A STUDY OF CYBER SECURITY TOWARDS CYBER CRIME PREVENTION AND DETECTION TECHNIQUE

-Dr. Devendra Singh, Assistant Professor, Haryana institute of Public Administration, Gurugram

ABSTRACT:

Cybercrime is an ever-evolving phenomenon that is difficult to understand. Cyber criminals are growing more and more skilled, and they're now going after individuals as well as businesses and government agencies. As a result, additional defences are necessary. Since businesses began using computers to conduct business, cybercrime has grown in complexity and cost. The Parliament attack is one of several cybercrime case studies. Cybercrime and cyber security have been explored in this paper, along with various cybercrime prevention and detection strategies, such as Tripwires, Honey Pots and anomaly detection systems on the operating system. This research includes discusses legislation enacted to combat cybercrime, as well as suggestions for staying secure when surfing the web. Child pornography, stalking, identity theft, cyber laundering, credit card theft, cyber terrorism, drug selling, data leakage, phishing, and other cyber hacking are all examples of common cybercrimes. In most cases, these types of cybercrimes result in user privacy breaches, security breaches, corporate losses, financial fraud, or damage to public and government property. As a result, this study examines in-depth how to detect and prevent cybercrime. After examining the many sorts of cybercrime, it explains how they might compromise computer systems' privacy and security. Cybercriminals may use various tactics to perpetrate these crimes against persons, organisations, and society. After that, the study goes on the current methods for detecting and preventing cybercrime. It analyses the advantages and disadvantages of each technique objectively. According to the paper's recommendations, cybercrime detection models should be developed that are more effective than the current methodologies.

KEYWORDS: Cyber Crime, Cyber Security, Honey pots, Trip wires, Anomaly detection, Case Study, Regulation Acts, Online safety tips

INTRODUCTION

A cybercrime is a crime committed with the aid of a computer or another form of electronic communication in order to terrorise victims or cause damage, hurt, or destruction to their property. Computer-assisted and computer-focused crimes are the two types of cybercrimes. Crimes committed using computers include child pornography, fraud, money laundering and stalking online [1]. Examples of crimes committed using computers include hacking, phishing, and website defacement. Owing to a variety of factors, including the culture in which the crime was committed, the gravity of the offence, and unreported cases due to lack of information or societal restraints, it is difficult to acquire accurate and official statistics on cybercrime. The level of detail reported in these incidents is heavily influenced by law enforcement [1].

Computer crimes, electronic crimes, and e crimes are all terms used to describe cybercrime. "Cyber" is shorthand for "cyberspace." The computer network's electrical medium. Where online conversation occurs. Computer-mediated acts that are either illegal or considered criminal by certain parties and that can be carried out via worldwide electronic networks are referred to as cybercrime," according to Wikipedia. A "cybercrime" is a crime that involves the use of a computer or network as part of the offence. cybercrime was broken into two categories and defined thus:

1. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

2. Cybercrime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

CYBERCRIME TYPES

Cybercrimes can be divided into several categories [1]. The following subsections name and explain these categories in detail.

A. CYBER TERRORISM

Unlawful acts of violence against persons and property are at the heart of what is known as cyber terrorism. Ideological and political motives are often present. As a result, this sort of cybercrime has the potential to cause fear, anxiety, and aggression in people or to disrupt and destroy property. Moreover (e.g. computers and networks). Cyber terrorism can also have an impact on the integrity and accessibility of data [2]. Terrorists use the Internet to disseminate propaganda, recruit individuals, influence public opinion, and shut down the national infrastructure (e.g., transportation, dams, traffic lights, and energy facilities). Ukrainian power grid attack, which began with phishing email in December 2015, is an example of cyberterrorism. Speculation about the safety of citizens is disrupted by some sequences of cyber terrorism. Political decision-making can also be influenced by such sequences. Cyber terrorism can cause serious economic losses, physical damage, and violence, which can lead to death and disrupt social cohesion [2].

B. CYBER WARFARE

When it comes to cyber warfare, there are no weapons involved, but rather cyber-attacks. Organizations or groups of hackers can carry it out without the government's consent, which can cause political issues between countries [15]. To this day, the most common kind of conflict is cyberwarfare and cyberattacks. In the previous 20 years, there have been a number of cyber battles. During the 2008 cyberwar between Russia and Georgia, for example, the Georgian government's websites were subjected to SQL injection assaults, distributed denial-of-service attacks, and cross-site scripting attacks [15]. Both Israeli and Arab hackers have engaged in numerous cyberwars during their conflict. A cartoon depicting the assassination of Hamas leader Khaled Meshaal was accompanied by the Arabic caption "Time is running out" after Israel assaulted Al-Aqsa in December 2008 [15]. The Estonian government's websites were hacked in 2007 by a group of hackers. The attacks were attributed by the Estonian government to Russia. On December 23, 2015, the entire country of Ukraine was left without electricity. Malicious attacks knocked out more than 50 substations and three regional power distribution businesses known as oblenergos [16]. Some 225,000 consumers were disrupted for a short period of time. Due to the attack, customers were unable to call the centre to report power disruptions. After six hours, the power was manually restored. Companies in three separate infrastructure sectors were determined to have malware, but their activities were unaffected. Once again, Ukraine's national railway system and some ministries were affected by a year-long attack on a Ukrainian power facility. [17] After the incident, all of the oblenergos were forced to work in constrained settings and manually try to recover.. Aside from slowing down and stopping the recovery process, the attackers employed ways to do just that. Remote disconnection of the uninterruptible power supply system is one example of this. The passwords of legitimate users have also been changed by the attackers. As a result, they were unable to access the system while it was being repaired. The power stations were shut down for six months as a result of the attack. As a result of the attackers' deployment of malicious firmware, all gateways were rendered unusable and could not be recovered. That's why they had to buy new equipment and integrate it into the system, but it cost a lot of money.

C. CYBER ESPIONAGE

Using spies and stealing sensitive information for the benefit of competitors or foreign governments is considered espionage. When it comes to cyber espionage, the tools of the trade are computers [15]. Cyber espionage assaults by Chinese entities affected more than 300 British businesses in December 2007 [15]. In addition, from 2003 to 2006, China launched a series of coordinated attacks on the computers and networks of the US Department of Defense. "Titan Rain" was the codename given to this coordinated assault.

D. CHILD PORNOGRAPHY

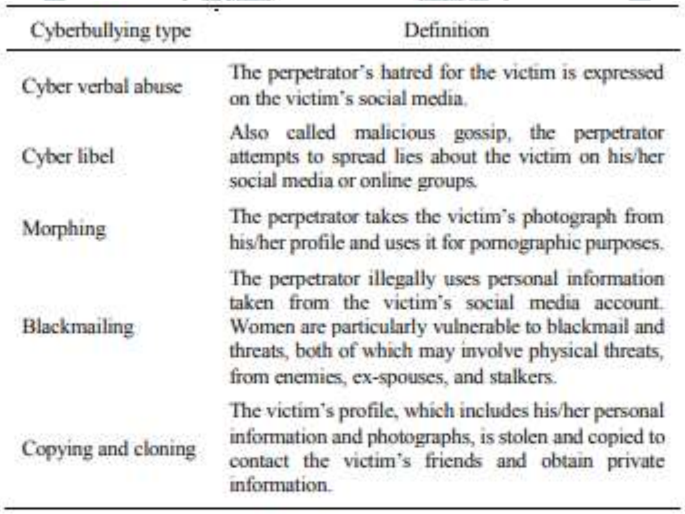
The term "child pornography" is used to describe images, movies, and audio recordings depicting children in sexually suggestive poses while wearing little or no clothing. In an effort to reduce the number of child pornography cases, numerous research have been carried out. Most child pornographic materials are disseminated for either profit or charity. There are numerous websites that sell child pornography for profit. P2P networks can be used to distribute and share child pornography content for non-profit objectives. It was illegal to produce, possess, or distribute any digital content including child pornography in the United States.

Self-esteem, trust in others, and sexual development issues are all included in this category. On the other hand, the long-term effects of this crime on the child's psychological well-being are extremely damaging. If a youngster is a victim of cyber-criminals who are targeting children for sexual objectives, the ramifications and troubles will only get worse if the digital content is released online.

E. CYBER BULLYING

With more people of all ages and genders using social media and other forms of technology, negative behaviours like bullying are more likely to occur. When it comes to bullying, youth is the worst possible time for it to happen. Children, teenagers, and women are the most common victims of bullying. A person's personality can change as a result of being bullied. Twitter, Facebook, and other social media can be used to harass and threaten the lives of victims of cyber bullying. When it comes to cyber bullying, identity theft, credit card theft, stalking, and psychological manipulation all fall under this umbrella term. Table 1 describes some of the cyber bullying types that could victim go through.

Table 1 Cyber bullying Types



Cyberbullying type	Definition
Cyber verbal abuse	The perpetrator's hatred for the victim is expressed on the victim's social media.
Cyber libel	Also called malicious gossip, the perpetrator attempts to spread lies about the victim on his/her social media or online groups.
Morphing	The perpetrator takes the victim's photograph from his/her profile and uses it for pornographic purposes.
Blackmailing	The perpetrator illegally uses personal information taken from the victim's social media account. Women are particularly vulnerable to blackmail and threats, both of which may involve physical threats, from enemies, ex-spouses, and stalkers.
Copying and cloning	The victim's profile, which includes his/her personal information and photographs, is stolen and copied to contact the victim's friends and obtain private information.

Women are more susceptible to cybercrime than men since they are more social by nature. They can quickly become acquainted with virtual pals or online groups with whom they can discuss cooking techniques, children and family difficulties, as well as post-pregnancy recommendations, with no trouble at all. According to Halder and Jaishankar, this kind of acquaintanceship could lead to cybercrimes, emphasising a variety of victimisation scenarios.

F. PHISHING

Due of its direct relationship to the end user, phishing is one of the most common attacks. Such attacks involve the attacker fooling the end user into disclosing personal information. Social engineering and spoofing techniques are used to carry out phishing attacks. In an email, the attacker asks the target for sensitive information, warns him or her of an impending attack, and convinces him or her to install malware. It is also possible to receive an email that includes a link to a phoney website. One of the most effective ways to protect yourself from scams is to avoid clicking on links in strange emails. To avoid being a victim of a phishing scam, use only secure websites, such as those that begin with 'https,' and install anti-virus, firewall, and anti-phishing toolbar software.

G. DENIAL-OF-SERVICE ATTACK

Denial-of-service (DoS) attacks are a major online threat in which the attacker compromises the availability of services. ICMP and SYN floods are two methods of DoS that cause compromised systems to be overwhelmed with requests, leading the systems to breakdown and stop providing the intended service. In a distributed denial-of-service (DDoS) assault, the attacker has access to several channels in a network and uses each victim as an agent to attack another system, much like a zombie would. Figure 1 illustrates an example of a DDoS attack. DoS and DDoS attacks take place through the following methods:

1) ICMP FLOOD ATTACK OR SMURF ATTACK: ICMP is a connectionless protocol used to diagnose networks and identify errors. The attacker overwhelms the target server with a huge number of ICMP messages, and the victim server deals with each message and processes it until the server becomes overwhelmed and crashes.

2) SYN FLOOD ATTACK: The attacker overwhelms the target system with a flood of SYN attacks to prevent the targeted system from responding to legitimate users.

3) TEARDROP ATTACK: The attacker uses a deluge of jumbled and overlapping packets to completely take down the target system. It is common for legitimate senders to break their communications into packets, but the attacker manipulates the packets to make them huge and payload-laden instead. While a result, the targeted system becomes overburdened and unable to react to genuine users as it attempts to reassemble the altered and overlapped packets. Both implementing DDOS attack prevention services and increasing the website's traffic bandwidth can help avoid or minimise DDOS attacks.

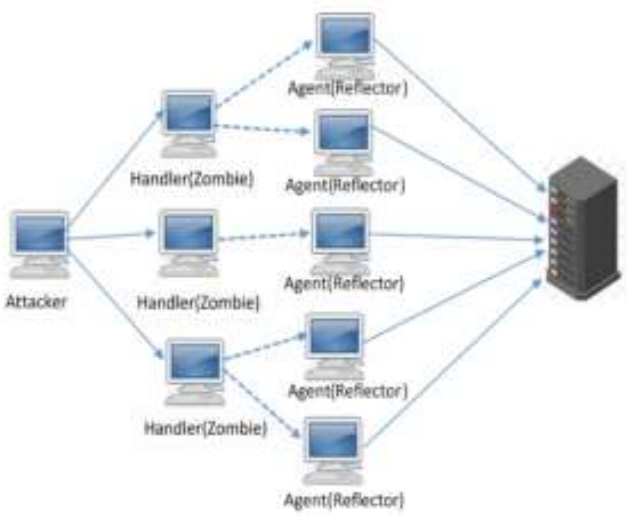


FIGURE 1. An example of a DDoS attack

H. SQL INJECTION ATTACK

It is possible for an attacker to get access to databases by executing SQL queries. Before modifying or erasing the data, the attacker can access the database and obtain its contents. Setting a high level of credentials, such as login and password, is one of the greatest ways to protect against this type of assault.

I. FUTURISTIC IN CYBER ATTACKS

Many new and current technology and devices, such as WiFi, health care devices, robots, and drones, can be the target of futuristic cyber-attacks. Cyber-attacks are a real possibility with these new technology. Wi-Fi technology is used by a wide range of people and businesses, which can put their security at risk. Man-in-the-middle attacks, key reinstallation attacks (KRACKs), and signal jamming are a few instances of potential threats to WiFi users.

Security flaws in implantable medical devices (IMDs) pose a threat to people's health if exploited in the health care sector. Implantable medical devices, or IMDs, are electronic devices that are surgically placed inside the body in order to treat or manage disease. Examples of IMDs devices include the following:

- Implantable cardioverter defibrillators (ICDs) are devices implanted to monitor the heart rate of the patient.

- Insulin pumps are devices implanted to deliver insulin regularly.

- Implantable nerve stimulators that are devices to treat chronic pain via sending electrical current in the human body.

CYBERCRIME DETECTION TECHNIQUES

The amount of cybercrimes has risen significantly because forensics researchers have been unable to totally stop or mitigate them. Due to the wide range of motives (such as money, fame, lust, and curiosity) and means (such as new technology) used by criminals to conduct crimes and achieve their aims, the people or entities targeted by cybercrime (e.g. people or institutions such as banks or properties) vary widely. The development of tools to identify cybercrimes has been the subject of numerous studies in the past. It is displayed in Figure 2 and explained in the following sections which procedures fall under each of these broad groups.

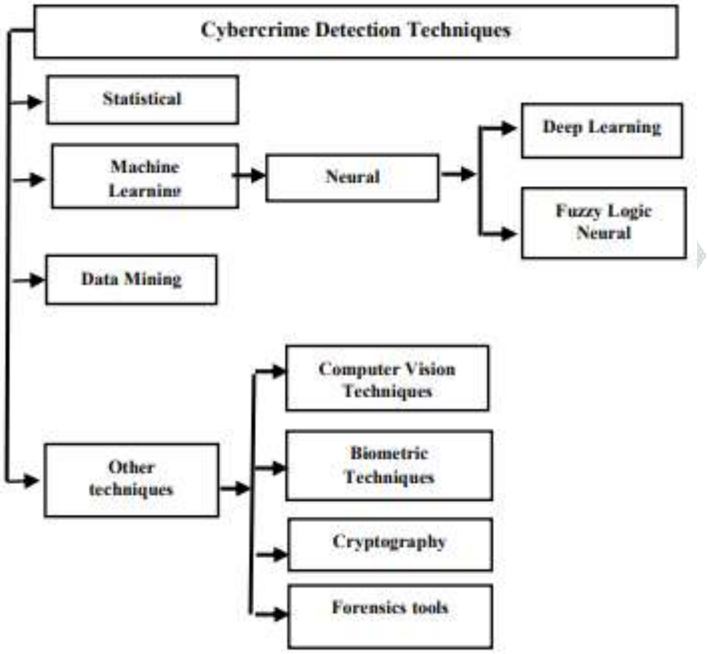


FIGURE 2. Categorization of cybercrime detection techniques

ELECTRONIC CRIME DETECTION

Typically electronic crimes are detected by one or more types of intrusion detection techniques. Such techniques include

- Tripwires;
- Configuration checking tools;
- Honey pots;
- Anomaly detection systems; and
- Operating system commands. Brief overview of each of these intrusion techniques follows:

1 Tripwires: snooping

It is possible to detect significant file changes using software programmes known as tripwires, which capture snapshots of key system parameters. For example, most infiltrating hackers make alterations when they install backdoor entry points or tamper with file system and directory attributes while snooping.

2. Configuration checking tools

Software programmes called tripwires, which take snapshots of important system metrics, can detect substantial file changes. While probing or installing backdoors, most invading hackers alter file system and directory properties to gain access.

3 Honey pots:

Tripwires, which capture snapshots of vital system parameters, can detect significant file changes. Most intruding hackers alter file system and directory properties to gain access while probing or installing backdoors.

4 Anomaly detection systems:

Focusing on anomalous patterns of activity, an anomaly detection system To put it another way, anomaly detection systems build and analyse user profiles, host and network activities, or system programmes in order to find deviations from expected activity. For example, unusual key stroke intervals, irregular orders, and unconventional software operations can provide evidence of an electronic crime.

5 Operating system commands:

The usage of specific operating system commands, such as scanning log files and comparing outputs of comparable applications, can also be used to detect intrusions. When searching for evidence of electronic crime, system administrators typically utilise these commands on a daily basis.

FEW ONLINE SAFETY TIPS:

1) Protect yourself from viruses by installing antivirus software and updating it regularly. You can download anti-virus software from the Web sites of software companies, or buy it in retail stores; the best recognize old and new viruses and update automatically.

2) Don’t open a file attached to an e-mail unless you are expecting it or know what it contains. If you send an attachment, type a message explaining what it is. Never forward any e-mail warning about a new virus. It may be a hoax and could be used to spread a virus.

3) Confirm the site you are doing business with. Secure yourself against "Web-Spoofing". Do not go to websites from email links.

4) Create passwords containing at least 8 digits. They should not be dictionary words. They should combine upper and lower case characters.

5) Send credit card information only to secure sites.

6) Never give out your address, telephone number, hangout spots or links to other websites or pages where this information is available

CYBER CRIME CASE STUDY

1) PARLIAMENT ATTACK CASE

Details about incident:

a) The top cyber cases, including analysing and retrieving information from the laptop recovered from terrorist, who attacked Parliament.

b) Two terrorists had used their laptop to create a Ministry of Home sticker and place it on their ambassador car in order to gain admission into Parliament House, as well as to carry a false ID card with a Government of India insignia and seal that one of the terrorists had.

c) The emblems (of the three lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

CONCLUSION

A wide range of cybercrimes, as well as the detection rates that have been obtained and some of their limitations, have been examined in this paper's comprehensive review. In order to demonstrate their outcomes and highlight their distinct advantages and shortcomings, the presented state of the art was appraised and a comparison was carried out using some tabulated information. In-depth discussion of previously used datasets was also included in this work. To test and evaluate the research's strategy for detecting cybercrime, finding the right data set is crucial. Because of the absence of cooperation between law enforcement and researchers in the collecting of cybercriminal data, benchmark datasets cannot be obtained. In addition, cybercrime can take place on a variety of platforms, including Twitter, YouTube and Instagram; as well as through networks; each of these platforms has its own unique databases. It is suggested that academics build cybercriminal profiling that may be utilised as cybercrime datasets to address the difficulty of data availability. To create cybercriminal profiling, law enforcement and researchers must work together, as well as governmental authorities. This information, which is mostly vital, sensitive, and private, may be used to create a cybercriminal profile, but it's unclear if doing so would be lawful. This is why researchers need to come up with a way to secure data privacy so that they can benefit from the data provided by law enforcement for research reasons and keep their private intact.

REFERENCES

[1] M. Yar and K. F. Steinmetz, Cybercrime and society. SAGE Publications Limited, 2019.

[2] B. Akhgar, A. Staniforth, and F. Bosco, Cyber-crime and cyber terrorism investigator's handbook. Syngress, 2014.

[3] S. Sibi Chakkaravarthy, D. Sangeetha, M. Venkata Rathnam, K. Srinithi, V. J. I. J. o. K.-b. Vaidehi, and I. E. Systems, "Futuristic cyber-attacks," vol. 22, no. 3, pp. 195-204, 2018.

[4] A. Tabasum, Z. Safi, W. AlKhater, and A. Shikfa, "Cybersecurity issues in implanted medical devices," in 2018 International Conference on Computer and Applications (ICCA), 2018, pp. 1-9: IEEE.

[5] J. Liang, M. Ma, M. Sadiq, and K.-H. J. K.-B. S. Yeung, "A filter model for intrusion detection system in Vehicle Ad Hoc Networks: A hidden Markov methodology," vol. 163, pp. 611-623, 2019.

[6] S. Nadali, M. A. A. Murad, N. M. Sharef, A. Mustapha, and S. Shojaee, "A review of cyberbullying detection: An overview," in 2013 13th International Conference on Intellient Systems Design and Applications, 2013, pp. 325- 330: IEEE.

[7] A. Karim, R. B. Salleh, M. Shiraz, S. A. A. Shah, I. Awan, and N. B. J. J. o. Z. U. S. C. Anuar, "Botnet detection techniques: review, future trends, and issues," vol. 15, no. 11, pp. 943-983, 2014.

[8] D. Ramalingam, V. J. C. Chinnaiah, and E. Engineering, "Fake profile detection techniques in large-scale online social networks: A comprehensive review," vol. 65, pp. 165-177, 2018.

[9] A. N. Shaikh, A. M. Shabut, and M. Hossain, "A literature review on phishing crime, prevention review and investigation of gaps," in 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), 2016, pp. 9-15: IEEE.

[10] W. Z. Khan, M. K. Khan, F. T. B. Muhaya, M. Y. Aalsalem, H.-C. J. I. C. S. Chao, and Tutorials, "A comprehensive study of email spam botnet detection," vol. 17, no. 4, pp. 2271-2295, 2015.

[11] H. Hassani, X. Huang, E. S. Silva, M. J. S. A. Ghodsi, and D. M. T. A. D. S. Journal, "A review of data mining applications in crime," vol. 9, no. 3, pp. 139-154, 2016.

[12] M. BinJubier, A. A. Ahmed, M. A. B. Ismail, A. S. Sadiq, and M. K. J. I. A. Khan, "Comprehensive Survey on Big Data Privacy Protection," 2019.

[13] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. J. e. s. w. a. Lin, "Intrusion detection by machine learning: A review," vol. 36, no. 10, pp. 11994-12000, 2009.

[14] A. Aldweesh, A. Derhab, and A. Z. J. K.-B. S. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," p. 105124, 2019.

[15] J. Carr, Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media, Inc., 2011, p. 316.

[16] F. Harrou, B. Bouyeddou, Y. Sun, and B. Kadri, "Detecting cyber-attacks using a CRPS-based monitoring approach," in 2018 IEEE Symposium Series on Computational Intelligence (SSCI), 2018, pp. 618-622: IEEE.

[17] J. Wang et al., "Detecting and mitigating target link-flooding attacks using sdn," 2018.

[18] V. BUTRIMAS, THREAT INTELLIGENCE REPORT CYBERATTACKS AGAINST UKRAINIAN ICS, 2016. [Online]. Available: https://www.sentryo.net/wpcontent/uploads/2017/10/EBOOK-UKRAINIAN-CYBERATTACKS-OCT2017.pdf. Accessed on 9/9/2019.