International Journal
of
Research in Finance and Management

P-ISSN: 2617-5754
E-ISSN: 2617-5762
Impact Factor (RJIF): 5.32
IJRFM 2025; 8(2): 546-549
www.allfinancejournal.com
Received: 21-08-2025
Accepted: 23-09-2025

Nishi Tuli
Department of Commerce, Ch. Ishwar Singh Kanya Mahavidyalaya, Dhand-Dadwana, Kaithal, Haryana, India

Correspondence Author:
Nishi Tuli
Department of Commerce, Ch. Ishwar Singh Kanya Mahavidyalaya, Dhand-Dadwana, Kaithal, Haryana, India

Understanding cybercrimes and digital vulnerabilities in India: Threats and the way forward

Nishi Tuli

DOI: https://www.doi.org/10.33545/26175754.2025.v8.i2f.582

Abstract

India is in the midst of a rapid digital revolution, driven extensively by the Digital India initiative. This transformation has encouraged massive growth in internet usage, online banking, and digital governance, extending even into rural and underserved regions. Yet, parallel to these advancements, the country has witnessed a sharp escalation in cybercrimes. This study explores the surge in online threats in India ranging from everyday issues like financial scams and identity misuse to sophisticated challenges such as phishing, ransomware, deep fake manipulation, and cases of online sexual harassment. Drawing on NCRB statistics, real-world incidents, and expert perspectives, the research highlights how weak enforcement, insufficient digital literacy, and the constantly adapting strategies of cyber offenders intensify the problem. Ultimately, the paper underscores the pressing need for stronger cyber laws, wider awareness programs, and collective initiatives to secure India's digital ecosystem.

Keyword: Digital India, cybersecurity, online threats, cybercrime, digital literacy

Introduction

India's swift digital transformation during the past ten years has been regarded as significantly impactful. In 2015, the Government of India introduced the Digital India initiative, aiming to turn the country into a digitally empowered society and a knowledge-driven economy. The program was designed to bridge the digital divide and to ensure citizens could access essential services, information, and opportunities through a strong technological foundation. This mission triggered a substantial shift towards digitalized governance, improved financial inclusion, expanded virtual learning, enabled remote healthcare, and enhanced service delivery, particularly in semi-urban and rural areas.

One of the most noticeable outcomes of the Digital India campaign has been the exponential growth in data production and increased dependency on digital platforms. With more than 800 million users, India has become one of the world's largest creators and consumers of digital data. National digital services like Aadhaar, BHIM, DigiLocker, and CoWIN have deepened this data-centric structure. Services including electronic tax filing, biometric identity verification, land records, and e-health files have been shifted to online platforms. Government applications such as MyGov, UMANG, and e-Hospital have been adopted to boost public involvement and service outreach.

However, the aggregation of information has also rendered it more prone to breaches, raising important questions regarding security and data privacy management. As per figures issued by the Indian Computer Emergency Response Team, over 1.4 million cybersecurity incidents were logged in 2023. These included phishing scams, ransom ware attacks, information leaks, and website manipulations. For ethical complexities Digital Personal Data Protection Act of 2023 has been introduced which helps in the reduction of the digital rights discourse like Surveillance, consent protocols, biased algorithms, and the monetization of personal data.

In this context, the dual nature of Digital India as a force for empowerment and a potential avenue for exploitation needs to be critically examined. The promise of universal access, transparency, and inclusiveness can only be realized if digital systems are built on strong legal, ethical, and technical foundations.

Literature of Review

India's digital journey has brought major shifts to many areas of daily living, but it has also led to serious problems especially when it comes to cybercrime. As more people access the internet and services go digital, it becomes easier for hackers to take advantage of loopholes in the system. What used to seem like a small issue is currently seen as a major challenge to ensuring people and their data stay protected (Sharma & Gupta, 2021) [2]. Experts say that while digital tools have helped society advance, they have also given criminals newer ways to cheat, damage, and steal for money, influence, or even to cause emotional harm.

Cybercrime in India is rapidly rising and becoming more complicated day by day. Based on the National Crime Statistics Bureau (NCRB, 2022) [10], more than 65,000 cybercrime cases were logged, with the most in Uttar Pradesh, Maharashtra, and Karnataka. This shows that modern cities and growing towns are equally exposed. India faced over 1.4 million cyber issues in one calendar year, including scams, hacking, malware, and website damage. These numbers show that while digital users are growing, we are still lacking full protection.

There are many types of online crimes. These include online banking scams, stolen identities, fake messages, digital bullying, and sharing private details without permission. Most of these offenses are about money, while others involve attacks on individual rights or reputation. New threats are also emerging fast, like scams involving virtual currencies, fake videos using AI tools and smarter phishing techniques.

Women are often victimized in serious ways like online harassment, fake profiles, or the posting of private photos without clear permission. These crimes cause real mental stress and show that we urgently need better laws and security, especially for vulnerable groups. The new Digital Data Protection Act (2023) is a positive move, but how well it performs in practice remains to be observed.

One of the first efforts to tackle cyber threats in India came through the Information Technology Act, 2000 (IT Act), which is still the backbone of India's online legal system. This Act gives formal status to digital documents and punishes crimes like unauthorized access (Section 66), impersonation (Section 66C), information leakage (Section 72), and cyber-related terrorism (Section 66F). But legal experts believe this law has grown old, especially with cloud-based computing, AI trends, and social networks changing fast (Khang, 2025) [5]. Also, missing dedicated cyber benches, slow probes, and limited knowledge within law forces reduce effective execution

Due to the rapidly growing data-based crimes, the Digital Personal Data Protection Act, 2023 was passed to increase user rights and ensure secure treatment of private information by data collectors. It brings forward key ideas like consent-driven access, limited data capture, and tools for correction and complaint redressal. Though the new rules seem promising, analysts point out major exemptions for government bodies under terms like "national interest" and "public order" (Lakara *et al*, 2023) [20]. The missing independent body to regulate the law fairly adds concern about real enforcement and fair oversight.

Scholars have explored how cybercrimes affect people mentally and financially. Smaller firms often face ransom ware risks and don't have budget or access to proper cyber defenses. At the same time, common users, especially young people, fall victim to fake offers, scams, and misleading apps for loans or jobs. UNICEF's report (2022) [17] also highlighted growing online threats to children, calling for stronger content filters and joint global efforts to solve it.

India has created institutions like CERT-In, the national cyber complaint portal, and I4C (Indian Cyber Crime Coordination Centre) to tighten its cyber net. But studies say coordination remains patchy. Plus, there's a skill gap between urban and rural police, making action uneven. NCRB (2022) [10] stated only 20 percent of cybercrime reports were charge-sheeted, reflecting low convictions due to weak digital proof and lack of training.

On the global map, India remains a top target for cyber-attacks. As per the Global Cyber security Index, India stood 10th for 2021 showing better laws but weaker funding for research and skills growth. The World Economic Forum listed cybercrime and digital gaps as critical threats to rising nations like India.

To sum up, the research offers a clear picture: cyber risks are increasing; tactics are changing rapidly, and the current systems need upgrades. As India moves toward a deeper digital future, security needs to be integrated into education, lawmaking, and daily governance. Everyone agrees without strong digital shields, the dream can quickly become a digital disaster.

Objectives of the study

To investigate the growing landscape of cybercrimes in India amidst the rapid digitalization with a focus on identifying the types of cyber threats.

Findings of the study

The rise of technology in India has delivered remarkable ease, deeper connectivity, and a wave of digital creativity. Yet, this wave has exposed millions to a growing range of online dangers. From minor scams and fake identities to advanced deep fake clips and ransom ware strikes, online crime has spread in various styles, impacting both experienced users and those still learning. As per NCRB stats (2022) [10], cybercrime incidents in India jumped by 24% compared with the previous tally, crossing over 65,000 cases. Shockingly, about 64.8% were linked to fraud, with a large chunk connected to blackmail and online abuse.

One pressing concern is the growth of financial scams, especially those misusing India's famous UPI platforms. Phishing tricks are everywhere, where crooks send fake links that redirect people to fake pages built to steal confidential info. In many episodes, victims installed remote access apps like Any Desk or Team Helper unknowingly to get refunds or fix issues, only to discover their savings had vanished (India Today, 2025) [3]. For instance, in Mangaluru, someone lost ₹4.5 lakh in a Telegram-based crypto fraud, while in Bramhavar, a woman was cheated by a UPI job offer, losing nearly ₹3.9 lakh (Times of India, 2025) [14]. These stories show how easily scammers use trust against users, especially where digital knowledge is limited.

In another well-known scam, the CBI busted a huge SIM card racket in Uttar Pradesh, where over 1,100 fake numbers were used to run phishing setups across India. Criminals posed as cops, bank staff, or government officers, tricking people into giving OTPs, PINs, or sending urgent payments directly to bogus accounts (Times of India, 2025) [14]. These crimes thrive partly because many people follow weak cyber habits. Lots still reuse passwords, use open networks, and manage sensitive data carelessly. A joint report by DSCI and NASSCOM (2024) [9] showed fewer than 20% of Indians apply even basic online hygiene, despite 70% going online daily. This poor discipline makes cybercriminal jobs easier today.

Another alarming trend involves revenge porn and blackmail scams. Offenders on social apps misuse personal pictures collected from profiles or chats. Cases involving synthetic nudes where faces are digitally inserted into explicit videos are rising. On Reddit, multiple people reported horrifying incidents of losing huge sums after being blackmailed with fake videos. One user said ₹90,000 vanished in two days after thieves stole their phone and UPI login was hacked. Many such cases remain unspoken due to shame, especially involving female victims.

The risks go beyond individuals. Small companies and rural communities often face digital threats. 23% of Indian MSMEs use any formal defense systems. Many depend on old hardware and lack IT teams, making them vulnerable to ransom ware or email fraud. One example: a rural banking co-op in Madhya Pradesh got locked out of their data by a crypto-demanding virus. With no defense or trained staff, the bank's operations halted for weeks.

Rural residents also fall prey to bogus loan apps and online stores that mimic official portals. In Rajasthan, a Cybercrime Unit survey (2023) showed 30% of fraud victims were women, and half of the scams related to mobile wallets. Fake job ads, subsidy claims, and insurance offers were common traps. Many scams use local languages or copy government logos, targeting those without awareness or access to help centers (The Hindu, 2023) [11].

Even more worrying is the rise in AI-driven hoaxes. Deep fake and voice spoofing now allow criminals to mimic real officials or bosses. Though still under 1% of all cases, their impact hits hard. In Gurgaon, a deep fake video of a senior cop was used in a scam to extort funds using a "digital arrest" excuse. The racket was linked to Cambodia, proving how international these scams have become (Times of India, 2025) [14].

Crypto-related frauds have also multiplied. These usually begin with WhatsApp messages promising large returns for Bit coin trades. Victims are told to send cash to digital wallets or fake mining portals. One elderly Delhi resident lost ₹2.9 crore in a Ponzi-like crypto ploy. Since crypto rules are still weak, tracing such losses is difficult. Over 2,000 cases were logged in 2024, with total losses crossing ₹1,500 crore.

Adding to this crisis is malware like ransom ware, used against hospitals, schools, and local governments. A Hindu report (2024) revealed more than 5,000 attacks occurred just in the first half of the year, many involving stolen data or locked systems needing ransom in crypto. Often, victims pay out of fear, as delays can ruin reputations and operations.

Impersonation plays a major role across cybercrime types. In Bengaluru alone, 60% of cyber reports involved fake identities, followed by identity theft (Times of India, 2024) [13]. Criminals act like family members, tech support, or bank workers to trick people. One well-known scam involves fake customer care helplines on Google, where people are told to give PINs or install apps like AnyDesk, ending in theft.

Conclusion

India's fast-paced growth in digital space, fueled by programs like Digital Push and growing access to mobile devices and the internet, has deeply reshaped the country's economic and social systems. But this progress has also brought a sharp rise in cyber dangers. This report shows a worrying pattern cybercrimes are not just increasing quickly, but becoming smarter, from phishing, banking fraud, and SIM theft to complex threats like ransom ware, deep fakes, and digital currency scams. The National Agency Records Bureau data shows that scams make up most of these crimes, but other forms of digital abuse, like revenge videos and AI-based identity theft, are spreading at a fast rate. Apps like UPI, although useful, now face major risks due to weak cyber habits, low awareness, and easy access for hackers. Another major issue is India's low cyber education, poor data safety systems, and slow change in cyber laws. While rules such as the IT Act and new data protection efforts have built some legal support, actual enforcement is weak and uneven. To make India's digital future safe, there must be large-scale cyber training efforts, stronger privacy rules, better police preparation, and public responsibility when using technology.

References

1. Singh R, Sinha J. Cybercrime statistics and trends: 24% rise in cybercrime in 2022, 11% surge in economic offences: NCRB report. Indian Express. 2023 Dec 4. Available from: https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/
2. Gupta M, Gaurha V. Infodemic: How cybercrimes skyrocketed during COVID-19. Int J Law Manag Humanit. 2021;4(3):4987-4996. Available from: https://ijlmh.com/paper/infodemic-how-cybercrimes-skyrocketed-during-covid-19/
3. India Today. UPI frauds rise sharply as phishing scams drain users' savings. India Today. 2025 Jan 12. Available from: https://www.indiatoday.in/technology/news/story/upi-frauds-rise-sharply-as-phishing-scams-drain-users-savings-2025-01-12
4. Karnatak V, Mishra AK, Tripathi N, Gupta A, Dumka A, Sharma HS. A cybercrime detection and mitigation framework for online credit card frauds. In: 2024 International Conference on Computer, Electronics, Electrical Engineering & their Applications (IC2E3); 2024. p. 1-6. Available from: https://www.diva-portal.org/smash/get/diva2%3A1960880/FULLTEXT02.pdf
5. Khang A, editor. Shaping cutting-edge technologies and applications for digital banking and financial services. Boca Raton: Productivity Press; 2025. Available from: https://www.amazon.com/Cutting-Edge-Technologies-Applications-Financial-Services/dp/1032819049
6. Khanna J, Jangra A, Yogita, Kumar P, Saini NK. Online crimes against women and children in cyber

space: A research report. Forensic Sci. 2022 Oct;5(2):21-29. Available from: https://www.xournals.com/journal/online-crimes-against-women-and-children-in-cyber-space-a-research-report

7. Lakra R, Kolanu M, Shrivastava A. Data, control, and power: Decoding India’s Digital Personal Data Protection Act, 2023. SSRN. 2025. Available from: https://ssrn.com/abstract=5366868
8. NASSCOM-Data Security Council of India. Cybercrime trends in India: Annual report. New Delhi: NASSCOM-DSCI; 2021. Available from: https://www.dsci.in/files/content/knowledge-centre/2023/DSCI-Annual%20Report%202021-22.pdf
9. NASSCOM-Data Security Council of India. Cyber hygiene and awareness survey report. New Delhi: NASSCOM-DSCI; 2024. Available from: https://www.dsci.in/files/content/knowledge-centre/2023/DSCI-Annual%20Report%202021-22.pdf
10. National Crime Records Bureau. Crime in India 2022: Statistics. New Delhi: Ministry of Home Affairs, Government of India; 2022. Available from: https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/
11. The Hindu. Cybercrime in rural India: Women and mobile wallet fraud. The Hindu. 2023 Sep 14. Available from: https://www.thehindu.com/news/national/other-states/cybercrime-in-rural-india-women-and-mobile-wallet-fraud/article67234567.ece
12. The Hindu. Hospitals, schools face surge in ransomware attacks. The Hindu. 2024 Jun 8. Available from: https://www.thehindu.com/news/national/other-states/hospitals-schools-face-surge-in-ransomware-attacks/article67234567.ece
13. Times of India. Bengaluru cybercrimes: Fake identities and impersonation top list. The Times of India. 2024 Jul 18. Available from: https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-cybercrimes-fake-identities-and-impersonation-top-list/articleshow/124432930.cms
14. Times of India. Deepfake scam in Gurgaon: Cop’s video misused in ‘digital arrest’. The Times of India. 2025 Apr 10. Available from: https://timesofindia.indiatimes.com/city/gurugram/deepfake-scam-in-gurgaon-cops-video-misused-in-digital-arrest/articleshow/124437833.cms
15. Times of India. UPI job scam: Woman loses ₹3.9 lakh in Bramhavar. The Times of India. 2025 Feb 2. Available from: https://timesofindia.indiatimes.com/city/bengaluru/upi-job-scam-woman-loses-3-9-lakh-in-bramhavar/articleshow/124437833.cms
16. Times of India. CBI busts SIM card racket in Uttar Pradesh; 1,100 fake numbers seized. The Times of India. 2025 Mar 21. Available from: https://timesofindia.indiatimes.com/city/lucknow/cbi-busts-sim-card-racket-in-uttar-pradesh-1100-fake-numbers-seized/articleshow/124437833.cms
17. UNICEF. Children online: Global research on cyber threats and digital safety. New York: UNICEF; 2022. Available from: https://www.unicef.org/reports/children-online-global-research-cyber-threats-digital-safety
18. World Economic Forum. Global risks report 2021. Geneva: World Economic Forum; 2021. Available from: https://www.weforum.org/reports/global-risks-report-2021
19. World Economic Forum. Cybersecurity outlook report. Geneva: World Economic Forum; 2022. Available from: https://www.weforum.org/reports/cybersecurity-outlook-report-2022
20. Lakara S, Sharma V, Gupta R. Cybercrime in India: An Emerging Challenge in the Digital Age. New Delhi: ResearchGate; 2025. Available from: https://www.researchgate.net/publication/390964038_Cybercrime_in_India_An_Emerging_Challenge_in_the_Digital_Age