2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. June 4-5, 2020

Classification and Imapct of Cyber Threats in India: A review

Sarvesh Tanwar
Amity Institute of Information Technology
Amity University
Noida, India
s.tanwar1521@gmail.com

Thomas Paul
Chitkara University of Engineering and Technology Chitkara University
Rajpura, India
thomas1699.cse18@chitkara.edu.in

Kanwarpreet Singh
Chitkara University of Engineering and Technology
Chitkara University
Rajpura, India
kanwar1687.cse18@chitkara.edu.in

Mannat Joshi
Chitkara University of Engineering and Technology
Chitkara University
Rajpura, India
mannat1649.cse18@chitkara.edu.in

Ajay Rana
AIIT, Amity University Uttar Pradesh
Noida, India
ajay_rana@amity.edu

***Abstract*— Due to rapid flaring criminal activities and offences in the cyber world, a deep and detailed research and study on this grave matter was very necessary. This research paper brings attention to this serious issue which is only increasing with time. The paper describes various crimes and potential threats a user might face on the internet and in the cyber world which can cause loss of sensitive or important data and even put the device in dangerous and risky situations. With graphs and pie charts, the paper throws light on the cyber-crime statistics which shouldn't be ignored. This paper compares data and information with previously written research papers on this matter.**

Keywords—cyber security; cyber threat; cyber crime; internet security; online crime; internet crime

I. INTRODUCTION

One click away is someone grievously fetching all the data out of your device and using it for ransom or a vicious virus ready to infiltrate your device or computer systems and reduce it to it's most undesirable state. All this falls under the category of cyber crime. With broad facilities of the internet comes mildly to strongly dangerous sub-platforms for criminal activities. The internet has a unique ability to connect a user to any other user which also allows exposure of sensitive data and personal information to hackers and malicious criminals.

Cybercrime is defined as a crime in which a computer is the target of the crimes (hacking, phishing, spamming) or is used as a device to perform an offensive crime such as hate crimes and child pornography. Hence, both origin and victim of the attack are people in the real world and the smart mobile terminals act as a catalyst for attack process [1] [52].

With a rapid increase in crime statistics, it has become an area of great concern and study on this area is necessary and required. Furthermore, a certain solution to this issue is also required and the solution can only be attained if we understand the seriousness and significance of this area efficiently.

Many individuals, businesses and organizations are using internet for most of business communications as these are done through mail, social media and other mediums connected openly. Cyber criminals get chance to access and attack the data through the open communication channel [2]. Hacking is done successfully to obtain mass information coupled with account information held by various cards used all around the world. [3][4]

There are various types of cyber attacks such as stalking, SQL injection attack, phishing and spear phishing attack, cross site scripting, privacy invasion, etc. Stalking can further give roots to spamming, cyber bullying, ATM cloning, financial fraud, fraggle at tacks, Denial-of-service (DOS), Distributed denial-of-service (DDOS). Some Value Added Service Provider (VASPs) now advertise using flash messages, unsolicited. This means unsuspecting mobile users are easily trapped into subscribing for services they otherwise would not have been subscribed to [5].

Cyber Threat is defined as the feasibility of a malicious attempt to destroy a computer network, system or device. Cyber threats can greatly affect an individual, property or government. They are of following types - Social Engineered Trojans, Unpatched Software (such as Java, Adobe Reader, Flash), Phishing, Network traveling worms and Advanced Persistent Threats.

II. MOTIVATION

With a rapid increase in the crime statistics, almost every internet user and individual or firm present in the cyber world feel highly unsafe. Personal and other sensitive data is vulnerable and risk of its misuse by hackers and cybercriminals is gradually flaring in the humongous cyber world. Protection of privacy is needed especially by women who constantly feel insecure on social platforms. Misusing of personal data, bullying, stalking and other crimes lead to trauma in the victims. A grand number of people are victimized by these criminal activities which are only increasing with time.

The cyber world has become a dangerous platform because of these ever accelerating crimes. People are skeptical to use web facilities. Cyber crimes like identity theft, cyber terrorism, cyber stalking, cyber bullying, cyber pornography, etc affect the victim emotionally and degrade his or her mental state. Just like any other crime, this needs to come to an end too. Hence, via this paper, we want to bring more eyes to this important issue so that necessary steps could be taken to terminate this issue for the betterment of society.

978-1-7281-7016-9/20/$31.00 ©2020 IEEE

III. OBJECTIVE

This research paper throws light on the field of cyber-crimes which are usually not given much attention and awareness. Awareness of this grave subject is far more important than what we usually guess. Cybercrimes today are reaching every possible tick-box in the field of ominous criminal activities; hence a prolix study of this matter is necessary. Moreover, this research paper widely describes the statistics of cyber thefts and other severe crimes with detailed graphs and charts to help understand and comprehend this issue more efficiently and effectively.

IV. LITERATURE REVIEW

Table 1 represents the extensive work done by some of the researchers in this field.

TABLE I. WORK DONE BY VARIOUS AUTHORS ON CYBER THREATS AND SECURITY

Sr. No.	Author	Year	Work
1	Prakash Kuppuswamy et al.[1]	2017	In this paper the author discusses about the new ways by which our current security systems can be compromised to cyber crimes. Thus a new method is proposed by the authors to prevent and secure data using an entirely new authentication method is used which is based on block chain.
2	Oluwafemi Osho et al. [5]	2014	The paper is based on how to prevent user smart phones from getting spammed by SMS messages. The authors propose a method which works by temporarily storing the messages and then filtering according to their destinations based on a defined criteria and then sending them to only those customers who have opted for those specific services.
3	David Gugelmann et al. [6]	2018	Cyber attacks can also happen if a spy or a person from a rival company infiltrates the company and starts leaking its information from the inside. Though traditional methods can be traced back which increases the chances of getting caught, on e can click images which cannot be traced back. The author implements a water mark technique which when applied to documents could be detected from their image thus catching the culprit.
4	Linggunag Lei et al. (3) [2]	2013	The authors present an attack which makes almost all the android smart phones vulnerable. The CPVT attack (Cyber-Physical Voice privacy Theft Trojan) is presented by the authors. Using this attack they can steal anyone's identity which is a very big concern.
5	KimKwang Raymond Choo[7]	2011	The author tries to emphasize that not only government but private sectors should also invest in cyber security against future threats. Private security firms should be hired and the companies which produce electronics and services should try implanting some methods to avoid these circumstances.
6	Adel S Elmaghraby[8]	2014	The two problems which the upcoming and the current smart cities face which is privacy, safety and security. The drop in the privacy and security due to the collection of data by smart devices leaves the end user vulnerable to many dangers.
7	Subil Abraham[9]	2014	The modes and methods of attacking and compromising security constantly changes. The authors try to implement a mechanism which can help the security engineer in developing his system with scope for prevention from future foreseeable attacks.
8	Wnye Wnag[10]	2013	In this paper it is discussed that the how smart grids are becoming more efficient and reliable. Different methodologies have been proposed by the author to prevent it from any cyber attacks.
9	Hemraj Saini [11]	2012	Cyber crimes cause a lot of problems such as threat to national security, financial loss and psychological stress. This paper gives the reader an understanding about is cyber crimes, how to safeguard yourself from it etc.
10	Martin Husák [12]	2018	This paper is a literature survey on how to predict cyber attacks. Various methods have been discussed. Four main tasks are- attack projection, intention recognition, intrusion prediction and network security situation forecasting.
11	Ye Yan et al. [13]	2012	The authors focuses on the vulnerability of a smart grid communication network in cyber crimes, despite of it being an efficient electricity network. They show the necessity of a comprehensive communication architecture with security build in as a solution for cyber security in smart grid .
12	Mauro Conti et al. (2) [14]	2018	This paper discusses the challenges and opportunities and the notion of cyber threat intelligence and further it address the identical challenges or present opportunistic solutions to provide threat intelligence.
13	Shipra Ravi Kumar, Suman Avdhesh Yadav, Smita Sharma, Akansha Singh [15]	2016	In this paper authors is discussing their views on effective cyber society. They are telling about the different types of the cyberattacks and also how to identify and prevent them. According to the authors for greater effectiveness all the researcher's community of private, government, academic sectors have to come together. They have also shared their views on how terrorist are using different cyberattacks on various critical information centres. They are showing great urge to rectify laws related to cyber security and awareness.
14	Shalini Gupta, Anamika Singh, Sheela Kumari, Neelma Kunwar [16]	2017	In this paper authors are discussing about the impacts of cybercrime on adolescents through social media. They are sharing their views on the fact that nearly across 10 million people access social media daily in India and out of this 33% are the social students (the largest ratio). According to them the prime task of every teenager is to maintain very good profile at social media and check likes and comment to the posts. As adolescents are having the major ratio so they are the main target of cybercrimes. According to author many youngsters are involved in online grooming and sexting and they are having exposure to many illegal content. To prevent youngsters they are suggesting that the prime responsibility is of their parents to acknowledge their children to use internet wisely.
15	Abu Shakil Ahmed, Sudip Deb, Al-Zadid Sultan Bin Habib,Nurunnabi Mollah,Abu Saleh Ahmed [17]	2017	In this paper the authors are sharing their views on simplistic approach to detect cybercrimes and deter cyber criminals. The authors are having a conversation on internet that it has become one of the core requisites of everyday life. They are telling us that many advanced technical countries are trying hard to make their cyber space safe and hard to break and in this work the less advanced technical countries are lagging and for them they had made a cybersecurity architecture which can be easily implemented. They are describing that they had used biometric detection technology for detection of cybercrimes. They had a strong belief that it can work very efficiently and can adapt with time. Also the results show that it can work accurately and can provide long term safety to cyber space.

V. RESEARCH GAPS

In [paper7] the author uses the Markov chains to analyze and predict future threats. The Markov chains have a major flaw that is they work reliably only under low noise. If the noise increases, error starts showing up in its readings.

VI. METHODOLOGY

In this paper we describe many of the cyber attack techniques used by individuals with theoretical analysis. Theoretical analysis includes relevant data of a few past years which tells us about the trend of cyber crimes occurring in India and the motives behind them.

VII. DIFFERENT TYPES OF CYBER ATTACKS

- *SQL Injection:* SQL injection is that sort of cyber attack where an attacker uses sql codes to perform the attack. In this attack, the statements used can bypass the security measures of the programme and can control the database of the programme. These codes can be used to modify, erase, delete the data from the database of the attacked programme/site. Before proceeding of this attack the attacker must find vulnerable user inputs in the programme or in the website [18] [19] [20].

Different forms Of SQL Injection

1. Classic SQLI
2. Database Management System-Specific SQLI
3. Blind or Inference SQLI
4. Compounded SQLI
    a) SQLI + DNS hijacking
    b) SQLI + Insufficient Authentication
    c) SQLI + XSS
    d) SQLI + DDOS attacks

- *Social Engineering (SE):* Social engineering attack is all about leaking some personal information or tricking someone by means of technology. The idea behind this attack using emotional and psychological reactions against them like leaking some sensitive content/information or making some security mistakes. This attack contains many steps starting from gaining trust of the victim to getting of information [21] [22] [23].

Most Common Forms Of Digital Social Engineering Assaults

1. Baiting
2. Shareware
3. Pretexting
4. Phishing
5. Vishing
6. Spear Phishing
7. Water holing

- *Cyber Stalking:* Stalking is the process of harassment to an individual, group, organisation by the means of internet, instant messaging or any other digital means. It is the form of *Cyber Bullying*. A cyber stalker relies upon the anonymity afforded by the internet to allow them to stalk their victim without being detected [24] [25] [26].

To Avoid Cyber Stalking

1. Keep a Low Profile
2. Hide Internet Protocol (IP)
3. Maintain Good Digital Hygiene
4. Never Disclose Sensitive Information
5. Update Antivirus/Programme

- *Denial of Service Attack:* An attack where the victim/executor aims to make a system either temporarily or permanently unavailable for the clients is known as DOS attack. This happens by interrupting the services of the host machine which is connected to the internet. These attacks are accomplished by sending some code/information that triggers them or by flooding the network with more traffic. This attack is targeted to only reputed organisations such as Media Companies, Law Enforcement Agencies, Banks etc [27] [28] [29].

Commonly, DOS attacks are of two types

1. *Flooding:* In this the targeted server is saturated by overwhelming of packets. This saturated server takes more time to buffer and execute the programme and in the end resulting in DOS attack.
2. *Buffer Overflow:* In this the targeted host's memory, hard disk or CPU time is consumed and results in the abnormal or sluggish behaviour of the system. It can even cause system crash.

- *Distributed Denial Of Services Attack (DDOS):* DDOS attacks are almost the same as the DOS attack. In this attack more than 1 system is used to flood the server with random requests so that the server takes much more time to respond and the end it crashes [30] [31].

- *Cross site scripting (XSS):* Cross site scripting is a type of injection attack. In this type of attack the attacker uses a website for an attack. That website is used to run the malicious code in the form of browser side script. XSS attacker can use to send malicious script and the victim's machine has to execute that specific code because it is unable to check that whether that script came from the trusted or untrusted source [32] [33].

Examples of such attacks are as follows

1. Stored
2. Reflected
3. DOM based attack

- *ATM Cloning:* ATM skimming is now a day a very popular type of cyberattack. In this attack the victim's ATM card s cloned using a module(chip) that is placed in the real place where an card is entered for any transaction, that module just duplicates the card and gives the duplicated copy of the card to the attacker. In this case only card is copied so to get the pin of the card some spy cameras are inserted from which the clear view of the keypad is there. It is how a ATM cloning attack is executed [34] [51].
- *Piracy:* Piracy is unauthorised copying of some data from a licenced user and then supplying it to other people. It is one of the most common attack. Live examples of this are torrent websites, these websites contain all the content (movies, games, TV series) just after few hours of release and at free of cost. So the normal people doesn't spend money on using official products and take a pirated copy from these websites [35].
- *Man in The Middle Attack (MITM):* The MITM attack is a vulnerable way to get information between two systems. In this attack when two systems are communicating with each other directly a third system comes in between and the communication exchange now takes place through that system. That system is entered by the attacker and can now intercept all the data from both the systems and can also vary the messages. This type of attack has power to exploit the real time transaction [36] [37] [38].
- *Birthday Attack:* Birthday attack is a cryptographic attack. These attacks are based on hash algorithms that are used to find the collision of a hash function. In this type of attack, the probability of finding two random messages that have same message digest. If any message's message digest is known than the attacker can successfully replace the victim's message by his message [36] [39].
- *Ransomware attack:* Ransomware (a.k.a rogueware or scareware)as its name suggest in this type of attack it threatens the victim as access to his machine is locked and to open it it either threatens or demands money. It is created by scammers who are highly knowledgeable in computer programming. They are generally carried out with the help of Trojan which is a legitimate file on seeing this nobody can guess that it is harmful and victim is tricked to download it and open it as it comes with email as an attachment. This kind of attack is most dangerous cyberattacks in the world and has caused around loss of $5billion till 2018.

  Ransomware are popularly further divided into two main types -

  - *CRYPTO Ransomware*- Crypto ransomware is as simple as weaponizing strong and sensitive data against victims and to deny them access to those files. The most common ways by which you can encounter this dangerous ransomware: -via corrupt links and files present in corruptly delivered emails, instant text or other messages or other networks or downloaded and installed onto your system or device by other harmful threat posing ways, such as Trojan-downloaders.
  - *LOCKER Ransomware*- It is widely known as computer locker because it lock the users out of their systems. The chief delivery approach of this malware so far is through infected and malicious websites and then it start vandalising the devices.
  Lock screen ransomware is transported along with bogus and false advertisements which pop up while using malicious and corrupt sites on web. Sometimes while browsing, clients get to see an advert which falsely warns them that they have to download a file to avoid their system from being infected. When they proceed, the malicious website downloads the lock screen ransomware onto the operating system which then harms it by executing criminal activities.
  Around 851 million such infections were disclosed by an organisation an year ago. [36] [40] [41] [42].
- *Botnet Attack:* In this type of attack millions of machines are filled with botnets that are just malware under hacker control. These botnets are used to carry out DDoS attacks on that specific machines. These attacks are difficult to trace because these botnets are located in very different locations [36] [43] [44].
- *Brute Force Attack:* This type of attack is based on hit and trial method. In this attack the victim's password is cracked. It is an automatic software which make all the possible combinations (using key derivation systems) to crack a single password. This type of attack takes a lot of time so it is now rarely used. The effectivity of this attack can be reduced by having long passwords and using special characters and symbols or by using phrases or by making a combination of text and numeric, all these can even stop the brute force [45] [46] [47].

VIII. THEORETICAL ANALYSIS

Cybercrime in India shows little to no decrement in passing years. Some states in India have cyber crimes and offenses ratio much higher than other states proving it to be an area of great concern. As per the IT Act, it was proven that 10 out of 29 Indian states experienced a rise in crimes associated with cyber cases from the year 2014 to 2016 [48]. Data in rendered graphs lucidly reveals how computer-based criminal activities are swiftly evolving in India. In Uttar Pradesh, maximum cybercrime cases were registered in 2016 [49].

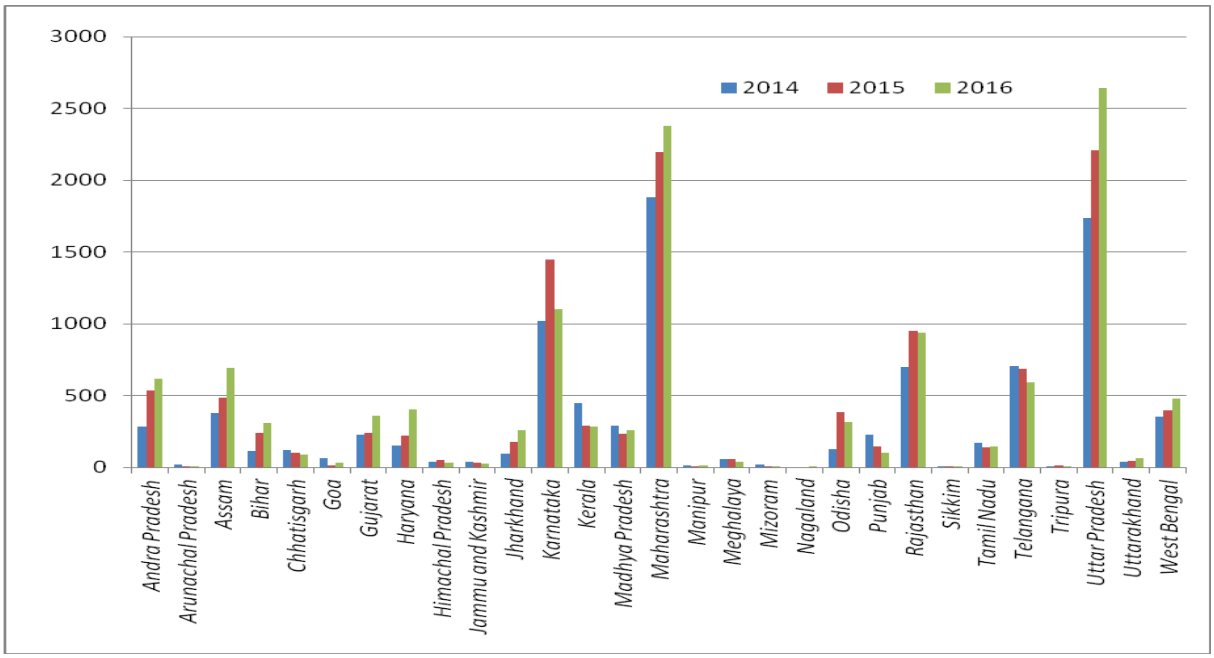

Fig. 1. Cyber Crimes in different states [50]

Figure 1 is representing the cybercrimes in different states of India from year 2014 to year 2016. On seeing this graph, we came to know that almost in every state the slope of the graph from year 2014 to 2016 is increasing i.e. every year the rate of cybercrimes in different parts of India is increasing. On studying the graph, it can be clearly seen that the rate of cybercrimes in Uttar Pradesh and Maharashtra followed by Karnataka. It is also noticed that

Nagaland has the minimum amount of Cyber Crimes. The Cyber Crimes have also decreased a bit in states like Punjab followed by Mizoram and Meghalaya. The deep study of this graph let us know about the lack of knowledge about cybercrimes in many states and in some states many preventive measures have also been applied to prevent cybercrimes and they are working in right way as the count has gone down significantly.

Figure 2 represents the cyber crime in different union territories in India from 2014 to 2016. Cyber crime has been nonexistent in UT's D&N Haveli, Daman and Diu, Lakshadweep, and Pondicherry in the period of 2014 to 2016. Whereas in UT's like Chandigarh, Delhi and Andaman and Nicobar Islands there has seen a steady decrease in the total reports filed from 2014 to 2016. This is because the Central Government is directly responsible for taking swift and fast action against such cases.

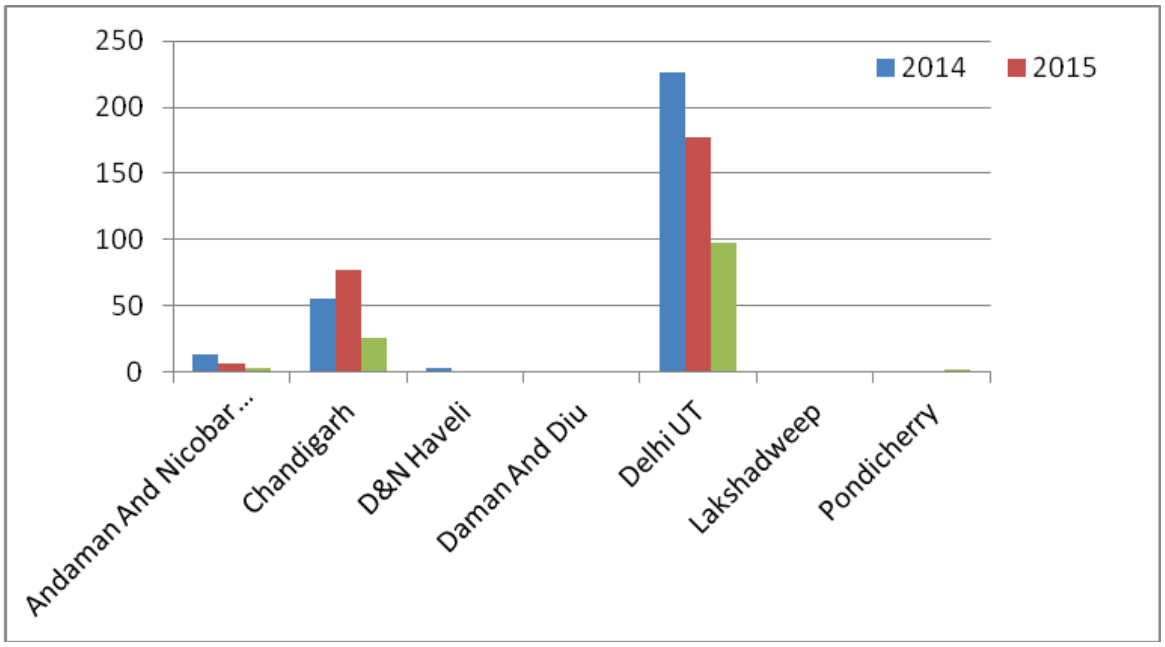

Fig. 2. Cyber Crimes in different Union territories [50]

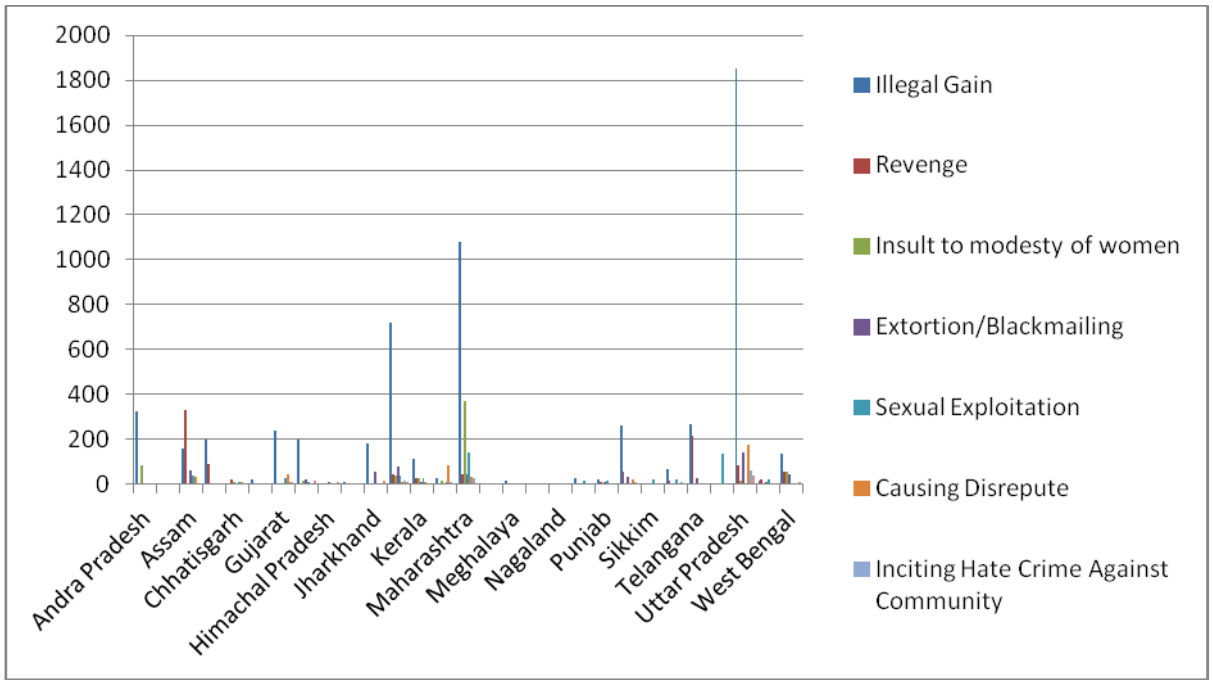

Fig. 3. Motives behind different Cyber Crimes [50]

Figure 3 represents the motive behind cyber crime in each state according to the data published in a report by the government of India in 2016[T1]. As we can see the main motive behind the cyber crimes was Illegal gain followed by revenge, insult to the modesty of women, extortion/blackmail, sexual exploitation, causing disrepute, inciting hate crimes against a community and developing own business/interest. We also see that the cases of cyber crime are extremely less in the eastern states like Mizoram, Meghalaya, Assam and Nagaland. Uttar Pradesh leads the charts with the highest no of cyber crimes followed by Maharashtra and Karnataka at second and third places respectively.

IX. CONCLUSION

The cyber criminal activities can be brought down with suitable measures and to find a solution to this issue, a detailed study of statistics of these activities and ways through which they are generally carried out are necessary. With more information on cyber-crimes, users can take more precautionary steps to ensure the safety of their devices or data and this brings more awareness to this matter hence resulting in more knowledge about the topic for users. The rates of cyber crimes are increasing in grand numbers and knowledge about this matter is needed.

ACKNOWLEDGEMENT

We would like to show our gratitude to our teachers, Mr. Rajnish Sharma and Mr. Kulbhusan Sharma who delivered immense knowledge to us and taught us everything. We would also like to thank our alloted guide, Mrs. Sarvesh Tanwar, who provided insight and whose guidance worked wonders for this manuscript and who helped us reduce our errors to a great extent. We thank Chitkara University for providing us with incredible faculty and this subject as a platform to learn about research papers.

REFERENCES

[1] Kuppuswamy, Prakash, et. al., "Preventing and securing data from cybercrime using new authentication method based on block cipher scheme", 2nd International Conference on Anti-Cyber Crimes (ICACC), IEEE, 2017.

[2] Lei, Lingguang, et. al., "A threat to mobile cyber-physical systems: Sensor-based privacy theft attacks on android smartphones", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2013

[3] Roberts, Lynne D., David Indermaur, and Caroline Spiranovic ,"Fear of cyber-identity theft and related fraudulent activity",Psychiatry, Psychology and Law,pp. 315-328, 2013

[4] https://www.techopedia.com/definition/2387/cybercrime, Accessed on 23 March 2019.

[5] Osho, Oluwafemi, Olasunkanmi Y. Ogunleke, and Adeyinka A. Falaye.,"Frameworks for mitigating identity theft and spamming through bulk messaging", 6th International Conference on Adaptive Science & Technology (ICAST), IEEE, 2014.

[6] Gugelmann, David, et. al., "Screen watermarking for data theft investigation and attribution", 10th International Conference on Cyber Conflict (CyCon), IEEE, 2018.

[7] Choo, Kim-Kwang Raymond., "The cyber threat landscape: Challenges and future research directions" ,Computers & security,pp. 719-731, 2011.

[8] Elmaghraby, Adel S., and Michael M. Losavio., "Cyber security challenges in Smart Cities: Safety, security and privacy", ,Journal of advanced research,pp. 491-497, 2014.

[9] Abraham, Subil, and Suku Nair, "Cyber security analytics: a stochastic model for security quantification using absorbing markov chains", Journal of Communications, pp. 899-907, 2014.

[10] Wang, Wenye, and Zhuo Lu, "Cyber security in the smart grid: Survey and challenges" ,Computer networks, pp. 1344-1371, 2013.

[11] Saini, Hemraj, Yerra Shankar Rao, and Tarini Charan Panda, "Cyber-crimes and their impacts: A review", International Journal of Engineering Research and Applications, pp. 202-209, 2012.

[12] Husák, Martin, et. al. , "Survey of attack projection, prediction, and forecasting in cyber security", ,IEEE Communications Surveys & Tutorials, pp. 640-660, 2018.

[13] Yan, Ye, et. al. , "A survey on cyber security for smart grid communications", ,IEEE Communications Surveys & Tutorials, pp. 998-1010, 2012.

[14] Conti, Mauro, Tooska Dargahi, and Ali Dehghantanha, “Cyber threat intelligence: challenges and opportunities”, Cyber Threat Intelligence, pp. 1-6, 2018, Springer, Cham.

[15] Kumar, Shipra Ravi, et. al. “Recommendations for effective cyber security execution.”, International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH). IEEE, 2016.

[16] Gupta Shalini, et. al. , “ Impact of cyber crime on adolescents through social networking sites”, International Journal of Law,vol.3[6],pp. 104-106,2017.

[17] Ahmed, Abu Shakil, et. al., “Simplistic Approach to Detect Cybercrimes and Deter Cyber Criminals”, 2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2), IEEE, 2018.

[18] https://www.acunetix.com/websitesecurity/sql-injection/,Accessed on 25 March 2019.

[19] Diallo Abdoulaye, et. al.,"A survey on SQL injection: Vulnerabilities, attacks, and prevention techniques." 2011 IEEE 15th international symposium on consumer electronics (ISCE). IEEE, 2011.

[20] https://www.w3schools.com/sql/sql_injection.asp, Accessed on 25 March 2019.

[21] Huber, Markus, et. al. , "Towards automating social engineering using social networking sites." 2009 International Conference on Computational Science and Engineering. vol. 3, IEEE, 2009.

[22] https://www.imperva.com/learn/application-security/social-engineering-attack/?utm_campaign=Incapsula-moved, Accessed on 25 March 2019.

[23] https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html, Accessed on 25 March 2019.

[24] Ogilvie, Emma. "Cyberstalking." Trends and Issues in Crime and Criminal Justice/Australian Institute of Criminology,2000

[25] https://searchsecurity.techtarget.com/definition/cyberstalking, Accessed on 26 March 2019.

[26] https://www.tripwire.com/state-of-security/security-awareness/what-cyberstalking-prevent/, Accessed on 26 March 2019.

[27] Carl, Glenn, et. al. "Denial-of-service attack-detection techniques." IEEE Internet computing, pp. 82-89,2006.

[28] https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/, Accessed on 10 April 2019.

[29] https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos,Accessed on 10 April 2019.

[30] https://www.cloudflare.com/en-in/learning/ddos/what-is-a-ddos-attack/, Accessed on 10 April 2019.

[31] https://www.digitalattackmap.com/understanding-ddos/, Accessed on 10 April 2019.

[32] https://www.acunetix.com/websitesecurity/cross-site-scripting/, Accessed on 23 April 2019.

[33] https://owasp.org/www-community/attacks/xss/, Accessed on 23 April 2019.

[34] https://money.howstuffworks.com/atm-skimming.htm, Accessed on 23 April 2019.

[35] https://whatis.techtarget.com/definition/piracy, Accessed on 23 April 2019.

[36] https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Eavesdropping%20attack, Accessed on 23 April 2019.

[37] https://www.veracode.com/security/man-middle-attack, Accessed on 23 April 2019.

[38] Nayak, Gopi Nath, and Shefalika Ghosh Samaddar. "Different flavours of man-in-the-middle attack, consequences and feasible solutions.", 2010 3rd International Conference on Computer Science and Information Technology, vol. 5, IEEE, 2010.

[39] Girault, Marc, Robert Cohen, and Mireille Campana,"A generalized birthday attack.",Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1988.

[40] https://www.malwarebytes.com/ransomware/, Accessed on 23 April 2019.

[41] https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html,Accessed on 23 April 2019.

[42] https://www.avast.com/c-topic-ransomware, Accessed on 23 April 2019.

[43] https://www.kaspersky.co.in/resource-center/threats/botnet-attacks, Accessed on 23 April 2019.

[44] https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html, Accessed on 23 April 2019.

[45] https://www.techopedia.com/definition/18091/brute-force-attack, Accessed on 23 April 2019.

[46] https://www.cloudflare.com/learning/bots/brute-force-attack/, Accessed on 23 April 2019.

[47] https://searchsecurity.techtarget.com/definition/brute-force-cracking, Accessed on 23 April 2019.

[48] Shinder, Debra Littlejohn, and Michael Cross, Scene of the Cybercrime, Elsevier, 2008.

[49] https://economictimes.indiatimes.com/tech/internet/bengaluru-is-indias-cybercrime-capital/articleshow/67769776.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst, Accessed on 27 April 2019.

[50] Crimes In India 2016, National Crime Records Bureau Ministry of Home Affairs, 10 October 2017, [ONLINE]. Available on ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf, 2016.

[51] Harshita, Sarvesh Tanwar, “Security Issues and Countermeasures of Online Transaction in E-Commerce” In Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, pp. 273-302. IGI Global, 2016.

[52] Tanwar Sarvesh et. al., “Design and Implementation of a Secure Hierarchical Trust Model for PKI” In Cyber Security, pp. 415-425. Springer, Singapore, 2018.