International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Types of Cyber Crimes and Various Data Mining Techniques: A Review

Gurleen Kaur

Amity University Rajasthan

ABSTRACT

The growth of internet technology and the depth of its knowledge result in a range of security problems, cybercrime, online intrusions, and hackers. The existence of the internet also strengthens network architecture, which encourages different types of online theft and fraud, commonly known as cybercrime or cyberattacks. Data mining tools are effective enough to identify this type of malicious attack more precisely. To identify these types of assaults, a variety of approaches like classification, clustering, and association rules are used.

KEY WORDS: Data Mining Methods, Cyber Crime, Types of Cyber Crime

INTRODUCTION

Data mining focuses on extracting data from numerous databases, identifying trends, and doing a comparative study. Data mining is expanding its application in many other fields, but it has a particularly notable impact on cybercrime. Data mining is the process of collecting useful information from data through mining or extraction. In the beginning of this essay, I described what cybercrimes are, who cybercriminals are, and why cybercrime is hazardous. Next, I listed various sorts of cybercrimes and provided a brief description of each. In the next sections of the paper, I've attempted to explore several data mining approaches used to find cybercrimes.Beginning it with need data mining, definition of data mining , various techniques of data mining and limitations of data mining techniques . At the end is the conclusion

CYBER CRIMES

Use of computer hardware or software to commit an illegal act through computer networks that violates laws and regulations is penalised by the state or another authority. Cyberbullying, cyberstalking, phishing, spamming, DoS assaults, identity theft, hacking transaction fraud, and software privacy are a few examples that are frequently used.

Both financial and nonfinancial offences fall under this category. Although they target the virtual bodies of a person or a business house, these attacks do not target a physical body. However, only such planned acts—not unintentional ones—are classified as cybercrime. ophcrack, encase, safe back, data dumper, and Md5sum are a few of the instruments frequently used in cybercrime. Kali Linux is another.

- **Why Cyber Crimes are so dangerous...?** - Cybercrimes are challenging to pinpoint because the perpetrator may be on another continent while committing the crime. Cybercrime is incredibly simple to learn how to do, requires fewer resources, and results in greater harm than anticipated. Additionally, there are enough legal loopholes in online laws to avoid paying the proper penalties. [1] As a result, cybercrimes are significantly riskier than traditional crimes.
- **Who are Cyber Criminals…?** - Teenagers (out of curiosity, rebellion, or ignorance of the consequences), organised hacktivists (with specific goals that may be religious or political), enraged employees (seeking retribution), and professional hackers make up most cybercriminals (for corporate espionage)
- **Why are Cyber Crimes arising…?** - Cybercrimes are becoming more prevalent as technology advances. Increases in cybercrime are caused by several variables, including motivation, ignorance, opportunities, broadband, and a lacklustre response from law enforcement. It takes time to create effective regulations that are fair to all individuals, give them protection, and respect their privacy, even when laws are amended to address this rise. Although there are certain laws, the enforcement agencies have little power to carry them out. Insufficient budget, outdated technology, inadequate training, poorly defined procedures and files, poorly defined forensic evidence, an undefined dedicated team, accountability, a lack of staff, and insufficient data storage are some of the problems.

VARIOUS TYPES OF CYBER CRIMES

There are two categories for cybercrimes. The first situation involves using a computer as a target, and the second involves using a computer as a weapon. Here are some of the most prevalent crimes explained.

- SCAMS- To conduct worldwide frauds, thieves use social networking sites. [1]. The major goal of criminals is to entice individuals to click on links on web pages that are of mutual interest to most people and are popular with everyone by using various alluring images. They typically seem suspiciously like a message that you have won a free prize, such as a voucher, astrological predictions about you, or a gift card that is waiting inside, etc. The hackers ask for personal information from us, such as our bank account information, debit or credit card information, social security numbers, pins, etc., to collect that price.
- CYBER BULLIYING- Social Media and the newest technologies are being used by people of all ages and genders more frequently, which raises the possibility of undesirable behaviours like bullying. One of the most upsetting things anyone can go through is bullying, especially when they are young. Children, women, and teenagers are more likely to be bullied than adults. Bullying results in psychological anguish, which affects people's personalities. Victims may get violent or threatening tweets, texts, or blogs that provoke them or endanger their lives. Any behaviour that is damaging to a person, including identity theft, credit card fraud, bullying, stalking, and psychological manipulation, is considered a kind of cyberbullying. [2].Women, who by nature are gregarious, are the group most at risk from cybercrime after children. They soon establish virtual friendships or join online groups where they may talk about various culinary methods, issues relating to children and families, post-pregnancy advice, etc.
- STALKING - Cyberstalking is a common crime that takes place on social networking platforms and has serious repercussions. [3] Cyberstalking often comprises persistently harassing someone online with messages, written threats, and other actions that endanger their safety. Even while it may only seem like unpleasant behaviour, online stalking frequently has a valid explanation for the issue and, if not treated seriously, can even turn into in-person stalking or endangerment. Therefore, it covers threats that are made through the internet, through email, over the phone, or through text messages, whether they are made expressly or implicitly.
- IDENTITY THEFT- Identity theft, which is the practise of pretending to be someone else, is a common method of cybercrime. Nowadays, identity theft and taking control of another person's financial activity are relatively common types of cybercrime.
- DEFAMATION- Defamation is the practise of breaking into people's devices and disclosing their personal information with the intent to harm them.
- HACKING- Hacking is the act of breaking into computer systems without authorization to obtain sensitive or private information about individuals or businesses.
- MALWARE- Software that gathers data without the user's consent is referred to as malware.
- VIRUS AND WORMS- Worms make copies of themselves and spread from computer to computer, infecting it. Viruses, on the other hand, attach themselves to files and infect other programmes, infecting the entire system.
- SPAM- It involves pretending to be another user and sending emails or texts from a different source than what is shown.
- SOFTWARE PIRACY- Making unlicensed copies of software and conducting business.
- CYBER TERRORISM- A criminal offence called "cyber terrorism" uses technology to carry out violent acts against people and property. [2] It frequently serves racial, political, or ideological objectives. Along with sabotage and material damage, this kind of cybercrime can also make people fearful, anxious, and aggressive. Cyberterrorism can potentially have an impact on information availability and integrity. Using the Internet, terrorists spread propaganda, gather recruits, sway public opinion, and destroy various national infrastructure. Cyberterrorism has the potential to cause significant financial loss, property damage, and violent acts that result in deaths and fracture social and cultural cohesion.
- CYBER WARFARE- When there is a battle, cyberattacks are utilised as weapons instead of physical ones. Organizations or groups of hackers may carry it out without the consent of the government, and it may cause political unrest between nations. [2] At the moment, cyberattacks and cyberwarfare are the most common sorts of conflict. In the past 20 years, there have been numerous cyberwars.
- CYBER ESPIONAGE- Espionage is the term used to describe any operation involving spies and the theft of sensitive information for the benefit of rival businesses or other governments. In cyber espionage, missions are carried out utilising computers. [2].
- CHILD PORNOGRAPHY- Child pornography is characterised by depictions of children in unsuitable clothing, with little or no clothing on, and in inappropriate situations, particularly in sexual poses.Child pornography is typically distributed for either financial gain or charitable purposes. Several websites sell child pornography for a profit. P2P networks can be used to transmit and disseminate content containing child porn for charitable purposes. [2]
- PHISHING- One of the most widespread attacks is phishing since it has a direct connection to the end user. In these circumstances, the attacker tries to convince the end user to give sensitive information. Phishing is a method that combines social engineering and spoofing. An email is sent to the recipient inquiring about vital information, warning them of an upcoming attack, and persuading them to install malicious security software. Additionally, it's possible that it links to a phoney website. Never clicking a link in an email, you aren't sure about is one of the simplest security precautions.
- DOS - A DoS attack happens when a computer resource is overloaded with requests that it cannot handle. This will always cause the system to crash, preventing authorised users from using the requested service.
- FUTURISTICS IN CYBER ATTACK - Future-oriented cyber-attacks can target Wi-Fi, medical equipment, robotics, and drones, among other contemporary and modern technology and devices. Because of this new technology, cyberattacks are incredibly vulnerable. Wi-Fi technology is used by both consumers and enterprises, endangering their security.
- CARDING - Carding occurs when a criminal withdraws money from a victim's account using a fake ATM card.

- DATA BREACHES - As a result of today's digitalization, people are saving an increasing amount of personal data either on their own computers (putting the data at risk from viruses, trojans, and other malware) or through social media platforms. Although many businesses save customer information, it has been found that only a small portion really do so; the majority instead collect and keep much more information than is necessary. This makes data breaches, or the theft of personal information, more likely. How a data breach will affect the people whose personal information has been compromised is impossible to predict. What happens to the private data that is stolen in numerous data breaches is unknown.
- MOBILE CRIMES- Cell phones, PCs, GPS, Bluetooth, and other mobile technology are mostly used to enhance services and make life more convenient. Since their release, cell phones have developed into devices that are comparable to laptops and desktop computers. There is therefore no genuine distinction between mobile crimes and cybercrime, unless on a very tiny scale. Some of the most frequent mobile crimes include cyberbullying, sexting, privacy invasion, phone phishing, email harassment, cyber stalking, distribution of pornographic material, defamation, hacking, cracking, email spoofing, carding, cheating and fraud, child pornography, assault by threat, and so forth.Two additional prevalent cybercrimes are marketing schemes for illegal goods and financial crimes. Email harassment, child pornography, theft of telecommunications services, political crime, money laundering, tax evasion, electronic terrorism, theft of Internet time, hate/communal crimes, altering websites, etc. [1]

DATA MINING

Data mining is a method for taking large amounts of unstructured data and extracting information that is useful. To analyse patterns in massive amounts of data, data mining software is utilised. Data analytics and data science both depend on data mining, which is an essential part of both fields. Although the terms "data mining" and "KDD" are frequently used interchangeably, they refer to two distinct techniques. Machine learning and artificial intelligence are two concepts that are frequently used interchangeably. Data mining is used by every sector of industry that produces data and aims to use it.

NEED OF DATA MINING

Due to the enormous amount of data being gathered globally, worries about crime prevention are growing and getting more complex. As a result of the insights included in the data being collected, which can help in the battle against cybercrime. Because cybercrime rates were low in the past, most of the data on crime came from police reports, press accounts, or other items that were all manually written or printed[1]. Data started to flow in as the crime rate rose, and manually archiving such a large amount of data became a tiresome and time-consuming operation. A modern analysis method saw a surge in demand as a result, and data mining entered the cyber security industry.These tools were found to have shortcomings, so a range of other tools were developed using data mining techniques. Data preparation Setting the format of the data is the first stage in cyber detection using a data mining approach[1]. The analysis of the data, the second step in the data mining process, is the most crucial since it gathers useful information from various sources. We use this data to look for patterns that can help us identify cybercrime. We'll use the data mining methods described below to locate such a pattern.

DATA MINING TECHNIQUES

a. Association Rule Mining - The links between each of the data elements are found using this method. It is a method of unsupervised learning. It lists all the regulations of the Association that satisfy standards, such as minimal confidence and assistance. To identify regularities, employ these principles. For instance, according to the rule (phishing, cyber stalking) (cybercrime), a cybercriminal who simultaneously participates in phishing and cyber stalking will conduct credit card fraud[1]. As a result, these patterns can help us apply data mining to the topic of cyber security more successfully.

b. Cluster Analysis - The term "cluster" describes how data are grouped or labelled. These classes have comparable information. The characteristics of data with distinct class designations therefore vary from one another. After it has been categorised or labelled using different analytical techniques, the information is extracted. The technical term for this process is "Cluster Analysis."

   K – Means- A popular clustering algorithm called K Means serves as a form of centroid model. It can be used to identify similar collections of data elements. The Euclidean distance metric is used to determine how similar' data items in 'k' clusters are to one another. This is one of the most used clustering techniques.

c. Classification- Data is categorised into these pre-established groups through this technique. Depending on an object's properties, it gives it a class. An algorithm that implements classification is called a classifier. The two main steps in creating a classifier are pre-processing the data and choosing the most suitable classification method[1]. Some classification methods include decision trees, Nave Bayes classifiers, and K-nearest Neighbours.

   Naïve Bayes Classification- It is a type of classification method built on the Bayesian theory of probabilities that uses conditional probability to forecast the likelihood of a pattern in the class. This method is simple to implement and gives a consistent categorization impact.

   K-Nearest Neighbour- The testing data is then given to the class that has the most common neighbours among its k closest neighbours after calculating the distance between new instances and all existing examples. It has a significant processing cost but can reduce errors and the repercussions of improper categorisation.

Decision Tree- Divide and conquer is used in the Decision Tree, a supervised learning technique for categorising data based on attribute values. The findings are shown as a tree, where each leaf denotes a decision, and each intermediate node denotes a test. Despite being straightforward, this method is worthless due to the unsorted tree structure.

LIMITATIONS OF DATA MINING TECHNIQUE

Data mining is one of the most efficient ways to fight cybercrime, although it has a variety of difficulties, including the following:
1. There is a dearth of qualified, experienced, and capable people to carry out the countermeasures.
2. The vast volume of audit data that is used to construct the profile rule sets is one of the biggest challenges for this technique. This approach takes time since a different detection model is needed for each resource in the target system.
3. Law enforcement and security personnel lack the tools necessary to combat high-tech crimes.
4. The rule sets of these detection systems may or may not remain constant throughout time, suggesting that learning is a continuous process.
5. Real-time detection must be feasible because data mining is an expensive activity in terms of both time and storage.

CONCLUSION

Several different forms of cybercrimes and numerous data mining techniques used to detect them have been explored in the thorough review in this paper. Additionally, these strategies have limitations. So, in my opinion, these data mining technologies ought to be more accessible and less expensive, and more people ought to be taught to utilise them. Such techniques are greatly needed as cybercrime is growing quickly, and more research should be done in this area.

REFRENCES

[1] Koppisetty, Harshitha, Kanak Potdar, and Shubhangi Jain. "Cyber-crime, Forensics and use of Data Mining in Cyber Space: A Survey." 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT). IEEE, 2019.
[2]Al-Khater, Wadha Abdullah, et al. "Comprehensive review of cybercrime detection techniques." IEEE Access 8 (2020): 137293-137311.
[3]Ganesan, M., and P. Mayilvahanan. "Cyber Crime Analysis in Social Media Using Data Mining Technique." International journal of pure and applied mathematics 116.22 (2017): 413-424.
[4] Prabakaran, S., and Shilpa Mitra. "Survey of analysis of crime detection techniques using data mining and machine learning." Journal of Physics: Conference Series. Vol. 1000. No. 1. IOP Publishing, 2018.