ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 12, Issue 5, September – October 2025

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.028

+91 9940572462 +91 9940572462 ijarasem@gmail.com www.ijarasem.com

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 | Bimonthly, Peer Reviewed & Refereed Journal|

| Volume 12, Issue 5, September - October 2025 |

A Survey on UPI Fraud Detection System

Prof. Sujata Jogdand-Gaikwad[1], Chetan Choudhary[2], Harsh Sharma[3], Abhishek Birajdar[4], Sushil Yadav[5], Vaibhav Raskar[6]

Department of Computer Engineering, Alard College of Engineering and Management, Pune, India[1 - 6]

ABSTRACT: Unified Payments Interface (UPI) has revolutionized digital transactions in India by enabling seamless, real-time money transfers through mobile platforms. However, the rapid rise in UPI usage has also led to an increase in fraudulent activities such as phishing, social engineering, and unauthorized transactions. This survey report titled **"Fraud Shield UPI"** focuses on analyzing the various types of UPI frauds, their underlying causes, and the security challenges faced by users and service providers. The report further reviews existing fraud detection techniques, user awareness levels, and the preventive mechanisms implemented by regulatory authorities and financial institutions. By consolidating research findings, user surveys, and case analyses, this study aims to identify the effectiveness of current fraud prevention strategies and propose recommendations for enhancing transaction security. The ultimate goal of **Fraud Shield UPI** is to contribute towards building a safer and more trustworthy digital payment ecosystem.

KEYWORDS: Unified Payments Interface (UPI), Digital Payments, Fraud Detection, Cybersecurity, Phishing, Social Engineering, Transaction Security, Financial Fraud, Machine Learning, User Authentication, Data Protection, Risk Mitigation, Secure Transactions, Real-Time Monitoring, Regulatory Compliance, Payment Gateway Security, Fraud Prevention, Mobile Banking, Secure FinTech, Digital Trust.

I. INTRODUCTION

The rapid digitalization of financial systems has transformed the way people conduct transactions, with the **Unified Payments Interface (UPI)** emerging as one of India's most successful digital payment innovations. Introduced by the **National Payments Corporation of India (NPCI)**, UPI enables instant money transfers between bank accounts through smartphones, offering convenience, speed, and accessibility to millions of users. However, as the adoption of UPI grows exponentially, so does the threat of **cyber frauds and financial scams** that exploit vulnerabilities in digital platforms and user awareness.

The rise of **UPI-related frauds**—such as phishing, vishing, fake payment links, app cloning, and social engineering—has raised significant concerns about transaction security and user trust. These fraudulent activities not only cause financial losses to individuals but also affect the overall reliability of the digital payment ecosystem. Consequently, there is an urgent need for robust mechanisms to detect, prevent, and respond to such fraudulent activities in real time.

This survey report titled **"Fraud Shield UPI"** aims to analyse the different types of UPI frauds, examine current fraud detection techniques, and assess the effectiveness of existing preventive measures. The report also highlights user behaviour, awareness levels, and the role of emerging technologies such as **machine learning, AI-based anomaly detection, and multi-factor authentication** in enhancing transaction security. By identifying gaps and proposing improved strategies, this study contributes toward building a **secure and fraud-resilient UPI ecosystem**.

II. LITERATURE SURVEY

1. Regulatory & institutional framework

The National Payments Corporation of India (NPCI) and the Reserve Bank of India (RBI) have steadily expanded operational and risk-management guidance for UPI participants, issuing circulars and fraud-risk management frameworks that mandate stronger merchant onboarding, transaction monitoring and customer-communication norms. NPCI also offers value-added real-time monitoring services to member banks and PSPs to help detect suspicious patterns.

2. Statistical trends and impact

Recent government and industry data show a sharp rise in reported UPI fraud incidents over the last few financial years, with large year-on-year increases in both case counts and amounts lost, prompting policy responses and awareness campaigns. At the same time, some RBI releases and industry analyses indicate mixed short-term improvements in specific categories after targeted interventions. These statistics highlight both the scale of the problem and the dynamic nature of fraud trends.

3. Taxonomy of UPI frauds

Academic studies, research organizations and investigative reports commonly classify UPI frauds into: (a) social-engineering scams (phishing, vishing, fake callbacks and fake merchant requests), (b) malware and device compromise (credential harvesting, overlay/OTP-stealing apps), (c) SIM-swap and SIM-related attacks, (d) merchant/QR code tampering and cloning, and (e) money-mule networks used for laundering proceeds. Social engineering remains the dominant vector in many datasets, while malware and mule accounts provide the financial plumbing that enables large losses.

4. Fraud detection techniques — rule-based and statistical methods

Early and widely deployed defences rely on deterministic, rule-based filters (velocity checks, blacklists, risk scoring by device/IP, geolocation heuristics) and manual transaction review. These approaches are fast and interpretable but struggle with evolving, low-signal fraud patterns and produce false positives that affect user experience. NPCI and banks combine these rules with business-logic checks for merchant and PSP compliance.

5. Machine learning and anomaly-detection approaches

A growing body of academic and practitioner research proposes machine-learning (ML) models for UPI fraud detection: supervised classifiers (random forests, XGBoost), unsupervised/semi supervised anomaly detectors, sequence models such as Hidden Markov Models (HMM) to capture temporal behaviour, and hybrid systems that fuse rules and ML. Recent project and conference papers report promising accuracy gains but also flag challenges: class imbalance, feature engineering for mobile/UPI-specific signals, model explainability, and latency constraints for real-time blocking.

6. Non-technical countermeasures and awareness studies

Surveys and industry reports stress that user education (recognising phishing links, secure smartphone practices, reporting channels) and ecosystem controls (SIM/IMEI blocking, stronger app sandboxing, merchant vetting, prompt dispute resolution) are critical complements to technical detection. Reports emphasize that adoption often outpaces awareness — making social-engineering scams persistently effective — and call for coordinated industry-government awareness drives.

7. Gaps identified in the literature

Across regulator publications, industry analyses, and academic papers the main gaps are consistent: (a) limited access to high-quality, labelled transaction datasets for robust ML research; (b) difficulties in real-time deployment due to latency and interpretability needs; (c) adversarial adaptation by fraudsters (e.g., use of mule accounts, device compromise); and (d) insufficient focus on end-to-end user experience when preventing false positives. These gaps point to research and operational priorities: privacy-preserving data sharing, lightweight explainable models, integrated device-level telemetry, and stronger coordination on mule-account detection.

8. Opportunities for “Fraud Shield UPI” research

Based on the surveyed literature, promising directions for the Fraud Shield UPI project include: building hybrid rule+ML pipelines optimized for mobile/UPI telemetry; exploring sequence and graph-based models to detect mule networks; developing model interpretability layers to support investigator workflows; and designing user-centric alerting that reduces friction while ensuring security. Pilots that combine NPCI’s real-time monitoring capabilities with bank-level telemetry and anonymized transaction sharing can accelerate practical improvements.

III. PROBLEM STATEMENT

The Unified Payments Interface (UPI) has become the backbone of India’s digital payment ecosystem, offering fast, convenient, and secure real-time fund transfers. However, with the exponential increase in UPI transactions, there has also been a significant surge in fraudulent activities such as phishing, social engineering, fake payment requests, and unauthorized access to user accounts. Despite the implementation of various security measures by banks, fintech firms, and the National Payments Corporation of India (NPCI), the frequency and sophistication of UPI frauds continue to rise. The main problem lies in the inadequate detection and prevention mechanisms that fail to effectively identify evolving fraud patterns in real time.

Additionally, limited user awareness, data privacy challenges, and insufficient coordination between financial institutions and regulatory bodies further worsen the issue. Existing systems often rely on rule-based or reactive models, which are not sufficient to counter emerging, adaptive fraud techniques.

Therefore, there is a pressing need to conduct a comprehensive survey and analysis of existing fraud detection systems,

preventive strategies, and technological solutions. The goal is to identify gaps in current approaches and propose a more robust, intelligent, and proactive framework — referred to as "Fraud Shield UPI" — to strengthen transaction security and build user trust in digital payment platforms.

IV. PROPOSED METHODOLOGY

The proposed methodology for the **"Fraud Shield UPI"** survey report involves conducting a comprehensive literature review to understand various types of UPI frauds and the existing detection mechanisms currently in use. Secondary data will be collected from reliable sources such as NPCI reports, RBI publications, and cybersecurity research papers to gain insights into the current fraud landscape. A user survey may also be conducted to evaluate awareness levels and identify common fraud experiences among UPI users. The collected information will be analyzed and classified into categories such as phishing, QR code scams, app cloning, and unauthorized access to determine major trends and vulnerabilities. Existing fraud detection methods, including rule-based systems and AI-based approaches, will be critically evaluated to identify their limitations. Based on this analysis, a new conceptual framework titled **"Fraud Shield UPI"** will be proposed, integrating machine learning, real-time anomaly detection, and user behavior analytics to enhance fraud prevention. The framework will then be validated conceptually against current strategies to assess its expected effectiveness. Finally, recommendations will be made to strengthen transaction security, improve user awareness, and promote safer digital payment practices across the UPI ecosystem.

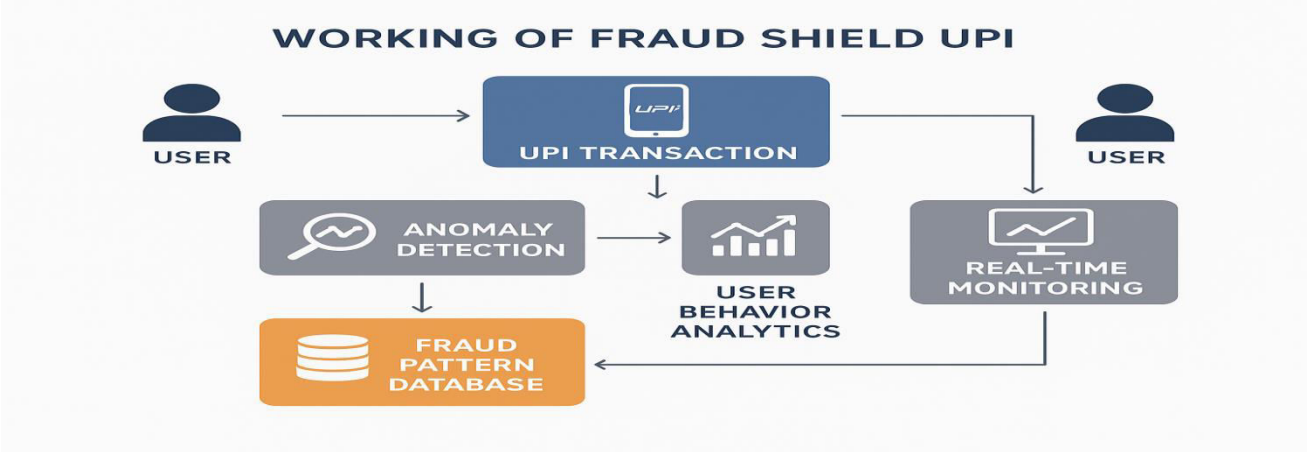


Fig. 1.1 Working of FRAUD SHIELD UPI.

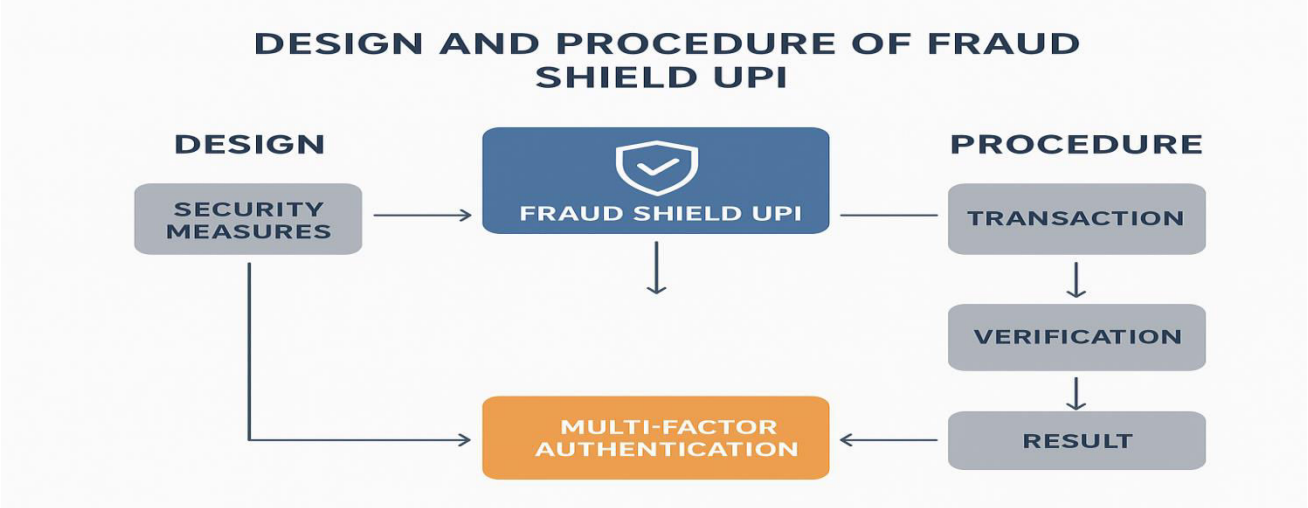


Fig. 1.2 Design and Procedure.

V. PROJECT PURPOSE

The purpose of the **"Fraud Shield UPI"** project is to analyze and address the growing issue of fraudulent activities within India's Unified Payments Interface (UPI) system. With the rapid adoption of digital payments, users are increasingly exposed to threats such as phishing, fake payment links, and unauthorized transactions. This project aims to study these vulnerabilities, evaluate the effectiveness of current fraud detection mechanisms, and identify the gaps that allow such attacks to persist.

Through a detailed survey and data-driven analysis, the project seeks to propose an intelligent and proactive framework—**Fraud Shield UPI**—that can strengthen the security of digital transactions. The purpose is not only to enhance fraud detection and prevention capabilities but also to raise user awareness and promote safer transaction behaviors. Ultimately, this project aspires to contribute toward building a **secure, transparent, and trustworthy UPI ecosystem** that ensures user confidence and supports the continued growth of digital payments in India.

VI. FUTURE ENHANCEMENT

The **"Fraud Shield UPI"** framework can be further enhanced by integrating advanced technologies and continuous learning mechanisms to strengthen fraud detection and prevention. In the future, artificial intelligence and deep learning algorithms can be employed to analyze real-time transaction patterns and detect suspicious behavior with higher accuracy. The system can also be enhanced by incorporating **blockchain technology** for secure transaction validation and data integrity.

Additionally, the development of a **centralized fraud monitoring dashboard** for banks and regulatory authorities can improve coordination and faster response to fraudulent incidents. Implementing **biometric authentication** and **voice recognition** can provide an extra layer of security for UPI users. Future versions of the system may also include **user awareness modules**, sending real-time alerts and educational notifications to prevent social engineering scams.

Continuous updates based on new fraud trends, regular data analysis, and collaboration between financial institutions, fintech companies, and cybersecurity experts will ensure that the **Fraud Shield UPI** system remains adaptive, intelligent, and effective in combating evolving digital payment threats. Ultimately, these enhancements will help in creating a **secure, reliable, and fraud-resilient UPI ecosystem** for all users.

VII. CONCLUSION

The "Fraud Shield UPI" survey highlights the growing importance of securing digital payment systems in the face of rising UPI-related frauds. While UPI has revolutionized financial transactions in India by offering speed, simplicity, and accessibility, it has also become a target for cybercriminals exploiting user unawareness and system vulnerabilities. Through this study, various types of UPI frauds—such as phishing, app cloning, and unauthorized access—have been analysed along with the strengths and limitations of existing detection and prevention mechanisms.

The findings emphasize the need for a more robust, intelligent, and proactive approach to combat these evolving threats. The proposed Fraud Shield UPI framework aims to integrate advanced technologies like machine learning, anomaly detection, and user behaviour analytics to enhance security and reduce fraud risks. Furthermore, promoting user education and awareness remains a crucial aspect of ensuring safe digital payment practices.

In conclusion, Fraud Shield UPI envisions a secure and trustworthy payment environment that combines technology, regulation, and awareness to protect users and sustain confidence in India's growing digital economy. Continued research and collaboration among banks, regulatory authorities, and cybersecurity experts will be essential to achieve this goal and maintain the integrity of the UPI ecosystem.

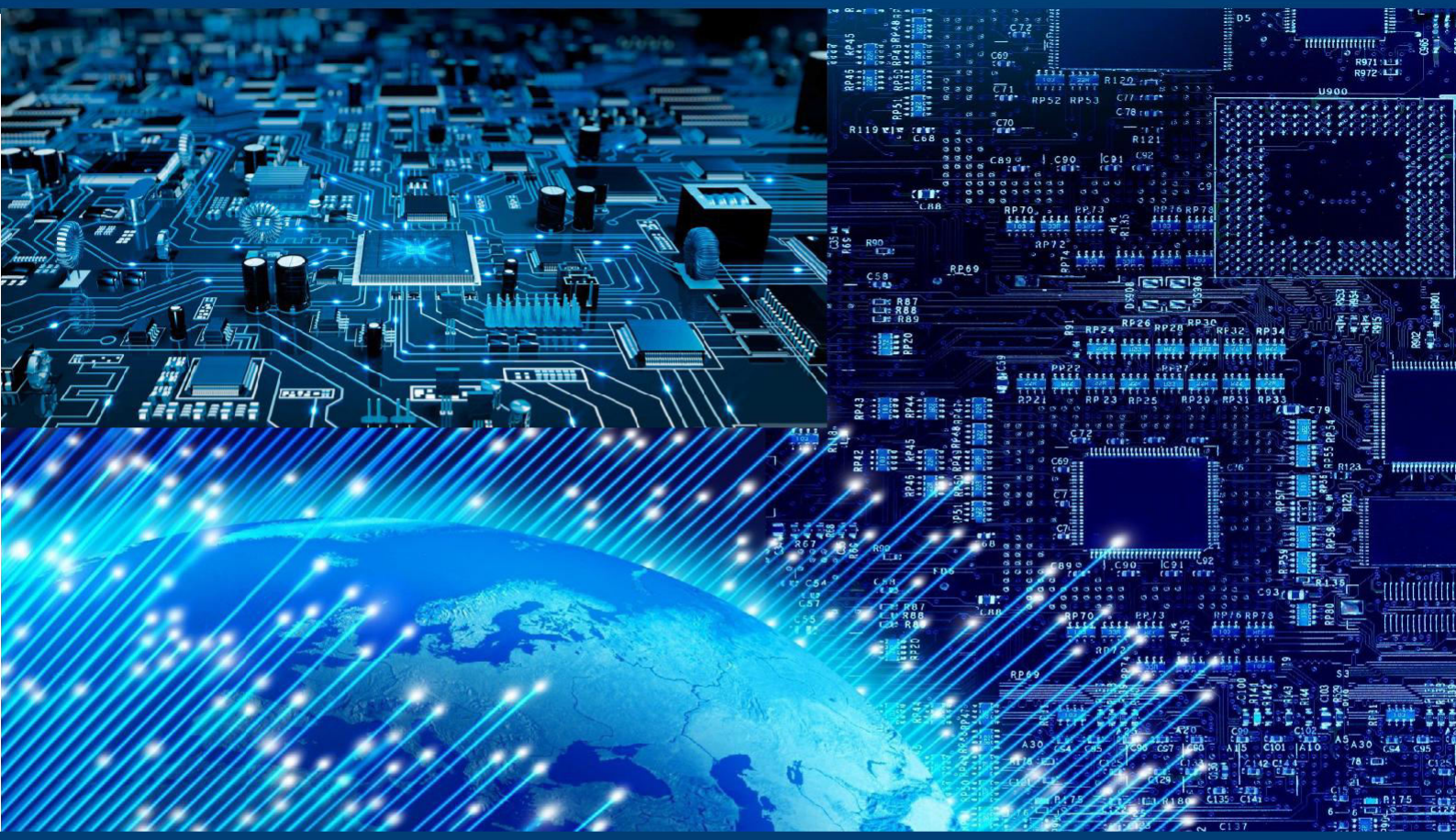
ACKNOWLEDGMENT

I am deeply grateful to all those who have contributed to the successful completion of this survey report titled "Fraud Shield UPI." I would like to express my sincere thanks to my guide Prof. Sujata Jogdand-Gaikwad for their valuable guidance, encouragement, and continuous support throughout this study. Their insightful suggestions and feedback have played a crucial role in shaping the direction and quality of this report. I would also like to extend my gratitude to the Department of Computer Engineering, Alard College of Engineering and Management for providing the necessary facilities and resources to carry out this work. Special thanks to my classmates, friends, and all the respondents who participated in the survey and shared their valuable insights on UPI usage and fraud experiences.

Finally, I would like to thank my family for their constant motivation, understanding, and moral support during the preparation of this report. Their encouragement has been instrumental in the successful completion of this project.

REFERENCES

1. National Payments Corporation of India (NPCI). *Unified Payments Interface (UPI) – Procedural Guidelines and Risk Management Framework.* Available at: https://www.npci.org.in
2. Reserve Bank of India (RBI). *Annual Report on Banking Ombudsman and Financial Fraud Cases (2023–2024).* Available at: https://www.rbi.org.in
3. Ministry of Finance, Government of India. *Digital Payment Security Guidelines.* Department of Financial Services, 2023.
4. PwC India. *Payments Fraud in India: Trends and Mitigation Strategies.* PwC Report, 2022.
5. CERT-In. *Cyber Security Threats and Incident Trends in India – Annual Report 2023.* Indian Computer Emergency Response Team, MeitY.
6. Singh, R., & Sharma, P. (2023). *Machine Learning Approaches for Detecting UPI Transaction Frauds.* International Journal of Computer Science and Information Security, 21(4), 55–62.
7. National Crime Records Bureau (NCRB). *Cyber Crime in India – Statistical Report 2023.* Ministry of Home Affairs, Government of India.
8. Kaur, M., & Verma, S. (2022). *Analysis of Phishing and Social Engineering Attacks in Digital Payment Systems.* Journal of Information Security and Privacy, 15(2), 102–110.
9. Economic Times. (2024). *UPI Fraud Cases Rise Despite Security Enhancements, Says RBI Report.* Available at: https://economictimes.indiatimes.com
10. Deloitte India. *Securing the Digital Payment Ecosystem: Emerging Threats and Best Practices.* Deloitte Insights, 2023.



International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |