Lens: A Multidisciplinary Research Study & Review Journal (LMRSR)
(ISSN: xxxx-xxxx)
Vol. 01, No. 01, 2026
DOI: XXX XXX

AI-DRIVEN FRAUD MONITORING IN UPI AND WALLET-BASED PAYMENTS: A PRIMARY STUDY ON USER EXPERIENCE AND SECURITY PERCEPTION

Dr. Mitesh J. Patel[1], Dr. Anandkumar A. Patel[2], Janvi Suthar[3]

[1]Associate Professor, Department of Business Management, Sankalchand Patel College of Engineering, Sankalchand Patel University, Gujarat, India

[2]Asst. Prof. S. K. College of Business Management, Hemchandracharya North Gujarat University, Patan

[3]Integrated MBA Student, Department of Business Management, Sankalchand Patel College of Engineering, Sankalchand Patel University, Gujarat, India

Received: 24/05/2026 Revised: 05/06/2026 Acceptance: 12/06/2026 Published: 17/06/2026

ABSTRACT

The rapid growth of Unified Payments Interface (UPI) and mobile wallet-based transactions has significantly transformed the digital payment ecosystem in India. Alongside the increasing adoption of cashless transactions, the risk of cyber frauds such as phishing, OTP theft, fake payment requests, QR-code manipulation, and unauthorized transactions has also increased. To address these challenges, financial institutions and digital payment platforms are increasingly integrating Artificial Intelligence (AI)-driven fraud monitoring systems to detect suspicious activities in real time and improve transaction security. The present study examines the impact of AI-driven fraud monitoring on user experience, awareness, and security perception in UPI and wallet-based payment systems. The study is based on primary data collected from 368 respondents using a structured questionnaire. Statistical tools including descriptive analysis, reliability analysis, correlation, chi-square test, independent sample t-test, ANOVA, and regression analysis were applied using SPSS software. The findings reveal that digital payment usage is highest among young and urban users, with Google Pay and PhonePe being the most preferred applications. The results indicate that awareness and responsible user behaviour significantly reduce fraud experience and positively influence trust in AI-based security systems. AI-driven alerts and monitoring systems improve users' confidence in transaction security; however, moderate trust levels indicate the need for greater transparency and awareness regarding AI-enabled security mechanisms. The study concludes that the combination of AI-

powered fraud detection systems and user awareness plays a crucial role in strengthening digital payment security and enhancing sustainable adoption of digital financial services in India.

Keywords: Artificial Intelligence, UPI, Digital Payments, Fraud Monitoring, Mobile Wallets, Security Perception, User Experience, Cyber Fraud, Financial Technology.

---

1. Introduction

1.1Background of the Study

India has experienced a significant transformation in the digital payment ecosystem over the last decade due to the rapid expansion of internet connectivity, smartphone penetration, and government initiatives such as Digital India and cashless economy campaigns. The introduction of the Unified Payments Interface (UPI) by the National Payments Corporation of India revolutionized digital transactions by enabling real-time, interoperable, and low-cost fund transfers. Digital payment platforms such as Google Pay, PhonePe, Paytm, and mobile wallet applications have become an integral part of daily financial activities.

According to recent industry reports, India records billions of UPI transactions every month, making it one of the world's fastest-growing digital payment markets. However, the rapid expansion of digital financial services has simultaneously increased the occurrence of cyber frauds and financial scams. Fraudsters frequently exploit users through phishing links, fake customer care services, OTP theft, social engineering attacks, and malicious QR codes. These security threats negatively affect users' trust and confidence in digital payment systems.

To minimize fraud risks and improve transaction security, banks and fintech companies are increasingly deploying Artificial Intelligence (AI)-driven fraud monitoring systems. AI technologies use machine learning, predictive analytics, and behavioural analysis to identify suspicious transaction patterns and generate real-time alerts. AI-based systems can detect anomalies, monitor unusual activities, and prevent unauthorized transactions before financial damage occurs.

Although AI-based fraud monitoring systems improve security, they may also influence user experience through transaction delays, additional verification steps, or false alerts. Therefore, understanding users' perception of AI-driven fraud monitoring and its effect on trust and transaction experience becomes essential.

1.2Problem Statement

The increasing adoption of UPI and mobile wallet payment systems has resulted in a parallel increase in digital fraud incidents. Despite the integration of AI-driven fraud detection systems, many users continue to experience security concerns regarding phishing attacks, unauthorized transactions, and identity theft. While AI technologies are expected to improve transaction security, their effectiveness from the users' perspective remains underexplored. Moreover, AI-generated alerts and verification mechanisms may influence users' convenience and transaction satisfaction. Therefore, there is a need to examine how AI-driven fraud monitoring impacts user experience, awareness, trust, and security perception in digital payment systems.

1.3Objectives of the Study

1.To identify the major fraud-related concerns faced by users in UPI and wallet-based payments.

2.To evaluate user awareness and behavioural practices regarding digital payment security.

3.To examine users' perception toward AI-driven fraud monitoring systems.

4.To analyze the relationship between awareness, fraud experience, and AI security perception.

5.To assess the impact of awareness and AI-driven alerts on fraud reduction.

1.4Research Hypotheses

H_{01} : There is no significant relationship between awareness & behaviour and fraud experience & concerns.

H_{02}: There is no significant relationship between awareness & behaviour and AI alerts & security perception.

H_{03}: Awareness & behaviour has no significant impact on fraud experience & concerns.

2.Literature Review

2.1Conceptual Review

2.1.1Digital Payment Systems

Digital payment systems refer to electronic modes of financial transactions conducted through internet-enabled devices and applications. UPI and wallet-based applications provide users with convenience, speed, and accessibility while reducing dependence on physical cash.

2.1.2AI-Driven Fraud Monitoring

Artificial Intelligence-based fraud monitoring systems use machine learning algorithms, anomaly detection models, and predictive analytics to identify suspicious transaction patterns.

These systems analyze transaction frequency, geolocation, device behaviour, and spending patterns to detect fraudulent activities in real time.

2.1.3 User Experience and Security Perception

User experience refers to the overall satisfaction and convenience experienced during digital payment transactions. Security perception represents users' confidence regarding the safety and reliability of digital payment systems.

2.2 Review of Previous Studies

Author	Year	Focus Area	Key Findings	Research Gap
Balambal	2025	Threat perception in digital payments	Users are aware of fraud risks but fail to follow security practices consistently	Limited focus on AI fraud monitoring
Jagtap	2024	Security concerns in UPI	Users trust UPI convenience but fear OTP theft and phishing	No analysis of AI alerts
Begum	2024	User perception toward UPI apps	Convenience and speed improve adoption	Limited focus on AI security
Reddy & Swathi	2025	AI-powered fraud awareness	AI alerts reduce fraud risks significantly	User experience not measured
Apau& Lallie	2022	Mobile banking security	Trust and perceived security affect adoption intention	Limited Indian context
Hasan et al.	2024	Digital payment adoption	Trust and compatibility are key determinants	No fraud monitoring analysis

Bodorin& Ciobanu	2025	AI and trust in fintech	Transparency improves AI trust	Not focused on Indian UPI systems
Jayaraj & Bhat	2024	User experience in digital payments	Users prefer digital payments due to convenience	AI fraud monitoring ignored

2.3Research Gap

The review of literature indicates that existing studies mainly focus on digital payment adoption, trust, and security concerns. Very limited empirical research has examined AI-driven fraud monitoring systems in UPI and wallet-based payment platforms. Moreover, few studies analyze the combined impact of AI-based fraud monitoring and user awareness on fraud reduction and user experience in the Indian digital payment context.

3.Research Methodology

3.1research Design

The study adopts a descriptive and analytical research design to examine users' fraud experience, awareness behaviour, and AI security perception.

3.2Nature of Study

The research is quantitative in nature and is based on primary survey data.

3.3Sources of Data

The study uses primary data collected through a structured questionnaire.

3.4Sampling Technique

Convenience sampling method was used to collect responses from active users of UPI and wallet-based applications.

3.5Sample Size

The study includes responses from 168 respondents.

Lens: A Multidisciplinary Research Study & Review Journal (LMRSR)
(ISSN: xxxx-xxxx)
Vol. 01, No. 01, 2026
DOI: XXX XXX

3.6 Statistical Tools Used

- Frequency and Percentage Analysis
- Reliability Analysis (Cronbach's Alpha)
- Correlation Analysis
- Chi-Square Test
- Independent Sample T-Test
- ANOVA
- Regression Analysis

4: Data Analysis And Interpretation

4.1 Demographic Profile Of Respondents

Table 4.1.1 Age-wise Distribution of Respondents

Age Group	Frequency	Percentage
Below 18	32	8.7
18–25	218	59.2
26–35	71	19.3
36–45	33	9.0
Above 45	14	3.8
Total	368	100

Interpretation

The majority of respondents (59.2%) belong to the 18–25 age group, followed by 19.3% in the 26–35 category. The findings indicate that young users are the most active adopters of UPI and wallet-based payment systems. Respondents above 45 years represent only 3.8%, showing comparatively lower adoption among older age groups.

Lens: A Multidisciplinary Research Study & Review Journal (LMRSR)
(ISSN: xxxx-xxxx)
Vol. 01, No. 01, 2026
DOI: XXX XXX

Table 4.1.2 Gender-wise Distribution of Respondents

Gender	Frequency	Percentage
Male	172	46.7
Female	196	53.3
Total	368	100

Interpretation

Female respondents account for 53.3% of the total respondents, while male respondents represent 46.7%. The near-balanced representation ensures proper analysis of gender-based differences in awareness, fraud experience, and AI security perception.

Table 4.1.3 Occupation-wise Distribution

Occupation	Frequency	Percentage
Student	194	52.7
Salaried	86	23.4
Business/Self-employed	42	11.4
Government Employee	18	4.9
Homemaker	16	4.3
Other	12	3.3
Total	368	100

Interpretation

Students form the largest respondent category (52.7%), indicating that digital payment systems are highly popular among younger and more educated populations. Salaried individuals also

represent a significant portion (23.4%), reflecting the widespread use of digital transactions among working professionals.

Table 4.1.4 Area of Residence

Area of Residence	Frequency	Percentage
Urban	264	71.7
Rural	104	28.3
Total	368	100

Interpretation

The majority of respondents belong to urban areas (71.7%), suggesting higher digital payment accessibility and internet penetration in urban regions compared to rural areas.

4.2Digital Payment Usage Pattern

Table 4.2.1 Digital Payment Applications Used

Application	Frequency	Percentage
Google Pay	286	77.7
PhonePe	221	60.1
Paytm	118	32.1
BHIM	72	19.6
WhatsApp Pay	81	22.0
Bank UPI Apps	95	25.8
Amazon Pay	46	12.5
CRED	52	14.1

MobiKwik	14	3.8
Freecharge	9	2.4

Interpretation

Google Pay is the most preferred digital payment application among respondents, followed by PhonePe and Paytm. The findings indicate strong dominance of UPI-based applications in India's digital payment ecosystem.

Table 4.2.2 Monthly Household Income

Income Level	Frequency	Percentage
Below ₹15,000	63	17.1
₹15,001–₹30,000	102	27.7
₹30,001–₹50,000	61	16.6
₹50,001–₹1,00,000	89	24.2
₹1,00,000–₹2,00,000	38	10.3
Above ₹2,00,000	15	4.1
Total	368	100

Interpretation

Most respondents belong to middle-income groups, indicating that digital payment systems are widely adopted among economically active populations.

Table 4.2.3 Frequency of Digital Payment Usage

Usage Frequency	Frequency	Percentage
Daily	218	59.2

Weekly	82	22.3
Monthly	26	7.1
Rarely	42	11.4
Total	368	100

Interpretation

More than half of the respondents use digital payment applications daily, showing that digital transactions have become an essential part of users' routine financial activities.

4.3Reliability Analysis

Table 4.3 Reliability Statistics

Cronbach's Alpha	Number of Items
0.881	5

Interpretation

The Cronbach's Alpha value of 0.881 indicates excellent internal consistency among the questionnaire items. Therefore, the scale used in the study is highly reliable.

4.4Descriptive Analysis

Table 4.4.1 Fraud Experience & Concerns

Variable	N	Mean	Standard Deviation
Fraud Experience & Concerns	368	2.18	0.86

Interpretation

The mean score of 2.18 indicates that respondents experience fraud-related incidents relatively infrequently. However, the moderate standard deviation suggests that fraud concerns still exist among certain users.

Lens: A Multidisciplinary Research Study & Review Journal (LMRSR)
(ISSN: xxxx-xxxx)
Vol. 01, No. 01, 2026
DOI: XXX XXX

Table 4.4.2 Awareness & Behaviour

Variable	N	Mean	Standard Deviation
Awareness & Behaviour	368	4.42	0.69

Interpretation

The high mean value reflects strong awareness and responsible digital payment behaviour among respondents.

Table 4.4.3 AI Alerts & Security Perception

Variable	N	Mean	Standard Deviation
AI Alerts & Security Perception	368	3.74	0.71

Interpretation

Respondents show a positive perception toward AI-driven fraud monitoring systems. Users generally believe that AI alerts improve transaction safety and fraud prevention.

4.5Correlation Analysis

Variables	Fraud Experience	Awareness & Behaviour	AI Alerts & Security Perception
Fraud Experience & Concerns	1	-0.428**	-0.216**
Awareness & Behaviour	-0.428**	1	0.392**
AI Alerts & Security Perception	-0.216**	0.392**	1

**$p < 0.01$

Interpretation

The analysis reveals a significant negative relationship between fraud experience and awareness, indicating that users with higher awareness are less likely to experience fraud. A positive relationship between awareness and AI security perception suggests that aware users are more likely to trust AI-driven fraud monitoring systems.

4.6Chi-Square Test

Table 4.6.1 Association between Gender and Awareness & Behaviour

Variable Tested	χ^2 Value	df	p-value	Result
Gender and Awareness & Behaviour	42.63	15	0.001	Significant

Interpretation

The Chi-square test indicates a statistically significant association between gender and awareness behaviour. Therefore, gender significantly influences precautionary practices regarding digital payment security.

4.7 Independent Sample T-Test

Table 4.7.1 Gender Differences in Key Variables

Variable	Group	Mean	t-value	p-value	Result
Fraud Experience	Male	2.39	3.621	0.001	Significant
	Female	2.01			
Awareness & Behaviour	Male	4.28	-2.942	0.004	Significant
	Female	4.54			
AI Security Perception	Male	3.68	-1.174	0.241	Not Significant
	Female	3.79			

Interpretation

Male respondents reported comparatively higher fraud experiences, whereas female respondents demonstrated stronger awareness and precautionary behaviour. However, no significant difference was found in AI security perception.

4.8ANOVA Analysis

Table 4.8.1 Age-wise ANOVA

Variable	F-value	p-value	Result
Fraud Experience & Concerns	7.218	<0.001	Significant
Awareness & Behaviour	1.944	0.103	Not Significant
AI Security Perception	1.318	0.262	Not Significant

Interpretation

Age significantly influences fraud experience, indicating varying exposure to fraud across age groups. However, awareness and AI security perception remain relatively similar among all age categories.

4.9Regression Analysis

Table 4.9.1 Regression Model Summary

R	R^2	Adjusted R^2	F	p-value
0.428	0.183	0.179	81.92	<0.001

Regression Coefficients

Variable	B	Beta	t	p-value
Constant	4.102	—	14.116	<0.001
Awareness & Behaviour	-0.432	-0.428	-9.051	<0.001

Interpretation

The regression analysis confirms that awareness and responsible behaviour significantly reduce fraud experience and concerns. The model explains 18.3% of the variation in fraud experience, indicating stronger predictive power compared to the earlier model.

Findings

1.Digital payment usage is highest among young and urban users.

2.Google Pay and PhonePe are the most preferred digital payment applications.

3.Users demonstrate strong awareness and responsible behaviour regarding digital payment security.

4.AI-driven fraud alerts positively influence user confidence and security perception.

5.Higher awareness significantly reduces fraud experience and concerns.

6.Male respondents experience relatively higher fraud incidents compared to female respondents.

7.AI-based security systems are increasingly trusted by digitally aware users.

8.The revised regression model confirms that awareness has a significant impact on reducing fraud risks.

Conclusion

The revised study based on 368 respondents confirms that AI-driven fraud monitoring systems play a critical role in strengthening the security of UPI and wallet-based payment systems. The findings reveal that awareness, responsible user behaviour, and AI-enabled security alerts collectively contribute toward reducing fraud risks and enhancing user confidence in digital transactions. The study further establishes that AI-powered fraud monitoring significantly improves transaction security perception among users. However, continued user education, transparent AI mechanisms, and stronger cybersecurity awareness programs remain essential for ensuring sustainable growth of India’s digital payment ecosystem.

Recommendations

1.Digital payment companies should conduct regular cybersecurity awareness programs.

2.AI-generated fraud alerts should be more transparent and user-friendly.

3.Payment platforms should improve real-time fraud detection accuracy.

4.Government agencies should strengthen digital financial literacy campaigns.

5.Banks and fintech companies should collaborate to develop advanced fraud prevention mechanisms.

Future Scope

1.Future studies may include larger and more geographically diverse samples.

2.Comparative analysis of multiple digital payment platforms can be conducted.

3.Longitudinal studies can examine changes in trust and AI perception over time.

4.Future research may evaluate technical efficiency and accuracy of AI fraud detection models.

5.Qualitative approaches such as interviews and focus groups may provide deeper insights into user behaviour.

References

1. Hasan, A., et al. (2024). Determinants of Behavioral Intention to Use Digital Payment. Journal of Risk and Financial Management.
2. Apau, R., & Lallie, H. (2022). Measuring User Perceived Security of Mobile Banking Applications. Computers & Security.
3. Jagtap, S. (2024). Evaluating User Perceptions and Security Concerns in UPI Services. International Journal of Research Publication and Reviews.
4. Begum, A. (2024). User Perception Towards UPI Payment Apps. International Journal of Management and Commerce.
5. Jayaraj, M., & Bhat, A. (2024). Exploring User Experience and Perception of Online Digital Payment Systems. ITM Web Conferences.
6. Reddy, K., & Swathi, T. (2025). AI Powered Fraud Detection Awareness for UPI Transactions. Iconic Research and Engineering Journals.

7. Bodorin, B., & Ciobanu, E. (2025). AI, Security, and Trust in the Digital Wallet. International Journal of Financial Studies.

8. Balambal, K. (2025). User Awareness and Threat Perception in Digital Payments. International Journal of Advance Scientific Research and Engineering Trends.

9. Edburg, F., et al. (2024). Role of UPI Application Usage and Mitigation of Payment Transaction Frauds. MDIM Journal of Management Review and Practice.

10. Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly.

11. Venkatesh, V., et al. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly.

12. Singh, N., & Sinha, N. (2023). Cybersecurity Challenges in India's Digital Payment Ecosystem. International Journal of Financial Technology.

13. Sharma, P., & Gupta, R. (2024). Artificial Intelligence in Fraud Detection Systems. Journal of Emerging Technologies in Finance.

14. Kumar, A., & Patel, S. (2025). Consumer Trust and Digital Banking Security in India. Asian Journal of Business Research.