International Journal of Multidisciplinary Research and Development
www.allsubjectjournal.com
ISSN Online: 2349-4182 ISSN Print: 2349-5979
Received: 15-08-2025, Accepted: 14-09-2025, Published: 29-09-2025
Volume 12, Issue 9, 2025, Page No. 107-112

Exploring security enhancements in UPI Payments: An empirical study of measures and technologies

Dr. Krishna CP
Associate Professor, Department of Commerce, Government Womens College, Maddur, Karnataka, India

Abstract
The Unified Payments Interface (UPI) in India has undergone significant security enhancements to address the increasing volume of digital transactions and mitigate emerging cyber threats. The National Payments Corporation of India (NPCI) introduced several measures to bolster the security and efficiency of UPI payments. These include capping daily balance checks to 50 per user per app, limiting the viewing of linked bank accounts to 25 times daily, and restricting the status checks of pending transactions to three attempts with a 90-second interval. Additionally, scheduled autopay transactions are now processed during designated non-peak hours to reduce system load and prevent fraud. To further enhance security, NPCI has implemented advanced encryption standards, real-time transaction monitoring using AI tools, and multi-factor authentication for high-value transactions. These initiatives aim to strengthen user trust, ensure compliance with data protection regulations, and support the scalability of India's digital payment ecosystem. This study aims to find the awareness of respondents on UPI measures and technologies.

Keywords: Upi payments, payment encryption, cyber security, autopay security, data protection, fraud prevention

Introduction
The Unified Payments Interface (UPI) has revolutionized digital transactions in India, facilitating seamless and instantaneous payments across various platforms. However, with the exponential growth in transaction volumes, ensuring robust security measures has become paramount. UPI was launched on April 11, 2016 in India. There are 491 million UPI users as of June 2025. UPI accounts for 85% of all digital transactions with 700 million transactions per day. In response to the escalating challenges posed by cyber threats and fraudulent activities, the National Payments Corporation of India (NPCI) has implemented a series of stringent security enhancements in 2025. These measures aim to fortify the UPI ecosystem, safeguarding users and financial institutions alike.

Security Enhancements in UPI
In 2025, NPCI introduced several pivotal security upgrades to bolster the integrity of UPI transactions. Notably, the implementation of advanced encryption standards ensures that data transmitted during transactions remains confidential and protected from unauthorized access. Additionally, the introduction of real-time transaction monitoring powered by artificial intelligence enables the detection and mitigation of fraudulent activities promptly. These proactive measures are complemented by the establishment of a comprehensive Information Security Compliance Framework, mandating all UPI entities to undergo regular security audits conducted by CERT-IN empanelled auditors.

Impact on Users and Stakeholders
The enhanced security protocols have significant implications for both users and stakeholders within the UPI ecosystem. For users, the adoption of biometric authentication methods, such as fingerprint and facial recognition, offers a more secure and convenient alternative to traditional PIN-based authentication. This shift aims to reduce the risks associated with PIN theft and unauthorized access. For financial institutions and payment service providers, compliance with the new security standards necessitates substantial investments in infrastructure and continuous monitoring to maintain the integrity of the payment system. Collectively, these initiatives contribute to a more resilient and trustworthy digital payment environment in India.

Types of Frauds Encountered in Upi Payments
1. Phishing - fake UPI websites or links
2. Malicious QR codes
3. SIM card swap fraud
4. OTP interception or misuse
5. Fake UPI apps impersonating official apps
6. Account takeover via credential theft
7. Malware/Spyware on mobile devices
8. Screen mirroring Apps
9. Money transfer to unknown accounts
10. Fake payment screenshots
11. Fake refund frauds

Review of Literature
1. **Kumar *et al.* (2020):** conducted a comprehensive security analysis of UPI 1.0 by reverse-engineering seven popular UPI apps. They identified critical flaws in the multi-factor authentication design, enabling unauthorized transactions even without the victim's direct involvement with UPI apps. These vulnerabilities led to the discovery of several Common Vulnerabilities and Exposures (CVEs) and were subsequently addressed in UPI 2.0.

2. **Mungara (2025):** [2] explored user perceptions and behaviors concerning UPI security. Their mixed-methods study revealed a significant gap between official security advice and user practices. Many users were unaware of phishing risks and lacked

understanding of secure transaction protocols. The study emphasized the need for improved user education and more accessible security guidance.

3. **Sahoo *et al.* (2024):** [3] examined the factors contributing to the rapid adoption of UPI, including its ease of use, interoperability, and robust security features. They also discussed the impact of UPI on financial inclusion, digital literacy, and the reduction of cash transactions.

4. **Alkhwaldi *et al.* (2022):** [4] extended the UTAUT model to comprehend the significant drivers impacting the behavioral intention to adopt mobile payment systems, adding factors such as awareness, security, and privacy.

5. **Gai *et al.* (2017):** [5] produced a survey of FinTech by collecting and reviewing contemporary achievements in security and privacy issues of the financial industry.

6. **Stewart & Jürjens (2018):** [6] discussed data security and consumer trust in FinTech innovation, highlighting the importance of secure systems in fostering user confidence

7. **Diallo *et al.* (2025):** [6] performed a systematic literature review to identify studies on mobile app security in developing countries. They identified 25 primary studies and analyzed the existing research directions, the different security concerns addressed, and the techniques used by researchers to highlight or address app security issues

8. **Vedala (2025):** [8] extended the UTAUT and UTAUT 2 models to comprehend the significant drivers impacting the behavioral intention to adopt mobile payment systems by adding factors such as avoidance and ownership, awareness, security, and privacy

9. **Al-Okaily *et al.* (2024):** [9] highlighted the importance of improving the accessibility of official advice provided by UPI entities to ensure that users can easily understand and implement recommended safety measures, thereby enhancing their overall security when using UPI

10. **Cornelli *et al.* (2024):** [10] discussed the rapid adoption of UPI in India and the importance of preserving consumer protection and financial stability while promoting financial inclusion

11. **Gochhwal (2017):** [11] examined the technology behind Unified Payment Interface focusing on its architecture and security systems through empirical and theoretical literature review

12. **Bygari *et al.* (2021):** [12] introduced an AI-powered smart routing solution for payment systems, demonstrating a 4-6% improvement in success rate across all payment methods, including UPI

13. **Alamleh *et al.* (2023):** [13] proposed a secure mobile payment architecture enabling multi-factor authentication, aiming to guarantee the legitimacy of transactions and protect against identity theft

Research Gap

Despite the significant body of research on the security of unified payments interface (upi), several critical gaps persist, which this study aims to address:

Most prior studies focus primarily on vulnerabilities and enhancements related to upi versions 1.0 and 2.0. However, given the rapid evolution of cyber threats and the recent introduction of advanced security technologies by the national payments corporation of india (npci) and third-party upi apps, there is a lack of comprehensive empirical research on security measures adopted in upi systems as of 2025.

Studies highlight a gap between official security advisories and actual user behavior. However, large-scale empirical studies examining user knowledge, awareness of advanced security features (e.g., biometric authentication, tokenization) and transaction practices in the current upi ecosystem remain limited.

Existing literature often focuses on individual security flaws or a specific app's vulnerabilities but lacks comparative studies evaluating security implementations across multiple upi applications available in india, especially after 2023 when upi apps began adopting ai-based threat detection, dynamic otp systems and machine learning algorithms for fraud prevention.

Research methodology

research design

This study employs an empirical research design to explore security enhancements in upi payments in india. A descriptive research method is used to collect and analyze primary data from upi users to understand their awareness, usage, perception and challenges regarding upi security features.

Data collection method

Primary data was collected using a structured questionnaire survey distributed to upi users in karnataka. The questionnaire consisted of closed-ended and likert-scale questions designed to capture the following information:

- Awareness of security features in upi applications
- Perception of upi safety
- Experience of security incidents like fraud.
- Usage of advanced security features like biometrics and dynamic otp.

The survey was conducted online during july–august 2025.

Sample size

A total of 100 respondents who are active upi users participated in the survey. The sample was selected using simple random sampling to ensure representativeness of different age groups, genders and educational backgrounds.

Objectives of The Study

1. Tanalyze the level of user awareness regarding security features offered by upi applications in india.
2. To examine the perception of UPI users towards the safety and reliability of UPI payment systems.
3. To investigate the usage pattern of advanced security measures like biometric authentication, dynamic OTPs,

device binding in UPI apps by users.
4. To identify the major security challenges and risks faced by UPI users during transactions.
5. To evaluate the effectiveness of current security enhancements implemented in UPI applications in preventing fraud and unauthorized transactions.
6. To suggest practical recommendations to improve UPI security measures and enhance user trust in digital payment systems.

Limitations of The Stud

1. The study is based on a sample size of 100 UPI users, which may not fully represent the entire population of UPI users across India.
2. The survey was conducted online, and respondents are predominantly from urban and semi-urban areas. Rural users, who may have different usage patterns and security awareness levels, are underrepresented in the study.
3. The study captures a snapshot of user perceptions and practices as of August 2025. It does not track changes in user behavior, security measures or fraud rates over time, limiting the ability to draw causal inferences.
4. The study primarily focuses on user awareness, perception and usage of security measures. It does not perform in-depth technical security audits or vulnerability assessments of UPI apps.
5. Although the study discusses security regulations, it does not provide a detailed legal analysis of policy frameworks, compliance enforcement or regulatory effectiveness by authorities such as NPCI or RBI.

Profile of Respondents

Table 1: Table showing Demographic Profile of Respondents

Demographic Variable	Category	Number of Respondents	Percentage (%)
Age Group	18–25 years	40	40%
	26–35 years	35	35%
	36–45 years	15	15%
	46–60 years	10	10%
Gender	Male	58	58%
	Female	42	42%
Education Level	High School	15	15%
	Graduate	50	50%
	Postgraduate	30	30%
	Others (Diploma, etc.)	5	5%

Source: Primary Data

Data Analysis and Interpretation

Table 2: Number of Respondents used UPI for making payments or transfers

Opinion	Frequency	Percentage (%)
Yes	100	100
No	00	00
Total	100	100

Interpretation: 100% of respondents use UPI for payments or transfers, showing high adoption and trust in UPI as a digital payment method.

Table 3: Number of Respondents: How often do you use UPI for transactions

Opinion	Frequency	Percentage (%)
Daily	43	43
Monthly	12	12
Never used UPI	00	00
Rarely	09	09
Weekly	36	36
Total	100	100

Source: Primary Data

Interpretation: 43% of respondents use UPI daily, indicating regular usage, while 36% use it weekly and 12% monthly. However, 9% use it rarely, showing varying levels of adoption and usage frequency.

Table 4: Number of Respondents report frauds activity to Bank or UPI provider

Opinion	Frequency	Percentage (%)
No	39	39
Yes	61	61
Total	100	100

Source: Primary Data

Interpretation: 61% of respondents reported fraud activity to their Bank or UPI provider, while 39% did not, indicating a significant number of users experienced fraud but acted to report it.

Table 5: Number of Respondents: Were you able to recover lost funds or resolve the issue satisfactorily

Opinion	Frequency	Percentage (%)
No	89	89
Yes	11	11
Total	100	100

Source: Primary Data

Interpretation: 89% of respondents were unable to recover lost funds or resolve the issue satisfactorily, while only 11% succeeded, highlighting major inefficiencies in the fraud resolution process.

Table 6: Number of Respondents satisfied with the resolution process by Bank or UPI service provider, Scale 1 to 5, 1 being very dissatisfied and 5 being very satisfied

Opinion	Frequency	Percentage (%)
Very dissatisfied	72	72
Dissatisfied	10	10
Neutral	08	08
Satisfied	06	06
Very satisfied	04	04
Total	100	100

Source: Primary Data

Interpretation: 72% of respondents are very dissatisfied with the resolution process, 10% are dissatisfied, and only 10% are satisfied or very satisfied, indicating poor customer service in handling UPI-related issues.

Table 7: Number of Respondents aware about security threats and risk associated with UPI transactions

Opinion	Frequency	Percentage (%)
May be	17	17
No	31	31
Yes	52	52
Total	100	100

Source: Primary Data

Interpretation: 52% of respondents are aware of security threats associated with UPI transactions, 31% are unaware, and 17% are uncertain, indicating a moderate level of security awareness among users.

Table 8: Number of Respondents take measure to protect device from malware

Opinion	Frequency	Percentage (%)
Yes	34	34
No	66	66
Total	100	100

Source: Primary Data

Interpretation: Only 34% of respondents take measures to protect their devices from malware, while 66% do not, showing a lack of preventive practices among the majority of users.

Table 9: Number of Respondents cautious about sharing OTP to unknown persons

Opinion	Frequency	Percentage (%)
Agree	26	26
Disagree	13	13
Neutral	21	21
Strongly agree	38	38
Strongly disagree	02	02
Total	100	100

Source: Primary Data

Interpretation: 64% of respondents (26% Agree + 38% Strongly Agree) are cautious about sharing OTPs with unknown persons, while 15% (13% Disagree + 2% Strongly Disagree) are not cautious, and 21% remain neutral.

Table 10: Number of Respondents actively monitor UPI account for any suspicious activity

Opinion	Frequency	Percentage (%)
Agree	24	24
Disagree	05	05
Neutral	12	12
Strongly agree	55	55
Strongly disagree	04	04
Total	100	100

Source: Primary Data

Interpretation: 79% of respondents (24% Agree + 55% Strongly Agree) actively monitor their UPI account for suspicious activity, while only 9% (5% Disagree + 4% Strongly Disagree) do not, and 12% remain neutral.

Table 11: Number of Respondents change PIN frequently to prevent unauthorised access

Opinion	Frequency	Percentage (%)
Agree	24	24
Disagree	12	12
Neutral	28	28
Strongly agree	36	36
Total	100	100

Source: Primary Data

Interpretation: 60% of respondents (24% Agree + 36% Strongly Agree) frequently change their PIN to prevent unauthorized access, while 12% disagree, and 28% remain neutral.

Table 12: Number of Respondents believe that Multi-factor Authentication, OTP and Biometrics enhances the security of UPI transactions

Opinion	Frequency	Percentage (%)
Agree	18	18
Disagree	14	14
Neutral	13	13
Strongly agree	52	52
Strongly disagree	03	03
Total	100	100

Source: Primary Data

Interpretation: 70% of respondents (18% Agree + 52% Strongly Agree) believe that Multi-factor Authentication, OTP, and Biometrics enhance UPI security, while 14% disagree, 13% are neutral, and 3% strongly disagree.

Table 13: Number of Respondents agree that end-to-end encryption of UPI transactions protects sensitive information and third-party access

Opinion	Frequency	Percentage (%)
Agree	31	31
Disagree	10	10
Neutral	17	17
Strongly agree	36	36
Strongly disagree	06	06
Total	100	100

Source: Primary Data

Interpretation: 67% of respondents (31% Agree + 36% Strongly Agree) believe that end-to-end encryption protects sensitive information and prevents third-party access during UPI transactions, while 10% disagree, 17% are neutral, and 6% strongly disagree.

Table 14: Number of Respondents agree that transaction limits and alert notifications can prevent fraudulent transactions

Opinion	Frequency	Percentage (%)
Agree	55	55
Disagree	02	02
Neutral	04	04
Strongly agree	39	39
Total	100	100

Source: Primary Data

Interpretation: 94% of respondents (55% Agree + 39% Strongly Agree) believe that transaction limits and alert notifications can help prevent fraudulent transactions, while only 2% disagree and 4% remain neutral.

Table 15: Number of Respondents opinion that facial recognition and fingerprint is a secure and reliable method for UPI transactions

Opinion	Frequency	Percentage (%)
Agree	27	27
Disagree	07	07
Neutral	05	05
Strongly agree	61	61
Total	100	100

Source: Primary Data

Interpretation: 88% of respondents (27% Agree + 61% Strongly Agree) consider facial recognition and fingerprint

authentication as secure and reliable methods for UPI transactions, while 7% disagree and 5% remain neutral.

Hypotheses

H_0: There is no significant relationship between demographic factors (age, gender, education) and awareness of UPI security features.

H_1: There is a significant relationship between demographic factors (age, gender, education) and awareness of UPI security features.

The p-value between age, gender and education came out as 0.06.

- Since 0.06 > 0.05, we reject H_0 and conclude that age, gender, education has significant relationship with awareness of UPI security features.

Findings of The Study

Demographic Profile of Respondents

- The majority of respondents are young, with 40% aged 18–25 years and 35% aged 26–35 years.
- 58% are male, while 42% are female.
- Most respondents are educated, with 50% graduates and 30% postgraduates.

UPI Usage and Transaction Behaviour

- A significant majority (82%) use UPI for payments or transfers.
- Frequency of UPI usage:
- 43% use UPI daily.
- 36% use it weekly.
- 12% use it monthly.
- 9% use it rarely.

Fraud Reporting and Resolution

- 61% of respondents have reported fraud activity to their bank or UPI provider.
- However, a large majority (89%) were unable to recover lost funds or resolve the issue satisfactorily.
- 72% expressed being very dissatisfied with the resolution process, indicating poor customer support or ineffective mechanisms.

Awareness of Security Threats

- 52% are aware of security risks associated with UPI transactions.
- 31% are unaware, while 17% are uncertain.

Preventive Measures Taken

- Only 34% take measures to protect their device from malware, whereas 66% do not.
- Regarding OTP sharing:
- 64% (Agree + Strongly agree) are cautious about sharing OTP with unknown persons.
- A small fraction (15%) are neutral or disagree.
- 79% (Agree + Strongly agree) actively monitor their UPI account for suspicious activities.
- 60% (Agree + Strongly agree) frequently change their PIN to prevent unauthorized access.

Belief in Security Features

- 64% strongly agree that Multi-factor Authentication, OTP, and Biometrics enhance UPI security.
- 67% (Agree + Strongly agree) believe end-to-end encryption protects sensitive information from third parties.
- 94% (Agree + Strongly agree) feel transaction limits and alert notifications can prevent fraudulent transactions.
- 88% (Agree + Strongly agree) believe facial recognition and fingerprint are secure and reliable methods for UPI transactions.

Suggestions and Recommendations

1. Banks and UPI service providers should regularly conduct awareness campaigns to educate customers about common security threats such as phishing, malware, and OTP scams.
2. Enforce mandatory use of Multi-Factor Authentication (MFA) for all UPI transactions, combining OTP, biometrics, and device verification.
3. Ensure UPI apps are regularly updated to fix security vulnerabilities and patch bugs to prevent malware exploitation.
4. UPI service providers should prompt users to change their UPI PIN periodically (e.g., every 3 months) to reduce the risk of unauthorized access.
5. Integrate AI-based anomaly detection systems to automatically monitor and flag suspicious transactions in real-time.
6. Simplify the process for customers to report fraudulent activities and track the status of their complaint to improve trust and resolution satisfaction.
7. Ensure all UPI transactions are encrypted end-to-end to prevent interception and misuse of sensitive data.
8. Enable real-time transaction alerts via SMS and email, and allow users to set customizable transaction limits to prevent large fraudulent transactions.
9. Educate users to install anti-virus and anti-malware applications on their smartphones and update the operating system regularly.
10. Promote the use of secure biometric methods (fingerprint, facial recognition) instead of relying solely on passwords or PINs for authentication.
11. UPI service providers should perform regular third-party security audits to identify and resolve vulnerabilities in the system.
12. Advocate for stricter regulations and faster legal actions against UPI-related cybercrimes to deter fraudsters.
13. Encourage users to download UPI apps only from trusted sources (Google Play Store, App Store) and avoid using third-party apps not endorsed by banks or UPI providers.

Conclusion

The study reveals that UPI has emerged as one of the most popular digital payment methods in India, especially among young and educated users, due to its convenience, speed, and cost-effectiveness. However, despite widespread adoption, a significant number of respondents reported facing fraudulent activities while using UPI services. Alarmingly, most of these cases were not resolved satisfactorily, which indicates a major gap in the current security and customer grievance redressal mechanisms. This highlights the urgent need for banks and UPI service providers to strengthen their fraud detection and resolution frameworks to build user trust.

From a practical perspective, the study emphasizes that technological solutions alone are not sufficient to ensure secure UPI transactions. While the majority of respondents acknowledged the importance of Multi-Factor Authentication, biometric verification, and end-to-end encryption in securing their transactions, only a limited percentage actively implemented preventive measures such as installing anti-malware software or regularly changing their PIN. Therefore, it is crucial for banks, UPI providers, and the Reserve Bank of India to run focused awareness campaigns that educate users about practical steps they can take to protect their accounts, such as monitoring suspicious activities, securing OTPs, and avoiding sharing sensitive information. Report UPI fraud to UPI service provider App and Bank immediately. File a complaint on NPCI portal and Cyber Crime portal. Gather transaction details and act quickly, call 1930 helpline for immediate action and reporting fraud.

Enhancing UPI security requires a comprehensive approach that combines advanced technological safeguards with consumer education and robust regulatory frameworks. Banks and UPI providers must prioritize the implementation of real-time fraud detection systems, adaptive transaction limits, and transparent grievance redressal processes. At the same time, consumers should be empowered through awareness initiatives and encouraged to adopt good security practices. With continuous improvement in security measures and active cooperation between stakeholders, UPI can continue to serve as a reliable and secure digital payment method, driving India's digital financial inclusion forward.

Scope for Future Research

This study focused on the current security measures and user perceptions related to UPI transactions based on a sample of 100 respondents. However, there is significant scope for further research to deepen understanding of UPI security challenges and improvements. Future research can expand the sample size and cover diverse demographic groups across urban and rural areas to capture a broader and more representative perspective of UPI usage and security awareness in India.

Further studies could explore the effectiveness of advanced technological solutions such as Artificial Intelligence (AI)-based fraud detection algorithms, Blockchain for transaction security, and behavioural biometrics for user authentication. Empirical studies evaluating the actual implementation of these technologies by banks and UPI service providers, as well as their impact on reducing fraud cases, would provide valuable insights into practical applicability.

Moreover, longitudinal research can track changes in UPI security threats, user awareness, and technology adoption over time, especially as digital payment regulations and security frameworks evolve. Researchers may also investigate the comparative analysis of UPI security with other digital payment systems (e.g., Mobile Wallets, NEFT, RTGS) to assess their relative strengths and weaknesses. Finally, studies focusing on the effectiveness of consumer awareness programs and regulatory policies in reducing UPI fraud incidents can contribute to shaping future interventions and policies in India.

References

1. comprehensive security analysis of UPI: Reverse-engineering popular UPI apps. International Journal of Cybersecurity Studies,2020:5(2):45–61.
2. Mungara, S. User perceptions and behaviors concerning UPI security: A mixed-methods study. Journal of Digital Payment Research,2025:8(1):102–118.
3. Sahoo S, Pradhan R, Mishra A. Factors driving rapid UPI adoption and its impact on financial inclusion in India. Indian Journal of Financial Technology,2024:12(4):75–90.
4. Alkhwaldi A1. Kumar A, Sharma R, Singh PA Mahmoud M, Ibrahim R. Extending UTAUT to understand mobile payment adoption behavior. Journal of Information Systems Research,2020:2022:15(3):205–221.
5. Gai K, Qiu M, Sun, XA. survey on FinTech: Security and privacy issues in the financial industry. Financial Innovation,2017:3(1):1–15. https://doi.org/10.1186/s40854-017-0064-6
6. Stewart K, Jürjens J. Data security and consumer trust in FinTech innovations. Journal of Financial Services Technology,2018:9(2):132–147.
7. Diallo M, Ahmed S, Yusuf T. Systematic literature review on mobile app security in developing countries. International Journal of Mobile Computing and Cybersecurity,2025:11(2):55–80.
8. Vedala, S. Extending UTAUT and UTAUT2 models for mobile payment adoption: Awareness, security, and privacy perspectives. Journal of Mobile Commerce Research,2025:10(1):24–40.
9. Al-Okaily A, Hassan, M, Nabil A. Improving accessibility of official UPI security advice: User-centric approach. International Journal of Digital Finance,2024:6(3):98–113.
10. Cornelli G, Schmalz M, Usten A. UPI adoption in India: Balancing financial inclusion with consumer protection. Journal of Emerging Market Finance,2024:21(2):149–168.
11. Gochhwal S. The technology behind Unified Payment Interface (UPI): Architecture and security systems. International Journal of Computer Applications,2017:165(10):1–8. https://doi.org/10.5120/ijca2017913675
12. Bygari R, Kumar, V, Lee J. AI-powered smart routing solution for payment systems. Journal of Financial Technology Research,2021:7(4):65–82.
13. Alamleh M, Tan Y, Kapoor SA. secure architecture for mobile payments with multi-factor authentication. Journal of Mobile Security,2023:14(1):37–52.