International Journal of Engineering & Technology, 7 (3.19) (2018) 39-48

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Multi-level Evidence-based Cyber Crime Prosecution Information System

Moses Adah Agana[1] and Ruth Wario[2]

[1]Department of Computer Science and Informatics, University of the Free State, South Africa
ganamos999@yahoo.com
[2] Department of Computer Science and Informatics, University of the Free State, South Africa
warioRD@ufs.ac.za

Abstract

This research work was designed to utilize multi-level cyber crime detection and control system to provide enhanced real-time evidence to cyber crime investigators to aid them in prosecuting cyber criminals. The design was based on a robust system combining user-identity, device identity, geographical location and user activities to provide evidences to uniquely identify a cyber user and detect crimes committed. The system captures the user's facial image and biometric finger print as mandatory login parameters in addition to username and password before granting access. The system was tested and implemented in a real time cyber security website www.ganamos.org. The results showed that it is possible to divulge the identity of cyber users and associate their activities with the devices they use, the date, time and location of operation. These can provide real-time evidences to law enforcement agencies to track down and prosecute cyber criminals.

Keywords:*Cyber, Crime, Identity, Prosecution, Evidence.*

1. Introduction

Information explosion and the ever increasing need to harness them for easy and timely dissemination has propelled the establishment of computer networks [1]. The increased need for information sharing among people and organizations has informed the over dependence on computer networks in our contemporary time, and the resulting security challenges are not easy to contend with. Unguarded access to the Internet and the information it hosts since its evolution has been characterized with various crimes [2].

The growing trend of insecurity in the cyberspace in recent times and the difficulty in detecting the culprits due to the anonymity of Internet users and difficulty in providing a proof (evidence) of a crime based on non-repudiation calls for a didactic approach towards providing a means of assisting cyber crime investigators to combat the menace and prosecute the culprits.

Deviant behaviours, which do not conform with societal norms or to the laws of the land, are said to be 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 such as the internet, they are said to be cyber crimes [1]. Cybercrimes refer to 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 [3].

While expressing worry over the insecurity of computer networks and the increasing dependence on them [4] emphasized the need to secure applications over the Internet as the interconnectivity of the emerging digital world would bring new opportunities and threats to both the private and public sectors. Lack of confidentiality and integrity of processed data in the cloud as well as non-availability of data on scheduled time due to some setbacks have been identified as some of the major problems that make it difficult to get concrete evidences to facilitate the prosecution of cyber crimes [5]. As a follow up, it has therefore been suggested that the integration of reviewable security measures into the cloud can enhance cyber crime policing and prosecution.

Russian hackers invaded sensitive State House data in the White House in spite of the sophisticated United States cyber security measures. Though the United States Government claimed that the hackers only had access to unclassified information, it was reported that the hackers were able to pry into the President's schedules [6]. The scenario provided fertile grounds for Daniel Trump of the Republican Party in the United States 2016 presidential to criticize his Democratic Party opponent Hilary Clinton of inefficiency because the hacking occurred in her time as Secretary of State. It was a major point that Trump used to convince the electorate that eventually saw his victory at the 2016 United States presidential polls. It is not only competitors that might be gaining access to the network of an organization or that of an individual. As larger businesses or individuals become more security conscious, criminals of varied kinds also plague the networks for various reasons (revenge, self-esteem, financial gain, etc). In most cases, people with criminal tendencies can set up wireless network nodes with strong signals to deceive others to connect to, and then use the nodes to exploit them.

Information security is really about business continuity while taking precautionary measures against a natural disaster, criminal attack, and errors committed by users or caused by system failure. The Internet and related technologies are prone to a variety of crimes orchestrated by a variety of persons or groups [7]. 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. Computer system vulnerabilities persist worldwide, and initiators of the random cyber attacks that plague computers on the Internet remain largely unknown. Conventional crimes such as armed robbery, rape, stealing, cultism, etc. are easy to detect and the culprits can be prosecuted by law enforcement agents because of their physical nature [8]. This is not the case with cyber crime due to the fact that the cyberspace is quite wide and is a virtual reality. This is partly due to lack of adequate security restrictions to Internet access, lack of proper cyber user identification/detection techniques and loose cyber regulations on prosecution of the culprits.

Technological innovations that make provision for obfuscation and encryption are greatly responsible for the difficulty in cyber crime policing and prosecution. Some of the electronic chips that cyber crime is mediated through are embedded in personal devices like wrist watches, mobile phones, and related wireless storage devices that can be hidden in ceilings, under carpets, in wall crevices, etc. not easily identifiable by crime investigators. Even if the investigators can identify the devices, techniques like steganography that enable images to be used in hiding data and data encryption make it arduous for the investigators to decipher the contents of the devices [9].

2. Statement of the Problem

Cyber crime investigators are always faced with the problem of locating and identifying cyber criminals. Even if a crime or intrusion is detected, getting a substantive evidence to enable crime investigators to prosecute the criminals is often a problem due to the fact that the cloud that hosts the Internet is too broad and is a virtual reality.

A major problem with cyber crime policing and prosecution that triggered this research is the anonymity of the criminals. They utilize techniques that conceal their identity such as cryptography, remailers (intermediary mail servers that act as gates between a sender and recipient of an email) to communicate an email discretely, etc. to achieve their purpose [10]. This scenario calls for the development of a logical protocol base to synchronize and secure the entire interconnection of network systems and also to serve as a repository for cyber crime investigators to get information that can aid them in detecting and prosecuting the criminals. The motivation for the research is premised on the fact that each cyber user has unique traits that are traceable to him during and after his session on the Internet.

3. Aim and Objectives of the Study

The aim of this research work is to design a model for detecting cyber crime by identifying the unique features of the cyber users and reporting their criminal activities to provide information to cyber crime investigators to use in prosecution.

The objectives of the study are to develop a system that can:

(1) Identify each Internet user uniquely (by capturing the system IP address, MAC address, facial image, fingerprint and geographical location of the user) then store them with the user's activities while online.

(2) Detect cyber crimes as well as the criminals and report them to authorities in charge of cyber crime investigation for appropriate prosecution.

(3) Provide a framework for future researches in cyber crime detection and control.

4. Crime Theories Relating to Cyber Crime

Certain theories exist that to the topical trend of cyber crime in the contemporary society. A brief pointer is made to some of them as follows:

4.1 Technology-Enabled Crime, Policing and Security Theory

This theory states that crimes are enabled and co-evolved by technologies. The theory upholds that the competition between security agents and criminals for technological edge results in relatively confusing and therefore unmanageable threats to society [11]. People may therefore gainfully use technological developments for betterment of living or misuse them. This theory applies to cyber crime because people take undue advantage of the versatility of the Internet as a new technology to anonymously commit crime.

4.2 The Routine Activity Theory

This theory postulates that for a crime to be committed, there must be a target, lack of an inhibitor to prevent the occurrence of the crime and the motivation to commit the crime. These three scenarios have to occur simultaneously for a crime to be committed [12]. This theory applies to cyber crime. Cyber criminals spend time to spy, practice how to break in and cover tracks if they succeed, expecting some gains. The numerous resources that people depend on for daily business are targets, the mobile technology nature of the Internet and its near unrestricted access make it easy for cyber crime to be successfully committed.

4.3 The Opportunity Theory

This theory states that crimes are committed due to the opportunities that exist for them to occur [13]. Cyber criminals succeed because the unbridled nature of the cyberspace, the anonymous nature of Internet users, etc. provide opportunities for them to do so.

4.4 The Technology Theory

Computer technology provides means of protecting data and information from unauthorized access or criminal tendencies. Some of such security measures that apply as counter measures to cyber crime include access authorization, user authentication, firewalls, etc. The security models and measures use such techniques as cryptography, steganography, etc. Criminals however devise means of circumventing some of these security measures [13]. The success of cyber crime in our contemporary time is as a result of the failure to incorporate into the cyberspace these security measures at the earlier design stage.

4.5 The Crime Displacement Theory

This theory postulates that criminals always devise strategies to displace or move crime from one place to another as well as to targets geographically and temporarily according to the crime type [13]. This theory applies to Internet resources which can be accessed even by mobile devices irrespective of geographical location. Some of reasons for the difficulty in prosecuting cyber criminals include the fact that most of them reside outside the country where the crime is committed, coupled with the difficulty in defining what is legal or illegal in the cyber space, lack of a single or unified cyber police, etc. [14].

5. Some Existing Network Intrusion/Cyber Crime Detection Strategies

There are several network data security measures in place but criminals have always devised means of circumventing them. Some of such existing security measures include the use of secure protocols, antivirus software, encryption, firewalls, etc.). Apart from detecting intrusion, there are also some software and hardware systems that can both detect and prevent intrusions in networks. Some of such models/systems are as follows:

5.1 A Simple Intrusion Detection Model

A simple model of a typical instruction detection system is made up of the ontology and knowledge bases, the fuzzy logic, the alarm system, the response, etc. Figure 1 illustrates the model, showing how a pre-knowledge of likely crime incidences is built into a network system utilizing a fuzzy logic system that will detect attacks and notify the system administrator of any attack via the alarm system for a counter measure to be initiated [15]. An intrusion detection system unfortunately only detects intrusion without identifying the intruder.

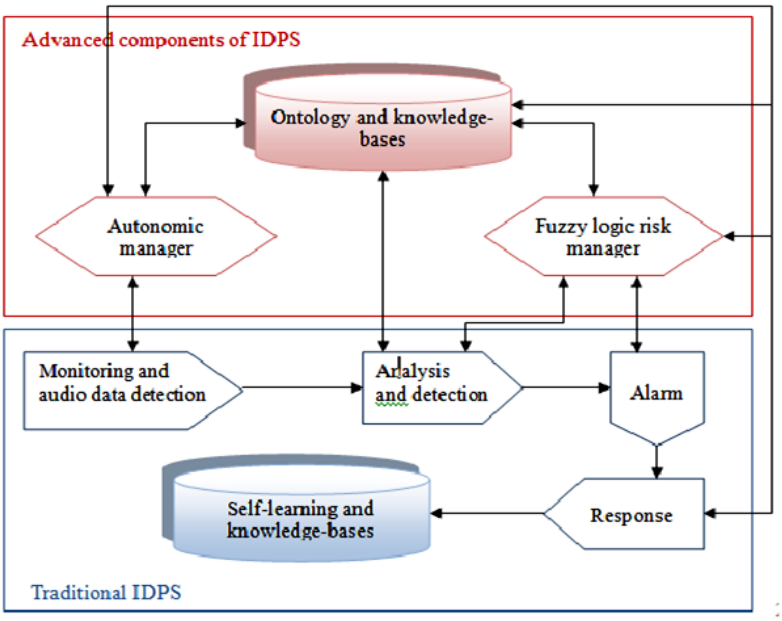

Figure 1. A Typical Intrusion Detection System [15]

5.2 Intelligent Agents

Intelligent agents are artificially intelligent systems that have autonomous powers controlled by computer systems. Such systems can plan and implement events by co-operating and sharing data with each other. Intelligent agents are suitable for combating crime such as cyber crime because of their mobile and adaptive features in the environments they operate. Intelligent agent systems are thus able to learn, recall, recognize and classify information. In the field of security, agents create networks of individuals infiltrating given theatre of actions in order to gather information that is necessary to sustain protected entity's security [16].

Artificial immune systems are models in computer technology derived from immune systems and function to provide security to computer systems (like intrusion detection and control) just as biological immune systems provide to body systems against disease infections. The agent framework proposed by [16] uses several types of agents that resemble the society in which different types of individuals perform dedicated, specialized tasks. The architecture of the intelligent collector agent shows that it uses a database that allows for classification of network traffic. The collector agent observes network flows and uses appropriate parsers to decode the required information. Identified network entities and their characteristics are stored in the profile database. Profiles are created and updated constantly while new information appears as illustrated in Figure 2.

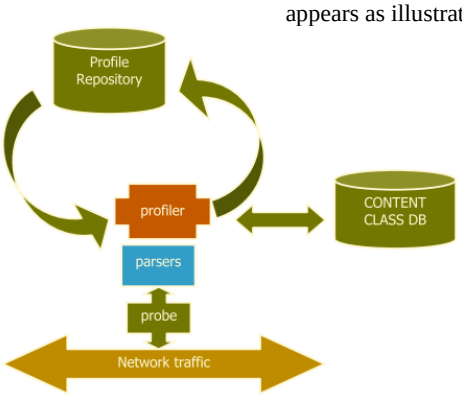

Figure 2. Collector Agent Architecture [16].

In a related development, there is a software agent that has been built to enhance network server security in a Windows NT network system and the work stations [17]. Such an agent responds to the message received from the other agent at the user end by creating a communication thread that transmits data back to the agent at the user end. This is illustrated in Figure 3.

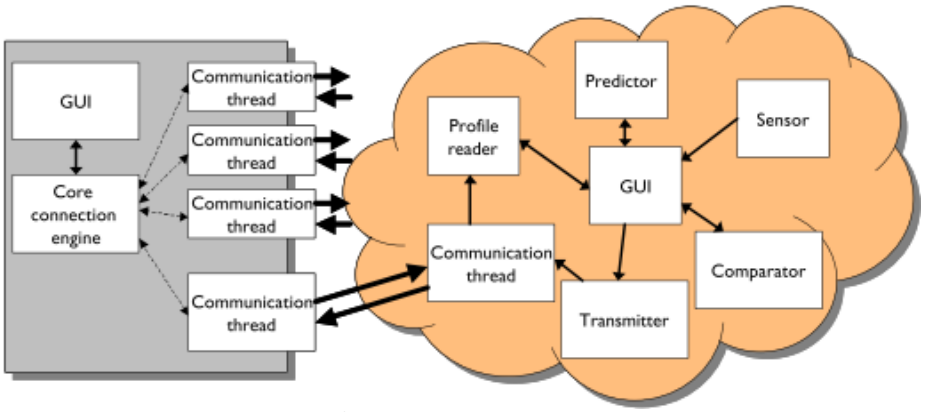

Figure 3. A Software Agent Environment Topology [17]

As illustrated in Figure 3, there are specialized processes that enable the intelligent agent to communicate with each user agent with effectiveness and efficiency to facilitate quick response to network monitoring requests. The agent is made up of the following:

(a). A sensor used in monitoring the various application programs that are currently running and keeps track of the user's activity and identity.

(b). A transmitter for transmitting signals to the main agent which can then respond by sending the profile of the user so far gathered as well as an audit-log file for a month.

(c). A profile reader for reading the user's profile.

(d). A comparator for comparing the user's profile with the information that the sensor has gathered. If there is a variation between the current behaviour profile and the accepted behaviour pattern defined by the user's profile, the comparator sends a signal to the transmitter describing the invalid behaviour which is in turn sent to the core agent. An invalid behavior detected can trigger some actions such as a warning signal to the system administrator or end user, inhibition of the application that caused the invalid behaviour and preventing the end user from running any further applications. Most available intelligent agents only detect and report the occurrence of an intrusion without keeping a log of the location of the intruder or his biometric identity.

5.3 Global Positioning System (GPS)

Advancements in technology have enabled the design of satellites that orbit the earth and transmit timed radio signals continuously for use in identifying positions on the earth [1]. Global positioning systems are used to identify the geographical locations of objects or people connected to the satellite system and therefore have applications in security, where they can be used to locate and track down criminals. A GPS usually has a receiver and a display screen that can either be hand-held or mounted on a moving or static device. The receiver picks up transmissions from nearby satellites, interprets the information gathered from them and computes the longitude, latitude, and altitude of what is monitored, displays the outcome on the screen or stores it to a database for easy access and processing [18]. It is possible to make a standard for all internet-based and other related telecommunication devices to have in-built GPS systems to identify users' locations at the point of accessing the cyberspace. This can also be incorporated in Host Monitors of Intrusion (HMIs) and Network Intrusion Detection Sensors (NIDSs) as a cyber policing strategy to control cyber crime. A GPS that only identifies the location of the intruder without an incorporated system to capture the identity of the user cannot provide enough evidence for crime investigators to use for prosecution.

5.4 Surveillance and Monitoring Systems

Cyber crime in most developed countries such as the USA is detected through surveillance (cyber policing) by specialized law enforcement agents. For instance, since 2001, the Florida Police Department has used a surveillance system called the Multistate Anti-Terrorism Information Exchange (MATRIX) to counter terrorism. The system combines police records with commercially available information about some U.S. adults to help crime investigators to trace patterns of events to people. The system is said to have extraordinary processing speed [19]. A variety of surveillance techniques and systems exist as enumerated below [20]:

Use of Network Sniffing Software

Network sniffing software is used to detect network sniffing especially in 802.11 layer 2. It is a wireless network detector that can run in both Windows and UNIX, example *Kismet*. This cannot however identify the intruder.

Access Point (AP) Monitoring

This is a means of detecting wireless network attack by keeping track of authorized access point equipment and their various service set identifications, MAC address, etc. by the wireless network owner so as to compare what the monitoring component gathers from the wireless frames it listens to with the pre-recorded information. If there are strange APs or signs of an attack, an alert is given on a possible man-in-the-middle attack without however identifying the attacker.

Access Control Mechanisms

Three major access control strategies have been identified to be useful in providing information to cyber crime investigators [1]. These include:

(a) What the user has; examples include personal access devices like entry identity cards, credit cards, debit cards, etc.

(b) What the user knows; examples include personal identification numbers (PINs), passwords, digital signatures, etc.

(c) What the user is (his physical/physiological traits). This is said to be the most dependable access control strategy that makes use of biometric verification and authentication (finger prints, facial recognition, iris scan, etc.) to uniquely identify a system user.

The various access control strategies if integrated with GPS and access point monitoring systems apart from authenticating and authorizing users can help to uniquely identify system users and provide useful information to crime investigators. Evidences of non-repudiation are drawn primarily from biometric features of system users and these can greatly aid in the prosecution of culprits.

6. Methodology

There are several network data security measures in place but criminals have always devised An iterative model of the object oriented systems development methodology was adopted for the system design. This is to enable periodic refinement of the system in line with the dynamic nature of web resources and the amorphous nature of cyber crime. The object oriented measure was used to represent the logical data and process design using Unified Modeling Language (UML) represented as a use case. The use case diagram of the system is illustrated in Figure 4.

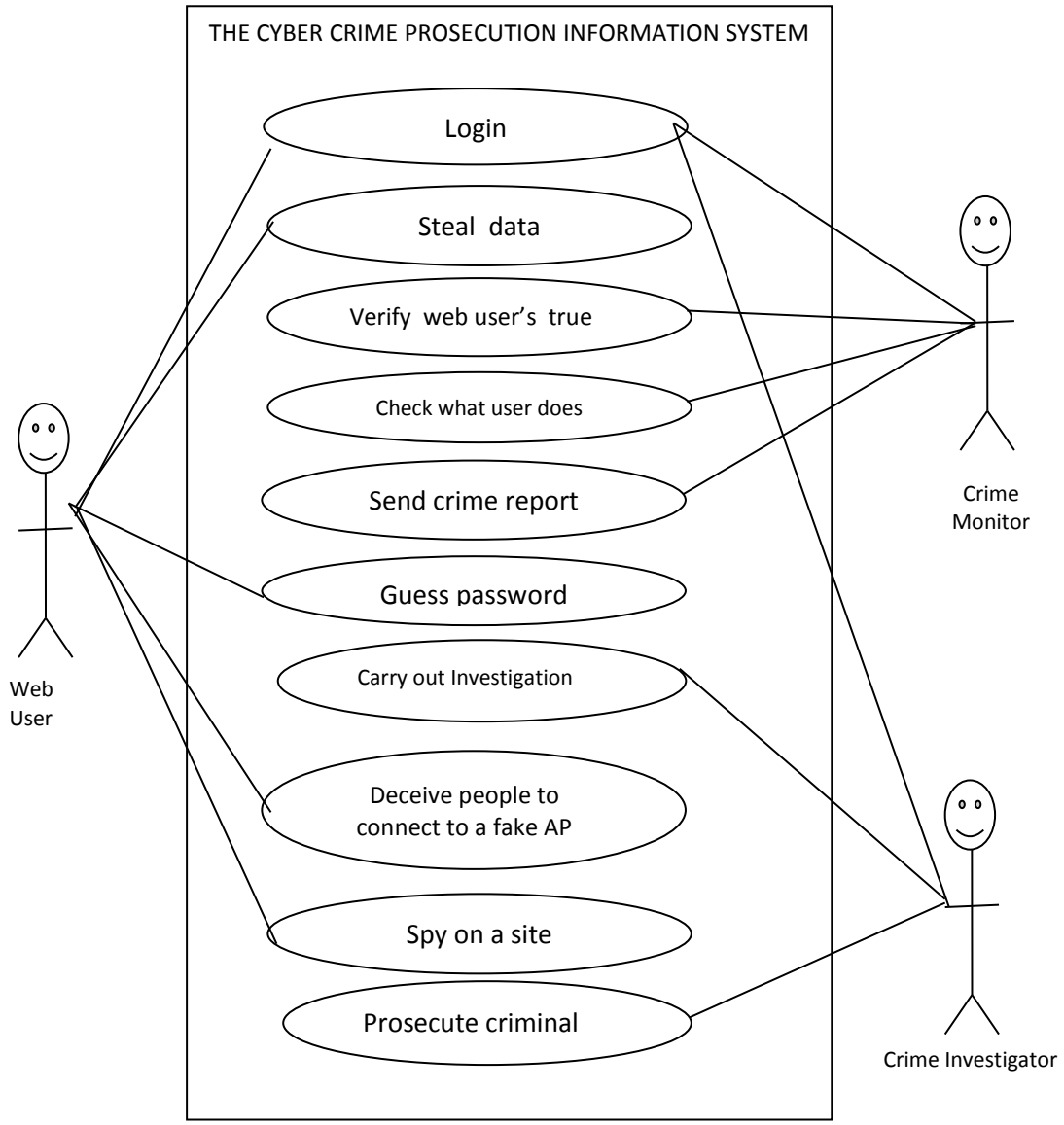

Figure 4. Use Case Model of the Enhanced, Evidence-Based Cyber Crime Prosecution Information System

Three actors are involved in the use case model illustrated in figure 7 (the web user, the crime monitor and the crime investigator). The web user commits crime, the crime monitor is the program module that monitors the user's activities and reports appropriately, while the crime investigator investigates the activities of a suspected criminal for appropriate prosecution.

To actualize this model, a real time cyber security website www.ganamos.org was designed. The website is hosted in the cloud and access is granted only if the biometric features (facial image and fingerprint) of the user are captured as mandatory login parameters in addition to the user's password. The motivational drive for the design is that every cyber user must create some impressions which are verifiable to identify him. The system records the user's geographical location (longitude and latitude), activities, date and time stamp, and tracks the Internet Protocol (IP) address and media access control (MAC) address of the system used. The system utilizes existing intrusion detection systems and cookies to keep track of a user's activities. The hardware on which the system runs must have an embedded webcam/an attached digital camera and a finger print scanner to capture the user's biometric features. An additional authentication of the username and password is required before access can be granted to the web resources. If a user indulges in any crime while in session, the system records the user's details captured plus the crime committed in a database which can be accessed by cyber crime investigators for determination and prosecution.

Four crime scenarios were used in testing the system:

Identity theft: This crime is recorded against any user who fails authentication test because he tries to log in with someone else's username and password after the mandatory facial image and finger print capturing.

Espionage: A user who stays for too long on the site without providing his login details or stays for too long without any activity after successfully logging in is accused of spying on the site (espionage).

Phishing: Use of a morally obscene word like 'sex' and terms requesting someone to pay gamble with money are considered phishing scam in the site.

Data theft: This crime is reported if a user who has successfully logged in tries to access the data of another user which is not associated with him.

6.1 Process Algorithm and Flowchart

The logic of the system are described in the process algorithm and flowchart that follow:
Crime Detection Algorithm

i. Login (capture facial image, fingerprint, username and password)
ii. Record the user's geolocation (in longitude and latitude) IP address and MAC address
iii. Report crime and Go to vi IF login is invalid
iv. Record the actions performed by the user
v. If actions are unlawful, record and report crime
vi. Prosecute crime
vii. Exit

Figure 5 illustrates the flowchart diagram of the system.

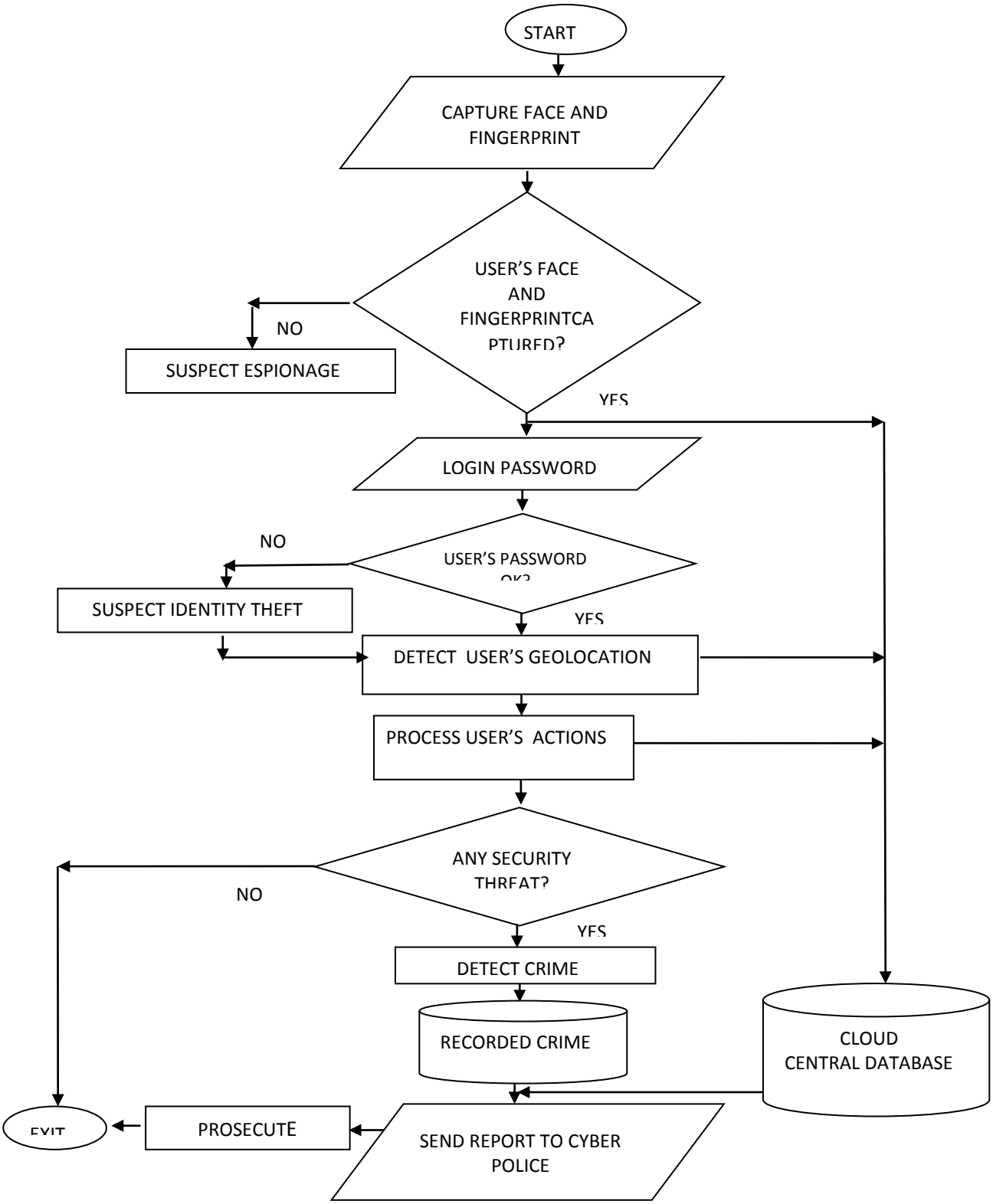

Figure 5. System Flowchart of the Enhanced Cyber Crime Prosecution Information System

Figure 6 illustrates the high level model of the system

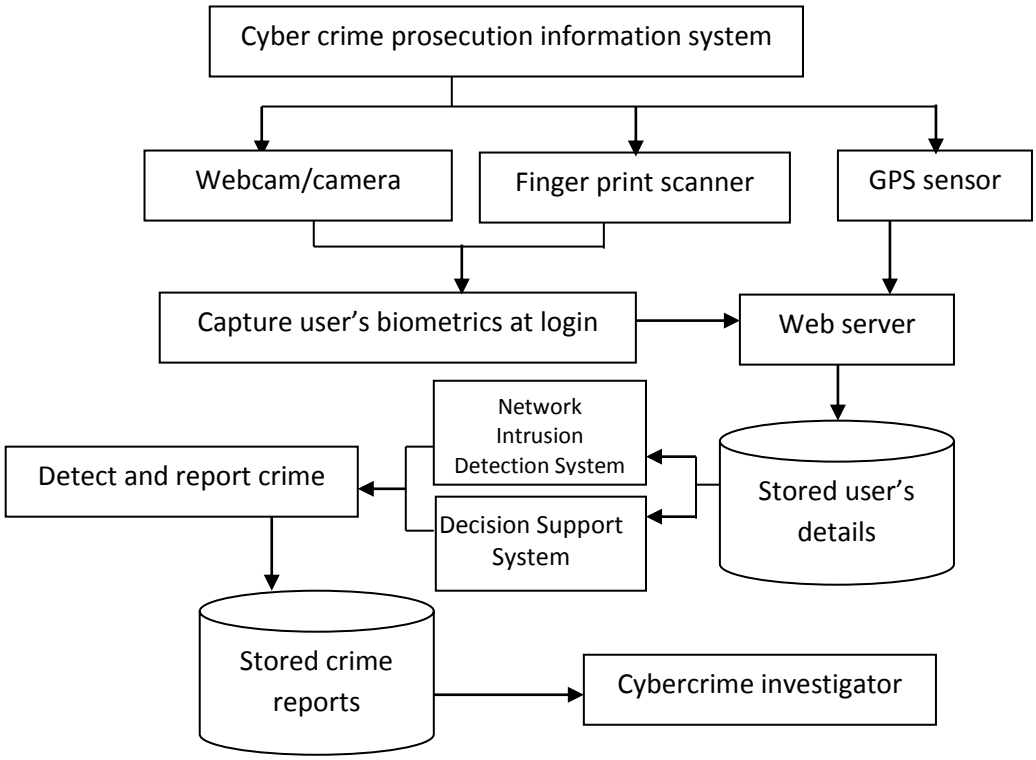

Figure 6: High Level Model of the Enhance Cyber Crime Prosecution Information System

7. System Testing

There are several network data security measures in place but criminals have always devised An The design represents a model of a portal as found in tertiary institutions of learning where students pay fees, register their courses and even check their results online while the portal administrator manages the site. The user access control measures include user name, password, school fees permit, personal identification number (PIN) and matriculation number in addition to the facial image and finger print captured before access is granted. In this circumstance, users can guess passwords, matriculation numbers, steal fee payment PINs, etc. of others and gain access to register their own courses. If a user attempts to check his neighbour's results, guess password, stay too long on a page attempting to log in, post some obscene words or uses some financial scam terms programmed into the system, and so on, he is reported to be a criminal.
Every unit of the software was tested to ascertain its functionality in accordance with the objectives of the system, errors were debugged, and the final working system was then integrated.

7.1 Test data

Some of the data that were used for the system testing are as follows:
i. **Login**
STAFF LOGIN
USER NAME: moses
PASSWORD: agana
STUDENTS LOGIN
USER NAME: 2009 (default)
PASSWORD: student (default)
ii. **Fees Payment**
For a student to qualify to pay fees, he must have been registered. Fee payment pin and serial number is generated for the user to proceed to pay fees. Some pins and serial numbers tested were:
Pin: 35434534534534443
Serial no: 456356363636
Pin: 39457529485294826
iii. **Phishing Words**
The words that were used to test for phishing in the advert web page are "Pay, $, Profit and Earn"
iv. **Result Permits**
Only duly registered students with matriculation numbers in the portal are eligible to check their results. They must be given result permits to enable them access their results. The following matriculation numbers and result permits were used to test the system:

Matric no: 2009	-	Permit no: 20005
Matric no: 2010	-	Permit no: 25605
Matric no: 2011	-	Permit no: 26601

Data theft was tested by using someone else's pin, serial number or result permit by a user who has successfully logged in. The test results conformed with the expected results.

8. Results

There are several network data security measures in place but criminals The results of the research design are discussed in this section. Figure 7 illustrates the mandatory facial image capturing. Once the user types the uniform resources locator (URL) www.ganamos.com at the address bar, the home page appears from where the user is prompted to take a snapshot before proceeding.

Figure 7: Mandatory Image Capturing

After taking the snapshot, the user's finger print must be captured as a second mandatory requirement as illustrated in figure 8.

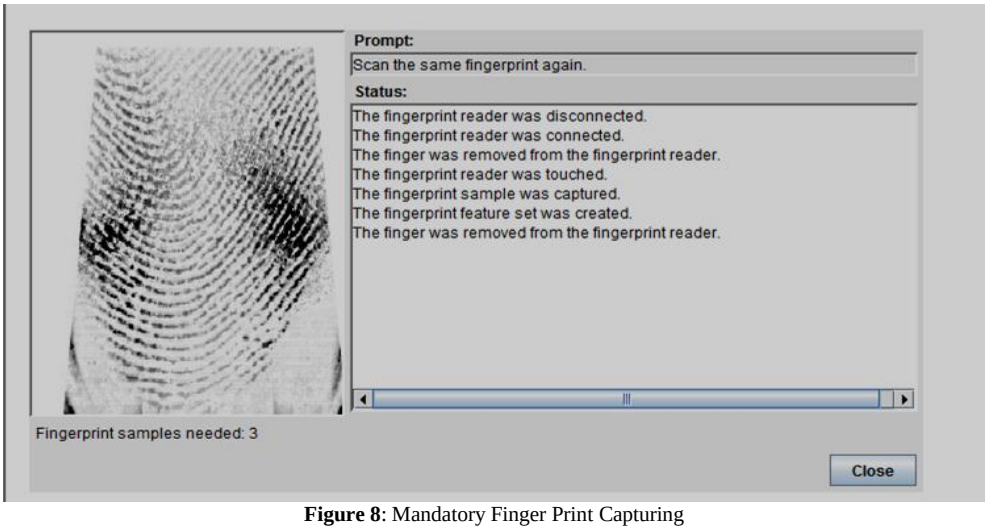

Figure 8: Mandatory Finger Print Capturing

A third mandatory access requirement after capturing the user's fingerprint is the username and password. This is used to detect identity theft and session hijacking. Figure 9 illustrates this session. This is the third tier of authentication before a user is granted access.

Figure 9: Username and Password Login session.

All the activities of the user are continuously tracked and recorded in the web database right from the initial login session of facial image capturing. A user who stays idle in a particular session after a given duration is suspected of spying on the site (espionage). All crime reports are documented in the web database as illustrated in Table 1. The database keeps track of the username, date and time stamp, IP MAC addresses of the system used, crime type, facial image and finger print URL.

Table 1: Crime Reports

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 Finger Image
2.	20160611307472334	2016-06-12 03:56:42 am	181.140.249.61	00-FH-0F-YL-WU-03	Longitude: -75.5636 Latitude: 6.2518	ESPIONAGE	View Facial Image	View Finger Image
3.	20160922458531772	2016-09-22 03:03:54 pm			Longitude: Latitude:	DATA THEFT	View Facial Image	View Finger Image
4.	20170329283577837	2017-03-30 02:02:24 am	197.210.24.222	00-17-0A-RV-KC-37	Longitude: 3.3958 Latitude: 6.4531	IDENTITY THEFT	View Facial Image	View Finger Image
5.	20170530496804518	2017-05-30 03:54:23 pm	154.66.35.50	00-ZB-X8-6V-LT-49	Longitude: 3.8964 Latitude: 7.3878	ESPIONAGE	View Facial Image	View Finger Image
6.	20170801038322993	2017-08-01 12:09:14 pm	197.210.227.74	00-RU-XS-1C-7N-45	Longitude: 3.3958 Latitude: 6.4531	IDENTITY THEFT	View Facial Image	View Finger Image
7.	20171219158717118	2017-12-20 12:25:18 am	146.182.18.96	00-FS-5U-0Q-VM-85	Longitude: 26.214 Latitude: -29.1211	PHISHING	View Facial Image	View Finger Image

The crime report form (Table 1) shows details of system-generated username codes, serial number assigned to each user, date/time when the user accessed the Internet, the IP address as at the time of access, the MAC address of the device used, geographical location at as the time of access represented in longitude and latitude, the type of crime committed while online, facial image URL and fingerprint URL. The facial image and finger image URLs are hyperlinks to the web pages where the cyber user's facial image and the finger print captured as mandatory access requirements are stored. Only the cyber crime investigators have the access authorization and authentication to these web pages where they can retrieve the data as evidences for crime prosecution. The facial image and finger print of each user are associated with his activities while on line and are used to verify if he committed a crime or not at such time.

9. Conclusion

There are several network data security measures in place but criminals The results obtained so far show that the system can uniquely identify any user who visits the website www.ganamos.org (using a 3-tier authentication: facial image, finger print and password), store the details of transactions, detect criminal acts indulged in by a user and store such details in a database which cyber crime investigators can retrieve for prosecution and actions. It is recommended that as a security standard, all websites should adopt the design to stem the menace of cyber crime. Cyber crime investigators should be trained on how to obtain evidences from crime monitoring systems to aid them in prosecution and those found guilty should be punished to serve as a deterrent to others. In addition, web developers and other information system designers should through continuous re-engineering of defensive policing and detection strategies incorporate into their designs technological solutions to the prevalent cyber insecurity. Specifically, all devices (including mobile phones) that have Internet access should have resources to unique identify, monitor and report any crime committed by any Internet user. Researchers are also encouraged to extend the research to cover the detection and control of all forms of cyber crimes in the future.

Acknowledgements

The authors are grateful to all, especially those whose materials were used as references for this paper.

References

[1]Hutchinson, S.E. & Sawyer, S.C. (2000). Computers, Communication and Information: A User's Introduction. New York: DP Publications.

[2] Decker, F. (2015). Business Risks of Insecure Networks. Hearst Newspapers, LLC. Accessed online from http://smallbusiness.chron.com/business-risks-insecure-networks-41202.html on 20-12-2017

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

[4] Obama, B. (2014). Presidential Proclamation – National Cybersecurity Awareness Month, 2014. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2014/09/30/presidential-proclamation-national-cybersecurity-awareness-month-2014 on 23-12-2017.

[5] Williams, T.D. (2016, 27 September). Top 3 Cloud Security Risks & What to Do?. Retrieved from https://www.linkedin.com/pulse/top-3-cloud-security-risks-what-do-tim-d-williams on 04/01/2018.

[6] Evan, P. and Shimon, P. (2015). How the U.S. thinks Russians hacked the White House.CNN News, April 8. Retrieved from

http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html on 09-11-2016.

[7] Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S. (2014). Organizations and Cyber Crime: AnAnalysis of the Nature of Groups engaged in Cyber Crime. International Journal of Cyber Criminology, 8(1), 1-20.

[8] Clay, W. (2005). Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues forCongress. Congressional Research Service Report for Congress. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a444799.pdf on 27-12-2017.

[9] Graham, J., Howard, R., and Olson, R. (Eds.) (2011). *Cyber Security Essentials*. Boca Raton: Taylor and Francis Group.

[10] Morris, S. (2004). The future of netcrime now: Part 1 – threats and challenges. Home Office Online Report 62/04. Retrieved from http://globalinitiative.net/wp-content/uploads/2017/01/the-future-of-netcrime-now-part-1- threats-and-challenges.pdf on 02/01/2018.

[11] McQuade, S. (2005). Technology-enabled Crime, Policing and Security. *The Journal of Technology Studies, 32(1), 32-42, ISSN 1071-6084*. Retrieved from http://scholar.lib.vt.edu/ejournals/JOTS/v32/v32n1/pdf/mcquade.pdf on 10-12-2017.

[12] Cohen L. E., and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44: 588-608

[13] Longe,O. B., Wada, F. and Danquah, P., (2012). Action Speaks Louder Than Words – Understanding Cyber Criminal Behavior using Criminological Theories. *Journal of Internet Banking and Commerce 17(1), 1-12.*

[14] Roger, A.G. (2016). Why it's so hard to prosecute Cyber Criminals. A CSO column available at https://www.csoonline.com/article/3147398, retrieved on 20/12/2017.

[15] Patel, A. Taghavi, M., Bakhtiyari, K. and Celestino J. J. (2013). An Intrusion Detection and Prevention System in Cloud Computing: A systematic Review, Journal of Network and Computer Applications, Elsevier, 36, 25–41.

[16] Baniak, K. (2007). Intelligent Agents in Support of Internet Security. *Annales UMC Informatica* AI (7), 117-125. Available online at https://journals.umcs.pl/ai/article/view/3190/2386 Accessed on 10-11-2017. DOI: 10.17951/ai.2007.7.1.117-125

[17] Pikoulas, J., Buchanan, W., Mannion, M. and Triantafyllopoulos, K. (2002). An Intelligent Agent Security Intrusion System. Available online at http://www.soc.napier.ac.uk/~bill/pdf/ecbs2002_agents_revised.pdf . Accessed on 11-12-2017.

[18] Miller, J. (2009). "Cell Phone Tracking Can Locate Terrorists - But Only Where It's Legal". *FOX News*. http://www.foxnews.com/story/0,2933,509211,00.html. Retrieved on 14-09-2017.

[19] O'Harrow, R. (2003). "U.S. Backs Florida's New Counterterrorism Database". *Washington Post*, Aug. 6, p. A01.

[20] Low, C. (2005). Understanding Wireless Attacks and Detection. © SANS Institute InfoSec Reading Room. Retrieved from https://www.sans.org/reading room/whitepapers/detection/understanding-wireless-attacks-detection-1633 on 10-06-2017.