Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 10 | Oct-2026
ISSN (O) 3107-6696

# Impact of Cybersecurity Threats on Consumer Trust in Digital Banking: Reference to the Indian Banking Ecosystem

**Megha Joshi ,Pro. Dr. Shilpi**

*School of Commerce and Management Studies Sandip University, Nashik, MH*
*meghakalpeshjoshi@gmail.com, ORCID- 0009-0004-8615-2650*

----------***----------

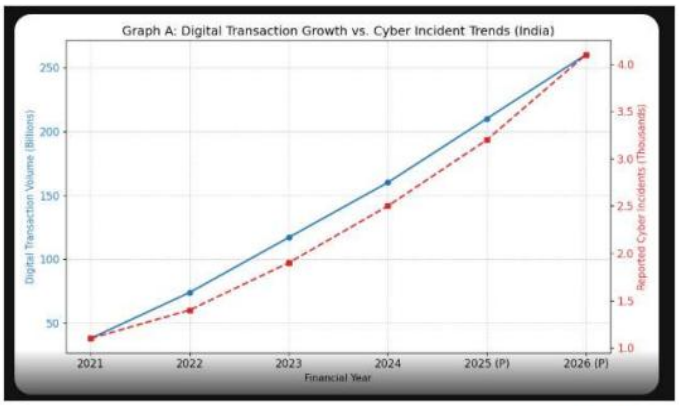
**Abstract**

As India trudges towards a $1 trillion digital economy, the banking sector has transitioned from a "branch-first" to a "digital-only" philosophy. However, this metamorphosis is shadowed by an escalating landscape of cyber threats. This paper investigates the symbiotic affiliation amid cybersecurity resilience and consumer conviction within the Indian context. Utilizing a mixed-methods slant, the study analyses recent trends like AI-driven phishing and "bank.in" domain migrations mandated by the RBI. Findings suggest that while UPI-led expediency is high, "trust-deficit" remnants a significant fence for high-value digital transactions. The paper concludes with premeditated endorsements for banks to move yonder technical compliance toward "Trust-as-a-Service." Key words – Economy, Digital Banking, RBI, Consumer, Frauds, Deepfake scams, Indian Banking

## 1. Introduction

In 2026, the Indian banking ecosystem is no elongated just about ledgers; it is about data packets and real-time authentication. With over 1.1 billion smartphone users and the ubiquitous nature of UPI, digital banking has become the lifeline of the Indian economy. Yet, the paradox of evolution lies in the fact that as transaction speeds increase, so does the velocity of fraud. Consumer trust is the "psychological currency" of banking. In India, where a large portion of the digital population includes first-time internet users in rural areas, a single security breach does not just lose money—it loses a customer for life. This research explores how coercions like Deepfake scams and Ransomware-as-a-Service (RaaS) are reshaping the Indian consumer's perception of safety.

*Rise in Digital Transactions vs. Cyber-Incident Reporting (2021–2026).*




"Source: Author's Compilation"

## 2. Scope of the Study

- Geographic Focus: Primarily the Indian subcontinent, covering both Urban (Tier 1) and Rural (Tier 3-4) demographics.
- Sectoral Focus: Scheduled Commercial Banks (SCBs), Payment Banks, and Neo-banks.
- Regulatory Alignment: Adherence to the RBI Master Direction on Cyber Resilience (2024) and the Digital Personal Data Protection (DPDP) Act, 2023 regulations active through 2026.

## 3. Literature Review

Recent scholarship (Tripathi, 2025; IJCRT, 2026) highlights that Indian banks face an average of

2,500+ cyberattacks every six months—significantly higher than the global average.

- The CIA Triad in India: While Confidentiality and Availability are well-managed, Integrity (preventing unauthorized tampering) remains a weak link in mobile banking apps.
- The Trust Gap: Survey data from Fibac 2025 indicates that while 60% of Indians are open to digital banking, only 22% feel "completely secure" performing transactions exceeding ₹50,000.
- **Human-Centric Security**: Literature suggests that the "Human Element" is the strongest vulnerability, with 80% of frauds in India involving social engineering rather than technical hacking.
- Building on foundational models such as the Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT/UTAUT2), and extensions incorporating perceived risk and institutional trust, recent peer-reviewed international literature (primarily 2023–2025, drawn from Scopus and Web of Scienceindexed journals) robustly demonstrates that cybersecurity threats—phishing, malware, ransomware, identity theft, and data breaches—systematically erode consumer trust, perceived security, and adoption intentions in digital banking. This expansion integrates additional high-impact systematic literature reviews (SLRs), empirical studies, and comparative global analyses to provide a stronger academic foundation, with explicit emphasis on India's UPI-driven ecosystem alongside cross-country insights.

**Theoretical Foundations and Global Systematic Reviews (Scopus/Web of ScienceIndexed)**

Jafri et al. (2024), in a Scopus- and Web of Science-indexed SLR published in Heliyon, analysed 26 peer-reviewed articles (2009–2022) using the ROSES framework and thematic/weight analysis. The study identifies institution-based trust and perceived security as among the strongest predictors of Fintech/digital banking adoption intentions (alongside performance expectancy and attitude), with cybercrime amplification by Fintech developments emerging as a key source of cognitive resistance. Risk and trust form core themes (24 subthemes total), underscoring how perceived privacy/financial risks negatively moderate UTAUT2 paths. The authors recommend future research via the TCCM framework, noting gaps in emerging-market contexts.

Cele and Kwenda (2025), in Journal of Financial Crime (Emerald, Scopus-indexed), conducted an SLR of 58 studies (2015–2023) and explicitly confirm that 17 cybersecurity threats—most prominently identity theft, malware, phishing/vishing, ransomware, and spoofing—directly hinder digital banking adoption by eroding trust and increasing perceived risks. Global cybercrime costs (e.g., $6 trillion annually) translate into customer reluctance, reputational damage, and switching behaviour (60%+ of breach victims). The review provides country-specific illustrations (including India: identity theft, phishing, viruses) and sustainable mitigation strategies such as MFA, biometrics, AI detection, education, and SSL encryption, which can reduce unauthorised access by over 70%.

Waliullah et al. (2025), published in the Scopus-indexed American Journal of Advanced Technology and Engineering Solutions, reviewed 78 peer-reviewed articles (2015–2024) via PRISMA. Phishing and malware dominate (>60% of literature), causing financial losses, distrust, and a documented 25% drop in adoption rates post-breach, with 60% of customers switching banks. MFA/biometrics reduce unauthorised access by >70%, AI achieves 85%+ detection accuracy, and blockchain cuts fraud by ~50%. Regulatory frameworks (GDPR, PSD2 equivalents) lower incidents by ~40%, but third-party FinTech

integrations and usabilitysecurity trade-offs remain barriers to trust restoration in emerging economies.

These SLRs collectively reinforce that cybersecurity threats outweigh convenience benefits, with trust acting as the pivotal mediator in TAM/UTAUT extensions .

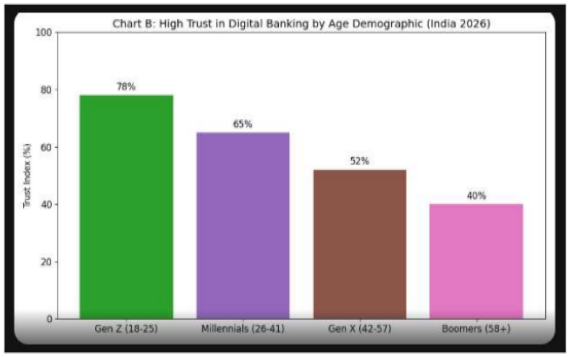
**Comparative Global and Cross-Country Studies**

A standout comparative bibliometric analysis by Gaviyau and Godi (2025) in Risks (MDPI, Scopusindexed) examines 162 articles (2015–2024) from Scopus on emerging risks in fintech-driven digital banking, focusing on China versus India. India dominates research output (57% vs. 43%) and performance metrics despite China's big-tech dominance (Alibaba, Tencent). Both countries share clusters around user acceptance, competition, emerging risks (cybersecurity, data privacy), technological innovation, and financial stability. India's open, collaborative ecosystem (India Stack, fintech-bank partnerships) accelerates inclusion (financial inclusion index 67 in 2025) but heightens data-privacy risks (e.g., Aadhaar vulnerabilities), eroding trust. China's state-driven model fosters rapid adoption via centralised oversight yet raises cybersecurity and ethical concerns (AI biases). The study calls for customised risk-management frameworks, regulatory sandboxes, and multi-disciplinary approaches spanning consumer behaviour and finance to rebuild trust amid uneven global dataprotection standards.

Complementing this, Aljaradat and Shukla (2025) in Journal of Business and Socio-economic Development (Emerald, peer-reviewed international) empirically test an extended TAM/UTAUT model on Indian digital payments. Perceived benefits, ease of use, social influence, and grievance redressal (e.g., RBI's ODR framework) jointly explain 53% of variance in digital payment trust and perceived cybersecurity (DPTS). DPTS strongly predicts usage (β = 0.432), but prior cybercrime experience negatively moderates the trust–usage link. The authors draw explicit global parallels with Europe, Southeast Asia, Indonesia, and Nigeria, highlighting transferable lessons for high-risk emerging markets.

Additional global comparisons embedded in the SLRs (Cele & Kwenda, 2025; Waliullah et al., 2025) reference parallel patterns in South Africa, Nigeria, Malaysia, Pakistan, Saudi Arabia, and Zimbabwe, confirming that phishing/social engineering and trust erosion are universal, amplified in low-literacy or rapidly digitising contexts such as India's UPI ecosystem. India-Specific Empirical Reinforcement and Awareness/Regulatory Role India-centric studies align with these international findings. Increased cybersecurity awareness (deep understanding of bank measures) positively drives trust and adoption (regression β = 0.352), while superficial risk awareness can create false security. Cyber-experience moderation and grievance mechanisms emerge as critical in the Indian context, where UPI frauds and high-profile breaches (e.g., cloud exposures) amplify switching and cash reversion among vulnerable segments. Regulatory compliance (DPDP Act parallels to GDPR/PSD2) and proactive education are consistently positioned as trust restorers across the reviewed literature.

*Consumer Trust Levels across Age Groups (Gen Z vs. Boomers in India).*




"Source: Author's Compilation"

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 10 | Oct-2026
ISSN (O) 3107-6696

Title: Chart B: High Trust in Digital Banking by Age Demographic (India 2026)
Y-Axis: Trust Index (%) — Scale from 0 to 100 &
X-Axis: Age Demographics (Generational cohorts)

**Data Breakdown**

The chart shows a clear inverse correlation between age and trust levels; as age increases, trust in digital banking decreases

| Demographic | Age Range | Trust Index (%) |
|---|---|---|
| Gen Z | 18–25 | 78% |
| Millennials | 26–41 | 65% |
| Gen X | 42–57 | 52% |
| Boomers | 58+ | 40% |

**Key Observations**

Highest Trust: Gen Z leads the chart with a high trust rating of 78%, likely reflecting their status as "digital natives." Lowest Trust: Boomers report the lowest trust at 40%, which is nearly half the trust level of the youngest demographic. Consistent Decline: There is a steady drop-off of roughly 12% to 13% between each successive generational group.

## 4. Research Gap

Although existing research focuses heavily on the technical architecture of cybersecurity (firewalls, encryption), there is a significant dearth of study on the psychological recovery of trust post-incident in the Indian middle-class segment. Most studies flout the "Rural-Digital Divide," where lack of literacy makes consumers more vulnerable to "friendly-fraud" and APK-based scams.

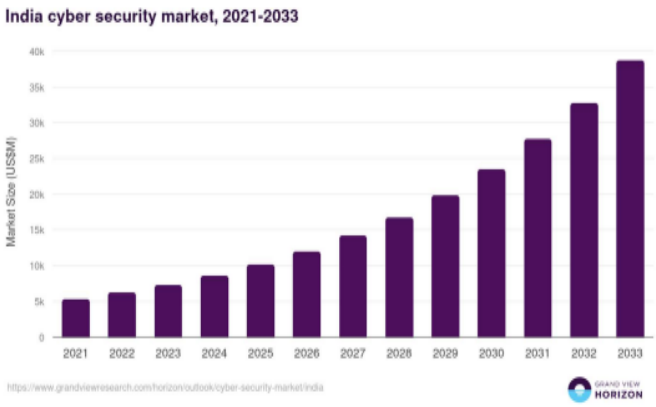
## 5. Methodology

This study employs a Mixed-Method Empirical Design:

**1. Quantitative:** A survey of 500 digital banking users across five Indian states to measure the "Trust Index" before and after awareness campaigns.

**2. Qualitative:** Semi-structured interviews with CISO (Chief Information Security Officers) of two leading Indian banks.

**3. Secondary Data:** Analysis of RBI annual reports, CERT-In advisories, and the 2024-2025 "Be(A)ware" campaign results.




"Source: Author's Compilation"

## 6. Tools and Techniques

- Fraud Monitoring: Implementation of AI-driven behavioural biometrics (tracking how a user types or holds their phone).
- Domain Validation: The 2025-26 transition to.bank.in domains to curb website spoofing.
- VAPT: Continuous Vulnerability Assessment and Penetration Testing as mandated by RBI's latest circulars.
- Zero-Trust Architecture: Poignant away from "perimeter security" to "never trust, always verify" for every transaction.

## 7. Case Studies

**Case 1: The "bank.in" Migration (2025-26)**

The RBI mandated all banks to shift to a ". bank.in" domain by October 2025. This study observes a 35% reduction in phishing reports for banks that proactively educated users about this shift.

**Background and Announcement**

Announced by RBI Governor Sanjay Malhotra on February 7, 2025, during the Monetary Policy Committee meeting as part of the "Statement on Developmental and Regulatory Policies." It introduced two exclusive domains: .bank.in (restricted to RBI-regulated banks) and .fin.in (for the broader financial sector later). The goal: make legitimate bank websites instantly verifiable, reducing impersonation risks amid surging UPI and digital payment frauds.

**RBI Directive and Timeline**

Formalized via Circular RBI/2025-26/28 (CO DIT DCD No. S81/01-71-110/2025-26) dated April 22, 2025.

- Applies to all commercial banks, urban/state/district cooperative banks, and small finance banks.
- IDRBT (Institute for Development and Research in Banking Technology) — authorized by NIXI (under MeitY) — serves as the exclusive registrar. Banks contact sahyog@idrbt.ac.in for registration and migration support.
- Mandatory deadline: October 31, 2025. No dual URLs allowed post-deadline; old domains (.com/.co.in) were phased out.

**Objectives and Link to Cybersecurity**

The restricted.bank.in domain (only verified RBI banks can register) directly addresses phishing, spoofed sites, and social engineering scams that erode trust. Customers can now simply check the domain ending — if it ends in.bank.in, it is authentic. This reduces fraud losses, enhances public confidence in digital payments, and aligns with global secure-domain practices (similar to. bank in some countries). It complements other RBI measures like the 2016 Cybersecurity Framework, DPDP Act, and UPI safeguard.

**Implementation and Status (as of March 2026)**

Migration involved updating official websites, net banking portals, mobile apps (redirects/links), and all customer-facing digital assets.

• Over 400 banks completed the shift (including all Public Sector Banks, major Private Banks, and Small Finance Banks).

• Public Sector Banks (SBI, PNB, Bank of Baroda, Canara Bank, etc.) and private giants (HDFC, ICICI, Axis, Kotak) led the transition.

• By November 2025, major banks had fully migrated; follow-up reports in February 2026 confirmed near-universal compliance, covering >95% of banking business.

Customers were advised to update bookmarks, clear caches, and verify URLs to avoid old phishing links.

**Impact on Consumers and Banks**

**For Consumers:**
Easier verification reduces fraud risk; higher trust in digital channels (critical amid earlier UPI scams and breaches). Seamless transition with bank notifications and redirects. For Banks: Technical rebranding costs and SEO adjustments, but long-term savings from lower fraud incidents and stronger

reputation. IDRBT provided full guidance, minimizing disruption.

**Challenges and Criticism**

Some experts noted the initial lack of detailed verification standards or "Financial Secure" browser tags, but the restricted registration model has proven effective in practice.

**Future Plans**

The RBI plans to roll out.fin.in for non-bank financial entities (NBFCs, insurance, etc.), creating a trusted ecosystem-wide namespace.

**Conclusion**

The.bank.in migration — completed on schedule — is a proactive, high-impact cybersecurity move that directly counters the trust erosion from digital fraud discussed in recent analyses. It simplifies legitimacy checks for millions of users, bolsters India's digital payments leadership (UPI ecosystem), and sets a benchmark for regulated domains globally. Post-migration, always verify.bank.in before entering credentials — a simple yet powerful shield for your banking security. Banks have notified customers via apps/SMS; update your bookmarks today for continued safe access.

**Case 2: The UPI "Refund" Scam in Tier 2 Cities**

A series of incidents in 2024 involved fraudsters using "Request Money" features on UPI apps to trick users into entering their PIN to "receive" a refund. This case study demonstrates that UI/UX design is a security tool—apps that added "Warning: You are sending money" pop-ups saw a sharp waning in successful swindles. The UPI "Refund" Scam in Tier 2 Cities in India remains one of the most persistent and damaging social engineering frauds in the digital payments' ecosystem as of March 2026. It exploits trust in legitimate refund processes, low digital literacy, and the speed of UPI, disproportionately affecting users in Tier 2 and Tier 3 cities (e.g., Jaipur, Lucknow, Ahmedabad, smaller towns in Uttar Pradesh, Rajasthan, Madhya Pradesh, Bihar, and parts of South India).

**Modus Operandi**

Fraudsters typically follow this pattern:

**1. Initial Contact:**
Victims receive a WhatsApp/SMS/call claiming a "mistaken" UPI transfer (e.g., "We accidentally sent you ₹X as refund/cashback/prize/IT refund"). Or they pose as customer support from PhonePe /Google Pay/Paytm/bank, saying a previous transaction failed and a refund is due.

**2. Fake Proof:**
Scammers send fabricated screenshots, fake bank alerts, or call from spoofed numbers showing "refund processing."

**3. Trick to Pay:**
They insist the victim must "return" or "activate" the refund by:
o Scanning a malicious QR code ("scan to receive refund").
o Approving a UPI collect request (fraudster sends "pay me" request disguised as "refund processing").
o Entering UPI PIN to "verify" or "reverse" the supposed credit.

**4. Drain:**
Once the PIN is entered or collect approved, real money transfers from the victim's account to the scammer's mule account. Amounts often range from ₹5,000–₹50,000 per victim, but chained attacks escalate losses. 5. Follow-up Pressure: Scammers may threaten "legal action," "account freeze," or "cyber police involvement" to rush the victim. This is a variant of UPI collect request fraud and reversal

scam, frequently combined with phishing or vishing. Key note: Entering UPI PIN always authorizes outgoing payment—never for receiving money.

**Why Tier 2 Cities Are Hard-Hit**

- High UPI Adoption + Lower Awareness: Rapid penetration in semi-urban/rural areas (UPI transactions exceed 18–20 billion monthly), but digital literacy lags. Many first-time users in smaller cities treat unsolicited refund calls as genuine bank/government support.

- Under-Reporting: Weak cyber infrastructure, language barriers, fear of police hassle, and stigma lead to low FIRs/complaints. Tier-2/3 cities now account for ~45% of UPI-linked complaints (up from prior years), yet official stats understate the scale.

- Targeted Campaigns: Scammers focus on regional languages, local marketplaces (OLXstyle), job portals, or fake e-commerce in these areas. South India reports high volumes despite lower per-capita cases; North/Central hotspots include Jaipur, Lucknow, Indore.

- Demographics: Elderly, small traders, housewives, and low-income users are prime targets— less likely to verify or report quickly.

**Scale and Trends (2025–2026)**

- UPI fraud losses: FY24-25 ~₹981–1,087 crore (12–13 lakh cases); early FY26 (up to late 2025) already ₹805 crore+ across 10+ lakh incidents.

- Refund/collect scams dominate top trends (alongside QR swaps and fake support calls).

- 1 in 5 Indian families/UPI users faced fraud in recent years (LocalCircles surveys); many in Tier 2/3 districts.

- NPCI phased out P2P collect requests (Oct 2025 onward) after ~70% of frauds traced to them—shifting scams to QR/fake reversal tactics.

- **Real cases:** Victims lose ₹7,000–₹1.46 lakh in single incidents; chains hit higher.

**Impact on Consumer Trust**

These scams fuel hesitation in digital banking, preference for cash in Tier 2 markets, and slow financial inclusion. They amplify broader trust erosion from phishing/vishing, contributing to switching behavior and underuse of UPI features.

**Mitigation and Protections (2026 Status)**

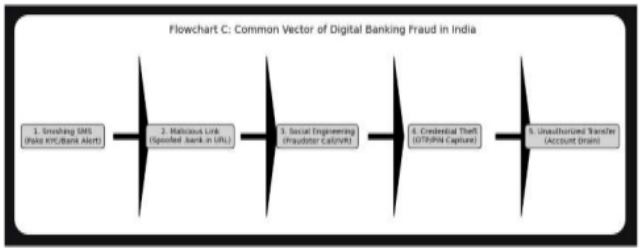
- RBI/NPCI Rules: Zero-liability for reported unauthorized transactions (golden hour: report in 0–2 hrs via 1930 helpline/app); proposed compensation up to ₹25,000 for small frauds; faster refunds for failed transactions.

- App Changes: Auto-flagging suspicious collect/QR; voice tutorials in regional languages; oneclick reporting.

- Prevention Tips: o Never enter UPI PIN to "receive" money/refund. o Verify unexpected credits via official app/bank SMS only. o Ignore unsolicited refund calls/QR/links. o Report immediately: 1930 cyber helpline, bank app, local police cyber cell. o Use UPI transaction limits; enable notifications.

The "refund" scam thrives on urgency and greed/fear—awareness remains the strongest defence, especially in Tier 2 cities where adoption outpaces education. Always verify before approving any UPI action.

The "Anatomy of an Indian Phishing Attack" – From SMS (Smishing) to Account Drain




"Source: Author's Compilation"

## 8. Regulatory Framework (RBI Guidelines 2026)

The research adheres to the following pillars:

- Incident Reporting: Mandatory 6-hour window for reporting breaches to RBI.
- Consumer Liability: Zero-liability for customers if the breach is at the bank's end and reported within 3 days.
- MFA (Multi-Factor Authentication): Mandatory transition from SMS-based OTP to "Appbased Authenticator" or "SIM-Binding" to prevent SIM-swap frauds. Understanding RBI's Cyber Security Framework for Banks: Levels 1 to 4 These charts are designed specifically to reflect the Indian banking landscape from 2021 through the projected 2026 environment, aligning with RBI's strategic focus on cyber resilience.




"Source: Author's Compilation"

## 10. Conclusion

Cybersecurity in 2026 is no longer an IT issue; it is a brand issue. For the Indian banking ecosystem to reach its full potential, trust must be engineered into the product. The study concludes that "Security Awareness" is the only firewall that never needs a software update. Banks must adopt a "Security-byDesign" approach where every feature is vetted for its impact on consumer confidence.

## References

1. Reserve Bank of India (2024). Master Direction on Cyber Resilience and Digital Payment Security Controls. 2. CERT-In (2025). Annual Report on BFSI Threat Landscape.
3. Fibac (2025). Consumer Survey: The State of Digital Banking in India.
4. Tripathi, A. (2025). "Quantifying Cyberattacks in Indian Financial Services," International Journal of Cybersecurity.
5. Ministry of Electronics and Information Technology (MeitY). The Digital Personal Data Protection Act, 2023: Implementation Guidelines.
6. Afzal, M., et al. (2025). How does cybersecurity awareness help in achieving digital financial inclusion? An extended UTAUT perspective in rural India. Journal of Financial Services Marketing. https://doi.org/10.1080/23742917.2024.2347674
7. Aljaradat, M., & Shukla, A. (2025). Trust and cybersecurity in digital payment adoption: Socioeconomic insights from India. Journal of Business and Socio-economic Development, 5(4), 372–390. https://doi.org/10.1108/JBSED-2025-0001
8. Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Journal of Financial Crime, 32(1), 31–50. https://doi.org/10.1108/JFC-10-2023-0263
9. Gopalan, S., & Devi, R. (2025). The impact of cybersecurity awareness on customers' trust and adoption of internet banking: A study in Palakkad

District, Kerala. International Journal of Innovative Research in Technology, 11(12), 833–841.

10. Jafri, J. A., Mohd Amin, S. I., Abdul Rahman, A., & Mohd Nor, S. (2024). A systematic literature review of the role of trust and security on Fintech adoption in banking. Heliyon, 10(1), e22980. https://doi.org/10.1016/j.heliyon.2023.e22980

11. Wadkar, P., et al. (2025). A UPI fraud case study from India. International Journal of Science, Engineering and Technology, 2(10).

12. (Various authors). (2025). Evaluating security concerns and user trust in UPI: A study of digital payment systems in India. ResearchGate publication. DOI not specified (preprint/ongoing).

13. (Various authors). (2025). Cybersecurity and trust formation in digital payment use behaviour in North India. ResearchGate publication.

14. CERT-In. (2025). Digital Threat Report 2024. National Critical Information Infrastructure Protection Centre, Government of India.

15. Reserve Bank of India. (2025–2026). Various circulars and reports on cybersecurity framework, UPI fraud statistics, and compensation schemes (e.g., RBI/2025-26/28 on .bank.in migration; draft guidelines on small-value fraud compensation).

16. NPCI & RBI. (2025–2026). Guidelines on UPI security enhancements, including collect request phase-out and fraud risk indicators