

Cybersecurity Challenges in UPI and Digital Payments

Shalini Deepak Maurya¹, Maitri Kamlesh Parmar², Aarti Sanjay Gawai³

^{1,2}Author, Students, Department of Information Technology and Computer Science, D.G Ruparel College, Mumbai, Maharashtra, India

³Co-Author, Assistant Professor, Department of Information Technology and Computer Science, D.G Ruparel College, Mumbai, Maharashtra, India

Abstract - UPI and other digital payment services have revolutionized the way people transfer money; moreover Obtain financial services and pay vendors. Such systems are convenient and fast, too.'

Options for cybercriminals to exploit technical weaknesses and human behaviour, specifically.

This paper.

Examines the significant cybersecurity obstacles that hinder UPI and digital payments, such as phishing and social engineering. Phrases such as engineering, counterfeit transactions or QR codes, malicious software, SIM theft, account hacked and fraud. Takeover and privacy risks. A structured questionnaire and semi-autograph system are utilized to suggest a mixed-method research design.

Structured interviews. For the section on analysis before actual field data are taken, an example can be provided to illustrate its use. The dataset comprises of 100 individuals who provided feedback. This analysis suggests that social-engineering threats are common. Why?

Although they are recognized, payment requests are not consistently verified. Why? The findings suggest that.

The combination of technical controls, user awareness, secure application practices, and other essential elements is crucial for a successful cybersecurity. Effective fraud-reporting mechanisms. Finally, the paper includes some suggestions and future research directions. Deliberate analysis through behavioural analytics and AI-assisted fraud detection.

Key Words: UPI, Digital Payments, Cybersecurity, Phishing, Social Engineering, QR Code, Payment Fraud, User Experience Speculation (defect or corruption), Information Security Awareness.

1. INTRODUCTION

Digital payment systems are now an integral part of modern financial activity. The integration of mobile applications for account-to-account payments has made it possible to use UPI, which simplifies everyday transactions and small amounts. The increasing necessity of mobile payments has made it crucial to safeguard payment applications, devices, accounts, and users. Digital-payment users may not always be targeted due to weak payment infrastructure. Deception is the basis for many

fraudulent actions.' An individual who impersonates a bank employee, customer-care representative, merchant, or trusted contact can use this method to convince unauthorized users to disclose confidential information or approve transactions. Other types of attacks may involve malicious applications, hacked devices or mobile numbers being used, as well as fraudulent.

The aim of this research is to investigate the significant cybersecurity concerns related to UPI and digital payments, as well as to comprehend users' awareness and security measures. The research investigates whether heightened cognition leads to safer payment practices.



Fig -1

2. Body of Paper

LITERATURE REVIEW

2.1 Studies on Digital Payment Security

The Reserve Bank of India has identified cybersecurity and consumer protection as important requirements for the continued adoption of digital payments. Its survey evidence provides information on fraud exposure and the methods used in fraud or attempted fraud. Regulatory guidance also emphasizes awareness because many attacks depend on users responding to deceptive communication.

2.2 Studies on UPI Fraud

Research specifically focused on UPI has investigated fraudulent transactions, phishing links, QR codes and automated fraud detection. Machine-learning studies have explored the identification of suspicious transaction patterns,

while user-focused studies examine awareness and safe payment behavior.

2.3 Phishing and Social Engineering

Phishing and social engineering exploit human decision-making. Attackers may create urgency or trust by impersonating banks, payment applications or customer support. These techniques are particularly relevant to UPI because the final authorization of many transactions requires user action.

2.4 Machine Learning for Fraud Detection

Recent research has increasingly examined machine-learning and deep-learning techniques for payment fraud detection. Anomaly detection and behavioral analysis can complement traditional security rules by identifying transaction patterns that differ from normal behavior.

2.5 Research Gap

Existing literature contains substantial work on technical fraud detection, but there is also a need to understand the user perspective. This paper therefore combines cybersecurity discussion with evidence from published surveys, focusing on the relationship between threat exposure, awareness and user behavior.

3. CYBERSECURITY CHALLENGES IN UPI AND DIGITAL PAYMENTS

3.1 Phishing and Social Engineering

Phishing and social engineering exploit human trust rather than relying only on technical vulnerabilities. Fraudsters may send deceptive messages or make calls that appear to come from a bank, payment provider or customer-support service. The attacker may create urgency and ask the victim to click a link, install an application or disclose confidential information. Such attacks can be difficult to prevent through technology alone because the final action is performed by the user.

3.2 QR-Code and Payment-Request Scams

QR codes simplify payments but can also be used as part of fraudulent schemes. A user may be asked to scan a QR code under the false impression that scanning will result in receiving money, when the intended action may instead initiate a payment. Similarly, unexpected collect or payment requests may be approved without checking the recipient. Clear user-interface warnings and user education can help reduce this risk.

3.3 Fake Applications and Malware

Fake payment or banking applications can imitate legitimate services and attempt to obtain sensitive information. Malware on a smartphone may also interfere with messages, notifications or other device functions. Installing applications from trusted sources, reviewing permissions and keeping operating systems and applications updated are important security practices.

3.4 SIM-Swap and Mobile-Based Attacks

Because a mobile number can be linked with banking and payment services, unauthorized control of a mobile number can create security risks. SIM-swap attacks attempt to transfer a victim's mobile service to another SIM under an attacker's control. Protecting account credentials, monitoring unexpected loss of mobile service and contacting the telecom provider promptly when suspicious activity occurs are relevant precautions.

3.5 Account Takeover and Credential Theft

Account takeover can occur when attackers obtain passwords, authentication information or control of a device. Users may unknowingly reveal credentials through phishing or install software that assists an attacker. Strong authentication, device security and careful handling of confidential information reduce the opportunities for unauthorized access.

3.6 Data Privacy and Information Leakage

Digital payments involve the processing of transaction and account-related information. Unauthorized access, inappropriate sharing or insecure handling of such information may create privacy risks. Users should avoid sharing confidential banking information through unverified channels, while service providers must maintain appropriate controls for protecting sensitive data.

4. EXISTING SECURITY MECHANISMS

4.1 UPI PIN and Authentication

The UPI PIN is used to authorize bank transactions. Users should keep the PIN confidential and should not enter it in response to unverified instructions. Authentication provides an important layer of protection, but it depends on users understanding when authorization is actually taking place.

4.2 Transaction Notifications

Transaction notifications allow users to monitor payment activity and identify unexpected transactions. Prompt recognition of suspicious activity can support faster reporting and response.

4.3 Device and Application Security

Device locks, operating-system updates, application updates, trusted application sources and appropriate application permissions can reduce several device-related risks. Users should avoid installing applications from unknown sources.

4.4 Fraud Monitoring

Financial institutions and payment providers can monitor transaction patterns to identify suspicious activity. Rule-based systems can be complemented by machine-learning approaches that identify unusual transaction behavior.

4.5 User Awareness

User awareness is an important layer of digital-payment security. Awareness programs should use practical examples of fake customer-care calls, suspicious links, QR-code scams and

fraudulent payment requests rather than relying only on general warnings.



Fig -2

5. RESEARCH METHODOLOGY

5.1 Research Design

The study follows a mixed-method and secondary-data-oriented design. Instead of presenting invented responses as original fieldwork, the quantitative discussion uses findings reported by publicly available surveys and published research. Qualitative interpretation connects these findings with common cybersecurity behaviors.

5.2 Data Sources

Three main evidence sources are used. First, the Reserve Bank of India's nationwide survey provides findings from approximately 90,000 consumers and merchants. Second, a Local Circles survey reported more than 32,000 responses from UPI users across 365 districts. Third, a 2026 academic study reports cybersecurity awareness, suspicious UPI communication and fraud-experience percentages.

5.3 Data Analysis

The published findings are analyzed using frequency and percentage comparison, identification of common fraud methods, comparison of awareness and exposure, and interpretation of reporting behavior. The percentages from different studies are kept separate because the samples, methodologies and periods differ.

5.4 Research Ethics and Data Limitations

No claim is made that the author independently collected the survey responses used in this paper. Published findings are



Fig -3

attributed to their original sources. Because the surveys differ in population, sample design and time period, their percentages should not be merged into a single statistical dataset.

6. INTERVIEW-BASED QUALITATIVE ANALYSIS

6.1 Fraud Exposure: RBI Survey

The RBI nationwide survey involved approximately 90,000 merchants and consumers across rural and urban areas. It found that 94.5% of users reported that they had not experienced fraud. The reported incidence of encountering fraud or attempted fraud was 4.1% in metropolitan areas and 6.4% in semi-urban areas.

Table -1:

RBI survey finding	Reported result
Users reporting no fraud experience	94.5%
Fraud/attempted fraud – metropolitan areas	4.1%
Fraud/attempted fraud – semi-urban areas	6.4%

The findings show that most respondents did not report fraud experience, while also demonstrating that attempted fraud occurs across different geographic settings. The figures should be interpreted as survey-specific estimates rather than a universal fraud rate.

6.2 Methods Used in Fraud or Attempted Fraud

Table -2:

Fraud/attack method	Percentage
Vishing	54.2%
Phishing	37.2%
Misuse of collect request	28.7%
Remote access	25.5%
Fake numbers associated with e-wallets/banks	~11%

Vishing was the most commonly reported method among the listed categories, followed by phishing. These categories are not necessarily mutually exclusive. The results demonstrate the importance of protecting users from social-engineering attacks in addition to technical attacks.

6.3 UPI Fraud Experience: Local Circles Survey

A Local Circles survey reported in June 2025 collected more than 32,000 responses from UPI users across 365 districts in India. The survey reported that approximately one in five families with a UPI user had experienced fraud at least once during the preceding three years.

Table -3:

Local Circles finding	Reported result
UPI-using families experiencing fraud	Approximately 1 in 5
Affected respondents who did not report fraud	51%

The finding that 51% of affected respondents did not report the incident is significant. Under-reporting may make it difficult for institutions and authorities to estimate the full scale of fraud and identify recurring attack patterns. It also indicates the importance of simple and accessible reporting mechanisms.

6.4 Cybersecurity Awareness: 2026 Academic Study

A 2026 academic study on cybersecurity risks in UPI-based digital payment systems reported three levels of cybersecurity awareness among its respondents.

Table -4:

Awareness level	Percentage
High	35%
Moderate	40%
Low	25%

The results indicate that awareness is not uniform. While 35% of respondents were classified as highly aware, 65% fell into moderate or low-awareness categories. This suggests that expanding cybersecurity education remains relevant even among users who regularly use digital payments.

6.5 Suspicious UPI Links and Calls

Table -5:

Experience	Percentage
Received a suspicious UPI link or call	48%
Did not report receiving one	52%

Nearly half of the respondents in the cited study had received a suspicious UPI-related link or call. This demonstrates that exposure to attempted fraud can be much broader than confirmed financial loss. It also corresponds with the RBI survey's identification of vishing and phishing as important methods.

6.6 Experience of UPI Fraud

Table -6:

Experience	Percentage
Experienced UPI fraud	18%
Did not experience UPI fraud	82%

The majority of respondents had not experienced UPI fraud, but 18% reported such an experience. Comparing this with the 48% who had received a suspicious link or call illustrates the difference between exposure to an attempted attack and actual reported fraud.

7. RECOMMENDATIONS AND FUTURE SCOPE

7.1 Practical User Awareness

Awareness programs should demonstrate real examples of fake customer-care calls, suspicious links, QR-code scams, fake cashback offers and fraudulent payment requests.

7.2 Intelligent Fraud Detection

Machine-learning models can be investigated for identifying unusual transaction behavior and risk patterns. Such systems should complement, rather than replace, existing authentication and monitoring controls.

7.3 Behavior-Based Risk Analysis

Future systems could consider transaction amount, frequency, device characteristics, recipient behavior and other contextual signals to identify anomalies while controlling false alerts.

7.4 Improved Fraud Reporting

Reporting pathways should be simple, visible and understandable. Faster reporting can support investigation and may reduce the impact of fraudulent transactions.

7.5 Privacy-Preserving Security

Future research should investigate fraud-detection methods that strengthen security while limiting unnecessary exposure of personal and transaction data.

7.6 Future Research

Future studies should use larger and more diverse samples and compare cybersecurity behavior across age groups, occupations, geographic settings and levels of digital-payment usage.

8. OVERALL FINDINGS

Table -7:

Area examined	Key evidence
Fraud exposure	RBI: 94.5% reported no fraud experience
Major method	RBI: vishing 54.2%
Phishing	RBI: 37.2%
Payment-request misuse	RBI: 28.7%
UPI fraud exposure	Local Circles: about 1 in 5 families
Non-reporting	Local Circles: 51% of affected respondents
High awareness	2026 study: 35%
Moderate awareness	2026 study: 40%
Low awareness	2026 study: 25%
Suspicious link/call exposure	2026 study: 48%
Reported UPI fraud experience	2026 study: 18%

The reviewed evidence presents a consistent research direction: digital-payment cybersecurity must address both the technology used to process transactions and the behavior of the people using it. Phishing, vishing, deceptive payment requests and social engineering demonstrate why user decisions remain important even when secure payment infrastructure is available.

At the same time, technical approaches such as anomaly detection and machine learning can provide additional protection by identifying suspicious behavior at scale. The strongest future direction is therefore a layered model in which user education, authentication, monitoring, automated detection and reporting mechanisms work together.

3. CONCLUSIONS

UPI and digital payments have transformed financial transactions by providing fast and convenient payment services. However, increased adoption has also created cybersecurity challenges involving phishing, social engineering, QR-code fraud, malicious applications, SIM swapping, account takeover and information leakage.

The reviewed literature and survey evidence show that both technical and behavioral factors contribute to digital-payment security. The RBI survey identifies vishing and phishing among important fraud or attempted-fraud methods, while the Local Circles survey highlights UPI fraud exposure and the problem of non-reporting. A recent academic study further indicates that

users have varying levels of cybersecurity awareness and substantial exposure to suspicious UPI communications.

The results should not be interpreted as a single combined statistical study because the evidence comes from different surveys and research populations. Instead, the studies collectively provide evidence that cybersecurity risk exists at several layers of the digital-payment ecosystem.

Securing UPI therefore requires a layered approach involving strong authentication, transaction monitoring, intelligent fraud detection, user awareness, secure application practices and effective reporting mechanisms. Future research can further investigate behavioral fraud detection, privacy-preserving machine learning and methods for improving user responses to social-engineering attacks.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to everyone who supported and guided us in completing our research paper titled “Cybersecurity Challenges in UPI and Digital Payments.”

We are deeply thankful to our co-author and guide, Prof. Aarti Sanjay Gawai, Assistant Professor, Department of Information Technology and Computer Science, D.G. Ruparel College, Mumbai, for her valuable guidance, encouragement, and support throughout the preparation of this research work.

We would also like to thank the Department of Information Technology and Computer Science, D.G. Ruparel College, for providing us with the opportunity and academic support to undertake this research.

We are grateful to the various published sources, surveys, and research studies referred to during this work, which helped us understand the cybersecurity challenges associated with UPI and digital payments.

Finally, we would like to thank our family, friends, and everyone who directly or indirectly supported and encouraged us during the completion of this research paper.

REFERENCES

1. National Payments Corporation of India (NPCI), UPI and digital-payment security information, official resources.
2. Reserve Bank of India (RBI), publications and guidelines relating to digital payments, payment systems and customer protection.
3. Ministry of Electronics and Information Technology (MeitY), Government of India, cybersecurity awareness resources.
4. Reserve Bank of India, Annual Reports and payment-system information, relevant editions.
5. Academic journal and conference literature on mobile-payment security, phishing, social engineering, fraud detection and cybersecurity awareness.
6. Additional peer-reviewed sources identified during the literature-review stage.