WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Evaluating User Perceptions and Security Concerns in Unified Payments Interface (UPI) Services

Dr. Swati Santosh Jagtap

Assistant Professor, Department of Commerce, Sanskar Mandir Sanstha's Arts and Commerce College, Warje, Pune, INDIA
Email: swatisjagtap@gmail.com
Doi : https://doi.org/10.55248/gengpi.5.0824.2136

ABSTRACT :

Online payment systems have become integral to modern economies, significantly influencing consumer behavior and economic transactions. In India, the adoption of digital payments has seen exponential growth, with BHIM UPI alone facilitating 8.03 billion transactions worth ₹12.98 lakh crore in January 2023. By December 2022, the nation recorded approximately 9.19 billion digital transactions for the fiscal year 2022-23, underscoring the increasing reliance on digital financial platforms. This research critically examines the perceived security of Unified Payments Interface (UPI) services, a key determinant of user adoption and trust. Despite robust security protocols implemented by financial institutions, concerns regarding fraud, phishing, and the overall security of UPI transactions persist. A survey of 400 respondents reveals unanimous agreement that UPI does not require the disclosure of sensitive information, reflecting a high level of trust in its confidentiality. However, only 70.75% of users believe in the system's resistance to tampering, with 29.25% expressing neutrality or concern. Besides, 76.5% of respondents affirm that advancements in UPI technology have made transactions safer, though 23.5% remain doubtful. Notably, 65% of users recognize the potential risk of monetary theft during UPI transactions, and 100% agree that compromising an OTP or PIN could result in financial loss. Despite these concerns, 88% of respondents report overall satisfaction with UPI services. These findings highlight the urgent need for continuous enhancements in UPI security to strengthen user confidence and support the sustained expansion of digital payment systems.

Keywords: UPI, Online Payments Interface, PhonePe, Paytm

Introduction :

In the past few years, digital payment systems have revolutionized the financial sector, playing a crucial role in shaping consumer behavior and propelling economic growth. The Unified Payments Interface (UPI) has especially become a cornerstone of India's digital economy, allowing seamless, real-time transactions nationwide. With BHIM UPI recording over 8.03 billion transactions worth ₹12.98 lakh crore in January 2023 alone and an astonishing 9.19 billion digital transactions logged by December 2022 for the fiscal year 2022-23, the widespread adoption of UPI reflects the rapid move towards cashless payments in India. However, this widespread adoption raises significant concerns about the security of online transactions, especially given the increasing incidents of fraud and phishing.

As the reliance on UPI and similar platforms continues to grow, ensuring the security of these transactions has become of utmost importance. Despite the strong security measures put in place by banks and financial institutions, users remain worried about the safety of their transactions, particularly in terms of fraud prevention and data protection. Understanding and addressing these concerns is crucial for maintaining trust and driving further adoption of digital payment systems.

This study focuses on the perceived security of UPI services, examining user concerns and assessing the effectiveness of current security protocols. By analyzing the viewpoints of 400 UPI users, this research aims to provide insights into the factors that influence user confidence in digital payment systems and to pinpoint areas where enhancements are required. The discoveries from this research are not only pertinent for bolstering the security of UPI transactions, but also for guiding the development of more secure and user-friendly digital payment solutions in the future.

Review of Literature :

UPI Services

Unified Payments Interface (UPI) has revolutionized digital payments in India since its introduction by the National Payments Corporation of India (NPCI) in 2016. UPI allows for instant transfer of money between bank accounts via a mobile platform, making transactions simple, quick, and secure

(Rath, 2021). As of 2023, UPI accounts for over 8 billion transactions monthly, reflecting its widespread adoption and critical role in India's digital economy (NPCI, 2023).

Evolution of Digital Payment Systems and UPI

The evolution of digital payment systems, particularly in India, has seen significant growth, with UPI emerging as a leader. From earlier systems like NEFT and IMPS, UPI has introduced a seamless, interoperable payment interface that integrates various banks and financial institutions (Mishra & Singh, 2022). Studies show that UPI's success is largely due to its simplicity, security, and government support (Patel, 2021).

Security Features of UPI

The UPI framework incorporates multiple layers of security, including two-factor authentication (2FA), end-to-end encryption, and real-time transaction monitoring (Chaturvedi, 2022). The 2FA requirement mandates users to verify their identity through a PIN or biometric method, adding a critical layer of security (Kumar, 2021). The UPI system utilizes a Virtual Payment Address (VPA), which masks the actual bank account details, thereby reducing the risk of direct account breaches (Jain & Gupta, 2022).

Two-Factor Authentication (2FA)

Two-factor authentication is a mandatory feature in UPI transactions. Studies highlight that 2FA significantly enhances transaction security by requiring users to authenticate via both a mobile device and a personal PIN (Natarajan et al., 2021). Despite the strong security, there is ongoing research into the vulnerabilities of 2FA, particularly concerning SIM-swapping attacks, which can compromise mobile-based authentication (Verma & Raj, 2022).

Encryption Techniques

UPI transactions are secured through advanced encryption protocols, including AES-256 and SSL/TLS encryption (Sharma, 2022). These encryption standards ensure that data transmitted between users and servers are protected from interception and unauthorized access. Sharma's (2022) research points out that while encryption is robust, the possibility of man-in-the-middle attacks, although rare, cannot be entirely ruled out.

Virtual Payment Address (VPA)

The use of a Virtual Payment Address (VPA) is a unique feature of UPI, allowing users to make transactions without revealing sensitive bank details. According to Gupta & Sharma (2021), this feature significantly mitigates the risks of phishing and social engineering attacks, which are prevalent in traditional banking systems.

Challenges and Threats to UPI Security

Despite its robust security measures, UPI is not immune to threats. Common security challenges include phishing attacks, malware, SIM-swapping, and social engineering (Mukherjee & Singh, 2021). A study by Rao (2022) indicates that the number of fraud cases reported in UPI transactions has risen with the increased adoption of the platform.

Phishing Attacks

Phishing remains one of the most common threats to UPI users. Fraudsters often impersonate legitimate entities to steal sensitive information such as PINs and OTPs. According to Raj & Reddy (2022), nearly 40% of reported UPI fraud cases in 2021 were related to phishing. The study suggests that despite increased awareness campaigns, users still fall victim to sophisticated phishing schemes.

SIM-Swapping and Mobile-based Frauds

SIM-swapping involves fraudsters gaining control of a victim's phone number by tricking the telecom provider into transferring the number to a new SIM card. This allows the fraudster to intercept OTPs and initiate unauthorized transactions. Singh & Kumar (2022) report that SIM-swapping is responsible for a significant portion of high-value UPI frauds, emphasizing the need for stronger telecom security policies.

Social Engineering and Impersonation

Social engineering attacks, where fraudsters manipulate users into divulging sensitive information, are increasingly sophisticated. Studies by Mishra (2022) show that these attacks often exploit trust, with fraudsters posing as bank officials or customer service agents.

Malware and Trojans

Mobile malware and Trojans pose a significant risk to UPI transactions. These malicious programs can compromise the security of the user's device, capturing sensitive information or enabling unauthorized access to UPI apps (Verma & Patel, 2022). Research indicates that while UPI apps are generally secure, the broader Android ecosystem remains vulnerable, necessitating continuous security enhancements (Chandra & Desai, 2021).

Regulatory and Institutional Framework

The security of UPI services is also supported by a robust regulatory framework. The Reserve Bank of India (RBI) and the NPCI have laid down stringent guidelines for the security of digital payment systems (RBI, 2021). These guidelines include mandatory 2FA, real-time transaction monitoring, and user education initiatives (NPCI, 2022).

Role of RBI and NPCI

The RBI, in collaboration with NPCI, plays a pivotal role in regulating and overseeing the security of UPI services. Studies by Das & Roy (2022) underscore the importance of regulatory oversight in maintaining the integrity and security of UPI, especially in the face of evolving cyber threats.

Government Initiatives and Public Awareness

Government initiatives, such as the "Digital India" campaign, have promoted the adoption of UPI while simultaneously increasing awareness of its security features (Mehta, 2021). However, despite these efforts, Mehta's (2021) study suggests that continuous public education is necessary to keep users informed about potential risks and security practices.

Objective:

1. To Evaluate User Perceptions of UPI Security.

Research Methodology :

In this study, questionnaires were gathered from 400 participants residing in Pune City. The study specifically examined the usage of different online payment platforms including BHIM, Google Pay, MobiKwik, Paytm, PhonePe, and other similar interfaces.

Analysis for Perceived Security

Security remains a critical concern in both banking and UPI services. Despite the security measures provided by banks, the literature review indicates that users are still apprehensive about adopting UPI services due to fears of fraud and phishing. If UPI services are perceived as unsafe, users may be reluctant to use them.

Descriptive Analysis for Perceived Security

Statement	Strongly Agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Strongly Disagree (%)	Total (%)
Not required to share any kind of sensitive information	67.25% (269)	32.75% (131)	0% (0)	0% (0)	0% (0)	100% (400)
No one can tamper with UPI services	38.5% (154)	32.25% (129)	18% (72)	5.25% (21)	6% (24)	100% (400)
Advances in UPI technology make banking transactions safer	37% (148)	39.5% (158)	13.25% (53)	5.5% (22)	4.75% (19)	100% (400)
Money can be stolen during UPI transactions	34.25% (137)	30.75% (123)	17% (68)	10.5% (42)	7.5% (30)	100% (400)
If fraudsters get my OTP or PIN, I can lose my money	91% (364)	9% (36)	0% (0)	0% (0)	0% (0)	100% (400)
I am happy with the UPI services	54.5% (218)	33.5% (134)	4.75% (19)	4.25% (17)	3% (12)	100% (400)

Analysis

1. **Sensitive Information**: A significant majority of respondents (100%) agreed that UPI services do not require sharing sensitive information. Of these, 67.25% strongly agreed, while 32.75% agreed. No respondents were neutral, disagreed, or strongly disagreed.
2. **Tampering with UPI Services**: About 70.75% of respondents believed that UPI services cannot be tampered with. Specifically, 38.5% strongly agreed, and 32.25% agreed. However, 18% remained neutral, 5.25% disagreed, and 6% strongly disagreed.
3. **Advances in UPI Technology**: The belief that advances in UPI technology make banking transactions safer was supported by 76.5% of respondents. Of these, 37% strongly agreed, and 39.5% agreed. Meanwhile, 13.25% were neutral, 5.5% disagreed, and 4.75% strongly disagreed.
4. **Risk of Money Being Stolen**: Concerns about the potential for money to be stolen during UPI transactions were shared by 65% of respondents. Here, 34.25% strongly agreed, and 30.75% agreed. On the other hand, 17% were neutral, 10.5% disagreed, and 7.5% strongly disagreed.

5. **OTP or PIN Fraud**: All respondents (100%) agreed that if fraudsters obtain their OTP or PIN, they risk losing money. A substantial 91% strongly agreed with this statement, while 9% agreed.
6. **Satisfaction with UPI Services**: A majority of respondents (88%) expressed satisfaction with UPI services. Specifically, 54.5% strongly agreed, and 33.5% agreed. Only a small percentage of respondents were neutral (4.75%), disagreed (4.25%), or strongly disagreed (3%).

Implications

The analysis reveals that while there is strong confidence in the security features of UPI, there are still concerns, particularly regarding the potential for money theft during transactions and the risk associated with OTP or PIN fraud. These findings highlight the need for UPI service providers to continually update and enhance security measures to address user concerns and further build trust in digital payment systems.

Conclusion :

The analysis of user perceptions regarding the security of UPI services reveals a complex landscape of confidence and concern. A unanimous agreement among respondents indicates that UPI services are seen as secure in terms of not requiring the sharing of sensitive information, which reflects strong trust in the system's confidentiality. However, the perception of UPI's resistance to tampering is less unanimous, with a notable minority expressing uncertainty or concern. Similarly, while most users believe that advances in UPI technology have made transactions safer, a significant portion still harbors doubts. The potential for money to be stolen during transactions and the risks associated with OTP or PIN fraud remain prominent concerns, underscoring the vulnerabilities that users perceive in the system. Despite these issues, the overall satisfaction with UPI services is high, suggesting that while users recognize the risks, they continue to value the convenience and efficiency that UPI offers.

These findings emphasize the need for continuous improvement in UPI security measures. Addressing the specific concerns about transaction safety and OTP/PIN vulnerabilities is crucial for maintaining and enhancing user trust. As digital payment systems become increasingly integral to daily transactions, ensuring their security will be key to their sustained adoption and success. Therefore, UPI service providers must prioritize the ongoing development and implementation of advanced security protocols to protect users and bolster confidence in digital payments.

The security of UPI services is critical to the continued growth and adoption of digital payments in India. While UPI has robust security features, including 2FA, encryption, and VPAs, it faces ongoing challenges from phishing, SIM-swapping, and other cyber threats. Continued research and technological advancements are essential to address these challenges and ensure the security of UPI services in the future.

References :

1. Bhattacharya, A. (2022). Phishing Scams Targeting UPI Users: A Case Study. *Journal of Digital Security*, 15(2), 45-58.
2. Chandra, S., & Desai, R. (2021). Mobile Malware and its Impact on UPI Transactions. *International Journal of Cybersecurity*, 12(3), 201-214.
3. Chaturvedi, S. (2022). Security Features of Unified Payments Interface: An Overview. *Indian Journal of Financial Technology*, 8(1), 34-48.
4. Das, K., & Roy, M. (2022). Regulatory Framework for UPI Security: The Role of RBI and NPCI. *Banking and Financial Review*, 14(2), 120-135.
5. Gupta, P., & Sharma, R. (2021). The Role of Virtual Payment Address in Enhancing UPI Security. *Journal of Financial Innovation*, 9(4), 123-137.
6. Jain, A., & Gupta, N. (2022). Encryption Techniques in UPI Transactions: A Comparative Analysis. *Journal of Information Security*, 18(3), 89-102.
7. Kumar, P. (2021). Two-Factor Authentication in UPI: Enhancing Digital Payment Security. *Cybersecurity Insights*, 10(4), 67-78.
8. Mehta, R. (2021). Digital India and UPI: Promoting Secure Digital Payments. *Economic Policy Journal*, 22(3), 145-159.
9. Mishra, A., & Singh, V. (2022). The Evolution of Digital Payments in India: The Role of UPI. *Journal of Financial Technology*, 11(1), 56-73.
10. Mukherjee, S., & Singh, R. (2021). Challenges in UPI Security: An Overview. *Journal of Financial Security*, 9(2), 98-110.
11. NPCI. (2023). Monthly UPI Transaction Statistics. National Payments Corporation of India.
12. Natarajan, K., et al. (2021). Assessing the Security of UPI Transactions: The Role of Two-Factor Authentication. *Indian Journal of Digital Payments*, 7(2), 101-115.
13. Patel, R. (2021). UPI: A Game-Changer in India's Digital Economy. *Journal of Financial Inclusion*, 8(3), 74-88.
14. Rath, S. (2021). The Impact of UPI on Digital Payments in India: A Statistical Overview. *Journal of Economic Policy and Development*, 14(1), 43-59.

15. RBI. (2021). Guidelines for the Security of Digital Payment Systems in India. Reserve Bank of India.
16. Rao, M. (2022). Analyzing SIM-Swapping Fraud in UPI Transactions. *Cyber Law Journal*, 13(2), 158-174.
17. Roy, A., & Sengupta, P. (2023). Blockchain and UPI: Future Directions in Digital Payment Security. *Journal of Financial Innovation*, 10(2), 78-91.
18. Sarkar, S., & Jain, M. (2023). The Role of AI and ML in Enhancing UPI Security. *Journal of Emerging Technologies in Finance*, 12(3), 134-147.
19. Sharma, T. (2022). A Study on Encryption Techniques Used in UPI. *Journal of Information and Communication Technology*, 14(1), 56-69.
20. Singh, A., & Kumar, D. (2022). SIM-Swapping: A Threat to Mobile-Based UPI Security. *Journal of Financial Security*, 10(3), 91-105.
21. Verma, R., & Patel, K. (2022). Analyzing Mobile-Based Frauds in UPI: Challenges and Solutions. *International Journal of Digital Payments*, 9(4), 134-148.
22. Ministry of Electronics & IT. (2023, February 8). Digital Transactions in India. Press Information Bureau, Government of India. Retrieved from https://pib.gov.in/PressReleasePage.aspx?PRID=1897272
23. Reserve Bank of India, National Payments Corporation of India, & Banks. (2023). Growth of Digital Payments in India. Retrieved from https://pib.gov.in/PressReleasePage.aspx?PRID=1897272
24. Statista. (2023). Digital Payments - Worldwide. Retrieved from https://www.statista.com/statistics/296453/digital-payment-transaction-value-worldwide/