ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 8.4
IJAR 2023; SP4: 71-73

Prashant
Student, Master in Computer Application, DPG Degree College, Gurugram, Haryana, India

Shivani Sharma
Assistant Professor, Computer Science Department DPG Degree College, Gurugram, Haryana, India

Correspondence
Prashant
Student, Master in Computer Application, DPG Degree College, Gurugram, Haryana, India

(*Special Issue*)
"National Conference on
Multidisciplinary research for sustainable development"

Cyber Crime in India: A review

Prashant and Shivani Sharma

Abstract
Humans have benefited enormously from the widespread use of computers and the internet, but some people have taken advantage of this progress in unethical ways, such as online fraud, hacking, spamming, cyber terrorism, and cyber stalking. Any crime that includes a computer and a network is referred to as cybercrime, sometimes known as computer crime. Too many people are victims of cybercrime, which has been on the rise recently. The repercussions of cybercrime may be catastrophic, including monetary loss and reputational damage as well as psychological suffering and physical pain. Most of the victims are teenagers and elderly people. As a result, awareness campaigns are necessary to stop or avoid cybercrime in India. In this paper, the current state and types of cybercrime in India is examined.

Keywords: Cyber-crime, hacking, cyber space, cyber terrorism, cyber stalking, internet fraud

Introduction
Cybercrime is a growing problem in India, as more and more people go online for communication, commerce, and entertainment. Cybercrime refers to any illegal activity that involves the use of computer systems, networks, or devices, such as hacking, identity theft, fraud, malware, and cyberbullying. In recent years, cybercrime has become increasingly sophisticated, with attackers using advanced techniques to steal data, compromise systems, and evade detection.

India has experienced a significant rise in cybercrime in recent years, with reports suggesting that the country is among the top 10 nations targeted by cyber-attacks globally [1]. The rapid adoption of digital technologies in India has led to an increase in cybercrime, with criminals targeting individuals, businesses, and government organizations alike. Despite efforts to combat cybercrime, such as the creation of the Indian Computer Emergency Response Team (CERT-In), the problem continues to be a major challenge for law enforcement agencies in the country.

Types of Cyber Crime
1. **Hacking:** Hacking refers to gaining unauthorized access to a computer system or network to steal data, manipulate information, or cause damage.
2. **Malware:** Malware is any type of malicious software that can infect a computer system, including viruses, worms, Trojan horses, and ransomware.
3. **Phishing:** Phishing is a type of online scam where attackers send fraudulent emails or messages to trick individuals into revealing sensitive information, such as login credentials or financial data.
4. **Identity theft:** Identity theft involves stealing someone's personal information, such as their name, address, and social security number, to commit fraud or other illegal activities.
5. **Cyber stalking:** Cyber stalking involves using the internet, social media, or other digital communication platforms to harass, threaten, or intimidate someone.

6. **Online fraud:** Online fraud encompasses a range of scams, including romance scams, investment scams, and job scams that are designed to deceive individuals and steal their money or personal information.
7. **Distributed Denial of Service (DDoS) attacks**: DDoS attacks involve overwhelming a server or network with traffic to cause it to crash or become unavailable.
8. **Ransomware:** Ransomware is a type of malware that encrypts a victim's files and demands payment in exchange for the decryption key to unlock them.
9. **Cyberbullying:** Cyberbullying involves using technology to harass, intimidate, or bully someone, typically through social media or messaging platforms.
10. **Child grooming:** Child grooming is a form of online abuse where an adult uses the internet to build a relationship with a child for the purpose of sexual exploitation [2].

Rising Cyber Crime in India

The increased use of technology and internet access in India has contributed to an increase in cybercrime in recent years. With more people having access to the internet via smartphones and other devices, internet usage has considerably grown in India over the past few years.

Lack of awareness and education: Many people in India are not aware of the risks associated with using the internet and may not take necessary precautions to protect themselves from cybercrime. Additionally, there is a lack of education and training available to help individuals and organizations understand the risks and how to prevent cybercrime.

Inadequate cyber laws and enforcement: India's cyber laws are still evolving, and there are gaps in the legal framework that make it difficult to prosecute cybercriminals. Additionally, law enforcement agencies may not have the necessary resources and training to effectively investigate and prosecute cybercrime cases.

Cyber-attacks on businesses: Indian businesses are increasingly becoming targets of cyber-attacks, with cybercriminals seeking to steal sensitive information or disrupt operations. This has led to financial losses for businesses and created challenges for the Indian economy as a whole.

Cyberbullying and online harassment: With the rise of social media and other online platforms, cyberbullying and online harassment have become a significant problem in India. Victims of cyberbullying may experience emotional distress and may not know how to protect themselves.

To address the rising threat of cybercrime in India, it is important for individuals, organizations, and the government to take steps to improve cyber security measures, increase awareness and education, and strengthen laws and enforcement mechanisms.

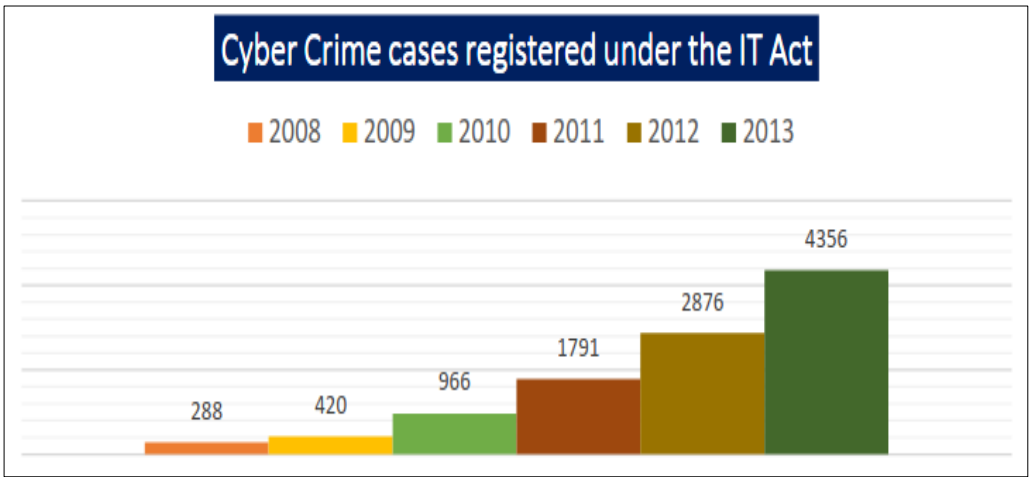

Fig 1: Cyber Crime cases [3]

According to data submitted to and recorded by CERT-In, there were 2,08,456, 3,94,499, 11,58,208, 14,02,809, and 13,91,457 cyber security incidents in each of the following years: 2018, 2019, 2020, 2021, and 2022.

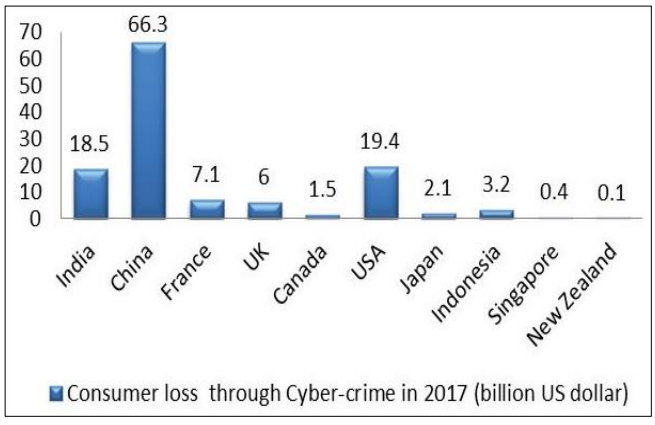

Fig 2: Consumer loss through Cyber Crime in 2017 [4]

Sectors prone to cyber-attacks in India

India, like any other country, has various sectors that are prone to cyber-attacks. Here are some examples of sectors in India that are commonly targeted by cybercriminals:

- **Banking and Finance:** Banks and financial institutions in India are highly targeted by cybercriminals due to the large amounts of financial transactions they handle and the sensitive financial data they store. Cyber-attacks on financial institutions in India can result in financial losses and reputational damage.
- **Healthcare:** The healthcare industry in India holds vast amounts of personal and sensitive information, making it a lucrative target for cybercriminals. Cyber-attacks on healthcare organizations can result in the theft of medical records, personal information, and other sensitive data.
- **Government:** Government agencies and institutions in India are frequent targets of cyber-attacks, as they hold sensitive information and provide critical services to

citizens. A successful cyber-attack on a government organization can result in the theft of sensitive information, disruption of services, and potential national security threats.

- **Telecommunications:** Telecommunications companies in India provide essential services to individuals and businesses, making them a target for cybercriminals seeking to disrupt services or steal sensitive data.
- **Energy and Utilities:** The energy and utilities sector in India provides critical services to communities and industries, making it an attractive target for cybercriminals seeking to disrupt operations or cause damage. Cyber-attacks on this sector can result in the disruption of energy supplies, power outages, and other serious consequences.

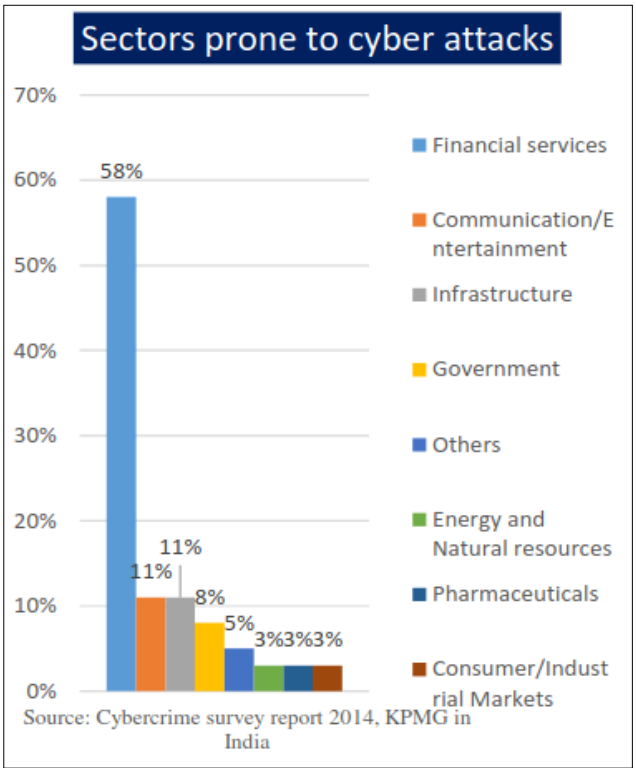

Fig 3: Sectors prone to cyber-Attacks [4]

Cyber-crime cases

There have been several high-profile cybercrime cases in India over the years. Here are some examples:

PNB Bank Fraud: In 2018, it was discovered that a group of hackers had stolen nearly $1.8 billion from India's Punjab National Bank (PNB). The hackers used fraudulent letters of undertaking to obtain loans from other banks, which were then transferred to overseas accounts [5].

Aadhaar Data Breach: In 2017, it was reported that the personal data of over 1 billion Indians had been compromised due to a security flaw in the government's Aadhaar database. The data included names, addresses, and biometric information [6].

Zomato Data Breach: In 2017, the personal data of over 17 million Zomato users was stolen by a hacker. The data included email addresses, usernames, and hashed passwords [7].

Conclusion

Above report demonstrates that India's rank is third on the world, where cyber-crimes are occurring frequently. Women, children and senior citizens of society are mostly affected by cyber-crimes according to various papers surveyed. Research works are increasing gradually in the field of cyber-crimes to understand the penetration level of it in the society. Banking Systems are very vulnerable to cyber-attacks. Almost in every day newspaper, we can have news regarding banking fraud cases. Due to this reason bank clients are now hesitant to utilize online banking services especially senior citizens, they still now in this digital era, stand in queue at banks to avail banking services. We need to protect ourselves from cyber-crimes and required to be very alert and aware about the latest types of scamming strategies for availing digital era benefits.

References

1. https://blogs.blackberry.com/en/2023/02/top-10-countries-most-targeted-by-cyberattacks-2023-report. 15 March; c2023.
2. https://www.vidhikarya.com/legal-blog/types-of-cyber-crime-and-prevention. 16 March 2023
3. Kumar PV. Growing cyber-crimes in India: A survey. In 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE). IEEE; c2016. p. 246-251.
4. Datta P, Panda SN, Tanwar S, Kaushal RK. A technical review report on cyber-crimes in India. In 2020 International Conference on Emerging Smart Computing and Informatics (ESCI). IEEE; c2020. p. 269-275.
5. https://www.linkedin.com/pulse/18-billion-punjab-national-bank-fraud-information-sakthivel/ 17 march,2023
6. https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html 17 March 2023
7. https://economictimes.indiatimes.com/small-biz/security-tech/security/zomato-hacked-security-breach-results-in-17-million-user-data-stolen/articleshow/58729251.cms?from=mdr17 March 2023