An Empirical Study of Cybercrime and Its Preventions

Shefali Batra
Department of Applied Science
Chitkara University School of Engineering and Technology, Chitkara University
Himachal Pradesh,India
shefali.batra@chitkarauniversity.edu.in

Madhu Gupta
Department of Applied Science
Chitkara University School of Engineering and Technology, Chitkara University
Himachal Pradesh,India
madhu.gupta@chitkarauniversity.edu.in

Jessicaa Singh
Department of Applied Science
Chitkara University School of Engineering and Technology, Chitkara University
Himachal Pradesh,India
jessicaa.28sept@gmail.com

Devshri Srivastava
Department of Applied Science
Chitkara University School of Engineering and Technology, Chitkara University
Himachal Pradesh,India
devshrisrivastava@gmail.com

Isha Aggarwal
Department of Applied Science
Chitkara University School of Engineering and Technology, Chitkara University
Himachal Pradesh,India
ishu06283@gmail.com

2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC) | 978-1-7281-7132-6/20/$31.00 ©2020 IEEE | DOI: 10.1109/PDGC50313.2020.9315785

Abstract— **In this modern era of technology, the world is heavily dependent on technology no matter where one goes. Due to our heavy dependency on technology criminals have taken this advantage for their benefit. Cybercrime is quickly becoming one of the fastest rising forms of modern crimes. Cybercrime are well known for the downfall of so many companies, organizations and personal identities. The main intent of this paper is to define cybercrime, various types of cybercriminals and cybercrime affecting the world and its prevention. This paper will also analyse statistical data on various types of cybercrime and its growth in last few years.**

Keywords— Cybercrime, Hackers, Crackers, Cyber stalking, E-mail spoofing, Machine learning, Data mining

I. INTRODUCTION

The World Wide Web or cyberspace is a massive community of billions of users and websites. The word "cyber" comes from ancient Greek which related to the idea of government. The obscure term "cyber" was popularised by the mathematician Norbert Wiener for his book 'Cybernetics' in 1940s. The word cybercrime, however, was come in existence in the late 90s as the internet extension. It was used to give a detail in a very slack way forth entire types of crime which occurred on the net [1]. The origin of cybercrime however is said to date back to 1834. There is someone out there trying to pick it or break in for every lock -David Bernstein. The two thieves execute the first cyber-attack in 1834 by stealing financial market information of French Telegraph System. The Blanc Brothers hacking the telegraph system gave the way to a group of teenagers who repeatedly and intentionally misdirected and disconnected customer's calls, two years after Alexander Graham Bell invented the telephone. Over time the techniques have grown more sophisticated making it harder to catch people on the web with malicious intent [2]. Merriam-Webster defines cybercrime as "criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit, or manipulate data." Other works correspond to the cybercrime as ―illegal activity in a straight line connected to the use of computers, specially against the law trespass into the computer system or database of another, manoeuvring or stealing of stored or on-line data, or damage of equipment and data [3]. Due to large dependency on internet there is rise in various types of cybercrime that include identity theft, cyber pornography, e-mail spoofing, financial theft, cyber terrorism etc. [4]. Cyber-attacks have great impact on economic condition of a country as well as on defence of a country. A daily struggle of cybercrimes has made combating situation for both individuals and organisations. This fight back has been aggravated by the fact of using complex techniques by cybercriminals [5]. Cybercrime is on rise because of many factors one of them including unemployment [6]. So, there is a great need to dig a deep insight to analyse the cases of cybercrime and acting on it. A range of algorithms and techniques like Artificial Intelligence, Clustering, Neural Networks, Association Rules, Decision Trees, Regression, Genetic Algorithm, etc., are used to discover knowledge from databases [7] .Data mining and Machine learning are good methods to deal with cybercrime [8]. This paper has been mainly divided into 4 sections: present section is introductory in nature. Section 2 is concerned with some common types of cyber criminals; section 3 defines and provides statistical data for various types of cybercrimes and section 4 mentions most widely used methods of prevention. At last conclusion has been given in Section 5.

II. TYPES OF CYBER CRIMINALS

Any person who engages in a criminal activity through computers or any other electronic media can be called a cyber-criminal. Though cyber criminals are commonly called hackers, there are many times of them like identity thieves, or internet stalkers. Some of the most common are hackers, crackers, hacktivists or nation state hackers.

A. Hackers

Hacker is a term commonly applied to a Computer user who intends to gain unauthorized access to a computer system [9]. Mass media often refer hacker as an intruder trying to break into the computer system to steal or destroy the data [10]. Hackers explore computers out of curiosity, to compete with peers, or to build a reputation. They use very powerful computers to explore and to peep into other computers [3].

B. Crackers

It is to gain unauthorized access to a computer in order to commit another crime such as destroying information contained in that system. These subgroups may also be defined by the legal status of their activities [11]. Crackers use computer security related skills to create Trojans, viruses, worms etc. Cracking is considered as riskless and is more practised by the youngsters because they just do this for their fun motives or antisocial motives [10].

C. Hacktivists

Hacktivists are certain type of criminal hackers who unite to carry out cyber-attacks in support of political or social causes. These are the people hacking for a particular purpose, people who are politically, socially motivated with the aim to reveal contentious truth about their opponents [12]. They target religious organizations, terrorists, or even governments for their purposes. They are generally dangerous as they intend to cause harm and steal information and spread it to embarrass the victim.

D. National State Hackers

Nation state hackers usually target government agencies, critical infrastructure or any industries known to have sensitive information. Sophisticated nation state hackers on the other hand are hired by the government, or other agencies. They have 'licence to hack'. They might be a part of semi hidden 'cyber army' or 'hackers for hire'. They generally launch cyber-attacks against other countries [13].They work for a government to obstruct other targeted organisations, individuals or governments, to obtain access to their sensitive and useful data to create incidents so that they can have international significance.

III. MOST COMMON TYPES OF CYBERCRIME

Cybercrime is any criminal activity on cyber space. One of the earliest forms of cybercrime is hacking, which had started around 1960s. Since then, with the advancement of technologies cybercrimes have also grown more complicated and can no longer be grouped under 'hacking'. Some of the most common types of cybercrime are identity theft, cyber stalking, etc.

A. Identity Theft

Identity theft is an unauthorized access to individual information or records. Furthermore, the use of false identity is a crime identity fraud [4]. Identity theft is purposeful use of someone else's identity to get hold of key pieces of their information. Identity thefts and frauds are intensifying and have go ahead to financial loses. The costs of preclusion and the costs of fraud, both have a substantial economic impact in the situations where preclusion fails. There are social and psychological impacts on victims in addition to economic losses. The occurrence and consequences of identity thefts and fraud can be minimising if business and governments play their role significantly, but a critical role remains for consumers. The diversity in point of concern by those who experienced credit card fraud and theft from those who experienced new account, existing account and other identity theft and fraud indicates that in the view of consumers, credit card crime is distinct [14]**.** After analysing " Fig. 1" (source: NCRB, 2018 [18]) given below, we can see that, Karnataka has the highest number of cases, accounting to 76% of the nation's total number of identity thefts.

B. E-mail Spoofing

Some people often spoof e-mails of known and unknown individuals. It means forging sender's address to create e-mail messages, so it appears to have been sent from another source [4]. It is one of the most common types of cybercriminal activity. E-mail spoofing is a popular tactic used in spam campaigns as people are likely to open an e-mail if they recognise the source. As the core e-mail protocols don't have many authentication methods it becomes easy for people to mislead others. This can be achieved because the Simple Mail Transfer Protocol (SMTP) does not provide any mechanism for address authentication. It is necessary to keep updated anti-malware software in order to avoid being a victim [4].

C. Financial Theft

In a world where technology is the future, people are starting to depend on online transactions more and more, as a result of which the rate of financial thefts has started to increase alarmingly. Financial thefts include stealing credit card numbers, important information like one-time passwords (OTP) to access online banking accounts, or bank account numbers [4]. One common example of financial fraud is when someone stole your credit card information or bank account information to make purchases that you did not validate. For the victims of financial fraud, the cost and consequences could last a very long time and be quite significant. They also exhibit reduced trust in credit card markets after thefts [15]. It is a global problem, which causes victims monetary loss, stress and inconvenience. However, gaining a solid understanding of what is financial theft and where the dangers lie, individuals can protect themselves against it.

D. Cyber Stalking

Cyber stalking is a form of internet or computer crime when a person or an organisation is pursued or followed online. This includes sending threatening or non-threatening messages to the victim, which could be done either through any social networking sites or through e-mails [4]. Cyber stalking mostly occurs with women and children, where a stalker can be a known or an unknown person. As the internet stalker is not required to leave their space, they become fearless in their pursuit of harassing the victim [9]. In 2018, Maharashtra had the highest number of cyber stalking incidents against woman and children. Out of almost 742 cases recorded in the country more than 95% were against women as seen from "Fig. 2" (source: NCRB, 2018[19,20]).

E. Cyber Pronography

Cyber pornography is an act of using the cyberspace in which pornography or pornographic materials are produced,

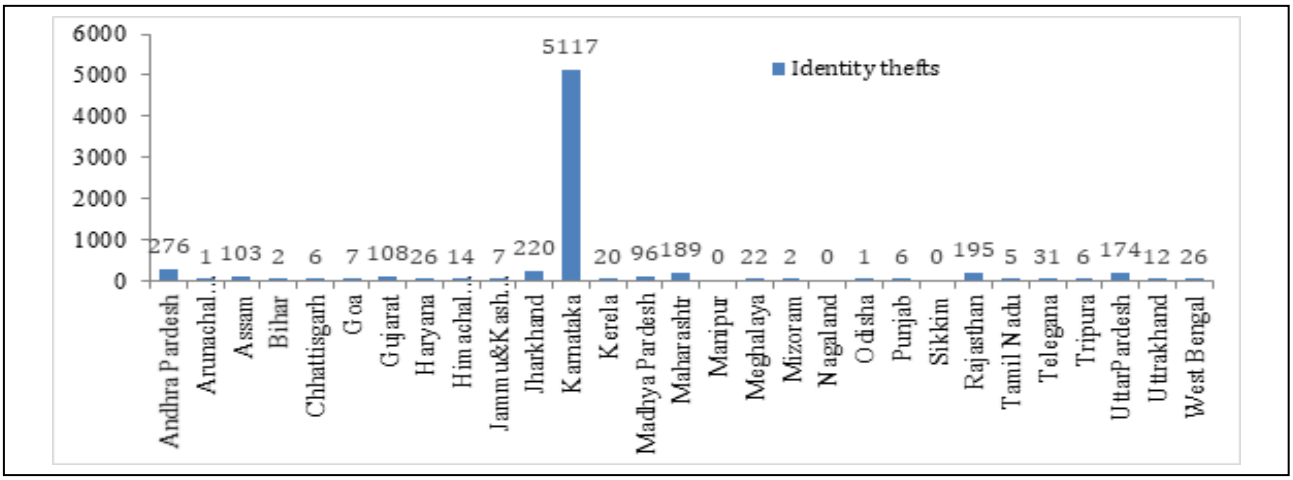

Fig. 1: Total Number of Identity Thefts in all states of India

displayed, circulated or imported. Cyberspace is technology that is used to rich the form of pornography. Cyber porn is one of the biggest misuses of technology having adverse effects on society which leads to moral degradation [16]. Even nowadays pornography has become a kind of business to the society. It refers to forcing and blackmailing the children to click abusive pictures and videos to get them uploaded on the illegal sites or the sites specially made for this purpose on the internet. The Internet is commonly used by children offenders worldwide. These kinds of websites also allow downloading of pornographic movies, videos and pictures [4].

F. *Drug Trafficking*

The global illegal trade which includes the production, processing, distribution and selling of substances subject to drug prohibition laws, is known as Drug Trafficking [17]. It involves the selling of illegal products like cocaine, tobacco, narcotics etc. through different types of websites or auction sites on the internet. Trafficking of drugs becomes easy through internet as people need not require sharing any personal information, so they can easily communicate through e-mail [4]. Several auction sites are even known for selling the cocaine in the form of 'honey' in India [9].

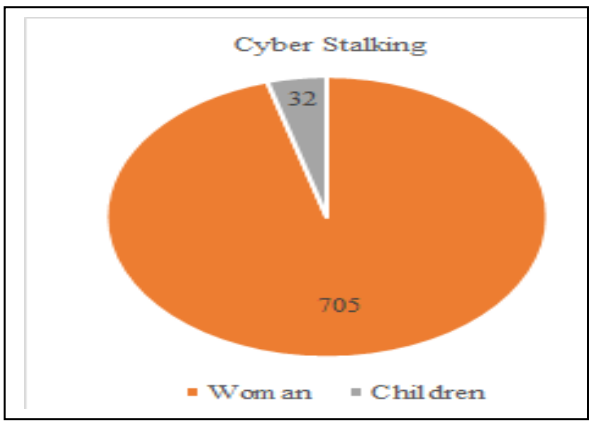

Fig. 2: Comparison between total number of cyber stalking cases in India against children and women

IV. PREVENTIONS

The exponential rise in digital crimes has led to the development of several revolutionary technologies in order to combat it. Individuals are often advised to use strong passwords or secure computers and mobile phones, to protect themselves. Experts around the world have come up with techniques such as machine learning and data mining to reduce the risks associated with cybercrimes.

A. *Machine Learning*

Machine learning is likely to remain as the most promising and era defining technologies for dealing with cyber-security threats and issues of all types [8] as various machine learning techniques and algorithms can be used to spot various threats related to cybercrime. In the process of machine learning, a computer can figure out the solutions for the given problem as per the instructions given to the computer without being specifically programmed. In machine learning, classifiers detect various data patterns whereas algorithms in this organize the data and arrange it in patterns. In security purpose various classifiers work together in algorithms, and then separate the suspected data compared to the normal one and are arranged in patterns, then are combined with actionable contacts to take some actions regarding it. Frameworks must be established to assist the forensic investigations, support the forensic community and to deal with different incidences [5]. Some examples of this process are sending warning messages before opening an encrypted site or a site that can harm your system, basically which is wrong to open that site

B. *Data Mining*

Data mining is a process which is used to find useful patterns or arrangements from the large amount of data or information. Research in the field of data bases and information technology has led to storage and data-forming strategy in line with our need for further decision-making [7]. It involves three processes: exploration, pattern the data is determined based on the problem or instruction. Next is pattern identification, that is to choose or form that pattern or arrangement that makes the best prediction. After that patterns are implemented for required or desired

outcomes. Techniques and algorithms of data mining such as classifications, clustering, etc., help to identify the patterns that could be used further to find encrypted passwords for the security purpose. Like regression in cyber security can be used for fraud detection, classification includes spam filter separating spam form other messages. Forensic Analysis is the best method for clustering, from which the causes, path and effects of an event becomes clear.

C. Data Mining

In this digital world, technologies are getting more and more sophisticated and so are crimes. As the number of internet users continues to rise, the need for legal framework has gathered momentum. In India, cyber laws come under Information Technology Act, 2000 which came into force on October 17, 2000. Some of the offences include (doj.gov.in):

1) Offences under Information Technology Act, 2000

- Tampering computer source documents

  Under section 65, it states that if any person knowingly or intentionally conceals or destroys computer code used for computer, when the foundation code was necessary to be reserved or maintained by law, the offender could face imprisonment of minimum term of three years.

- Computer Related Offences (Section 66 and Section 66B to 66E)

  It includes hacking with computer systems (section 66), receiving stolen computer or communication device (section 66B), using password of another person (section 66C), cheating using computer resource (section 66D), and publishing private images of others (section 66E).

- Acts of cyber Terrorism (Section 66F)

  Cyber terrorism under this section is defined as, when someone denies authorised personnel access to computer resource or when someone contaminates a system with the intention of harming the nation's security and integrity. The offender could face imprisonment up to life if found guilty.

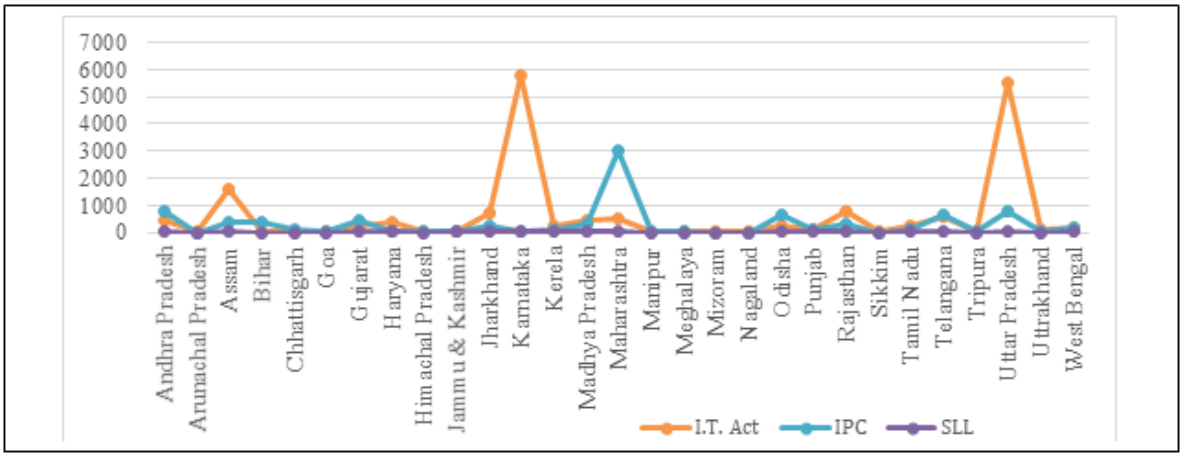

Fig. 3: Cybercrimes practiced in all states under cyber acts of India

- Publication/Transmission of Obscene/Sexually Explicit Content

  Under sections 67, 67A and 67B, any person found transmitting or publishing material in electronic form, which is obscene, sexually explicit or lascivious in nature could face imprisonment of term of five to seven years.

- Breach of Confidentiality & privacy/ Disclosure of Information in Breach of Lawful Contract

  Under sections 72 and 72A, any person found to be guilty could face up imprisonment for term which may extend for up to two or three years.

According to "Fig. 3" (Source: NCRB, 2018 [21]), the state of Karnataka records the highest number of offences committed with majority of the cases classified as identity frauds and computer related offences.

2) Offences under Indian Penal Code

- E-mail spoofing (Section 465)
- Cyber Fraud (Section 420)
- Web-Jacking (Section 384)
- Forgery of online records (Section 465)
- Sending defamatory messages through e-mail (Section 500)

Studying "Fig. 3" given below, we can see that under the IPC, offences committed are highest in the state of Maharashtra with majority of the cases falling under Section 420 (878 cases new cases registered).

3) Under SLL (Special & Local Laws) Act

- The Copyright Act, 1957

  Long form: An act to amend and consolidate the law relating to copyright. Under section 63, any person knowingly infringes or abets infringement (who copies another author's work) of the copyright in a work are covered by Copyright Act. Such a person may be punished with imprisonment of minimum term of 6 months.

- Trademarks Act, 1999

  The Courts in India apply Trademarks Act (Remedy of Infringement) which permits the owner of trademark to benefit the cure of breach only when trademark is registered.

V. CONCLUSION

It has been found that with the advancement of technology, cybercrime poses a serious threat to not only an individual's safety but also to nation's security. Individuals and businesses suffer tremendous financial losses and it is a high threat to military technology. The data breaches result in significant data losses which affects millions of people. There are aspects of cybercrime which feature in all forms of criminal behaviour, even crimes which are considered as more traditional offences like drug trafficking, and terrorism. In addition to financial and technological losses, there are emotional and psychological impacts on victims. Worldwide law enforcement authorities are working together to develop new technologies and forensic methodologies in order to ensure safety and security on internet. Datamining, machine learning and bioprinting are some of the few advanced technologies used to combat cybercrime. However, a critical role remains for individual consumers. Individuals must be aware of different types of cybercrimes and remain cautious to avoid any damages. An intellectual mindset is a very valuable weapon to put a stop to these activities to some extent.

ACKNOWLEDGMENT

We sincerely thank our professors and teachers at Chitkara University for their valuable comments and feedback.

REFERENCES

[1] R. Moore, *Cybercrime: Investigating high-technology computer crime*. 2014.

[2] S. Schjolberg, *The History of Cybercrime: 1976-2014*. 2014.

[3] S. Hemraj, S. yerra Rao, and Panda T.C., "cybercrimes and their impacts:A review," *Int. J. Eng. Res.*, vol. 2, no. 2, pp. 202–209, 2012.

[4] E. Ramdinmawii, S. Ghisingh, and U. M. Sharma, "A Study on the Cyber-Crime and Cyber Criminals: A Global Problem," *Int. J. Web Technol.*, 2015, doi: 10.20894/ijwt.104.004.001.003.

[5] N. M. Karie, V. R. Kebande, and H. S. Venter, "Diverging deep learning cognitive computing techniques into cyber forensics," *Forensic Sci. Int. Synerg.*, 2019, doi: 10.1016/j.fsisyn.2019.03.006.

[6] N. Al-Suwaidi, H. Nobanee, and F. Jabeen, "Estimating Causes of Cyber Crime: Evidence from Panel Data FGLS Estimator," *Int. J. Cyber Criminol.*, vol. 12, no. 2, pp. 392–407, 2018.

[7] B. Ramageri M, "Data Mining and its Applications," *Indian J. Comput. Sci. Eng.*, vol. 1, no. 4, pp. 301–305, 2010.

[8] N. K. Mutyala, K. V. S. Koushik, and Sundar K. John, "Data Mining and Machine Learning Techniques for Cyber Security Intrusion Detection," *Int. J. Sci. Res. Comput. Sci. Inf. Technol.*, vol. 3, no. 3, pp. 162–127, 2018.

[9] N. Jain and V. Srivastava, "'CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY,'" *Int. J. Comput. Appl.*, vol. 1, no. 4, pp. 76–87, 2014.

[10] J. L. Richet, "From young hackers to crackers," *Int. J. Technol. Hum. Interact.*, 2013, doi: 10.4018/jthi.2013070104.

[11] R. D. Clifford, *Cybercrime: The Investigation, Prosecution and Defense of a Computer-related Crime*, 3rd ed. Carolina Academic Press, 2011.

[12] T. Sorell, "Human rights and hacktivism: The cases of wikileaks and anonymous," *J. Hum. Rights Pract.*, 2015, doi: 10.1093/jhuman/huv012.

[13] S. Mansfield-Devine, "Nation-state attacks: the start of a new Cold War?," *Netw. Secur.*, 2018, doi: 10.1016/S1353-4858(18)30114-4.

[14] GILBERT JOHN A., "Consumer Identity Theft Prevention and Identity Fraud Detection Behaviours: An Application Of The Theories Of Planned Behaviour And Protection Motivation," McMaster University, 2014.

[15] Philippe Jougleux, "Identity theft and internet," *Int. J. Liabil. Sci. Enq.*, vol. 5, no. 1, pp. 37–45, 2012.

[16] H. Puspitosari and A. S. Bidari, "ETHIC CYBER STRENGTHENING ASCRIMINAL LAW POLICY FORMULATIONS IN RESPONSE CYBERPORN," *UNTAG Law Rev.*, 2017, doi: 10.36356/ulrev.v1i2.594.

[17] S. Chawla *et al.*, "World report 2005: Analysis," 2005.

[18] TABLE 9A.2Cybercrimes - IT Act Cases (Crime Head-wise & State/UT-wise) – 2018. http://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table%209A.2. pdf

[19] TABLE 9A.10 Cybercrimes against Women (States and UTs) – 2018. https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table%209A.10.pdf

[20] TABLE 9A.10 Cybercrimes against Children (State/UT-wise) - 2018 https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table%209A.11.pdf

[21] TABLE 9A.2 Cybercrimes – IT Act Cases (Crimes Head-wise & State/UT-Wise)2018 – https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table%209A.2.pdf