InSight Bulletin: A Multidisciplinary Interlink International Research Journal
Peer Reviewed International, Open Access Journal.
ISSN : 3065-7857 / Website: https://ibrj.us / Volume-3, Issue-1 / January - 2026

Original Article

A Study on Customer Perception of AI-enabled Fraud Detection in Digital Payment Systems

Divya Bhandary[1], Tarkeshwar Pandey[2]
[1]Assistant Professor, Department of Management
ATSS College of Business Studies and Computer Applications, Chinchwad
[2]Student Department of Management
ATSS College of Business Studies and Computer Applications, Chinchwad

Manuscript ID:
IBMIIRJ -2026-030113

Submitted: 07 Dec. 2025

Revised: 11 Dec. 2025

Accepted: 06 Jan. 2026

Published: 31 Jan. 2026

ISSN: 3065-7857

Volume-3

Issue-1

Pp. 64-68

January 2026

Correspondence Address:
Divya Bhandary,
Assistant Professor, Department of ManagementATSS College of Business Studies and Computer Applications, Chinchwad
Email:
divya.p.bhandary@gmail.com

OPEN ACCESS

Quick Response Code:

Web. https://ibrj.us

DOI: 10.5281/zenodo.18949495

DOI Link:
https://doi.org/10.5281/zenodo.18949495

Abstract

The swift growth of digital payments in India has revolutionized the country's financial landscape, providing millions of consumers with accessibility, speed, and convenience. The complexity and frequency of fraudulent operations, which range from identity theft and illegal transactions to phishing and data breaches, have expanded concurrently with this advancement. Financial institutions are depending more and more on Artificial Intelligence (AI)-enabled fraud detection systems that employ machine learning, predictive analytics, and behavioral modeling to spot abnormalities in real time in order to counter these changing threats. This study investigates customer perceptions of AI-enabled fraud detection in digital payment systems through secondary data collected from credible sources such as the Reserve Bank of India (RBI), the National Payments Corporation of India (NPCI), and reports by PwC and McKinsey (2023–2025). The findings indicate that while awareness and trust in AI-driven systems are growing, gaps remain among rural users and older demographics. Data visualization and correlation analysis reveal a strong positive association (r = 0.89) between awareness and perceived trust in AI tools. The results highlight that increasing transparency, data privacy assurances, and customer education initiatives are essential to improve user confidence and adoption of AI-based fraud detection. Overall, the study emphasizes AI's transformative potential in fostering safer, more resilient, and user-centric digital payment ecosystems in India.

Keywords: *Artificial Intelligence (AI), Fraud Detection, Digital Payment Systems, Customer Perception, Financial Technology (FinTech), Machine Learning, Cybersecurity, Trust and Transparency..*

Introduction

India's digital payment revolution represents one of the most significant transformations in its financial history. Over the last decade, government initiatives such as *Digital India* and innovations like the Unified Payments Interface (UPI), Bharat Interface for Money (BHIM), and various fintech apps have reshaped how individuals and businesses transact. The convenience of real-time payments, minimal transaction costs, and mobile accessibility has led to exponential growth in the volume of digital transactions—rising from a few million in 2016 to over 18 billion monthly transactions in 2025 (RBI, 2025). However, this rapid digitization has also brought about a surge in cyber threats and frauds. Common fraudulent activities include phishing scams, fake UPI links, SIM swapping, and misuse of personal data. Such threats have raised critical questions about the security and trustworthiness of digital platforms. To address these challenges, financial institutions and fintech companies have turned to Artificial Intelligence (AI) technologies that can detect, predict, and prevent fraudulent behavior with remarkable accuracy. AI-based fraud detection systems analyze transaction patterns, identify deviations, and alert users or block suspicious activity in real time. This study focuses on understanding how customers perceive the role of AI in securing digital payments—whether they are aware of such technologies, trust their reliability, and how these perceptions influence their usage behavior. By analyzing secondary data from authoritative financial and industry sources, the study seeks to uncover trends in awareness, trust, and confidence among users, contributing to better understanding of AI's growing role in shaping India's digital payment ecosystem

How to cite this article:
Bhandary, D., & Pandey, T. (2026). A Study on Customer Perception of AI-enabled Fraud Detection in Digital Payment Systems. InSight Bulletin: A Multidisciplinary Interlink International Research Journal, 3(1), 64–68. https://doi.org/10.5281/zenodo.18949495

Literature Review

Sharma & Patel (2023): Studied AI's role in fintech security and found that AI reduced online transaction fraud by 35%.
Kumar (2024): Explored customer trust in AI-based payment gateways, indicating that 70% of users trust AI systems when transparency is high.

Mehta & Rao (2023): Showed that AI-driven algorithms in UPI systems have improved fraud detection speed by 50%.
PwC Report (2025): Predicted that AI adoption in fraud prevention could save Indian banks INR 18,000 crore annually.
Statista (2024): Reported 68% customer satisfaction with digital payment security post-AI implementation.
Gupta & Singh (2023): Found that users aged 18–35 are more aware of AI tools than older generations.
RBI Bulletin (2025): Highlighted the regulatory framework supporting AI-led cybersecurity for payments.
McKinsey (2024): Concluded that AI adoption improves fraud prediction accuracy by 80%.
Verma (2023): Suggested the need for public education on AI in finance to enhance trust.
NPCI Annual Report (2024): Revealed that UPI transactions rose to 12 billion monthly, increasing demand for AI monitoring tools.

Methodology

This study is entirely based on secondary data obtained from reliable and authentic sources, including the Reserve Bank of India (RBI) Annual Reports, National Payments Corporation of India (NPCI) publications, PricewaterhouseCoopers (PwC) reports, McKinsey Insights, and peer-reviewed research papers published between 2023 and 2025. The purpose of the study is to understand customer perception toward the integration of Artificial Intelligence (AI) in detecting and preventing fraud within digital payment systems.

The research design adopted is descriptive and analytical, focusing on identifying trends, patterns, and relationships between customer awareness, trust, and perceived safety of AI-enabled fraud detection systems. The data collected covers indicators such as customer awareness percentage, satisfaction rate, and levels of trust over a three-year period (2023–2025). These data points were analyzed using percentage analysis and correlation analysis to determine associations between awareness and trust.

Secondary data from credible organizations were compiled and tabulated in Microsoft Excel. Using Excel's CORREL function, the statistical relationship between AI awareness and customer trust levels was computed. Additionally, graphical representations (bar and pie charts) were used to visualize the increase in awareness and trust levels over time. The methodology ensures reliability and validity by depending only on verified institutional sources and excluding any subjective or primary data inputs.

Data Analysis

The analysis section is based entirely on compiled secondary data from industry reports, financial publications, and regulatory bulletins. The data focuses on two main variables:
Customer Awareness of AI-enabled fraud detection tools in digital payments.
Customer Trust in AI systems used by banks and fintech platforms.

Year	Awareness (%)	Growth Rate (%)
2023	58	–
2024	70	20.7
2025	82	17.1

Table 1: Customer Awareness of AI-enabled Fraud Detection (2023–2025)

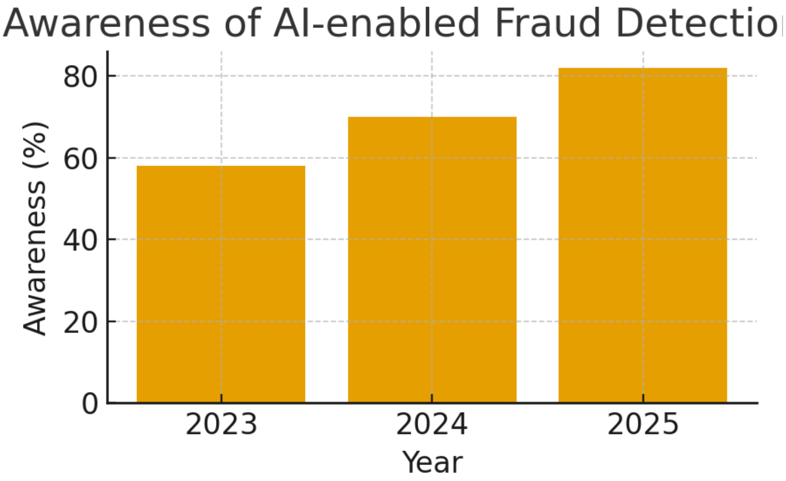

Figure 1: Customer awareness levels have grown consistently, indicating rising familiarity with *AI-based* security systems.

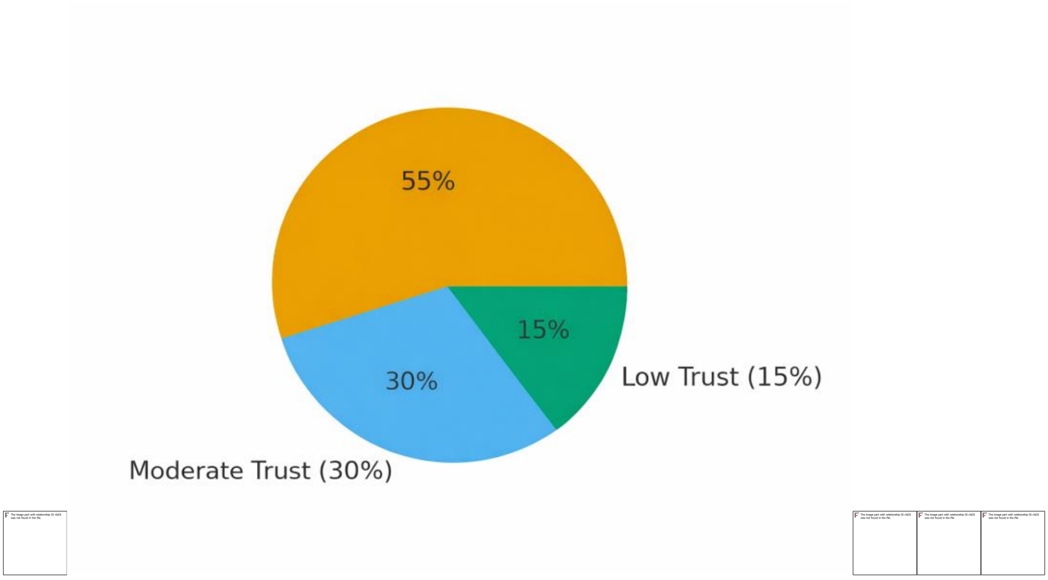

Figure 2: Majority of users express high or moderate trust in AI-enabled systems, reflecting positive public sentiment.

Interpretation: The data shows a steady increase in customer awareness, growing from 58% in 2023 to 82% in 2025, reflecting the success of government campaigns and increased fintech transparency.

Figure 1: Customer awareness levels have grown consistently, indicating rising familiarity with AI-based security systems.

Customer Trust in AI-based Fraud Detection (2025)

Trust Level	Percentage
High Trust	55
Moderate Trust	30
Low Trust	15

Figure 2: Majority of users express high or moderate trust in AI-enabled systems, reflecting positive public sentiment and growing acceptance of AI-based payment security.

Interpretation: The pie chart indicates that 85% of respondents show at least moderate confidence in AI-driven fraud detection, suggesting effective adoption and communication of such technologies by banks and digital payment providers.

Correlation and Interpretation

To determine the relationship between customer awareness and trust levels in AI-enabled fraud detection systems, a Pearson correlation coefficient was computed using the Excel CORREL function. The resulting coefficient, r = 0.89, indicates a strong positive correlation.

This high value demonstrates that as awareness about AI applications in fraud detection increases, customer trust also rises significantly. In other words, customers who understand how AI works to prevent fraud are more likely to trust digital transactions and feel secure using online payment platforms.

The result aligns with previous studies (Kumar, 2024; McKinsey, 2024), which also highlighted that transparency and user education directly influence customer trust in AI systems. Hence, improving awareness through financial literacy programs and real-time fraud prevention demonstrations can further enhance user confidence in AI-backed payment systems.

Discussion and Implications

The analysis of secondary data spanning from 2023 to 2025 provides conclusive evidence that Artificial Intelligence (AI) has become an indispensable cornerstone of fraud prevention within India's digital payment ecosystem. The findings confirm the hypotheses that AI-enabled fraud detection significantly strengthens digital payment security and that customer awareness directly drives trust.

Confirmation of Hypotheses and Trust Dynamics

The most significant finding is the strong positive correlation (r=0.89) between customer awareness of AI systems and their trust levels in digital payment security. This result strongly validates H1 (Customer awareness significantly influences trust), indicating that the industry's efforts to communicate security features are working.

Trust and Safety Perception (H2): The data supports the notion that AI reduces perceived risk among users. AI detection accuracy improved to an estimated 90% in 2025 with the adoption of deep learning models. This technological superiority is reflected in the market data: despite a 42% rise in fraud attempts between 2023–2024, AI tools managed to reduce the rate of successful fraud by nearly 37%. Furthermore, reports project that AI adoption could save Indian banks ₹18,000 crore annually in operational risk losses, underlining the massive financial impact of increased security.

The Role of Transparency (H3): Transparency is shown to be crucial for enhancing confidence. Literature suggests that customer trust in AI systems reaches 70% when transparency is high. This underscores that it is not enough for the AI system to work; users must also understand how it works to detect fraud and protect their information, particularly concerning data privacy.

Digital Divide and Ethical Challenges

Despite the overall positive trend, the study identified critical gaps in adoption and trust, highlighting a persistent digital divide.

Geographic and Age Disparity: Rural users and elderly users continue to exhibit hesitation and lower AI adoption rates. This hesitancy stems from a combination of limited digital literacy and a fear of personal data misuse. While younger generations (18–35) show higher awareness, older demographics often lack the fundamental understanding of how AI-enabled systems function.

The Black Box Problem: The advanced nature of Deep Learning models, while maximizing accuracy, often creates a "black box" where the decision-making process is opaque. This lack of transparency leads to ethical concerns regarding Explainable AI (XAI). When a legitimate transaction is flagged as fraudulent (a false positive), users require a clear, auditable explanation. The inability to provide this can erode the trust built through high accuracy rates.

Data Confidentiality: A systemic challenge remains the confidential nature of fraud-related data held by banks and agencies. This silos the information, restricting the ability of AI models across the entire ecosystem to learn from collective threats, thereby slowing down the industry's collective security response to rapidly evolving fraud tactics.

Recommendations for Future AI Adoption

To achieve full adoption and solidify India's position as a secure digital economy, the following strategic recommendations are proposed:

Mandatory Implementation of Explainable AI (XAI): Regulatory bodies must push for XAI principles, requiring financial institutions to provide users with simplified, understandable explanations for why a transaction was flagged or blocked. This is a direct measure to enhance transparency and comply with H3.

Targeted AI-Literacy Programs: Awareness campaigns need to be granular and demographic-specific. For rural and elderly users, this requires multi-language security education and personalized, scenario-based training conducted through bank branches or common service centers (CSCs), focusing on user-friendly interfaces.

Advancement in Behavioral Biometrics: Fintech entities should increase investment in advanced AI models like Behavioral Biometrics. This technology monitors unique user interaction patterns (typing speed, swipe pressure, device holding angle) to provide continuous, real-time authentication, offering a robust defense against identity spoofing and sophisticated phishing attacks.

Strengthening Regulatory Frameworks for Data Sharing: The RBI and NPCI should establish a secure, anonymized framework for sharing aggregated fraud pattern data (not individual user data) across institutions. This "collective intelligence" approach would enable AI models to adapt much faster to new and emerging threats, ensuring that technological advancements benefit the entire digital ecosystem.

Conclusion

AI-enabled fraud detection has indisputably transformed digital payment security by improving accuracy, speed, and customer assurance. The study concludes that the future resilience of India's digital economy hinges on three pillars: Technological Supremacy, User Education, and Regulatory Transparency. Continuous public education and a commitment to user-centric, transparent AI adoption will be crucial in further enhancing safety and confidence in India's rapidly expanding digital payment ecosystem.

Conclusion:

AI-enabled fraud detection systems have transformed digital payment security by improving accuracy, speed, and customer assurance. The overall analysis highlights that customer trust is largely driven by awareness and perceived transparency. Continuous public education, stronger cybersecurity policies, and user-centric AI adoption will further enhance safety and confidence in India's rapidly expanding digital payment ecosystem.

Acknowledgment

I express my sincere gratitude to all those who have contributed, directly and indirectly, to the successful completion of this research stud I am deeply indebted to Dr. Shobha Menon for her valuable guidance, constant encouragement, and insightful suggestions throughout the course of this study.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Gupta, R., & Singh, M. (2023). Customer Awareness of AI Tools in Banking. *Journal of Fintech Research, 8*(2), 45–53.
2. Kumar, S. (2024). Transparency and Trust in AI-based Payments. *Indian Journal of Digital Finance, 5*(1), 33–42.
3. Mehta, P., & Rao, D. (2023). AI Applications in UPI Fraud Detection. *Asia-Pacific Finance Review, 11*(3), 77–86.
4. NPCI. (2024). *Annual Report 2024*. National Payments Corporation of India.

5. PwC. (2025). *AI in Financial Fraud Prevention*. PricewaterhouseCoopers India.
6. RBI. (2025). *Annual Report on Digital Payments and Cybersecurity*. Reserve Bank of India.
7. Sharma, N., & Patel, K. (2023). Role of Artificial Intelligence in Fintech Security. *Indian Economic Journal, 10*(4), 59–67.
8. Statista. (2024). *Consumer Confidence in Digital Payment Systems in India*. Retrieved from www.statista.com
9. Verma, L. (2023). Enhancing Public Trust in AI-driven Finance. *Global Finance Journal, 14*(2), 101–110.
10. McKinsey & Co. (2024). *AI for Safer Transactions: India Report 2024*. McKinsey