Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 11, November 2017, pg.94 – 113

CYBER SPACE TECHNOLOGY: CYBER CRIME, CYBER SECURITY AND MODELS OF CYBER SOLUTION, A CASE STUDY OF NIGERIA

DAMBO ITARI, EZIMORA OKEZIE ANTHONY, NWANYANWU MERCY

DEPARTMENT OF FOUNDATION STUDIES, COLLEGE OF HEALTH TECHNOLOGY OTUOGIDI BAYELSA STATE, NIGERIA, anidam43@gmail.com

DEPARTMENT OF COMPUTER SCIENCE, CONVENANT POLYTECHNIC ABA, NIGERIA, okezieanthony3@gmail.com

DEPARTMENT OF COMPUTER SCIENCE, PORTHARCOURT POLYTECHNIC RUMUOLA, NIGERIA, nnamsnd@gmail.com

ABSTRACT: Cyber space is a domain characterized by the use of electronics and electromagnetic spectrum to store, modify, and exchanged data via networked systems and associated physical infrastructures. Cyber space is a boundless space known as the internet. It can be seen as the space in which computer transactions occur, particularly transactions between different computers. Images and text on the Internet exist in cyberspace. The term is used in conjunction with virtual reality, designating the imaginary place where virtual objects exist. If a computer produces a picture of a building that allows the architect to "walk" through and see what a design would look like, the building is said to exist in cyberspace.

Cyber crime is a series of organized crime attacking cyberspace and cyber security. Cyber crime such as; hacking into Computers. It can be through a network system and clicking into unfamiliar links connecting to unfamiliar Wi-Fi, downloading software and files from unsafe sites, power consumption, electromagnetic radiation waves, and many more.

However, Cyber security is a critical issue and should be taken seriously because it has risen to become a national concern. Currently, most electronic devices such as Computers, laptops and cell-phones come with built-in firewall security software, but despite this, Computers are not 100 percent accurate and dependable to protect our data.

Computers can be protected through well built software and hardware. By having strong internal interactions of properties, software complexity can prevent software crash and security failure.

Keywords: Cyber space, Cyber crime, Cyber security, Technology, Nigeria.

1.0 INTRODUCTION

In today's world cyber systems provide flexibility leading to its illicit use with the government framed internet policy, Internet along with making life easy with economy activities like buying, selling, online transactions and social networking brings along many threats. The internet has simplified business processes such as sorting, summarizing, coding, editing. Cyberspace refers to a 'global and dynamic domain' (subject to constant change) characterized by the combined use of electronics and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate, inform and disrupt physical resources.

The Cyberspace can also be seen as a 'notional environment in which communication over computer networks occurs'. The word became popular in the 1990s when the uses of the Internet, networking and digital communication were all growing drastically and the term was able to represent the many new ideas and phenomena that is emerging.

However, it is through the same cyber networks which intrude and attack our privacy, economic, social life in a way which is harmful. It has also brought unintended consequences such as criminal activities, spamming, credit card frauds, phishing, and ATM fraud. Some scholars have interestingly argued that "In the internet nobody knows you are a dog". This raises some legal issues and concerns. IT revolution has brought about a wide array of aides and conveniences that have indelibly influenced modern communication travel, security and commerce. The massive gains brought by the information age are not perfect, with the pervasive correlation of human activity with electronic resources and infrastructure there is a crucial vulnerability, which is the ever present risk of abuse, insidious manipulation and sabotage of computer and computer networks. It has been established that Nigeria is an impressionable country. The advent of the internet to her was both welcome and full of disadvantages. The exceptional outbreak of cyber crime in Nigeria in recent times was quite alarming, and the negative impact on the socio economy of the country is highly disturbing. Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has caused unease about the state of cyber and personal security. This trend has increased recently and has called for quick response in providing laws that would protect the cyber space and its users.

The first recorded cyber murder was committed in the United States seven years ago. According to the Indian Express, January 2002, an underworld don in a hospital was to undergo a minor surgery. His rival went ahead to hire a computer expert who altered his prescriptions through hacking the hospital's computer system. He was administered the altered prescription by an innocent nurse, this resulted in the death of the patient. Statistically, all over the world, there has been a form of cyber-crime committed every day since 2006. Prior to the year 2001, the trend of cyber-crime was not globally associated with Nigeria. This resonates with the fact that in Nigeria we came into realization of the full potential of the internet right about that time. Since then, however, the country has acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the Internet. Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals are no longer suitable for to deal with their new tricks.

Since the issue of cyber security is raising a number of questions in the minds of Nigerians, it is only fair that we answer these questions. This paper seeks to give an overview of cyber space, cybercrime and cyber-security, importance of cyber security, types of cyber crime, outline the causes and effect in Nigeria, ways of combating cyber crime and give models of cyber solution.

2.0 OVERVIEW OF CYBER SPACE, CYBER CRIME AND CYBERSECURITY

As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale that could cause harm or disrupt services upon which our economy and daily lives of millions of Nigerians depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyber space as become security mission. Cyber space refers to the boundless space known as the internet. It refers to the interdependent network of information technology components that underpin many of our communications technologies in place today. Cyber space is an electronic medium used to form a global computer network to facilitate online communication. It is a large computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities. Crimes are now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual Property violations, and other crimes, all of which are substantial human and economic consequences. Nigeria’s economic vitality and national security depend on a vast array of interdependent and critical networks, systems, services, and resources known as cyberspace. Cyber-space has transformed the ways we communicate, travel, power our homes, run our economy, and obtains government services.

Cyber crime refers to the series of organized crime attacking both cyber space and cyber security. Cyber crime refers to criminal activity done using computers and the Internet. It also involves illegal access (unauthorized access, transmissions of computer data, to, from or within a computer system .This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the internet to steal personal information from other users.

Cyber-security is the body of technology, processes and practices designed to protect networks, computers, programs and data from attacks, damage, or authorized access. In the computing or cyber context, the word security simply implies Cyber-security. Ensuring cyber-security requires coordinated efforts from both the citizens of the Nigeria and their information system. The threat posed by breaches in our cyber-security is advancing faster than we can keep up with it. It is not possible to concentrate efforts on only one aspect of the breach as it means negligence and allowance of growth for other aspects of the breach. This leads us to conclude that we have to attack cyber security breaches as a whole. Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. Cyber-security is the body of rules put in place for the protection of the cyber space. But as we become more dependent on cyberspace, we undoubtedly face new risk. Sophisticated cyber criminals and nation-states, among others, present risks to our economy and national security. Cyber-security is the body of technology, processes and practices designed to protect networks, computers, programs and data from attacks, damage, or authorized access.

2.1 IMPORTANCE OF CYBER SECURITY

The following are the importance of cyber security:

- To work collaboratively with public, private and international entities to secure cyber space.
- To help individuals and institutions develop and nurture a culture of cyber security.
- Integrity, which may include authenticity.
- Confidentiality.
- To help understand the current trends in IT/ cybercrime and develop effective solutions.
- To help people reduce the vulnerability of their information and communication Technology (ICT) systems and networks.

2.2 TYPES OF CYBER CRIMES

There are various cyber crimes, but this paper will examine the cyber crimes that are dominating Nigeria based on current trends;

- **CEO Email Scam:** It is a phishing scheme that targets businesses by spoofing their email or use social engineering to assume the identity of their CEO .The cyber criminals achieve this by researching employees who are in charge of finance and request a wire fraud transfer to fraudulent account claiming to be CEO.

- **Cyber Terrorism:** Cyber Terrorism involves the use of internet to commit terrorism or launch terrorist attacks. This is a new way or means which insurgents or religious extremists (eg Boko Haram) use to recruit new members and form strategies on how to attack nations.

- **Ransomware:** With the rise of ransom ware as- service, cyber criminals can now purchase a user friendly kit they could deploy with little or no cyber expertise from the dark web. A Ransom ware is a type of malware that infects a machine when user clicks on a seemingly legitimate link and unknowing downloads a malicious file. The virus will then encrypt the user's files, share devices and servers. Leaving them inaccessible unless the victim pays for the decryption key usually in crypto currency.

- **Online Assisted Kidnapping:** That kidnapping is on the rise in Nigeria is no news, what many people don't know is that kidnappers are being assisted by their victims' social media activities and geolocation data on their smart phones. Geolocation data is information that can be used to identify an electronic device physical location using smart phones built in global positioning system (GPS) functionality allows location- based services (or geo-location) to locate and publish information about owners whereabouts. Kidnappers have started using geolocation and geotagging to target their victims.

Geotagging are pieces of information that can be attached to a tweet, status or photo on a social networking site that show the physical location of where something had been posted. Social media that have location geotagging implemented include; Twitter, Face book, Instagram, amongst many others.

- **On line Impersonation :**The can be classified into two categories base on their activities in Nigeria .The first category impersonates politicians and religious leaders on social media by creating profiles with the aim of defrauding their victims . The second category usually creates fake profiles with attractive fake pictures so they can engage in what is called “romance scam” .The romance fraud criminals are mainly interested in targeting foreigners, claiming they are in love with them and establishing a love relation to be able to swindle them.

- **Fraud- Identity Theft**: It is a criminal activity in which someone pretends to be somebody and retrieve vital information to someone. For instance, making a false bank webpage to retrieve information of account of someone. The concept is simple; someone gains access to your personal information and uses it for it for his own benefit .In Nigeria people design web links forms requesting users to fill in their basic information including ,unique details like pin numbers and use that to commit crime.

- **Internet Pornography**: The use of the web for sexual abuse remains a very active research interest. It has been found that internet pornography is a disturbing trend especially among the youths. The use of web filtering programme has been advocated to check internet pornography in Nigeria. It also involves using internet to download and transmit pornography pictures, photos, writings etc. Internet is used as an avenue for luring unsuspecting children to pedophiles, and for distributing child pornography. Another trend is the use of mobile phones and internet for prostitution. Hence, prostitutes now advertise their trade via internet by exposing their sensitive, sensual and private parts to the internet users.

- **Cyber Plagiarism**: This is the act of stealing people's ideas through public domains. This is common in educational institutions as students and lecturers use it to steal other people's idea to publish them as their own original work.

- **Hacking:** Hackers make use of the weaknesses and loop holes in operating systems to destroy data and steal important information from victim's computer. It is normally done through the use of a backdoor program installed on your machine. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what u do on your computer and can also import files on your computer. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of the company.

3.0 CAUSES AND EFFECT OF CYBER CRIME IN NIGERIA

Cyber crime is increasing astronomically and some of the causes (reasons) for the vast increase of internet fraud in Nigeria are;

a. **Poverty:** Most Nigerians lack means of subsistence and they barely have a place to lay, food to eat, clothes to wear, etc and this makes individuals engage in cyber crimes as listed above for sustenance. This is because life seems to be survival of the fittest and the poor sees the internet fraud as a means of making life meaningful to them.

b. **Greed:** Most people actually involve in cyber crimes not because they don't have what it takes to live a normal life but because they are never contempted with what they have and the desire to have quick and more wealth without having to go through the right process.

c. **Lack of Confidence:** It is one of the reasons people engage into cyber crimes. Some people believe they can no longer make it in life, they feel disappointed and they think the only way to make up their mistakes and to move forward is by making quick wealth, In this case they fall back to internet fraud.

d. **Unemployment:** This is one of the major reasons people get involved in cyber crimes. After all educational qualifications one seems to have obtained in Nigeria, jobs are still not available for them and this lead to frustration and for them to live an average life, they see internet fraud has a means of survival. Even the employed are not paid for months, sometimes years and this can also lead to individuals engaging in Cyber crimes.

3.1 EFFECT OF CYBER CRIME

a. Reduces the Competitive Edge of Organizations

Computer crimes over the years have cost a lot of havoc to individuals, private and public business organization in Nigeria, causing a lot of financial and physical damage. Due to cyber crime, there has being loss of billions, such crimes may threaten a nation’s security and financial health.Cyber crimes has great effects in Nigeria economy, for example the recent ponzi scheme such as MMM, Ultimate Cycler etc in which most Nigerians engaged into. It has been recorded that Nigerians lost eight million to MMM which is a great loss to Nigerian economy.

b. Time Wastage and Slows Financial Growth

Wastage of time is another problem because many IT personals may spend a lot of time on handling, rectifying harmful incidents which may be caused by computer criminals. The time spent should have earned a profit to the organization. One peculiar problem is that, when a hacker enter in an organization and steals confidential information from the company the people who entrust the company loses their confidence in the company as the company may contains confidential information like credit cards of customers and as the information is stolen the customer will not trust the company again and will move to someone else who could protect their confidential information.

c. Slows Production Time and Add to Over Head Cost

Computer crime reduces the productivity of a company, as a company will take measure to reduce cybercrime, by entering more password or other acts this will take time to do and therefore will affect productivity. Computer crime will increase the cost as to stop viruses and malware companies must buy strong security software to reduce the chances of attacks from such attacks.

d. Defamation Of Image

With high level of cyber crime in the nation, the slogan “GOOD PEOPLE GREAT NATION “by Nigerians will be tarnished and global community will view the other side of the coin thereby increases Nigerian world crime record. When individuals involved are caught, it tarnishes the image of the family of the individual
Other effects includes the consumption of computer and network, can also cost an individual involved his education and career when caught and it deprives him of becoming who he wants to be in life.

3.2 COMBATING CYBER CRIME

The specifications below are very essential in combating cyber crime:

1. **Use of legislation:** This is a very important step towards combating cyber crime. The government both state, local and federal should have a very effective legislation that stipulates the proper punishment for these cyber criminals. The problem is that most countries’ laws are weak and thus allow these cyber criminals to strike from international boarders and remain undetected. Even when identified these criminals avoid being punished or extradited to a country, such as the US, that has developed laws that law for prosecution. While this proves different in some cases, agencies such as the FBI, have used deception and subterfuge to catch criminals. Example: Two Russian hackers have been evading the FBI for some time. The FBI set up a fake computing computer-based in Seattle, Washington. They proceeded to lure the two Russians in the US by offering them work in this company. Upon completion of the interview, the suspects were arrested outside the

building. Clever tricks like this are sometimes a necessary part of catching cyber criminals when weak legislation make it impossible otherwise.

2. **Creation of awareness:**
   As technology advances and more people rely on the Internet to store sensitive information such as banking or credit card information, criminals are going to attempt to steel that information. Cyber crime is becoming more of a threat to people across the world. There must be a rising awareness about how information is being protected and the tactics criminals use to steal information. The government both local, state, and federal must as matter of urgency make sure that the people are made to know the activities of these hoodlums and how to protect their files, systems, networks etc from unauthorised access. Also, the NGOs (Non-governmental organisations) and anti-crime agencies have to make sure that, this ugly trend is reduced to the barest minimum if not eradicated completely.
3. **Use of cryptography:** This is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit.

However, in today’s computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

i. Confidentiality: The information cannot be understood by anyone for whom it was unintended.

ii. Integrity: The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

iii. Non-repudiation: The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

iv. Authentication: The sender and receiver can confirm each other's identity and the origin/destination of the information.

3.3 HOW ENCYPTION WORKS

Encryption is an interesting piece of technology that works by scrambling data so it is unreadable by unintended parties. Let's take a look at how it works with the email-friendly software PGP (or GPG for you open source people).

Say I want to send you a private message, so I encrypt it using either one of these programs. Here's the message:

wUwDPglyJu9LOnkBAf4vxSpQgQZltcz7LWwEquhdm5kSQIkQlZtfxtSTsma
q6gVH8SimlC3W6TDOhhL2FdgvdIC7sDv7G1Z7pCNzFLp0lgB9ACm8r5RZ
N5ske9cBVjlVfgmQ9VpFzSwzLLODhCU7/2THg2iDrW3NGQZfz3SSWviwC
mNIvp5jEkGPCGcla4Fgdp/xuyewPk6NDlBewftLtHJVfPAb3

Once encrypted, the message literally becomes a jumbled mess of random characters. But, equipped with the secret pass code I text you, you can decrypt it and find the original message.

Come on over for hot dogs and soda!

Whether it's in transit like our hot dog party email or resting on your hard drive, encryption works to keep prying eyes out of your business – even if they happen to somehow gain access to your network or system. If you want to learn more about how encryption helps protect business data, you can read our article on how encryption aids cloud security.

The technology comes in many forms, with key size and strength generally being the biggest differences in one variety from the next.

CRYPTOGRAPHY ALGORITHMS

1. Triple DES

Triple DES was designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry.

Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits in key strength is more like it.

Despite slowly being phased out, Triple DES still manages to make a dependable hardware encryption solution for financial services and other industries.

2. RSA

RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in our PGP and GPG programs.

Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You've got your public key, which is what we use to encrypt our message, and a private key to decrypt it. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers quite a bit of time and processing power to break.

3. Blowfish

Blowfish is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually.

Blowfish is known for both its tremendous speed and overall effectiveness as many claim that it has never been defeated. Meanwhile, vendors have taken full advantage of its free availability in the public domain.

Blowfish can be found in software categories ranging from e-commerce platforms for securing payments to password management tools, where it used to protect passwords. It's definitely one of the more flexible encryption methods available.

4. Twofish

Computer security expert Bruce Schneier is the mastermind behind Blowfish and its successor Twofish. Keys used in this algorithm may be up to 256 bits in length and as a symmetric technique, only one key is needed.

Twofish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments. Like Blowfish, Twofish is freely available to anyone who wants to use it. As a result, you'll find it bundled in encryption programs such as Photo Encrypt, GPG, and the popular open source software True Crypt.

5. AES

The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations.
Although it is extremely efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy duty encryption purposes.
AES is largely considered impervious to all attacks, with the exception of brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher. Still, security experts believe that AES will eventually be hailed the de facto standard for encrypting data in the private sector.

4.0 MODELS OF CYBER SOLUTION

Legislature should make laws, providing penalties for any fellow involved in any form of cybercrime in Nigeria. This will create fear in the general public because of the punishment involved. I also posit that there should be more agencies in charge of cyber crime e.g. The Nigeria cyber crime working group, which was created by Olusegun Obasanjo in order to reduce the rate of cyber crimes, should be empowered.
Economic and Financial Crimes Commission (Establishment) ACT 2004. Nigerian Criminal Code can also be used to deal with cyber crime.

Since poverty is one of the major causes of internet fraud in Nigeria, government should organize poverty alleviation programmes in order to reduce the rate of poverty in Nigeria .Also, free education should be provided by the government to enable those who can’t afford the fees paid in private schools.

Cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence We need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.

Firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall typically guards an internal computer network against malicious access from outside the network.

More so, Agencies in charge of cyber crimes should be equipped and should have good knowledge of the internet for them to know where the problem is coming from and how to deal with them.

Finally, Youths should be empowered with different skills such as tailoring, hairdressing, shoe making etc in order to be economically independent and this will reduce the rate at which cyber crimes grows. Since the level of unemployment in the country has contributed significantly to the spate of e-crime in Nigeria, the government should create employments for these youths and set up IT laboratories/forum where these youths could come together and display their skills. This can be used meaningfully towards developing IT in Nigeria at the same time they could be rewarded handsomely for such novelty.

CONCLUSION

Information and communication Technology (ICT) systems are now as basic to our lives as water and electricity. Many individuals, corporate organizations and Government agencies depend on ICT and computer networks to perform simple as well as complex tasks. However, the cyber space is increasing becoming vulnerable as many businesses, agencies and individuals are being swindled by cyber criminals in the country.

There is an upsurge of cyber crime in Nigeria. The country is ranked third in global internet crime after the United States of America and United Kingdom while 7.5 percent of the world's hackers are said to be Nigerians. Committed mostly by the young, often called "yahoo" boys, the fraudsters are increasingly taking advantage of the rise in online transactions, electronic shopping and e-commerce to engage in heinous crime. Therefore cyber security must be addressed seriously as it is affecting the image of the country in the outside world.

RECOMMENDATIONS

i. Government should make provision for intensive training of law enforcement agencies on ICT so that they can track down the cyber criminals, no matter how intelligent and cunning they may be.

ii. Financial institutions in Nigeria should establish fraud detection departments.

iii. There should be a centralized electronic data bank containing specific Information on each individual resident and visitor to Nigeria.

iv. Education is a vital weapon for literacy, as such seminars and workshops organized from time to time with emphasis on cyber safety so that individual will learn to keep their personal information safe and youth will flee cyber crime.

v. The internet service providers should provide their customers, especially financial institution and cyber cafe with well guided security codes to protect their information and software from hackers.

REFERENCES

[1]. Anah B.H; "Cyber crime in Nigeria" Causes, Effects and Wayout", 2002 ARPN Journal of Science and Technology No 7, P.626.

[2]. "Announcing the ADVANCED ENCRYPTION STANDARD (AES)" (PDF). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST).November 26, 2001.Retrieved October 2,2012.

[3]. "Cryptography: Description of a new variable – Lengthy key, 64-Bit Block Cipher (Blow fish) – Schneir on Security ". www.schneier.com Retrieved 2015-12-31.

[4]. Esharenana E,& Igun "Combating cyber crime in Nigeria" Electronic library, Vol26, Delta, Emerald Group publishing Ltd, 2008, P.717.

[5]. Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations.Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

[6]. Lynn Hathaway (June 2003). "National Policy on the use of the Advanced Encryption Standard (AES) to protect National Security Systems and National Security Information" (PDF). Retrieved 2011- 02-15.

[7]. Mohsin, A (2006) ; Cyber crimes and solutions ,retrieved from http://ezinearticles.com

[8]. Moore, R. (2005) "Cyber crime: Investigating High-Technology Crime," Cleveland, Mississippi: Anderson Publishing.

[9]. "New Comparative Study between Des, 3 DES and AES within Nine Factors". Journal of Computing. 2(3). March. ISSN 2151-9617. Retrived 2017-09-05.

[10]. Olumide, O.O. Victor, F.B (2010); E- Crime in Nigeria; Trends, tricks and Treatment. The Pacific Journal of Science and Technology volume//.Number1 May 2010 (Spring).