



Original Article

Cyber security Concerns and Consumer Trust in Digital Payments in India A Descriptive Analytical Study (2021–2024)

Jitendra Harichandra Raut

Assistant Professor of Commerce, Adarsh Arts, Commerce and Science College,
Desaiganj, Wadsa, Maharashtra, India

Manuscript ID:

RIGJAAR-2025-0204040

ISSN: 2998-4459

Volume 2

Issue 4

Pp. 221-225

April 2025

Submitted: 20 Feb 2025

Revised: 27 Feb 2025

Accepted: 15 Apr 2025

Published: 30 Apr 2025

Correspondence Address:

Jitendra Harichandra Raut
Assistant Professor of Commerce,
Adarsh Arts, Commerce and
Science College, Desaiganj,
Wadsa, Maharashtra, India
Email: jitraut8@gmail.com

Response Code:



Web: <https://rlgjaar.com>



DOI: 10.5281/zenodo.20769994

DOI Link:

<https://doi.org/10.5281/zenodo.20769994>



Creative Commons



Abstract

India's rapid adoption of digital payments, driven by the Unified Payments Interface (UPI), smartphone penetration, and digitalization initiatives, has transformed financial transactions. However, this growth has also increased cyber security risks such as phishing, OTP fraud, SIM-swapping, and data breaches. This study uses a descriptive analytical approach based on secondary data from the Reserve Bank of India (RBI), CERT-In, the National Payments Corporation of India (NPCI), and consumer trust surveys (2021–2024) to examine the impact of cyber security threats on consumer trust in digital payments. The findings reveal that rising cybercrime incidents negatively affected consumer confidence, particularly among first-time and semi-urban users, while regulatory measures helped mitigate some of these concerns. The study highlights the need for stronger cyber security frameworks and enhanced financial literacy to sustain trust in India's digital payment ecosystem.

Keywords: Cyber security, Consumer trust, Digital payments, UPI, Phishing, Data breach, Fintech, India, Mobile banking, OTP fraud

Introduction

India's digital payment ecosystem has expanded rapidly over the last decade, driven by UPI, smartphone penetration, and government initiatives promoting a less-cash economy. UPI transactions increased significantly between 2021 and 2024, making India a global leader in real-time digital payments. The growth of mobile banking, digital wallets, and other fintech innovations has enhanced financial inclusion and transformed everyday transactions across urban and rural areas.

However, the rapid adoption of digital payments has also increased cyber security risks, including phishing, OTP fraud, SIM swapping, QR code scams, and data breaches. Rising cybercrime incidents have raised concerns about consumer trust, particularly among first-time and semi-urban users. This study examines the relationship between cyber security threats and consumer trust in India's digital payment landscape during 2021–2024 using secondary data and descriptive analytical methods, with the aim of identifying trends and policy implications for strengthening digital payment security and user confidence.

Review of Literature

The relationship between cybersecurity and consumer trust has been widely examined in technology adoption research. Gefen, Karahanna, and Straub (2003) identified trust as a key factor influencing the adoption of digital technologies, while Pavlou (2003) found that trust mediates the effect of perceived risk on online transaction intentions. Similarly, Kim, Ferrin, and Rao (2008) highlighted system security, privacy protection, and institutional reputation as major determinants of consumer trust in digital payment environments.

In the Indian context, studies by Bhasin and Bhattacharjee (2022) and Das and Teng (2019) revealed that fraud experiences, security concerns, and privacy risks significantly reduce consumer confidence and digital payment adoption, particularly among first-time users. Arner, Barberis, and Buckley (2020) emphasized the role of strong regulatory frameworks in enhancing trust.

Creative Commons (CC BY-NC-SA 4.0)

This is an open access journal, and articles are distributed under the terms of the [Creative Commons Attribution-Noncommercial-ShareAlike 4.0 International Public License](https://creativecommons.org/licenses/by-nc-sa/4.0/), which allows others to remix, tweak, and build upon the work noncommercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.

How to cite this article:

Raut, J. H. (2025). Cyber security Concerns and Consumer Trust in Digital Payments in India A Descriptive Analytical Study (2021–2024). *Royal International Global Journal of Advance and Applied Research*, 2(4), 221–225. <https://doi.org/10.5281/zenodo.20769994>

Measures such as the RBI's Digital Payment Security Controls Framework, Fraud Risk Management Directions, and the Digital Personal Data Protection Act have strengthened security governance, although challenges related to enforcement and consumer awareness continue to affect their effectiveness.

Objectives of the Study

1. To examine the growth trend of digital payment transactions in India during 2021–2024.
2. To analyze the trend and nature of cyber security fraud incidents in digital payments during the study period.
3. To assess the impact of cyber security concerns on consumer trust in digital payment platforms.
4. To examine the moderating role of regulatory measures and consumer awareness on the trust–security relationship.
5. To evaluate implications for policy, industry practice and financial literacy in India.

Research Hypotheses

H1: An increase in reported cybersecurity fraud incidents is negatively associated with consumer trust in digital payment platforms.

H2: Stronger regulatory frameworks and consumer protection measures are positively associated with consumer confidence in digital payments.

H3: Consumer awareness and financial literacy are positively associated with the perceived security of digital payment transactions.

Research Methodology

1. Nature of the Study

The study is descriptive and analytical in nature, examining the behaviour of cybersecurity incidents and their influence on consumer trust without predictive econometric modelling.

2. Period of Study

The study covers 2021–2024—a period characterized by post-pandemic digital acceleration and a sharp escalation of financial cybercrime.

3. Sources of Data and Tools of Analysis

The study draws exclusively on secondary data from: (i) Reserve Bank of India—Annual Reports and Payment System Reports; (ii) National Payments Corporation of India (NPCI)—UPI Monthly Statistics; (iii) CERT-In Annual Cybersecurity Reports; (iv) Ministry of Home Affairs—National Cybercrime Reporting Portal (NCRP); and (v) published consumer-trust surveys by KPMG India (2024) and PwC India (2023). Trend analysis, percentage change computation and comparative interpretation are applied. Hypotheses are examined through directional pattern analysis across corroborating data sources; causal statistical modelling is not employed.

Growth of Digital Payment Transactions in India (2021–2024)

India's digital payment ecosystem expanded at a historically significant pace during the study period. The following tables present volume, value and instrument-wise distribution of digital transactions.

Table 1: UPI Transaction Volume and Value in India (2021–2024)

Year	Transactions (Crore)	Value (₹ Lakh Crore)	YoY Growth (%)
2021	3,885	83.4	—
2022	7,395	126.0	90.4%
2023	11,761	173.0	59.1%
2024	15,547	200.7	32.2%

Source: NPCI Monthly Transaction Statistics, 2021–2024.

UPI transactions grew nearly four-fold from 3,885 crore in 2021 to 15,547 crore in 2024. Growth rates moderated year-on-year as the base expanded, yet absolute volumes reflect deep structural integration of digital payments into everyday commerce. The corresponding

value growth from ₹83 lakh crore to ₹200 lakh crore underscores the macroeconomic significance of the digital payment channel and the scale within which cybersecurity threats operate.

Table 2: Digital Payment Instruments – Volume and Value Share (2023–24)

Payment Instrument	Volume Share (%)	Value Share (%)
UPI	66.8%	53.4%
IMPS / NEFT / RTGS	12.3%	37.2%
Debit / Credit Cards	14.7%	6.4%
Digital Wallets	4.9%	2.1%
Others (NACH etc.)	1.3%	0.9%

Source: RBI Report on Payment and Settlement Systems, 2023–24.

UPI commands 66.8% of digital payment volumes, underscoring its central role and the outsized implications of any UPI-related cybersecurity vulnerability for overall consumer trust and systemic payment stability.

Cyber security Threats in Digital Payments

Taxonomy of Fraud Types

The rapid growth of digital payments in India has been accompanied by a rise in cybersecurity threats. Major fraud types reported during 2021–2024 include phishing and vishing attacks, OTP fraud, SIM swapping, QR code

manipulation, identity theft, fake mobile applications, malware attacks, and Remote Access Tool (RAT) fraud. Most of these frauds exploit users through social engineering techniques, making human vulnerability a critical security concern alongside technological risks.

The incidence of financial cybercrime increased significantly during the study period. Reported cases rose from 2.35 lakh in 2021 to 7.40 lakh in 2024, representing an increase of approximately 215%. Similarly, the amount defrauded increased from ₹4,200 crore to ₹14,560 crore, reflecting a growth of nearly 247%. Despite various preventive measures, the recovery rate remained low, ranging between 10% and 13% throughout the period. The persistent rise in cyber fraud and the limited recovery of lost funds have contributed to growing consumer concerns regarding the safety of digital payment platforms, thereby affecting trust and confidence in the digital payment ecosystem.

Vulnerability of Specific Consumer Segments

KPMG India (2024) and RBI Ombudsman Annual Reports indicate that elderly users, first-time digital payment adopters and residents of Tier-2 and Tier-3 cities are disproportionately affected by cyber fraud. These groups share lower digital literacy, limited familiarity with fraud-detection cues and higher susceptibility to social engineering. Their victimisation causes direct financial harm and has a chilling effect on broader digital payment adoption within their communities, threatening the inclusivity goals of India's digital payment agenda.

Consumer Trust in Digital Payment Platforms

Consumer trust in digital payments comprises several dimensions, including confidence in platform security, trust in regulatory and legal protections, faith in the reliability of payment technologies, and positive perceptions shaped by peer experiences. Any decline in these dimensions can influence user behaviour, leading to reduced usage of digital payment platforms or a return to cash-based transactions.

Survey findings from 2021–2024 indicate a gradual decline in consumer confidence regarding digital payment security. The proportion of users rating digital payment security as 'High' or 'Very High' decreased from 62% in 2021 to 49% in 2024. During the same period, the percentage of users reporting at least one fraud attempt increased from 17% to 34%. The behavioural impact of fraud was also significant, with the share of fraud victims reducing their digital payment usage rising from 38% to 47%. Satisfaction with fraud grievance redressal declined from 36% in 2021 to 30% in 2023 before improving slightly to 35% in 2024. Similarly, trust in regulatory protection fell from 52% to 47% between 2021 and 2023 but recovered to 51% in 2024. These trends suggest that rising cyber fraud negatively affected consumer trust, while recent regulatory measures helped restore confidence to some extent.

Regulatory Framework and Consumer Confidence

The regulatory environment plays a pivotal role in building and sustaining consumer trust. The following measures were introduced or strengthened during the study period:

Table 5: Key Digital Payment Security Regulatory Measures in India (2021–2024)

Year	Measure	Objective
2021	RBI Digital Payment Security Controls Framework	Mandated strong authentication, transaction monitoring and fraud reporting for banks and PSPs
2022	Revised CERT-In Incident Reporting Rules	6-hour mandatory reporting of cybersecurity incidents for critical sector entities
2022	RBI Directions – Card Tokenisation	Replaced raw card data with tokens for online transactions, reducing data breach risk
2023	RBI Master Directions – Fraud Risk Management	Board-level oversight, early warning systems and fraud classification framework for banks
2023	DoT Telecom Cybersecurity Rules	SIM-swap verification controls and mandatory telecom fraud reporting protocols
2024	Digital Personal Data Protection Act (DPDPA)	Consent-based data processing, data localisation norms and breach penalty regime

Source: RBI Notifications; CERT-In Publications; Ministry of Electronics & IT; DoT, 2021–2024.

The progressive strengthening of the regulatory framework contributed to a modest but meaningful recovery in consumer trust by 2024. The DPDPA is particularly significant, granting users explicit rights over financial data and imposing stringent penalties on entities for data breaches. However, consumer awareness of these protections remains critically low: fewer than 30% of digital payment users in Tier-2 cities are aware of the RBI Ombudsman complaint scheme, limiting practical reach.

Hypothesis Testing: Detailed Analysis and Interpretation

Testing of Hypothesis 1

Hypothesis (H1): An increase in reported cybersecurity fraud incidents is negatively associated with consumer trust in digital payment platforms.

Analysis

Financial cybercrime cases grew from 2.35 lakh (2021) to 7.40 lakh (2024), a 215% increase. Concurrently, the

proportion of users rating digital payment security as 'high' or 'very high' fell from 62% to 49%. Fraud victims who reduced digital payment usage post-incident rose from 38% (2021) to 47% (2024). The clear inverse directional relationship across all consumer trust indicators and fraud data series is consistent with H1.

Inference

H1 is supported by observed trends across all secondary data sources.

Testing of Hypothesis 2

Hypothesis (H2): Stronger regulatory frameworks and consumer protection measures are positively associated with consumer confidence in digital payments.

Analysis

Six major regulatory measures were introduced between 2021 and 2024. The DPDPA enforcement and RBI Fraud Risk Management Directions in 2023–2024 coincided with a recovery in trust in regulatory protection (from 47% in 2023 to 51% in 2024) and improved grievance satisfaction (from 30% in 2023 to 35% in 2024). Despite the continued rise in absolute fraud cases, the moderation in the trust decline and the partial recovery align positively with regulatory strengthening, consistent with H2.

Inference

H2 is supported by the positive directional alignment between regulatory development and consumer confidence recovery.

Testing of Hypothesis 3

Hypothesis (H3): Consumer awareness and financial literacy are positively associated with the perceived security of digital payment transactions.

Analysis

KPMG India (2024) data indicate that users who received at least one form of cybersecurity literacy intervention were 2.3 times more likely to rate their payment platform as 'secure'. Fraud-aware users showed significantly lower rates of permanent digital payment disengagement post-fraud (28%) compared to low-awareness users (52%), confirming that financial literacy is both a fraud-prevention factor and a trust-restorative mechanism. This finding has particularly strong policy implications for semi-urban and rural India.

Inference

H3 is supported. Consumer awareness is a key moderator of cybersecurity risk perception and trust resilience.

Findings of the Study

- UPI transactions grew nearly four-fold from 3,885 crore (2021) to 15,547 crore (2024), making India one of the world's largest real-time payment markets; yet this growth also intensified exposure to cybersecurity threats.
- Financial cybercrime cases more than trebled (2.35 lakh to 7.40 lakh) during 2021–2024, with amounts defrauded rising 247%, while recovery rates remained below 14%—highlighting the structural challenge of fraud restitution.
- Consumer security trust in digital payments declined from 62% (2021) to 49% (2024), directly inversely

tracking the escalation in fraud incidents, confirming H1.

- Nearly 47% of fraud victims reduced their digital payment usage post-incident in 2024, indicating significant behavioural consequences that threaten digital payment adoption momentum.
- Regulatory strengthening in 2023–2024—particularly DPDPA and RBI Fraud Risk Management Directions—contributed to a partial trust recovery, supporting H2; however, consumer awareness of redressal mechanisms remains critically low in Tier-2/3 cities.
- Digitally and financially literate users demonstrated both lower fraud vulnerability and greater trust resilience post-fraud, validating H3 and underscoring the strategic importance of financial literacy.
- OTP fraud, phishing and SIM swapping dominate reported fraud categories, identifying human-factor vulnerabilities as primary attack vectors requiring behavioural and awareness-based countermeasures.
- Elderly users, first-time digital adopters and residents of smaller cities are disproportionately affected, creating a trust deficit that threatens the inclusivity of India's digital financial inclusion agenda.

Suggestions

- Strengthen the RBI's Unified Fraud Management System to enable real-time fraud detection, cross-institutional information sharing, and faster freezing of suspicious transactions.
- Conduct large-scale multilingual cybersecurity awareness campaigns, particularly targeting rural, semi-urban, and elderly users, while promoting digital payment safety through educational institutions and adult literacy programmes.
- Ensure effective implementation of the Digital Personal Data Protection Act (DPDPA) and introduce clear compensation mechanisms for consumers affected by data breaches or digital payment fraud.
- Improve consumer grievance redressal by simplifying access to the RBI Ombudsman scheme and providing easy in-app complaint and dispute-resolution facilities.
- Encourage banks and payment service providers to adopt AI-driven fraud detection systems, user-controlled transaction limits, cooling-off periods, and advanced security measures such as encryption and tokenisation.
- Promote community-based digital literacy initiatives through self-help groups (SHGs), panchayats, NGOs, and local institutions to enhance cybersecurity awareness and strengthen consumer trust in digital payments.

Limitations of the Study

The study relies exclusively on secondary data and descriptive methods; causal statistical relationships are not empirically tested. Reported cybercrime figures likely understate actual fraud incidence due to significant under-reporting, particularly among rural and elderly victims. Consumer trust data drawn from third-party surveys may

reflect sampling biases. The national-level analysis does not disaggregate findings at the state or district level, potentially masking regional heterogeneity. Future research may employ primary survey data, structural equation modelling or longitudinal panel data analysis for deeper empirical validation.

Conclusion

This study examined cybersecurity concerns and their relationship with consumer trust in India's digital payment ecosystem during 2021–2024 using a descriptive analytical framework based on secondary data. India's digital payment ecosystem grew to extraordinary scale during the study period, yet this expansion was accompanied by a near trebling of financial cybercrime cases, a 247% rise in amounts defrauded and a significant decline in consumer security trust from 62% to 49%.

The evidence consistently supports all three hypotheses: fraud escalation erodes consumer trust (H1), regulatory strengthening moderates this erosion and aids partial recovery (H2), and consumer awareness and financial literacy are key protective and restorative factors (H3). The partial trust recovery observed in 2024, coinciding with major regulatory developments, demonstrates that policy-driven trust restoration is achievable.

Ultimately, the long-term sustainability of India's digital payment revolution hinges on establishing a secure, trustworthy and inclusive ecosystem. Cybersecurity is not merely a technical challenge—it is a foundational precondition for sustainable digital financial inclusion and India's aspiration to become a \$1 trillion digital economy. Coordinated action by regulators, payment service providers, technology firms, civil society and consumers is essential to secure and advance this digital future.

Acknowledgment

The author expresses sincere gratitude to all those who contributed to the successful completion of this research paper titled “Cyber Security Concerns and Consumer Trust in Digital Payments in India: A Descriptive Analytical Study (2021–2024)”.

Special thanks are extended to colleagues, academic mentors, and institutional authorities of Adarsh Arts, Commerce and Science College, Desaijanj (Wadsa), Maharashtra, for their continuous encouragement, valuable guidance, and academic support throughout the study.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Arner, D. W., Barberis, J., & Buckley, R. P. (2020). Fintech, regtech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business*, 37(3), 371–413.
2. Bhasin, M., & Bhattacharjee, A. (2022). Trust and loyalty in mobile payment adoption: Evidence from India. *Journal of Financial Technology*, 14(2), 88–104.
3. CERT-In. (2021–2024). Annual Cybersecurity Reports. Ministry of Electronics & Information Technology, Government of India. <https://www.cert-in.org.in>
4. Das, R., & Teng, J. (2019). Security perceptions and mobile payment adoption in urban India. *International Journal of Electronic Commerce Studies*, 10(1), 45–68.
5. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51–90.
6. Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce. *Decision Support Systems*, 44(2), 544–564.
7. KPMG India. (2024). Digital Payments and Fraud: A Consumer Trust Perspective. KPMG India Insights.
8. Ministry of Home Affairs. (2021–2024). Annual Report – National Cybercrime Reporting Portal (NCRP). Government of India.
9. NPCI. (2021–2024). UPI Monthly Transaction Statistics. National Payments Corporation of India. <https://www.npci.org.in>
10. Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134.
11. PwC India. (2023). India FinTech Report: Digital Payments and Cybersecurity. PricewaterhouseCoopers.
12. Reserve Bank of India. (2021–2024). Annual Report on Trend and Progress of Banking in India. RBI Publications.
13. Reserve Bank of India. (2021–2024). Report on Payment and Settlement Systems in India. RBI.
14. Reserve Bank of India. (2023). Master Directions on Fraud Risk Management. RBI.
15. Reserve Bank of India. (2021). Digital Payment Security Controls Framework. RBI Notifications.
16. World Bank. (2023). Digital Financial Services: Risks and Regulatory Considerations. World Bank Group.