International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Banking Fraud in India: Typologies, Victim Behaviour, and AI-Enabled Risk Governance in a Global Context

Ritika Maini[1], Vivek Kumar Sindhi[2]

[1]Assistant Professor, Computer Science, Govt. Bikram College of Commerce, Patiala
[2]Assistant Professor, Commerce, Govt. Bikram College of Commerce, Patiala

Abstract
The rapid expansion of digital financial services in India, including Unified Payments Interface (UPI), mobile wallets, and internet banking, has significantly enhanced financial inclusion and convenience. However, this digital transformation has simultaneously created new vulnerabilities for fraudsters to exploit. This study synthesizes insights from global and Indian literature, case reports, and regulatory documents to examine the typologies of digital banking fraud, patterns of victim behaviour, institutional responses, and the potential of artificial intelligence (AI) driven detection mechanisms. Drawing upon Reserve Bank of India (RBI) Ombudsman reports, the National Electronic Fraud Forum (NeFF), international case studies from Zimbabwe, the European Union, and Saudi Arabia, as well as criminological perspectives, the paper develops a holistic framework for understanding and combating digital fraud in India. Findings indicate that phishing, vishing, SIM swap, QR/UPI scams, ATM skimming, and Ponzi schemes remain dominant, with social engineering as a critical enabler. Victim susceptibility stems from trust in authority, urgency appeals, and low digital literacy, particularly among rural and elderly populations. Despite RBI initiatives such as the BE(A)WARE campaign and regulatory enhancements, significant challenges remain, including underreporting, fragmented detection systems, and cross-border fraud networks using the dark web and cryptocurrencies. The paper recommends multi-stakeholder strategies: AI-enabled fraud monitoring platforms, unified reporting mechanisms, consumer digital literacy programs, and international collaboration for cybercrime intelligence. The study concludes that India's success in balancing financial inclusion with cyber resilience will depend on integrating technology, regulation, and behavioural insights.

Keywords: Digital banking fraud, UPI scams, social engineering, RBI, artificial intelligence, fraud detection, financial inclusion, cybercrime

1. Introduction

Digital banking in India has witnessed a remarkable transformation over the past decade, propelled by the government's Digital India initiative, the Reserve Bank of India's (RBI) regulatory push, and consumer adoption of mobile-based payment platforms such as the Unified Payments Interface (UPI). According to the National Payments Corporation of India (NPCI), UPI transactions crossed 14 billion monthly transactions in 2025, highlighting its centrality in India's payment ecosystem. This digital revolution has advanced financial inclusion, expanded access to credit, and improved efficiency in banking services.

Yet, the convenience of digital banking has come at a cost: a surge in electronic frauds. RBI's Ombudsman office reported exponential increases in fraud complaints relating to phishing links, QR code scams, SIM swaps, ATM skimming, and Ponzi schemes, disproportionately affecting first-time digital users (Office of RBI Ombudsman, 2021). The National Electronic Fraud Forum (NeFF, 2016) reported over 19,500 e-fraud cases in India in 2016 alone, representing an 82% increase from the previous year (Thakur, 2019). With the rise of UPI and mobile banking, fraudulent techniques have become more sophisticated, leveraging social engineering, malware, and dark web data markets.

Globally, cyber-enabled fraud has been recognized as a systemic risk for banking institutions. For example, in Zimbabwe, inadequate cybercrime laws and lack of consumer awareness contributed to widespread fraud vulnerabilities (Dzomira, 2014). In the European Union and UK, large-scale payment frauds exploited vulnerabilities in SWIFT networks and airline platforms (European Cybersecurity Agency, 2018). Victimology research in the UK revealed that susceptibility arises from urgency pressures, trust in authority figures, and embarrassment in reporting (Button et al., 2014). These findings resonate with the Indian context, where digital literacy gaps make rural and elderly populations especially vulnerable.

This study, therefore, seeks to provide a comprehensive examination of digital banking fraud in India by situating it within a global comparative lens. Specifically, it aims to:

1. Identify and classify the typologies of fraud affecting Indian digital banking.
2. Analyse victim behaviours and vulnerabilities in the Indian context.
3. Evaluate the effectiveness of institutional responses and governance mechanisms, including RBI initiatives and fraud detection systems.
4. Explore the potential of AI-enabled solutions for fraud detection and prevention.
5. Provide policy recommendations for strengthening India's fraud resilience while sustaining financial inclusion.

Social engineering in the Indian context is a complex issue rooted in a blend of psychological and socio-cultural factors. Fraudsters exploit inherent cognitive biases like urgency and authority bias, causing victims to bypass critical thinking and act on impulse. This vulnerability is heightened by a significant digital literacy gap, especially among first-time internet users and the elderly who may lack awareness of basic cybersecurity hygiene. Furthermore, socio-cultural norms, such as a deep-seated respect for authority and a reluctance to report due to shame, create a fertile ground for scams to thrive. These factors, combined with sophisticated tactics like grooming victims over time, allow fraudsters to normalize small, repeated payments, making it difficult for both individuals and banking systems to detect the cumulative loss until it becomes substantial. The following flowchart and figure 1 depicts the cycle of the frauds that occur in a life cycle.

Fraud Lifecycle and Response

1. **Attack**
   - Victim Response: Social Engineering (phishing, romance scams, fake jobs), Malware, Data Breaches. Fraudster initiates contact/exploit.
2. **Victim Response**
   - Bank Detection: Falls prey to cognitive biases (urgency, authority, greed). Unknowingly provides info or authorizes transactions. Delayed realization of fraud.

3. **Bank Detection**
   - Reporting: Transaction monitoring systems, AI/ML anomaly detection. Two-factor authentication, fraud alerts. Often reactive; can miss incremental losses.
4. **Reporting**
   Enforcement: Victim reports to bank/authorities. Reluctance due to shame/lack of awareness. Low reporting rates reduce comprehensive data.
5. **Enforcement**
   - Attack (implied feedback loop for deterrence) : Investigation, prosecution, recovery of funds. Deterrence through legal action. Weak prosecution can lead to repeat offenses.

Fig 1: Fraud Lifecycle and Response

This structure covers the flow from the initial attack to the final enforcement, with key aspects of each stage. By integrating insights from Indian and global studies, the paper contributes to the scholarly understanding of e-banking fraud as a socio-technical phenomenon. It argues that addressing digital fraud requires not only technological upgrades but also behavioural interventions, regulatory coherence, and international cooperation.

2. Literature Review

The emergence of core banking systems, UPI, and mobile payment platforms has revolutionized financial services in India. Internet banking allows customers to perform transactions without visiting a branch, enabled by centralized databases and online channels. With this transition, fraud has migrated from physical cheque manipulation and insider collusion to cyber-enabled mechanisms such as phishing, spyware, skimming, and hacking.

The RBI Ombudsman's BE(A)WARE report (2021) emphasizes that fraudsters exploit social engineering, including phishing links, vishing calls, QR code scams, and SIM swaps, often targeting digitally inexperienced consumers. Fraud via online selling platforms and UPI "request money" scams have become increasingly prevalent, with unsuspecting victims authorizing debit transactions believing they are receiving money. Similarly, fake loan websites, Ponzi schemes, and forged documents have emerged as prominent threats in the NBFC sector.

Indian studies highlight a dual gap: (1) Consumer awareness remains low, leading to behavioural vulnerabilities; (2) Bank governance structures often rely heavily on technological firewalls, without adequately addressing fraud through customer education and reporting clarity (Thakur, 2019). Globally, the problem of e-banking fraud is not unique to India. Zimbabwe's banking sector, for example, has faced challenges of inadequate cybercrime legislation, weak detection tools, and poor awareness programs (Dzomira, 2014). The EU and UK experiences with SWIFT and large-scale breaches highlight the need for strong institutional coordination and cross-border cooperation. Victimology research from the UK and Australia emphasizes the role of grooming, authority, and urgency in facilitating fraud (Button et al., 2014).

3. Typologies of Fraud in Indian Digital Banking

The figure 2 and figure 3 shows typologies of Fraud in Indian Digital Banking. Table 1 shows the detailed typologies of digital banking fraud in India.

Fig 2: Fraud in Indian Digital Banking

3.1 Phishing and Smishing

Phishing remains one of the most common entry points for fraudsters. Fraudsters design websites resembling legitimate banking portals or e-commerce platforms, luring customers via links sent over SMS (smishing), email, or instant messaging. Once users input login credentials, the data is captured and used for unauthorized transactions (RBI Ombudsman, 2021).

In India, phishing often exploits themes such as income tax refunds, KYC updates, and fake RBI or bank 'security alerts.' The 2019 CERT-In advisory reported that phishing cases increased markedly, with UPI and net banking users as prime targets.

3.2 Vishing (Voice Phishing)

Vishing involves fraudsters impersonating bank officials, RBI representatives, or government agents through phone calls, seeking to extract OTPs, PINs, or card details. Fraudsters often build trust by citing personal data already obtained from leaked databases. Tactics commonly include threats of account suspension or offers of loan approvals, creating urgency to bypass victims' skepticism.

3.3 QR Code and UPI 'Request Money' Scams

With India's rapid shift to UPI, fraudsters have devised scams targeting QR codes and UPI's 'collect' feature. Customers scanning fraudulent codes to 'receive payments' end up initiating debit transactions. Fraudsters posing as buyers on platforms like OLX send 'payment requests,' tricking sellers into authorizing debits instead of credits. These scams are uniquely Indian in scale and prevalence, reflecting both UPI's success and its vulnerabilities.

3.4 SIM Swap and SIM Cloning

SIM swap fraud occurs when fraudsters obtain a duplicate SIM card of the victim's mobile number, enabling interception of OTPs and alerts. Cloning exploits telecom service loopholes or social engineering against customer service staff. In India, SIM swap incidents have been tied to organized fraud rings colluding with telecom agents.

3.5 ATM Skimming and Card Cloning

Though mobile fraud dominates headlines, ATM skimming persists, particularly in semi-urban areas. Fraudsters install skimming devices and hidden cameras on ATMs to capture card data and PINs. Despite RBI's mandate for EMV chip cards, vulnerabilities remain in legacy systems.

3.6 Remote Access and Malware Attacks

Fraudsters trick victims into downloading remote access apps (e.g., TeamViewer, AnyDesk) under the guise of 'customer support.' Once installed, fraudsters gain full access to the victim's device, capturing banking credentials. Malware-based frauds also intercept SMS OTPs or manipulate banking apps in the background.

3.7 Lottery, Job, and Investment Scams

Indian consumers are often targeted with fraudulent job offers or lottery winnings requiring upfront 'processing fees.' Ponzi schemes and MLM models continue to thrive in rural areas, despite RBI and SEBI crackdowns.

3.8 Social Media and Impersonation Scams

Fraudsters impersonate trusted contacts on WhatsApp, Facebook, or Instagram to solicit urgent money transfers. Fake celebrity or government profiles are also used to spread fraudulent links or investment opportunities.

3.9 Juice Jacking and Device-Based Fraud

'Juice jacking' involves malware installed in public USB charging stations that capture banking credentials when users connect their phones. Several metropolitan police departments have issued advisories warning commuters.

3.10 Cross-Border and Dark Web Enabled Frauds

Fraud networks increasingly leverage the dark web to purchase stolen credentials, card data, or malware kits. Payments are laundered using cryptocurrencies, complicating enforcement. Indian agencies like CERT-In and FIU-IND have highlighted cases where domestic frauds were coordinated from international call centers.

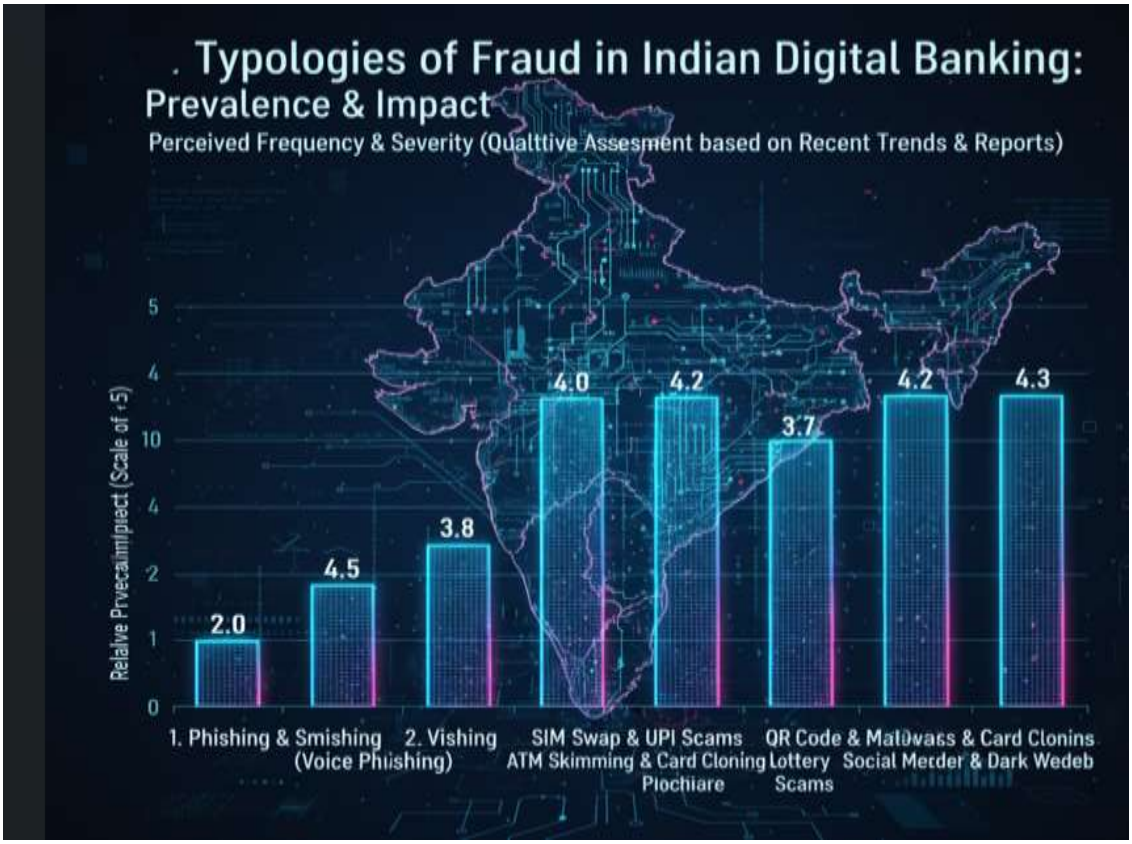

Fig 3: Bar Graph representation of Topologies Reports

Table 1: Detailed Typologies of Digital Banking Fraud in India

Fraud Type	Modus Operandi	Example	Mitigation
Phishing/Smishing	Fake websites/SMS links harvest login details	Fake RBI tax refund site	Awareness, URL verification, two-factor auth
Vishing	Phone calls impersonating officials ask for OTP/PIN	Caller posing as bank officer	Never share OTPs, authentication training
UPI/QR Scams	Fake QR codes or 'request money' misuse	Marketplace OLX scam	App warnings, QR verification
SIM Swap	Duplicate SIM obtained for OTP interception	Fraudulent SIM replacement	Telecom KYC, port protections
ATM Skimming	Skimmer devices capture card data	Cloned cards withdrawals	EMV chips, ATM inspections
Remote Access	Malicious remote apps gain control	AnyDesk scam	Avoid remote apps, verify support
Investment/Ponzi	Fake investment promises	Crypto Ponzi platform	Regulatory enforcement, education
Social Media Impersonation	Fake profiles request funds	WhatsApp family impersonation	Verify via alternate channels
Juice Jacking	Public USBs install malware	Public charger malware	Use own chargers, data-blockers

Dark Web Trade	Sale of stolen creds & malware	Card dumps sold online	Trace & international cooperation

4. Victim Behaviour and Social Engineering in the Indian Context

Fig 4 shows the victim behavior and social engineering (2024) and the detail on the basis of Indian context is shown here.

Fig 4: Victim Behavior and Social Engineering

4.1 Cognitive Biases and Decision-Making Traps

Victims often fall prey due to inherent cognitive biases: authority bias, urgency effect, greed and opportunity bias, and trust in technology. These biases cause victims to act quickly without verifying legitimacy.

4.2 Socio-Cultural Factors

The Indian socio-cultural environment intensifies susceptibility: respect for authority, reluctance to report fraud due to shame, and community-based spread of schemes in rural areas.

4.3 Digital Literacy Divide

India's digital inclusion drive has brought millions of first-time users into the banking system, but the gap between access and literacy is stark. Rural and elderly populations often lack awareness of basic cybersecurity hygiene.

4.4 Grooming and Relationship-Based Fraud

Beyond one-off scams, fraudsters often invest time in grooming victims via romance scams or fake job relationships, lowering defenses and increasing the likelihood of compliance.

4.5 Incremental Losses and Normalization

Small, repeated payments reduce suspicion and normalize illicit transfers until cumulative losses become substantial, evading simple threshold-based detection systems.

4.6 Victim Profiles in India

Victim profiles include first-time digital adopters, elderly account holders, aspirational youth, and urban users with overconfidence in their digital skills.

4.7 Criminological Perspectives

Routine Activity Theory and the Fraud Triangle provide frameworks (2024) for understanding victimization; low reporting and weak prosecution reduce deterrence.

5. Fraud Risk Governance and Detection Mechanisms

Table 2 shows the RBI & CERT-In Initiatives from 2011-2025. Table 3 shows the models from artificial intelligence in digital fraud.

5.1 Risk Governance in the Indian Banking Sector

Fraud governance refers to the structured frameworks and institutional controls banks employ to prevent, detect, and respond to fraud. RBI mandates include two-factor authentication, chip-and-PIN cards, transaction monitoring systems, and compensation frameworks. However, governance remains uneven across institutions.

5.2 RBI and National-Level Initiatives

BE(A)WARE Campaign (2021), NeFF's centralized fraud repository, CERT-In's six-hour incident reporting rule, and Digital Payment Security Controls (2023) are important national-level initiatives shifting focus toward proactive detection.

5.3 Traditional Detection Mechanisms

Rule-based systems (thresholds, blacklists) detect known fraud patterns but struggle against adaptive, low-value, or novel frauds.

5.4 AI and Machine Learning in Fraud Detection

Supervised models (Random Forest, Logistic Regression), unsupervised models (clustering, anomaly detection), and deep learning (2022) for behavioural biometrics are increasingly used. Indian fintechs employ device fingerprinting and behavioural analytics, though data quality and privacy constraints persist.

5.5 Multi-Layered Controls

Best practice combines prevention (education, authentication), detection (AI/ML), response (freezing accounts, law enforcement), and recovery (refunds). A central fraud registry enhances systemic resilience.

5.6 Challenges in Risk Governance

Fragmented oversight, resource gaps in smaller banks, data privacy concerns, and underreporting of incidents undermine governance effectiveness.

6. Indian Regulatory and Policy Landscape

The RBI is the apex regulator. Key measures: mandatory 2FA, zero liability policy, BE(A)WARE consumer campaigns, CERT-In incident reporting, the Digital Personal Data Protection Act (2022), and digital lending guidelines.

Inter-agency coordination initiatives (RBI-CERT-In Task Force 2024) and FIU-IND tracking of crypto laundering are recent steps. Enforcement and prosecution remain challenging.

Table 2: RBI & CERT-In Initiatives (2011–2025)

Year	Initiative	Focus	Impact
2011	Mandatory 2FA	Authentication	Reduced card-not-present fraud
2017	Zero Liability Policy	Consumer protection	Encouraged reporting
2019	National Cyber Crime Portal	Complaint filing	Centralized reporting

2021	BE(A)WARE Campaign	Awareness	Increased awareness
2022	CERT-In 6-hour rule	Incident reporting	Faster response
2023	Digital Personal Data Protection Act	Data privacy	Reduced mass leaks
2023	Digital Lending Guidelines	Fake app control	Improved governance
2024	RBI-CERT-In Task Force	Coordination	Integrated intelligence

Table 3: AI/ML Models for Fraud Detection

Model	Use Case	Advantage	Limitation
Random Forest	Transaction classification	High accuracy, handles features	Needs labeled data
Logistic Regression	Binary fraud prediction	Interpretable	Linear assumptions
Autoencoders	Anomaly detection	Detects novel frauds	Requires tuning
Clustering (K-Means)	Segment anomalous patterns	Unsupervised	May miscluster
Behavioral Biometrics (DL)	User authentication	Hard to spoof	Privacy concerns

7. Challenges and Gaps

Key challenges: fragmented oversight, limited AI adoption in smaller banks, low digital literacy, underreporting, slow judicial processes, deepfake and crypto laundering risks.

8. Recommendations

8.1 Consumer Awareness and Behavioural Interventions:

- National Digital Literacy Mission for Banking
- Behavioural nudges in apps
- Gamified training
- Community-level outreach

8.2 Institutional and Banking Sector Strategies:

- Centralized Fraud Intelligence Platform
- Cross-bank blacklisting
- Dedicated fraud redressal cells
- Fast-track refund mechanisms

8.3 Technological Solutions:

- AI/ML deployment (supervised & unsupervised)
- Device fingerprinting & geo-tagging
- Deepfake detection tools
- Crypto-tracing frameworks

8.4 Regulatory and Policy Enhancements:

- Unified Fraud Reporting Portal
- Mandatory fraud insurance

- Periodic fraud audits
- Global cooperation

8.5 Academic and Research Initiatives:

- Fraud victimology studies
- Fraud analytics research hubs
- Open data on fraud cases

9. Conclusion

The rapid digitization of India's financial ecosystem has advanced financial inclusion but widened opportunities for fraud. A multi-layered approach combining consumer education, AI-driven detection, regulatory cohesion, and international cooperation is essential to mitigate risks while preserving the benefits of digital finance.

References

1. Ali, M. A., Hussin, N., & Abed, I. A. (2019). E-banking fraud detection: A short review. International Journal of Innovation, Creativity and Change, 6(8), 67–78.
2. Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology.
3. Dubey, R. D., & Manna, A. (2014). E-banking frauds and fraud risk management. Tactful Management Research Journal, 2(3), 20–25.
4. Dzomira, S. (2014). Electronic fraud (e-fraud) risk in the banking industry: The case of Zimbabwe. Risk Governance & Control: Financial Markets & Institutions, 4(2), 104–112.
5. LOVE, S. P. (2024). Fraud Management Life Cycle And Firms Profitability In Nigeria. *Journal for Business and Management Sciences (JBMS)*, *1*(2), 40-69.
6. Luo, B., Zhang, Z., Wang, Q., Ke, A., Lu, S., & He, B. (2024). Ai-powered fraud detection in decentralized finance: A project life cycle perspective. *ACM Computing Surveys*, *57*(4), 1-38.
7. Office of RBI Ombudsman. (2021). BE(A)WARE: Modus operandi and precautions to be taken against fraudulent transactions.
8. Thakur, S. (2019). Electronic banking fraud in India: Effects and controls. International Journal of Science and Research, 8(10), 823–829.
9. Pillai, S. (2023). Identity Theft: Prevention of Modern Crimes in the Era of Internet. *Issue 2 Indian JL & Legal Rsch.*, *5*, 1.
10. Zaman, K. T., Zaman, S., Bai, Y., & Li, J. (2022). Empowering digital forensics with AI: Enhancing cyber threat readiness in law enforcement training. *Available at SSRN 5039717*.
11. Aslam, F., Hunjra, A. I., Ftiti, Z., Louhichi, W., & Shams, T. (2022). Insurance fraud detection: Evidence from artificial intelligence and machine learning. *Research in International Business and Finance*, *62*, 101744.