International Journal of Science, Strategic Management and Technology
Volume **02** Issue **08** August- **2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

A STUDY ON AN ANALYSIS OF CYBER RISKS IN DIGITAL FINANCE WITH A FOCUS ON UPI PAYMENTS

1. VENISHETTY SAIRAGHAVA (24UJ1E00P7) Student of 2nd Year MBA, Malla Reddy Engineering College and Management Sciences, Medchal, Hyderabad – 501 401.
2. T NIHARIKA REDDY, Assistant Professor, Dept of MBA in Malla Reddy Engineering College and Management Sciences, Medchal, Hyderabad – 501 401.

https://doi.org/10.55041/ijsmt.v2i8.084

Cite this Article: SAIRAGHAVA, V. & REDDY, T. N. (2026). A STUDY ON AN ANALYSIS OF CYBER RISKS IN DIGITAL FINANCE WITH A FOCUS ON UPI PAYMENTS. International Journal of Science, Strategic Management and Technology, *02*(8), 1-5. https://doi.org/10.55041/ijsmt.v2i8.084

ABSTRACT

The growth of digital finance has transformed financial transactions in India, with the Unified Payments Interface (UPI) becoming a widely used payment mechanism. However, increasing activity has also created exposure to phishing, fake applications, OTP fraud, QR scams, identity theft, malware, SIM swapping, and unauthorized access. This study examines cyber risks associated with UPI payments, users' cybersecurity awareness, security practices, and confidence in payment systems. Primary data from 100 UPI users were analysed using percentage analysis. Findings indicate that phishing is the leading reported threat, while awareness and security practices influence confidence. The study recommends stronger security measures and continuous user awareness.

Keywords: Unified Payments Interface (UPI), Cybersecurity, Digital Payment Security, Cyber Risks, Digital Finance

1. INTRODUCTION

Digital finance has changed the way financial services are accessed and delivered in India. Smartphones, internet connectivity, financial inclusion initiatives, and electronic payment facilities have enabled individuals and businesses to transfer money, pay bills, purchase products, and conduct banking activities without depending entirely on physical bank branches and conventional channels. Among the various digital payment mechanisms, the Unified Payments Interface (UPI) has emerged as an important platform because it supports instant, convenient, interoperable, and mobile-based transactions. UPI enables users to make person-to-person and person-to-merchant payments through mobile applications, virtual payment addresses, QR codes, and linked bank accounts. Its simplicity and speed have encouraged regular use among consumers and merchants. The uploaded study shows that UPI has become deeply integrated into everyday financial activities and that many respondents use it frequently. This expansion supports digital finance and financial inclusion, but it also increases the importance of cybersecurity and responsible user behaviour. Cyber risk refers to the possibility of financial loss, operational disruption, privacy violations, data theft, or reputational damage resulting from cyberattacks or unauthorized digital activity. UPI users may encounter phishing messages, fake applications, OTP fraud, QR-code scams, fraudulent customer-service calls, malware, SIM swapping, social engineering, and unauthorized account access. Human error and inadequate awareness can increase exposure because users may disclose OTPs, UPI PINs, passwords, or other confidential information. Financial institutions and payment providers employ measures such as encryption, multi-factor

authentication, biometric verification, transaction monitoring, artificial intelligence-based fraud detection, and behavioural analytics. Regulatory and institutional bodies also promote security standards, customer awareness, and grievance redressal. Nevertheless, technology alone cannot eliminate cyber risks. Safe digital behaviour, continuous user education, and timely fraud reporting remain essential. The present study therefore focuses specifically on cyber risks in digital finance with reference to UPI payments. It examines the major threats faced by users, their awareness of cybersecurity, security practices, and confidence in UPI after security awareness. The study also identifies practical measures that can strengthen transaction security. By understanding both technological and behavioural dimensions of cyber risk, the study seeks to support safer UPI usage and greater confidence in India's expanding digital financial ecosystem. The source report similarly explains UPI's convenience and rapid adoption and identifies phishing, QR-code fraud, identity theft, malware, SIM swapping, and unauthorized access as major concerns.

2. REVIEW OF LITERATURE

Sharma and Gupta (2021) examined the expansion of digital payments in India and reported that greater smartphone adoption, internet connectivity, and government initiatives increased digital payment usage, while cyber risks such as identity theft and phishing also increased. Kumar and Singh (2020) studied cybersecurity safeguards in Indian banks and emphasized encryption, biometric authentication, artificial intelligence, and fraud monitoring, while noting the importance of addressing human error. Patel and Mehta (2022) investigated customer awareness of UPI fraud and found gaps concerning OTP sharing, QR-code scams, fake customer-service calls, and malicious applications. Verma and Joshi (2022) reported that cybersecurity awareness, security alerts, and grievance redressal strengthen customer confidence in digital payments. Bhatia and Arora (2021) highlighted the role of RBI, NPCI, and CERT-In in strengthening digital-payment security and recommended continuous regulatory improvement. Rao and Nair (2023) identified phishing, fraudulent payment requests, remote-access applications, SIM swapping, and social engineering as important UPI-related threats. Reddy and Thomas (2024) emphasized artificial intelligence, tokenization, blockchain, biometric authentication, and real-time monitoring, while stressing continuous technological development. These studies support the present investigation of user awareness and practical security behaviour. effectively.

3. OBJECTIVES OF THE STUDY

1. **To determine** the main cyber threats connected to digital payment transactions using UPI.
2. **To assess** consumers' knowledge of cybersecurity procedures in UPI payments.
3. **To assess** how well banks, fintech firms, and government agencies' security measures work to prevent cybercrime.
4. **To examine** how users' trust and uptake of digital finance services are affected by cyber hazards.
5. **To make** appropriate recommendations for improving cybersecurity and guaranteeing secure UPI transactions.

4. RESEARCH METHODOLOGY

A descriptive research design was adopted to study cyber risks in UPI payments. Primary data were collected through a structured questionnaire from 100 UPI users selected using convenience sampling. Secondary information was obtained from RBI publications, official websites, and related sources. Percentage analysis was used to summarize and interpret responses.

The source specifies descriptive research, primary and secondary data, convenience sampling, 100 respondents, and a structured questionnaire.

4.1 STATISTICAL TOOL

Percentage Analysis

Percentage analysis is selected as the primary statistical tool because the study mainly analyses categorical responses relating to cybersecurity awareness, cyber threats, and security practices.

The study used percentage analysis along with other tools; for this concise report, percentage analysis is the most appropriate tool for presenting the three selected categorical tables.

5. DATA ANALYSIS AND INTERPRETATION

Table 5.1: Awareness of Cyber Threats in UPI Transactions

Category	Respondents	Percentage
Highly Aware	24	24%
Aware	46	46%
Neutral	16	16%
Less Aware	8	8%
Not Aware	6	6%
Total	**100**	**100%**

Analysis: The highest response is recorded for the **Aware** category, with 46 respondents representing 46%.

Interpretation: Most respondents demonstrate awareness of cyber threats associated with UPI transactions. When highly aware and aware respondents are combined, **70%** of respondents show awareness of cyber risks.

Table 5.2: Major Cyber Threat Faced

Cyber Threat	Respondents	Percentage
Phishing	34	34%
Fake Apps	22	22%
OTP Fraud	18	18%
QR Scam	16	16%
Others	10	10%
Total	**100**	**100%**

Analysis: Phishing records the highest response, with 34 respondents representing 34%.

Interpretation: Phishing is the most commonly reported cyber threat among the respondents. Fake applications, OTP fraud, and QR scams are other significant threats experienced by UPI users.

Table 5.3: Security Practices Used in UPI Transactions

Security Practice	Respondents	Percentage
Protect OTP/PIN	36	36%
Two-Factor Authentication	24	24%
Regular Updates	18	18%
Avoid Public Wi-Fi	12	12%
Others	10	10%
Total	**100**	**100%**

Analysis: Protecting OTPs and UPI PINs has the highest response, with 36 respondents representing 36%.

Interpretation: Protecting confidential authentication information is the most commonly followed security practice. However, the lower percentages for regular updates and avoiding public Wi-Fi indicate scope for stronger cybersecurity awareness among users.

6. RESULTS

1. UPI has become an important and widely used digital payment mechanism because of its speed, convenience, and simplicity.
2. Most respondents use UPI regularly for financial transactions.
3. **70% of respondents are either highly aware or aware of cyber threats** associated with UPI.
4. **Phishing is the leading cyber threat**, accounting for 34% of responses.
5. Fake applications constitute the second-highest reported cyber threat at 22%.
6. OTP fraud and QR scams also represent significant security concerns.
7. Protecting OTPs and UPI PINs is the most commonly adopted security practice, at 36%.
8. Two-factor authentication is used by 24% of respondents.
9. The findings indicate that cybersecurity awareness is important for safer UPI usage.
10. The study indicates that banks and financial institutions have an important role in providing cybersecurity information and awareness.
11. Security awareness contributes to greater confidence in using UPI-based digital financial services.
12. Respondents emphasize stronger security measures and awareness campaigns to reduce cyber risks.

7. SUGGESTIONS

1. Banks and UPI service providers should conduct **regular cybersecurity awareness campaigns**.
2. Users should never disclose UPI PINs, OTPs, passwords, or other confidential banking information.
3. Banks should strengthen real-time fraud detection and transaction monitoring systems.
4. Users should carefully verify payment requests, QR codes, links, and recipient details before completing transactions.
5. Two-factor and multi-factor authentication should be promoted wherever available.
6. Users should regularly update banking and UPI applications to reduce security vulnerabilities.
7. Financial institutions should provide immediate alerts for suspicious or unusual transactions.
8. Customers should avoid using unsecured public Wi-Fi networks for sensitive financial transactions.
9. Banks, fintech companies, regulators, and law-enforcement agencies should strengthen cooperation against emerging cyber fraud.
10. Regulatory bodies should continuously update cybersecurity requirements according to changing cyber threats.
11. Digital payment platforms should improve customer support and rapid grievance-redressal mechanisms.
12. Continuous cybersecurity education should be provided because technology-based controls alone cannot completely eliminate human-related cyber risks.

8. CONCLUSION

The study concludes that the rapid expansion of UPI has improved the speed, convenience, and accessibility of digital financial transactions in India, but it has simultaneously increased exposure to cyber risks. The findings show that users are generally aware of cyber threats, with 70% of respondents classified as highly aware or aware. Phishing is identified as the most common reported threat, followed by fake applications, OTP fraud, and QR scams. The study also shows that users adopt several protective practices, particularly safeguarding OTPs and UPI PINs. However, the relatively lower adoption of other security practices indicates the need for continuous cybersecurity education. Banks, fintech companies, regulators, and users all have important responsibilities in maintaining secure digital payment systems. Financial institutions should strengthen fraud detection, transaction monitoring, authentication, customer alerts, and grievance-redressal mechanisms, while users should follow safe digital payment practices. Regulatory institutions should continue updating security standards to address emerging threats. Overall, effective UPI security requires a combination of advanced technology, regulatory supervision, institutional responsibility, and informed user behaviour. Strengthening these areas can reduce cyber risks, improve consumer

confidence, and support the sustainable growth of digital finance in India. The study therefore emphasizes that cybersecurity should remain a continuous priority as UPI usage and India's digital financial ecosystem continue to expand.

9. REFERENCES

1. Bhatia, R., & Arora, S. (2021). *Cybersecurity and regulatory measures in India's digital payment ecosystem*.
2. Kumar, R., & Singh, A. (2020). *Cybersecurity safeguards for digital payment systems in Indian banks*.
3. Patel, M., & Mehta, R. (2022). *Customer awareness of cyber fraud in UPI transactions*.
4. Rao, S., & Nair, P. (2023). *Cyber fraud trends in digital payment platforms with reference to UPI transactions*.
5. Reddy, V., & Thomas, K. (2024). *Cyber risk management in India's digital banking ecosystem*.
6. Reserve Bank of India. (2021). *Master direction on digital payment security controls*. RBI.
7. Reserve Bank of India. (2024). *Master directions on cyber resilience and digital payment security controls for non-bank payment system operators*. RBI.
8. National Payments Corporation of India. (2024, November 6). *NPCI unveils UPI safety awareness campaign to champion safe digital payment practices*. NPCI.
9. Indian Computer Emergency Response Team. (2024). *Digital threat report 2024*. CERT-In. (
10. Sharma, A., & Gupta, P. (2021). *Expansion of digital payment systems in India following the launch of UPI*.
11. Verma, S., & Joshi, A. (2022). *Cybersecurity awareness and consumer trust in digital finance*.