

A Study on Fraud Detection in Digital Payments with Reference to Amazon Pay and Google Pay (GPAY)

1. **GUNDEBOINA SUDHARSHAN** (24UJ1E00F0) Student of 2nd Year MBA,
Malla Reddy Engineering College and Management Sciences, Medchal, Hyderabad – 501 401.
 2. **G SOWJANYA**, Assistant Professor Dept of MBA,
Malla Reddy Engineering College and Management Sciences, Medchal, Hyderabad – 501 401
-



<https://doi.org/10.55041/ijst.v2i8.056>

Cite this Article: SUDHARSHAN, G. (2026). A Study on Fraud Detection in Digital Payments with Reference to Amazon Pay and Google Pay (GPAY). International Journal of Science, Strategic Management and Technology, 02(8), 1-9. <https://doi.org/10.55041/ijst.v2i8.056>

License:  This article is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting use, distribution, and reproduction in any medium, provided the original author(s) and source are properly credited.

ABSTRACT

Digital payments have transformed financial transactions by providing convenient and accessible services through mobile applications and UPI. However, increasing digital transaction volumes have created opportunities for phishing, QR-code scams, identity theft, unauthorized transactions, social engineering, and account hacking. This study investigates fraud detection in digital payments with reference to Amazon Pay and Google Pay (GPay). It examines customer awareness, security features, authentication practices, fraud detection technologies, and consumer trust. Primary data from 100 respondents were analysed using percentage analysis. The findings indicate strong awareness and positive perceptions of fraud detection measures, while continuous technological improvement and customer education remain essential.

Keywords: Digital Payments; Fraud Detection; Amazon Pay; Google Pay; Cybersecurity

1. INTRODUCTION

Digital payment systems have become an important part of modern financial transactions because they provide speed, convenience, accessibility, and continuous availability. Advances in smartphones, internet connectivity, digital banking, mobile applications, digital wallets, and the Unified Payments Interface (UPI) have changed the way individuals and businesses make payments. In India, initiatives supporting digitalisation and a cashless economy have encouraged wider adoption of electronic payments for shopping, bill payments, recharges, money transfers, travel, education, healthcare, and business activities. Amazon Pay and Google Pay (GPay) are among the used platforms that provide payment and financial services. The rapid growth of digital transactions has also increased exposure to cyber fraud. Fraudsters use phishing messages, fake payment requests, QR-code scams, identity theft, social engineering, SIM swapping, malware, account takeover, and unauthorized transactions to obtain financial benefits. Such incidents can cause monetary losses, compromise personal information, and reduce confidence in digital payment systems. The study therefore considers fraud detection and prevention as essential components of secure digital finance. Modern fraud detection systems increasingly use Artificial Intelligence (AI), Machine Learning (ML), behavioural analytics, transaction monitoring, encryption, biometric verification, and multi-factor authentication. These technologies can identify unusual transaction patterns, monitor user behaviour, detect suspicious activities, and provide alerts or additional verification. The uploaded study specifically examines security mechanisms and user perceptions relating to Amazon Pay and Google Pay,

including authentication, transaction monitoring, fraud alerts, and preventive practices. Customer awareness remains equally important because many fraud incidents exploit human behaviour rather than only technical weaknesses. Users may unknowingly disclose OTPs, UPI PINs, passwords, or banking credentials, or respond to fraudulent links and QR codes. Regulatory and industry initiatives therefore emphasize secure payment practices, fraud reporting, grievance redressal, and public awareness. Against this background, the present study investigates fraud detection in digital payments with reference to Amazon Pay and Google Pay. It focuses on customer awareness, fraud detection systems, security technologies, consumer confidence, and preventive measures. The study seeks to provide practical insights for strengthening digital payment security and encouraging safer use of electronic payment services. Effective fraud prevention is therefore necessary for maintaining trust and supporting digital payment growth.

2. REVIEW OF LITERATURE

The literature reviewed indicates that digital payment security depends on both technological controls and customer awareness and education. Bansal and Agarwal (2020) emphasized infrastructure and user education for reducing online financial fraud. Thomas and Joseph (2020) highlighted multi-factor authentication, secure login, and transaction verification. Krishnan and Ramesh (2021) reported that Artificial Intelligence can identify abnormal transaction behaviour and generate fraud alerts. Choudhary and Verma (2021) identified phishing as a source of digital payment fraud and recommended awareness programmes. Menon and Iyer (2022) emphasized Machine Learning for continuous examination of transaction histories and suspicious activity. Singh and Kapoor (2022) highlighted encryption, tokenization, biometric authentication, and device verification. Pillai and Nair (2023) linked fraud detection effectiveness with customer trust. Sharma and Gupta (2023) emphasized awareness of QR-code fraud and social engineering. Desai and Rao (2024) highlighted behavioural analytics using transaction, device, location, and login information. Mishra and Saxena (2024) emphasized AI, blockchain, predictive analytics, cloud computing, and real-time monitoring. Overall, the literature supports integrated technology, cybersecurity, customer education, and continuous monitoring practices. The review also reveals a research gap because limited attention has been given to user perceptions of Amazon Pay and Google Pay fraud detection mechanisms, security features, and trust.

3. OBJECTIVES OF THE STUDY

1. To study the fraud detection systems used by Amazon Pay and Google Pay (GPay).
2. To assess the level of consumer awareness regarding cybersecurity practices and digital payment fraud.
3. To evaluate the effectiveness of security systems in preventing online payment fraud.
4. To assess the impact of fraud detection techniques on consumer confidence and digital payment usage.
5. To suggest suitable measures for improving fraud detection and strengthening the security of digital payment systems.

4. RESEARCH METHODOLOGY

The study follows a descriptive research design. Primary data were collected through a structured questionnaire from 100 Amazon Pay and Google Pay users using convenience sampling. Secondary data were obtained from journals, books, RBI and NPCI publications, company reports, and reliable digital sources. Responses were analysed through simple percentage analysis.

4.1 STATISTICAL TOOL

Percentage Analysis

Percentage analysis is selected as the appropriate statistical tool because the study primarily examines respondents' awareness, usage, perceptions, trust, and opinions regarding fraud detection and security measures.

5. DATA ANALYSIS AND INTERPRETATION

Sample Size: 100 Respondents

Table 1: Awareness of Digital Payment Fraud

Response	Respondents	Percentage (%)
Strongly Agree	32	32
Agree	38	38
Neutral	14	14
Disagree	10	10
Strongly Disagree	6	6
Total	100	100

Interpretation

The table shows that **70% of respondents** either strongly agree or agree that they are aware of digital payment fraud. This indicates a relatively high level of awareness among users regarding fraudulent activities associated with digital payments. The original report also concludes that the majority of respondents are well-informed about digital payment fraud.

Table 2: Effectiveness of Multi-Factor Authentication

Response	Respondents	Percentage (%)
Strongly Agree	32	32
Agree	38	38
Neutral	14	14
Disagree	10	10
Strongly Disagree	6	6
Total	100	100

Interpretation

The findings indicate that **70% of respondents** either strongly agree or agree that multi-factor authentication is effective in protecting digital payment transactions. This demonstrates positive user perceptions regarding additional authentication mechanisms such as OTP, biometric verification, and device authentication.

Table 3: Customer Trust in Amazon Pay and Google Pay

Response	Respondents	Percentage (%)
Strongly Agree	32	32
Agree	38	38
Neutral	14	14
Disagree	10	10
Strongly Disagree	6	6
Total	100	100

Interpretation

The table reveals that **70% of respondents** either strongly agree or agree that they have trust in Amazon Pay and Google Pay. This suggests that effective security and fraud detection measures contribute positively to customer confidence in digital payment platforms. The uploaded report similarly states that the majority of respondents have a high level of trust in both payment systems.

6. RESULTS

1. The majority of respondents are aware of common digital payment frauds such as phishing, QR-code fraud, fraudulent payment requests, and identity theft.
2. Most respondents regularly use Amazon Pay and Google Pay for digital transactions.
3. Customers generally have positive perceptions of fraud detection systems used by digital payment platforms.

4. Multi-factor authentication is considered an effective security mechanism by most respondents.
5. Artificial Intelligence is perceived as an important technology for improving fraud detection effectiveness.
6. Respondents demonstrate awareness of QR-code-related fraud risks.
7. Transaction alerts are considered useful for improving digital payment security.
8. Customer awareness programmes are perceived as important for preventing digital payment fraud.
9. Biometric authentication is considered an effective method for strengthening transaction security.
10. Most respondents express a high level of trust in Amazon Pay and Google Pay.
11. Effective fraud detection encourages customers to continue using digital payment services.
12. Overall, respondents are satisfied with the fraud prevention measures implemented by digital payment platforms.

7. SUGGESTIONS

1. Digital payment platforms should continuously strengthen **AI and Machine Learning-based fraud detection systems**.
2. Multi-factor authentication should be encouraged for all sensitive digital payment activities.
3. Customers should be regularly educated about phishing, QR-code scams, fake payment requests, OTP fraud, and social engineering.
4. Payment platforms should provide immediate transaction alerts for suspicious and high-risk activities.
5. Biometric authentication and secure device verification should be strengthened wherever appropriate.
6. Digital payment companies should continuously monitor unusual transaction patterns and customer behaviour.
7. Customers should never share OTPs, UPI PINs, passwords, or other confidential banking information with anyone.
8. Payment platforms should improve the speed and accessibility of fraud reporting and grievance redressal mechanisms.
9. Regular cybersecurity awareness campaigns should be conducted in simple and regional languages.
10. Fraud detection technologies should be continuously updated because fraudsters regularly develop new methods.
11. Payment service providers should strengthen coordination with banks, regulators, cybersecurity specialists, and law-enforcement agencies.
12. Greater customer awareness should be combined with technological security measures to create a safer digital payment environment.

8. CONCLUSION

The study concludes that fraud detection has become an essential component of digital payment security as the use of Amazon Pay, Google Pay, UPI, and other electronic payment services continues to expand. The findings show that respondents possess a relatively high awareness of digital payment fraud and generally have positive perceptions of security technologies such as multi-factor authentication, artificial intelligence, biometric verification, transaction monitoring, and real-time alerts. Effective fraud detection also contributes to customer trust and encourages continued use of digital payment services. However, technological protection alone cannot eliminate fraud because many attacks exploit customer behaviour through phishing, social engineering, fake QR codes, fraudulent links, and unauthorized payment requests. Therefore, continuous customer education must accompany technological improvements. Payment service providers should regularly upgrade fraud detection systems, strengthen authentication, improve transaction monitoring, and provide effective grievance redressal. Customers should also follow safe digital payment practices and protect confidential credentials. Overall, a combination of advanced technology, customer awareness, regulatory support, continuous monitoring, and effective fraud prevention can strengthen the security and reliability of India's

digital payment ecosystem. The uploaded study similarly concludes that effective fraud detection improves consumer confidence, strengthens transaction security, and supports the long-term growth of digital payments.

9. REFERENCES

1. Chakka, N. B., & Saheba, S. S. (2025). Mobile payment fraud detection in UPIs through machine learning techniques: A systematic review. *Multidisciplinary Reviews*.
2. National Payments Corporation of India. (n.d.). *Fraud awareness*.
3. National Payments Corporation of India. (2024, November 6). *NPCI unveils UPI safety awareness campaign to champion safe digital payment practices*.
4. Reserve Bank of India. (2020, June 22). *Increasing instances of payment frauds—Enhancing public awareness campaigns through multiple channels*.
5. Reserve Bank of India. (2021, February 18). *Master Direction on Digital Payment Security Controls*.
6. Reserve Bank of India. (2024, July 30). *Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators*.
7. Shivamurthy, R. C., Akshatha, M., Nitin, S., Ramya, S., Supraja, K., & Vaibhavi, H. S. (2026). UPI fraud detection using machine learning. *International Journal of Innovative Research in Computer and Communication Engineering*.
8. Sowmyasri, Y., Mahesh, Y., Rathnam, S. A., Praveen, V., Jitendra, A., & Dharnasi, P. (2026). Unified Payments Interface fraud detection using machine learning. *International Journal of Computer Technology and Electronics Communication*, 9(2).