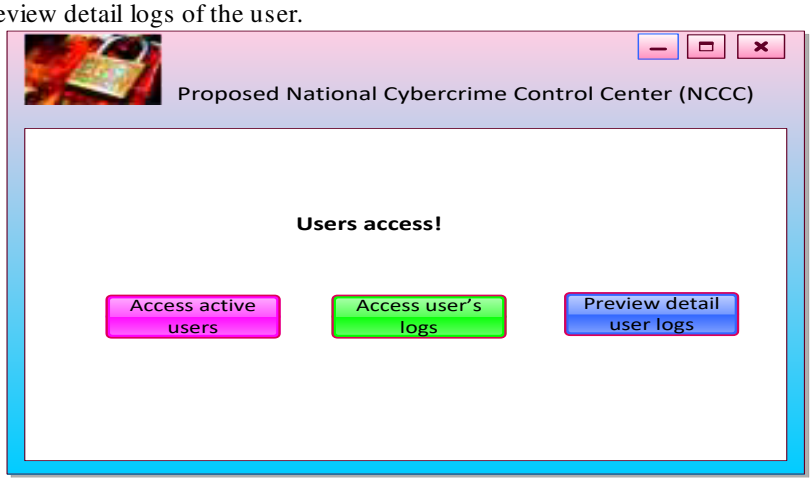

Fig. 8 Users access

Figure 9 below is the user log display interface at the control center. The NCCC could display the detail logs of any user with the user's captured image, the particulars of the screen based device that was used by the user. The anonymous with question mark in the user log display is actually the criminal whose captured image appeared along with other details, that is, user's device number, node number (state node in this case), computer's mac address, login time, logout time and the date the date that the user's device access the internet.

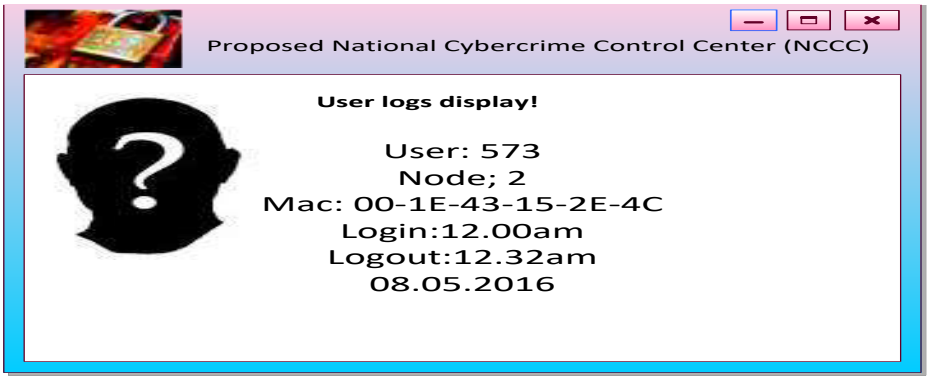

Fig. 9 User logs display

4 The Discussion of the System Design

The system design was based on the concept of IP addressing system where every device can be assigned an IP address. All devices on the network can be tracked through the IP address given to it.

Each of the 37 states of Nigeria was assigned to be a node. From the network shown in 3.2 above, node 1 was assigned to the Federal Capital Territory (FCT), node 2 for Lagos state, node 3 for Kaduna state and node 4 for Rivers State and so on to the 36th State which shall be assigned node 37. Every screen-based systems like laptop, desktop, ipads and phones that attempt to connect to the internet in any of the nodes shall prompt the NCCC server which shall automatically activate the imagery device to have the user's image captured and thus allow access to the internet. The sequence of the operations of any anonymous user and the control center is as explained and presented in figures 4 to 9.

The authority simply needs to implement the policy that ensure all Internet Service Providers (ISPs), GSM operators rout their network through the NCCC thereby putting all nodes on the same network of the NCCC.

The configuration and implementation of the network security Virtual Private Network (VPN) and the tunnelling technology will ensure the NCCC access to every nodes and users on the Nigerian cyber space.

5 Conclusion and Recommendations

From our investigation on cybercrimes, we observed its threat to the economy of a nation and even peace and security. This paper has been able to identify some common cyber crimes in Nigeria and their frequency of occurrences and came up with a design framework to combat them. The design concept was successfully simulated with a CISCO network tool. In this system, utmost secrecy, policy definition and its enforcement is of very high essence. Therefore, the authors of this paper shall cooperate with the authority for the practical implementation of the system. This practical approach shall reduce the incidences of cybercrimes in Nigeria to the barest minimum.

The foremost recommendation of this paper is for the National security and regulatory agencies like the Military and paramilitary, the Police, Department of State Services (DSS), Economic and Financial Crime Commission (EFCC), and Independent Corrupt Practices Commission (ICPC) to as a matter of urgent, see to the implementation of this practical frame work design system as proposed by this paper.

7 References

1. Abhatise, E. J.: Cybercrime definition, Computer crime Research Center. Retrieved on February 4 2016 from http:/www.crime-research.org/articles/joseph06/2 (2008)
2. Aluko, M.: 17 ways of stopping financial corruption in Nigeria (2004)
3. Anah, B. H., Funmi, D. L. Makinde, J.: Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology. www.ejournalofscience.org (2012)
4. Andreas, H.: University of Pennsylvania, Fighting Cybercrime with Packet Attestation (2011)
5. Ayantokun, O.: Fighting Cybercrime in Nigeria. http://archive.cert.uni-stuttgart.de/isn/2006/06/msg00034.html (2016).
6. CGI White paper: Cyber security in Modern Critical Infrastructure Environments. http://www.canadianinstitute.com/files/pdf/marketing/CGI-Whitepaper.pdf (2014)
7. Chawki, M.: Nigeria Tackles Advance Fee Fraud, Journal of Information, Law and Technology. http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/chawki/ (2009)
8. Deloitte Development LLC: USA, Combating the fastest growing cyber security threat. (2010).
9. Internet Society Global Internet Report 2014. https://www.internetsociety.org/ (2015)
10. Kofo, A. A.: Significance of 2006 Head Counts and House Census to Nigerian Sustainable Development. International Journal Of Basic And Applied Science, Vol. 01, No. 02 http://www.insikapub.com/ (2012)
11. Longe, O. B., Chiemeke, S. C.: 'Cyber crime 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)
12. Maitanmi, O., Ogunlere, S., Ayinde, S., Adekunle, Y.: Impact of Cyber Crimes on Nigerian Economy. The International Journal of Engineering and Science (IJES) www.theijes.com Vol. 2, Issue 4, pp 45-51 (2013)
13. Marco, G.: Understanding cybercrime: phenomena, challenges and legal response (2012)
14. Michael, B., PayPal.: www.pdffiller.com/en/project/63758181.htm?form_id=43555194 USA, Combating Cybercrime: Principles, Policies and Programs (2011)
15. Wada, F., Odulaja, G. O.: Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using Social Theories. African Journal of Computing & ICT www.ajocict.net Volume 5, No. 1. pp 69-82 (2012)
16. Wada, F., Odulaja, G. O.: Electronic Banking and Cyber Crime in Nigeria - A Theoretical Policy Perspective on Causation. African Journal of Computing & ICT www.ajocict.net Volume 4. No. 3. Issue 2 pp 69-82 (2012)