Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Digital Payments and Security: A Study on UPI User Awareness

Mr. Vinayak Eknath Midgule
Computer Science Department
Sri.Jagadishprasad Jhabarimal Tibrewala University
Rajasthan, India

Dr.Archana Tukaram Bhise
Computer Science Department
Sri.Jagadishprasad Jhabarimal Tibrewala University
Rajasthan, India

Abstract **- The rapid adoption of Unified Payments Interface (UPI) has transformed India's digital payment ecosystem, offering convenience, speed, and accessibility to millions of users. However, this surge in usage has also exposed users to increasing cybersecurity risks such as phishing, malware attacks, fraudulent apps, and social engineering scams. Despite the government and financial institutions implementing robust security frameworks, the problem persists largely due to inadequate user awareness and unsafe practices. Many UPI users lack sufficient knowledge about secure transaction methods, password hygiene, and recognizing fraudulent activities, which makes them vulnerable to exploitation. This study investigates the level of cybersecurity awareness among UPI users, identifying gaps in knowledge and behavior that contribute to financial fraud. The research highlights the problem statement: while technological safeguards exist, user negligence and limited awareness remain critical vulnerabilities in the digital payment ecosystem. To address this issue, the paper proposes a multi-pronged solution. First, structured awareness campaigns should be launched by banks, fintech companies, and regulatory bodies to educate users about common threats and safe practices. Second, integrating user-friendly security prompts and real-time fraud alerts within UPI applications can reinforce secure behavior. Third, digital literacy programs at community levels can empower new users, especially in rural and semi-urban areas, to adopt safe practices. By combining technological innovation with user education, the study argues that cybersecurity resilience in UPI transactions can be significantly enhanced. Ultimately, strengthening user awareness is not just a protective measure but a prerequisite for sustaining trust and growth in India's digital payment ecosystem.**

Keywords - Cybersecurity Awareness, Unified Payments Interface (UPI), Digital Payments, Financial Fraud Prevention, User Education.

I. INTRODUCTION

Digital payment systems have become a vital part of India's financial transformation, reshaping the way individuals and businesses conduct everyday transactions. Among these systems, the Unified Payments Interface (UPI) has emerged as one of the most widely adopted and trusted platforms. Developed by the National Payments Corporation of India (NPCI), UPI enables users to transfer money instantly through smartphones, removing the dependence on cash, debit cards, and traditional banking infrastructure. Its ease of use, interoperability across banks, and minimal transaction costs have made it accessible to people across urban, semi-urban, and rural regions, significantly promoting financial inclusion.

Despite its success, the rapid expansion of UPI has also created new opportunities for cybercriminals. Rather than targeting technical weaknesses in the system, fraudsters increasingly exploit human behavior and lack of awareness. Users are often deceived through phishing messages, fake customer care calls, malicious links, and fraudulent mobile applications that closely imitate genuine UPI services. These attacks have led to substantial financial losses and have raised serious concerns about the safety of digital payment users.

Although banks, fintech companies, and regulatory authorities continuously enhance security mechanisms such as multi-factor authentication, encryption, and transaction monitoring, cyber fraud continues to persist. This highlights a critical gap between technological safeguards and user behavior. Many users remain unaware of basic cybersecurity practices, such as identifying suspicious requests, protecting personal credentials, and responding appropriately to fraud attempts. As a result, technology alone cannot ensure complete security in digital payment systems.

This study underscores the importance of user awareness and responsible usage as key elements in strengthening cybersecurity within the UPI ecosystem. By understanding user behavior and identifying gaps in awareness, the research aims to contribute toward creating a safer and more resilient digital payment environment in India.

II. LITERATURE REVIEW

Kumar et al. [1] point out that although users appreciate the speed and convenience of UPI, many are unaware of basic safeguards such as two-factor authentication, proper fraud-reporting mechanisms, and secure transaction practices. Their analysis shows that common threats like phishing, fake apps, and social engineering succeed mainly because of low user awareness rather than purely technical weaknesses. The authors stress that improving UPI security requires not only stronger technologies but also focused user education through multilingual campaigns and in-app guidance.

Focusing more closely on user perceptions,
Mungara et al. [2] explore how Indian UPI users actually understand and experience security risks. Through interviews and analysis of official guidelines, they find that while users are concerned about scams and data misuse, they often depend on scattered and unclear information. Much of the official advice is either too generic or poorly aligned with the real

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

threats users face. The study suggests that security guidance should be simpler, more contextual, and embedded directly within UPI apps to better support safe user behavior.

Looking beyond India, Zwilling et al. [3] compare cybersecurity awareness and behavior across users in four countries. Their findings show that even when people are aware of cyber threats, they often follow only basic protective practices. Awareness alone does not always translate into safer behavior, and cultural factors play an important role. This insight is especially relevant for UPI users, who may know about fraud risks but still act carelessly during real-world transactions.

Measurement of awareness itself is examined by Rohan et al. [4], who review studies that attempt to quantify information security awareness. They show that many existing tools suffer from weak design and poor validation. Their proposed framework provides guidance on how to build reliable awareness measurement scales, which is particularly useful for research that aims to assess cybersecurity awareness among UPI users in a structured and credible way.

User diversity is highlighted by Bhuyan et al. [5], who study working women in Assam to understand their use of UPI and mobile banking. While smartphone ownership is high, actual usage of banking apps remains limited, mainly due to security concerns and lack of confidence. The study reveals that UPI is mostly used for small, low-risk transactions and that education level alone does not guarantee adoption. The authors emphasize the need for targeted awareness programs, especially for women, to build trust and encourage broader use of digital payments.

From a broader smartphone security perspective, Kamarudin et al. [6] review studies on cyber risk mitigation and identify awareness, knowledge, and behavior as the three core elements of effective protection. Their review shows that users are frequently exposed to cyber risks but rarely convert awareness into safe actions. This finding directly applies to UPI users, whose security depends as much on daily behavior as on technical safeguards.

Technical vulnerabilities are explored in depth by Kaur et al. [7], who analyze popular UPI apps and identify weaknesses in authentication and design that can be exploited through social engineering attacks. Their work shows that users across age groups are often easily manipulated by fraudulent calls and messages. The study concludes that improving UPI security requires both protocol-level improvements and stronger user awareness to reduce susceptibility to scams.

Shifting to awareness training strategies, Khando et al. [8] review methods used to improve information security awareness in organizations. They find that human error is a major cause of security incidents and that interactive approaches such as gamification and feedback-based learning are more effective than traditional, passive training. These insights suggest that similar engaging methods could be useful for improving cybersecurity awareness among UPI users.

To place this topic within the wider research landscape, Muhammad et al. [9] conduct a bibliometric analysis of cybersecurity awareness studies published between 2018 and 2023. Their results show rapid growth in interest, especially during the COVID-19 period, and highlight human factors as a dominant theme. This helps position UPI awareness research as part of a broader global shift toward understanding user behavior in cybersecurity.

Finally, Sağlam [10] reviews cybersecurity education for children and adolescents and highlights large differences in curriculum quality and coverage across countries. Although the focus is on minors, the study reinforces important principles such as structured content, engaging teaching methods, and shared responsibility among institutions. These lessons are valuable when designing awareness initiatives for young and first-time UPI users.

III. RESEARCH METHODOLOGY

The following methodology is identified for this research work to provide a clear and systematic approach. It explains how data is collected, analyzed, and interpreted to support the findings of the study.

A. Data Collection

- Primary Data: will be Collected through structured questionnaires and interviews with UPI users from different demographic backgrounds.
- Secondary Data: will be Sourced from academic journals, government reports, RBI and NPCI publications, and credible online resources.

B. Sample Design

The study includes UPI users from urban, semi-urban, and rural areas to capture diverse usage patterns and awareness levels.

C. Data Analysis

Collected data is analyzed using percentage analysis and comparative methods to evaluate awareness levels and identify key risk factors.

D. Cybersecurity Threats in UPI Transactions

The increasing popularity of UPI has made it an attractive target for cybercriminals who exploit both technological access and human behavior. While UPI platforms are designed with strong security mechanisms, users continue to face several cybersecurity threats that primarily take advantage of a lack of awareness and unsafe usage practices.

E. Data Analysis

Collected data is analyzed using percentage analysis and comparative methods to evaluate awareness levels and identify key risk factors.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

IV. CYBERSECURITY THREATS IN UPI TRANSACTION

The increasing popularity of UPI has made it an attractive target for cybercriminals who exploit both technological access and human behavior. While UPI platforms are designed with strong security mechanisms, users continue to face several cybersecurity threats that primarily take advantage of a lack of awareness and unsafe usage practices.

A. Phishing Attacks

Phishing remains one of the most common threats faced by UPI users. In such attacks, fraudsters send deceptive messages through SMS, emails, or messaging applications that appear to come from legitimate banks or UPI service providers. These messages often contain urgent warnings about account suspension, failed transactions, or reward offers, prompting users to click malicious links or share sensitive details such as UPI PINs and OTPs. Many users, especially first-time or less tech-savvy individuals, fall victim to these scams due to the convincing nature of the messages and the fear of losing access to their accounts

B. Social Engineering Scams

Social engineering scams involve psychological manipulation rather than technical hacking. Fraudsters impersonate bank officials or customer care executives and contact users through phone calls or messages. By creating a sense of urgency or authority, they persuade users to disclose confidential information, approve fraudulent payment requests, or install remote access applications. These scams are particularly effective because they exploit trust and human emotions, making users believe they are interacting with legitimate representatives.

C. Malware and Fraudulent Applications

Another major cybersecurity threat arises from malware-infected and fraudulent mobile applications. Cybercriminals often design fake UPI apps or modified versions of popular applications that closely resemble genuine ones. When users unknowingly download these apps from unofficial sources, malware can be installed on their devices, allowing attackers to capture keystrokes, access stored credentials, and monitor transactions. Such applications can lead to unauthorized fund transfers and long-term data breaches.

D. Weak Authentication Practices

Weak authentication practices significantly increase the vulnerability of UPI users. Many individuals reuse simple or predictable PINs, fail to update passwords regularly, or share OTPs with others during transactions. In some cases, users approve payment requests without verifying the recipient's identity. These careless practices undermine the effectiveness of built-in security mechanisms and make it easier for cybercriminals to gain unauthorized access to accounts.

V. FINDINGS AND DISCUSSION

The findings of the study indicate that a considerable number of UPI users possess limited knowledge of safe digital payment practices, which significantly increases their vulnerability to cyber fraud. While most users are familiar with performing basic transactions such as sending and receiving money, many lack awareness of essential security precautions. Practices such as verifying payment requests, checking the authenticity of links and messages, and promptly reporting suspicious activities are often overlooked or misunderstood.

The study further reveals that users frequently respond impulsively to urgent messages or calls claiming to be from banks or customer care services. This behavior suggests a gap between awareness of UPI functionality and understanding of cybersecurity risks. In several cases, users were unaware that banks and UPI service providers never request sensitive information such as PINs or OTPs through calls or messages. Such misunderstandings make users easy targets for phishing and social engineering attacks.

A notable disparity in awareness levels is observed among different demographic groups. Rural users and elderly individuals show comparatively lower levels of cybersecurity awareness, largely due to limited exposure to digital technologies and a lack of formal digital literacy training. These users often rely on assistance from others to complete transactions, which further increases the risk of information leakage and fraud. In contrast, younger and urban users demonstrate relatively higher awareness but are still prone to risky behaviors, such as reusing passwords or ignoring security warnings.

The discussion highlights that user behavior plays a decisive role in cybersecurity breaches related to UPI transactions. Even with robust technological safeguards in place, unsafe practices and negligence can compromise system security. These findings reinforce the argument that cybersecurity is not solely a technical issue but a socio-behavioral challenge. Strengthening user awareness, promoting responsible digital habits, and designing user-friendly security features are essential to reducing fraud and ensuring the long-term sustainability of the UPI ecosystem.

A. Proposed Solutions and Recommendations

To address these challenges, the study proposes the following measures:

1. Structured Awareness Campaigns: Banks, fintech companies, and regulators should conduct regular, targeted cybersecurity education programs.

2. In-App Security Enhancements: User-friendly security prompts, transaction confirmations, and real-time fraud alerts should be integrated into UPI applications.

3. Community-Level Digital Literacy Programs: Training programs in rural and semi-urban areas can empower new users with safe digital practices.

4. Simplified Reporting Mechanisms: Easy-to-use fraud reporting features can encourage timely action.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level

VI. CONCLUSION

The success of the Unified Payments Interface (UPI) as a digital payment platform is not determined solely by the strength of its technology but also by the awareness and vigilance of its users. While UPI systems are equipped with

advanced security features, this study highlights that informed user behavior plays an equally crucial role in preventing cyber fraud. A lack of cybersecurity awareness and unsafe transaction practices continue to expose users to financial risks, despite the presence of robust technological safeguards.

The findings of this research emphasize that cybersecurity awareness is a fundamental requirement for the sustainable growth of digital payments in India. Educating users about potential threats, safe transaction practices, and timely fraud reporting can significantly reduce vulnerabilities within the UPI ecosystem. When users are empowered with the right knowledge, they become an active line of defense against cybercrime rather than passive victims.

In conclusion, strengthening user education alongside continuous technological innovation is essential to building a secure and trustworthy digital payment environment. A balanced approach that combines advanced security mechanisms with widespread awareness initiatives can enhance cybersecurity resilience, reinforce user confidence, and ensure the long-term success of UPI in India's rapidly evolving digital economy.

REFERENCES

[1] Kumar, K. (2025). Examining User Awareness and Addressing Security Challenges in the UPI Framework: A Comprehensive Analysis Framework. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. .

[2] Mungara, D., Ramulu, H., & Acar, Y. (2025). Security and Privacy Advice for UPI Users in India. , 6085-6103.

[3] Zwilling, M., Klein, G., Lesjak, D., Wiechetek, L., Çetin, F., & Basım, H. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62, 82 - 97. .

[4] Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon, 9.

[5] Bhuyan, B., Kalita, M., Meenakshi, N., Mishra, S., Channu, V., & Baruah, S. (2025). Awareness and Adoption of UPI Facilities among Working Class Women in An Academic Institution: A Study with Special Reference to Assam Agricultural University, Jorhat, India. Archives of Current Research International. .

[6] Kamarudin, S., Tang, L., Bolong, J., & Adzharuddin, N. (2023). A systematic literature review of mitigating cyber security risk. Quality & Quantity, 58, 3251 - 3273. .

[7] Kaur, S., Mishra, H., & Goyal, A. (2023). Cyber-Security in UPI Payments. International Journal for Research in Applied Science and Engineering Technology. .

[8] Khando, K., Gao, S., Islam, S., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Comput. Secur., 106, 102267.

[9] Muhammad, G., Pratama, A., Shaloom, C., & Cassandra, C. (2023). Cybersecurity Awareness Literature Review: A Bibliometric Analysis. 2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS), 195-199.

[10] R. B. Sağlam, V. Miller and V. N. L. Franqueira, "A Systematic Literature Review on Cyber Security Education for Children," in IEEE Transactions on Education, vol. 66, no. 3, pp. 274-286, June 2023.

[11] Reserve Bank of India (RBI). (2022). *Report on Trend and Progress of Banking in India*. Reserve Bank of India, Mumbai.

[12] National Payments Corporation of India (NPCI). (2023). *Unified Payments Interface (UPI) Product Statistics and Guidelines*. NPCI, India.

[13] Sharma, R., & Verma, S. (2021). Cybersecurity awareness and safe usage of UPI among digital payment users in India. *International Journal of Cyber Security and Digital Forensics*, 10(2), 45–54.

[14] Kshetri, N. (2017). Cybersecurity, economic development, and the digital divide: An analysis. *Journal of Global Information Technology Management*, 20(2), 75–93.

[15] Bansal, G., Zahedi, F. M., & Gefen, D. (2016). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2), 138–150.

[16] Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610–613.

[17] Garg, V., & Panchal, R. (2020). Digital payment systems and cybersecurity threats in India. *International Journal of Advanced Research in Computer Science*, 11(5), 112–118.

[18] OECD. (2020). *Consumer policy and fraud prevention in the digital age*. Organisation for Economic Co-operation and Development, Paris.

[19] Das, A., & Kumar, S. (2019). Adoption of digital payment systems in India: A study of UPI. *Journal of Internet Banking and Commerce*, 24(3), 1–15.

[20] CERT-In. (2022). *Guidelines for Cyber Security Incidents and Digital Payment Frauds*. Indian Computer Emergency Response Team, Government of India