International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Role of Artificial Intelligence in Detecting and Preventing Financial Scams in the Banking Sector

Dr. Richa Singhal[1], Dr. Anupam Gupta[2]

[1]Associate Professor, Department of EAFM, S. S. Jain Subodh PG College, Jaipur.
[2]Assistant Professor, Department of EAFM, S. S. Jain Subodh PG College, Jaipur.

Abstract

The rapid expansion of digital banking and online payment platforms has transformed the banking sector by making financial transactions faster and more accessible. India has witnessed a sharp rise in technology-enabled financial scams alongside the growth of UPI, mobile wallets, and app-based banking. Reports indicate a significant increase in digital payment frauds, phishing attacks, and UPI-related scams in recent years, raising serious concerns over consumer safety and trust (**The Economic Times, 2023)**[1]. This growing incidence of cyber-enabled fraud has compelled banks to rely increasingly on Artificial Intelligence (AI) for fraud detection and prevention. However, despite technological advancement, customer confidence in digital banking systems remains fragile (**Mint,2024)**[2].

This study examines the role of Artificial Intelligence in detecting and preventing financial scams in the banking sector, with a focus on customer perception and usage behaviour. The article covers major scams such as phishing and spoofing attacks, OTP and UPI frauds, fake banking applications, identity theft, and social engineering–based financial frauds that are frequently reported in Indian media (**The Times of India, 2023)**[3]. Primary data were collected from 50 online application users who regularly conduct financial transactions through scheduled interview and analysed through descriptive statistical methods.

The study concludes that AI-driven solutions must be complemented by robust regulatory frameworks, enhanced cybersecurity measures, and targeted financial literacy initiatives. Preventive measures such as advanced AI monitoring systems, multi-factor authentication, and continuous user awareness programs are suggested to strengthen customer confidence in digital banking systems.

Keywords: Artificial Intelligence, Financial Scams, Digital Banking, Fraud Detection, Cybersecurity, Online Payment Systems, Financial Literacy Initiatives.

Emerging Financial Scams in the Banking Sector

Indian media reports highlight that cybercriminals increasingly target users of UPI platforms, mobile banking applications, and digital wallets, particularly first-time users and senior citizens (**The Economic Times, 2024)**[4]. The ease of real-time fund transfers and widespread smartphone usage have further intensified exposure to digital fraud.

Phishing and Spoofing Attacks- Phishing and spoofing attacks continue to dominate digital banking fraud cases, with fraudsters using fake emails, SMS alerts, and spoofed caller IDs to impersonate banks. Such deceptive practices have significantly reduced users' ability to distinguish between genuine and fraudulent

communications (**The Hindu, 2023**)[5].

OTP and UPI Frauds- OTP- and UPI-based frauds have increased sharply due to the real-time nature of instant payment systems. Several cases reported in the financial press indicate that users are often tricked into sharing OTPs or approving fraudulent collect requests, leading to immediate financial losses (**Mint, 2024**)[6].

Fake Banking Applications and Identity Theft- Cybercriminals have also developed counterfeit banking applications resembling official apps, resulting in identity theft and unauthorized transactions. Such incidents have been widely reported in the mainstream press, highlighting serious data security concerns (**The Times of India, 2023**)[3].

Social Engineering–Based Frauds-Social engineering–based frauds exploit emotional triggers such as fear, urgency, or trust. Fake customer-care calls and investment scams relying on psychological manipulation have been frequently reported in the Indian press (**The Economic Times, 2024**)[4].

Role of Artificial Intelligence in Fraud Detection and Prevention

Indian banks and fintech firms are increasingly deploying AI-driven fraud detection systems to counter the rising sophistication of cybercrime. Media reports indicate growing investment in machine learning, behavioural analytics, and real-time transaction monitoring to enhance fraud prevention capabilities (**Mint, 2024**)[7].

Machine learning algorithms analyse large volumes of transaction data to detect abnormal behaviour, while Natural Language Processing (NLP) is used to identify phishing emails and scam messages by analysing deceptive language patterns

Real-Time Transaction Monitoring- AI-powered systems enable real-time monitoring of millions of transactions simultaneously. Suspicious transactions can be blocked or flagged instantly, preventing financial losses before they occur.

Behavioural Analytics- Behavioural analytics assess user behaviour patterns such as typing speed, device usage, and transaction habits. Any deviation from normal behaviour can trigger alerts for further verification.

Natural Language Processing- NLP is used to detect fraudulent communications, including phishing emails and scam messages, by analyzing language patterns and identifying deceptive content.

Research Methodology

The present study adopts a descriptive and analytical research design, combining conceptual discussion with primary data collected through scheduled interviews to examine user perception of AI-enabled digital banking systems and experiences with financial scams. The study is based on a sample of 50 respondents who actively use online banking applications, UPI platforms, and mobile wallets, selected through convenience sampling to ensure representation across different age groups, occupations, and levels of digital literacy. Primary data were gathered through structured scheduled interviews conducted face-to-face or via telephonic/video calls, focusing on the frequency of digital transactions, awareness of AI-based fraud detection systems, experiences with online scams, trust in digital banking, and preference for cash versus digital payments. The interview-based approach facilitated in-depth interaction, clarification of responses, and enhanced reliability of the collected data. The data were coded and analyzed using descriptive statistical tools such as percentages, frequency distribution, and comparative analysis, with findings presented through tables for effective interpretation.

Objectives of the Study

1. To study the level of awareness of AI-based fraud detection systems among digital banking users.
2. To examine customer experience with financial scams and its impact on digital banking usage.
3. To analyze customer trust in AI-enabled digital banking systems.

Data Analysis and Findings

The analysis of data collected through scheduled interviews provides valuable insights into user behaviour and perception regarding AI-enabled digital banking systems.

Objective 1: To study the level of awareness of AI-based fraud detection systems among digital banking users.

Table 1: Awareness of AI-Based Fraud Detection Systems (n = 50)

Awareness Level	Number of Respondents	Percentage (%)
High Awareness	18	36%
Moderate Awareness	20	40%
Low Awareness	12	24%
Total	**50**	**100%**

Interpretation:

The findings presented in Table 1 indicate that awareness of AI-based fraud detection systems among digital banking users is moderate to low. While 36 per cent of respondents reported high awareness, a substantial proportion either possessed moderate (40 per cent) or low awareness (24 per cent) regarding the role of Artificial Intelligence in safeguarding digital transactions. This clearly fulfils Objective 1, which aimed to assess the level of awareness of AI-driven fraud prevention mechanisms among users.

In the present digital banking environment, limited awareness restricts customers' ability to fully trust and utilize AI-enabled security features, thereby weakening confidence in digital payment systems. As digital frauds continue to rise, insufficient understanding of protective technologies may increase user vulnerability.

Recommendation:

Banks should adopt proactive communication strategies, including in-app notifications, awareness campaigns, and simplified disclosures explaining AI-based security mechanisms. Financial literacy initiatives focusing on digital safety and AI-enabled protections should be integrated into customer onboarding processes.

Objective 2: To examine customer experience with financial scams and its impact on digital banking usage.

Table 2: Experience with Financial Scams and Transaction Preference

Experience with Online Fraud	Prefer Digital Transactions	Prefer Cash Transactions	Total
Yes (Experienced/Witnessed)	10	18	28
No	16	6	22

Experience with Online Fraud	Prefer Digital Transactions	Prefer Cash Transactions	Total
Total	**26**	**24**	**50**

Interpretation:

Table 2 highlights a strong relationship between customer experience with financial scams and their preferred mode of transaction. Among respondents who had experienced or witnessed online fraud, a higher inclination towards cash transactions was observed, whereas respondents with no prior fraud exposure showed greater preference for digital transactions. This analysis successfully fulfils Objective 2, which sought to examine the impact of financial scam experiences on digital banking usage behaviour.

In the present scenario, the growing incidence of cyber frauds has contributed to a visible trust deficit in digital banking platforms. The shift towards cash transactions among affected users reflects psychological fear and perceived insecurity, posing a challenge to India's vision of a cashless economy.

Recommendation:

Banks should strengthen post-fraud grievance redressal mechanisms and offer quick resolution and compensation frameworks. Transparent communication about fraud prevention and recovery processes can help restore customer confidence and reduce the tendency to revert to cash-based transactions.

Objective 3: To analyze customer trust in AI-enabled digital banking systems

Table 3: Level of Trust in AI-Enabled Digital Banking Systems

Level of Trust	Number of Respondents	Percentage (%)
High Trust	14	28%
Moderate Trust	21	42%
Low Trust	15	30%
Total	**50**	**100%**

Interpretation:

Table 3 reveals that although Artificial Intelligence has enhanced fraud detection capabilities, customer trust in AI-enabled digital banking systems remains moderate. Only 28 per cent of respondents expressed high trust, while a significant proportion reported moderate (42 per cent) or low trust (30%). This outcome fulfils Objective 3, which aimed to analyze the level of customer trust in AI-driven digital banking systems.

In the current digital ecosystem, trust is a critical determinant of technology adoption. The findings suggest that technological advancement alone is insufficient to ensure widespread acceptance of AI-based systems. Customers require assurance regarding transparency, accountability, and regulatory oversight.

Recommendation:

Banks and regulators should jointly work towards improving transparency in AI decision-making processes. Regular customer education programs, visible regulatory guidelines, and the implementation of multi-factor authentication can significantly enhance trust and encourage sustained adoption of digital banking services.

Findings of the Study

The findings of the study reveal important insights into customer awareness, experience, and trust related to Artificial Intelligence–enabled fraud detection systems in the banking sector. Firstly, the study finds that awareness regarding AI-based fraud detection mechanisms among digital banking users is only moderate. Although some respondents were familiar with AI tools used by banks to monitor suspicious transactions, a significant proportion lacked clear understanding of how these systems function. This limited awareness reduces customers' confidence in digital banking security despite technological advancements.

Secondly, the study observes a strong association between experience with financial scams and transaction preferences. Respondents who had experienced or witnessed incidents such as phishing, OTP fraud, or UPI-related scams exhibited a noticeable preference for cash transactions over digital modes. This shift indicates a trust deficit arising from fear of financial loss and inadequate understanding of protective mechanisms, thereby hindering the adoption of cashless banking.

Thirdly, the findings highlight that customer trust in AI-enabled digital banking systems remains moderate. While respondents acknowledged the role of AI in improving fraud detection, concerns regarding transparency, accountability, and data security persisted. Overall, the findings suggest that although AI has strengthened fraud prevention capabilities, technological solutions must be supported by enhanced awareness, regulatory assurance, and financial literacy initiatives to build sustained customer trust in digital banking systems. These interview findings mirror wider public concerns reported in Indian newspapers, where users affected by digital frauds increasingly express declining trust in online banking platforms **(The Times of India, 2023)**[8]. Financial news analyses also emphasize that insufficient understanding of AI-based fraud prevention systems continues to contribute to this trust gap.

RBI Circulars and India-Specific Regulatory Framework

India's central banking regulator, the Reserve Bank of India (RBI), has issued multiple formal circulars and directions to strengthen fraud risk management in the context of digital banking and emerging technologies. These regulatory measures emphasize robust authentication mechanisms, proactive fraud risk governance, cybersecurity standards, and the use of technology-enabled systems to combat financial scams.

One key regulatory mandate is the RBI's directive on digital domains and cybersecurity standards for banks. In its circular dated April 22, 2025, the RBI stated:

"It has now been decided to operationalise the '.bank.in' domain for banks … to serve as the exclusive registrar for this domain" **with the objective of "strengthening the cybersecurity framework and enhancing public confidence in digital banking and payment systems." (India Today)**[9]

To address authentication vulnerabilities that contribute to online fraud, the regulator issued the Reserve Bank of India (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025 (effective April 1, 2026). The RBI's circular states explicitly:

"All Payment System Providers and Payment System Participants, including banks and non-bank entities, shall ensure compliance with these directions by April 01, 2026 … [and] digital payments must now be secured by at least two distinct factors of authentication." **(The Economic Times)**[10]

Further, the RBI has reinforced broader fraud risk governance in banks through its Master Directions on Fraud Risk Management in Commercial Banks and All India Financial Institutions (effective 15 July 2024). These directions mandate that regulated entities establish Board-approved fraud risk management

policies, integrate Early Warning Signals (EWS) and Red Flagging mechanisms into core banking systems, and set up Data Analytics and Market Intelligence Units to detect suspicious transactions promptly. **(static.ixambee.com)**[11]

To strengthen digital payment resilience beyond banks, the RBI also issued Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-Bank Payment System Operators (effective 30 July 2024), laying out baseline cyber risk management measures, incident response protocols, and vendor risk requirements for non-bank payment platforms. **(TaxGuru)**[12]

Overall, these regulatory instruments reflect the RBI's policy direction toward integrating technology-driven safeguards, risk-based authentication mechanisms, and institutional fraud governance standards to support secure digital financial ecosystems in India.

Conclusion

Artificial Intelligence has emerged as a powerful tool in detecting and preventing financial scams in the banking sector. AI-driven systems offer real-time monitoring, predictive capabilities, and adaptive learning that significantly enhance fraud management. However, the study reveals that customer trust remains a critical challenge, with many users perceiving cash transactions as more reliable than digital alternatives.

The study concludes that the successful deployment of AI in banking fraud prevention requires a holistic approach that integrates advanced technology, strong regulatory frameworks, and sustained customer awareness initiatives. By addressing both technological and behavioural dimensions, banks can strengthen trust and ensure secure and inclusive digital financial systems.

The proactive measures undertaken by the Reserve Bank of India, including enhanced authentication standards and fraud risk governance, are vital in strengthening the digital banking ecosystem. Building customer trust through transparency, awareness, and regulatory assurance is essential for the sustainable and secure growth of digital banking in India.

References

1. The Economic Times. (2023, November 18). *Digital payment frauds rise as cybercriminals target UPI users*. The Economic Times. https://economictimes.indiatimes.com
2. Mint. (2024, May 10). *Why customer awareness is key to preventing online banking scams*. Mint. https://www.livemint.com
3. The Times of India. (2023, December 14). *Fake banking apps and OTP scams trap digital payment users*. The Times of India. https://timesofindia.indiatimes.com
4. The Economic Times. (2024, February 5). *How artificial intelligence is helping banks fight sophisticated financial frauds*. The Economic Times. https://economictimes.indiatimes.com
5. The Hindu. (2023, October 9). *Phishing and online banking frauds pose growing threat to digital users*. The Hindu. https://www.thehindu.com
6. Mint. (2024, April 3). *UPI frauds and the trust deficit in India's digital payments ecosystem*. Mint. https://www.livemint.com
7. Mint. (2024, May 10). *Why customer awareness is key to preventing online banking scams*. Mint. https://www.livemint.com
8. The Times of India. (2024, February 28). *Online banking frauds push users back to cash transactions*. The Times of India. https://timesofindia.indiatimes.com

9. Reserve Bank of India (RBI). (2025, April 22). *Circular on operationalising ".bank.in" domain to strengthen cybersecurity and enhance public confidence.* (India Today)
10. Reserve Bank of India (RBI). (2025). *Reserve Bank of India (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025.* (The Economic Times)
11. Reserve Bank of India (RBI). (2024, July 15). *Master Directions on Fraud Risk Management in Commercial Banks and All India Financial Institutions.* (static.ixambee.com)
12. Reserve Bank of India (RBI). (2024, July 30). *Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-Bank Payment System Operators (PSOs).* (TaxGuru)