GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 14, Issue 02, Feb 2026 Impact Factor: 8.466

www.aarf.asia,**Email** : editoraarf@gmail.com

An Analytical study of Cyber-crime in Indian Banking Sector

Dr. Rupali Prakash Kotwal
Commerce, Management & Computer Science College, Nashik.
Affiliated by Savitribai Phule Pune University, Pune.

Abstract

The Indian banking sector has undergone an unprecedented digital transformation in the past decade, driven by rapid adoption of online transactions, digital payments, mobile banking and financial technologies. While this evolution bolstered by initiatives like Pradhan Mantri Jan-Dhan Yojana (**PMJDY)** has democratized access to finance. It has simultaneously introduced a complex array of cyber threats. In 2026, the landscape of digital financial threats in India has moved past simple scams into a high-stakes "AI-driven arms race." As India processes nearly 46% of the world's real-time digital transactions, the banking sector has become the primary target for organized cybercriminal networks. Cybercriminals exploit technological vulnerabilities, weak cyber hygiene and growing digital footprints to commit fraud, siphon funds, breach data, and compromise systems. This paper examines the nature and scale of cybercrime in Indian banking, analyzes the primary causes and trends, evaluates impacts, reviews case studies, legal frameworks and proposes recommendations for strengthening cyber security.

Keywords: Cyber Crime**,** Financial Frauds, Digital Banking, Cyber security, Fintech

Introduction

Cybercrime involves unlawful acts conducted through digital platforms such as computers, smartphones, communication networks, and the internet, with the objective of stealing sensitive information, interrupting digital services, or causing monetary damage. In the banking industry, cybercrime has become a major concern as financial institutions increasingly rely on digital channels to deliver services. Typical cyber threats faced by banks include internet banking fraud, phishing scams, malicious software attacks, identity misuse, unauthorized fund transfers, ATM skimming, ransomware incidents, and breaches of confidential customer data.

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 14, Issue 02, Feb 2026 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

India's banking sector faces heightened cyber risk due to the speed and scale of its digital expansion. The widespread adoption of systems such as the Unified Payments Interface (UPI), mobile wallets, internet banking platforms, and instant fund transfer services has led to an exponential rise in digital transaction volumes. A large segment of users—especially new adopters from rural and semi-urban regions—access banking services primarily through mobile devices. Limited awareness of online safety practices among some users increases their vulnerability to fraudulent calls, fake websites, deceptive messages, and harmful mobile applications. Official data highlights the seriousness of the issue: Between January 2020 and June 2023, over **75% of cybercrime cases in India were financial frauds**, many tied to banking and digital transactions. As digital banking continues to grow, it is essential for banks, regulators, and customers to collectively focus on stronger cyber security measures, enhanced user education, and effective regulatory frameworks to maintain confidence in the digital financial system.

Overview of Digital Banking in India

India's banking sector has rapidly evolved into a digital powerhouse, with technology transforming how consumers and businesses access financial services. In calendar year 2024, digital payments accounted for ~99.7% of all transaction volumes and ~97.5% of total transaction value, reflecting near-universal adoption of electronic channels over cash and cheques.

- **UPI and Mobile Wallets:** The Unified Payments Interface (UPI) has become the backbone of India's retail payment system. In 2024, UPI processed over 17,221 crore (172.21 billion) transactions, up sharply from 1,079 crore in 2019, with a transaction value of ₹246.8 lakh crore — and H1 2025 alone saw 10,637 crore UPI transactions worth ₹143.3 lakh crore. Mobile wallets and UPI apps (like PhonePe, Google Pay, and BHIM) contribute to the massive billions of transactions monthly, often exceeding 18–20 billion UPI payments per month in 2025.
- **Online & Mobile Banking Apps:** Major banks (e.g., SBI YONO, HDFC Bank MobileBanking, ICICI iMobile) provide apps for account access, bill payments, loans, and investments, reducing reliance on physical branches and enhancing convenience.

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 14, Issue 02, Feb 2026 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

- **NEFT, RTGS, and IMPS:** Traditional inter-bank systems remain vital. NEFT volumes more than tripled from 262 crore in 2019 to 926 crore in 2024, while IMPS doubled to ~594 crore, and RTGS grew to 29.5 crore transactions handling large-value transfers.
- **Fintech Partnerships & APIs:** Banks and fintech firms collaborate through API-based services to integrate payments, lending, account aggregation, and investment tools, expanding reach and creating seamless solutions.

While digital finance democratizes access and supports financial inclusion, it also broadens the cyber risk landscape with rising fraud, phishing, and scam cases tied to increased online activity, prompting stronger security and awareness efforts.

Scope and Scale of Cybercrime in Indian Banking

I. National Crime Data Trends

According to the National Cyber Crime Reporting Portal (NCRP*)* and government disclosures:

- In **2024**, **36,37,288 cybercrime cases** were filed, up sharply from previous years.
- Financial losses due to cyber fraud in India exceeded **₹22,845 crore (~$2.7 billion)** in 2024.
- Registered cybercrime complaints increasing year on year: from ~10.29 lakh in 2022 to ~15.96 lakh in 2023 and ~22.68 lakh in 2024.

These figures reflect both higher reporting and a rising trend of cyber fraud, much of which involves banking and financial fraud.

II. Banking Sector Specific Incidents

Bank-level data illustrates how cyber threats have impacted core players:

- **State Bank of India (SBI)** recorded nearly **16,000 cyber fraud cases** across branches between 2024 and 2025, leading to significant financial losses.
- Other banks, including private and scheduled commercial banks, also regularly report fraud cases related to ATM, online banking, mobile apps, and fraudulent accounts.

III. Types of Cybercrime in Banking

The most frequent forms of cybercrime affecting Indian banks include:

1. Bank Account and Online Banking Fraud: Bank account and online banking fraud

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 14, Issue 02, Feb 2026 Impact Factor: 8.466

www.aarf.asia,**Email** : editoraarf@gmail.com

involves unauthorized access to customer accounts and illegal fund transfers. In India, such scams account for nearly 30–35% of total banking cybercrime cases. Criminals exploit weak passwords, compromised credentials, or unsecured devices to perform unauthorized transactions, causing significant financial losses to banks and customers.

2. Phishing and Social Engineering: Phishing and social engineering attacks use fake emails, SMS, calls, or websites to steal login credentials and OTPs. Reports indicate that over 60% of banking-related cyber frauds originate from phishing scams. Fraudsters impersonate banks or government agencies, exploiting customer trust and lack of awareness to gain access to sensitive banking information.

3. Malware and Ransomware Attacks: Malware and ransomware attacks involve malicious software infiltrating banking systems or customer devices. In 2024, malware-related incidents accounted for nearly 15–20% of reported banking cyber-attacks. Ransomware encrypts data and demands payment, disrupting banking operations, compromising customer information, and causing financial and reputational damage to institutions.

4. ATM and Card Skimming: ATM and card skimming fraud uses physical devices or digital malware to capture debit or credit card details. Around 10–12% of card-related frauds in India include skimming techniques. Criminals install skimming devices on ATMs or compromise POS terminals, enabling cloning of cards and unauthorized withdrawals from customer accounts.

5. Identity Theft and KYC Data Breaches: Identity theft involves misuse of personal and KYC data such as Aadhaar, PAN, or bank credentials. Nearly 20% of financial cybercrime cases involve identity theft or data breaches. Stolen data is used to open fake accounts, apply for loans, or conduct fraudulent transactions, increasing financial and legal risks for banks.

6. Payment and UPI Fraud: UPI and digital payment fraud includes unauthorized transfers, fake collect requests, and deceptive QR codes. In 2024, UPI-related frauds added to above 40% of digital payment fraud cases. Instant transactions, combined with limited user awareness, allow fraudsters to quickly siphon funds before detection or recovery is possible.

7. Internal Collusion: Internal collusion involves bank employees abusing privileged access or sharing confidential data with fraudsters. Studies indicate that **8–10% of major banking frauds** involve insider participation. Weak internal controls, inadequate monitoring, and lack

of employee background checks increase the risk of internal misuse of sensitive banking systems and customer information.

Recent news reports indicate specialized syndicates using fake APKs to harvest banking credentials, multi-state mule accounts to launder funds, and international links to sophisticated organized cybercrime rings.

Causes of Rising Cybercrime in Indian Banking

Several interrelated factors contribute to the surge:

1. Rapid Digital Adoption: India's rapid shift to digital banking has significantly expanded the cyber-attack surface. In 2024, UPI alone processed over 10 billion transactions per month, while mobile banking users exceeded 300 million. Each digital platform adds multiple endpoints, increasing vulnerability to cyber-attacks, unauthorized access, and transaction fraud.

2. Insufficient Cyber Awareness: Despite widespread digital banking usage, cyber awareness remains low among users. Studies indicate that nearly 60% of cyber fraud victims fall prey to phishing, fake links, or OTP sharing. Limited understanding of cyber security practices, especially among first-time digital users, increases susceptibility to social engineering and financial scams.

3. Weak Security Implementation: Cyber security readiness varies across Indian banks, particularly among cooperative and regional banks. Reports suggest over 40% of banking systems still rely on legacy infrastructure. Delayed adoption of multi-factor authentication, real-time threat monitoring, and advanced encryption creates security gaps, making systems vulnerable to malware and intrusion attacks.

4. Organized Crime and Technology Sophistication: Cybercrime has evolved into organized, technology-driven operations. In 2024, over 70% of large-scale banking frauds were linked to organized networks using AI-based phishing, bots, and encrypted malware. Cross-border syndicates, mule accounts, and automated attacks enable criminals to evade detection and launder stolen funds efficiently.

Impacts of Cybercrime on the Banking Sector

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 14, Issue 02, Feb 2026 Impact Factor: 8.466

www.aarf.asia,**Email** : editoraarf@gmail.com

1. Financial Losses: Cybercrime causes significant financial losses to banks and customers through unauthorized transactions, fraud, and data breaches. In 2024, losses exceeding ₹22,000 crore highlight the severe economic impact. Such losses affect bank profitability, increase reimbursement costs, and strain insurance and risk management systems.

2. Reputational Damage: Repeated cyber incidents damage customer confidence and trust in banking institutions. Security breaches create perceptions of weak protection of customer data and funds, leading to customer attrition. Reputational harm can reduce market competitiveness, affect investor confidence, and require costly public relations and trust-building efforts.

3. Regulatory and Compliance Costs: Banks must comply with stringent RBI cyber security guidelines, increasing expenditure on secure IT infrastructure, audits, compliance reporting, and risk management systems. Non-compliance can result in penalties and restrictions. These rising regulatory costs significantly impact operational budgets, especially for smaller and regional banks.

4. Operational Disruption: Cybercrime often disrupts normal banking operations due to system shutdowns, transaction delays, and service outages during incident response and forensic investigations. Recovery processes such as patching vulnerabilities and restoring data affect customer service, productivity, and operational efficiency, causing temporary inconvenience and financial losses.

Legal and Regulatory Frameworks

India has implemented significant cyber law and institutional reforms to combat cybercrime.

1. Information Technology Act, 2000 (IT Act, 2000): The Information Technology Act, 2000 is India's primary cyber law addressing electronic governance and cyber offenses. It prescribes penalties for hacking, unauthorized access, data theft, identity theft, cyber terrorism, and data breaches. The Act provides legal recognition to electronic transactions and enables investigation and prosecution of cybercrime.

2. Banking Regulations by Reserve Bank of India (RBI): The Reserve Bank of India mandates banks to follow strict cyber security and digital banking guidelines. These include periodic risk assessments, multi-factor authentication, secure encryption, real-time transaction monitoring, incident reporting, customer alerts, and cyber security audits. RBI also requires banks to establish cyber-resilience and data protection frameworks.

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 14, Issue 02, Feb 2026 Impact Factor: 8.466

www.aarf.asia,**Email** : editoraarf@gmail.com

3. Cybercrime Reporting and Enforcement Mechanism: The National Cyber Crime Reporting Portal (NCRP) enables citizens to report cybercrime online, particularly financial frauds. The helpline number 1930 allows immediate reporting of digital payment frauds to help freeze transactions. These mechanisms enhance coordination between banks, law enforcement agencies, and cybercrime cells.

Cyber Security Challenges

1. Evolving Threat Landscape: Cyber threats in the banking sector are becoming more sophisticated with the use of AI, deep fake technology, and automation. In 2024, over 65% of reported banking cyber frauds involved advanced phishing or social engineering techniques. For example, fraudsters used deep fake voice calls impersonating bank officials to trick customers into sharing OTPs, leading to large-scale UPI frauds. Automated bots now execute thousands of login attempts per minute, making traditional security defenses ineffective.

2. Resource Constraints: Smaller banks and cooperative banks face severe resource limitations in adopting advanced cyber security solutions. Nearly 45–50% of cooperative banks in India still operate on outdated or partially digital systems. Due to budget constraints, many lack Security Operations Centers (SOCs), AI-based monitoring, and skilled cyber security staff. For instance, several urban cooperative banks have reported repeated cyber frauds due to delayed system upgrades and weak network security controls**.**

3. Data Privacy and Integration Issues: Indian banks often rely on legacy core banking systems combined with newer digital platforms, leading to data silos. Reports indicate that over 40% of banks continue to use legacy infrastructure, making real-time data integration difficult. Inconsistent encryption standards and fragmented databases delay fraud detection. Past incidents of KYC data leaks demonstrate how poor data integration and weak privacy controls expose sensitive customer information.

4. Human Factor: Human error and insider threats remain major cyber security challenges. Studies show that 8–12% of major banking fraud cases involve insider collusion or employee negligence. Employees with privileged access may unintentionally leak credentials or deliberately assist fraudsters. For example, bank staff sharing customer account details has enabled mule account creation, facilitating large-scale fund diversion and laundering across multiple states.

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 14, Issue 02, Feb 2026 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

These challenges highlight the need for continuous technological upgrades, stronger internal controls, employee training, and regulatory oversight to protect the Indian banking sector from evolving cyber threats.

Mitigation Strategies and Best Practices

1. Strengthened Technical Controls: Banks should implement:

- **Multi-factor authentication (MFA)**
- **Advanced encryption**
- **Real-time monitoring and AI-based anomaly detection**
- **Regular security audits and penetration testing**

2. Customer Education and Awareness: Public campaigns informing customers about phishing, OTP safety, safe UPI practices, and reporting procedures can reduce successful fraud attempts.

3. Collaboration with Law Enforcement: Banks should establish real-time coordination channels with cybercrime cells to freeze suspicious transactions and trace fraud quickly.

4. Regulatory Compliance and Incident Response: Instituting formal incident response plans, compliance reporting systems, and disaster recovery protocols can ensure rapid reactions.

5. Workforce Training: Internal staff must receive continuous cyber security training, including secure coding, data handling, and threat identification.

Case Studies:

1. SBI Cyber Fraud Trends: Between January 2024 and October 2025, SBI reported **15,956 cyber fraud cases** with losses of over **₹118 crore** related solely to cyber fraud. Losses from related fraud categories exceeded another **₹477 crore**.

2. Organized Mule Account Scheme: Police in Uttar Pradesh and Madhya Pradesh uncovered syndicates that created multiple mule bank accounts to divert fraud proceeds.

3. Cross-State Syndicate Arrests: A Kerala-based gang operating in Bihar was arrested for organized cyber fraud involving multiple banking credentials and ATM cards.

Conclusion

Cybercrime in India's banking sector has escalated dramatically in recent years, fueled by rapid digitization, increased cyber-attack sophistication, and gaps in awareness and security

infrastructure. With financial frauds comprising a majority of cyber offenses, protecting digital financial ecosystems has become a national priority. While legal frameworks, reporting systems, and policing efforts have improved, significant work remains to fortify the banking sector against evolving threats. Strengthening cyber security protections, investing in technology, enhancing customer education, and fostering coordinated defense mechanisms between banks, government agencies, and security researchers are crucial for creating a resilient banking environment.

References

1. Reserve Bank of India Report, (2022), Cyber Security and Information Technology Framework in Banks.
2. Government of India, (2013), National Cyber Security Policy. Ministry of Electronics and Information Technology.
3. Sood, M. (2021), Cyber Crime and Cyber Security in India. Springer.
4. Kumar, R. (2020), The Growing Threat of Cyber Fraud in Indian Banking. Banking Financial Services & Insurance Review.
5. 'National cybercrime reporting statistics and financial loss data', Jagaran, 22/7/2025
6. 'IIT Kanpur study on financial fraud proportions in cybercrime', Times of India, 18/9/2023
7. 'SBI cyber fraud case numbers and loss figures', Times of India, 26/12/25
8. www.wikipedia.com
9. www.rbi.org.in