International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Rise of UPI Fraud in India: Vulnerability Analysis and Prevention Framework

Aniket Garg
Chitkara University

Abstract- The rapid growth of the Indian digital payments ecosystem which is controlled mainly by the Unified Payments Interface (UPI) has improved financial inclusion whilst alleviating transaction friction. Meanwhile, the magnitude, speed, and functionality of UPI have increased vulnerability to phishing, impersonation, scams, and synthetic identities, mule accounts, and AI-enforced social engineering. The paper under consideration investigates the UPI fraud proliferation in India through the qualitative analysis of official circulars, payment data, cybersecurity reports, and the latest regulatory interventions. It has been shown in the analysis that user confusion, ineffective verification conduct, quick payment rails that cannot be reversed, and more advanced threat agents are the proximal factors influencing the rise in fraud. A multi-level framework of prevention that incorporates beneficiary authentication, concatenation of devices, behavioural danger rating, mule-account recognition, consumer knowledge, and amplified inter-institutional reports is proposed. The paper concludes that future achievements in minimizing fraud through the integration of scale-induced innovation with security-by-design and timely redress framework will be dependent on it. [1], [3], [4], [5].

Keywords – UPI fraud, digital payment, fraud in India, cybercrime, phishing, deepfake fraud, fintech risk, RBI, NPCI, fraud prevention.

I. INTRODUCTION

The digital payment ecosystem in India has undergone a structural change in the last 10 years. The interoperability, immediate settlement, acceptance of QRs, and the convenience of the application has made UPI the major low-cost retail payment channel. According to public data offered by the National Payments Corporation of India (NPCI), UPI finalized 18.68 billion transactions in May 2025 (increasing the volume of transactions by 18.68 billion in May 2024), and the volume of transactions finalized amounted to 25.14 lakh crore (in May 2024, the same number had increased to 25.14 lakh crore). The success and strain of this development are two-fold: with the expansion of the network, it becomes more and more appealing to fraudsters.

In contrast to legacy fraud in card or branch banking, fraud against UPI is largely based on social engineering in lieu of a more technical compromise. Trust, urgency, and confusion with the user-interface are used by attackers through counterfeit payment links, collection requests, manipulation of QR-codes, screen-sharing, claims of KYC updates, impersonation calls and the use of more and more authentic AI-generated voice or video. What it has created is a world of fraud whereby technical control measures are not sufficient unless they are supplemented by user awareness, monitoring by the banks, and quick banking synchrony.

The paper aims at achieving three goals: defining the main reasons of UPI fraud proliferation in India, discussing the weaknesses on the user and system levels that can support such fraud, and suggesting an effective prevention framework in accordance with the new regulatory and operational response. [1], [9], [16].

II. RELATED WORK

The literature available on digital payment fraud in India highlights the conflict between adoption and security preparedness. The customer liabilities principle of RBI provides a focus on timely reports and recurrent customer notifications as the fundamental security measure [2]. The new fraud-risk framework that was introduced by RBI to regulated entities also puts the emphasis not on the post-facto reporting but on the prevention of the frauds, their early identification, and the governance as well as the observation of the mule accounts and the suspicious activity [3].

According to recent threat-intelligence resources in the banking, financial services, and insurance sector, the digital risk has become more antagonistic. According to the Digital Threat Report 2024 by CERT-In, in India, phishing attacks in the financial industry have increased by 175 per cent in the first half of 2024 compared to the same period of the year before [4]. The targeted modern-day fraud involving

deepfakes discussions further indicate that generative AI is fueling the extent, the quality and the persuasiveness of fakehood, especially in scams that evolve around impersonation [5].

Much of this writing is, however, divided up in policy notes, circulars, cybersecurity reports, and media summaries. A specialized academic style synthesis that includes UPI fraud is thus useful in that there is a relationship between the growth of transactions, development of attacks, regulatory reaction along with gaps in implementation in a unified analytical model.

III. RESEARCH AND METHODOLOGY

The investigation methodology used is a qualitative review. A total of four categories of sources were used to select secondary sources, namely: official payments statistics, regulatory and institutional circulars, reports of cyber security threats, and plausible explanatory analyses. All sources were analysed regarding evidence related to four dimensions including transaction growth, typology of fraud, structural vulnerability, and preventive measures.

The thematic coding method was used in the analysis. Observations reported were categorized into user vulnerabilities, operational, platform, and policy or technical controls. Where the percentage changes were only available, the study used them as a guide of the risk intensification and not an overall measure of the absolute fraud incidences. [1], [3], [4], [15].

IV. UPI FRAUD ECOSYSTEM AND ANALYSIS

User-Level Vulnerabilities
A considerable percentage of UPI frauds work since attackers can control user behaviour during the time of decision. Most users are still not accustomed to the difference between accepting money and placing a debit request. This confusion is exploited by fraudsters who make collection request in the form of refund, reward, or KYC confirmation requests. It is the same with QR-based scams where the user is convinced to scan a code to get money, despite the fact that a payment activity is usually triggered.

Smartphone reliance and trust in a conversation is a factor that intensifies social engineering. Victims can be persuaded by initiating calls that purport to be banks, e-commerce outlets or customer-care desks. The attacker is able to monitor credentials, manipulate taps, or cause unauthorised transfers once a victim has installed a remote-access or screen-sharing application. Lack of awareness on complaint-escalation routes is also a factor that slows down the reporting and the probability that money could become frozen. [2], [6], [17].

System-/Platform-Level Vulnerabilities
Unified Payments Interface (UPI) is designed to be fast and intraoperative; however, the same features create significant enforcement and recovery issues. Payments are handled almost immediately, hence with only a small margin of time to make manual checks. Fraudulent proceeds are usually washed via mule accounts, in more than one account, or expeditiously. The old banking systems were never structured to support the scale and speed of the modern digital fraud trends and as such, detection of anomalies in real-time is a challenge in some institutions.

Another issue is that there is the imbalance between a smooth customer experience and a strong authentication. Even though a design that allows a frictionless adoption towards adoption is preferable, poor contextual checking can be used to support dishonest activity. Before the recent intervention, the users were often relying on application branding or informal indicators of trust rather than official proof of the beneficiary. Exposure to API, reliance on third-party applications, and unequal fraud mitigation across participating institutions could also widen the attack surface where there is no further consistent governance. [5], [10], [12], [13].

Threat Typology
Phishing, vishing, smishing, attempting account-takeover via impersonation, joining a merchant as a fake account, synthetic identities, mule-account abuse, malicious applications, spoofed screenshots, scam dispute-resolution agents and AI-generated deepfakes calls or videos are examples of the modern UPI fraud ecosystem. The similarity to these modalities of attack is the turn of trust into authorization. The criminal goal focuses on convincing a legitimate user to perform, reveal, or ignore an operation at a significant point, instead of trying to break cryptographic processes. [3], [4], [18].

Types of UPI Fraud
UPI has transformed the process of digital payment making it possible to transfer funds in an instant and more conveniently than ever before. However, this fast growth has simultaneously increased the exposure of the users to the range of fraudulent activities. UPI fraud normally follows in the footsteps of the fraudsters who utilise trust, lack of awareness or technological flaws of the user to gain unauthorised access to finances. Phishing is one of the most common types, as scammers send fake messages, links, or fake customer-care emails to cheat users into sharing their sensitive data (UPI PINs, OTPs, or bank account details).

The other notable type is QR -code fraud whereby attackers post virulent or deceitful QR codes that fool users into

thinking that scanning the code will enable them to receive money, but in reality, it triggers a payment prompt. Similarly, collect-request scam is closely practiced in UPI systems, as users unknowingly approve request money requests, hence leading to unwanted money transfer. Screen-sharing programs are also used to access sensitive banking information remotely by the fraudsters when making fake support calls.

SIM -swap fraud represents another sophisticated scheme, whereby criminals gain access to the user mobile number; thus, gaining access to the OTP based authentication schemes associated with bank accounts.

Besides, fake mobile apps and duplicated payment interfaces are also used more to collect user login credentials and PIN. The social-engineering-based scams, including impersonation of bank officers, merchants, or other acquaintances, are significantly effective because they would work in the human psyche instead of the vulnerabilities in the system.

These kinds of frauds show that UPI fraud does not just exist as technical attacks; it is a combination of manipulation by humans, misappropriation of the platform and the vulnerability of the digital environment. Therefore, it is essential to understand the types of fraud to create effective checking and detection mechanisms. [2], [4], [11], [17].

V. PREVENTION FRAMEWORK AND IMPLEMENTATION CONSIDERATIONS

The prevention of fraud in UPI should be performed in a layered manner as opposed to a single point of check. On the user level, recurring awareness efforts are to be put on the behavioural indicators: never use UPI PIN to get money, never install remote-access software to obtain customer support, and seek independent means of confirmation of a pressing request.

At platform level, spoofing and unauthorized portability is avoided by verifying beneficiary-name and binding devices. This is a massive lep towards the right direction based on NPIC 2025 circular that requires display of beneficiary name in transactions of UPI.

On the institutional level, banks and fintechs are required to adopt adaptive risk scoring, velocity limit, device and behavioural detecting anomalies, merchant due diligence and graph-based mule-account detection. RBI 2024 directions on fraud-risk clearly highlight the need to prevent, detect and monitor early signs of unusual transactions and money-mule accounts.

Interoperable reporting and complaint resolution is necessary at the ecosystem level. The online dispute resolution system on the digital payments by RBI was brought in so as to create a more clear and system-driven grievance system. In combination with complaint-handling portals, internal fraud registries and greater coordination of law enforcement, such a structure can help decrease the time gap between the occurrence of fraud, its reporting, and remedial measures. [3], [5], [6], [7], [8], [10].

VI. RESULTS AND ANALYSIS

The evidence reviewed reveals a central paradox in the scale of UPI, namely, its ability to be scaled in real-time is the same factor that increases exposure to fraud when a trust system fails to scale with an increase in transaction volume. Figure 1 and figure 3 are illustrations of the disproportion between ecosystem growth and conflict escalation. The volume and the value of payment system has grown rapidly and at the same time, fraud indicators and sophistication of attacks have also grown.

One of the analytical results is that the majority of UPI fraud can be classified as social-technical, but not entirely technical. Most attack vectors are exploited due to human approval, lax verification, or slow responses as opposed to cryptographic violations. As a result, the effectiveness of prevention depends on making the decisions more ambiguous to the users, supplementing the verification of contextual identities, and decreasing the time interval in which the stolen money can be dispersed.

The fact also indicates that institutional responses are on the right way. The presentation of the name of the beneficiary improves transparency of the transactions. Guidelines in the management of fraud-risks create an enhanced governance expectation. ODR and integrated complaint channels enhance post-incident management.

However, the measures will have the best results when used together with interoperable intelligence sharing, uniform application warnings, and increased detection of coordinated mule-account networks.

Policy wise, the reported rise in incidences cannot be viewed as an indication of control failure only. Part of the increase could also be due to better reporting habits, increased awareness of the users and additional use of the system.

Nevertheless, the fast rate of innovation in attack means that investment on security needs to match the pace of payment adoption at least. Practically, UPI can be kept at low-friction in real-life situations but can be turned into high-friction in suspicious situations by risk-adaptive controls. [1], [3], [4], [5], [6].

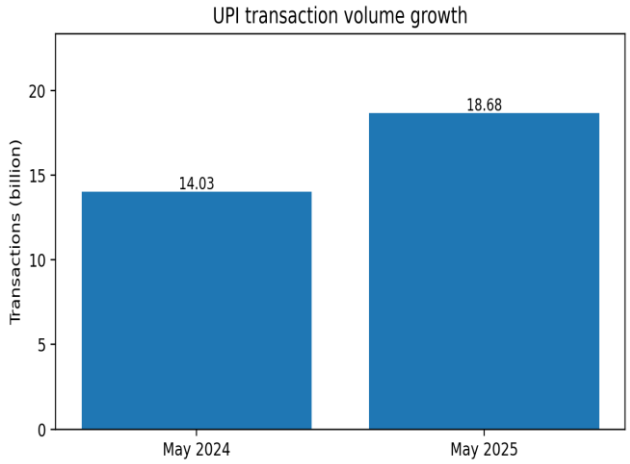

Figure 1. UPI transaction volume growth

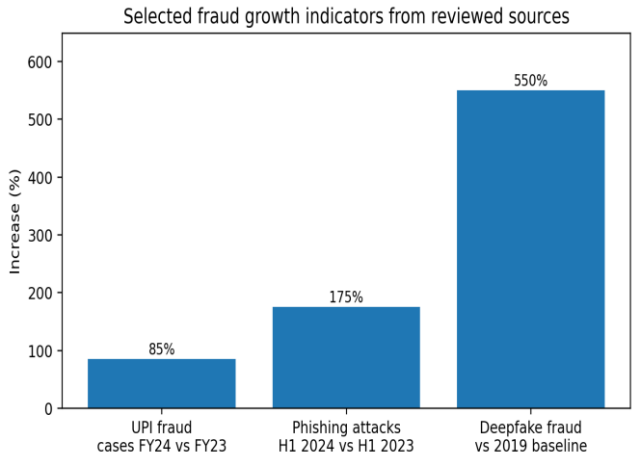

Figure 2. Selected fraud growth indicators from reviewed sources

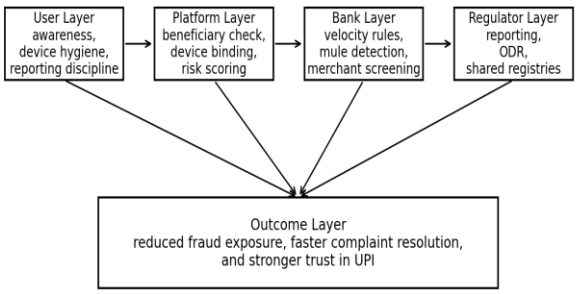

Figure 3. Multi-layer prevention framework for UPI fraud mitigation

TABLE 1. SELECTED INDICATORS USED IN THE ANALYSIS

Indicator	Reported value	Interpretation
UPI transaction volume (May 2025)	18.68 billion	Shows network scale and attractiveness to fraudsters
UPI transaction value (May 2025)	Rs. 25.14 lakh crore	Indicates the systemic importance of the payment rail
Increase in UPI fraud cases FY24	85% over FY23	Signals rapid fraud growth relative to adoption
Increase in BFSI phishing H1 2024	175% y/y	Shows escalation of social-engineering exposure
Deepfake-related fraud since 2019	550% increase	Highlights AI-enabled deception risk

VII. DISCUSSION

The emergence of UPI fraud shows that digital inclusion and digital resilience are to be advanced at the same time. The payment architecture in India has been of world interest in lowering transaction costs and extending the formal finance but the prevention of fraud has now become a design goal and not a downstream service problem. This requires a greater cooperation of banks, payment service providers, telecommunications channels, and cybercrime agencies and campaigns to create awareness to the people.

This study can be followed three directions in the future. To begin with, more quantitative analysis would be possible with empirical data on types of fraud, the delay in customer reporting and rate of fund-recovery. Second, application usability tests might determine the ability of certain interface indicators to alleviate collect-request or QR-code fraud. Third, mule-account networks graph analytics could reveal recurring patterns of paths that traditional rule-based monitoring could ignore.

The problem of UPI fraud in India is not the mere side effect of digitalisation, but a systemic risk posed by the combination of user behaviour, platform design, institutional readiness, and the fast-changing cybercrime strategies. The examination in this paper suggests that deception via phishing and lax

verification customs, immediate transfer of funds and by growing application of artificial intelligence in impersonation is accelerating fraud. At the same time, new actions of NPCI and RBI indicate strengthening the position of governance and control.

The conclusion here is that the next stage of success of UPI will rely on the measures that would preserve the trust. Security has to be integrated with the means of beneficiary verification, device based monitoring and behaviour based monitoring, faster complaint escalation, and specific user education. Therefore, a multi-level and integrated prevention approach is the key to keeping faith in the digital payment system in India. [3], [5], [6], [19], [20].

VIII. CHALLENGES AND LIMITATIONS

The emergence of UPI fraud shows that digital inclusion and digital resilience are to be advanced at the same time. The payment architecture in India has been of world interest in lowering transaction costs and extending the formal finance but the prevention of fraud has now become a design goal and not a downstream service problem. This requires a greater cooperation of banks, payment service providers, telecommunications channels, and cybercrime agencies and campaigns to create awareness to the people.

This study can be followed three directions in the future. To begin with, more quantitative analysis would be possible with empirical data on types of fraud, the delay in customer reporting and rate of fund-recovery. Second, application usability tests might determine the ability of certain interface indicators to alleviate collect-request or QR-code fraud. Third, mule-account networks graph analytics could reveal recurring patterns of paths that traditional rule-based monitoring could ignore.

The problem of UPI fraud in India is not the mere side effect of digitalisation, but a systemic risk posed by the combination of user behaviour, platform design, institutional readiness, and the fast-changing cybercrime strategies. The examination in this paper suggests that deception via phishing and lax verification customs, immediate transfer of funds and by growing application of artificial intelligence in impersonation is accelerating fraud. At the same time, new actions of NPCI and RBI indicate strengthening the position of governance and control.

The conclusion here is that the next stage of success of UPI will rely on the measures that would preserve the trust. Security has to be integrated with the means of beneficiary verification, device based monitoring and behaviour based monitoring, faster complaint escalation, and specific user education. Therefore, a multi-level and integrated prevention approach is the key to keeping faith in the digital payment system in India. [3], [4], [12], [19].

IX. FUTURE SCOPE

Intelligent, adaptive and user-friendly security frameworks are the future scope of the UPI fraud prevention. One of the directions is the implementation of machine learning and artificial intelligence to detect fraud in real-time. Greater analytics can be used to examine transaction behaviour, device usage history, user activity history, and anomaly alerts to detect suspicious transactions better than the previous more traditional methods. These systems are capable of learning new fraud cases and changing their strategy to attacks continuously.

The other potential solution is the use of behavioural analytics. Further systems may not be limited to just credentials or transaction values, and in the future, they can consider typing speed, timing of transaction, location consistency, device fingerprints, and spending patterns in order to build a more resilient risk profile. This would go a long way in early fraud detection. Similarly, the multi-factor authentication and biometric verification methods can also be enhanced to curb unauthorised access and the fraudulent activities based on impersonation.

Fraud awareness implemented as part of payment applications can also be investigated in future. Human error can be reduced by providing context-sensitive alerts, fraud-education pop-ups, warning signs about suspicious QR-codes, and user confirmation prompt. Also, cooperation between banks, fintech firms, telecommunication companies and regulators can facilitate a higher level of fraud intelligence exchange and prompt blacklisting of suspicious subjects.

The other scope is development of explainable models of fraud detection where users and institutions are able to know why a particular transaction was indicated as being a risky one. This would improve the trust, transparency and usability. All in all, the future of the UPI security lies in integrating robust technical defence mechanisms with constant user education and cross-platform integration. [3], [4], [10], [20].

X. CONCLUSION

Unified Payments Interface (UPI) has become one of the most popular innovations in the sphere of the digital payment system, providing millions of people with rapidity, convenience, and financial inclusion. However, with the increase in the uptake of UPI, the possibility of fraud has grown significantly. The phishing, QR code fraud, counterfeit collection request, SIM-swap attacks, and social engineering

are some of the techniques used by fraudsters: they can take advantage of both technical and human weaknesses.

This paper highlights that UPI fraud is a complex issue that cannot be averted by technical protection only. The combination of safe system architecture, real-time monitoring, advanced fraud-detection systems, and intensive user education is essential towards effective prevention. In spite of the fact that present solutions can provide a basic level of protection, constraints like limited datasets, continuously evolving types of fraud, and high false-positives still reduce the general performance of the fraud-prevention systems.

Subsequent improvements to UPI fraud control as suggested by the analysis include intelligent methods of detection, behavioural monitoring, highly authenticated procedures and user-conscious design. Finally, ensuring the UPI ecosystem is crucial not only to protect the users against financial loss but also to maintain trust in the technologies of digital payments. Users, banking institutions, payment service providers, and regulatory bodies must work together in order to create a more resilient and more-fraud-resistant digital payment environment. [2], [3], [5], [6], [8].

REFERENCES

1. National Payments Corporation of India, "Unified Payments Interface (UPI) Product Statistics," NPCI, 2025.
2. Reserve Bank of India, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," RBI/2017-18/15, Jul. 6, 2017.
3. Reserve Bank of India, "Master Directions on Fraud Risk Management in Regulated Entities, 2024," Jul. 15, 2024.
4. CERT-In, "Digital Threat Report 2024," 2025.
5. National Payments Corporation of India, "Addendum to OC-101: Strengthening beneficiary name verification and display during UPI transactions," Apr. 24, 2025.
6. Reserve Bank of India, "Online Dispute Resolution (ODR) System for Digital Payments," Aug. 6, 2020.
7. Reserve Bank of India, "Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems," Sept. 20, 2019.
8. Reserve Bank of India, "The Reserve Bank – Integrated Ombudsman Scheme, 2021: FAQs," 2021.
9. National Payments Corporation of India, "UPI: Unified Payments Interface – About UPI," NPCI.
10. National Payments Corporation of India, "Risk Management," NPCI.
11. National Payments Corporation of India, "User Complaint Status / UPI safety guidance," NPCI.
12. Reserve Bank of India, "Master Direction – Know Your Customer (KYC)," updated 2025.
13. Reserve Bank of India, "Payment and Settlement Systems Act, 2007: FAQs," RBI.
14. Reserve Bank of India, "Payment and Settlement System – FAQs," RBI.
15. National Payments Corporation of India, "Unified Payments Interface Circulars," NPCI.
16. National Payments Corporation of India, "UPI product page," NPCI.
17. Reserve Bank of India, "Customer Liability in Unauthorised Electronic Banking Transactions – Public guidance," RBI.
18. AuthBridge, "Digital Threat Report 2024 for the BFSI Sector – summary," 2025.
19. Reserve Bank of India, "National Strategy for Financial Inclusion 2019–2024," RBI.
20. National Payments Corporation of India, "Customer Experience and Confidence in Digital Payments," NPCI.