Examining User Awareness and Addressing Security Challenges in the UPI Framework: A Comprehensive Analysis Framework

Authors: Kishan Kumar, Krishna, Tanmay Tiwary, Akashdeep Sharma, Kartik Kumar
Affiliation: University School of Business, Chandigarh University, Punjab, India

Abstract

The Unified Payments Interface (UPI), launched in 2016 by the National Payments Corporation of India (NPCI), has rapidly revolutionized digital transactions in India. Its widespread adoption, however, has outpaced user awareness and exposed various security vulnerabilities. This study explores the landscape of user awareness regarding UPI security, identifies the types of cyber threats faced, and evaluates the existing security infrastructure and user behavior. Through survey analysis and literature review, it reveals that although users appreciate the platform's convenience, a significant portion lacks understanding of critical security features such as two-factor authentication, fraud reporting mechanisms, and secure transaction practices. The study proposes strategic recommendations for stakeholders—including banks, fintech firms, and regulators—to enhance user literacy and fortify the UPI ecosystem through technological upgrades like biometric authentication, AI-powered fraud detection, and multilingual awareness campaigns. The findings contribute to a more secure and inclusive digital financial system in India.

Keywords: UPI, user awareness, digital payments, cybersecurity, NPCI, financial inclusion

1. Introduction

The digital revolution in India has transformed the nation's financial landscape, with the Unified Payments Interface (UPI) emerging as a cornerstone. UPI enables real-time, 24x7 transactions through mobile devices, linking multiple bank accounts via a single application. Despite its remarkable convenience and utility, the growth of UPI usage has introduced serious concerns about user security and cyber threats.

UPI was introduced by the NPCI in 2016 to unify disparate banking services and promote cashless transactions. It has significantly contributed to India's "Digital India" initiative and financial inclusion goals. However, the growing sophistication of cybercrimes, including phishing, QR scams, and unauthorized transactions, has raised alarms about user readiness and awareness.

This paper addresses critical issues related to user security, evaluates UPI's technological strengths and weaknesses, and recommends solutions to bridge the gap between functionality and safe usage.

2. Literature Review

Prior studies underscore the dual nature of UPI as both an enabler of financial empowerment and a potential risk factor due to inadequate digital literacy. Researchers such as Sharma & Kumar (2020) highlight that users' low awareness of phishing, fake apps, and weak passwords contributes significantly to UPI-related frauds.

Other works (e.g., Mehta & Patel, 2021) advocate for AI-based fraud detection and education programs to mitigate risks. The growth of smartphone access, favourable government policies, and increased internet penetration have

expanded UPI's reach—but not uniformly improved user awareness. This research builds on these foundations, targeting the intersection of user behaviour, awareness, and digital safety.

3. Methodology

This study adopts a mixed-methods approach involving:

- **Survey Design:** A questionnaire-based survey of 300+ respondents from urban and rural areas in Punjab.

- **Sampling:** Stratified random sampling focused on demographics such as age, occupation, and digital literacy.

- **Data Collection:** Primary data through online forms and in-person interviews.

- **Analysis Tools:** Descriptive statistics, cross-tabulation, and percentage analysis.

The objective was to measure awareness levels, types of threats experienced, and user attitudes toward UPI safety features.

4. Results and Analysis

Key insights from the data include:

- **User Awareness:** Only 33.7% of users consistently verify transaction details; 57.4% are unaware of fraud reporting features.

- **Security Practices:** 42.6% of fraud victims did not pursue resolution, citing lack of knowledge or platform support.

- **Threat Exposure:** Phishing, social engineering, and QR fraud were common, especially among young users.

- **Trust Factors:** Users prefer apps like PhonePe and Google Pay but often ignore security prompts.

Tables and charts presented in the original study further detail the distribution of responses and behaviour patterns.

5. Discussion

The findings suggest that technological infrastructure alone is insufficient. The ease of UPI usage can become a vulnerability in the absence of user education. Many users, particularly in semi-urban and rural settings, demonstrate gaps in identifying secure practices. This exacerbates risks, making them easy targets for scammers.

Furthermore, while apps offer two-factor authentication and fraud notifications, user engagement with these features remains low. There is a disconnect between the tools provided and their effective utilization.

6. Recommendations

To enhance the UPI ecosystem's resilience, the following strategies are suggested:

- **User Education:** Launch multilingual awareness campaigns across TV, social media, and rural outreach programs.

- **Technology Improvements:** Incorporate biometric login and AI-driven fraud detection into all UPI apps.

- **Regulatory Measures:** Streamline and mandate response timelines for fraud reporting and grievance redressal.

- **Offline Support:** Promote UPI Lite for feature phone users and areas with low internet penetration.

7. Conclusion

While UPI has successfully revolutionized financial transactions in India, its continued success hinges on closing the security-awareness gap. Educating users, strengthening digital hygiene, and deploying smarter security tools must be prioritized by all stakeholders.

A secure UPI framework ensures not only transaction safety but also promotes sustained trust and adoption—key to India's digital transformation.

References

- Sharma, R., & Kumar, P. (2020). User Security Awareness in Digital Transactions.

- Mehta, V., & Patel, D. (2021). Cybersecurity Measures in Mobile Payments.

- NPCI Reports and RBI Bulletins (2022–2024)

Appendix

- Glossary of Terms: VPA, UPI, NPCI, BHIM

- Sample Survey Instrument

- Abbreviations List