Journal of Artificial Intelligence in Business
Volume 1, Issue 1 | July - September 2026 | www.journalindiapublication.com | 2026 Journal India Publication

Artificial Intelligence in Banking Fraud Detection: The Role of Accuracy, Real-Time Detection and False-Positive Management

*Likitha B**

ABSTRACT

Purpose. This study examines the perceived effectiveness of artificial intelligence (AI)-based fraud detection systems in banking, focusing on real-time detection, false positives, customer experience and detection accuracy.

Design/methodology/approach. The study adopts a descriptive, cross-sectional survey design using primary data from 85 respondents who regularly use digital banking services. Descriptive statistics, correlation analysis and regression analysis were used to examine relationships among the study variables. The source manuscript also reports ANOVA, although the complete ANOVA output is not provided.

Findings. The reported correlation matrix indicates positive associations between overall effectiveness and accuracy ($r = 0.352$), real-time detection ($r = 0.114$), false positives ($r = 0.129$) and customer experience ($r = 0.020$). The source manuscript reports that accuracy is the only factor with a statistically significant effect on perceived effectiveness. It also reports that false positives negatively affect customer experience.

Originality/value. The study provides exploratory evidence from digital-banking users on the factors shaping perceived effectiveness of AI-enabled fraud detection. It highlights accuracy as the central performance dimension while emphasising the need to balance fraud prevention with customer convenience and false-alert management.

Keywords: artificial intelligence; fraud detection; banking; machine learning; real-time detection; false positives; customer experience; accuracy; digital banking

* *Corresponding Author: Assistant Professor, Department of commerce, Millenium city commerce evening college, Bengaluru, India [Email: likithab7154@gmail.com]*

JOURNAL India Publication
Journal of Artificial Intelligence in Business
Volume 1, Issue 1 | July - September 2026 | www.journalindiapublication.com | 2026 Journal India Publication

1. Introduction

The rapid expansion of digital banking has transformed the way customers access and use financial services. Mobile banking, internet banking, cards, UPI and digital wallets have increased transaction speed and convenience, but the same digital environment has expanded the surface available for fraud, including unauthorised transactions, identity theft, phishing and other cyber-enabled attacks. The growth and diversification of fraud require financial institutions to continuously strengthen monitoring and detection capabilities [1–4].

Artificial intelligence has become an important component of modern fraud-management systems because machine-learning models can analyse large volumes of transactional data, identify patterns and flag anomalous behaviour. Compared with conventional rule-based systems, data-driven approaches can adapt to changing patterns and can support near-real-time decision-making [1,2,6].

However, the effectiveness of an AI fraud-detection system is not determined solely by its ability to identify suspicious transactions. Excessive false positives can inconvenience legitimate customers, while delays in detection can increase exposure to losses. Accuracy, speed and customer experience must therefore be considered together when assessing the effectiveness of AI-based fraud prevention [3–5].

Against this background, this study investigates how digital-banking users perceive AI-based fraud detection, with specific attention to real-time detection, false positives, customer experience and accuracy.

Journal of Artificial Intelligence in Business
Volume 1, Issue 1 | July - September 2026 | www.journalindiapublication.com | 2026 Journal India Publication

2. Problem Statement

Despite increasing use of AI in banking, fraud continues to evolve through new transaction patterns, social-engineering techniques and cyber threats. Conventional rules may struggle with novel patterns, while overly sensitive AI systems may generate false alerts and inconvenience genuine customers. The challenge for banks is therefore to achieve high detection capability without compromising customer experience. The source study identifies limited empirical evidence concerning how users perceive these dimensions in the Indian banking context.

The study therefore addresses the following problem: which characteristics of AI-based fraud detection are most strongly associated with perceived effectiveness among users of digital banking services?

3. Objectives

1. To examine the relationship between real-time detection and the perceived effectiveness of AI-based fraud detection.

2. To examine the relationship between false positives and the perceived effectiveness of AI-based fraud detection.

3. To assess the relationship between customer experience and perceived effectiveness.

4. To determine whether detection accuracy is significantly associated with perceived effectiveness.

5. To provide practical recommendations for improving AI-based fraud detection while maintaining customer convenience.

4. Hypotheses

H01: Real-time detection has no statistically significant relationship with perceived effectiveness.

H02: False positives have no statistically significant relationship with perceived effectiveness.

Journal of Artificial Intelligence in Business
JOURNAL India Publication
Volume 1, Issue 1 | July - September 2026 | www.journalindiapublication.com | 2026 Journal India Publication

H03: Customer experience has no statistically significant relationship with perceived effectiveness.

H04: Accuracy has no statistically significant relationship with perceived effectiveness.

5. Literature Review

AI and financial fraud detection. Ngai et al. [3] provide a broad review of data-mining approaches used in financial fraud detection and demonstrate the importance of classification and pattern-recognition techniques. Phua et al. [4] similarly establish the breadth of data-mining methods used in fraud detection and identify the continuing challenge of detecting evolving fraudulent behaviour.

Machine learning and accuracy. Ala'raj and Abbod [1] compare machine-learning and artificial-neural-network approaches for financial-fraud prediction, illustrating the relevance of model selection and predictive performance. Research on hybrid AI approaches further emphasises the importance of improving detection accuracy in complex financial environments [6].

False positives and customer experience. Fraud detection systems must distinguish genuine transactions from fraudulent ones without generating excessive false alerts. Credit-card fraud research demonstrates the value of combining classification techniques to improve detection performance [5,9]. From a banking-service perspective, false positives may also affect customer trust and satisfaction because legitimate transactions can be delayed or blocked.

Real-time fraud detection. Streaming fraud-detection architectures demonstrate how transaction monitoring can be performed at scale and with low latency [7]. This is particularly relevant to digital banking, where fraud prevention often requires intervention while a transaction is still in progress.

Research gap. Existing literature provides extensive technical evidence on fraud-detection algorithms, but fewer exploratory studies integrate technical performance dimensions with customer perceptions of AI-enabled fraud detection. The present study addresses this gap by

Journal of Artificial Intelligence in Business
Volume 1, Issue 1 | July - September 2026 | www.journalindiapublication.com | 2026 Journal India Publication

examining accuracy, real-time detection, false positives and customer experience within a single empirical framework.

6. Research Methodology

6.1 Research Design

The study follows a descriptive, cross-sectional research design. Primary data were collected through a structured questionnaire, supported by secondary literature on AI and fraud detection. Because the design is cross-sectional and perception-based, the findings should be interpreted as associations and respondent perceptions rather than direct measures of banks' algorithmic performance.

6.2 Data Collection and Sample

The questionnaire was distributed to 85 respondents who regularly use digital banking services, including mobile banking, internet banking, debit cards and UPI. Convenience sampling was used because respondents were selected based on availability and willingness to participate. This approach is suitable for exploratory analysis but limits the generalisability of the findings.

6.3 Variables

Perceived effectiveness of AI-based fraud detection is the dependent variable. The independent variables are real-time detection, false positives, customer experience and accuracy.

6.4 Statistical Tools

Descriptive statistics were used to summarise respondent perceptions. Pearson correlation was used to examine associations among the study variables. Multiple regression was used to identify the relative contribution of the independent variables to perceived effectiveness. ANOVA was reported in the original methodology, but complete ANOVA results are not available in the source document.

Journal of Artificial Intelligence in Business
Volume 1, Issue 1 | July - September 2026 | www.journalindiapublication.com | 2026 Journal India Publication

6.5 Decision Rule

Statistical significance is assessed at the 5% level. A p-value below 0.05 indicates evidence against the corresponding null hypothesis. A correlation coefficient without an associated p-value or confidence interval is not, by itself, sufficient to establish statistical significance.

7. Results and Analysis

7.1 Descriptive Findings

The source manuscript reports that respondents generally perceive AI-based fraud detection as effective. Accuracy received the highest mean score among the studied dimensions, indicating that respondents regard correct identification of fraudulent and legitimate transactions as particularly important. The source also reports that real-time detection contributes to early identification of suspicious transactions and that false positives can negatively affect customer experience.

7.2 Correlation Analysis

Variable	Effectiveness	Real-time detection	False positives	Customer experience	Accuracy
Effectiveness	1.000	0.114	0.129	0.020	0.352
Real-time detection	0.114	1.000	0.389	0.488	0.377
False positives	0.129	0.389	1.000	0.368	0.472
Customer experience	0.020	0.488	0.368	1.000	0.262
Accuracy	0.352	0.377	0.472	0.262	1.000

The displayed correlation matrix shows the strongest association with overall effectiveness for accuracy ($r = 0.352$), followed by false positives ($r = 0.129$), real-time detection ($r = 0.114$) and customer experience ($r = 0.020$). The correlations among the independent variables are moderate,

Journal of Artificial Intelligence in Business
Volume 1, Issue 1 | July - September 2026 | www.journalindiapublication.com | 2026 Journal India Publication

with the highest being between real-time detection and customer experience (r = 0.488) and between false positives and accuracy (r = 0.472).

Because the source document does not provide correlation p-values, the numerical correlations should be described as associations rather than individually classified as statistically significant or insignificant unless the original statistical output confirms those tests.

7.3 Regression Analysis

The source manuscript reports that accuracy is the only independent variable with a statistically significant effect on overall effectiveness, while real-time detection, false positives and customer experience show weak or non-significant effects. This finding supports the interpretation that the perceived correctness of fraud classification is more important than speed or convenience alone.

The result should nevertheless be interpreted cautiously because the complete regression table—model R^2, adjusted R^2, coefficients, standard errors, t-statistics and p-values—is not included in the source document. The final submission should insert the complete regression output so that readers can independently evaluate model fit and hypothesis decisions.

7.4 Hypothesis Evaluation

Hypothesis	Reported evidence	Decision
H01: Real-time detection	Reported as weak/non-significant in regression	Do not reject H01, subject to verification of regression p-value
H02: False positives	Reported as weak/non-significant for effectiveness	Do not reject H02, subject to verification of regression p-value
H03: Customer experience	Reported as weak/non-significant for effectiveness	Do not reject H03, subject to verification of regression p-value

Journal of Artificial Intelligence in Business
Volume 1, Issue 1 | July - September 2026 | www.journalindiapublication.com | 2026 Journal India Publication

H04: Accuracy	Reported as statistically significant predictor	Reject H04, subject to verification of regression p-value

The hypothesis decisions above follow the statistical interpretation reported in the source manuscript. They should be checked against the complete regression output before journal submission.

8. Discussion

The central finding is that accuracy is the most important reported predictor of perceived AI fraud-detection effectiveness. This is theoretically plausible because a fraud-detection system creates value only when it can distinguish suspicious activity from legitimate transactions with sufficient reliability. Existing research on machine learning and financial fraud detection similarly emphasises predictive accuracy and model performance [1,3,6].

The study also highlights the tension between security and customer convenience. False positives may protect against some risks by triggering additional verification, but repeated incorrect alerts can inconvenience legitimate users and undermine trust. Technical fraud-detection research therefore needs to be complemented by customer-experience considerations.

Real-time detection is also operationally important because digital transactions can be completed within seconds. Streaming approaches demonstrate the feasibility of large-scale, low-latency fraud monitoring [7]. However, speed without adequate accuracy can increase false alerts. The practical objective is therefore not maximum speed alone, but timely and accurate intervention.

The findings reinforce the need for a balanced fraud-management architecture in which accuracy, latency, false-positive control and customer communication are managed together.

9. Practical Implications

9.1 Implications for Banks

Banks should prioritise continuous model monitoring and retraining so that fraud-detection systems can adapt to emerging patterns. Model evaluation should include precision, recall, false-positive rates and customer-impact measures rather than relying on a single accuracy metric. Streaming and real-time architectures can support rapid intervention, while human review can be retained for high-risk or ambiguous cases [7].

9.2 Implications for Customer Experience

Banks should reduce unnecessary transaction blocks by using risk-based authentication and graduated interventions. Clear customer notifications and rapid resolution channels can reduce frustration when legitimate transactions are flagged.

9.3 Implications for Governance and Ethics

AI fraud systems should be subject to appropriate governance, monitoring and validation. Banks should document model performance, monitor bias and ensure that automated decisions can be reviewed when customers dispute an alert. Greater transparency can support trust while maintaining security.

10. Limitations and Future Research

The study has several limitations. First, the sample consists of only 85 respondents selected through convenience sampling, limiting generalisability. Second, the dependent variable is perceived effectiveness rather than an objective bank-level fraud metric such as precision, recall, fraud-loss reduction or false-positive rate. Third, the source document does not provide the complete regression and ANOVA outputs, limiting independent verification of statistical significance. Fourth, the study does not distinguish among different AI techniques or banking institutions.

Journal of Artificial Intelligence in Business
Volume 1, Issue 1 | July - September 2026 | www.journalindiapublication.com | 2026 Journal India Publication

Future research should use larger and more representative samples and combine customer-survey data with actual bank-level fraud-detection performance metrics. Comparative studies could evaluate machine learning, deep learning, graph-based models and hybrid systems. Longitudinal research could also examine how model performance changes as fraud patterns evolve.

11. Conclusion

This study examined the perceived effectiveness of AI-based fraud detection in banking through four dimensions: real-time detection, false positives, customer experience and accuracy. The reported findings identify accuracy as the strongest and statistically significant predictor of perceived effectiveness, while the other dimensions show weaker relationships.

The study therefore suggests that banks should not evaluate AI fraud detection solely on the basis of speed or the number of alerts generated. Effective systems must accurately distinguish fraudulent from legitimate activity while controlling false positives and maintaining a satisfactory customer experience. Continuous model improvement, real-time monitoring, risk-based intervention and strong governance can help banks achieve this balance.

The findings provide useful exploratory evidence, but stronger conclusions require larger samples, objective performance measures and complete statistical reporting. The study should consequently be positioned as an empirical perception-based investigation rather than as proof of the technical superiority of any specific AI algorithm.

References

[1] Ala'raj, M. and Abbod, M. (2020), “Predicting financial fraud using artificial neural networks and machine learning techniques: A comparative study”, Journal of Financial Crime, Vol. 27 No. 4, pp. 1253–1274.

[2] Bhatnagar, R. and Sharma, A. (2021), "Artificial intelligence in banking fraud detection: A review of machine learning approaches", International Journal of Information Management, Vol. 56, 102–118.

[3] Ngai, E.W.T., Hu, Y., Wong, Y.H., Chen, Y. and Sun, X. (2011), "The application of data mining techniques in financial fraud detection: A classification framework and an academic review", Decision Support Systems, Vol. 50 No. 3, pp. 559–569.

[4] Phua, C., Lee, V., Smith, K. and Gayler, R. (2010), "A comprehensive survey of data mining-based fraud detection research", Artificial Intelligence Review, Vol. 34 No. 4, pp. 489–530.

[5] Sahin, Y. and Duman, E. (2012), "Detecting credit card fraud by decision trees and support vector machines", Expert Systems with Applications, Vol. 39 No. 1, pp. 513–518.

[6] Zhang, Y., Teng, Y., Yu, F. and Guo, L. (2022), "Improving accuracy in financial fraud detection through hybrid AI models", Expert Systems with Applications, Vol. 195, 116652.

[7] Carcillo, F., Dal Pozzolo, A., Le Borgne, Y.A., Caelen, O., Mazzer, Y. and Bontempi, G. (2019), "SCARFF: A scalable framework for streaming credit card fraud detection with Spark", Information Fusion, Vol. 53, pp. 284–294.

[8] Kou, Y., Lu, C.-T., Sirwongwattana, S. and Huang, Y.-P. (2004), "Survey of fraud detection techniques", Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Vol. 3, pp. 2521–2526.

[9] Bhattacharyya, S., Jha, S., Tharakunnel, K. and Westland, J.C. (2011), "Data mining for credit card fraud: A comparative study", Decision Support Systems, Vol. 50 No. 3, pp. 602–613.

[10] Arora, S. and Raju, R. (2021), "Customer perception and acceptance of AI-based fraud detection systems in digital banking", Journal of Banking and Financial Technology, Vol. 5 No. 2, pp. 125–138.