International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

An Empirical Study on Cybersecurity Risks in UPI-based Digital Payment Systems

Dr. Ranita B. Valave[1], Pramod D. Borhade[2]

Assistant Professor, PIRENS Institute of Business Management & Administration (IBMA), Loni Bk, Tal. Rahata, Dist. Ahilyanagar
Email: *valave.ranita[at]gmail.com*

Assistant Professor, PIRENS Institute of Business Management & Administration (IBMA), Loni Bk, Tal. Rahata, Dist. Ahilyanagar
Email: *pramodborhade5566[at]gmail.com*

Abstract: ***The rapid development of digital payments in India, particularly through the Unified Payments Interface (UPI), has changed the financial landscape by enabling fast, interoperable, and user-friendly transactions. However, the rising volume of digital transactions has concurrently increased cyber threats such as phishing, malware attacks, identity theft, and fraudulent UPI links. This research paper aims to analyse the cybersecurity risks associated with UPI-based payment systems, evaluate user awareness and protecting behaviour, and examine the effectiveness of existing security measures applied by banks and FinTech platforms. Using both primary and secondary data, the study reveals key weaknesses, user behaviour gaps, and systemic challenges affecting cybersecurity in digital payments. The paper concludes with strategic recommendations to strengthen UPI security and enhance user trust in India's digital financial ecosystem.***

Keywords: Unified Payments Interface (UPI), Cybersecurity, FinTech platforms, Digital Financial Ecosystem

1. Introduction

The Unified Payments Interface (UPI), introduced by the National Payments Corporation of India (NPCI) in 2016, has played a major role in the financial sector's revolutionary shift towards digitalization in India. With billions of transactions every month, UPI has grown to become one of the biggest real-time payment networks in the world. Despite its popularity, users are now more vulnerable to a variety of cyberthreats due to their increased reliance on digital devices.

Cybercriminals take advantage of poor authentication procedures, user behaviour, and mobile device vulnerabilities. Phishing calls, fake UPI links, malware apps, SIM swap scams, and social engineering attempts are common cyberthreats. Understanding cybersecurity issues is essential for protecting user funds and fostering trust as UPI transactions increase. This study explores the extent of cybersecurity risks in UPI transactions and assesses users' awareness and behaviour. It also evaluates whether existing security mechanisms are sufficient in preventing digital payment fraud.

2. Review of Literature

Sharma and Dubey (2021), in their research featured in the International Journal of Cybersecurity, noted that phishing attacks, fraudulent mobile apps, OTP scams, and social engineering deceptions were the predominant cybersecurity threats impacting users of digital payments in India. Their results emphasize the necessity of enhancing user awareness and protective actions to decrease fraud occurrences**.**

Gupta and Arora (2020) emphasized in the Journal of Digital Economy that awareness among users is vital for safeguarding mobile-based digital transactions. They noticed that numerous users unintentionally provide excessive app permissions or disclose sensitive data like PINs and OTPs, rendering them susceptible to cyber threats. The research determined that enhancing digital literacy among users greatly lowers the risk of fraud.

Singh and Pandey (2019), in their study featured in the Indian Journal of Finance, noted that although the adoption of UPI has risen because of its user-friendliness, security issues have also escalated concurrently. They discovered that malware attacks, identity impersonation, and unauthorized access are increasing concerns in UPI transactions. Their research highlighted the necessity for more stringent security measures at the app level.

As stated by the National Payments Corporation of India (NPCI, 2022) in its UPI Security and Risk Management Guidelines, UPI is founded on robust security principles including encrypted transactions, device binding, and two-factor authentication. NPCI noted that primary vulnerabilities stem from users, such as disclosing sensitive information and installing unofficial applications, making them susceptible to cyber fraud**.**

CERT-In (2023), in its Cybersecurity Advisory Report, reported a significant rise in digital payment frauds in India, particularly involving UPI phishing links, QR code scams, and remote screen-sharing tools. The advisory highlighted that cybercriminals take advantage of user carelessness instead of system vulnerabilities, underscoring the importance of user training**.**

Sinha (2020), in the International Journal of Management Studies, noted that consumer behavior significantly affects the safety of digital payment transactions. The research revealed a notable disparity between users' confidence in digital payments and the safety measures they actually follow. Numerous users believed that digital payments were secure yet persisted in dangerous practices like saving PINs on their smartphones.

The Reserve Bank of India (RBI, 2021), in its Cybersecurity Framework for Digital Payments, emphasized that payment

service providers need to implement multi-factor authentication, tokenization, enhanced encryption, and AI-driven fraud detection systems. The RBI emphasized the need for consumer awareness initiatives to combat phishing and social-engineering scams.

Kaur and Sandhu (2018), in their piece published in the International Journal of Computer Applications, noted that mobile wallets and payment applications encounter risks from insecure APIs, poor encryption methods, and insufficient user safety measures. Their results emphasized the importance of ongoing security updates and user training to stay ahead of changing cyber threats.

Mishra and Reddy (2022), in the Asian Journal of Finance & Banking, noted that most fraud incidents in real-time payment systems in India arise from social engineering tactics and counterfeit payment request links. Their research revealed that 60% of frauds resulted from impersonation calls, while 40% were linked to fraudulent UPI links, highlighting the increasing sophistication of scammers.

Bansal and Raj (2023), in their research featured in the Journal of FinTech Research, indicated that robust cybersecurity measures- such as biometric verification, device-specific security, and immediate fraud notifications—greatly enhance user confidence in digital payment applications. They highlighted that cybersecurity is closely related to customer contentment and ongoing utilization of FinTech offerings.

3. Research Problem

Although existing research highlights several cybersecurity susceptibilities in digital payment systems, there is a lack of observed, primary-data-driven studies examining UPI users' awareness, experiences with fraud, risk perception, and trust levels in India.

Thus, a complete analytical study based on primary data is needed to understand actual cybersecurity risk exposure among UPI users and evaluate the effectiveness of existing security practices.

4. Objectives of the Study

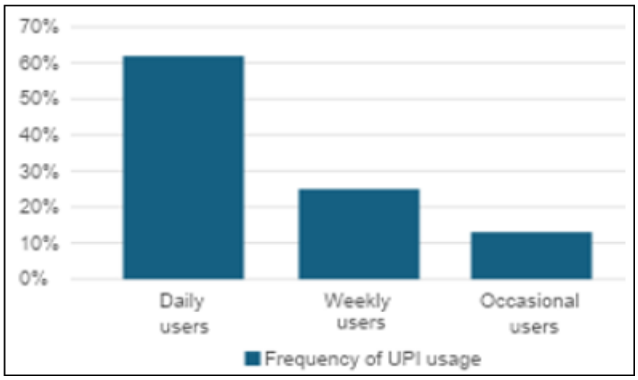
1) To identify key cybersecurity risks in UPI-based digital payment systems.
2) To analyse user consciousness and behaviour related to UPI cybersecurity.
3) To assess the efficiency of security features provided by UPI apps and banks.
4) To offer suggestions for improving cybersecurity in UPI transactions.

5. Research Methodology

The current research utilizes a descriptive design to analyze cybersecurity threats linked to digital payment systems, particularly focusing on India's UPI framework. The research relies on both primary and secondary information. Data was gathered from 100 UPI users using a structured questionnaire aimed at collecting details on demographic profiles, frequency of UPI use, awareness of cyber threats, experiences of fraud, trust in UPI services, and understanding of safety protocols. Secondary data were sourced from trustworthy references including RBI reports, NPCI publications, CERT-In alerts, academic journals, and reputable news articles to bolster the conceptual and analytical basis of the research. A convenience sampling method was utilized to choose participants because it effectively reaches individuals who are easily accessible and actively engaged with digital payment systems. The survey contained multiple-choice, binary, and Likert-scale questions to guarantee structured data gathering on user behavior and awareness of cybersecurity. The gathered data underwent percentage analysis, enhanced by charts and graphs to effectively display trends, patterns, and user perceptions in a clear and understandable way. This methodological approach facilitates a thorough understanding of the cybersecurity issues encountered by UPI users and offers a solid foundation for analysis and policy suggestions

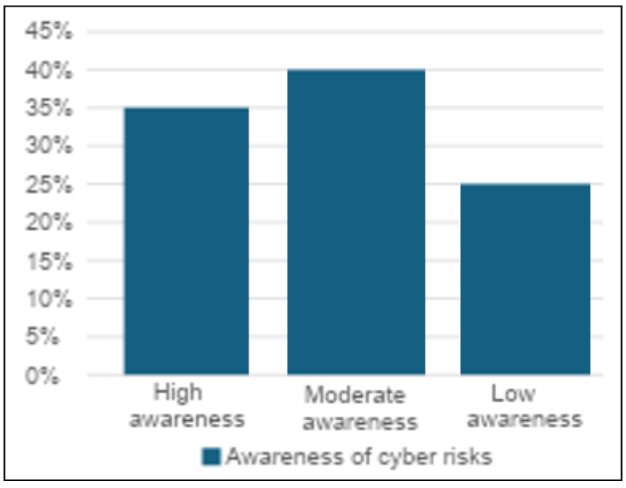
6. Data Analysis & Interpretation (Based on Sample of 100 Respondents)

6.1 Frequency of UPI usage



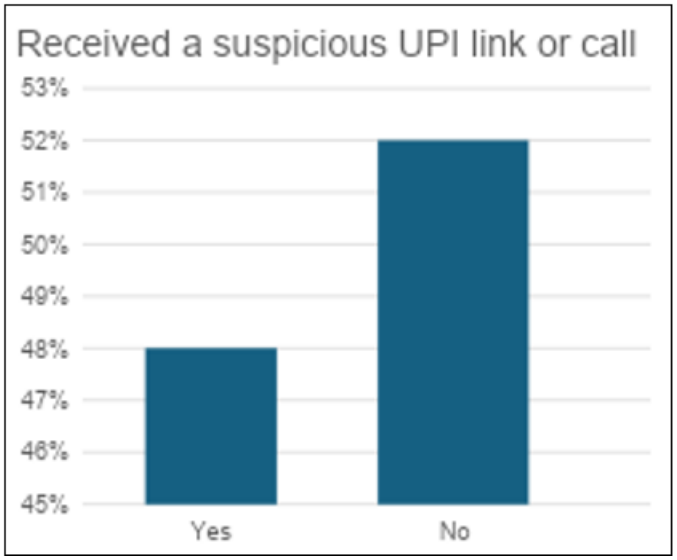
The data shows that 62% of respondents are daily UPI users, indicating high dependence on digital payments. Around 25% use UPI weekly, while only 13% use it occasionally, reflecting that UPI has become a regular and essential mode of transaction for the majority of users. UPI is widely used for daily transactions.

6.2 Awareness of cyber risks



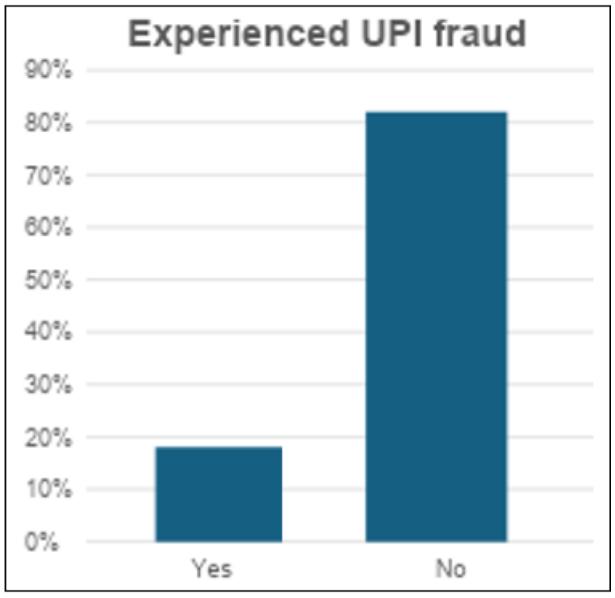
The findings indicate that only 35% of users have high cybersecurity awareness, while the majority (40%) possess moderate awareness, and 25% have low awareness, suggesting a significant need for improved cyber safety education among UPI users. A substantial portion remains unaware of advanced cyber threats.

6.3 Have you ever received a suspicious UPI link or call?



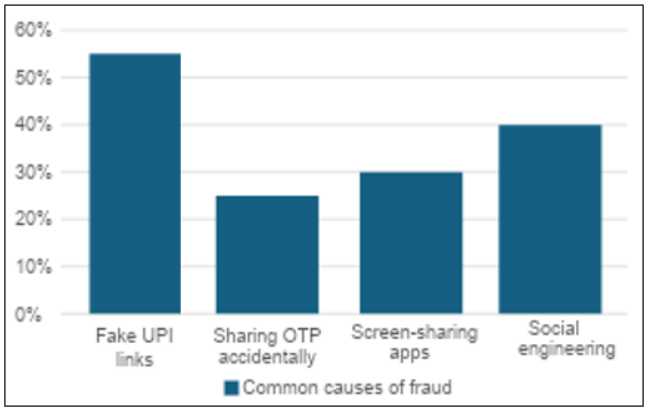
The data shows that 48% of respondents have received suspicious UPI links or calls, while 52% have not, indicating that nearly half of the users are exposed to potential cyber-fraud attempts, highlighting the need for stronger user awareness and security measures. Cybercriminals frequently target users.

6.4 Have you ever experienced UPI fraud?



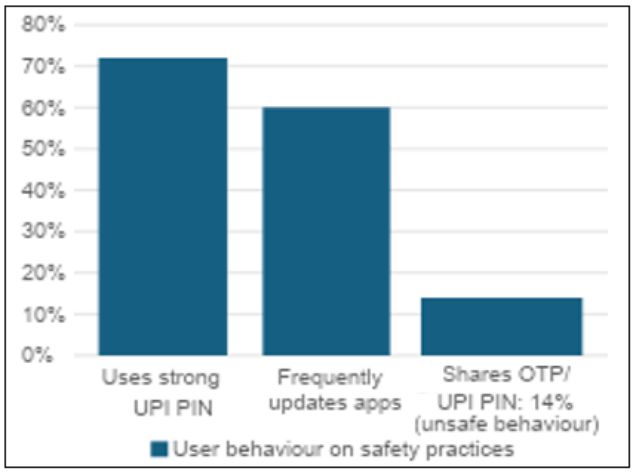
The results indicate that 18% of respondents have experienced UPI fraud, while 82% have not, suggesting that although the majority remain unaffected, a considerable minority still faces real fraud incidents, reflecting existing vulnerabilities in the system.

6.5 Common causes of fraud



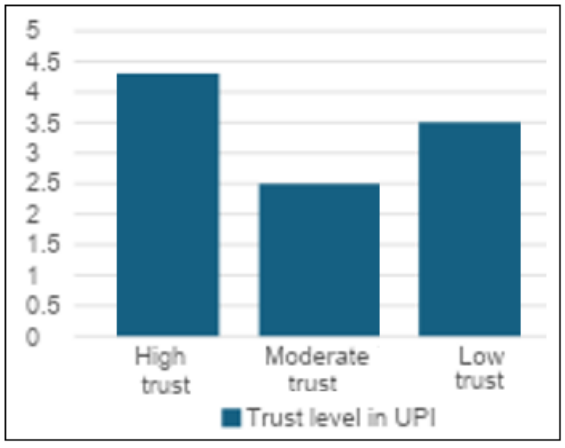
The findings reveal that fake UPI links (55%) are the most common cause of fraud, followed by social engineering (40%), screen-sharing apps (30%), and accidental OTP sharing (25%), indicating that both technical vulnerabilities and user behaviour contribute significantly to cybersecurity risks in UPI transactions.

6.6 User behaviour on safety practices



The data indicates that most users follow basic safety practices, with 72% using strong UPI PINs and 60% regularly updating apps, while 14% still engage in unsafe behaviour by sharing OTPs or UPI PINs, highlighting a gap in secure user practices.

6.7 Trust level in UPI



The data shows that 70% of users have high trust, 25% moderate trust, and 5% low trust in UPI. Despite potential cybersecurity risks, the majority of users continue to rely on and trust the system for digital transactions.

7. Major Findings

1) UPI is used daily by most respondents, indicating strong dependency.
2) Cyber risks such as phishing, fraudulent links, and fake calls are increasing.
3) Nearly half the users have received suspicious UPI-related messages.
4) 18% of users have experienced some form of UPI-related fraud.
5) Poor awareness of security practices contributes to cyber incidents.
6) Social engineering remains the most common fraud method.
7) Users trust UPI, but their security knowledge is insufficient.
8) App-level features such as encryption, biometric lock, and fraud alerts increase trust.
9) There is a gap between system-level security and user-level caution.

8. Suggestions

1) Awareness programs should be conducted at colleges, banks, and workplaces.
2) UPI apps should display mandatory safety tips before transactions.
3) Banks must strengthen AI-based fraud detection systems.
4) Government should increase public cyber safety campaigns.
5) Users must avoid screen-sharing apps and respond only to official communication.
6) Multi-factor authentication should be enhanced further.
7) Telecom service providers should identify and block suspicious numbers.
8) NPCI should introduce real-time fraud reporting and immediate payment reversal mechanisms.

9. Conclusion

The study concludes that while UPI has revolutionized the digital payment ecosystem in India, it also faces growing cybersecurity challenges. The primary vulnerability arises not only from technological loopholes but significantly from user behaviour and lack of awareness. Strengthening cybersecurity mechanisms, improving user education, and implementing robust fraud detection frameworks are essential to ensure the sustainability and trust of UPI. By adopting the recommendations outlined in this study, stakeholders-including users, banks, FinTech firms, and regulators—can collectively enhance the safety and reliability of digital transactions in India.

References

[1] RBI Annual Reports (2021–2024)
[2] NPCI UPI Product Statistics
[3] CERT-In Cyber Safety Advisories
[4] Journals on Cybersecurity and Digital Finance
[5] Research articles from Google Scholar, IEEE, Elsevier
[6] Sharma, P., & Dubey, A. (2021). Cybersecurity Challenges in Digital Payments in India. *International Journal of Cybersecurity*, 9(2), 45–52.
[7] Gupta, R., & Arora, S. (2020). User Awareness and Security Behaviour in Mobile Payment Systems. *Journal of Digital Economy*, 5(1), 22–34.
[8] Singh, V., & Pandey, R. (2019). Adoption of UPI and Associated Security Concerns. *Indian Journal of Finance*, 13(4), 65–72.
[9] National Payments Corporation of India (NPCI). (2022). UPI Security and Risk Management Guidelines. Mumbai: NPCI Publications.
[10] CERT-In. (2023). Advisory on Digital Payment Frauds in India. New Delhi: Indian Computer Emergency Response Team (CERT-In), Government of India.
[11] Sinha, P. (2020). Consumer Behaviour and Cyber Safety Practices in Digital Transactions. *International Journal of Management Studies*, 7(3), 101–115.
[12] Reserve Bank of India (RBI). (2021). Cybersecurity Framework for Digital Payments. Mumbai: RBI Publications.
[13] Kaur, G., & Sandhu, H. (2018). Security Issues in Mobile Wallets and Payment Apps. *International Journal of Computer Applications*, 182(21), 1–6.
[14] Mishra, S., & Reddy, T. (2022). Fraud Patterns in Real-Time Payment Systems: Evidence from India. *Asian Journal of Finance & Banking*, 6(2), 88–99.
[15] Bansal, K., & Raj, A. (2023). Impact of Cybersecurity on Trust in FinTech Applications. *Journal of FinTech Research*, 4(1), 54–68.