

CONSUMER TRUST AND ADOPTION OF AI-ENABLED DIGITAL PAYMENTS: THE ROLE OF SECURITY, PRIVACY AND PERCEIVED RISK

J. Saliha Farah^{1*}

1. UG Student, Department of Commerce, Velumanoharan Arts and Science College for Women, Ramanathapuram, Tamil Nadu, India

Abstract

Artificial intelligence (AI) has become an important part of digital payment systems, supporting fraud detection, transaction monitoring, risk assessment and customer support. AI-enabled payments can provide speed, convenience and additional security, but consumers may also be concerned about privacy, data protection and financial risk. This paper examines how perceived security, privacy concerns and perceived risk influence consumer trust and the adoption of AI-enabled digital payments. It develops a conceptual framework in which security perceptions are associated with trust, while privacy concerns and perceived risk may influence adoption and continued use, and it proposes a survey-based methodology and measurement constructs for empirical testing. The paper also highlights transparent data practices, effective security mechanisms, consumer awareness and grievance redressal as important areas for building confidence in AI-enabled digital payments.

Keywords

Artificial Intelligence, Digital Payments, Consumer Trust, Security, Privacy, Perceived Risk, Adoption

1. Introduction

Digital payments have become an important part of modern commerce (National Payments Corporation of India [NPCI], n.d.; Reserve Bank of India, 2025). Consumers can transfer money, purchase goods and services, pay bills and manage financial activities through mobile applications, online banking, cards and other electronic payment platforms, and smartphones and internet connectivity have made these services convenient and accessible. AI is increasingly used within payment ecosystems to identify unusual transaction patterns, detect possible fraud, monitor anomalies and support risk assessment, analysing large volumes of transactions and helping payment providers respond to suspicious activities.

However, technology alone does not determine whether consumers will use a payment service. Consumers consider whether their money is safe, whether personal information is protected and whether problems can be resolved effectively, and concerns about unauthorised transactions, misuse of

information, technical failures and cyber threats create perceived risk. Consumer trust is therefore important for understanding adoption. This paper focuses on perceived security, privacy concerns, perceived risk and trust as factors connected with the adoption and continued use of AI-enabled digital payments.

2. Statement of the Problem

The use of AI in digital payment systems creates opportunities for stronger fraud detection and transaction monitoring. At the same time, consumers may not fully understand how AI systems use their information or make automated decisions, which creates uncertainty about data collection, privacy, security and accountability. A consumer may recognise the convenience of digital payments while still being concerned about financial loss, unauthorised access or misuse of personal information, and such concerns can affect confidence in the payment provider and the intention to adopt or continue using digital payment services. The issue is therefore

*Corresponding author: salihafarahjaffer@gmail.com

not only technological but also involves consumers' perceptions of security, privacy and risk. This study addresses the need for a conceptual understanding of how these perceptions and consumer trust are related to the adoption of AI-enabled digital payments.

3. Objectives of the Study

1. To examine consumer awareness and usage of AI-enabled digital payment services.
2. To study the influence of perceived security, privacy concerns and perceived risk on consumer trust and adoption intention.
3. To examine whether consumer trust is associated with the intention to continue using digital payment services.
4. To identify practices that can improve trust, security awareness and the responsible use of AI in digital payments.

4. Review of Literature

Gupta et al. (2023) examined perceived risks, perceived benefits, trust and willingness to adopt the digital rupee in India. Their study considered financial, regulatory, security, privacy and operational risks and reported that risk factors are relevant to the willingness to adopt a central bank digital currency, with trust playing a mediating role. A 2024 study of Indian women using mobile payment services examined risk perception, trust, satisfaction and continuance intention; financial and performance risks were negatively associated with

satisfaction and trust, while trust and satisfaction were related to continued use ("Financial Equality through Technology," 2024). Aljaradat and Shukla (2026) studied cybersecurity and trust formation in digital payment use behaviour in North India, considering perceived cybersecurity risk, trust, performance expectancy, effort expectancy, social influence and grievance redressal, and showed the relevance of cybersecurity concerns and service support. Ofosu-Ampong et al. (2026) examined AI-enabled security features and trust in digital payment systems, considering transaction procedures and technical safeguards such as real-time fraud detection, anomaly monitoring and biometric authentication, thereby providing evidence for studying security perceptions and trust in AI-supported payments.

5. Conceptual Framework

The proposed framework connects perceived security, privacy concern and perceived risk with consumer trust and adoption intention (Figure 1). Consumer trust is positioned as the central factor between these perceptions and adoption intention: when consumers believe that payment providers use appropriate security mechanisms and handle information responsibly, trust may be strengthened, whereas strong privacy concerns or perceived risks may reduce confidence. Adoption intention represents the willingness to use or continue using AI-enabled digital payment services.

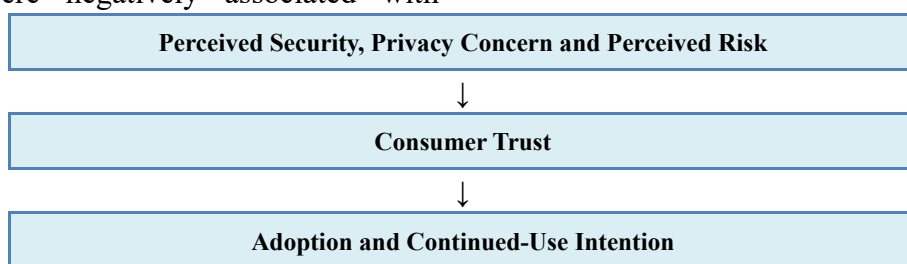


Figure 1. Proposed Conceptual Framework

5.1 Perceived Security

Perceived security refers to the consumer's belief that a digital payment system can protect transactions, financial information and personal data from unauthorised access or misuse. It is important because digital payments involve the transfer of

financial value through electronic systems. AI supports payment security through automated monitoring of transaction patterns, identifying unusual behaviour, flagging suspicious transactions and supporting fraud detection, while real-time monitoring helps providers respond to potentially risky

activities. Consumers also consider authentication methods, transaction alerts and platform reliability when forming security perceptions, and clear communication about security features helps them understand how transactions are protected. The presence of AI does not automatically create trust, however; consumers may still require information about security practices, blocked transactions and complaint handling, so effective security involves both technical protection and consumer confidence.

5.2 Privacy Concerns

Digital payment transactions generate information that may include transaction details, account information, device information and other personal data, and consumers may be concerned about how payment providers collect, store, process and share it. While data-driven security supports fraud prevention, consumers want to know why information is collected and how it is protected, and lack of clarity increases privacy concerns. Transparent privacy notices that explain the purpose of data collection, the types of information involved, security measures and available controls in clear language help consumers understand data practices. A payment system may be technically secure, yet consumers may still hesitate if they believe personal information is handled without sufficient transparency.

5.3 Perceived Risk

Perceived risk refers to the uncertainty or possible loss that consumers associate with a digital payment transaction. Financial risk arises when consumers fear that money could be transferred without authorisation or that recovery after fraud may be difficult; privacy risk arises from uncertainty about the collection or use of personal information; and technical risk involves failed transactions or system interruptions. Higher perceived risk may reduce confidence and the willingness to adopt or continue using digital payments. AI-enabled monitoring, strong authentication, transaction alerts and accessible grievance redressal can help address these risks, and consumer awareness is also important so that users can recognise suspicious links, fraudulent requests and unauthorised communication.

5.4 Consumer Trust

Consumer trust is the confidence that a consumer places in a digital payment provider, system or platform. It develops when consumers believe that transactions will be processed reliably, financial information will be protected and problems will be handled responsibly. Because consumers cannot physically observe the digital transaction process, they depend on the platform, its security mechanisms and the service provider, so reliability and transparency influence confidence. AI-enabled security features may contribute to trust when they are perceived as effective and understandable, whereas uncertainty about automated decision-making or data use may create additional concerns. Clear communication about AI practices and grievance procedures supports trust formation, and consumers who trust a provider are more comfortable using its services repeatedly. Trust is therefore the central factor connecting security, privacy and risk with adoption intention.

5.5 AI-Enabled Security Features and Adoption

AI supports digital payment security through several mechanisms: fraud-detection systems analyse transaction patterns and identify activity that differs from expected behaviour, anomaly monitoring flags unusual transactions for additional verification, and biometric authentication adds a further layer of identity verification (Ofosu-Ampong et al., 2026). Adoption, however, depends on more than the availability of technology. Consumers consider whether security procedures are convenient, whether alerts are understandable and whether genuine transactions are unnecessarily interrupted, so a balance between protection and usability shapes the user experience. Responsible AI use also requires appropriate governance, data protection, human oversight and accessible channels for resolving payment problems, so that technological security and consumer confidence develop together.

6. Proposed Research Methodology

The study is proposed as a descriptive and analytical study of users of digital payment services. The population includes individuals who use UPI, mobile banking, cards or other digital payment services in India, and a convenience or purposive

sample of approximately 200–300 respondents may be considered; the final sample size should be reported after data collection. Primary data may be collected through a structured questionnaire, with voluntary participation and respondents informed of the academic purpose of the study. Frequency and percentage analysis may describe respondent characteristics and usage patterns, mean and standard deviation may summarise construct scores,

Cronbach's alpha may assess internal consistency, and correlation and multiple regression may examine relationships among perceived security, privacy concern, perceived risk, trust and adoption intention; mediation analysis may be used where appropriate. The suggested questionnaire constructs, measured on a five-point Likert scale from strongly disagree to strongly agree, are listed in Table 1.

Table 1. Suggested Questionnaire Constructs and Sample Items

Construct	Sample items
Perceived security	AI-based fraud detection makes digital payments feel safer. I believe security mechanisms can detect suspicious transactions.
Privacy concern	I am concerned about how payment applications collect and use my personal data. I worry about unauthorised access to payment information.
Perceived risk	I am concerned about financial loss from digital payment fraud. I worry that technical problems may affect my transactions.
Consumer trust	I trust digital payment providers to protect my financial information. I believe payment providers will act responsibly when problems occur.
Adoption intention	I intend to continue using digital payments. I would use AI-enabled payment features when available. I would recommend trusted digital payment services to others.

Source: Developed by the author

7. Practical Implications

Payment providers can communicate the purpose and limitations of AI-based fraud detection in clear language and design security alerts and authentication procedures that provide protection without unnecessary confusion. Privacy notices can explain what information is collected, why it is used and how it is protected. Accessible grievance redressal is also important: consumers should know how to report unauthorised transactions, technical problems and suspected fraud. Consumer education can include guidance on suspicious links, OTP and PIN protection, impersonation scams and safe reporting procedures.

8. Limitations and Future Research

The present paper is conceptual and does not claim original survey findings; no respondent numbers, percentages or statistical results are presented because primary data have not been collected.

Future studies can test the framework empirically and compare consumers across age groups, education levels, locations and levels of digital payment experience.

9. Conclusion

AI can contribute to fraud detection, anomaly monitoring and transaction security, but consumer adoption of digital payments also depends on perceptions of security, privacy and risk. The proposed framework places consumer trust at the centre of these relationships, and empirical testing can provide further evidence on the factors shaping the adoption and continued use of AI-enabled digital payments.

References

- [1]. Aljaradat, A., & Shukla, S. (2026). Cybersecurity and trust formation in digital payment use behaviour in North India. Discover

- Sustainability, 7, Article 498.
<https://doi.org/10.1007/s43621-026-02769-x>
- [2]. Financial equality through technology: Do perceived risks deter Indian women from sustained use of mobile payment services? (2024). International Journal of Information Management Data Insights, 4(2), Article 100266.
<https://doi.org/10.1016/j.jjime.2024.100266>
- [3]. Gupta, S., Pandey, D. K., El Ammari, A., & Sahu, G. P. (2023). Do perceived risks and benefits impact trust and willingness to adopt CBDCs? Research in International Business and Finance, 66, Article 101993.
<https://doi.org/10.1016/j.ribaf.2023.101993>
- [4]. National Payments Corporation of India. (n.d.). Unified Payments Interface (UPI) product statistics. NPCI.
- [5]. Ofosu-Ampong, K., Ansong, E., Akandekumtiim, J. M., Asmah, A., Commey, N. O., Amankwaa, T., & Tsedzah, V. (2026). How AI-enabled security features shape payment security perceptions and trust in digital payment systems. Telematics and Informatics Reports, 21, Article 100298.
<https://doi.org/10.1016/j.teler.2026.100298>
- [6]. Reserve Bank of India. (2025). Annual report 2024–25. Reserve Bank of India.