International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 06 | Jun 2026 www.irjet.net p-ISSN: 2395-0072

Cybersecurity Risks in UPI Ecosystems: Fraud Mechanisms, User Vulnerabilities

Ms. Manasi Kalgutkar[1], Mr. Himanshu Sharma[2], Dr. Shiv Kumar Goel

Associate Professor / H.O.D.[3] Department of Computer Applications (MCA)
Vivekanand Education Society's Institute of Technology (VESIT), Chembur, Mumbai

---

Abstract - *The Unified Payments Interface (UPI) has emerged as one of the most important parts of India's digital payments eco-system in terms of providing instant, cheap and inter-operable payments. However, while there has been tremendous growth in adoption of UPI, there have also been increasing instances of cyber fraud, such as phishing, fake payment links, QR code manipulation, scams using KYC norms, misuse of AutoPay service, etc. This paper will look at security threats to UPI eco-systems, focusing in particular on how frauds leverage user vulnerabilities. For research purposes, a mixed method approach consisting of literature review and descriptive survey of 50 people is used. A total of 30% of respondents stated that they were very much aware about cybersecurity threats, while 36% were unaware of the PIN safety rule of UPI, and 38% of respondents were unaware of the QR code threat. Moreover, 30% of the respondents stated that either they themselves or those known to them had been victims of fraud from UPI. Also, respondents stated that fraud was mainly caused due to poor security, carelessness while transacting, and social engineering.*

Key words - UPI, cybersecurity, digital payments, fraud detection, social engineering, user awareness

1. INTRODUCTION

The evolution of financial transactions in India has been aided significantly by digital payments, and among these, UPI is perhaps the most important. A product of NPCI, UPI facilitates real-time fund transfer services using mobile applications. It is widely adopted for peer-to-peer payments, merchant payments, bill payments, and recurring payments. Past studies cite convenience, interoperability, low transaction costs, and integration of banking/FinTech applications as the driving forces behind its fast adoption [1], [4].

However, the increasing use of UPI increases the potential exposure to cyber frauds as well. The previous literature on the topic identifies phishing attacks, vishing, spoofing of payments, cloned apps, QR-code attacks, KYC scams, misuse of AutoPay, and unauthorized access as some of the most common threats to users [2]-[5]. While such issues don't generally arise due to vulnerabilities of the underlying payment system, these vulnerabilities occur at the level of the user, their devices, and applications [3], [4].

In this paper, the UPI fraud is treated as a socio-technical problem in terms of cybersecurity. A combination of literature review findings and the survey results of 50 respondents is used to investigate fraud mechanisms' exploitation of user vulnerabilities, user perceptions of cyber risks, and the limitations of current security measures.

2. LITERATURE REVIEW

UPI cybersecurity literature can be classified according to four main topics: adoption, fraud typologies, user vulnerability, and fraud detection.

The first set of papers provides an overview of UPI adoption in India. It describes UPI as a revolutionary technology in the country's digital payments system. High-speed, accessibility, interoperability, and user-friendly interface have significantly promoted the transition to cashless economies. On the other hand, excessive use reduces user's attention to security warnings and transaction verification, increasing vulnerability to fraud [1], [4].

Another group of articles presents typical types of UPI frauds: phishing/vishing, fake collection request, app cloning, QR-code manipulation, Know Your Customer scam, subscription/AutoPay fraud, and false customer-care interaction [2]-[5]. In general, all of them represent frauds based on deception. Attackers exploit urgency, trust, fear, and official-looking communication to convince users to verify transactions by themselves [2], [5].

A third group analyzes the behavioral and socio-demographic vulnerability. Previous works reveal that fraud exposure is determined by digital literacy, user confidence, education, age, and transaction habits [3], [4]. Overconfidence and inexperience increase the risk: some users confirm requests instantly, and some cannot recognize unusual prompts. The awareness-behavior gap is another important factor: some users know basic safety regulations but do not follow them in practice [3], [4].

Finally, the last set of papers analyzes security controls and fraud detection. Available protection methods consist of encryption, device binding, PIN authentication, blacklisting, and rule-based monitoring [4]. While these mechanisms remain valuable, recent papers claim that they become

insufficient to detect deception-based frauds. Thus, technical literature proposes several approaches like Random Forest, XGBoost, SVM, CNN, LSTM, and hybrid rule-ML models as solutions to detect suspicious behavior in near-real-time [2], [5]. However, these approaches encounter several difficulties, including lack of labeled data, class imbalance, false positive detections, delays, and implementation difficulties [2].

Overall, the literature reveals that UPI fraud is not merely a technical problem. It is a result of interactions between fraud techniques, user behavior, and institutional measures. That is why the integration of the secondary literature and primary survey data is necessary.

3. PROBLEM DEFINITION

While UPI made payments easier and faster, at the same time, this technology created cybersecurity threats. Current literature demonstrates that a majority of UPI fraud schemes does not require hacking the system itself; it rather exploits vulnerabilities related to manipulation of users into carrying out or enabling fraud transactions. These include phishing, fraud requests, QR-code fraud, KYC fraud and social engineering [2]-[5].

Survey results confirm these concerns. Awareness is inconsistent, users' knowledge of critical security rules is insufficient, and exposure to fraud cases persists. Thus, the key problem consists in analyzing interaction of different fraud mechanisms and user vulnerabilities and explaining reasons for failures of current protection measures to prevent these attacks.

4. Objectives and Scope

4.1 Objectives

The purpose of the research includes the following:

1. Identification of main types of UPI fraud disclosed in previous studies.
2. Determination of how user awareness and behavior and socio-demographic features affect vulnerability to fraud.
3. Analysis of survey data from 50 UPI users on usage, awareness, fraud exposure, and views on security of UPI.
4. Evaluation of methods of fraud detection and prevention, rule-based and ML-based
5. Propose recommendations for strengthening UPI cybersecurity through technical, behavioral, and institutional measures.

4.2 Scope

The research covers the UPI environment in India alone. It is a mixture of secondary research coupled with a primary survey conducted on 50 participants. It considers aspects such as fraud mechanisms, user vulnerability, awareness, transaction behavior, and perception of security. This study does not include real-time fraud detection models or analysis of transaction data.

5. RESEARCH METHODOLOGY

The study adopts a research methodology involving literature review and descriptive survey analysis. Literature review was based on recent academic papers and technical documents in regards to the UPI usage, types of frauds, user vulnerability, and fraud detection techniques. The five source papers included in the study were the core references [1]-[5].

Primary data was collected through a structured survey questionnaires on 50 participants. This included questions on demographic profile, duration and frequency of using UPI services, main use case, platform used, cybersecurity awareness, knowledge of UPI PIN rule, knowledge of risks associated with QR-code, verification methods, exposure to suspicious transactions, experience of being victimized by fraud, causes of fraud and perception about user awareness and security measures.

Descriptive statistics were applied to the obtained data – specifically, the number and percentage of the answers. The research was exploratory – it aimed to provide additional user-level information in order to supplement the existing literature on the topic.

6. ANALYSIS AND FINDINGS

6.1 Demographic Profile

The respondents belonged to four age groups: 18-25 years (12%), 26-35 years (24%), 36-45 years (34%), and 46+ years (30%). In terms of occupation, there were more homemakers (32%) than other categories: self-employed people (28%), working individuals (24%), students (10%), and other occupations (6%).

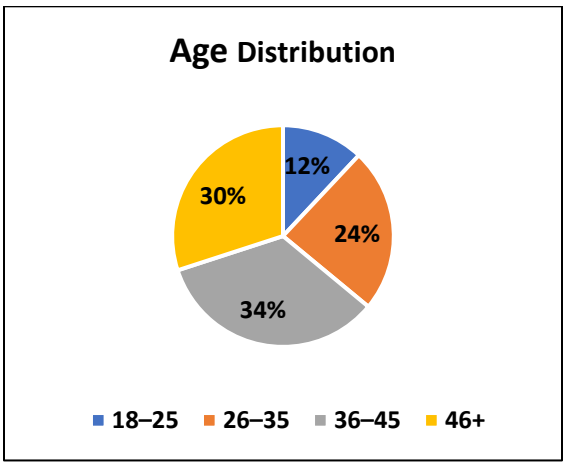

Figure 1: Age Distribution

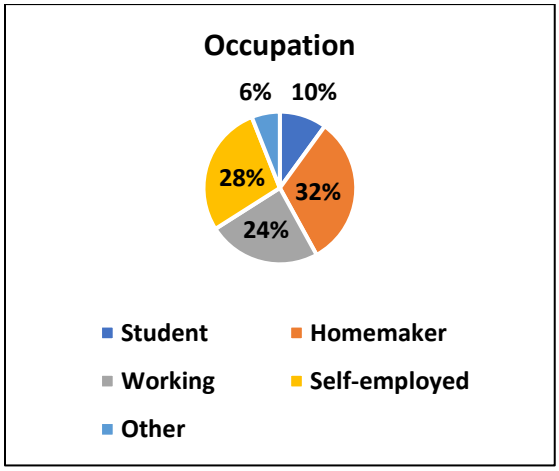

Figure 2: Occupation

It means that UPI is used by the socially diverse community. Indeed, the literature states that users who are vulnerable to frauds do not belong to the same category [3].

6.2 UPI Usage Behavior

Most of the respondents were regular users of UPI. As far as the time spent using UPI is concerned, 32% used it for 3-5 years, 30% for 1-3 years, 22% for less than 1 year, and 16% for more than 5 years. Also, usage frequency was quite high – 26% used it multiple times per day, 24% once per day, 24% weekly, and 26% occasionally.

The most frequent purposes of the use were bills (26%) and QR payments (26%). Other reasons were receiving money (18%), shopping (16%), and sending money (14%).

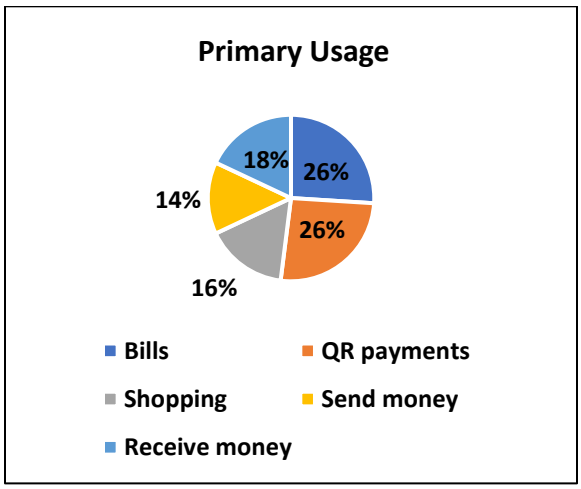

Figure 3: Primary Usage

Regarding the platform, the most popular one was Google Pay (60%), followed by PhonePe (28%) and BHIM (12%).

All these results confirm the literature claim that UPI is an integral part of financial activities [1], [4]. Regular use and habituality may lead to lack of attention and increased risk of accepting suspicious actions without verification.

6.3 Awareness of Cybersecurity Risks

Levels of awareness were different among the respondents. 30% described their level of awareness as high, 20% moderate, 32% low, and 18% stated that they are not aware.

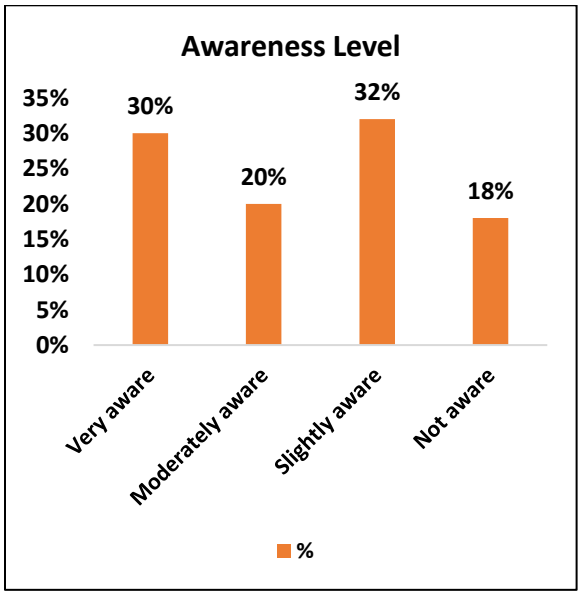

Figure 4: Awareness Level

This fact is important due to previous studies where it is shown that fraud is usually successful in cases when awareness is not sufficient or superficial [3], [4]. It is confirmed by the survey results that many users are not really aware of cybersecurity threats.

6.4 Knowledge of PIN and QR-Code Security

Users were knowledgeable about particular rules related to cybersecurity.

Only 34% claimed that they know the UPI PIN safety rule, while 36% denied this and 30% were unaware of it. Similar results were found regarding QR-code risks (only 28% claimed to be familiar with them).

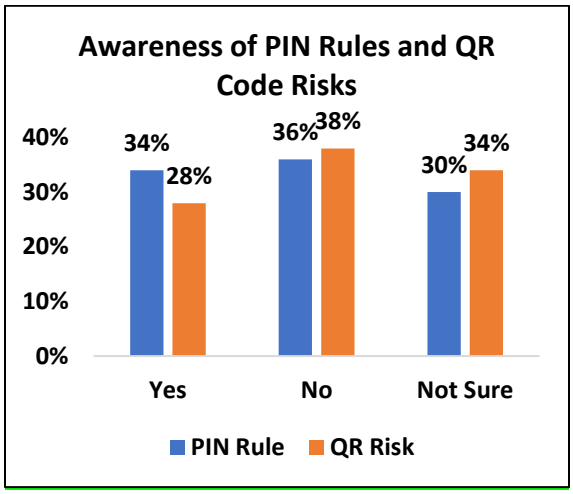

Figure 5: Awareness of PIN Rules and QR Code Risks

The findings of the survey correspond well to previous research on collecting fake requests, phishing, and QR code scams [2]-[5]. Often, scammers use the user's misunderstanding of when it is necessary to enter a PIN and whether scanning a QR code will lead to an unsafe transaction.

6.5 Exposure to Fraudulent Activity and Frauds

As regards suspicious payment requests, 26% stated that they have been exposed to them, 36% that they haven't been exposed to such requests, and 38% were unsure about that. As for direct experience of fraud, 30% mentioned that they or their acquaintances experienced UPI frauds, 42% mentioned that they didn't and 28% were unsure.

The high percentage of "not sure" answers is very important as it may mean that many users cannot distinguish between suspicious request, an error and a fraud case. This supports the assertion of the literature that User uncertainty regarding suspicious payment requests may increase the likelihood of becoming a victim of deception-based fraud [3], [4].

6.6 Transaction Verification Behavior

The transaction verification behavior of users is varied. Only 22% claimed that they always check transactions, 12% - often, 22% - sometimes, 16% - rarely, and 28% - never.

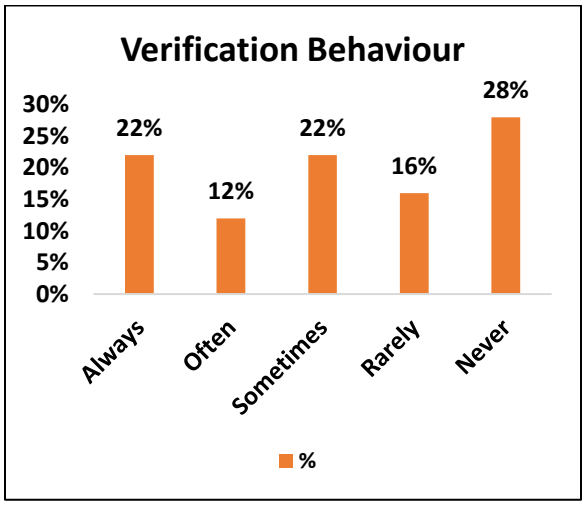

Figure 6: Verification Behavior

It is one of the most significant behavioral findings from the survey because many fraud cases occur during the final stage of transactions. The literature makes the same point and highlights that the mere awareness without careful transaction behavior does not ensure sufficient protection [3], [4].

6.7 Causes of Fraud

The causes of the fraud that the respondents mention the most often are weak security practices (26%), carelessness during the transactions (24%) and social engineering (22%). Lack of awareness and technical vulnerabilities were mentioned by 14% of respondents each.

These findings support the socio-technical perspective on the problem that is discussed in the literature [2]-[5]. It means that users understand that fraud is not only about system's vulnerability but also about unsafe practices and deception. Still, they do not neglect the importance of platform's side protection.

6.8 Awareness Programs and Security Sufficiency

On the necessity of awareness, 22% of respondents strongly agreed and 26% agreed, while 26% were neutral and 26% disagreed. Concerning awareness programs' importance, 30% strongly agreed and 22% agreed. On sufficiency of current security measures, 14% strongly agreed, 34% agreed, 16% were neutral, and 36% disagreed. This implies two conclusions. Firstly, awareness continues being important, but users do not believe that current approaches are sufficient. Secondly, trust in existing measures is ambivalent. This confirms the literature that finds current controls to be necessary but insufficient in the case of social engineering [3]-[5].

7. Proposed Solutions and Recommendations

Combining the results of the literature review and survey reveals that UPI cybersecurity must be reinforced using multi-layered approach.

Firstly, user awareness and digital literacy must be enhanced using practical and scenario-based education. As most participants did not know about safety rules for PIN codes and QR codes, awareness initiatives must emphasize specific threats: fake collect requests, malicious modifications of QR code, phishing, remote access frauds, and false customer care scams [2]-[5].

Secondly, context-aware authentication must be reinforced. While traditional PIN/OTP control is essential, it is not sufficient if users become victimized through manipulation to confirm their consent to any transactions. Additional verification step must be introduced for irregular transactions, new beneficiary, risky QR payments, and creating an AutoPay mandate [2], [4].

Thirdly, real-time monitoring and anomaly detection must be increased. Survey respondents reported about fraud exposure even in presence of security controls, which proves the literature's claim that static rule-based systems have limitations. Real-time detection must identify suspicious transaction patterns, repetitive suspicious requests, and abnormal user behavior [2], [4], [5].

Fourthly, hybrid models of fraud detection combining rule-based and machine-learning approaches must be introduced gradually. According to the literature, hybrid models prove to be better solutions than purely static ones to cope with sophisticated patterns of fraud [2], [5].

Fifthly, secure interface and QR code design must be improved. Details of the merchant, debit direction, and payment warnings must be displayed before confirming transaction. Because QR code understanding was extremely low in the survey, the design of the interface must minimize confusion among users [2]-[5].

Finally, fraud reporting and response must be easier and more visible. Users must be able to easily report suspicious activity in-app, and institutions must react to these reports sufficiently fast to minimize loss and accumulate experience [4], [5].

Lastly, coordination within the institutions, that is banks, NPCI, RBI and FinTech providers is essential. Since UPI system is interconnected, then security controls, warning patterns and fraud intelligence should align more often on each platform [2], [4], [5].

8. LIMITATIONS AND FUTURE SCOPE

There are certain limitations to this research paper. It is conducted based on the answers provided by just 50 participants; hence, the results are purely descriptive and cannot be generalized to any further extent. In addition, the sample size has low geographical representation and may not include users of all UPI segments. Furthermore, the survey is based on subjective data, that is there may be potential recall bias, uncertainty and even interpretation mistakes. The real-time fraud detection models are not tested.

The future research may include expanding the sample size of the survey, conducting inferential statistical analyses, comparing different UPI platforms and testing the efficacy of hybrid fraud detection systems as well as interface security enhancements.

9. CONCLUSION

This research paper demonstrates that the problem of UPI fraud can be defined from the point of view of socio-technical cybersecurity. The existing literature proves that the main kinds of UPI fraud, for example phishing, fake requests, QR-code scamming, KYC fraud and AutoPay fraud do not depend on compromising the main payment system, but on its manipulation [2]-[5]. The conclusions from the survey are consistent with these assumptions – low awareness and knowledge of the safety rules, inconsistent transaction verification and significant level of fraud exposure on the part of respondents.

The combined results suggest that the fraud mechanisms succeed because of the intersection of their capabilities and users' weaknesses, namely, insufficient awareness and uncertainty, routine confirmation of transactions and trust in the official interface [3], [4]. While security controls are still relevant, they are not enough alone.

REFERENCES

[1] D. K. Sahoo, B. C. M. Patnaik, and I. Satpathy, "Adoption of Unified Payment Interface (UPI): A Literature Review," Journal of the Oriental Institute, Jun. 2024.

[2] N. B. Chakka and S. S. Saheba, "Mobile Payment Fraud Detection in UPIs through Machine Learning Techniques: A Systematic Review," 2025.

[3] R. Sharma, R. Matharu, and R. Sinha, "Socio-demographic and Behavioral Determinants of UPI Fraud Vulnerability: A Descriptive Study from Shimla District, Himachal Pradesh," J. Forensic Sci. Res., vol. 10, no. 1, pp. 009-014, 2026.

[4] R. B. Valave and P. D. Borhade, "An Empirical Study on Cybersecurity Risks in UPI-based Digital Payment Systems," International Journal of Science and Research (IJSR), 2025.

[5] S. Jogdand-Gaikwad, C. Choudhary, H. Sharma, A. Birajdar, S. Yadav, and V. Raskar, "A Survey on UPI Fraud Detection System," International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM), vol. 12, no. 5, Sep.-Oct. 2025.