IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008166 |

Emerging Cyber-crimes and Challenges for its Security

Rounak Jha[1], Tanvi Pinjari[2]

UG Student, Department of Information Technology, B.K. Birla College of Arts, Science and Commerce (Autonomous), Kalyan, Maharashtra, India[1]

UG Student, Department of Information Technology, B.K. Birla College of Arts, Science and Commerce (Autonomous), Kalyan, Maharashtra, India[2]

ABSTRACT*:* Every single dimensions of human life are facilitated by a digital age now a days which hasnow covered the whole world. Universally, there has been a massive emergence in the use of computers, electronic gadget and IOT devices. Thus, the rapid growth of the Internet connections has gave a marginal increase to a massive growth of cyber-attacks which has some unmanageable consequences. Cyber Security plays an important role in the field of information technology and Computer Science because it protects all categories of data from theft and damage. Security of the information have become one of the biggest challenges now. Not only affecting national security, but also these attacks have reached at a very immense level that could harm individuals. The paper discusses the offenders of a cyber-attack and the techniques which are continuously used to achieve their goal. The types of cyber-crime, the data mining and other techniques used in security phase will be explained in detail. Detecting the digital data source, authenticating the scene will be studied in detail.

KEYWORDS: Cyber-crime, cyber frauds, security, detection techniques, Data mining.

I. INTRODUCTION

In this digital based era, revolution in around all small and large businesses, corporates, governments and organizations are dependent on computerized systems attaching with the IT sector to manage their day-to-day activities and thus making cybersecurity an important asset to keep their data safe from various online attacks or any unauthorized access that is from various different kinds of cyber-attacks The first thing comes in our mind while thinking cyber security is 'cyber-crimes" which are increasing day by day. Each day, different types of crime are invented. According to observation, crime which is most open to change and development are cyber-crimes.In this world of interconnected networks, it becomes difficult to capture these cyber criminals than in the physical world which is the possible reason in increase in the cases cyber-crimes. These kind of developments enables serious challenges for law and criminal justice, as there are struggles to adapt these crimes does not takes place in the terrestrial world but in the virtual environment of cyber space, which expands the globalization through the Internet's instantaneous communication, and afford these criminals new opportunity for anonymity, deception and disguise.

In the year of lockdowns and restrictions, cybercrimes have become more stubborn. A huge increase in the margin has observed in the cases of man-in-middle (MIM) attacks, phishing, hacking and email spoofing. In India, ransomware attack is the tremendously happening attack in cyber-crime taking 40 per cent of all attacks. Followed by manufacturing and professional services, financerelated crimes like identity theft, online shopping fraud was the most targeted sector taking 60 per cent of other attacks. Gaining correct and real statistics on cybercrimes is one of the most challenging issue because of the behaviour in which the crimes were committed, the seriousness in offences, and the most common issue is unreported incidents from the people due to the lack of knowledge about these types of crimes.

II. RELATED WORK

The main reason behind this huge and rapid growth in cyber-crimes is the usage of inadequate and unwanted software, security tools that are expired, programming and installation errors, availability of various online hacking tools, lack of awareness in people and higher rated financial returns, etc. In our day-to-day life, we usually do different economic

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008166 |

activities such as mobile banking, uses social media, online Shopping etc and moreover our national security are highly depended upon stability, safety in our cyberspace. Security is not just an easily available product, but is actually a sequential layer of processes. An overall state of computer security is a basic conceptual idea which can be achieved by the use of three processes: threat prevention, detection, and response. These processes are dependent on different policies and system components, which includes:

• Cryptography techniques that can protect systems files and data, respectively with user account accesses and controls.

•Till now the most common preventive measure systems for a network security perspective are firewalls (if properly configured) they shield and protect the unwanted or unauthorised access to internal network services, and block certain attacks by packet filtering.

• Intrusion Detection Systems (IDSs) are designed and inserted to detect network related attacks which are in progress and gives assistance in post attack forensics, while for individual systems audit trails and saved logs are served as a similar function.

• "Response" can be said as a necessarily defined security requirements assessed for a individual system and covers the range from just a simple upgrade of protections to the notification of legal authorities and the protection from other future counter-attacks.

The task of protecting cyber-space is one of the most difficult and challenging task as advanced threats in this digital era plays a very active role. Thus, it has become necessary to get the concepts of security in IT, their defence mechanisms, different techniques and trending topics in the area of information, network and individual systems security.

III. METHODOLOGY

The study is commenced to see the progressive review of cyber-crime's current status, through the review literatures, including analysis of different research papers. The main aim was to gain an overall overview of the cyber-attacks from all over the cyber space, and to understand the cyber-crimes potential impact upon businesses or individuals, as well as the preventive measures that are taken to address such risks. The research was based on attacks identified and witnessed. As in big number of cyber-attacks happens on a daily basis all around the world and usually limited amount of information is displayed by the companies when they become the victim of such cyber-crimes and in fact some of the attacks are even so hard that are not be able to trace. However, the study was based on the information by fetching data regarding the attacks that are detected and traced throughout the decade, collected from reports and surveys issued by expert market players in security consulting. The already existed methods are analysed by many review and survey searches, This study gives a brief review of cybercrime's security and its challenges which can be based on the use of different detection methods.

IV. EXPERIMENTAL RESULTS

I. Challenges:

This COVID-19 pandemic has enabled the situation in increased rate of cyber-attack invoked at a wider range. This has led to change in working practises and socialization which means people are now spending increased periods of time online which can result in more threats:

- Malware and Denial of Service (DoS) attacks are forms of cyber-crime that are often carried out by more technical and skilled attackers as this involves hacking which means compromising and changing the confidentiality or integrity of a system and this requires an effective and reasonable amount of skill. The technique's aim is exploiting system vulnerabilities to break into the systems. Malware is a malicious software and can be used for interrupting the services, data extraction and a range of many other kinds of attacks. Most common types of malware that can be found are: viruses, worms, trojans, spyware, ransomware, adware and scareware. Today, ransomware has become one of the most common type of malware which combines malware with extortion attempts.
- DoS attack are the types of attacks which target the availability of the system and work by continuously flooding the services and spamming with illegitimate requests thus making the system inoperable.
- Phishing is a technique which aims to steal private information from users disguising as a trustful source (e.g. website); Usually, many of the cyber-attacks begin with a phishing which directs victims to download a type

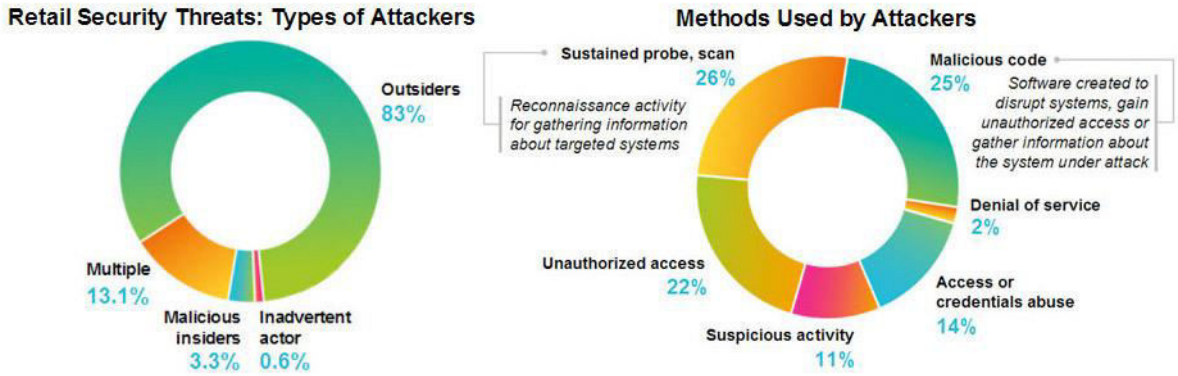
| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008166 |

of file or access a URL through spamming their emails. The file or the URL act as the medium of malware which, when installed, acts as the vehicle for financial fraud.

- Man in the middle is a type of attack which occurs when the attacker interferes between the two communication ends, thus every message sent from the sender to receiver reaches to the attacker first before reaching to its destination. This risks further get more complicated as the attack get comprised of unauthorized access to subtle information or there are possibilities that alteration of the information/message before it reaches to the destination by the attacker.
- Brute force attack is a attack which comprises of repeated attempts to gain access to protected information that are passwords or encryption until the correct word is found, and thus the information can be reached.
- Social engineering is the general term that uses the psychological manipulation technique used to gain unauthorized access to information through human interaction.



II. Detection technique used: Data Mining

Data mining is a flow of processes with the discovery of unexpected patterns and new rules that are hidden in large databases. It is a multidisciplined method which has the origin on the basis of sciences such as applied statistics, artificial intelligence, pattern recognition, database, theory of algorithms and others. The most common techniques used in data mining are classification, clustering, association, forecasting and visualization. In this paper the Data Mining techniques used in cyber-crime are in two directions:

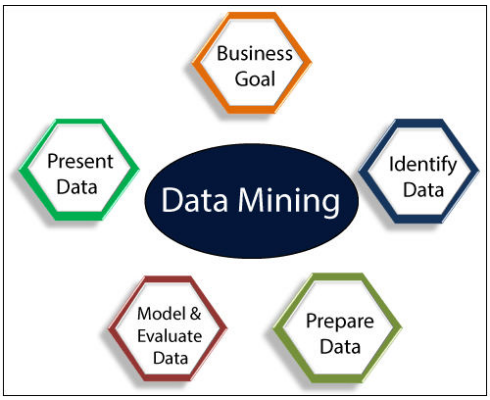
1. Classification: The classification is the most simple and common task in data mining. The solution of the problem is the signs which are characterized groups of objects (classes) that are detected when an unusual pattern is seen. The main aim of classification is to predict the targeted class for each case in the database. Thus, this model can be used for identifying the usage of credit card as valid or scam by observing the relationship among the attributes such as employment history, years of residence, number of investments and their type and so on.

2. Clustering: Clustering is a logical extension of classification. The task is more complicated than the classification. The objects are parted into groups. In contrast to the tasks of classification, clustering allows to analyse various types of data such as number of intervals and frequency. This technique recognizes the occurrences of relatable behaviour of cyber-crimes cases that had taken place in an area. Once the same patterns are determined they are formed into consequent clusters, and cluster are reviewed to outline a particular attribute description.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008166 |



- Applications:

I. Banking Sector - Supervision of frauds is an intensive task. Data mining technique provides assistance to observe patterns and dealings that leads to scam. One of the important aspect in scam detection is to observe the regular transactions performed by the account owners. For such purpose we can utilize this technique which ensures and separates the transactions that do not recognize in to a precise group or not regular transactions.

II. E- Commerce - Due to the development of E-Commerce technology the usage of credit cards had grown up rapidly. At present, the credit card transactions and online payment has become one of the vital form of payments. With the increase in this type of transactions, the credit card frauds had also become a common cyber threat as well. Thus, to balance the consistency of the payment schemes, it is essential to build an advanced and enhanced fraud detection system in business organizations and other corporates. As in virtual E-Bank, many transactions endure digitally, so a fraud detection system should be utilized to distinguish between valid, safe, suspicious frauds and an illegal transaction.

III. Genetic Algorithm for the detection of Credit Card scam - A Genetic algorithm generally aims to attend the enhanced patterns to correctly eradicate the fraud and also to build a secured and well organized e-payment scheme to identify whether the happened transaction is fake or not. On the basis of customer deeds, this algorithm has to reduce the scams and the number of false alarm while undergoing credit card transactions. To identify and generate fraud transactions attributes which are required are current bank balance, card custom frequency count, Credit over draft, Credit and location etc. The best result can be seen when there is a repeating pre-specified number of iterations. The goal is to attain the advanced and best possible result. In the E-Banks when a transaction is performed, the algorithm predicts the probability of any fraud transaction and implements a sequence of anti-fraud policies and notifies the bank from huge losses and also shrinks cyber threats.

V. CONCLUSION

In this paper we conceptualize cybercrime and it its various types. Further we also discussed about some methods related to data mining that are used for cybercrime all over the world and concluded with techniques that can be used to detect and recover from cyberattacks. Perceiving and taking cyber-crimes for granted due to some preventive measure is tricky, because due to different technologies cyber criminals are that kind of skilled that they can innovate latest proposals all the time, and those schemes develop more and more sophisticated inventions for easy detection. In short, understanding the relation between the analysis and the characteristics of cyber-crime type can provide investigators more effective utilization and those techniques to recognize trends and patterns, tackle problem areas and even predict forthcoming cyber-crimes. There is actually a general lack of understanding attacks (types, characteristics, impact) thus the world is facing a crisis in assurance of proper security of information. The first thing to do is a world-wide awareness in order to handle the problem of increasing cyber-crime. And another main problem is probably could be the common legal perspective that is even though each state or region has its own implemented set of laws and regulation, still the internet is an international tool for attackers thus the only way to defeat the cyber-crime is for authorities to think and act at a global level. It is also the responsibility of each individual, company or authority to assure a level of security, in order to support the information security and data privacy.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008166 |

VI. ACKNOWLEDGEMENT

We are thankful to Prof. Swapna Augustine Nikale, Department of Information Technology, B.K. Birla College (Autonomous), Kalyan for her guidance throughout our research work.

REFERENCES

[1] Bendovschi, A. (2015b). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 28, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

[2] Sahu, N., &Darokar, S. (2017). DATA MINING TECHNIQUES TO CLUSTERING CYBER CRIME DATA. INTERNATIONAL EDUCATION AND RESEARCH JOURNAL, 3(7). http://ierj.in/journal/index.php/ierj/article/view/1288.

[3] Okutan, A., &ÇEbi, Y. (2019). A Framework for Cyber Crime Investigation. Procedia Computer Science, 158, 287–294. https://doi.org/10.1016/j.procs.2019.09.054

[4] Jang-Jaccard, J., & Nepal, S. (2014b). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

[5] REDDY, G. N., & REDDY, G. U. (2014). A Study of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. A Study of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. Published. https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

[6] Alghamdi, M. I. (2020). A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide. INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 06 (June 2020), 09(06). https://www.ijert.org/a-descriptive-study-on-the-impact-of-cybercrime-and-possible-measures-to-curtail-its-spread-worldwide

[7] Wadhwa, A., & Arora, N. (2017). A Review on Cyber Crime: Major Threats and Solutions. International Journal of Advanced Research in Computer Science, 8(5), 2218–2221. https://www.researchgate.net/publication/322384427_A_Review_on_Cyber_Crime-_Major_Threats_and_Solutions

[8] Katzan, H. (2016b). Contemporary Issues in Cybersecurity. Journal of Cybersecurity Research (JCR), 1(1), 1–6. https://doi.org/10.19030/jcr.v1i1.9745

[9] Alshahrani, M., & Ramadan, A. (2021). CYBER ATTACKS - TRENDS,PATTERNS, AND SECURITY COUNTERMEASURES. PAIDEUMA JOURNAL, XIV(7), 22–39. https://paideumajournal.com/gallery/2-july2021.pdf

[10] Back, S., &LaPrade, J. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. International Journal of Cybersecurity Intelligence & Cybercrime, 2(2), 1-4. https://www.doi.org/10.52306/02020119KDHZ8339

[11] Lekha, K. C., &Prakasam, S. (2018). IMPLEMENTATION OF DATA MINING TECHNIQUES FOR CYBERCRIME DETECTION. International Journal of Engineering, Science and Mathematics, 7(4), 607–613. https://www.indianjournals.com/ijor.aspx?target=ijor:ijesm&volume=7&issue=4&article=060

[12] Mohsin, K. (2021). The Internet and its Opportunities for Cybercrime – Interpersonal Cybercrime. SSRN Electronic Journal. Published. https://doi.org/10.2139/ssrn.3815973

[13] Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017b). The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services. International Journal of E-Education, e-Business, e-Management and e-Learning, 7(1), 70–78. https://doi.org/10.17706/ijeeee.2017.7.1.70-78

[14] Kirichenko, L., Radivilova, T., & Anders, C. (2017). Detecting cyber threats through social network analysis: short survey. SocioEconomic Challenges, 1, 20–34. https://doi.org/10.21272/sec.2017.1-03

[15] https://securityintelligence.com/wp-content/uploads/2014/07/Retail-cyber-security-threats-types-of-attackers-methods-used-by-attackers.jpg

[16] https://static.javatpoint.com/tutorial/data-mining/images/data-mining-introduction.png.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details