An Exploratory Survey of Emerging Cybercrime Attacks and Counter-Detection Approaches

Oyeleye Christopher, Fagbola Temitayo, Akinpelu James, Oloyede Ayodele, Egbetola Funmilola and Olayan Olatayo

Abstract – Cybercrime is the illegal activities committed through the use of computers and the internet. The evolution of the internet and its diversity in the world are the sources of cybercrimes. Now that information can be utilized for educational, commercial, personal usefulness. Therefore a robust and ideal methodology need to produce for tracing and detecting terror based activities over the internet. Several approaches have been proposed and developed for the detection and prevention of cybercrimes over the years. This paper provides an up-to-date review of models, parameters, architecture and frameworks used in detecting and preventing cybercrimes.

Keywords – Cybercrime, Attack, Detection, Distributed-Denial-of-Service.

I. INTRODUCTION

The internet is a global data communication system. Over the last two decades, the Internet community has grown from a curiosity fact or thinking to an essential element of modern life for most users. Considering the aspect of globalization, its rapid expansion has grown beyond regulatory limit, and this absence of authority has creates space for many abuses. The problem is compounded by the fact that the Internet was fashioned on a military system designed to circumvent interference and external controls (Udotai, 2015). Even though the main players in the creative anarchy of internet (i.e. the military) have come to see that some basic ground rules must be established and antisocial behavior, vehemently discouraged if the Internet is to reach its full potential (Okeshola and Adeta, 2013). The main question now remains “how exactly to do this”.

Cybercrime can be dated back to the year 1820. The case of Joseph-Marie Jacquard, a textile manufacturer in France, created a loom in order to reduce the stress of weaving fabrics. Joseph had to let some of his staffs go as the loom was already carrying out their jobs. In a bid save their jobs, they sabotaged this invention trying to discourage Joseph from using the loom (Price, 2010). The first "hackers" rose in the 1960s at M.I.T. and were more interested in toy trains than PCs. They were individuals from a model train aficionado bunch on grounds who adjusted and rerouted toy prepare tracks and changes to make them perform speedier and in an unexpected way. The expression "hack" implied a rich, witty or propelled method for completing things. M.I.T. understudies being M.I.T. understudies, it was not some time before some of these prepare programmers started utilizing their gear aptitudes to the new centralized computer registering frameworks being contemplated and created on grounds (Snow, 2011). The PC programmer was conceived. Unavoidably, motivation swung to misuse. The main case of system hacking happened in 1972 when a man named John Draper found that a toy shriek given away inside Cap'n Crunch oat produced a tone at 2600 MHz. This was a similar recurrence that empowered a man to get access to AT&T's long-remove exchanging framework. Mr. Draper, who wound up noticeably known by the moniker 'Top n Crunch', fabricated a gadget he called a "blue box" that utilized the tone to make free phone calls (Jart, Bryn and Kijewski, 2016). Phone programmers wound up plainly known as "phreakers" and included Steve Wozniak and Steve Jobs, future organizers of Apple Computer, who propelled a home industry making and offering blue boxes. The invent and development of computers, have increased and provided more opportunities for cybercrime today. Although, computers and the internet in general provide an easy way of doing things unimaginable to the human mind, but it has also brought along with it various forms of harmful crimes that have negative effects synonymous to regular conventional crimes (Schulberg, 2008).

Cybercrime is a serious threat that affects counties, states, organizations and even individuals (Price, 2010). It ranges from different types of attacks that could either cause damage financially, physically or even emotionally. Cybercrime is just as dangerous as conventional crime and could even be said to be more dangerous since these crimes are committed in a virtual world and are very stealthy and difficult to tackle (Udotai, 2015). The definition of cybercrime, its classifications, types, different cases of cybercrimes over the years and lastly some preventive measures against cybercrimes will be discussed in the following sections.

II. CYBERCRIME ATTACK

The word ‘crime’ is synonymous to words like misconduct, wrongdoing, illegality, offense, felony, villainy. Saulawa and Abubakar in 2014 describe crime as the act of engaging in illegal activities that would most likely have a negative impact on people, organizations or a nation as a whole. Crime has been in existence since the creation of man and has increased steadily with the evolvement of man. Crime tends to reduce the development of a nation because it has a negative effect on the social and economic development of a nation. Merriam-Webster dictionary defines cyber as anything that involves computers or computer networks such as the internet. The word cyber involves information technology (IT), the culture of computers and virtual reality.
Nayak and Tapaswini in 2013 define cybercrime as crimes that involve the use of a computer as a tool or as a targeted victim and just like real word crimes, Cassim states in 2015 that cybercrime is not totally different from conventional crime as they both involve committing acts that are punishable by law and that the only difference is that cybercrime is committed over the internet with the use of computers. Cybercrime primarily involves the use of computers, internet or computing devices, all these can either be used as a tool or as a target. This gives the two classifications of cybercrimes i.e: Computer as a tool and Computer as a target. Tables 1 describe the classification and types of cybercrime attacks.

Table 1. Types and Classification of Cybercrimes

<table>
<thead>
<tr>
<th>Computer as a tool</th>
<th>Computer as a target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Crime</td>
<td>Email Bombing</td>
</tr>
<tr>
<td>Cyber pornography</td>
<td>Denial of Service attack</td>
</tr>
<tr>
<td>Cyber defamation</td>
<td>Virus or Worm Attack</td>
</tr>
<tr>
<td>Cyber Stalking</td>
<td>Web Jacking</td>
</tr>
<tr>
<td>Cyber Terrorism</td>
<td>Financial Crime</td>
</tr>
</tbody>
</table>

1. Computer as a Tool:
When a computer is used as a tool to commit cybercrime, the target or victim is mostly individuals (also their properties) and the society at large. The effect of the damages done is seen in real life and does not exist in the virtual world. It is in a way similar to conventional crimes but in this case, the computer can be likened to a gun an armed robber uses to kill an individual. The computer is used to cause actual and real life damages. The damage dealt is largely psychological and intangible, which makes it even more difficult to take legal actions against the perpetrator (Dashora, 2011).

2. Computer as a Target:
This type of crimes is mostly committed by hackers. The effect can lead to loss of a lot of money. It involves having technical knowledge of computers. These type of crimes started only when computers came into existence. Black hat hackers often try to cause harm to a system either by introducing a virus, Trojan horse or other malwares. They often try to get unauthorized access into other people’s computers or networks in order to get restricted data or perform malicious acts (Dashora, 2011). These types of crimes affect organizations mostly and in most cases makes them lose credibility, which could in turn affect the business adversely even leading to its closure. These crimes are very dangerous and hard to deal with especially in our country as we lack the technical knowledge on how to deal or manage these crimes.

Actual attack scenarios with dates, losses recorded and possible causes are discussed as follows:

a. Financial Crimes:
This involves a crime that leads to the loss of money. Most times it involves stealing of credit cards or ATM cards. A recent case in Africa was the famous high yield investment program (HYIP), MMM (Mavrodi Mundial Movement) which in reality was a Ponzi scheme to get people to put up money in order to get double their investment in return. After millions of people had put in their money, this platform shut down. This left people in emotional and financial distress and because this crime (theft) was done over the internet, no one was held responsible and the victims never got back their money.

b. Cyber Pornography:
This would include all forms of pornography either done on the internet or done using the internet such as pornographic magazines produced using computers (to publish and print the material) and the Internet to download and transmit pornographic pictures, photos, writings (Price, 2010). One of these cases was that of a student that was bullied in school by his classmates and teachers (Dashora, 2011). To get back at them, he morphed their faces against nude obscene images and put these pictures up on the internet. Another incident, was that of a Swiss couple in Mumbai (2000) that took indecent photos of underage children and put up these pictures on a site for pedophiles.

c. Cyber Defamation:
This is the act of damaging the reputation of people. The internet can be used as an easy tool to do this. The result of this crime is a negative psychological impact on the victims. A case example were colleagues of a certain man (India, 2000) who sent defamatory emails to his boss in order for him not to be awarded with a promotion at work. After much investigation, it was discovered that it was only a plot against the man and the perpetrators were duly punished (Dashora, 2011).

d. Cyber-Stalking:
Stalking can be defined as “pursuing stealthily” (Dashora, 2011). Bombarding people with emails also constitutes cyber stalking. This could cause victims to be scared of an unknown danger and often leads to psychological trauma.

e. Cyber Terrorism:
A cyber terrorist can be described as someone who launches an attack on government or organization in order to distort and or access stored information stored on the computer and their networks (Hassan, Lass and Makinde, 2012). Cyber terrorism can be defined as any acts that threatens or tends to intimidate a person or organization. Cases of these are seen by terrorist groups such as Boko Haram and ISIS who use the internet to instill fear on people by means of violent acts.

f. Email Bombing:
This involves sending so many emails to a company’s mail server leading to the crash of mail server. In one case, a foreigner who had been living in Simla, India for about thirty years wanted to take advantage of a scheme introduced by the Simla Housing Board to purchase a land at a lower rate. His application was rejected due to the fact that the 169 schemes were only for Indian citizens. In a bid to revenge, he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed (Price, 2010).

g. Denial of Service Attack:
This involves flooding a system with so many false connection requests that the system does not respond to legitimate requests. A variation of DoS is known as Distributed Denial of Service Attack (DDoS). DDoS is worse that DoS because in this case, the perpetrators are widespread in different geographical locations, so it is
difficult to control such an attack. The attack involves sending excessive demands to the targets computer that exceeds the limit causing the servers to crash. Websites like Amazon, Yahoo, eBay, CNN have been victims to DoS attacks.

h. Virus or Worm Attacks:
Viruses are small programs that replicate and hide itself in order programs usually without your knowledge (Snow, 2011). The most common way of spreading virus is through the targets email address by sending it to everyone on the victims’ contacts. Most viruses do not cause actual harm to the target but they cause network slow down due to the heavy network traffic caused by the network replicating itself. Other viruses also alter or delete the data on a targets computer. Unlike viruses, worms do not need a host, they make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory (Abdullahi and Abubakar, 2014). Viruses or worms are developed by hackers and placed on the internet for the main purpose of causing harm to people’s systems. Viruses can also be spread through email attachments. Viruses can also lead to the crash of an organizations network.

i. Web Jacking:
This happens when a hacker forcefully takes over control of a website by changing the password (Ani, 2015). The rightful owner would have no control over the website. In most cases these control is leveraged for money. Just like a kidnapping case, the hackers might ask for a huge sum of money to release control of the website. In a case, the owner of a hobby website for children received an email that her website had been hijacked and she was to pay a certain amount of money. Thinking it was a joke, she ignored the message (Price, 2010). The hackers then altered a page on the website entitled “How to Have Fun with Goldfish” and put up “How to Have Fun with Piranhas”. The kids who went on this site thought it was okay to play with these dangerous animals, were severely injured. This was a case of cybercrime that led to damages on both the owner of the site and on innocent kids.

The above cybercrimes are examples of crimes conducted using computers as a tool and computer as a target, computers which could lead to the crash of servers and even lead to loss of money and also downtime.

III. CYBERCRIME DETECTION MODELS

The main aim of all cyber criminals is to find a way through the security controls and gaining access into the protected network of an individual or organization for many reasons. It can be through gathering of sensitive data or money fraud from the individual or organization. That is why organizations, companies, governments and institutions, as well as ordinary citizens all over the world are interested in the detection of all attempts of malicious actions targeting their computer networks and single machines (Chaminda, Nasser, Hannan and Bruce, 2014). These sections highlight the detection, prevention and hybrid models (parameters, architecture, results) developed for cybercrimes by different researchers with different approaches.

Jasiul, Szpyrka and Sliwa (2014) developed a malware detection model using coloured petri-net. The model was developed to take a set of suspicious events as an input, this set of suspicious event is received from the process ‘hooking engine’, so-called PRONTology developed by the same authors in a different research work. This “hooking engine” is based on ontology reasoning used for the purpose of filtering single malicious incidents among hundred of thousands of regular ones. These single events are passed on to the PRONToNet engine (the PRONTology model developed in Coloured Petri-Net). The hierarchical structure of colored petri net (CP-net) model of PRONToNet, CP-net model primary module of PRONToNet and acquisition module is presented in Figures (1, 2 and 3) respectively.

Fig. 1. Hierarchical Structure of Colored Petri net (CP-net) model of PRONToNet (Jasiul, Szpyrka and Sliwa, 2014).

The primary module of the CP-net model represents the PRONToNet threat tracking tool. As presented on the left-hand side of Figure 2, the places marked with ellipses stores tokens that represent particular assets that might be affected by malware: F, a place storing tokens indicating files; R, registry entries; P, processes; D, domains; IP, IP addresses that the malware may communicate with. All these places represent tracked symptoms. The second column in Figure 2 consists of substitute transitions that are relatively related to the acquisition process in Figure 3. The next column is made up of places indicating particular assets affected by malware activated in the monitored system. Markings of these places represent observed symptoms.
They are processed by a substitute transition called Verify, which is aimed at reasoning if the system is infected by a certain malware type. As a consequence, the place RESULT is marked with a vector informing about particular malware type and related symptoms.

In 2014, Chaminda, Nasser, Hannan and Bruce proposed an intrusion detection framework for cybercrimes using Bayesian Network to detect and prevent attacks such as denial of service, probes, user to root and remote to user attacks. The proposed IDS framework has three major functionalities which were implemented using WEKA Java API for machine learning. The first function is the IDS enquired with a dataset pre-processing technique such as, attribute selection, attribute filtering, and instance filtering. Second is the Bayesian network classification model, which is the key component in the system, which does the classification of the network data and the third is the Inference analyzer which was designed as the prediction module for incoming testing network traffic. These modules named as data preprocessing, Bayesian network structure learning and inference algorithm module to classify the incoming new data respectively as presented in Figure 4.

**Pre-processing:**
Pre-processing is responsible for data preparation for the Bayesian network model learning process. In this section dataset feature will be analyzed based on the attacks nature and additional domain knowledge. WEKA attribute filtering has been used with other pre-processing techniques such as attribute selection, attribute discretize and filling missing instances. Cyber-attacks are recorded in KDD dataset, therefore, Bayesian network by focusing on each attack type was built with identified attack types of DDoS, R2L, U2R and Probes.

**Bayesian Network Structure Learning (Building Bayesian Models):**
This is the main module of the proposed IDS, the proposed architecture contains four Bayesian networks to detect four different attack types. Data distributor is used to feed relevant data (network traffic) to relevant Bayesian network model for training. These models are adaptable to detect new attacks since proposed IDS support adding new Bayesian networks or modifying of existing network with attack’s features.

**Inference Analyzer:**
Once all the Bayesian network models are built (trained on network traffic) and those networks are ready for predicting attacks in incoming network traffic. Test data divided by inferential analyses to each Bayesian network to classify in the attacks. Inference Analyzer classifies each record of the input data to normal connection or to a relevant attack.
The IDS was experimented in Java and shows the ability of detecting novel attacks by continuing learning with different datasets. The testing dataset constructed by sampling the original KDD dataset to contain balance number of attacks and normal connections. The experiments show that the system is effective in detecting attacks in the test dataset and is highly accurate in detecting all major attacks recorded in DARPA dataset.

Hanif and Yashwant (2012) developed a cybercrime detection and prevention model by using Support Vector Machine (SVM) and AdaBoost algorithm in order to reduce data damaging due to running of malicious codes. Another good cybercrime detection model was developed by Sayyada, Perumal, Mohammed, Quadri and Quadri in 2015, the model was developed to learn Cybercriminal' Behavior as part of methodology and represents the typical behavior of cybercriminal users based on the content of their Web activities. The author assumed that it is possible to collect Web pages from criminals-related sites. Figure 5 depicted the architecture of the cybercriminal behavior. The collected pages serve as the input to the Vector Generator module that converts the pages into vectors of weighted terms (each page is converted to one vector). The vectors are stored in the Vector of Cyber criminals Transactions DB for processing. The collected vectors are accessed by the clustering module and unsupervised clustering was performed upon it leading to n clusters that represent the typical topics viewed by cybercriminal users. For each of the clusters, the cybercriminal Represent or module computes the centroid vector which represents a topic typically accessed by cyber criminals. In the Monitoring module of the detection model, the Vector-Generator converts the content of each page accessed by a user into a vector representation (referred to as the ‘access vector’).

\[
\text{Similarity} = \frac{\sum_{i} \cos(x_{iCv}, x_{Bv})}{p}
\]

\[\text{where } i_{Cv} \text{ is the } i^{th} \text{ centroid vector, } Bv \text{ - the access vector, } i_{1xCv} \text{ - the } i^{th} \text{ term in the vector } i_{Cv}, i_{1xBv} \text{ - the } i^{th} \text{ term in the vector } Bv, \text{ and } p \text{ - the number of unique terms in each vector.}
\]

The Detector uses the access vector and the criminal Behavior and tries to determine whether the access vector belongs to criminal groups. This is done by computing similarity between the access vector and all centroid vectors of the criminal Behavior. The cosine measure is used to compute the similarity. The detector issues an alarm when the similarity between the access vector and the nearest centroid is higher than the predefined threshold denoted by following expression Xr:

\[
\text{If } \text{Similarity} > X_r \text{ then issue alarm}
\]
Neeru (2014) developed an intelligent cyber defense system (ICDS) using Artificial Intelligence and Data Mining techniques. Artificial Intelligence was used for developing intelligent system for Cyber Defense. Data mining is being applied to problems such as intrusion detection and auditing. Figure 7 depict the system model of ICDS the module of the model according to the author is discussed as follows:

- **Cyberspace:** The word Cyberspace was used to describe the whole range of information resources available through the computer networks. It is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures (Olabiyisi et al., 2012).
- **Knowledge Base:** Whenever a user uses cyberspace for any purpose, it is stored in the knowledge base as a web log file that maintains the history of all the activities performed in the cyberspace. It must get more and more intelligent with every activity made in the cyberspace. It becomes the basis for detection and analysis of any suspected/false activity performed (Ogirima et al., 2013; Oyediran et al., 2016).
- **Intelligent cyber sensor agents:** Intelligent cyber sensor agents are computer-generated forces which detect, evaluates and responds to cyber-attacks in a timely manner.
- **DM Techniques:** Data mining is being applied to problems such as intrusion detection and auditing to detect unusual patterns and behaviors. Some data mining techniques (like clustering, classification, association rules and prediction) can be applied to identify some unusual patterns in the web log file.
- **AI Techniques:** Once the DM techniques applied to data for pattern recognition, some AI techniques (like neural network, genetic algorithms) can also be applied to make the system more intelligent to monitor, analyze and find the actual cybercrime. DM and AI techniques together use cyberspace for performing their functions at various stages.
- **Response:** After detecting the actual cybercrime performed by criminals/intruders on a cyberspace, the results in the form of alerts, alarms are provided.
- **Visualization tools:** Results can also be shown by various visualization techniques like GUI, graphs, charts, etc. Decision making: Once the results are shown, appropriate decision can be made by the concerned authorities.

Jyothsna and Nilina (2013) analyzed the AI based intrusion detection and prevention system. The author defines Intrusion Detection System (IDS) as a system that can offer protection from external users and internal attackers, where traffic doesn't go past the firewall at all. The firewall defend an organization from malicious attacks from the Internet and the IDS if someone tries to break in through the firewall or manages to break in the firewall security then tries to have access on any system in the trusted side. It alerts the system administrator in case there is a breach in security. An IDS is like a smoke detector that raises an alarm if specific things occur. Figure 8 depicted an IDS system based on AI, the author established that Artificial Neural Networks (ANNs) can enhance the performance of Intrusion Detection Systems (IDS) when compared with traditional methods. ANNs is an information processing system which is inspired by biological nervous system.

**IV. CONCLUSION**

In our day to day activities we do most of our living online, most of our everyday communications and commercial activities now take place via the Internet. However, it also gave birth to difficult issues such as cybercrime. Available academic resources show that AI and data mining techniques already have numerous applications in combating cybercrimes. This paper has briefly presented possibilities of techniques and models so far in cyber field for combating cybercrimes and their current limitations. In conclusion, the development of more robust cybercrime detection and prevention models is required as the cybercrime tends to increase daily.

**REFERENCES**


