North Asian International Research Journal of Social Science & Humanities

ISSN: 2454-9827 Vol. 11, Issue-11 November-2025

IRJIF I.F. : 3.015

Index Copernicus Value: 57.07 Indian Citation Index Thomson Reuters ID: S-8304-2016

NAIRJC A Peer Reviewed Refereed Journal

INCREASING CYBERCRIME IN INDIA: TRENDS, CAUSES, IMPACTS AND POLICY RESPONSES

DR ASHIQ HUSSAIN MALIK

E-mail: aashiqmalik5@gmail.com

ABSTRACT

India has experienced a sharp rise in cyber incidents over the last several years. This paper synthesizes government statistics, industry reports and academic studies to describe trends (volume and type of incidents), examine drivers (digital adoption, fintech growth, social engineering, weak policing capacity), measure socio-economic impact (financial losses, privacy breaches), evaluate institutional responses (CERT-In, NCRB reporting, helplines, legislative updates), and provide actionable recommendations to reduce risk. Key findings show a substantial year-on-year rise in incident counts and financial losses, with fraud dominating reported cases; improvements in reporting and incident handling coexist with capacity and coordination gaps that must be addressed.

KEYWORDS: ***Cybercrime in India, Digital fraud, Cyber security, CERT-In, NCRB cybercrime data, online financial fraud, Phishing attacks, Ransom ware, Social engineering, Digital literacy***

1. INTRODUCTION

Rapid digitalization (internet/ mobile penetration, UPI/online banking adoption, digital government services) has delivered economic and social benefits for India but also expanded the attack surface for cybercriminals. Official statistics and independent reports indicate considerable increases in cyber incident volumes and associated economic losses in recent years. This paper aims to quantify those trends, identify root causes, and evaluate responses at technical, legal, and social levels.

2. LITERATURE REVIEW AND BACKGROUND

Several recent studies and government releases document the growth of cybercrime in India and globally. The National Crime Records Bureau's Crime in India 2023 report reported an increase in recorded cybercrimes (noting fraud as the dominant category), while CERT-In and industry bodies (DSCI) report large numbers of security incidents handled annually and provide threat-landscape analysis. Scholarly articles emphasize social engineering, phishing, and fraud as recurring themes; public-sector reporting initiatives (e.g., National Cyber Crime Reporting Portal) have improved visibility but also reveal investigation and prosecution challenges.

3. DATA AND METHODS

This study synthesizes multiple data sources for 2019–2024/2025 where available: NCRB (Crime in India 2023), CERT-In annual incident statistics, Ministry of Home Affairs/Press Information Bureau releases on cyber incidents and government actions, industry threat reports (DSCI India Cyber Threat Report 2025), and reputable press coverage of major breaches and financial loss figures. Where raw microdata are unavailable, trend descriptions follow the cited sources' aggregated numbers.

4. FINDINGS / TRENDS

4.1 Volume of incidents

CERT-In reported handling over 2.04 million incidents in 2024, signaling a very high operational caseload for national incident response. Government releases also indicate cyber security incidents rose substantially between 2022 and 2024. These high numbers reflect both an increase in attacks and greater reporting/visibility.

4.2 Recorded cybercrime cases (police statistics)

NCRB's Crime in India 2023 shows registered cases under cybercrimes rising (e.g., from ~65,893 in 2022 to ~86,420 in 2023), with fraud-related offences constituting the majority. Regional variation is notable: some states show sharp percentage increases.

4.3 Economic impact

Government data presented to Parliament and media reporting indicate dramatic increases in financial losses: one government disclosure reported losses of roughly ₹22,845 crore in 2024 — a steep year-on-year jump. This highlights how cyber fraud has moved from isolated incidents to sizable fiscal impact.

4.4 Attack types and vectors

Frequent incident types include phishing, banking/UPI frauds, SIM swap and identity-theft schemes, business email compromise (BEC), ransomware and data leaks/exfiltration. Social engineering and targeted fraud remain dominant modes for monetary gain. Industry threat reports note increasing automation (botnets, scam-broadcasters) and data-market activity.

5. CAUSES AND ENABLING FACTORS

5.1 Expanding digital footprint

Rapid adoption of internet services, mobile banking, e-commerce and digital identity systems increases exposure; the majority of households are now online, enlarging the pool of potential victims.

5.2 Economic incentives and monetization routes

Easy monetization via UPI and other instant payment rails, resale markets for stolen data, and cryptocurrency channels (for some attackers) make cybercrime profitable.

5.3 Human factors and low digital literacy

Users with limited awareness of phishing, OTP/credential safety, and safe device usage are more likely to fall victim. Social-engineering attacks exploit trust in messages and calls appearing to come from banks or officials.

5.4 Law-enforcement and capacity gaps

While reporting mechanisms and national response have improved, state/UT police investigation capacity, forensic capability, cross-jurisdictional coordination, and prosecution pipelines lag relative to incident growth. Delays in FIR conversion and limited cyber forensic specialists hamper effective legal redress.

5.5 Organized and professionalized criminal groups

Attacks increasingly show professional models: specialized roles (malware development, money mules, data brokers), use of automated tooling, and cross-border operations complicate attribution and enforcement.

6. CASE STUDIES

- **Large insurer data leak (Star Health, 2024)**: Reported data exfiltration and leak via Telegram chatbots highlighted risks to personal health data and the scale of sensitive records at risk. The incident highlighted the challenges of detecting and containing large exfiltrations
- **Mass financial fraud patterns**: Government reporting and media coverage document schemes involving SIM cloning/SIM swap and social-engineering calls that drained bank accounts or persuaded victims to transfer funds. The aggregated financial loss figures reflect many such incidents.

7. INSTITUTIONAL AND POLICY RESPONSES

7.1 CERT-In operational role

CERT-In handles incident reporting and technical coordination over 2 million incidents handled in 2024 while also issuing advisories and facilitating mitigation. However, the sheer volume strains resources.

7.2 NCRB reporting and National Cyber Crime Reporting Portal

Greater emphasis on centralized reporting (cybercrime.gov.in) and improved data collection helps visibility and policy design but does not automatically translate into faster prosecutions.

7.3 Government funding and initiatives

Budgetary allocations and helplines (e.g., the national cybersecurity helpline 1930) reflect governmental prioritization of the problem. Public-private partnerships and industry initiatives (DSCI, CERT-In collaborations) contribute threat intelligence and capacity building.

7.4 Legal framework

Existing laws (IT Act, IPC provisions) and proposed/upgraded rules seek to provide enforcement tools, but implementation challenges (evidence collection, cross-border cooperation) remain important hurdles.

8. DISCUSSION GAPS AND CHALLENGES

- **Under-reporting & attribution:** Many victims do not report fraud due to stigma or perception of low recovery; attribution is technically and legally difficult, especially with cross-border actors.
- **Capacity bottlenecks:** State police cyber units are uneven in capability; forensic labs and trained cyber-investigators are in short supply.
- **Public awareness:** Digital literacy campaigns exist but need to scale and tailor messages to local languages and contexts.
- **Private sector responsibilities:** Financial institutions and large platforms must improve anomaly detection, anti-fraud controls, and faster customer recourse processes.

9. RECOMMENDATIONS

9.1 Strengthen reporting → investigation pipeline

Improve conversion of portal complaints into timely FIRs and equip state agencies with trained cyber forensic teams and standardized procedures for evidence preservation.

9.2 Expand CERT-In and state SOC capacity

Scale incident-handling capacity, regional CERT coordination, and public-private threat-sharing. Invest in automation to triage high volumes of alerts.

9.3 Financial sector controls and customer protections

Banks and payment firms should implement stricter multi-factor authentication, transaction-anomaly detection, and faster reversible measures for contested transfers. Regulators should mandate fraud-reporting timelines.

9.4 National digital literacy acceleration

A nationwide, multilingual digital safety curriculum (schools, workplaces, community centres) focusing on phishing, OTP safety, SIM security, and privacy settings.

9.5 Legal and international cooperation

Strengthen mutual legal assistance treaties (MLATs), expedite cross-border takedowns, and harmonize evidence standards for cyber investigations.

9.6 Data minimization and corporate security hygiene

Mandate minimum cybersecurity standards for large data holders (healthcare, insurance), periodic audits, and breach disclosure norms to incentivize security investments.

10. CONCLUSION

Cybercrime in India is rising in both volume and economic impact. The trend is driven by rapid digital adoption, financially motivated fraud, and persistent human-factor vulnerabilities, combined with the professionalization of criminal activity. India has put in place many building blocks CERT-In, reporting portals, helplines, and budgetary measures — but must scale technical capacity, strengthen law enforcement pipelines, and invest in preventive public education to curb the trend. Coordinated, multi-stakeholder action (government, industry, civil society) will be essential to reduce harm and preserve the benefits of digital transformation.

REFERENCES

1. National Crime Records Bureau Crime in India 2023 (summary coverage). The Indian Express
2. Indian Computer Emergency Response Team (CERT-In) Annual incident statistics / Annual Report 2024. CERT-IN
3. Press Information Bureau / Ministry of Home Affairs “Curbing Cyber Frauds in Digital India” (Oct 2025 briefing with incident trends). Press Information Bureau
4. India Cyber Threat Report 2025 Data Security Council of India (DSCI). Data Security Council of India
5. Media reporting: Times of India “India’s cyber fraud epidemic: Rs 22,845 crore lost in 2024” (reporting government figures). The Times of India
6. Reuter’s major breach reporting (Star Health incident). Reuters