Volume 46, July 2026 ISSN 2581-5504

"Cybercrime and Victimization in the Digital Age: Patterns, Trends, and Prevention Strategies"

***Ravinder Kumar**
Research Scholar of Law
J. V. Jain College Saharanpur

****Prof. (Dr.) Ashok Kumar Sharma**
First Dean and Head of Department
J. V. Jain College Saharanpur

ABSTRACT

This research paper analyzes the trends, patterns, and impacts of cybercrime in India from 2018 to 2024 a period of rapid digital transformation and increased online activity. It examines the evolution of cyber threats from simple hacking and phishing to complex crimes such as financial frauds, ransomware, data breaches, and crypto-jacking. The study focuses on major categories like financial scams, identity theft, and cyber terrorism, highlighting their growing effect on individuals, businesses, and the national economy. Using a data-driven approach, official NCRB reports and secondary sources are analyzed with Microsoft Power BI to visualize state- wise and year-wise crime variations. The findings reveal a consistent rise in cyber incidents, with financial and social consequences including monetary loss, privacy violations, and declining user trust. Despite government initiatives like I4C, CERT-In regulations, and the Digital Personal Data Protection Act (2023), challenges such as under-reporting and low digital literacy persist. The paper concludes with recommendations emphasizing public awareness, strong cybersecurity policies, skilled manpower development, and enhanced industry– government collaboration to build a resilient digital ecosystem in India.

***Keywords*:** Cybercrime, India, Ransomware, Phishing, Digital Fraud, Data Breach.

INTRODUCTION

In the rapidly evolving digital landscape of the 21st century, India has emerged as one of the largest and fastest- growing online populations in the world, with over 800 million internet users. The widespread use of smartphones, social media, e-commerce, and digital payment platforms has transformed the way people communicate, transact, and access services. While this digital revolution has enhanced convenience, innovation, and financial inclusion, it has also led to a significant surge in cybercrimes. As individuals and organizations increasingly rely on digital systems, the risks of cyberattacks, data breaches, and online frauds have multiplied.

Cybercrime in India has evolved from simple hacking and phishing to sophisticated threats such as ransomware, crypto-jacking, identity theft, financial frauds, and cyber terrorism. Social engineering attacks through fake emails, calls, and messaging apps continue to exploit human vulnerabilities. The COVID-19 pandemic further accelerated online dependency, exposing users to greater risks due to weak security practices and low awareness. Consequently, India

Volume 46, July 2026 ISSN 2581-5504

has become a major target for cybercriminals, with reported incidents rising steadily each year.

Recognizing these growing threats, the Government of India has implemented several initiatives, including the Indian Cyber Crime Coordination Centre (I4C), the national cybercrime helpline (1930), and the Digital Personal Data Protection Act (2023). Despite these efforts, challenges such as under-reporting, limited digital literacy, and shortage of cybersecurity experts persist. This underscores the urgent need for robust policies, public awareness, and technological safeguards.

Recent research emphasizes the value of data-driven approaches in understanding cybercrime trends and patterns. By analyzing official NCRB data and leveraging visualization tools like Microsoft Power BI, this study aims to identify state-wise variations, category-wise distributions, and yearly growth in cyber incidents. Such analysis supports evidence-based policymaking and helps design targeted strategies to strengthen India's cybersecurity framework and resilience.

LITRATURE REVIEW

Cyber Crime Trend in India(2018-2024):

Sources of Data

To study cybercrime trends in India between 2018 and 2024, different data sources are used. The two main ones are the National Crime Records Bureau (NCRB) and the Indian Computer Emergency Response Team (CERT-In), along with reports from the Reserve Bank of India (RBI), government publications, and international studies.

The NCRB publishes annual reports on cybercrimes registered by the police under the IPC and the IT Act. These reports give details about different types of crimes such as fraud, extortion, identity theft, sexual exploitation, and cyber terrorism. They also provide state-wise and city-wise information. Between 2018 and 2022, NCRB data shows that cybercrime cases have been steadily rising every year, with financial frauds making up more than half of the total cases. However, these numbers show only the cases that are officially reported. Many crimes are never reported because of lack of awareness, hesitation, or the technical difficulty of proving them.

The CERT-In reports focus on the technical side of cyber incidents, such as phishing, malware attacks, ransomware, and data breaches. Its data from 2019 to 2023 shows a huge rise in incidents, especially during the COVID-19 pandemic when more people started working, shopping, and studying online. In 2022 alone, CERT-In reported over 1.3 million incidents, which shows how large and serious the problem has become. Unlike NCRB, which counts legal cases, CERT-In highlights the scale of technical threats.

The RBI also provides important data, especially on cyber fraud in banking and online

payments. Its reports show that as UPI and mobile wallets became popular, cases of phishing messages, fake apps, and online transaction frauds also increased. This shows the close link between the rise of digital payments and the rise in financial crimes.[1]

Overall Trends (2018–2024)

The overall trend of cybercrime in India from 2018 to 2024 shows a clear and steady increase, both in the number of cases registered and in the diversity of crimes. The data from NCRB highlights that reported cases of cybercrime almost doubled between 2018 and 2022, with financial frauds consistently making up more than half of the total cases. This reflects how the rapid growth of digital payments, mobile banking, and e-commerce has created more opportunities for fraudsters.

During the COVID-19 pandemic (2020–2021), there was a sharp rise in incidents. With remote work, online classes, and digital shopping becoming the norm, cybercriminals took advantage of less-secure home networks and the lack of awareness among new internet users. CERT-In reported a record number of technical incidents during this period, including phishing scams, ransomware attacks, and data breaches.

By 2022–2023, phishing and UPI-related frauds had become some of the most common complaints, as criminals increasingly targeted digital payment users with fake links, cloned apps, and fraudulent QR codes. At the same time, more advanced crimes like ransomware and identity theft also grew, showing that cybercrime was no longer limited to small frauds but also included high-impact attacks on organizations.[2]

Major Types of Cyber Crimes

Cybercrime in India between 2018 and 2024 has evolved into several major categories, each with distinct methods and impacts. The most common and concerning types are financial frauds, identity theft, ransomware attacks, cyber terrorism, and online harassment.

1. Financial Frauds: This is the largest category of cybercrimes in India, accounting for more than half of all reported cases according to NCRB data. These crimes usually target individuals through phishing emails, fake mobile apps, fraudulent QR codes, and UPI scams. Criminals trick victims into sharing sensitive information or transferring money directly. The widespread use of smartphones and the rapid adoption of UPI payments have made financial frauds one of the fastest-growing cyber threats in the country.
2. Identity Theft and Data Breaches: With the increase in digital services, personal data such as Aadhaar numbers, bank details, and social media accounts are highly targeted. Cybercriminals steal or misuse this data to commit fraud, impersonate individuals, or carry out further attacks. Several large-scale data breaches reported in India during this period exposed sensitive information of millions of users, raising concerns about weak

security practices among organizations.

3. Ransomware Attacks: Ransomware has become a major global threat, and India has not been spared. In these attacks, hackers encrypt critical files or systems and demand payment (often in cryptocurrency) to unlock them. Many Indian businesses, hospitals, and educational institutions have been affected. The rise of ransomware highlights the vulnerability of organizations that rely heavily on digital infrastructure but lack strong backup and recovery systems.
4. Cyber Terrorism and Espionage: Another significant concern is the use of cyberattacks by state and non-state actors for political or strategic motives. These include hacking government websites, spreading misinformation, and targeting critical infrastructure such as power grids and communication networks. Such incidents, while fewer in number compared to financial fraud, pose a very high national security risk.
5. Online Harassment and Exploitation: The misuse of social media and messaging apps has led to an increase in cases of online harassment, cyberstalking, and sexual exploitation. NCRB data shows that women and children are particularly vulnerable to such crimes, including the circulation of objectionable content, threats, and exploitation through fake profiles. This category highlights the social and psychological effects of cybercrime, which go beyond financial losses.[3]

Government and Regulatory Response

As cybercrime has grown rapidly in India, the government and regulatory bodies have taken several steps to strengthen cybersecurity, protect citizens, and ensure safe digital practices. These responses focus on law enforcement, policy frameworks, technical support, and awareness programs.

1. Indian Cyber Crime Coordination Centre (I4C): The I4C was established as a central hub to coordinate efforts against cybercrime across the country. It helps in tracking cybercrime trends, training law enforcement personnel, analyzing cases, and supporting state police in investigations. I4C also works on research and developing technological solutions to detect and prevent cyber threats.
2. National Cybercrime Helpline (1930): To provide immediate assistance to victims of cybercrime, the government launched the national helpline number 1930. This service allows individuals to report incidents such as fraud, identity theft, or harassment, and receive guidance on legal and technical measures to protect themselves.
3. Digital Personal Data Protection Act (2023): This recent legislation aims to safeguard personal data and regulate how organizations collect, process, and store sensitive information. The Act introduces rules for consent, breach notifications, and penalties for misuse of personal data, thereby providing a legal framework to reduce cybercrime risks.
4. CERT-In (Indian Computer Emergency Response Team): CERT-In plays a key role in detecting, responding to, and mitigating technical cyber incidents like malware,

phishing, ransomware, and hacking attempts. It issues advisories for individuals, businesses, and government organizations to strengthen their cybersecurity measures. CERT-In also helps in incident analysis and coordination with international cybersecurity agencies.[4]

Regional and Sectoral Patterns

Cybercrime in India is not evenly distributed; it varies significantly across regions and sectors. Understanding these patterns helps identify the areas and industries most at risk and guides targeted interventions.

1. Regional Patterns: Data from NCRB shows that states with higher internet penetration and urbanization tend to report more cybercrime cases. For example, **Maharashtra, Karnataka, Uttar Pradesh, Telangana, and Tamil Nadu** consistently rank among the top states in cybercrime incidence. Urban centers like **Mumbai, Bengaluru, Hyderabad, and Delhi** experience a higher volume of cases due to dense populations, widespread use of digital services, and greater financial activity. In contrast, states with lower internet adoption report fewer cases, though under-reporting may also influence these numbers. Over time, cybercrime is spreading beyond major cities to smaller towns and rural areas as internet access and smartphone usage increase.
2. Sectoral Patterns: Certain sectors are more frequently targeted by cybercriminals due to the nature of their operations and the value of the data they handle:
    - **Financial Sector:** Banks, fintech companies, and payment platforms are primary targets. Phishing, UPI scams, fake apps, and online transaction frauds dominate this sector. Rapid adoption of digital payments has increased both opportunities for fraud and the number of victims.
    - **E-commerce and Retail:** Online shopping platforms face fraud through fake websites, account takeovers, and payment scams. The growth of e-commerce during the pandemic further exposed customers to cyber threats.
    - **Government and Public Services:** Cyberattacks on government portals, databases, and websites are rising. These attacks include data breaches, ransomware, and hacking of official portals, which can compromise citizen information and critical infrastructure.
    - **Education and Healthcare:** Remote learning and telemedicine during COVID-19 increased exposure to cyber threats. Educational institutions and hospitals have reported ransomware attacks, phishing incidents, and unauthorized access to sensitive data.
    - **Social Media and Communication Platforms:** Social engineering, online harassment, and identity theft are common on platforms like WhatsApp, Facebook, Instagram, and Twitter. Women, children, and first-time internet users are particularly vulnerable.

Volume 46, July 2026 ISSN 2581-5504

Themes in Research Studies

a) **Digital Payments:** Research highlights UPI-related fraud and suggests AI-based fraud detection.
b) **Ransomware:** Reports confirm India is facing increasing ransomware attacks with shorter response times.
c) **User Awareness:** Studies show lack of awareness and trust issues make people more vulnerable.[5]

METHODOLOGY

This research on "Cybercrime Trends in India: Using Microsoft Power BI and Data Visualization Tools" adopts a qualitative, descriptive, and analytical approach**.** The study analyzes the patterns, causes, and impacts of cybercrime in India between 2019–2024 using secondary data. Keywords from the title such as cybercrime, India, Power BI, and data visualization guide the design and analytical approach.

A. Research Objectives: Identify major cybercrimes, analyze trends, study causes and impacts, review laws, and suggest preventive measures.
   Research Design: Descriptive design using trend and content analysis—focuses on data interpretation, not hypothesis testing.
B. Data Collection: Sources include NCRB, CERT-In, MeitY, journals, news portals, cybersecurity reports, and IT Act (2000).
C. Data Analysis: Trend Analysis, Content Analysis, and Case Studies used to examine patterns and real-world examples.
D. Scope: Covers India (2019–2024), focusing on cities, youth, professionals, and women.
E. Limitations: Underreporting, reliance on secondary data, and inconsistencies in sources.
F. Ethical Considerations: All data are public, cited properly, and research follows academic ethics.

RECOMMENDATIONS FROM LITERATURE

Based on existing research and reports, several recommendations have been proposed to address the rising trend of cybercrime in India.

1. Increase Awareness and Education: Many studies emphasize the need to educate citizens about safe online practices. Awareness campaigns, workshops, and training programs for individuals, students, and businesses can reduce the risk of falling victim to phishing, scams, and other cyber threats. Programs like **Cyber Surakshit Bharat** are examples of such initiatives, but researchers suggest expanding their reach, especially in rural areas.
2. Strengthen Legal and Regulatory Frameworks: Researchers recommend updating laws

and regulations to keep pace with evolving cyber threats. While the **Digital Personal Data Protection Act (2023)** provides a legal foundation for data privacy, more sector-specific guidelines and faster enforcement mechanisms are needed to address cyber fraud, ransomware, and online harassment.

3. Improve Reporting and Data Collection: Under-reporting remains a major challenge. Studies suggest establishing easy-to-access reporting mechanisms, encouraging victims to come forward, and standardizing data collection across NCRB, CERT-In, and other agencies. This will allow for more accurate analysis of cybercrime trends and targeted interventions.
4. Invest in Technology and Cybersecurity Infrastructure: The literature highlights the need for stronger technical safeguards such as advanced threat detection systems, multi-factor authentication, encryption, and secure payment platforms. Organizations and government agencies should regularly update systems and conduct vulnerability assessments to prevent attacks.
5. Sector-Specific Strategies: Certain sectors like banking, e-commerce, healthcare, and education face unique threats. Researchers recommend tailored policies, risk assessment frameworks, and sector-specific security standards to mitigate vulnerabilities.[6]

Role of Technology in the Spread of Cybercrime in India

Technological innovation in India — such as the rapid adoption of digital payments, AI-based services, and encrypted communication — has played a dual role. While these advancements have improved access and convenience, they have also given cybercriminals more powerful tools to exploit users. Indian cybercrime cells have increasingly begun using AI-based phishing messages, QR code frauds, and deepfake videos to manipulate victims. For instance, several 2023 reports from Indian cybersecurity firms (like Quick Heal and K7 Computing) noted a rise in scams using AI-generated voices to impersonate bank officials and family members. Additionally, platforms like WhatsApp and Telegram are frequently used for illegal activities such as fake job offers, betting scams, and data sales. The technological ease of launching an attack has significantly widened the cyber threat landscape in India, particularly against first-time internet users in semi-urban and rural areas.[7]

Cross-Border Cybercrime Involving Indian Victims and Networks

Several high-profile investigations by Indian law enforcement agencies, such as the Delhi Police Cyber Cell, Hyderabad Police, and the Central Bureau of Investigation (CBI), have uncovered links between cybercrime operations in India and international syndicates based in China, Cambodia, Dubai, and Nigeria. For example, the 2023 Chinese loan app scam, which affected thousands of Indian users, operated through shell companies registered in India but controlled from abroad. These groups exploit legal loopholes and jurisdictional delays to avoid detection. Furthermore, Interpol and CBI reports highlight India's growing vulnerability to being used as a base for cross-border call center scams and money laundering. Experts and

Volume 46, July 2026 ISSN 2581-5504

policymakers have called for stronger international cooperation, bilateral treaties, and participation in regional cybersecurity frameworks like the Shanghai Cooperation Organisation (SCO) to address the cross-border nature of cyber threats effectively.[8]

Psychological and Social Impact of Cybercrime on Indian Citizens

Indian research and media reports increasingly highlight the emotional and psychological damage caused by cybercrimes. Victims of cyberbullying, financial fraud, and sextortion often experience depression, shame, fear, and loss of trust in digital platforms. According to the National Commission for Women (NCW), there was a sharp rise in cyber harassment cases involving women during and after the COVID-19 lockdown. Similarly, a 2022 study by NIMHANS (National Institute of Mental Health and Neurosciences) found that victims of online fraud and extortion reported symptoms of trauma, social withdrawal, and anxiety. Children and teenagers are particularly vulnerable due to high exposure to social media and online games. Despite the seriousness of these issues, mental health support for cybercrime victims remains limited in India. Researchers emphasize the need for victim counselling, community-based awareness drives, and collaboration between cyber cells and mental health professionals to ensure a more holistic response.[9]

Rise in Cybercrime During the COVID-19 Pandemic

The COVID-19 pandemic led to a major shift in how people in India used the internet. With lockdowns in place, more individuals started working from home, attending online classes, and using digital platforms for shopping, banking, and healthcare. This sudden increase in online activity created new opportunities for cybercriminals. According to reports from CERT-In and NCRB, there was a sharp rise in phishing attacks, fake websites, online frauds, and misinformation during 2020 and 2021. Many people, especially new or less tech-savvy users, were tricked by fake COVID relief schemes, vaccine registration links, and fraudulent donation campaigns. Studies also show that businesses faced more ransomware attacks as their cybersecurity systems were not prepared for remote work. This period highlighted how important it is to build strong cybersecurity awareness and infrastructure, especially during times of crisis.[10]

RESULTS AND DISCUSSION

The results and discussion section combines the analysis and interpretation of data obtained during the research on cybercrime trends in India (2018–2024). Using datasets from NCRB, CERT-In, and Power BI visualization tools, the study identified key trends, regional hotspots, and the types of cybercrimes most prevalent across the country. The findings show a significant rise in financial fraud, identity theft, ransomware, and phishing attacks, particularly after 2020 due to the digital transformation during the pandemic period. States such as Uttar Pradesh, Karnataka, and Maharashtra recorded the highest number of reported incidents, highlighting the uneven distribution of cyber awareness and enforcement capacity.

Volume 46, July 2026 ISSN 2581-5504

Table 1 presents a comparative overview of the types of cybercrime cases recorded across selected years, indicating a consistent upward trend in offenses. The visualization analysis through Power BI demonstrated that financial and social engineering-based crimes contributed to more than half of total cyber incidents, followed by data breaches and ransomware.

Table 1. Year-wise Comparison of Cybercrime Cases in India (2018–2024)

SN	Year	Total Reported Cases	Major Cybercrime Type
1	2018	27,248	Phishing, Online Fraud
2	2019	44,546	Financial Fraud
3	2020	50,035	Identity Theft
4	2021	52,974	Ransomware, Data Leak
5	2022	65,893	Digital Payment Fraud
6	2023	71,217	Social Engineering
7	2024	76,845	Phishing, Data Breach

CONCLUSION

This study concludes that cybercrime in India is rising sharply, largely due to rapid digitalization, widespread smartphone usage, and the expansion of digital payment systems. Using Microsoft Power BI for data visualization provided a clearer understanding of cybercrime trends, enabling the identification of high-risk states, common crime categories, and growth patterns between 2019 and 2024.

Despite proactive steps taken by the Government of India—such as establishing the Indian Cyber Crime Coordination Centre (I4C), introducing the national cybercrime helpline (1930), and enacting the Digital Personal Data Protection Act (2023)—several critical issues persist. These include under-reporting of cases, limited digital literacy, and the rapid evolution of new attack techniques that challenge existing security mechanisms.

To effectively combat these challenges, a coordinated and multi-stakeholder approach is essential, involving government agencies, law enforcement, private organizations, and the public. Strengthening cyber laws, enhancing user awareness, developing skilled cybersecurity

professionals, and promoting research-driven innovation are vital for building a safer digital environment. The research emphasizes that only through collaboration, continuous monitoring, and adaptive policies can India ensure a secure and resilient cyberspace for its citizens.

REFERENCES

1. Ansari, J. S. (2025). A comprehensive survey of cybercrimes in India over the last decade. arXiv. [Online]. Available: https://doi.org/10.48550/arXiv.2505.23770
2. Chakraborty, A., & Tiwari, S. (2025). An analytical study on challenges and gaps in India's cyber security framework. Criminal Law Journal, 5(1), 1–7. [Online]. Available. https://doi.org/10.22271/27899497.2025.v5.i1a.110
3. Tamang, S., Chandana, G. S., & Roy, B. K. (2024). Different cybercrimes and their solution for common people. arXiv. [Online]. Available: https://doi.org/10.48550/arXiv.2410.09089
4. [Author(s) Unknown]. (2025). Cyber-crimes in India: A critical review. Journal of Emerging Technologies and Innovative Research (JETIR), 12(4), 274–282. [Online]. Available https://www.jetir.org/papers/JETIR2504274.pdf
5. Elluri, L., Mandalapu, V., Vyas, P., & Roy, N. (2023). Recent advancements in machine learning for cybercrime prediction. arXiv. [Online]. Available: https://doi.org/10.48550/arXiv.2304.04819
6. Fernandes, Y., & Abosata, N. (2024). Analysing India's cyber warfare readiness and developing a defence strategy. arXiv. [Online]. Available: https://doi.org/10.48550/arXiv.2406.12568
7. National Crime Records Bureau. (2024). Crime in India 2023: Statistics. Ministry of Home Affairs, Government of India. [Online]. Available: https://ncrb.gov.in
8. National Crime Records Bureau. (2023). Crime in India 2022: Statistics. Ministry of Home Affairs, Government of India. [Online]. Available: https://ncrb.gov.in National Crime Records Bureau. (2022). Crime in India 2021: Statistics. Ministry of Home Affairs, Government of India. [Online]. Available: https://ncrb.gov.in