Cyber Crime Detection and Control Using the Cyber User Identification Model

Moses A. Agana - correspondence author
ganamos999@yahoo.com
+2348057847633
Department of Maths/Statistics/Computer Science
Federal University of Agriculture
Makurdi, Nigeria

Hight C. Inyiama
drhcinyiama@gmail.com
+2348034701121
Department of Computer and Electronic Engineering,
Nnamdi Azikiwe University
Awka, Nigeria

***Abstract* –This research was designed to identify cyber users as a strategy to detect and control cyber crime. The motivation was premised on the fact that every cyber user must create some impressions which are verifiable to identify him. The methodology adopted is the object oriented paradigm of system analysis and design. The crime scenario considered for detection are phising, identity theft and data theft. The platform for implementation of the system is PHP and java. MySQL was used as the database. The hardware used for implementation has inbuilt webcam or attached digital camera for facial image capturing, a GPS sensor to locate a cyber user's position, and a fingerprint scanner. The research is modeled to provide interfaces to capture the digital signatures for each information sent to the cyberspace, the user's fingerprints and facial image as mandatory login parameters, identify and record the geographical location of the user, the MAC address of the system used, the date, time and the kind of action carried out by the user while online, then record security threats for further investigation by cybercrime investigators. The results showed that the system can genuinely identify the cyber user and his/her criminal activities while online.**

Keywords – Cyber, Cyberspace, Cybercrime, biometrics, fingerprint, detection, investigation.

I. INTRODUCTION

Unguarded access to the Internet and the information it hosts ever since its evolution has been characterized with theft of data and information, abuse of privacy, data and information distortion, and related cyber vices, leaving the perpetrators hardly noticed. They can therefore be neither tracked down nor prosecuted. The menace is compounding security threats to individuals and the society at large. This is partly due to lack of adequate security restrictions to access, lack of proper cyber user identification/detection techniques and loose cyber regulations on prosecution of the culprits. It therefore becomes pertinent to provide a means that can assist cyber crime investigators to police and detect cyber criminals to enable them track down and prosecute the perpetrators.

Deviant behaviours, which do not conform with societal norms or with the laws of the land are termed "criminal acts". Some of the perpetrators of such criminal acts either do so deliberately as a mark of revenge, for financial or material gains, or out of leisure.

When crimes are committed via computer networks like the internet, they are said to be cybercrimes. Cybercrimes according to Halder, & Jaishankar [1] are defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".

The increasing dependence of businesses on computer systems has made many more organizations vulnerable to the impact of computer crime. Indeed, more companies are worried about the risk of computer crime than they are about product liability, fraud and theft. Cyber crimes can threaten a nation's security and financial health.

A. Statement of the Problem

The society has been so bedeviled with crime that there is every need to put security measures in every sphere of life. Conventional crimes like armed robbery, raping, stealing, cultism, etc. are easy to detect and the culprits can be prosecuted by law enforcement agents because of their physical nature. This is not the case with cyber crime, due to the fact that the cyberspace is quite wide and is a virtual reality. Cyber security is quite challenging, this is due to varied degrees of security features and management schemes within the cloud entities in the cyberspace. Majority of cyber criminal activities do not involve physical damage or stealing of equipment, but are rather intellectual manipulations, what the researcher has decided to coin ***white collar crime***. This makes it difficult to track down the cyber criminals. More so, there is no comprehensive policing system to check the activities of cyber users nor stringent regulations on the prosecution of the criminals if at all they can be detected. In this circumstance, one logical

protocol base needs to evolve so that the entire interconnection of components operates synchronously and securely [2].

Computer system vulnerabilities persist worldwide, and initiators of the random cyber attacks that plague computers on the Internet remain largely unknown. Most of the random attacks on computer resources are now increasingly implemented through the use of automated tools, called "bots", that direct large numbers of compromised computers to launch attacks through the Internet as swarms [3]. The growing trend toward the use of more automated attack tools has also overwhelmed some of the current methodologies used for tracking Internet cyber attacks. People take advantage of the anonymity of the Internet to facilitate their digital life. Abuse of the anonymity of the Internet by criminals is a predictable but inevitable dark side in an information society. Still in [3], the difficulty of tracing and identifying criminals is one of the main hurdles that cyber investigators meet every day.

Reporting these attacks is an essential first step to overcoming the growing problem of cyber insecurity. Several security control measures have been in existence, but do not appear to be efficacious. Some of such measures include:

- The International Cybercrime Reporting and Cooperation Act - H.R.4962" promulgated in 2010 by the United States government [2].
- The UK Data Protection Act 1998
- The Computer Misuse Act 1990 of the UK Parliament.
- The Payment Card Industry Data Security Standard (PCI DSS).
- The Personal Information Protection and Electronics Document Act (PIPEDA).

In addressing these problems, the following are pertinent questions to be answered.

- Is it possible to identify each user of the cyberspace?
- If it is possible to identify a cyber user, is it possible to identify cyber crime and the criminal?
- Is it possible to have a central control of all users of the cyber space as to be able to monitor and report cyber crime and the culprits to cyber crime investigators?

The concern of this study is thus to consider cyber security from the access control perspective, specifically by identifying the cyber user and reporting any criminal tendencies to cyber crime investigators who can then carry out further investigations, and possibly prosecute culprits.

B. Aim and Objectives of the Study

The aim of this research work is to design a model of cyber crime detection and control system using cyber user identification to secure the cyber space from crime by identifying users and their respective activities, so as to report such criminals to cyber crime investigators for appropriate prosecution to serve as a deterrent to others.

The following are the objectives of the study:

i. To uniquely identify each cyber user (through facial image and fingerprint capturing) with the IP address, MAC address of the system used and geographical position, then store information about his person and activities while on line.
ii. To secure data and information in the cyberspace from criminal tendencies/activities.
iii. To detect cyber crimes and the perpetrators at the time of access and report them to authorized cyber crime investigators for further investigation and prosecution.
iv. To design and implement a model of a cyber crime detection and control system using an eduportal site (www.ganamos.org) with the features in i – iv above.

C. Significance of the Study

This study is significant in several ways.

- The outcome of this research work will be useful to cyber crime investigators by helping them to detect the identity and location of a cyber criminal. This will ease further investigation and possible prosecution of the criminals.
- If the Cyber User Identification and Crime Detection System (CUICDS) designed in this study is put into use, it will scare cyber users from indulging in criminal acts. This is because it is common knowledge that once a criminal is identified, it is easier to prosecute him to serve as a deterrent to others, and once criminals know that they can be easily detected, they are scared of indulging in crimes.
- The implementation of the CUICDS will also give confidence of data and information security to Internet users as well as to individuals and organizations who host their valuable data and information in the cyberspace.
- This study will also open a new horizon of research for network security researchers to explore on how to detect and combat cyber crime through the cyber user identification approach.
- The findings of this research will also help governments of various nations on how to

promulgate legislations on the combat of cyber crime and the prosecution of cyber criminals.

D. Scope of the Study

Several techniques for network crime/intrusion detection exist, but this study is confined to the identification of the network (cyber) user. Considering the diverse and virtual nature of the cyberspace, the objectives are only achievable through an enterprise website like that of a bank or shopping mall since it will be quite arduous to control other people's websites. It is hoped that if it becomes an international standard, the same control can then be propagated to all other websites in the cyberspace.

II. THE CONCEPT AND SCOPE OF CYBER CRIME

A. Meaning of Cyber Crime

Moore [4] defines computer crime as any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target [5]. A computer attack may be defined as actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data [3]. When crimes are committed via computer networks like the internet, they are said to be cybercrimes. Cybercrimes are also defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)" [1].

Some authors prefer to tag cyber crime as ***cyber terrorism.*** Some definitions for cyber terrorism focus on the intent of the attackers. For example, the Federal Emergency Management Agency (FEMA) defines cyber terrorism as: "Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" [6]. Denning [7] defines cyber terrorism as the "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage". Krasavin [8] asserts that any deliberate use of information technology by terrorist groups and their agents to cause harm constitutes cyber terrorism.

Some security experts define cyber terrorism based on the effects of an attack. Included are activities where computers are targeted and the resulting effects are destructive or disruptive enough to generate fear potentially comparable to that from a traditional act of terrorism, even if initiated by criminals with no political motive. Under this "effects" view, even computer attacks that are limited in scope, but lead to death, injury, extended power outages, airplane crashes, water contamination, or major loss of confidence for portions of the economy, may also be labeled cyber terrorism[9]. Some observers state that cyber terrorism can take the form of a physical attack that destroys computerized nodes for critical infrastructures, such as the Internet, telecommunications, or the electric power grid, without ever touching a keyboard [10].

Different attack methods target different vulnerabilities and involve different types of weapons, and several may be within the current capabilities of some terrorist groups. Three different methods of attack based on the effects of the weapons used identified by [3] are:

- **Physical Attack:** A physical attack involves conventional weapons directed against a computer facility or its transmission lines.
- **Electronic Attack*:*** An electronic attack (EA) involves the use of the power of electromagnetic energy as a weapon, more commonly as an electromagnetic pulse (EMP) to overload computer circuitry, but also in a less violent form, to insert a stream of malicious digital code directly into an enemy microwave radio transmission; and
- **Network Attack:** A computer network attack (CNA), usually involves malicious code used as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an organization or computer user. Other forms of CNA are enabled when an attacker uses stolen information to enter restricted computer systems.

The third form of attack mentioned above is the focus of this study. Cyber crime is mediated via computer networks (the Internet in particular).

The increasing dependence of businesses on computer systems has made many more organizations vulnerable to the impact of computer crime. Indeed, more companies are worried about the risk of computer crime than they are about product liability, fraud and theft. Cyber crimes can threaten a nation's security and financial health.

Neil [11] advanced two reasons why computer crime investigators believe that the level of computer crime is usually much higher than reported.

i. Most computer-related crimes probably go undetected. A 1994 UN report estimated that the number of reported incidents might represent only five per cent of the total number of offences committed. This is consistent with reports from Australian law enforcement agencies. For example, during investigations into unlawful intrusion to computer and

communications systems, the Australian Federal Police determined that at least 80 per cent of computer crime victims were completely unaware that an offence involving their system had been committed.

ii. Few crimes that are detected are made public because many companies are loath to admit that their security systems are fallible. The 1997 OSCA survey in [11] showed that fewer than 20 per cent of those companies that had admitted to suffering some form of computer misuse reported the incidents to law enforcement. Some respondents were quite candid in their comments, indicating that their organizations had no mechanisms for determining whether or not computer misuse had or was occurring. Such a bias or indifferent approach to computer security is worrying to law enforcement, as it is in this environment that computer crime can thrive undetected.

B. Types of Cyber Crime

Cyber crimes exist in various forms. Crimes that use computer networks or devices to advance other ends include:

- Cyberstalking (blocking of networks)
- Fraud and identity theft
- Information warfare (through espionage and distortion)
- Phishing scams (Phishing attacks involve sending of emails from a trusted source which will then trick the recipient into giving his personal information. Phishing can easily cause identity theft). A phish attack is a mass e-mailing guiding recipients to sites where they are asked to divulge private information such as account passwords, credit card information, or bank account numbers [12].
- Hacking: This involves the unauthorized taking or stealing of information ranging from passwords to account numbers and usernames for the hackers to be able to take it and use it as their own for their benefit. This involves bogus websites and e-mails which require the victims to enter necessary information that are usually confidential. Hackers can as well send viruses to destroy programs in the hacked computers or networks[13]. Computer hackers opportunistically scan the Internet looking for computer systems that are mis-configured or lacking necessary security software. Once infected with malicious code, a computer can be remotely controlled by a hacker who may, via the Internet, send commands to spy on the contents of that computer or attack and disrupt other computers.
- Cyber stalking: the act of excessive tracking of an account with the purpose of torturing or blackmailing its owners.
- Cracking
- Copyright infringement (piracy and plagiarism)
- Child pornography
- Espionage
- Obscene or offensive contents sent into websites or as e-mails
- Drug trafficking. Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier websites to track illegal packages of pills.
- Cyber terrorism. A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer-based attack against computers, networks, and the information stored on them [14].
- Cyber warfare which involves activities that cross international network borders and the interests of at least one nation/state
- Financial theft (using networks to transfer money from people's bank accounts without authorization)
- Cyber scamming, such as multi-level marketing frauds, pyramid schemes, investment frauds, stock manipulation, credit card frauds and copyright violations**.**
- Telemarketing Fraud: This involves tricking one to send money to people he does not know personally or to give personal or financial information to unknown callers. This also involves false adverts of goods and services on the internet fooling people to subscribe to using their credit cards or other forms of payment without delivering the goods or services to the victims. This is termed **419** in Nigeria [15].
- Website cloning: This is the duplication of a website for criminal use. Often times, website cloning will take the form of known chat room or trade sites so that people will either unknowingly give information to the criminal or make a "fake" purchase, willingly giving money for a product that does not actually exist.
- Online gambling.

Abuse of privacy, whereby valuable and confidential information is lost or intercepted, lawfully or otherwise.

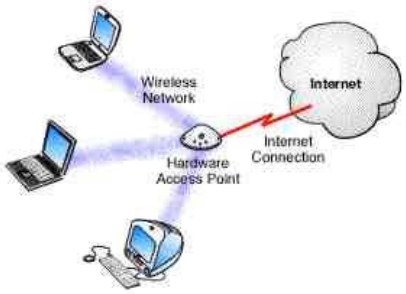


Figure 1: Wireless Packet Sniffing [16]

III. SYSTEMS ANALYSIS AND DESIGN METHODOLOGY

Interaction with Internet users, cyber crime investigators, law enforcement agents, website owner and web developers helped in the data gathering for this research.

The cyber user's identity, his activities while on line, the geo-location of the user and the time the user is on line, the MAC address and the IP address of the system used constitute the data used for the research.

The information in the database of the system is captured using three parameters supporting data mining viz: exploration, knowledge discovery and knowledge exploitation (informing authorities on information discovered).

A. Analysis of Terms and Conditions for Granting Access to Users of the System

A person is qualified to browse the Internet only if he meets the following conditions:

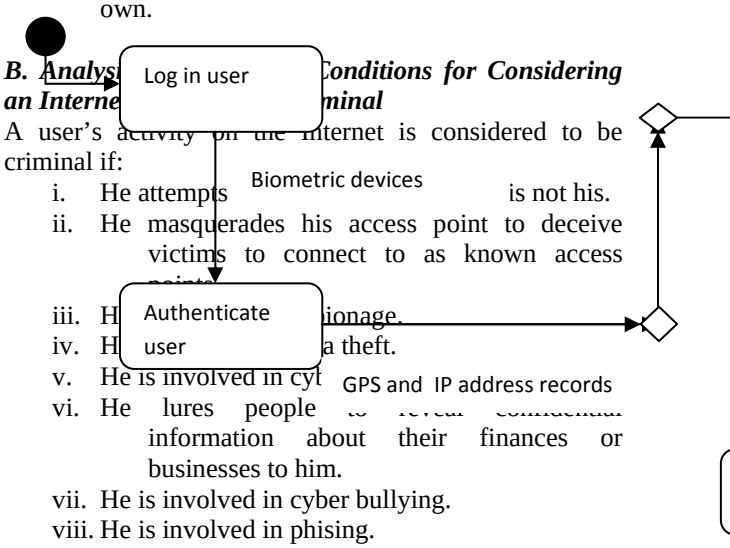
i. He allows his identity (especially facial photograph and finger prints) to be captured by the system.

ii. His user name, password and the captured facial identity are verified and authenticated to be his own.

B. Analysis of Terms and Conditions for Considering an Internet User to be Criminal

A user's activity on the Internet is considered to be criminal if:

i. He attempts [illegible] is not his.
ii. He masquerades his access point to deceive victims to connect to as known access [illegible]
iii. H[illegible]ionage.
iv. H[illegible]a theft.
v. He is involved in cyb[illegible]
vi. He lures people [illegible] information about their finances or businesses to him.
vii. He is involved in cyber bullying.
viii. He is involved in phising.
ix. He sends scams to people
x. He is involved in any known criminal activity not mentioned above using the Internet.



C. Conceptual Design of the CUICDS

The conceptual design of the proposed system will be carried out using activity diagram, data flow diagram and use case diagram.

Figure 2: Activity diagram of the CUICDS

As illustrated in figure 2 above, the activities performed by the cyber user identification system are as follows:

i. The cyber user logs in to surf the net.
ii. The cyber user's identity is captured at the point of log in and authenticated by the admin system before access is granted to the Internet.
iii. The system verifies and store the user's activities and location while online .

iv. If the user's activities have criminal tendencies, the cyber crime investigator is notified for appropriate action.

The flow of the activities is illustrated in the data flow diagram (figure 3).

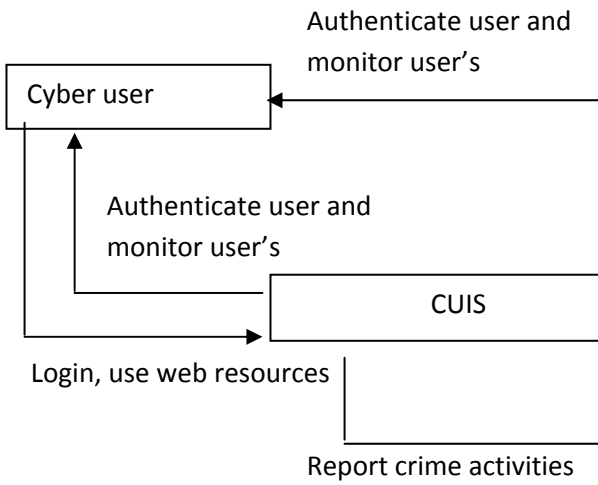


Figure 3: Data flow diagram of the CUICDS

The use case diagram of the CUICDS (figure 4) has three actors: the cyber user (criminal), the cyberspace administrator and the cyber crime investigator.

The cyberspace administrator performs four activities:

i. He logs in
ii. He authenticate the user's identity before access is granted him.
iii. He verifies the activities of the user while online.
iv. If the user commits any crime, the system generates a report to the cyber crime investigator.

The use case of the cyber crime investigator shows three activities:

i. He logs in.
ii. He investigates reported crime.
iii. He initiates the prosecution of the criminal.

The use case of the cyber criminal shows various criminal tendencies exhibited by the cyber criminal while on line:

i. The user logs in.
ii. He uses the web (Internet) resources and may commit crimes like:
    a. Stealing user ids,
    b. Guessing passwords,
    c. Masquerading access points,
    d. Stealing data, etc.

Figure 5 shows the context diagram of the CUICDS. There are five major entities in the system with varying roles:

i. The cyber user who logs in and uses resources of the web.
ii. The database of the user's identity and location which is a repository of who the user is and where he is at the time of access to the Internet.
iii. The cyber user identification system that collects and processes the user's activities while online.
iv. A database of reported criminal cases that stores information about cyber users who commit crime and the types of crime committed.
v. The cyber crime investigator who investigates criminal cases and initiates prosecution of criminals.

Figure 6 shows the system flowchart for the system architecture of the cyber user identification and crime detection system.

As illustrated in figure 6, the system flowchart shows the various steps in the cyber user identification and crime detection system in a top-down design as follows:

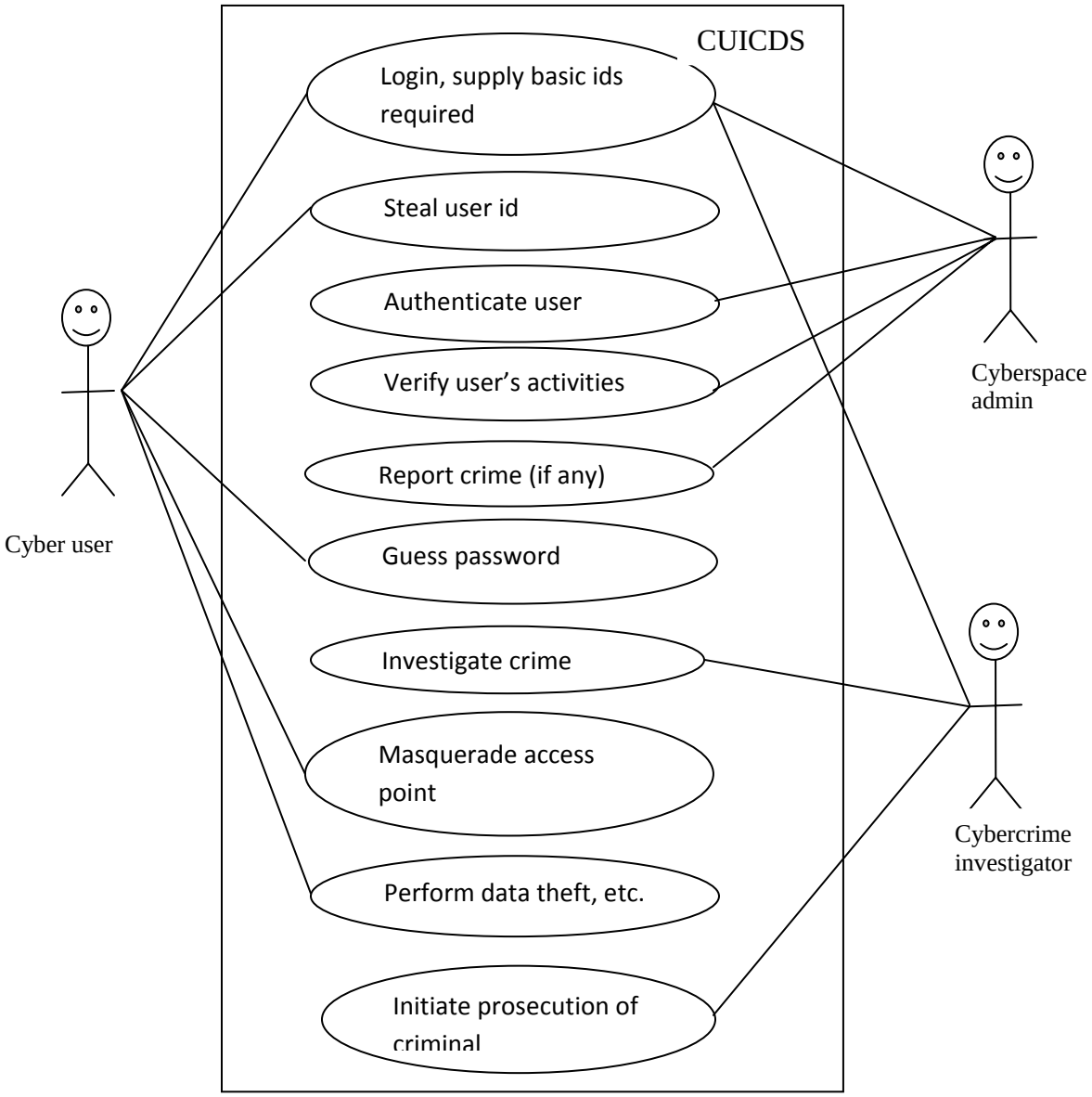
i. The system must be powered on first
ii. The user logs in, supplying his user name and password
iii. If the user's name and password are incorrect, the user is denied access and the process terminates.
iv. If the user name and password are correct, the user is granted access, then his biometric

features (finger print, facial image, iris scan, etc.) are captured and stored in the database.

v. The user's geographical location at the time of access is captured and stored in the database.

vi. The user's activities while on line are captured and stored in a database. If the user's activities while on line are criminal, a report is sent to the cyber police to investigate for further action, otherwise, the system terminates.

Figure 7 shows the object model of the cyber user identification and crime detection system. The system under considering is modeled to identify users, their locations, record the user ID and location at the time of access to the cyberspace, and report any threat to security exhibited by the user to the host cyber crime detector and monitor of intrusion from where the cyber police is notified of the crime for further investigation and possible prosecution.



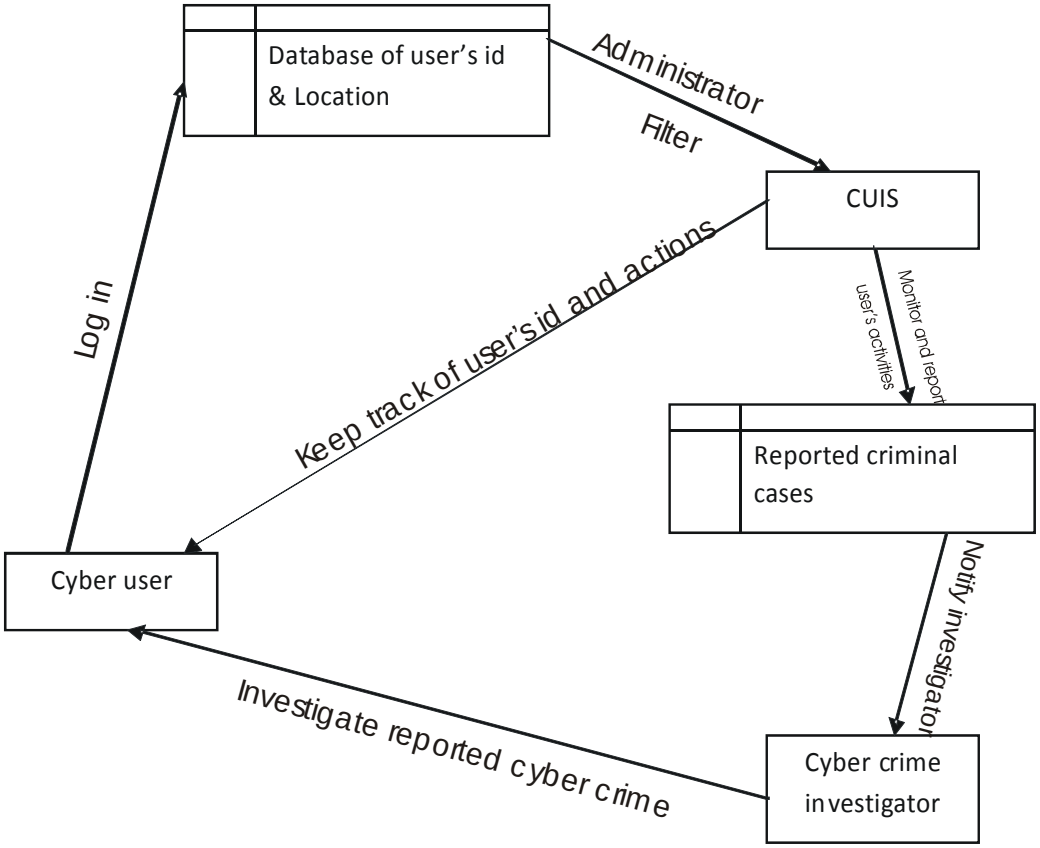


Figure 5: Context diagram of the CUICDS

D. Resources

The hardware and software resources needed for the successful execution of this research are enumerated in this section.

1. Hardware Resources

The hardware resources needed for the development of the Cyber User Identification and Crime Detection System (CUICDS) are as follows:

- Laptops/notebooks/desktops with in-built camera (webcam)
- PC digital camera/web cam for face/iris recognition
- Fingerprint scanners
- Palm print scanners
- Embedded Fingerprint Sensors
- DNA scanner/analyzer
- Live scan devices (International Standard Organization/FBI- compliant)
- GPS sensors
- Mobile monitoring stations for law enforcement officers.

2. Software Resources

- As stated earlier, the software requirements for the Cyber User Identification and Crime Detection System (CUICDS) are and HTML, with MySQL as the database.

IV. RESULTS, CONCLUSION AND RECOMMENDATIONS

A. Results

The general test implementation of the system is on-going in a website www.ganamos.org. The dependable results so far are the system models such as activity diagram, data flow diagram, use case diagram, entity relationship diagram, system flowchart and object model illustrated in the previous section. The results empirical results generated from the system so far are illustrated in the screen forms that follow:

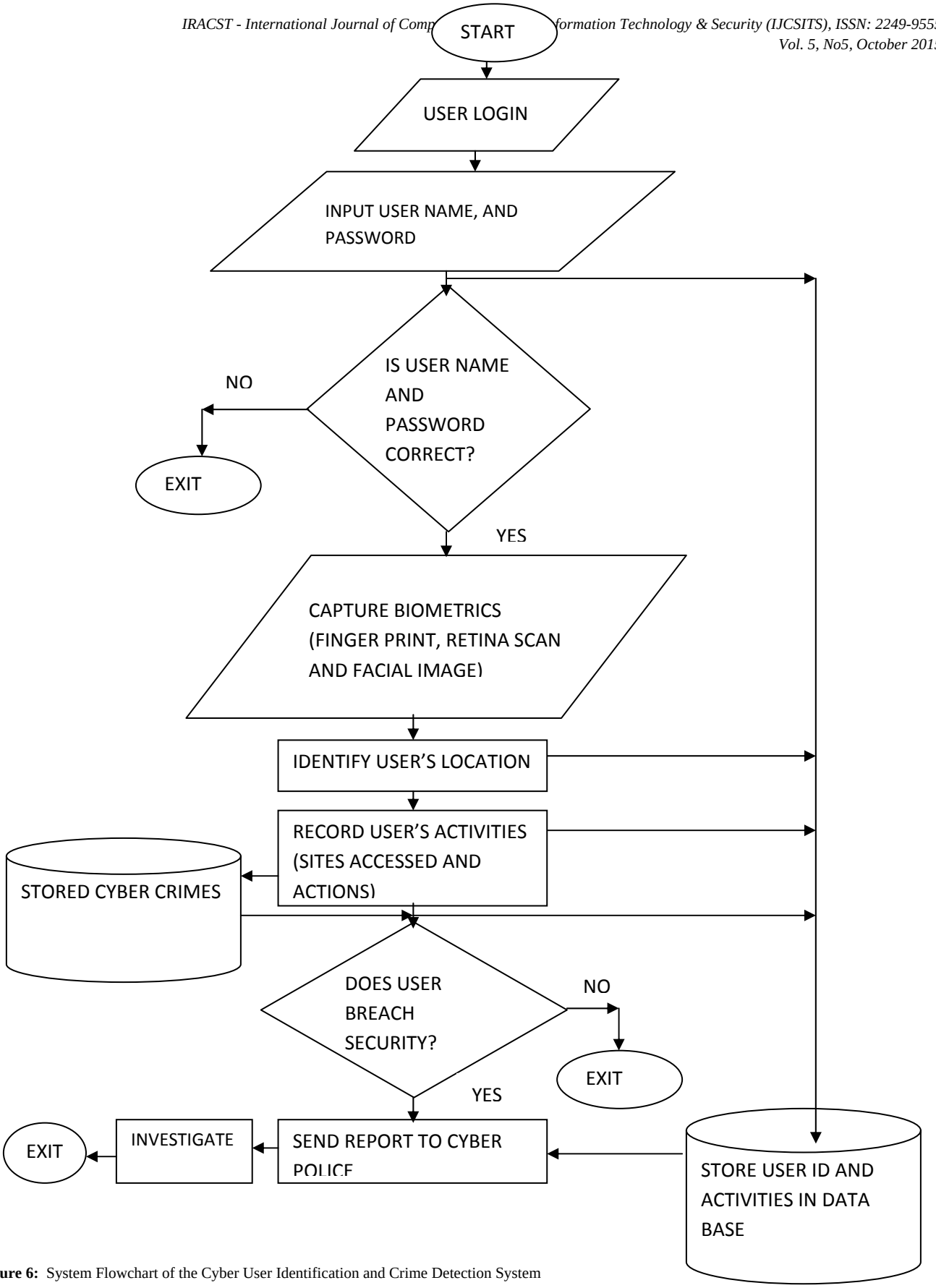
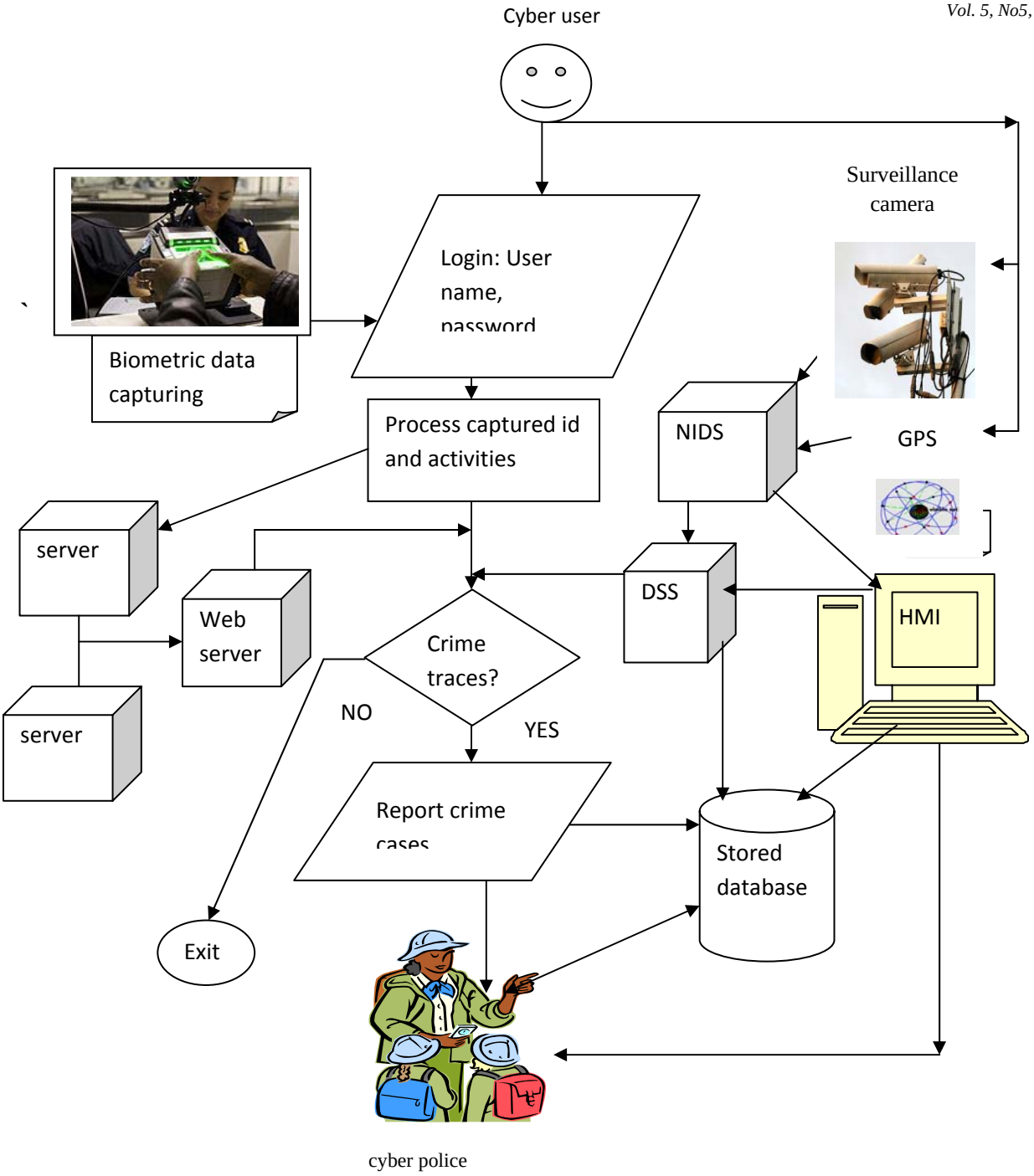


Figure 6: System Flowchart of the Cyber User Identification and Crime Detection System



7: Object Model of the Cyber User Identification and Crime Detection System

Figure 8: Log in screen

The log in screen above shows the access point for one who wants to log on to the website.

Figure 9: Facial Image login Session

Figure 9 above shows how the user's facial image is captured as he logs in.

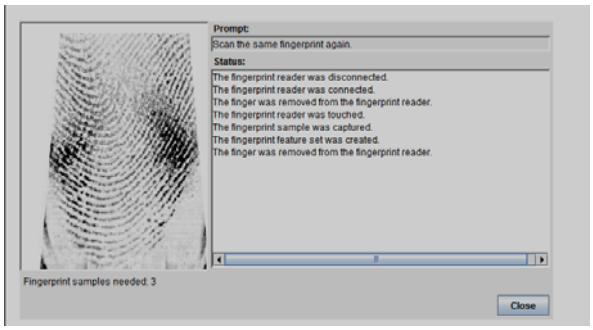


Figure 10: Fingerprint login Session

Figure 10 above shows how the user's fingerprint is captured as he logs in.

Figure 11: Password login Session

Figure 11 above shows a user's password login session

Figure 12: User's Home Page

Figure 12 above shows the home page from where a user that utilize web resources. This is where criminal activities can be tracked from.

Figure 13 shows the admin page from where an administrator can click on the ***crime report*** option to view crime reports. The administrator can also post adverts in this page. The report viewed by the administrator on the activities of a cyber user (visitor to the website) is as illustrated ion table 1.

B. Security of the System

Since criminals always device new strategies to achieve their purpose, it is pertinent to secure the proposed system especially from session hijack due to distributed denial of service by ensuring that as an international standard, all systems with access to the Internet must identify users and recursively too while on line. A page refreshes at intervals of seconds to capture parameters of users recurrently to forstall session hijack.

Figure 13: Administrator's Home Page

Table 1: Log Report for Visitor 20150608512047857

Crime Report!

Mr Agana Moses

S/N	USERNAME/ VISITOR	DATE & TIME	IP ADDRESS	MAC ADDRESS	GEOLOCATION	CRIME TYPE	FACIAL IMAGE URL	FINGERPRINT
1.	20150913412059381	2015-09-13 10:57:25 pm	154.66.38.179	System Denied	Longitude: 3.8964 Latitude: 7.3878	DATA THEFT	View Facial Image	View Facial Image
2.	20150914379357498	2015-09-14 12:14:15 pm	197.211.53.15	System Denied	Longitude: 8 Latitude: 10	ESPIONAGE	View Facial Image	View Facial Image
3.	20150914379357498	2015-09-14 12:14:34 pm	197.211.53.15	System Denied	Longitude: 8 Latitude: 10	PHISHING	View Facial Image	View Facial Image

The three-tier authentication (facial image, fingerprint and password) required during loggging in also guarantees the security of the system. Furthermore, the system is not to run independent of network intrusion mechanisms and techniques such as the Open Source Security Information Management (OSSIM). The goal of OSSIM is to provide a comprehensive compilation of tools which, when working together, grant network/security administrators with a detailed view over each and every aspect of networks, hosts, physical access devices, and servers.

C. Conclusion

Identity-based attacks (IBAs) are one of the most serious threats to wireless networks. There have been several attempts to detect network attacks (cyber crime) using various techniques. Recently, received signal strength (RSS) based detection mechanisms were proposed to detect IBAs in static networks [17]. Although mobility is an inherent property of wireless

networks, limited work has addressed IBA detection in mobile scenarios. More so, emphases have always been on attack detection and control without stressing the identification of the criminals (culprits). In this research, we propose a paradigm shift from mere cyber attack detection and control, to the detection/identification of the cyber criminal, who hitherto appeared to be anonymous.

This is based on the fact that every system user (whether criminal or law abiding) usually leaves or creates an impression at the scene of operation, and different persons can be distinguished with the help of biometric identification technology according to the unduplicated features of the human body. Biometric authentication determines the identity of the person mainly through examining the physiological or behavioral features of different people.

As an iterative system still under design, the design objectives have so far been achieved at the level of development.

D. Recommendations

1. Strong legislations should be enacted by each nation and at United Nations level on combating cyber crime.
2. A special anti-cybercrime police force should be established to combat cybercrime.
3. All websites in the Internet should specify and contain surveillance software for security checks against threats, and should permit cyber police access to check threats as to detect and apprehend criminals.
4. Punitive measures should be specified for various categories of cybercrime as is the case with conventional crime and the criminals should be prosecuted when apprehended.
5. Cyber security education should be introduced at all levels of education to enlighten netizens and prospective ones on possible threats they are likely face while using the Internet.
6. Trans-border synergy should be initiated among nations with wireless connection through GPRS for trans-border cyber police officers working in the field. Such a system should also be designed to provide a communication tool with international organization networks and information databases as well as national organizations under the protocol of e-government projects to combat cyber crime
7. Organizations should initiate strong security measures to protect their digital data.
8. Hardware and software developers should be persuaded to build into new products technological solutions to the prevalent cyber insecurity.

REFERENCES

[1] D. Halder and K. Jaishankar, Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global, 2011.

[2] http://en.wikipedia.org/wiki/computersecurity. Computer Security. Accessed on 08/03/2013.

[3] W. Clay. (2005), Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Service Report for Congress, 2005. Accessed on 3rd February, 2013 at http://www.history.navy.mil/library/online/computerattack.htm#summ .

[4] R. Moore, Cybercrime: "Investigating High-Technology Computer Crime", 2005. Anderson Publishing, Cleveland, Mississippi.

[5] G.K. Warren and G.H. Jay, Computer forensics: incident response essentials. Addison-Wesley, New York, 2002, p. 392.

[6] http://www.fema.gov/pdf/onp/toolkit_app_d.pdf. Computer Attack. Accessed on 12/03/2013.

[7] D. Denning, "Activism, Hactivism, and Cyber terrorism: The Internet as a tool or Influencing Foreign Policy," in Arquilla, J. and Ronfeldt, D. (ed.), Networks and Netwars. Rand, USA, 2001, p. 241.

[8] S. Krasavin, What is Cyberterrorism?, Computer Crime Research Center, April 23, 2004. Accessed from http://www.crime-research.org/analytics/Krasavin/ on 12/03/2013.

[9] D. Denning, Is Cyber War Next?, Social Science Research Council, November 2001. Accessed on 12/03/2013 from http://www.ssrc.org/sept11/essays/denning.htm.

[10] D. Verton, A Definition of Cyber-terrorism, Computerworld, August 11, 2003.

[11] B. Neil, Digital Crime: Policing the Cybernation. Kogan, London, 1997, p.10.

[12] B. Vijay B, G. Ajay and A. Ala, Detection of masquerade attacks on Wireless Sensor Networks, 2010. Available at http://www.ists.dartmouth.edu/library/343.pdf. Accessed on 13/03/2013.

[13] http://www.infobarrel.com/. Different Types of Cyber Crimes: A Pressing Cyber World Issue. Accessed on 05/05/2013.

[14] J. Balkin, J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman and T. Zarsky, (eds). Cybercrime: Digital Cops in a Networked Environment. New York University Press, New York:, 2006.

[15] http://www.fbi.gov/ . Common Fraud Schemes. Accessed on 04/05/2013.

[16] C. Low, Understanding Wireless Attacks and Detection. Available at http://www.sans.org/reading-room/click/528. Accessed on 10-04-2014.

[17] INFOCOM, Identity-based Attack Detection in Mobile Wireless Networks. Proceedings of the IEEE held in Shanghai, April 10-15, 2011, pp. 1880-1888. Available at http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp. Accessed on 02-04-2014.

AUTHORS PROFILE

Moses A. Agana is a lecturer in the Department of Maths/Statistics/Computer Science, Federal University of Agriculture Makurdi, Nigeria. He is a Ph.D. student researching on Cyber security at the Ebonyi State University Abakaliki, Nigeria.

Hight C. Inyiama is a professor of computer science in the Department of Computer and Electronic Engineering, Nnamdi Azikiwe University Awka, Nigeria.