2022 International Conference on Smart and Sustainable Technologies in Energy and Power Sectors (SSTEPS) | 978-1-6654-6414-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/SSTEPS57475.2022.00039

Survey on Cyber Crime Problems and Prevention

C Balarengadurai
Department of Computer Science Engineering
Vidyavardhaka College of Engineering
Karnataka, India
balarengadurai@vvce.ac.in

Divya C D
Department of Computer Science Engineering
Vidyavardhaka College of Engineering
Karnataka, India
divyacd@vvce.ac.in

Harshitha C
Department of Computer Science Engineering
Vidyavardhaka College of Engineering
Karnataka, India
harshitha.c@vvce.ac.in

Abstract— **Attackers' main objective is to commit the most modern and evolving forms of crime. As new researchers concentrate their studies primarily on cyber security, the field of online crime prevention systems has been evolving. The topic of cybercrime is one that is getting more and more attention every day. It is challenging to take on. Online crime prevention solutions based on digital forensics provide the public with a mechanism to lodge complaints and get services more quickly and simply while storing criminal information in a single database. The customer or person can submit the FIR online by entering information about the case type, incident specifics, and other crucial factors. Even with older records, all complaint information can be viewed and added. Anomaly detection systems, honeypots, tripwires, configuration checking tools, and working system instructions are some of the techniques encompassed using a variety of techniques like k-means, k-nearest neighbors, ML, NPL, and Deep Learning with neural networks these algorithms useful in crime detection and prevention purpose using a variety of clustering algorithms, naive Bayes, and linear algorithm helps by systematic approach to identifying and evaluating patterns examining online criminal activity, it is possible to recognize and evaluate criminal patterns and trends.**

Keywords— Attackers, Cybercrime, Online problems, Prevention.

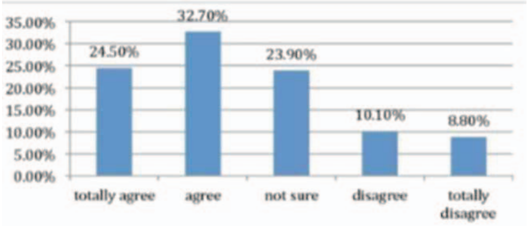
I. Introduction

The online crime prevention system has been improved in order to properly assume the responsibility of reporting crime in a way that would benefit the public. People from all around the world can interact with online district police stations, share information, and connect with one another via online or offline methods thanks to the distributive aspect of the online solution [1]. The primary cause of the daily increase in cybercrime and cyberattacks needs to be loo ked at. Crime is a behavioral issue that results from a combination of social, economic, and environmental factors. In the modern world, the need for money for one's own needs or on demand from anyone—insiders or strangers—society's peace has become more prominent and diverse Both urban and rural areas face difficulties from cyberattacks like hacking and phishing, and new issues including, human trafficking, handling of online transactions, and management of fraud and scams in relation to public policy and safety services are arising.[2- 6] Digital forensics, also referred to as "digital forensic science" is a branch of cybersecurity that focuses on recovering and analyzing data from digital devices and cybercrimes. People can locate safe routes to their destinations and recognize high-crime regions, can complaint online police station to get updates online reporting system.

II. Impacts of Cyber Crime on Social Media

The use of a computer as a tool for criminal activity, suchas fraud, the trafficking of child pornography and stolen goods, identity theft, and privacy violations, is known as Cybercrime known as computer crime. It is impossible to picture a world without the internet and social media since they have become such an integral part of our daily lives. Our lives have grown reliant on online media as source of all information due to the development of technology, the rapid spread of mobile information, and the use of social media, which offers platforms for simple connection with people all over the world. Even if technology offers numerousbenefits, it also poses risks to people. Social media, in particular, has turned into a sanctuary for criminals as a resultof the surge of crimes committed in the online space [7] Theanonymity of social media and the development of a virtual world where users may communicate, swap photos, make friends, play games, fall in love, engage in conflict, and other activities without ever having to physically interact are the main drivers of the platform's success victim's personal information, including name, address, location, and photos. Cyber violence has increased among people of all ages, worldwide scale due to the factors of anonymity and fakeness in social media as well as jurisdictional difficulties. Fig 1: The survey related on most crimes are online than offline. Social media poses risks to an individual's security, privacy, and even dignity [8].

A. *Types of Cyber Attacks*



.

Fig 1: The survey related on most crimes are online than offline.

Techno-crime and techno-vandalism are types of cyber-attacks that damage or destruction takes place in digital form, such as copying files and making victim's private photos or videos public. Online crimes are classified on the basis of crime and can happen against an individual, organization,property, or the society [9].

There are three types of cybercriminals.

Type 1- Criminals seeking attention (IT professionals, terrorist groups, and perverts).

Type 2- Criminals not seeking attention (psychological perverts).

Type 3- Insider Cybercriminals (former employees, Revenge).

Some of the common attacks are listed below:

1). *Phishing Attack*: Phishing is type of Social

978-1-6654-6414-7/22/$31.00 ©2022 IEEE
DOI 10.1109/SSTEPS57475.2022.00039

engineering attacks, the act of attackers sending nefarious emails with the intention of getting receivers to fall for a scam. Spear Phishing Vishing, Smishing, Mishing are other type of cyberattack where malicious actors send messages while impersonating a reputable person or Institution.

*2). Malware Attack***:** Malware attacks are frequent cyberattacks in which the victim's machine is used to carry out unwanted acts, Malware comes in a variety of forms, including Trojan horses, spyware, ransomware, viruses, adware, and worms. Fig 2: Crime Rate of countries in the world. Key loggers, worms, ransomware, rootkits, spyware, and adware and leads to computer sabotage.

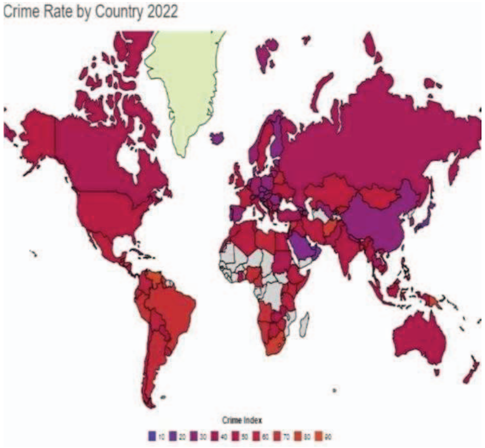


Fig 2: Crime Rate of Countries in the world

3). Password Attack: Password assaults are commonly used to avoid or take advantage of user account authentication. Password hackers one of the most common perseverance security vulnerabilities, caused more than 81%of data breaches in 2022. Brute-force password assaults**.** Fig.3. Pie Chart represents the maximum cybercrime countries in the world. Dictionary password attacks, password spraying attacks, and keylogging are some examples of password attacks.

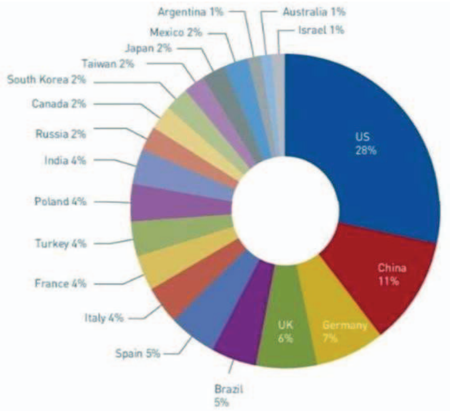


Fig 3: Pie Chart represents the maximum cybercrime countries in the world

4). Man-in-the-Middle Attack: MITM attacks include IP and DNS spoofing, SSL hijacking, browser cookie theft, and Wi-Fi eavesdropping. They involve a malicious 3 player interjecting himself into a conversation between two parties, and gaining access to the information that the two parties were trying to share. MITM attack types are IP and DNS spoofing, SSL hijacking, Browser cookies theft, Wi-Fi eavesdropping.

5). Injection of SQL Attack: Attackers can access a web application database without permission by using the SQL injection technique to insert a string of malicious code into a database query. SQL injection (SQLite) allows for the execution of malicious, Fig. 4. Yearly growth of Cybercrime Costs and Losses in India, SQL instructions and the access to resources.

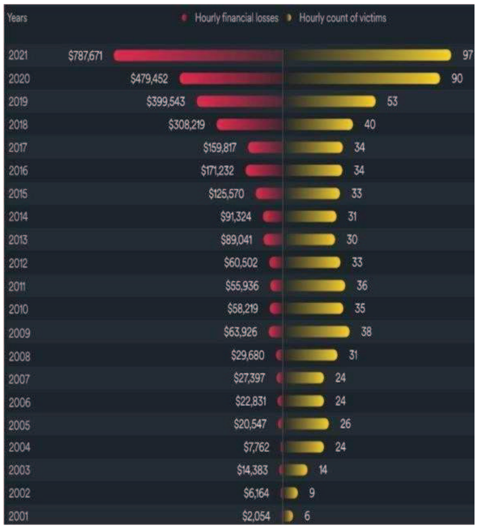


Fig 4: Yearly Growth of Cybercrime financial cost and Losses

6). Zero-Day Exploit: A hacker's success in taking advantage of the flaw before software makers can patch it is referred to as a "zero day attack." Zero vulnerabilities can appear as any form of more widespread software defect. Zero-day vulnerability is the target of a zero-day exploit.

7). Watering Hole Attack: To conduct a watering hole assault, one must locate a website that is often visited by people working for the targeted company or perhaps an entire industry, Fig. 5. Percentage of internet users in selected countries experienced cybercrime**,** such as the military, government, or healthcare.

8). Crypto jacking: The phrase "Crypto jacking" has a lot to do with cryptocurrencies. In order to mine bitcoins, hackers must get access to another person's computer. Access is made possible by infecting a website or duping a victim into clicking on a dangerous link.

9). DDOS Attack: The term "Distributed Denial-of-Service (DDoS) Attack" refers to a cybercrime in which an attacker overwhelms a server with internet traffic to prohibit users from accessing linked online services and websites [1-4].

10). Cyber Stalking/ harassment: The common persistent use of electronic means of communication for the purpose of intimidating or harassing someone, such as sending threatening emails.

11). Salami Attack and Data diddling attack: The assault known as **"salami"** is a sort of cybercrime from 1990 that is commonly employed by attackers to perpetrate money fraud and scams. This attack happens when a number of smaller attacks combine to create a stronger strike Fig 6: High Crime Rate of States**.** Data diddling is a form of attack consists of modifying the raw data immediately before it is processed by a computer.

B. Cyber Attacks Representation and Figures

The average weekly attacks per organization worldwide reached a peak of 1.2K attacks. The number of attacks per company increased from 106 to 270 year on year. Cyberattacks have significantly risen in the modern world; utilizing histograms, a graphical representation, we can more readily identify the assault in country and state, how the attackers or hackers trick the user or victim.[15]. Security threats surged 35% between 2020 and 2022, according to Accenture's State of Cybersecurity Resilience 2021 study. According to Check Point Research (CPR), the second quarter of 2022 saw an all-time high for worldwide cyberattacks, which rose by 32% compared to Q2 2021[10-12]. The peak number of assaults per company each week was 1.2K. Attacks per firm jumped from 206 to 270 each year.

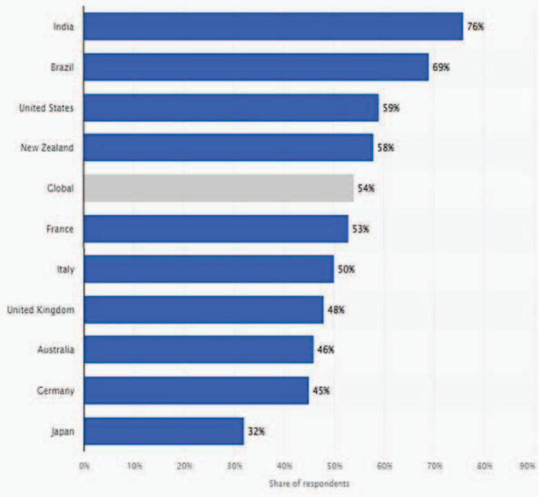


Fig. 5. Percentage of internet users in selected countries experienced cybercrime.

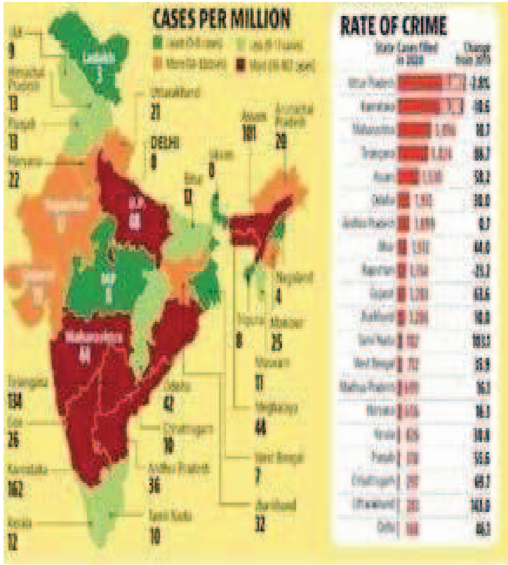


Fig 6: High Crime Rate of States in India

III. Literature Survey

Serial No	Tittle	Authors	Methodology /Algorithm	Uses	Year
1.	A study of data mining-based internet crime prediction.	Cocea Michaela	CRISPDM (Cross IndustryStandard Processfor Data Mining)	It contains explanations of the usual project stages, a list of the activities associated with each phase, and an explanation	2017
2.	Crime Rate Prediction Using Machine Learningand Data Mining	Sakib Mahmud, Musfika Nuha	Z-CrimeTools andAdvanced ID3algorithm	Based on a dataset of simulated criminal behavior the Id3 algorithm is used to classifycriminal behavior.	2015
3.	Technological Innovation in Crime prevention andpolicing	James Byrne1 and Gary Marx	Python matplotliband KNN algorithm	A methodical technique to discovering and analyzing patterns and trends in crime is called "crime analysis and prevention."	2016
4.	Analysis of criminal careers using data mining techniques	Jeroen De Bruin	Clustering method and visualization	Market research, pattern identification, data analysis, and image processing all involve clustering analysis.	2018
5.	Online Crime Reporting and Management System using DataMining	Anabasis. A	KNN Algorithm, K-Means Algorithm.	Clustering analysis is used in image processing, data analysis, market research, and pattern recognition.	2013
6.	Cybercrime Prevention onSocial Media	Pandya Ogale	Convolutional neural network	Classification of image segmentation, and autocorrelation of data for images.	2014
7.	The Perpetration and Prevention ofCybercrime	Murphy Smith	NLP Algorithm	In a broad sense, text analysis helps with everything from homicide investigations to giving information for policy research.	2016
8.	Online newspapers to analyse and map crime	D.vijaya rohini	*Decision trees* \ k-means algorithm	used in criminal investigation, law enforcement, intelligence has the potential to solve this issue.	2015

9.	An Interactive World Crime News Retrieval System	Dr.P.ISAKKI.	Tripwires method Data mining ,linear regression , naïve Bayes	Using naive Bayes, Tripwire integrates expert analysis and reports with pertinent documents, photos, and videos information regarding the cause, time, and setting of crime.	2017
10.	SITUATIONAL CRIME PREVENTION (SCP) TECHNIQUES	Sridhar Shinde	KDD methodology /Semma process	the method of carrying out a data mining project, an iterative, multi-stage procedure.	2019
11.	Online crime prevention and detection analysis	Pinkie Babar	Honey pots/Configuration checking tools, KNN algorithm	The Electronic crime detection system used to find in secured systems and store the original information	2022
12.	Patterns of online recurrent victimisation and implications for crime prevention	Sara Giro Correia	Demonstrates the extent to which deep learning limits the use of RV analysis.	Intelligence analysis and law enforcement use carries the potential to solve such an issue.	2021
13.	Implementation of Crime Prevention System Using Public Big Data	InBaek, Se, Kang, Byeong Ki	Crime prevention system is expected to provide reliable crime risk by K-Mean's algorithm and gather information	Crime prevention aims to reduce crime, boost security, but also to stop the harm that can result from it.	2016
14	Signal and image processing for crime control and crime Prevention	S. Hackwood	Focused PRISMA method, paper clarifies terminologies, SCP for responding to cybercrimes	Data helps in getting the district police stations to share information and get in contact with one another.	2018
15	Using CCTV Cameras CCTV Cameras for Traffic Surveillance and Alternative Route	C.Heemen G Hoo	The algorithm has been simulated in SUMO, with successful outcomes.	Aiming to enhance the efficiency of The transportation system has been made possible by advances in technology, tighter budgetary Restrictions	2015
16	Crime Data Mining, Threat Analysis and Prediction	Alireza Daneshkha, Chatrabgon	KDD methodology	Data mining tools are specialized tools needed to analyze this massive quantity of data and make deductions and conclusions.	2015
17	A Strong Data-Obfuscation Approach for Clustered Data Privacy Preservation	Rupa Param Eswaran and Douglas M. Bough	The penetration methodology is used	The preservation of the natural grouping of the source data serves as a benchmark for usability.	2018
18	Mental influenced crime offence and investigation prevention	Yun-ShengYen; Annie Chang	A firewall and intrusion detection software	Multimedia forensics deals with the prevention and detection of crime by extracting and examining fingerprints on the digital evidences	2019
19	A Study on Digital Forensics Standard Procedures of SQLfor WirelessCybercrime	A Hutchings, RG Smith, L James	An open-source programme called SQLmap is used in penetration testing to find and take advantage of SQL injection problems.	Investigation of "people" and identification of "things" are the primary goals of a criminal investigation.	2021
20	Image processing-based big data analytics for crime prevention and control	DO Anderez, E Kanjo, A Anwar, S Johnson	K-nearest neighbours technique used using network converging	This project was built on a cloud computing model to better manage criminal behavior.	2018

IV. Drawback In Existing System

- Lack of information on a secured site, The URL and website cannot be changed since the information obtained is different from the user who sends different messages to one another at the same time [14].
- Pop-up messages are not more secure, and vulnerabilities grow as a result of spoofing attacks, which make it difficult to recover a system when an unfamiliar user sends
- It only supports small and medium-sized data sets because the majority of data is saved in list format, and huge data sets require big data analysis, which isa bigger issue and results in less accurate data.
- In the current system, they are using a traditional machine learning algorithm like logistic regression, which will not allow users to ignore or remove their crime reports because there are old records present and the large amounts of data are difficult to manage because, in a DDoS attack, the hacker sends a flood of calls or messages to make it difficult for the user to identify and secure the system [15].
- System scenario filings the process of filing a FIR or a complaint is difficult and time-consuming. More automated protection is necessary since large amounts of data can be lost by using just one system or electronic device. Since neither side of the users is aware of the type of man-in-the- middle attack, the data can be traced by the middle person [18].
- Data breaches are on the rise, which is a major issue in phishing attacks where a victim is contacted by phone, email, or text from an unknown number. The victim may find it difficult to pick up the phone or text and may question

whether the call is legitimate before disclosing any personal information.

V. Few Prevention For Cyber Crime

- More models must be developed to anticipate crime rates and crime hotspots; in this case, the technique will concentrate on the crime-prone areas and identify the common suspects by assisting in the deployment of police to the crime scenes.
- Passwords, authentication, and verification must be strengthened with the addition of biometrics, which will make them harder to discover, in the future system. Unique IP and Mac addresses can be given more importance to search in details [19].
- In order to analyses images and videos, a significant quantity of CNN algorithms and data mining techniques must be used. The Tripwire setups that need to be put up for checking tools that need to be installed to obtain adequate verification Google API so that users may examine hot zones.
- By adding message or authentication verification to Gmail, a direct alert message to the cyber station can be issued whenever an unauthorized individual tries to message or send an email.
- Creating closed networks, powerful firewalls, spam filters, monitoring controllers, closed alert systems, and anti- malware software to prevent network trafficking and increase security [20].
- When a message or video that can be misused is sent on social media, the message or video is immediately blocked and reported to the cyber police.

VI. Conclusion

The Survey on Online Crime method relates to significant losses and scary online experiences for consumers, which are challenging for government organizations and the emergence of various civilizations. A simple and uncomplicated strategy may be used to assist, online crime is a modern issue that is on the rise, damaging, and makes it challenging to digitally transform individuals. After consulting this data, we can obtain a basic sense of how we may try to address the issue of reporting complaints and the disconnection or gap between the general public and the police. By implementing a new online crime prevention system, the issue of reporting false crimes will be resolved since this system will need police verification before reporting incidences.

References

[1] Balarengadurai, C. and Saraswathi, S., 2012, Detection of exhaustion attacks over IEEE 802.15. 4 MAC layer using fuzzy logic system. In *2012 12th International Conferenceon Intelligent Systems Design and Applications (ISDA)* (pp. 527-532). IEEE.

[2] Balarengadurai, C. and Saraswathi, S., 2013. A fuzzy logic system for detecting ping pong effect attack in IEEE 802.15. 4 low rate wireless personal area network. In *Intelligent Informatics* (pp. 405-416). Springer, Berlin, Heidelberg.

[3] Balarengadurai, C. and Saraswathi, S., 2012,.Detection of exhaustion attacks over IEEE 802.15. 4 MAC layer using fuzzy logic system. In *2012 12th International Conference on Intelligent Systems Design and Applications (ISDA)* (pp. 527-532). IEEE.

[4] Balarengadurai, C. and Saraswathi, S., 2012, Detection of jamming attacks in IEEE 802.15. 4 low rate wireless personal area network using fuzzy systems. In *2012 International Conference on Emerging Trends in Science, Engineering and Technology (INCOSET)* IEEE.

[5] J. Agarwal, R. Nagpal, and R. Sehgal, ―Crime analysis using k-means clustering, International Journal of Computer Applications, Vol. 83 – No4, December 2018.

[6] J. Han, and M. Kamber, ―Data mining: concepts and techniques, Jim Gray, Series Editor Morgan Kaufmann Publishers, August 2021.

[7] P. Berkhin, ―Survey of clustering data mining techniques, In: Accrue Software, 2003.

[8] W. Li, ―Modified k-means clustering algorithm, IEEE Congress on Image and Signal Processing, pp. 616- 621, 2016.

[9] D.T Pham, S. Otri, A. Afifty, M. Mahmuddin, and H. AlJabbouli, Data clustering using the Bees algorithm,proceedings of 40th CRIP International ManufacturingSystems Seminar, 2006.

[10] J. Han, and M. Kamber, ―Data mining: concepts and techniques, 2nd Edition, Morgan Kaufmann Publisher, 2021.

[11] Amarnathan, L.C. (2013) Technological Advancement: Implications for Crime, The Indian Police Journal, April June.

[12] Abraham, T. and de Vel, O. (2016) Investigative profiling with computer forensic log data and association rules," in Proceedings of the IEEE International Conference on Data Mining (ICDM'02), Pp. 11 – 18.

[13] Brown, D.E. (1998) The regional crime analysis program (RECAP): A frame work for mining data to catch criminals," in Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, Vol. 3, Pp. 2848-2853.

[14] Corcoran J.J., Wilson I.D. AND Ware J.A. (2022) Predicting the geo- temporal variations of crime and disorder, International Journal of Forecasting, Vol. 19, Pp.623–634.

[15] Jayaweera, C. Sajeewa, S. Liyanage, and T. Wijewardane, "Crime analytics: Analysis of crimes through newspaper articles," Moratuwa Engineering Research Conference (MERCon), IEEE, April 2015, pp. 277 – 282.

[16] Marshall, G.M. and Marshall, D.R. (2008) CRIME IN INDIA, Annual Series, 1954-2006, Published by the Government of India, Ministry of Home Affairs, National Crime Records Bureau , Electronic Dataset and Codebook,

[17] Nath, S. (2020) Crime data mining, Advances and innovations in systems, K. Elleithy (ed.), Computing Sciences and Software Engineering, Pp. 405-409

[18] Ozkan, K. (2004) Managing data mining at digital crime investigation, Forensic Science International, Vol. 146, Pp.S37-S38.

[19] Senator, T.E., R.W.H. (1995) The FinCEN Artificial Intelligence System: Identifying Potential Money Laundering from Reports of Large Cash Transactions, AI Magazine, Vol.16, No. 4, Pp. 21-39.

[20] John Hani, Mohamed Nashaat, Mostafa Ahmed, Zeyad Emad, and Eslam Amer. "Social Media Cyberbullying Detection and prevention using Machine Learning International Journal of Advanced Computer Science and Applications, (IJACSA) Vol. 10, No. 5, 2019.