The Role of AI in Fraud Detection in Digital Payments Sector

A Study on User Perceptions, Trust, and Privacy Concerns in Indian Digital Payment Systems

Sneha Sridhar-MBA student, Jain Deemed-To-Be-University CMS Business School.

Under the guidance of Professor and Program Coordinator – Finance **Dr. Vinoth S**

ABSTRACT

The expansion of digital payment systems has significantly changed how people carry out financial transactions, making them faster, easier, and more accessible than ever before. At the same time, this shift has brought an increase in fraudulent activities, creating serious concerns for both users and financial institutions. This study focuses on understanding how effective AI is in this role, while also examining how it influences user trust, confidence, and concerns related to data privacy.

A quantitative research approach was used for this study, with primary data collected from 148 respondents through a structured questionnaire. The data was analyzed using Jamovi, applying statistical techniques such as frequency analysis, descriptive statistics, chi-square tests, correlation, reliability analysis, and ANOVA. The results indicate that although most users are aware of AI in fraud detection and show a moderate level of confidence in its performance, their level of trust is comparatively lower.

The findings also suggest that when users perceive AI as effective, their trust in it tends to increase. However, confidence alone does not necessarily lead to higher trust, highlighting a more nuanced relationship between these factors. Furthermore, demographic variables play a role, with gender showing a significant influence on users' comfort levels, while age does not appear to have a meaningful impact on trust.

In conclusion, while AI holds strong potential to enhance fraud detection and improve the security of digital payment systems, gaining user trust and addressing privacy concerns remain essential for its wider adoption.

Keywords: Artificial Intelligence (AI), Fraud Detection Systems, Digital Payment Platforms, User Trust, Data Privacy Concerns

RATIONALE

As digital payment platforms grow exponentially in India and globally, the threat of financial fraud has become an equally pressing concern. While AI-based fraud detection has emerged as a technological solution, limited empirical research examines how users actually perceive, trust, and feel comfortable with these systems. This study therefore investigates user attitudes toward AI-driven fraud detection across dimensions of effectiveness, trust, confidence, and comfortability, with a focus on demographic influences and actionable implications for platform design.

INTRODUCTION

Over the past decade, digital payment systems have moved from being optional to becoming a core part of everyday financial activity. With the growing use of smartphones, online banking, mobile wallets, and e-commerce platforms, the way people handle money has changed significantly. Governments and financial institutions have also played a key role in promoting digital payments, as they enhance transparency, encourage financial inclusion, and extend financial services to a broader segment of the population.

Despite these advantages, the shift toward digital payments has introduced new risks. Cybercriminals use various methods such as phishing, identity theft, fake payment links, and unauthorized access to exploit system vulnerabilities. In the past, banks and financial institutions relied mainly on rule-based systems to identify suspicious activities. With millions of transactions being processed daily, such static systems are often insufficient for accurate fraud detection.

To address these limitations, Artificial Intelligence (AI) has gained attention as a more advanced approach to fraud detection. Technologies such as machine learning and data analytics allow systems to process large volumes of transaction data and identify patterns that may signal fraudulent behavior. Unlike fixed rule-based methods, AI systems can learn from past data and continuously improve their performance. However, the effective deployment of AI requires not just technical capability but also user trust, regulatory compliance, and transparent data practices.

Given the rapid expansion of digital payments and the increasing complexity of financial fraud, the role of AI in this area has become increasingly significant. The present study seeks to explore how AI supports fraud detection in digital payment systems, while assessing its contribution to improving overall security and efficiency, and examining user attitudes toward its adoption.

STATEMENT OF THE RESEARCH PROBLEM

As digital transactions continue to rise, fraud in the digital payments space has become an increasingly serious issue. Traditional rule-based fraud detection systems struggle to keep up with the complexity of modern digital payment ecosystems, and fraudsters continuously evolve their tactics to bypass static detection mechanisms.

Artificial Intelligence (AI) has emerged as a promising solution; however, practical challenges such as data quality, integration with existing systems, and data privacy concerns influence the effectiveness of these technologies. Despite increasing adoption, there is a gap in understanding how users perceive AI-based fraud detection in terms of effectiveness, trust, confidence, and comfortability. This study addresses that gap.

FRAMING OF RESEARCH HYPOTHESES

To systematically test the research objectives, the following hypotheses were formulated:

Hypothesis 1:

- H0: There is no significant relationship between perceived AI effectiveness and user trust in digital payment systems.
- H1: There is a significant positive relationship between perceived AI effectiveness and user trust in digital payment systems.

Hypothesis 2:

- H0: Gender does not significantly influence user comfortability with AI-based fraud detection systems.
- H1: Gender significantly influences user comfortability with AI-based fraud detection systems.

Hypothesis 3:

- H0: Age group does not significantly influence the perception of AI effectiveness in fraud detection.
- H1: Age group significantly influences the perception of AI effectiveness in fraud detection.

Hypothesis 4:

- H0: Frequency of digital payment usage does not significantly affect user confidence in AI-based security.
- H1: Frequency of digital payment usage significantly affects user confidence in AI-based security.

REVIEW OF LITERATURE

Sheed Iseal (2025) demonstrated that AI has emerged as a powerful tool in detecting fraud within digital payment systems by analyzing large volumes of transactional data. These systems examine multiple variables such as transaction

value, user behavior, frequency, and geographic location to identify irregular patterns. Unlike traditional methods, AI models continuously learn from new data, allowing them to adapt to evolving fraud strategies.

Pradeep Jeyachandran (2024) found that machine learning plays a critical role in strengthening fraud detection by analyzing historical transaction data to identify patterns associated with fraudulent behavior. These systems are capable of recognizing anomalies such as unauthorized payments or unusual transaction sequences, and their ability to operate in real time enables financial institutions to respond quickly to suspicious activities.

Muhammad Umar Khan (2025) highlighted that advanced AI techniques, including graph-based models and ensemble learning methods, have significantly improved fraud detection capabilities. These approaches analyze relationships between different entities such as users, devices, and transactions to uncover hidden connections. By identifying complex fraud networks, these models are particularly effective in detecting coordinated fraudulent activities.

Sukumaran (2025) showed that deep learning and behavioral analytics have transformed fraud detection by enabling systems to analyze complex transaction patterns and user activities. These models can capture subtle variations in behavior that may indicate fraudulent intent, and compared to traditional rule-based systems, deep learning approaches are more flexible and adaptable to changing fraud patterns.

Mula (2025) illustrated that techniques such as anomaly detection and biometric authentication have further enhanced fraud prevention strategies. By analyzing behavioral traits like typing patterns, login habits, and device usage, AI systems can identify deviations that may signal fraudulent activity, providing an additional layer of security beyond standard credentials.

S N Prajwalasimha (2025) argued that Explainable Artificial Intelligence has gained importance in fraud detection as it improves transparency and accountability in decision-making processes. These systems provide clear explanations for why certain transactions are flagged as suspicious, allowing analysts to better understand the reasoning behind predictions. This transparency builds trust among users and financial institutions.

P. Sundaravadivel (2025) introduced privacy-preserving techniques such as federated learning to address concerns related to data security. This approach allows multiple organizations to collaboratively train AI models without sharing sensitive customer data. By keeping data decentralized, federated learning ensures user privacy while still benefiting from large and diverse datasets.

Ali et al. (2022) conducted a systematic review of machine learning in financial fraud detection, demonstrating that ML-based approaches substantially outperform traditional systems in terms of both accuracy and scalability. Chang et al. (2022) further established that AI-powered digital payment fraud detection significantly reduces financial losses and operational burdens for institutions.

IDENTIFICATION OF RESEARCH GAPS

- Limited empirical research examines user perceptions of AI fraud detection across multiple psychological dimensions effectiveness, trust, confidence, and comfortability simultaneously.
- The influence of demographic variables such as gender and age on user attitudes toward AI fraud detection remains underexplored in the Indian context.
- The counterintuitive relationship between cognitive confidence and personal trust in AI systems has not been systematically investigated in digital payment contexts.

RESEARCH METHODOLOGY

Parameter	Details
Approach	Quantitative, following descriptive and analytical methods
Data Collection	Primary data via structured questionnaire using 5-point Likert Scale
Sample Size	148 respondents (students, professionals, and digital payment users)
Sampling Method	Convenience sampling
Variables	Effectiveness, Trust, Confidence, and Comfortability regarding AI fraud detection
Analysis Tools	Frequency analysis, descriptive statistics, Chi-square tests, Pearson Correlation, Reliability Analysis (Cronbach's Alpha), and Welch's ANOVA using Jamovi software

DATA ANALYSIS AND HYPOTHESIS TESTING

A. Demographics

Age Group Distribution:

Age Group	Frequency	Percentage
18–25	122	82.4%
26–35	8	5.4%
36–45	6	4.1%
46 and above	12	8.1%
Total	148	100%

Interpretation: The sample is dominated by the 18-25 age group (82.4%), indicating strong digital payment engagement among young adults. This demographic concentration reflects the digitally active population most exposed to AI-driven payment security systems.

Gender Distribution:

Gender	Frequency	Percentage
Male	102	68.9%
Female	46	31.1%
Total	148	100%

Interpretation: Male respondents constitute 68.9% of the sample. While this reflects a common skew in technology-focused survey samples, the gender imbalance is noted as a limitation and shapes the chi-square findings on comfortability.

B. Descriptive Statistics

Effectiveness, Trust, Confidence, and Comfortability

Variable	N	Mean	Std. Deviation	Min	Max
Effectiveness	148	2.91	0.964	1	5
Trust	148	2.80	0.808	1	5
Confidence	148	3.58	0.948	1	5
Comfortability	148	2.43	1.360	1	5

Interpretation: Confidence recorded the highest mean (3.58), indicating that users broadly believe in AI's capability to detect fraud. Effectiveness scored moderately (2.91), while Trust (2.80) and Comfortability (2.43) are notably below the neutral midpoint. The high standard deviation of Comfortability (1.36) reflects significant variation in user attitudes toward data sharing.

C. Hypothesis Testing

Hypothesis 1: Relationship between AI Effectiveness and User Trust (Pearson Correlation)

Relationship	Pearson r	p-value	Result
Trust – Effectiveness	0.342	< 0.001	Significant positive correlation
Trust – Confidence	-0.467	< 0.001	Significant negative correlation

Interpretation: A statistically significant positive correlation exists between perceived AI effectiveness and user trust ($r = 0.342$, $p < 0.001$), supporting H1 and rejecting H0. Notably, a significant negative correlation was found between confidence and trust ($r = -0.467$, $p < 0.001$), suggesting that cognitively confident users are paradoxically less personally trusting – a finding that challenges linear technology acceptance models.

Hypothesis 2: Gender and Comfortability (Chi-Square Test)

Gender	Comfortability 1	Comfortability 3	Comfortability 4	Comfortability 5	Total
Female	22	24	0	0	46
Male	40	38	8	16	102
Total	62	62	8	16	148

χ^2 Value	df	p-value	Result
13.7	3	0.004	Significant – H0 rejected, H1 accepted

Interpretation: The chi-square test reveals a statistically significant association between gender and comfortability ($p = 0.004$). Female respondents demonstrate substantially lower comfort with AI data practices. This finding highlights a gender-differentiated privacy concern that calls for targeted and empathetic communication strategies.

Hypothesis 3: Age Group and Perceived AI Effectiveness (Chi-Square Test)

χ^2 Value	df	p-value	Contingency Coefficient	Result
17.7	12	0.125	0.327	Not Significant – H0 retained

Interpretation: No statistically significant relationship was found between age group and perceptions of AI effectiveness ($p = 0.125$). This indicates that concerns about AI fraud detection are not generationally differentiated, simplifying communication strategies for platform providers.

Hypothesis 4: Usage Frequency and Confidence (Chi-Square Test)

χ^2 Value	df	p-value	Result
Approx. 7.3	9	0.652	Not Significant – H0 retained

Interpretation: Frequency of usage does not significantly influence user confidence in AI security systems (p = 0.652). This challenges the assumption that greater platform exposure naturally builds security confidence, suggesting that targeted education is more effective than passive usage exposure.

Reliability Analysis (Cronbach's Alpha)

Scale	Cronbach's Alpha	Interpretation
Trust, Confidence, Comfortability, Effectiveness	-0.372	Weak internal consistency - driven by inverse Confidence item

Interpretation: The low Cronbach's Alpha (-0.372) indicates measurement limitations in the composite scale, primarily due to the inverse behavior of the Confidence variable. While individual variable analyses remain valid, future studies should refine the instrument for stronger psychometric properties.

ANOVA: Age Group and Trust (Welch's)

Test	F-value	df	p-value	Result
Welch's ANOVA – Age & Trust	1.310	3, 26.9	0.275	Not Significant – H0 retained

Interpretation: Trust levels do not differ significantly across age groups (p = 0.275). The trust deficit observed in the sample is a broadly shared phenomenon rather than concentrated in specific demographics, making it a systemic challenge requiring platform-wide responses.

FINDINGS AND RECOMMENDATIONS

Research Findings

The study surfaced several significant and practically important findings:

- Confidence is the highest-rated perception variable (Mean: 3.58), indicating that users broadly believe AI is capable of detecting fraud. However, this cognitive confidence does not translate into personal trust.
- Trust recorded a mean of 2.80, which is slightly below neutral, pointing to hesitation rooted in concerns about data practices, transparency, and system opacity.
- Comfortability is the lowest-rated variable (Mean: 2.43), with the highest standard deviation (1.36), reflecting deep and widely varying discomfort around data sharing – even among users who acknowledge AI's protective benefits.
- Gender significantly influences comfortability (p = 0.004), with female respondents expressing substantially lower comfort. This gender gap in data privacy acceptance is one of the most actionable findings for platform designers.
- The negative correlation between Confidence and Trust (r = -0.467) is counterintuitive and theoretically significant: users who are more cognitively confident about AI capability are paradoxically less personally trusting, possibly because greater knowledge surfaces greater awareness of AI's limitations and opacity.

- The positive correlation between Trust and Effectiveness (r = 0.342) confirms that platforms which demonstrably show their fraud prevention outcomes can meaningfully elevate user trust over time.
- Age and usage frequency do not significantly influence AI effectiveness perceptions or confidence, respectively, suggesting that education-driven and platform-wide responses are more effective than age- or usage-targeted interventions.

Recommendations

Based on the findings, the following strategic recommendations are offered:

- Boost Transparency: Digital payment platforms should invest in clear, empathetic communication about how AI uses, protects, and governs personal transaction data. Dedicated privacy dashboards and user-controlled data settings can meaningfully reduce the comfortability gap.
- Make AI Protection Visible: Personalized fraud prevention notifications and periodic security impact summaries can transform abstract AI capability into tangible, trust-building user experiences.
- Proactive User Education: In-app explainer content, micro-learning features, and interactive security walkthroughs can cultivate informed confidence more durably than passive usage exposure alone.
- Gender-Responsive Design: Features such as opt-in AI monitoring settings, clear data deletion options, and accessible fraud detection explanations can address gender-differentiated privacy concerns and support broader digital payment participation.
- Embrace Explainable AI: Honest acknowledgment of AI's limitations, paired with clear explanations of human oversight mechanisms, can convert informed skepticism into reasoned confidence among digitally sophisticated users.

CONCLUSION

This study has investigated the role of Artificial Intelligence in fraud detection within digital payment systems, exploring how users perceive AI across four key dimensions: effectiveness, trust, confidence, and comfortability. Drawing on data from 148 respondents analyzed through Jamovi, the study has surfaced a nuanced and practically significant portrait of contemporary user attitudes toward AI-powered payment security in India.

The findings confirm that awareness of AI in fraud detection is high and that users hold a generally optimistic view of its capabilities, as reflected in elevated confidence scores. However, this optimism coexists with a meaningful trust deficit and a pervasive discomfort around data-sharing practices. The significant gender-based comfortability gap and the counterintuitive inverse relationship between confidence and trust are among the most thought-provoking findings, suggesting that the path to full user acceptance is neither straightforward nor uniform across demographic groups.

AI undeniably holds transformative potential for strengthening the security of digital payment ecosystems. Its ability to analyze vast transaction datasets in real time, detect evolving fraud patterns, and respond proactively to emerging threats positions it as an indispensable tool for financial institutions. However, realizing this potential in ways that genuinely serve users requires as much attention to human dimensions – trust, transparency, privacy, and communication as to technical capability and algorithmic sophistication.

Building effective AI-based fraud detection systems is only half the challenge. Building the human trust and comfort necessary for users to fully embrace these systems is equally important. Only by treating user trust and comfort as core design objectives rather than secondary concerns can the full promise of AI in digital payment fraud detection be responsibly and sustainably realized.

REFERENCES

Ali, A., Abd Razak, S., Othman, S. H., et al. (2022). Machine learning in financial fraud detection: A systematic review. IEEE Access, 10.

Akavaram, M. (2025). Hybrid AI frameworks for multi-layered fraud detection in digital payment systems.

Almazroi, A. A., & Ayub, N. (2023). Machine learning for online payment fraud detection. Journal of Financial Technology.

Bello, O., et al. (2023). AI fraud detection across financial institutions.

Chang, V., Doan, L. M. T., Di Stefano, A., Sun, Z., & Fortino, G. (2022). Digital payment fraud detection methods. Internet of Things.

Dhirani, L. L., et al. (2023). Privacy and ethical governance in AI-powered fraud detection.

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques. IEEE Access.

Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection system. Journal of Big Data, 9(1), 1–20.

Jeyachandran, P. (2024). Machine learning in digital payment fraud detection.

Juniper Research. (2022). AI-enabled fraud detection market forecast 2022–2027. Juniper Research Ltd.

Kantheti, P. R., & Bvuma, S. (2024). Digital payment fraud as systemic economic threat.

Khan, M. U. (2025). AI-based fraud detection using graph neural networks and ensemble methods.

Mohanty, S., & Mishra, S. (2023). AI fraud detection in multi-party digital transactions.

Mula, A. (2025). Anomaly detection and biometric authentication in AI fraud prevention.

Noviandy, T. R., et al. (2023). Digital payment fraud detection using XGBoost.

Patel, A. (2025). Machine learning models in genuine vs. fraudulent transaction classification.

Prajwalasimha, S. N. (2025). Explainable AI in financial fraud detection: Transparency and accountability.

Roshanaei, M., et al. (2024). Governance mechanisms for AI fraud detection systems.

Sheed Iseal. (2025). AI in fraud detection in digital payments.

Sukumaran, A. (2025). Deep learning and behavioral analytics for fraud detection in digital payments.

Sundaravadivel, P. (2025). Federated learning for privacy-preserving AI fraud detection.

Xu, L., et al. (2024). Advanced AI architectures for payment fraud detection and prevention.