 ISSN-2581-8953

DIGITAL PAYMENT FRAUD: EMERGING THREATS AND MITIGATION STRATEGIES

Ms. Prerana Bhatnagar[1] and Mr. Amit Singhal[2]

[1]Assistant Professor, Indirapuram Institute of Higher Studies, Ghaziabad, Uttar Pradesh-201014

[2]Associate Professor, Monad University, Hapur, Uttar Pradesh 245304

ABSTRACT

The rapid expansion of the internet in recent years has significantly boosted the adoption of digital payments in India. With the rise of e-commerce and online transactions, various digital payment systems have been developed and widely adopted. However, this growth has also led to an increase in digital payment fraud, posing a major challenge to the financial ecosystem. As digital transactions become more prevalent, fraudsters continue to devise sophisticated techniques to exploit vulnerabilities. For businesses and financial institutions, managing fraud has become a critical concern, leading to substantial financial losses. This paper provides an overview of digital payment fraud in the Indian context, highlighting key fraud trends, their impact on revenue loss, and statistical insights. It also discusses various fraud detection and prevention measures, including security frameworks and regulatory initiatives implemented to safeguard digital transactions. The primary objective of this research is to reduce fraud in digital payments and mitigate financial losses by implementing effective detection and prevention strategies.

Keywords: *Digital Payment System, Digital Payment Frauds, Multifactor Authentication, Cybersecurity*

1. INTRODUCTION

In the current digital age, countries across the globe are striving to advance technologically to foster comprehensive development. Among them, India has made remarkable progress in digital transformation, especially in the area of digital payments. According to the Report on Currency and Finance (2024), India leads the world in real-time digital payment transactions, contributing to nearly 48.5% of global volume, ahead of Brazil and China. The rapid expansion of digital payment systems has significantly altered the way individuals and businesses conduct financial transactions. Services like online banking, mobile payment apps, and digital wallets have made financial operations more accessible and user-friendly.

However, this technological advancement is accompanied by a troubling rise in digital payment frauds, largely due to the unregulated circulation of sensitive personal information across open databases. This growing risk

 ISSN-2581-8953

poses serious challenges to both users and financial institutions. The volume and complexity of fraud have increased over time, testing existing cybersecurity frameworks and creating new vulnerabilities for exploitation. Digital payment fraud typically involves unauthorized access to someone's payment credentials to complete illicit transactions. The widespread adoption of digital payment platforms has made it easier for fraudsters to exploit unsuspecting users. While technology is meant to simplify lives, it has also become a double-edged sword—where its misuse has led to an increase in cybercrime. Unified Payment Interface (UPI) applications link multiple financial instruments—debit cards, credit cards, and bank accounts—with mobile numbers and wallets, streamlining the transaction process. However, this convenience can be misused by cybercriminals who can launch fraudulent attacks through phishing links or fake calls asking for OTPs

1.1. PHISHING

Phishing is a fraudulent attempt where an attacker poses as a credible entity or individual, often through email or other communication channels. The attacker typically sends malicious links or attachments intended to steal the user's money, personal identity, or data. On August 24, 2022, a 45-year-old woman from Ahmedabad lost ₹4 lakh in a phishing attack after receiving a message instructing her to click a hyperlink to update her "suspended" bank account. Upon entering her credentials and OTP, she received notifications confirming the withdrawal of funds from her account.

1.2. VISHING

Vishing, or voice phishing, involves fraudulent calls made by scammers who impersonate legitimate representatives to extract sensitive information. These calls might be live or automated, often warning of fake issues with the recipient's bank account and requesting personal banking credentials to "resolve" them. In July 2018, a 59-year-old retired official in Mumbai received a call from someone posing as a government official and lost nearly ₹70,000 after sharing his credit card information and OTPs.

2. REVIEW OF LITERATURE

Sanjeev T. A. et al. cite start aimed to assess the awareness levels of banking customers regarding electronic banking frauds in Kerala. Using a descriptive research methodology, the study found that convenience, accessibility, authentication, and connectivity influence the use of internet banking. They recommended further research into the financial and market mechanisms that facilitate fraud.

 ISSN-2581-8953

Ray K. P. (https://www.google.com/search?q=2023) examined the prevalence of cyber financial crimes in Jamtara, Jharkhand, focusing on the tools used by fraudsters and the challenges faced by investigators. Using a survey-based method, the research highlighted challenges such as ambiguous jurisdiction and a lack of trained personnel. The author emphasized the need for enhanced jurisdictional clarity and specialized training for police officers.

Ruangmei T. & Gethe R. (https://www.google.com/search?q=2023) explored vulnerabilities in digital transactions and examined consumer perceptions and trust regarding online fraud. The study concluded that while digital payments have enhanced security and convenience, user vigilance is crucial for maintaining a safe payment environment.

3. OBJECTIVES OF THE STUDY

- To investigate and analyze the root causes responsible for the increase in digital payment frauds.
- To explore and evaluate effective preventive and corrective measures to address issues related to digital payment fraud.
- To examine the role of government policies, initiatives, and regulations in mitigating digital payment fraud in India.

4. HYPOTHESIS

- **H01:** There is no significant difference in how respondents rank different measures for preventing digital payment fraud.
- **HA1:** There is a significant difference in how respondents rank different measures for preventing digital payment fraud.

5. RESEARCH METHODOLOGY

This research is empirical and analytical in nature, using both primary and secondary data. Primary data was collected from 280 responses to a structured questionnaire in Ghaziabad district from December 2024 to January 2025 using a random sampling method. Secondary data was gathered from websites like the RBI and NPCI. The collected data was analyzed using simple average, Mann-Whitney U test, and Friedman test via SPSS.

 ISSN-2581-8953

6. DATA ANALYSIS AND INTERPRETATION

6.1. DEMOGRAPHIC PROFILE

The study collected 280 responses from Ghaziabad district. The gender distribution was 52.8% male and 47.2% female. The majority of respondents (49.2%) were aged 26 to 35. Most respondents held a postgraduate degree (61.6%). Students were the largest occupational group (44%), and 70% of respondents resided in urban areas.

6.2. ANALYTICAL FRAMEWORK

For analysis, the responses were divided into two sections. The first section identifies the causes of digital payment fraud and compares perceptions between victims and non-victims. Out of 250 valid responses, 118 were victims and 132 were non-victims. Six major causes were identified: Financial Illiteracy, Low Awareness, Cyber Security Issues, Technology Complexity, Operational Changes, and Slow Investigation. This data was analyzed using the Mann-Whitney U test. The second section identifies suitable measures to resolve digital payment issues, analyzed using the Friedman rank test.

6.3. NORMALITY TEST

A normality test was conducted on all dependent variables, and both the Kolmogorov-Smirnov and Shapiro-Wilk tests were applied. The results showed that all variables significantly deviate from a normal distribution (p < 0.001). Due to this violation of normality, non-parametric tests like the Friedman Test were deemed appropriate for the analysis.

7. RESULTS AND FINDINGS

The study reveals a significant rise in digital payment fraud in India. The monetary value of these frauds increased from ₹129 crore in 2020 to ₹1,457 crore in 2024, with reported incidents growing from 2,667 to 29,082 in the same period. Common fraud types include Card Not Present (CNP) fraud and modern methods like phishing and vishing. The analysis shows that awareness and education are considered the most effective prevention measures, followed by strict regulations and security intelligence. Technologies like sound wave authentication are seen as less effective, possibly due to low familiarity. Government initiatives such as Strong Customer Authentication (SCA) and data protection laws have helped, but further enhancements like consumer financial literacy programs and investment in AI-based fraud detection are needed.

 ISSN-2581-8953

8. DISCUSSION

The research highlights a critical shift where traditional large-scale financial frauds are declining, while digital payment-related frauds are escalating at an alarming rate. Between 2020 and 2024, the number of digital fraud incidents in India skyrocketed from 2,677 to 29,082. This surge underscores an urgent need for stronger cybersecurity and regulatory oversight.

A key finding is that users perceive education and awareness as the most critical components in combating fraud, ranking them higher than specific technological solutions. This suggests that while security measures like two-factor authentication are important, they are not sufficient if users are not equipped with the knowledge to identify and avoid threats. The lower ranking of newer technologies like network tokenization indicates a gap in user adoption and trust, likely due to limited awareness.

Government interventions like SCA and data protection laws have laid a necessary foundation. However, the escalating fraud statistics prove that a more dynamic, multi-stakeholder approach is essential. This requires collaboration between government, financial institutions, and users to create a secure and resilient digital payment ecosystem.

9. SUGGESTIONS

To effectively combat digital payment fraud, the following interventions are recommended:

- **ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR REAL-TIME FRAUD DETECTION:**
  - Deploy advanced AI and ML models to analyze transaction data in real time, detecting anomalies based on historical fraud patterns.
  - Implement behavioral biometrics that monitor user-specific actions like typing speed and mouse dynamics for a non-intrusive layer of security.
- **ENHANCED TOKENIZATION AND ENCRYPTION TECHNOLOGIES:**
  - Use dynamic, single-use tokens for transactions to minimize the risk of credential theft.
  - Ensure end-to-end encryption of payment data to protect it from interception.

- **MULTI-FACTOR AUTHENTICATION (MFA) USING ADVANCED METHODS:**
  - Introduce context-aware MFA that evaluates transaction parameters like device and location before requiring authentication.
  - Strengthen MFA by integrating multiple biometric identifiers such as fingerprints, facial scans, and voice recognition.

- **ADOPTION OF ZERO TRUST SECURITY ARCHITECTURE:**
  - Implement a Zero Trust framework that requires continuous verification of all users and devices, reducing risks from insider threats.
  - Use micro-segmentation to divide networks into distinct zones, preventing the lateral movement of cyber threats.

10. CONCLUSION

The surge in digital payment usage in India has brought an alarming rise in digital payment fraud. The value of these frauds grew from ₹129 crore in 2020 to ₹1,457 crore in 2024, with reported cases increasing more than tenfold. This highlights an urgent need to address vulnerabilities in the ecosystem. Key factors contributing to this problem include financial illiteracy, low public awareness, and cybersecurity weaknesses. The most effective preventive strategies identified are awareness and education, followed by strong regulations. While technologies like two-factor authentication are valuable, they are not sufficient on their own. Government initiatives have contributed to resilience, but more proactive efforts, including investment in AI and machine learning, are needed. Ultimately, securing the digital payment landscape demands a coordinated effort from government, financial institutions, and consumers to ensure a trustworthy transaction environment.

11. REFERENCES

Akintoye, K. A., & Araoye, O. I. (2011). Combating e-fraud on electronic payment system. *International Journal of Computer Applications, 25*(8), 48-53.

Anas, S., Banarasi, A. B., Yadav, J., Kumar, S., Bhimrao, D. B., Srivastava, S. P., Anas Ansar, S., Kumar Dwivedi, S., Pandey, A., Ishrat, M., Khan, W., Pandey, D., Khan, R. A., & Khan, M. W. (2021). A critical analysis

 ISSN-2581-8953

of fraud cases on the internet. *Turkish Journal of Computer and Mathematics Education, 12*(1). https://www.researchgate.net/publication/352157135

Chatterjee, A. (2021). Analysis of financial frauds in electronic payment systems in India and China. *Turkish Online Journal of Qualitative Inquiry (TOJQI), 12*(7).

Chichwadia, A. E., & Mpekoa, N. (2024). Detecting smishing and vishing attacks using machine learning. *International Journal of Intelligent Computing Research (IJICR)*.

DeSantis, M., Dougherty, C., & McDowell, M. (2011). *Understanding and protecting yourself against money mules*. United States Computer Emergency Readiness Team.

Eneeji, S., Udie, M., Eyong, W., & Chimdike, K. (2019). A study of electronic banking fraud, fraud detection, and control. *International Journal of Innovative Science and Research Technology, 4*(3).

Fernandes, L. (2013). Fraud in electronic payment transactions: Threats and countermeasures. *Asia Pacific Journal of Marketing & Management Review, 2*(3), ISSN 2319-2836.

Folami, R. A., Yinusa, G. O., & Toriola, A. K. (2024). Digital payment fraud and bank fragility.

Ruangmei, T., & Gethe, R. (https://www.google.com/search?q=2023). A study on modes of digital payment system, analysis of frauds occurring through digital payment systems. *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/irjmets42773