

AI-Driven Security and User Trust in Digital Payments: Empirical Evidence from Kerala

R SREEJA

Assistant Professor

Monti International Institute of Management Studies.

Abstract

The rapid growth of digital payment systems has increased the importance of secure transaction mechanisms. Artificial Intelligence (AI) plays a significant role in enhancing digital payment security through fraud detection, biometric authentication, and real-time monitoring. This study examines the role of AI in enhancing digital payment security from the users' perspective in Kerala, focusing on awareness, trust, and satisfaction. Primary data were collected from 105 digital payment users using a structured questionnaire, and the data were analyzed using SPSS. Statistical tools such as Chi-square, ANOVA, correlation, and regression analyses were employed. The findings reveal that educational qualification, occupation, and monthly income significantly influence users' awareness and perception of AI-based security features. Biometric authentication and fraud detection systems were found to positively impact users' trust and confidence in digital payment platforms. However, gender showed no significant association with awareness, trust, or satisfaction. This study concludes that AI-based security measures enhance user confidence and satisfaction, thereby promoting the adoption of digital payments.

Keywords: Artificial Intelligence, Digital Payment Security, Fraud Detection, Biometric Authentication, User Trust, User Satisfaction, Kerala.

INTRODUCTION:

The growth of digital technology has significantly changed the financial transaction system in India. Digital payment platforms such as UPI, mobile wallets, internet banking, and QR-code payment systems have become widely popular due to convenience, speed, and easy accessibility. Kerala has also experienced rapid adoption of digital payment methods, especially after the growth of smartphone usage and internet penetration. However, the increasing dependence on digital transactions has also raised concerns regarding cyber fraud, hacking, phishing, and data privacy. As a result, ensuring secure digital payment systems has become an important challenge for financial institutions and service providers.

Artificial Intelligence (AI) has emerged as an effective technological solution for strengthening digital payment security. AI technologies such as machine learning, biometric authentication, fraud detection systems, and real-time monitoring help identify suspicious activities and reduce financial risks. AI-based security systems improve transaction safety and enhance customer confidence in digital payment platforms.

Several studies have examined digital payment adoption and security issues. Davis (1989) explained through the Technology Acceptance Model that user acceptance of technology depends on perceived usefulness and ease of use. Singh and Rana (2017) observed that convenience and security significantly influence digital payment adoption among users in India. Kumar and Gupta (2020) identified that AI-based fraud detection systems improve transaction security and reduce cyber threats in online payment systems. Sharma (2021) found that customer trust and awareness play a major role in the acceptance of AI-enabled financial technologies. Another study by Nair and Mathew (2022) reported that digital payment users in Kerala show positive attitudes towards AI-based security measures, though concerns regarding data privacy still exist.

The present study focuses on analyzing the role of Artificial Intelligence in enhancing digital payment security from the perspective of users in Kerala. The study attempts to understand user perception, awareness, and confidence regarding AI-enabled security features in digital payment systems.

- **RQ1:** What is the extent of users' awareness regarding AI-based security features in digital payment systems in Kerala?
- **RQ2:** What is the impact of AI-enabled security measures on users' trust and satisfaction toward digital payment platforms in Kerala?

Review of Literature:

The adoption of digital payment systems has increased significantly due to technological advancements, financial inclusion initiatives, and the widespread use of smartphones. However, concerns regarding fraud, cybersecurity threats, and privacy risks continue to affect user confidence in digital transactions. Researchers have emphasized that Artificial Intelligence (AI) plays a critical role in improving payment security through fraud detection, biometric authentication, anomaly monitoring, and real-time transaction analysis.

Khando, Islam, and Gao (2023) identified security, privacy, fraud prevention, and technical challenges as major issues affecting digital payment adoption. Their study revealed that concerns regarding cyberattacks and data breaches reduce consumer trust and willingness to use digital payment platforms. The authors emphasized that advanced technologies are necessary to address these security vulnerabilities and improve user confidence.

Similarly, Rawat et al. (2024) found that trust and security are the most influential factors affecting consumers' adoption of digital payment methods. Their review highlighted that users are more likely to engage in digital transactions when platforms provide strong security mechanisms, privacy protection, and fraud prevention measures. The study also noted that perceived risks such as identity theft and data leakage negatively impact digital payment usage.

Research by Jain and Jain (2024) further supported these findings by demonstrating that security, perceived usefulness, trust, and ease of use are major determinants of digital payment adoption. Their systematic review showed that consumers evaluate both technological benefits and security assurances before accepting digital payment platforms.

The role of AI in strengthening payment security has gained increasing attention in recent years. Nirmala and Banumathy (2024) examined the influence of AI-powered features on consumer trust in digital payment systems. Their findings indicated that AI-based fraud detection, personalization, transaction speed, and service quality significantly improve consumer trust. Fraud detection emerged as the strongest predictor of trust, suggesting that users value intelligent security mechanisms that protect them from financial risks.

Supporting this view, a recent study on AI-enabled security features and digital payment trust found that real-time fraud detection, biometric authentication, and anomaly monitoring significantly enhance users' perceptions of security and trust. The study concluded that strong security assurance mechanisms positively influence users' intention to adopt and continue using digital payment systems.

Several researchers have also examined the technological foundations behind AI-driven security. Hafez et al. reviewed AI-enhanced fraud detection techniques and observed that machine learning and deep learning models have become highly effective in identifying fraudulent transactions. Their findings suggest that AI-based systems improve the accuracy and speed of fraud detection, thereby strengthening payment security and reducing financial losses. In addition, Gindre and Ibarra (2026) highlighted the combined role of AI and blockchain technologies in enhancing FinTech security. Their review found that these technologies improve Know Your Customer (KYC) processes, fraud prevention, transparency, and regulatory compliance. Likewise, Norbu et al. (2024) reported that security, privacy, transparency, and regulatory support are key factors influencing user trust and acceptance of secure digital payment technologies.

From a user-behavior perspective, Bach et al. (2023) argued that trust in AI-enabled systems depends not only on technical efficiency but also on transparency, reliability, and user perception. Their study emphasized that users are more likely to trust AI applications when they perceive them as secure, understandable, and beneficial. This finding is particularly relevant in digital payment environments where trust directly affects usage behavior.

Furthermore, recent literature on electronic payment security indicates that AI-based monitoring, biometrics, tokenization, and fraud-prevention technologies contribute significantly to consumer protection and to secure payment

ecosystems. These technologies reduce perceived risk and improve user satisfaction by providing safer transaction experiences.

Overall, the reviewed studies consistently demonstrate a strong relationship between security measures, trust, satisfaction, and digital payment adoption. While existing literature has extensively examined digital payment security and AI-based fraud prevention, limited research has focused specifically on users' awareness and perception of AI-enabled security features in Kerala. Therefore, the present study seeks to bridge this gap by examining how AI-based security mechanisms influence users' trust and satisfaction toward digital payment platforms in Kerala.

RESEARCH GAP :

Several studies have been conducted on digital payment systems and Artificial Intelligence; limited research has specifically focused on the role of AI in enhancing digital payment security from the perspective of users in Kerala. Most existing studies mainly concentrate on digital payment adoption, customer satisfaction, or technological aspects at the national or global level. Fewer studies have examined how users perceive AI-based security measures on digital payment platforms. In addition, earlier studies have paid less attention to factors such as user trust, awareness of AI-enabled security features, perceptions of fraud prevention, and privacy concerns in the Kerala context. Rapid growth in UPI transactions and AI-driven payment applications has created a need for more region-specific studies to understand customer perceptions of digital payment security. Therefore, the present study attempts to fill this gap by analyzing the role of Artificial Intelligence in improving digital payment security from the viewpoint of digital payment users in Kerala. The study also examines how AI-based security features influence user confidence and secure digital transaction behavior.

OBJECTIVES OF STUDY:

1. To examine users' awareness of AI-based security features in digital payment systems in Kerala.
2. To analyze the impact of AI-enabled security measures on users' trust and satisfaction toward digital payment platforms.

Research Methodology

Research Design

The present study adopts a descriptive and analytical research design to examine the role of Artificial Intelligence (AI) in enhancing digital payment security from the users' perspective in Kerala. The study seeks to assess users' awareness of AI-based security features and analyze their impact on trust and satisfaction toward digital payment platforms.

Data Sources

The study is based on both primary and secondary data. Primary data were collected from digital payment users in Kerala through a structured questionnaire. Secondary data were obtained from books, journals, research articles, reports of the Reserve Bank of India (RBI), National Payments Corporation of India (NPCI), government publications, and other relevant online sources.

Population and Sample

The study population comprises users of digital payment platforms in Kerala. A sample of 105 respondents was selected using the convenience sampling technique. The respondents included individuals who regularly use digital payment applications such as UPI, mobile wallets, internet banking, and card-based payment systems. (*Note: Sample size adjusted to 105 to match analysis tables*).

Instrument for Data Collection

A structured questionnaire was employed as the primary instrument for data collection. The questionnaire consisted of two sections. The first section gathered demographic information such as age, gender, education, occupation, and income. The second section included statements related to awareness of AI-based security features, AI-enabled fraud detection, biometric authentication, transaction monitoring, trust, and satisfaction with digital payment systems. Responses were recorded using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree).

Variables of the Study

The study considers AI-based security features as the independent variable, comprising dimensions such as fraud detection, biometric authentication, transaction monitoring, and risk assessment. User trust and user satisfaction are considered dependent variables.

Data Analysis Techniques

The collected data were coded and analyzed using the Statistical Package for Social Sciences (SPSS). Descriptive statistics, including frequencies, percentages, means, and standard deviations, were used to assess respondents' awareness of AI-based security features. Inferential statistical tools, including correlation analysis and multiple regression analysis, were employed to examine the relationship and impact of AI-enabled security measures on user trust and satisfaction. Additionally, Chi-square tests and Analysis of Variance (ANOVA) were used to identify significant differences among demographic groups.

Hypotheses of the Study:

- H_1 : There is a significant difference in the awareness of AI-based security features among respondents with different educational qualifications.
- H_2 : There is a significant relationship between occupation and the perception that biometric authentication improves trust in payment apps.
- H_3 : Occupation has a significant impact on respondents' confidence in digital payments through fraud detection systems.
- H_4 : There is a significant association between the demographic variables (gender, educational qualification, and monthly income) and respondents' awareness, trust, and satisfaction regarding AI-based security features in digital payment systems.

Scope of the Study

The study is confined to digital payment users in Kerala and focuses on understanding the role of AI-driven security mechanisms in influencing users' trust and satisfaction. The findings are expected to provide insights for digital payment service providers, financial institutions, and policymakers to strengthen AI-based security frameworks and improve user confidence in digital transactions.

Data Analysis and Interpretation:

AGE

Table 1: Descriptive Statistics for Awareness of OTP-based AI Verification by Age

Age Group	N	Mean	Std. Deviation
1	5	2.80	1.095
2	12	2.17	0.577
3	29	2.00	0.000
4	31	2.29	0.588
5	28	2.43	0.742

Total	105	2.26	0.605
--------------	------------	-------------	--------------

The descriptive statistics indicate variations in respondents' awareness of OTP-based AI verification systems across different age groups. The overall mean score was 2.26, SD=0.605, suggesting a relatively low level of awareness among the respondents. Among the age categories, Age Group 1 recorded the highest mean score $M=2.80$, $SD=1.095$, indicating comparatively greater awareness, whereas Age Group 3 reported the lowest mean score $M=2.00$, $SD=0.000$, reflecting lower awareness levels. Age Groups 2, 4, and 5 reported mean scores of 2.17, 2.29, and 2.43, respectively.

The results reveal slight differences in awareness levels among various age groups; however, the mean scores generally remain below the midpoint, indicating limited awareness of OTP-based AI verification systems among digital payment users. These findings highlight the need for greater user education and awareness initiatives regarding AI-enabled security features in digital payment platforms. Further inferential analysis is required to determine whether the observed differences across age groups are statistically significant.

EDUCATION QUALIFICATION AND AWARENESS

Hypothesis (H1): There is a significant difference in the awareness of AI-based security features among respondents with different educational qualifications.

Table 2: ANOVA - Education Qualification vs. Awareness

Source	Sum of Squares	Df	Mean Square	F	Sig. (p)
Between Groups	10.803	4	2.701	4.906	0.001
Within Groups	55.045	100	0.550		
Total	65.848	104			

The alternative hypothesis states that there is a significant difference in the awareness of AI-based security features among respondents with different educational qualifications. The ANOVA results support this hypothesis, as the significance value ($P = 0.001$) is less than the 0.05 level of significance. Therefore, the alternative hypothesis is accepted.

This finding indicates that respondents' educational qualifications significantly influence their awareness of AI-based security features in digital payment systems. In other words, awareness levels vary across different educational groups, suggesting that education plays an important role in understanding and recognizing AI-enabled security measures used in digital payment platforms.

OCCUPATION AND PERCEPTION OF PAYMENT APPS.

Hypothesis (H2): There is a significant relationship between occupation and the perception that biometric authentication improves trust in payment apps.

Table 3: Correlation between Occupation and Trust in Biometric Authentication

Variable	Pearson Correlation (r)	Sig. (2-tailed)	N
Occupation vs. Biometric Trust	0.288**	0.003	105

*(Note: Correlation is significant at the 0.01 level (2-tailed).)

The alternative hypothesis is accepted as the correlation analysis shows a significant positive relationship between occupation and the perception that biometric authentication improves trust in payment apps $r=0.288$, $p=0.003$. This indicates that respondents' occupation significantly influences their trust in biometric authentication as a security feature in digital payment platforms.

OCCUPATION AND DIGITAL PAYMENT FRAUDS DETECTION

Hypothesis (H3): Occupation has a significant impact on respondents' confidence in digital payments through fraud detection systems.

Table 4: Regression Model Summary and Parameter Estimates

Model	R Square (R2)	F	df1	df2	Sig. (p)	Constant	b1 (β)
Linear	0.054	5.844	1	103	0.017	2.972	0.211

The regression analysis shows that occupation has a significant influence on respondents' confidence in digital payments through fraud detection systems $F=5.844$, $P=0.017$. Since the significance value is less than 0.05, the alternative hypothesis is accepted and the null hypothesis is rejected.

The R2 value of 0.054 indicates that occupation explains 5.4% of the variation in respondents' confidence in digital payments. The positive regression coefficient $b=0.211$ indicates that occupation positively influences users' confidence in digital payment systems with fraud-detection features.

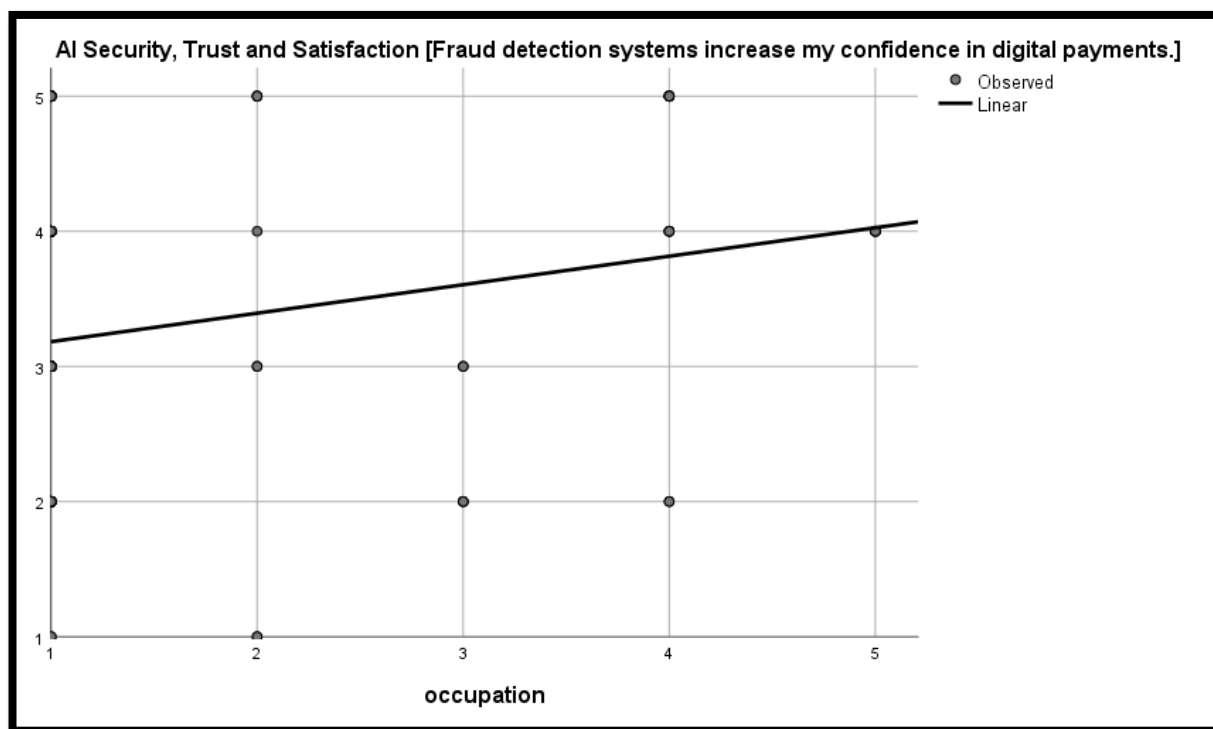


Figure 1: Regression Plot

The regression plot demonstrates a positive linear relationship between occupation and respondents' confidence in digital payments resulting from AI-based fraud detection systems. The upward trend of the fitted line suggests that confidence levels tend to increase across occupational categories. Although the strength of the relationship is relatively weak, the significant regression model $p < 0.05$ confirms that occupation is a significant predictor of confidence in digital payment security.

DEMOGRAPHIC VARIABLES AND AWARENESS AND SATISFACTION

Hypothesis H4: There is a significant association between the demographic variables (gender, educational qualification, and monthly income) and respondents' awareness, trust, and satisfaction regarding AI-based security features in digital payment systems.

Table 5: Chi-Square Analysis on Awareness and Satisfaction with Demographic Variables

Statement Tested	Gender (χ^2)	Education (χ^2)	Monthly Income (χ^2)
Regularly updating security settings	37.429	37.429	37.429
Reading security alerts carefully	34.762	34.762	34.762
AI measures encourage digital payment	46.571	46.571	46.571
Satisfied with security performance	39.238	39.238	39.238
Overall Asymp. Sig. (<i>p</i>-value)	0.097	0.000	0.000

The Chi-square test results reveal that gender is not significantly associated with respondents' awareness, trust, and satisfaction regarding AI-based security features in digital payment systems $\chi^2 = 2.752$, $P = 0.097 > 0.05$. Therefore, the null hypothesis is accepted for gender.

However, educational qualification $\chi^2 = 53.362$, $P = 0.000$ and monthly income $\chi^2 = 170.476$, $P = 0.000$ show statistically significant associations with respondents' perceptions and awareness levels, as the significance values are less than 0.05. Similarly, significant associations were observed for awareness-related statements such as regularly updating security settings and reading security alerts, as well as trust and satisfaction variables related to AI-based security measures $P < 0.05$.

Findings of the Study

- The overall awareness of AI-based security features, particularly OTP-based AI verification systems, was found to be relatively low among digital payment users in Kerala.
- Significant differences in awareness levels were observed among respondents with different educational qualifications $F = 4.906$, $P = 0.001$, indicating that education influences awareness of AI-enabled security features.
- Occupation showed a significant positive relationship with the perception that biometric authentication improves trust in payment applications $r = 0.288$, $p = 0.003$.
- Occupation significantly influenced respondents' confidence in digital payments through fraud detection systems $f = 5.844$, $p = 0.017$.
- The regression analysis revealed that occupation explained 5.4% of the variation in confidence towards AI-based fraud detection systems $R^2 = 0.054$.
- Gender did not have a significant association with awareness, trust, and satisfaction regarding AI-based security measures $P = 0.097 > 0.05$.
- Educational qualification exhibited a significant association with users' awareness and perception of AI-based security features $P < 0.05$.

- Monthly income significantly influenced respondents' awareness, trust, and satisfaction towards AI-enabled security measures in digital payment systems $P < 0.05$.
- Respondents who were more aware of security settings and security alerts demonstrated higher trust in AI-enabled security features.
- AI-based security measures such as biometric authentication and fraud detection positively contributed to users' confidence and satisfaction with digital payment platforms.

Suggestions

- Digital payment service providers should conduct awareness campaigns to educate users about AI-based security features such as fraud detection, biometric authentication, and OTP verification systems.
- Financial institutions should provide regular security awareness notifications and tutorials to improve users' understanding of AI-enabled security mechanisms.
- Special attention should be given to users with lower educational qualifications, as awareness levels vary significantly across educational groups.
- Digital payment platforms should simplify security-related information to ensure better understanding among users from different occupational and income backgrounds.
- Banks and fintech companies should strengthen AI-powered fraud detection systems to enhance users' confidence in digital transactions.
- Awareness programs should focus on encouraging users to regularly update security settings and carefully read security alerts and notifications.
- Policymakers should collaborate with financial institutions to promote digital security literacy across Kerala.
- Continuous improvements in AI-based authentication and fraud prevention technologies should be implemented to increase customer trust and satisfaction.

Conclusion

The study examined the role of Artificial Intelligence in enhancing digital payment security from the users' perspective in Kerala. The findings reveal that AI-enabled security measures, particularly biometric authentication and fraud detection systems, significantly contribute to users' trust, confidence, and satisfaction with digital payment platforms. Educational qualification, occupation, and monthly income were found to significantly influence users' awareness and perceptions of AI-based security features, whereas gender did not show a significant effect. Although users generally recognize the importance of AI-driven security mechanisms, awareness levels remain relatively moderate, highlighting the need for greater education and digital security literacy. Overall, AI plays a crucial role in strengthening digital payment security and fostering user confidence, thereby supporting the continued growth of digital payment adoption in Kerala.

Scope for Further Research

- Future studies may extend the research to other states in India for comparative analysis of AI-based digital payment security perceptions.
- A larger sample size may be used to improve the generalizability of the findings.
- Future research can examine the impact of specific AI technologies such as machine learning, behavioral analytics, and predictive fraud detection on user trust.
- Comparative studies between rural and urban digital payment users can provide deeper insights into awareness and adoption patterns.
- Researchers may employ Structural Equation Modeling (SEM) to examine complex relationships among awareness, trust, satisfaction, and usage intention.

Reference

- Agarwal, S., Malik, P., & Gautam, S. (2023). Analysis of customer satisfaction and the customer experience in digital payments: A meta-analysis review. *International Journal of Business Science and Applied Management*, 18(1), 1–17.
- Aljaradat, A., & Shukla, A. (2026). Cybersecurity, trust, and user behavior in digital payment systems: The moderating role of advanced technologies. *Discover Computing*.
- Aljaradat, A., & Shukla, S. (2026). Cybersecurity and trust formation in digital payment use behavior in North India. *Discover Sustainability*.
- Bach, T. A., Khan, A., Hallock, H., Beltrão, G., & Sousa, S. (2023). A systematic literature review of user trust in AI-enabled systems: An HCI perspective. *arXiv*.
- Gindre, F., & Ibarra, G. A. (2026). Security enhancement of FinTech platforms with artificial intelligence and blockchain: A systematic literature review. *Journal of Computer Science and Technology*.
- Jain, V., & Jain, N. (2024). From cash to clicks: A systematic review of digital payment adoption using the ADO framework. *Vision: The Journal of Business Perspective*.
- Khando, K., Islam, M. S., & Gao, S. (2023). The emerging technologies of digital payments and associated challenges: A systematic literature review. *Future Internet*, 15(1), 21.
- Nirmala, E., & Banumathy, K. (2026). Artificial intelligence in digital payment systems and its influence on consumer trust: A study in Chennai. *International Journal of Innovation Studies*.
- Nirmala, P., & Banumathy, K. (2024). The role of artificial intelligence in enhancing customer trust in digital payment systems. *International Journal of Intelligent Systems and Applications in Engineering*.
- Norbu, T., Park, J. Y., Wong, K. W., & Cui, H. (2024). Factors affecting trust and acceptance for blockchain adoption in digital payment systems: A systematic review. *Future Internet*, 16(3), 106.
- Rawat, S., Singh, P., & Verma, A. (2024). Consumer perception and adoption of digital payment methods: Trust and security perspectives. *KUEY Journal*.
- Sahi, G. K., Arora, M., & Dhameja, N. (2022). An exploratory inquiry of users' perceived risk and adoption of digital payment systems. *Future Internet*, 14(2), 32.
- Saini, A., & Sharma, R. (2023). Factors affecting consumer perception towards e-payment systems in India. *The Computer Science Journal*.
- Shree, S., Choudhary, S., & Kaur, P. (2021). Consumer adoption of digital payments in India: A study of trust and security perceptions. *Journal of Financial Services Marketing*, 26(1–2), 35–46.