Detection Techniques of Cyber Crime

Aher Rutuja Kisan
Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Otur, Pune India

***Abstract* - The world is more advanced in communication after the invention of the Internet. Cybercrime also called as a computer crime, is any crime that involves computer and a network. As individuals and businesses increase their reliance on technology, they are exposed to the growing cybercrime threats. Using the computers for our day-to-day transactions is quite common now a day. A lot of problem facing today's society is the increase a cybercrime or a e-crimes. Thus e-crimes pose threats to nations, organizations and individuals across the globe. Cyber security and searching methods to get secured part of the study. Cybercrime has caused lot of damages to individuals, organizations and even the government. cyber security plays an important role in the field of information technology. This paper aims to provide a review of cybercrime and crimes in India.**

***Index Terms* - cybercrime detection techniques, security, fuzzy logic, data mining, machine learning, cybercrime, e-crime, financial crimes.**

I.INTRODUCTION

Cybercrime are threaten a person, company or a nations security and financial health. The cybercrime is similar to the DOS attacks. cybercrime is criminal activity that either targets or uses a computer or a computer network device. The cybercrime is done by a cybercriminals or hackers to make a money.

Cybercrime is carried out by individuals or organizations.[5] Cybercriminals may also carry out what is known as a Distributed-Denial-of-Service attack. Cybercrime or computer-oriented crime is a crime that involves a computer or a network. The cybercrime, especially through the Internet has grown in importance as the computers has become control to commerce, entertainment, and government.

Most cybercrime is an attack on information about the individuals, corporation, or government.[1] Cybercrime is any criminal act dealing with computers or networks. In addition to crime against computers, such as hacking. Cybercrime include traditional crime conducted through the use of a computers.[1] The major categories of computer crime are follows:

1. Computer Assist
2. Computer incidental
3. Computer specific

1) Computer Assist:

Computer assist crime is criminal activity that is not exclusive to computers, but computers were used to tools commit the crime. Examples of computer assist are theft and fraud, child pornography.

2)Computer incidental:

Computer incidental crime is a criminal activity in which the computer provided information but way incidental to the actual crime. Examples includes customer list used by traffickers.

3)Computer specific:

This crime is criminal activity directly involving or targeting networks, stored information, and computer systems. Examples include hacking, defeating access codes, or denial of service attacks.

The nature of a cybercrime makes it difficult to assess damage determines a point of entry and track the physical location of computer criminals. In order to efficiency collect information in trans-border crimes, most of Europe has adopted the following procedures:

1. Collect information fairly and lawfully.
2. Only use information for the intended purpose.
3. Hold information for a reasonable amount of time.
4. Allow individuals to make corrections to the data.
5. Only obtain current data.
6. Never disclose information to others.

Cybercrime really began to take off in the early 2,ooos when the social media came to life. The surge of people putting all the information they could into a profile database created a flood of personal information and the rise of ID theft.

The first major wave of cybercrime came with the proliferation of email during the late 80's. it allowed

for a host of scams and malware to be delivered to your inbox.
The next wave in the cybercrime history timeline came in the 90's with the advancement of a web browsers.
The latest wave is the establishment of a global criminals industry totaling nearly a half-trillion dollars annually. These criminals operate in gangs, use well established methods and target anything and everyone with a presence on the web.
The literature review of this study covered studies that a technique for detection and prevention of cybercrimes.
This study provides a comprehensive review of the cybercrime detection techniques, which are categorized based on the different detection methods.
Machine learning techniques for predicting output according to input data.[1]
Neural network based on methods are used to find the reasonable solution on the cybercrime.
Fuzzy logic and genetic algorithm which are intended to minimize the false alerts. [4]

II. TYPES OF CYBER CRIME

A. DDOS Attacks

There are used to make an online service unavailable and take the network down by a overwhelming the site with traffic from a variety of source. The hacker then hacks into the system once the network is down. DDOS attacks achieve effectiveness by utilizing the multiple compromised computer system as source of attack traffic.
DDOS attacks are carried out with network of internet connected machines. Criminals perpetrators of DOS attacks after target sites or services hosted on high profile.

B. Botnets

A botnet is a collection of a internet connected devices infected by the malware that allows hackers to control them. Botnet owners can have access to several thousand computers at a time and can command them to carry out malicious activities.
The number of bots will vary from botnet to botnet and depends on the ability of the botnet owner to infect unprotected devices.

C. Identity Thefts

This is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or a purchase. Identity theft occurs when someone steal your personal information and credential to commit fraud.
There are various forms of identity theft, but the most common is financial. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government benefits in your name. they may do this by finding out users password through hacking.

D. Phishing

Phishing is the fraudulent attempts to obtain sensitive information or data. phishing is a method of trying to gather personal information using deceptive e-mails and websites. Phishing is a cyber-attack that uses disguised email as a weapon.

E. Cyberbullying

The cyberbullying are takes place over the digital devices like phone, computers, and tablets. Cyberbullying can occur through SMS, text, and app its ides sending, posting or sharing negative, harmful, false or mean content about the someone else.
Some cyberbullying crosses the line into unlawful or criminal behavior.

F. Cyber Extortion

Cyber extortion is when the cyber-attacks demand money or something another in return for stopping the attacks or returning your access system data. Cyber extortion attacks start with a hacker gaining access to an organization system.
Cyber extortion occurs when hacker access your sensitive data, including customer information and trade secrets.[1]

G. Unauthorized System Access

It is refers to individuals accessing an organizations networks, data, endpoints, applications or devices, without receiving permissions. Unauthorized access is when a person who does not have permissions to connect to or use a system gains entry in a manner unintended by the system owner.

III. DETECTION TECHNIQUES OF CYBER CRIME

1. Cybercrime detection techniques using machine learning.
2. Cybercrime detection techniques using neural network.
3. Cybercrime detection techniques using Deep learning.
4. Cybercrime detection techniques using fuzzy logic neural network.
5. Cybercrime detection techniques using Data mining.

1] Machine Learning Techniques:
Machine learning is the science of predicting output based on given input data also called as training data.[1] Machine learning is the study of computer algorithm that improve automatically through experience and by the use of data.

2]Neural Network techniques:
A neural network technique is a simulation of how the human brain works.[1] The amount of research has been conducted on the application of neural network to detect the computer instruction is very limited.[2]
Neural network offers the potential to resolve a number of the problems encountered by the other current approaches to instruction detection.

3] Deep Learning:
It is also used to feedforward neural network to detect Arabic cyberbullying using tweets as the data set.[1]

4] Fuzzy Neural Network:
It is belong to the hybrid structure family which perform several acts in various contents PF pattern classification which include the detection of abnormal or anomalous behavior. The use of fuzzy systems is necessary in cases where the classical logic approach becomes unfeasible for solving the problem due to the nature of its complexity.[4]

5] Data Mining:
Data mining technology is applied to fraud detection to ascertain the scam detection model to depict the process of creating the scam detection model and then to begin the data model with any classifier.
Data mining emphasize the extraction of data from database and various patterns can be concluded for deriving association rules. Data mining which is defined as the process mining or extracting data into productive information. [3]

IV. DATASET

The KDD ’99 dataset are generate in 1999 by stolfo. The dataset focuses on four types of attacks: DOS, U2K, Remote to local and probing attack. The KDD ’99 dataset is no longer. Thus NSL-KDD was created in 2009 by Tavallaes.[1]
This dataset consists of KDD dataset records. DARRA 2000, which included DDOS attack it generated in 2000 by the MIT Lincoln laboratory.
The CICIDS2017 dataset was presented in 2017 by the Canadian institute of cyber security.

V. CONCLUSION

The detection techniques of comprehensive cybercrime paper have covered all several types of cybercrimes and their achieved detection techniques as well as some their limitations.
This paper also intensively on the available datasets finding the proper detection techniques or a cybercrime. There are aspects of the research of cybercrime analysis, to prevention of cybercrime and decreases the lot of cybercrime. Many of the studies on the current literature have focused on the which factor affecting e-crime such as sexual, financial, cultural, social, and political. Applied the data mining techniques for identifying the DOS attacks. The aim of this paper to overcome a lot of crime, cybercrime, or e-crimes.

REFERENCES

[1] Wadha Abdullah Al-Khater, Somaya Al-maadead Abdulghani Ali Ahmed, Muhammad Khurram Khan: Comprehensive Review of Cyber Crime Detection Techniques, August 5, 2020.
[2] JinLi, PingHe: Detection and prevention of cybercrime Based on Diamond Factor neural network.
[3] Mr.G.Sivaselvan, Dr.V.Vennila, R.Senbagavalli, E.Shanmugapriya, K.umadevi, S.Suganthi: Applying Data mining Techniques in cybercrime.
[4] Lucas Oliveira Batista, Gabriel Adriano de Silva, Vanessa Souza Araujo: Fuzzy neural network to create an expert system for detecting attacks by SQL injection.

[5] Mariam M.H.Alansari, Zainab Aljazzaf, Muhammad Sarfraz: On Cybercrime and cyber security.
[6] Esther Ramdinmawalli, Seema Ghisingh, Usha maty Sharma: Astudy on the Cybercrime and cyber criminals: A Global Problem-3 june 2014.