Pages : 5-14

# Cyber Crimes in India: A Review Paper

Aayushi Patel
Department of Information Technology and Computer Science
S. K. Somaiya College, Somaiya Vidyavihar University, Mumbai, India
aayushi.patel@somaiya.edu

## Abstract

As the nation is being fully occupied or covered by internet technologies .In other terms, we can say that the internet has trapped every human,online shopping, online studying, online jobs, every possible thing man can do with the medium of internet. By these advancements India as well as other countries are facing big issues related to the security of their data ,networks and personal information. To avoid this people should be aware of threats happening around the world.

In this review paper-types of cybercrimes, analyze the problem areas, main targets of hackers are going to be discussed. Also the paper suggests recommendations to strengthen India's defense against cyber frauds.

## Keywords

cybercrimes,ransomware,awareness,social frauds,ransomware,challenges,india

## 1.Introduction

Cybercrime refers to a criminal activity that is done through the use of computers and the internet.The attacker first follow the opponent or keep an eye to his/her networks and the security measures they use then at the right time they initiate the attack.The attacks like ransomware, phishing attacks are growing rapidly in India.The attackers harm other computer networks through installing malware or any suspicious account to their system ,hack and then steal their personal data/information. In India,there should be awareness regarding this cause so every single citizen should take primitive steps before and after the attack happens. “The Reserve Bank of India (RBI) reported that the ‘value of financial cyber crimes exceeded ₹615 crore in 2020, highlighting the increasing sophistication of phishing scams, unauthorized transactions, and data breaches targeting individuals and organizations alike”[1].Other major attack is increasing in india named ransomware in which the attackers hack the opponent's network and demands money to unlock the system. In 2020, over 50,000 cases of cybercrime were reported in India, marking a substantial increase from previous years [2].

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇
Received : 17 October 2024
Revised : 01 November 2024
Accepted : 02 December 2024

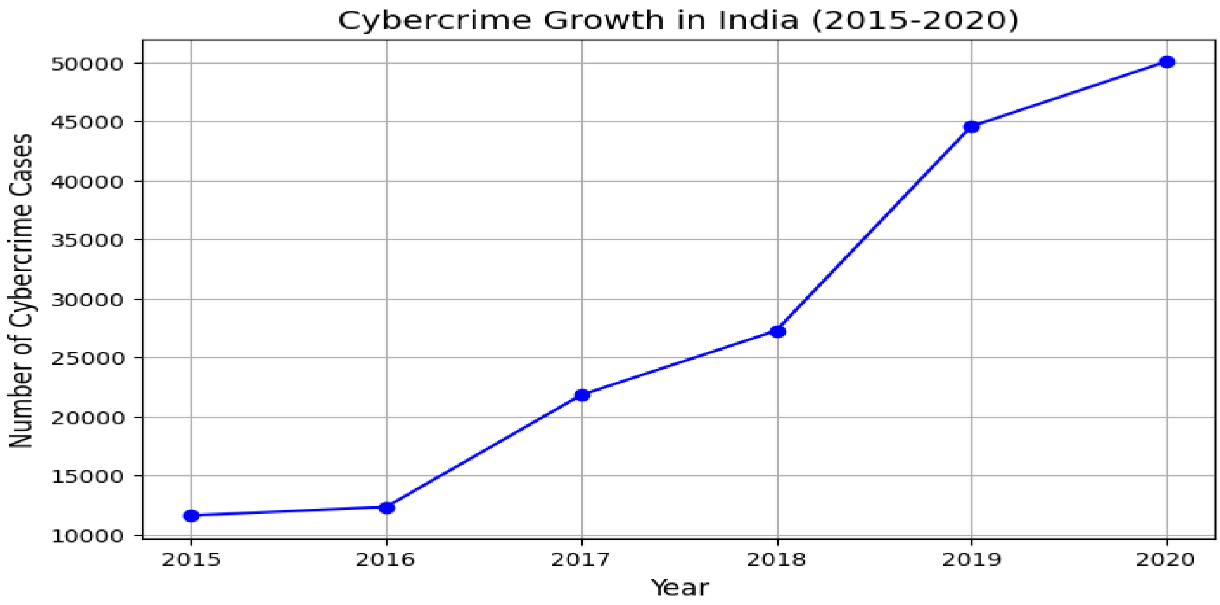

Figure 1:The figure shows the rapid growth of cybercrimes in the year 2020.Data generated using NCRB data.[3].

Another alarming trend is the expansion in ransomware attacks, with India ranking as the second-most affected country globally in 2021 [4].

Crimes like cyber stalking, online harassment have increased due to the increasing use of mobile phones.They use technology to target the person.It includes blackmailing the targeted person, releasing confidential information, posting fake information regarding the person etc.Due to instantly development of digitalization there are pros as well as cons of it.

This research review is done in a broadway which includes types of cybercrimes, increasing ratio of crimes in India,awareness, key challenges and primitive measures and future scope for improving the nation's cybersecurity.

## 2.Literature review

The literature surrounding cyber crimes in India showcase challenges,trends and strategies provided by researchers over the time. The review provides comprehensive inspection of gone by studies, areas requiring more research and findings.

A. Categories of Cyber Crime

There are several types of cyber crime in India.Gupta et al. (2020) categorize cybercrimes into:

~Financial frauds: Phishing attacks, credit card scams, and fraud online transactions.

~Identity theft: Stealing personal information to commit fraud.

~Ransomware: Attack initiated for the sake of money.

~Cyberterrorism: Attack through networks initiated between two countries.[5]

B. Cyber Crime during the COVID-19 Pandemic

The COVID-19 pandemic has resulted in a rise in cybercrime universally,India too.In that crucial period,all organizations and every single human being shifted to online work.

Due to exponential usage of the internet,the attacks increased at such a rate which leads to a high ratio of crimes in India.

According to Khan et al. (2021**)**, the figures of cyberattacks in India increased by 300% during the first few months of the COVID-19[6].

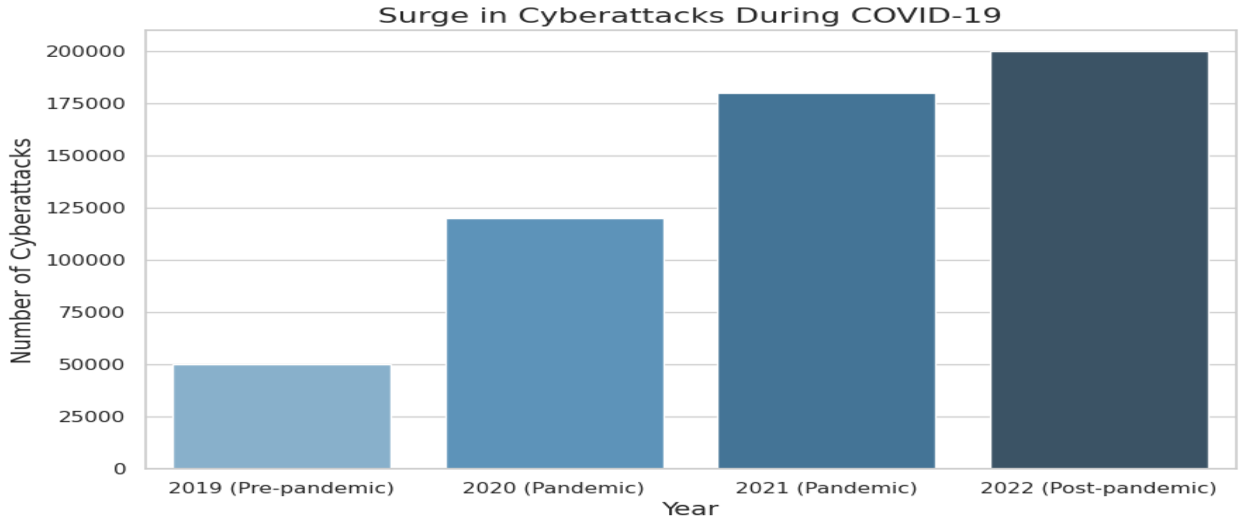

Figure 2:The figure shown, analyzes the exponential growth of pre-pandemic attacks and post-pandemic attacks.Mainly hospitals are targeted during this phase [7].

C.Government Initiatives and Legal Framework

In response to the increasing cyber threat, the Indian Government started taking various initiatives to minimize cybercrime. As the IT Act in 2000 forms the bedrock of India's cyber law, changes are also done with time to suit emerging threats. The Indian government established the Indian Cyber Crime Coordination Centre, I4C, in the year 2018, where all the efforts were coordinated from different legal enforcements. Experts believe that even with such attempts, the present legal system cannot be fully equipped to counter contemporary advanced cyber threats such as AI-driven attacks.[8]

In 2017, the government launched a new initiative known as Cyber Swachhta Kendra with an objective of creating awareness and aiding the users to protect their systems. However, the above schemes still require comprehensive success due to very low general population cybersecurity awareness levels.[9]

D. Rise in Cybercrime

Cybercrime has been one of the most prominent and significant crimes in India in the last decade, as it has also been conditioned by the growth in digitization of governmental services, banking and trading. The statistics from the NCRB indicate the rising trend of reported cybercrime cases in the country in the last few years, especially between 2015 and 2020. Cases of cybercrime reported over the years include a total of 11,592 in 2015 to 50,035 for the year 2020; summarized on NCRB reports.[10]

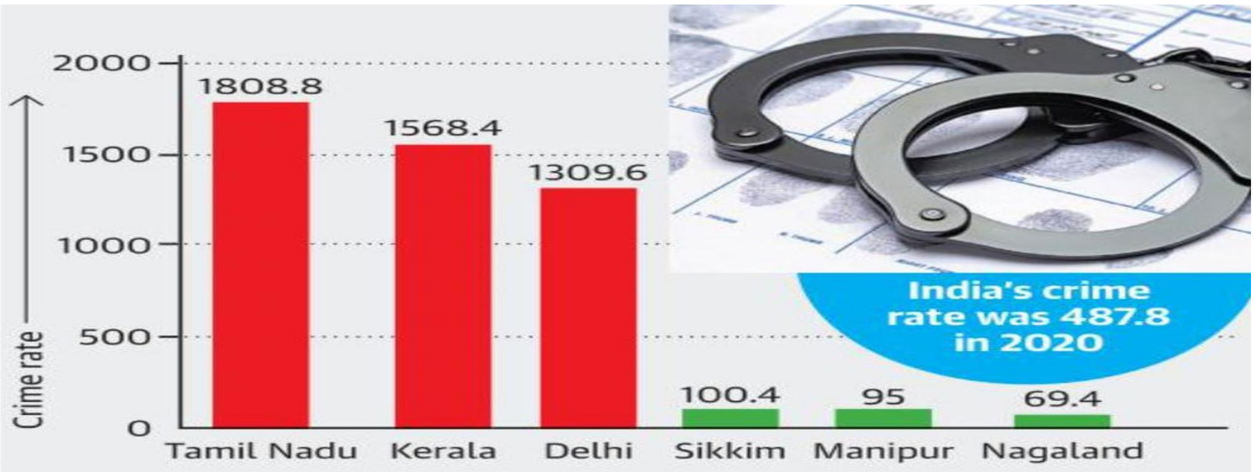

Figure 3:The above graph shows the rapid increasing growth seen in the year 2020 in India.[11].

E.Challenges during investigation of Cyber Crime

Cybercrime takes many forms and encompasses a range of criminal activities such as criminal psychology, while some are a direct attack on local jurisdiction. But even more interesting is the fact that Indian legislation on emerging threats corresponding to the growth of IT, has some relevant gaps. Striking is the fact that Indian law agency investigators are not computer literate.

Understanding the fundamentals of IP addressing is crucial as it enables the identification of the geographical location of the Internet user. It also controls several use registrations, allowing access to any of the local networks via another PC and allowing communication across two computers. The investigator must understand how each of these systems is designed, their functions and how to search for critical case information that has been contained in communications or earlier exchanges. Criminal policies have stayed static over time; investigators tend to suffer from lack of awareness of the variety of forms that digital media may come in and the formats that they may be located in the field.

There is the problem of the number and particularly the capacity of media, to be considered when submitting an application for search warrants where one suspects there is digital evidence; the number of hiding places for this type of storage is literally limitless.

In addition, as observed by CERT-In (2020), though some developments do exist in cybersecurity framework building, the cyber threats are always static in nature and outpace government efforts.

Moreover, instead of prevention of attacks, law enforcement agencies often have to be on the responding side of the attacks.[12]

F.Impact of Cyber Crime over teenager

This incorporates modern anxiety in the perspective of adolescents, also known as Cyber Bullying. It is becoming more and more prevalent over the past five years, generally those below eighteen are more prone and frightened from Cyber Bullying as per analysis. It is becoming an important trend in our society. All this is performed by means of core technologies as described above, mainly over the Internet. People can bully through various social platforms. In my interpretation, if an average feared person goes through a lot of depression, embarrassment and threats, then it is possible for him to reach a certain limit.As noted by Jha and Verma (2020), teens who have been harassed online have higher rates of anxiety and self-harm and sleeping disturbances[13].

Lacking face-to-face contact in the case of internet use, the aggressor can attack with relative impunity because no immediate consequences will occur, thus making the experience more emotionally devastating.

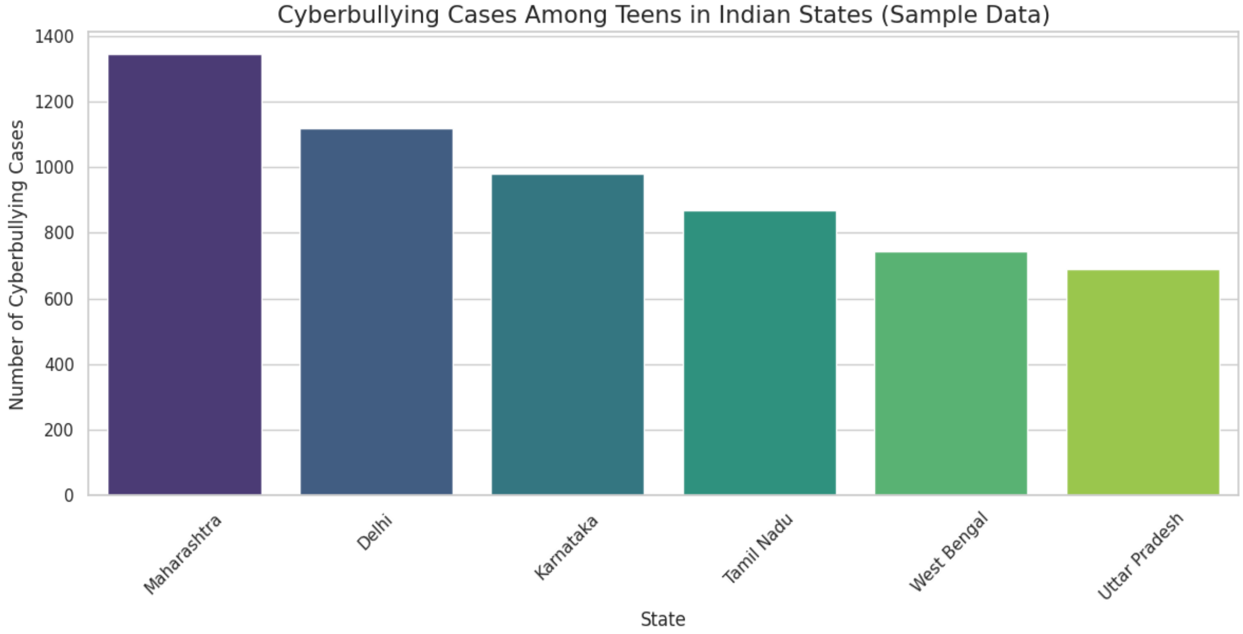

Figure 4: The bar illustrates the rise of cyber bullying cases in several states in India.[14]

G.Sexual Proposition

Another issue that is alarming for the youth of today who use forms of cyber communication is sexual solicitation. It is observed in different forums and even in social networks. Also, an online teenager could receive requests for disclosing his personal details, as well as for watching pornographic materials or even participating in an online sex talk.

About 70% of the teens that are sexually solicited on the internet are girls. There is a need for vigilance on the part of the teens while posting and sharing suggestive pictures and while interacting with unknown people on the net.

### H.Impact of Cyber crime over consumer behavior

There are two main causes of cybercrime on consumer behavior: first trust,Consumers are not trusting online environments or platforms due to break of trust and frauds happening all around the world.According to Accenture survey 2021,around 42% of customers fear to trust online platforms due to security risks and personal information leaks.[15]

There is a call to design models that would enable business organizations to carry out research on the effects of cybercrime on online consumer confidence and to complement this by finding remedies through benefits accruing from the latest developments in cyber security.On the other hand, it affects the online consumer with these two aspects of e-commerce that corporations must ensure that the measures they will execute will until consumers trust them.

Nair and Patel (2022) have found that 58% consumers today seek explicit security certifications, including SSL, ISO 27001, and other trust seals, before making online purchasing decisions[16]. Moreover, a consumer acts more safely when surfing the internet, such as using stronger passwords, updating the software regularly, and refraining from unverified websites[17].

### I.Impact of Cyber crime over Business

One of the negative effects of a cyber attack is that revenue drops dramatically because consumers run away to avoid cybercrime. The hackers also end up bleeding a company dry through extortion as well as erode the confidence of the investors who can withdraw interest, influence, and funds.

According to Ponemon Institute's 2022 study, 54% of customers said they would stop doing business with a company,if the company is not safe-how would they preserve the people's data[18].On the other hand people are also asking to companies for maintaining transparency.The main concern of consumers is data protection.

Businesses have started adopting protection measures and focus on Virtual Private Networks for securing access.In the recent report of Cisco's 2023 they analyze that over 78% of businesses have improved their security measures to implement a new work model.[19]After reviewing Fortinet's 2022 report,there is a strange increase in the number of phishing attacks by 600%.[20].Additionally people are taking cyber frauds insurance to compensate for the threat.

Analyzing McKinsey's 2023 report,they mentioned that many companies have adapted security measures and funding between 10-15% of their annual IT budgets[21]. According to the study carried out by Sophos in 2022,ransomware attacks covered 66% of organizations and these companies have to bear the downfall[22].
A study carried out by Accenture in 2022,they have found that cyberattacks aim to target small businesses which are not being prepared or defend themselves. [23]

## 3.Conclusion

The growth of cyber crime has increased at an exponential rate.The attacks like ransomware,data breaching,cyber stalking.harassment has reached its peak. Due to advancement in technology, every human has to face such challenges in their daily lives.The sectors like healthcare,education,big enterprises have been affected by these types of attacks.
Due to the increase of digital transactions,the financial frauds are becoming more challenging for the human to identify whether the opponent person is correct or a scam.Also major challenge is for small businesses who do not have a high budget to install quality security measures.

As India is becoming more digital,challenges like data hacking, stealing personal information, cyber terrorism,financial frauds are going to happen but primitive steps should be taken for the cause of public safety and maintaining the integrity of the nation.

For preventing cyber crimes one should know all the security measures like using strong passwords,always log out if you are surfing the internet in cybercafe,strengthen your home networks and many more.Through these measures one can be safe from several threats that are going to happen.

## 4.Future Perspectives

Rise in public awareness and providing education related to this crucial topic.The topics like how to detect cyber frauds,use strong passwords,don't click on malicious links.Adopting advanced technologies like Machine learning and Artificial Intelligence.These technologies help in detecting real time frauds,fraud analysis and decrease the risk of attack.

Team-up between private sector and government,because it is very essential for minimizing the risk of threats.They jointly can decrease the risk of frauds through technology sharing,fraud intelligence and can protect other sectors from being hacked.

India needs to build more knowledge in cyber security,it should be added into the curriculum and also offer training sessions. To reduce the gap in between,encourage people with the help of certificates. In this way the professionals become motivated and support the nation in this crucial period.

## 5.References

1.Reserve Bank of India. (2021). Financial cybercrime report 2020. RBI Annual Report.

2.National Crime Records Bureau. (2021). Cyber crime report 2020. Government of India.

3.National Crime Records Bureau. (2020). Crime in India 2020 - Statistics. Ministry of Home Affairs, Government of India.

4.Kaspersky Lab. (2022). Cyberthreats to Indian enterprises in 2021. Kaspersky Annual Threat Report.

5.Gupta, N., Agarwal, A., & Kumar, P. (2020). Cybersecurity in India's digital age. Computers & Security, 92, 29-41.

6.Khan, A., Ali, M., & Sharma, R. (2021). The impact of COVID-19 on cybercrime in India. Cybersecurity Review, 28(3), 66-75.

7.Cyber attacks in India during COVID-19. (n.d.). Economic Times.

8.Patel, V., & Singh, S. (2019). Challenges in implementing cybersecurity policies in India. International Journal of Cyber Law, 5(1), 100-115.

9.Mukherjee, S., & Rathi, K. (2021). Cybersecurity practices among SMEs in India: Challenges and opportunities. Journal of Information Systems, 33(2), 112-125.

10.National Crime Records Bureau. (2020). Crime in India 2020 - Statistics. Ministry of Home Affairs, Government of India.

11.CERT-In. (2020). Cybersecurity threats: A government perspective. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India.

12.Jha, S., & Verma, M. (2020). Cyberbullying and mental health consequences among teenagers. Youth & Adolescence Journal, 8(2), 80-92.

13.CyberPeace Foundation. (2022). Cyberbullying trends in India: A study on teenage vulnerability. CyberPeace Foundation.

14.Accenture. (2021). The digital trust imperative: Consumer confidence in the age of cybercrime. Accenture.

15.Nair, V. (2022). Consumer awareness of cybersecurity certifications: A new era in digital trust. Journal of Consumer Protection, 8(3), 101-115.

16.Patel, S. (2022). Consumer awareness of cybersecurity certifications: A new era in digital trust. Journal of Consumer Protection, 8(3), 101-115.

17.Ponemon Institute. (2022). Impact of data breaches on customer trust: A global study. Ponemon Institute.

18.Cisco. (2023). 2023 global hybrid work index: Security challenges and solutions. Cisco.

19.Fortinet. (2022). 2022 cybersecurity threat report: Phishing and remote work. Fortinet.

20.McKinsey & Company. (2023). The cybersecurity imperative: How companies are responding to rising cyber risks. McKinsey & Company.

21.Sophos. (2022). The state of ransomware 2022. Sophos.

22.Accenture. (2022). Cost of cybercrime 2022: How cyberattacks are impacting SMEs. Accenture.

23.McKinsey & Company. (2023). The cybersecurity imperative: How companies are responding to rising cyber risks. McKinsey & Company.