Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

AI-Driven Banking Technologies and Their Effectiveness in Improving Fraud Detection Mechanisms in Digital Banking Services

Poonam Saini[1], Arjun Khateek[2]

[1]Research Scholar, Banking and Business Economics Department, UCCMS, MLSU, Udaipur
[2]Research Scholar, Accountancy and Business Statistics Department

Abstract:
The growing expansion of digital banking has increased the need for stronger fraud detection mechanisms that can respond to complex and fast-moving transaction risks. In this context, AI-driven banking technologies have gained importance for their ability to support transaction monitoring, real-time alerts, suspicious activity identification, and customer confidence in digital banking security. The present study examines the effectiveness of AI-driven tools and systems in improving fraud detection mechanisms in digital banking services. The study followed a quantitative approach and used a structured questionnaire based on fifteen Likert-scale statements covering five dimensions of AI-enabled fraud detection. Data were collected from 318 digital banking users and analysed through descriptive statistics, reliability analysis, one-sample t-test, and one-way ANOVA. The findings indicate that respondents generally perceived AI-driven banking technologies as effective in strengthening fraud detection mechanisms. The overall effectiveness score was above the neutral level, and the hypothesis testing results showed a significant difference in respondents' perceptions. The results also revealed significant perception differences across age groups, with younger respondents reporting more favourable views. The study contributes to understanding user perceptions of AI-enabled fraud detection and offers practical relevance for banks seeking to improve digital banking security, customer trust, and fraud monitoring systems.

Keywords: AI-Driven Banking, Fraud Detection, Digital Banking Security, Artificial Intelligence in Finance, Customer Trust

INTRODUCTION

Artificial Intelligence and Fraud Detection in Digital Banking

Digital banking has transformed the way customers access financial services, making transactions faster and more convenient and increasingly reliant on technology-based platforms. With this growth, however, the risk of digital fraud has also become more complex. Fraudulent activities in digital banking may occur through suspicious transaction behaviour, unauthorised access, abnormal account activity, and misuse of digital payment channels. These challenges have encouraged banks to adopt more advanced technological mechanisms that can detect fraud-related risks with greater speed and accuracy.

Artificial intelligence has emerged as an important technological support in the banking sector because of its ability to process large volumes of transaction data, identify unusual patterns, and assist in the early detection of suspicious activity. AI-driven tools can support banks through transaction monitoring, fraud alert generation, risk identification, and security-based decision support. In digital banking services, these systems are particularly relevant because fraud detection often requires timely recognition of abnormal behaviour and quick response mechanisms. As a result, AI-enabled banking technologies are increasingly viewed as useful tools for strengthening fraud detection processes.

The importance of AI-driven fraud detection is also linked to customer confidence in digital banking. Customers are more likely to trust digital banking platforms when they believe that banks have effective systems to monitor transactions, detect suspicious activities, and respond to possible fraud. However, customer perception may not be uniform across all user groups. Differences in digital banking experience, technology familiarity, and comfort with AI-based systems may influence how users evaluate the effectiveness of such technologies. Therefore, examining user perception becomes important for understanding the practical acceptance of AI-enabled fraud detection mechanisms.

The present study focuses on AI-driven banking technologies and their perceived effectiveness in improving fraud detection mechanisms in digital banking services. It considers broad dimensions such as AI-based transaction monitoring, real-time fraud alert and detection, suspicious activity identification, accuracy and efficiency of AI fraud detection, and customer trust in AI-driven fraud detection. The study seeks to analyse whether digital banking users perceive AI-driven tools and systems as effective in strengthening fraud detection and whether such perceptions differ across age groups.

REVIEW OF LITERATURE

(Yaseen & Al-Amarneh, 2025) examined the adoption of AI-driven fraud detection in banking with specific attention to trust, transparency and fairness perceptions among financial institutions in the United Arab Emirates and Qatar. The study focused on how institutional confidence in AI systems is influenced not only by detection capability but also by explainability and perceived fairness. Its findings indicated that transparent and trusted AI mechanisms are important for wider acceptance of fraud detection systems in banking. The study is directly relevant to the present research because customer trust and confidence in AI-driven fraud detection form one of the key dimensions of perceived effectiveness in digital banking services.

(AbouGrad & Sankuru, 2025) proposed an online banking fraud detection model based on a decentralised machine learning framework. The study used deep autoencoders and evaluated the model on credit card fraud and bank account fraud datasets, with emphasis on detection effectiveness, data privacy and regulatory compliance. The results suggested that decentralised anomaly detection can support fraud identification while reducing the need to expose sensitive banking data. This study supports the present research by highlighting how AI-based fraud detection in online banking must balance transaction monitoring, operational effectiveness and customer data protection.

(Aljunaid et al., 2025) developed an explainable AI-driven federated learning model for financial fraud detection. The study combined federated learning with explainability tools such as SHAP and LIME to improve transparency, classification accuracy and privacy preservation. The findings indicated that explainable and privacy-preserving AI models can strengthen fraud classification while supporting trust and regulatory compliance. This work is relevant to the present study because it connects AI-based fraud detection with customer trust, transparency and the need for reliable digital banking security mechanisms.

(Dichev et al., 2025) analysed the use of machine learning as a tool for assessing and managing fraud risk in banking transactions. The study compared advanced machine learning techniques such as Classification and Regression Trees, Gradient Boosting and Extreme Gradient Boosting with traditional modelling approaches. The results indicated that machine learning methods offer stronger discriminatory power for identifying fraudulent banking transactions, especially in large and imbalanced datasets. This study strengthens the foundation of the present research by showing that AI-driven banking technologies can improve accuracy, efficiency and risk management in fraud detection.

(Chen et al., 2025) conducted a systematic review of deep learning applications in financial fraud detection, covering 108 peer-reviewed publications from 2019 to 2024. The review examined model architectures such as convolutional neural networks, long short-term memory networks, transformers and ensemble methods across financial fraud domains. It identified major challenges related to data imbalance, automation, explainability and privacy compliance. The study is relevant to the present research because it shows that AI-enabled fraud detection is not only a technical issue but also a matter of trust, governance and practical implementation in financial services.

(Patil et al., 2024) introduced a graph-based machine learning model for fraud detection in banking operations, including credit card, debit card and online banking transactions. The study used graph databases with machine learning to analyse customer behaviour, transaction links and suspicious patterns almost immediately. Its findings suggested that graph-based methods can improve the recognition of complex fraud patterns that may remain hidden in conventional rule-based systems. This study is closely aligned with the present research because it supports the role of AI-driven tools in suspicious activity identification and real-time transaction monitoring.

(Detthamrong et al., 2024) studied the enhancement of banking fraud detection through advanced machine learning techniques. The study examined how machine learning can improve fraud identification by processing banking transaction data and identifying behavioural irregularities. Its results emphasised that advanced algorithms can strengthen fraud detection performance and support more efficient banking risk control. This literature is relevant to the present study because it directly supports the examination of AI-driven banking technologies as tools for improving fraud detection mechanisms in digital banking services.

(Boulieris et al., 2024) explored fraud detection using natural language processing and machine learning. The study showed that privacy-safe NLP-based features can improve the performance of fraud detection models and help organisations safeguard user accounts. The research also addressed the challenge of class imbalance, which is common in fraud detection because fraudulent events are usually rare compared with legitimate transactions. This study is relevant to the present research because it highlights the importance of intelligent pattern recognition, privacy-conscious analysis and model performance in AI-enabled fraud detection.

(Nobel et al., 2024) investigated banking fraud detection through machine learning and explainable AI on imbalanced data. The study focused on the limitations of traditional fraud detection systems and demonstrated how explainable AI can support fraud identification while making model decisions more interpretable. Its contribution lies in connecting technical accuracy with transparency, which is essential for practical banking adoption. This study is useful for the present research because customer trust in AI-driven fraud detection depends not only on detection accuracy but also on whether users and institutions can understand and rely on AI-supported decisions.

(Ali et al., 2022) conducted a systematic literature review on financial fraud detection based on machine learning. The review followed a structured approach and synthesised 93 selected articles, identifying common fraud types, frequently used machine learning techniques and evaluation measures. It reported that support vector machines, artificial neural networks and other classification techniques are widely applied in financial fraud detection. This study provides a broad foundation for the present research by showing that AI and machine learning have become central to improving fraud detection, particularly in transaction-based financial environments.

A. Research Gap

The reviewed literature indicates that recent research has largely concentrated on technical modelling, algorithmic performance, data imbalance, explainable AI, privacy preservation and institutional adoption of AI-based fraud detection systems. These studies establish that AI and machine learning can strengthen transaction monitoring, real-time detection, suspicious activity identification, accuracy and operational efficiency in financial fraud detection. However, comparatively less attention has been given to how digital banking users perceive the effectiveness of AI-driven banking technologies across these practical dimensions, particularly with reference to age-based differences in perception. The present study addresses this gap by examining user perceptions of AI-driven banking technologies in improving fraud detection mechanisms in digital banking services.

RESEARCH OBJECTIVE

To analyse the effectiveness of AI-driven tools and systems in improving fraud detection mechanisms in digital banking services.

RESEARCH METHODOLOGY

A. Research Design

The study adopted a descriptive and analytical research design. The descriptive component was used to examine respondents' perceptions regarding the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms in digital banking services. The analytical component was used to test whether such perceptions differed from the neutral level and whether they varied across age groups. This design was considered suitable because the study aimed not only to describe perception patterns but also to test the proposed hypotheses through statistical analysis.

B. Research Approach

The study followed a quantitative research approach. This approach was appropriate because the research was based on measurable variables, structured responses, Likert-scale statements, and statistical testing. Respondents' perceptions were converted into numerical scores, which were further analysed through descriptive statistics, reliability analysis, one-sample t-test, and one-way ANOVA. Thus, the quantitative approach supported objective examination of the relationship between the study variables and the stated hypotheses.

C. Population and Sample

The target population of the study consisted of users of digital banking services. Since the study focused on perceptions regarding AI-driven banking technologies and fraud detection mechanisms, respondents who had experience with digital banking services were considered relevant for the research. The study was conducted on a sample of 318 respondents. A non-probability convenience sampling technique was used, where respondents were selected on the basis of accessibility, willingness to participate, and experience with digital banking services. The sample size was considered adequate for conducting perception-based statistical analysis and comparing responses across age groups.

D. Research Variables

The independent variable of the study was AI-driven banking technologies. It referred to the use of artificial intelligence-based tools, systems, and mechanisms in digital banking for transaction monitoring, fraud alert generation, suspicious activity identification, and fraud detection support. The dependent variable was the perceived effectiveness of AI-driven banking technologies in improving fraud detection mechanisms in digital banking services. It reflected respondents' views regarding the extent to which AI-based systems strengthen fraud detection, improve accuracy, support timely alerts, and enhance perceived security. Age group was used as the grouping variable for examining whether perceptions differed across different age categories.

Construct-level mean scores were calculated to measure respondents' perceptions across specific dimensions of AI-driven fraud detection. The fifteen Likert-scale statements were grouped into five constructs, namely AI-Based Transaction Monitoring, Real-Time Fraud Alert and Detection, Suspicious Activity Identification, Accuracy and Efficiency of AI Fraud Detection, and Customer Trust in AI-Driven Fraud Detection. Each construct included three statements, and the construct score was calculated by taking the average of the three respective item scores. The overall effectiveness score was calculated by averaging all fifteen Likert-scale statements. This composite score represented respondents' overall perception regarding the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms and was used for testing the first hypothesis.

E. Instrument Development and Measurement

A structured questionnaire was used as the research instrument. The questionnaire included fifteen Likert-scale statements related to the effectiveness of AI-driven banking technologies in fraud detection. These statements were divided into five constructs, with three statements under each construct. The constructs covered AI-based transaction monitoring, real-time fraud alert and detection, suspicious activity identification, accuracy and efficiency of AI fraud detection, and customer trust in AI-driven fraud detection. Responses were measured on a five-point Likert scale, where 1 represented Strongly Disagree, 2 represented Disagree, 3 represented Neutral, 4 represented Agree, and 5 represented Strongly Agree.

F. Data Collection Procedure

Primary data were collected from respondents through the structured questionnaire. The questionnaire was administered to digital banking users who were willing to participate and had relevant experience with digital banking services. The data collection process focused on obtaining perception-based responses regarding the use of AI-driven banking technologies in fraud detection. The collected responses were coded, organised, and analysed statistically to address the research objective and hypotheses.

G. Reliability of the Instrument

The reliability of the instrument was examined using Cronbach's alpha. The overall effectiveness scale, consisting of fifteen items, produced a Cronbach's alpha value of 0.928, indicating excellent internal consistency. Construct-wise reliability values were also assessed. AI-Based Transaction Monitoring reported an alpha value of 0.721, Real-Time Fraud Alert and Detection reported 0.734, Suspicious Activity Identification reported 0.687, Accuracy and Efficiency of AI Fraud Detection reported 0.697, and Customer Trust in AI-Driven Fraud Detection reported 0.740. These values indicate that the instrument demonstrated acceptable to excellent reliability, although two constructs reflected comparatively moderate reliability levels.

H. Statistical Tools and Techniques

The data were analysed using descriptive statistics, reliability analysis, one-sample t-test, and one-way ANOVA. Descriptive statistics, including frequency, percentage, mean, and standard deviation, were used to summarise respondents' opinions on each Likert-scale statement and construct. Cronbach's alpha was applied to assess the internal consistency of the overall scale and construct-wise measures.

A one-sample t-test was used to test H01, which examined whether respondents' perceptions regarding the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms differed significantly from the neutral test value of 3. This test was suitable because the hypothesis focused on the overall mean perception score. One-way ANOVA was used to test H02, which examined whether respondents' perceptions differed significantly across age groups. This test was appropriate because age group was a categorical grouping variable with more than two categories, while the dependent variable was measured through the overall effectiveness score. The level of significance was fixed at 5 percent for hypothesis testing.

LIKERT SCALE STATEMENT ANALYSIS

Table 1: Likert Scale Statements on AI-Based Transaction Monitoring

Code	Statement	SD	D	N	A	SA	$\bar{X}$	σ
St1	AI-driven banking technologies help in monitoring digital banking transactions more effectively.	1	15	102	144	56	3.75	0.81
St2	AI-based transaction monitoring assists banks in identifying unusual transaction patterns.	1	20	110	139	48	3.67	0.82
St3	AI-enabled monitoring systems improve the detection of suspicious digital banking activities.	0	22	94	135	67	3.78	0.86

The findings indicate a favourable response pattern towards AI-based transaction monitoring. The mean scores for the three statements ranged from 3.67 to 3.78, showing that respondents generally agreed that

AI-driven banking technologies help in monitoring digital transactions, identifying unusual transaction patterns, and improving the detection of suspicious banking activities. This suggests that transaction monitoring is perceived as an important dimension of AI-enabled fraud detection.

Table 2: Likert Scale Statements on Real-Time Fraud Alert and Detection

Code	**Statement**	**SD**	**D**	**N**	**A**	**SA**	$\bar{X}$	σ
St4	AI-driven fraud alert systems help banks detect possible fraud in real-time.	1	13	102	141	61	3.78	0.81
St5	Real-time AI-based alerts improve the speed of fraud detection in digital banking services.	0	17	87	147	67	3.83	0.82
St6	AI-enabled alert mechanisms support timely action against fraudulent digital banking transactions.	1	21	110	127	59	3.70	0.86

Respondents showed a positive perception of real-time fraud alert and detection systems. The mean scores ranged from 3.70 to 3.83, with the highest agreement observed for the speed of fraud detection through real-time AI-based alerts. This indicates that respondents recognise the usefulness of AI-enabled alert mechanisms in supporting timely detection and response to potentially fraudulent digital banking transactions.

Table 3: Likert Scale Statements on Suspicious Activity Identification

Code	**Statement**	**SD**	**D**	**N**	**A**	**SA**	$\bar{X}$	σ
St7	AI-driven banking technologies help identify suspicious customer activities in digital banking.	0	28	108	139	43	3.62	0.83
St8	AI-based systems are effective in recognising abnormal behaviour in digital banking transactions.	0	13	97	145	63	3.81	0.80
St9	AI technologies assist banks in detecting activities that may indicate potential fraud.	1	14	101	144	58	3.77	0.81

The responses suggest moderate to favourable agreement regarding the ability of AI-driven banking technologies to identify suspicious activities. The mean values ranged from 3.62 to 3.81, indicating that respondents perceived AI systems as useful in recognising abnormal behaviour and detecting activities that may indicate potential fraud. However, the relatively lower score for suspicious customer activity identification reflects some scope for further confidence building.

Table 4: Likert Scale Statements on Accuracy and Efficiency of AI Fraud Detection

Code	**Statement**	**SD**	**D**	**N**	**A**	**SA**	$\bar{X}$	σ
St10	AI-driven tools improve the accuracy of fraud detection in digital banking services.	1	9	108	142	58	3.78	0.78
St11	AI-based fraud detection systems reduce delays in identifying fraudulent digital banking transactions.	3	19	117	134	45	3.63	0.83

St12	AI-driven banking technologies enhance the overall efficiency of fraud detection mechanisms.	1	18	94	162	43	3.72	0.78

The findings reflect a generally favourable perception of the accuracy and efficiency of AI-based fraud detection. Mean scores ranged from 3.63 to 3.78, suggesting that respondents agreed that AI-driven tools improve accuracy, reduce delays, and enhance the overall efficiency of fraud detection mechanisms. This pattern indicates that respondents view AI as a useful support system for improving operational effectiveness in digital banking fraud detection.

Table 5: Likert Scale Statements on Customer Trust in AI-Driven Fraud Detection

Code	Statement	SD	D	N	A	SA	$\overline{X}$	σ
St13	AI-driven fraud detection increases customers' confidence in digital banking services.	0	18	118	133	49	3.67	0.80
St14	Customers are more likely to trust digital banking services when AI-based fraud detection is used.	0	24	120	133	41	3.60	0.81
St15	AI-enabled fraud detection strengthens perceived security in digital banking services.	0	14	106	129	69	3.80	0.83

The findings show that respondents moderately agreed that AI-driven fraud detection strengthens trust in digital banking services. The mean scores ranged from 3.60 to 3.80, with the strongest response observed for perceived security. This suggests that AI-enabled fraud detection may contribute to customer confidence, although trust building still requires consistent system performance, transparency, and user awareness.

HYPOTHESES

H_{01}: There is no significant difference in respondents' perceptions regarding the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms in digital banking services.

A one-sample t-test was applied to examine whether respondents' overall perception regarding the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms differed significantly from the neutral test value of 3.

Table 6: Descriptive Statistics

	n	Mean	Std. Deviation	Std. Error Mean
Overall Effectiveness Score	318	3.73	0.58	0.03

The results showed that the overall effectiveness score was above the neutral level, with a mean score of 3.73 and a standard deviation of 0.58.

Table 7: One Sample T-test

	t	df	p	Mean Difference
Overall Effectiveness Score	22.48	317	<.001	0.73

The test result was statistically significant, $t(317) = 22.48$, $p < .001$, with a mean difference of 0.73. This indicates that respondents' perceptions were significantly higher than the neutral point. The result suggests that respondents generally perceived AI-driven banking technologies as effective in improving fraud detection mechanisms in digital banking services.

Decision

For H_{01}, the one-sample t-test was applied to examine whether respondents' perceptions regarding the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms differed significantly from the neutral test value. Since the p-value was less than .05, H01 is rejected. The null hypothesis is rejected.

Finding

Respondents showed a favourable perception of AI-driven banking technologies in improving fraud detection mechanisms in digital banking services. This suggests that AI-based tools are viewed as useful for strengthening fraud detection through transaction monitoring, alert generation, suspicious activity identification, and improved perceived security.

Conclusion

Since the null hypothesis is rejected, the researcher concludes that there is a significant difference in respondents' perceptions regarding the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms in digital banking services.

H_{02}: There is no significant difference in respondents' perceptions regarding the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms in digital banking services across different age groups.

One-way ANOVA was conducted to examine whether respondents' perceptions regarding the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms differed across age groups.

Table 8: Descriptive Statistics

	n	Mean	Std. Deviation
Above 55 years	35	3.14	0.55
26–35 years	92	3.95	0.50
46–55 years	49	3.36	0.39
36–45 years	68	3.80	0.55
18–25 years	74	3.90	0.51
Total	318	3.73	0.58

The descriptive results showed variation in mean perception scores across the age categories. Respondents aged 26–35 years reported the highest mean score (M = 3.95, SD = 0.50), followed by respondents aged 18–25 years (M = 3.90, SD = 0.51) and 36–45 years (M = 3.80, SD = 0.55). Lower mean scores were observed among respondents aged 46–55 years (M = 3.36, SD = 0.39) and above 55 years (M = 3.14, SD = 0.55).

Table 9: ANOVA

	Sum of Squares	df	Mean Square	F	p
Age Group	25.89	4	6.47	25.53	<.001
Residual	79.36	313	0.25		

	Sum of Squares	df	Mean Square	F	p
Total	105.24	317			

The ANOVA result was statistically significant, $F(4, 313) = 25.53$, $p < .001$. This indicates that respondents' perceptions differed significantly across age groups.

Decision

For H_{02}, one-way ANOVA was applied to examine whether respondents' perceptions regarding the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms differed significantly across age groups. Since the p-value was less than .05, H_{02} is rejected. The null hypothesis is rejected.

Finding

The findings indicate that perceptions regarding AI-driven banking technologies vary across age groups. Younger and middle-age respondents, particularly those in the 26–35 years and 18–25 years age groups, reported more favourable perceptions than respondents in the older age categories.

Conclusion

Since the null hypothesis is rejected, the researcher concludes that there is a significant difference in respondents' perceptions regarding the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms in digital banking services across different age groups.

OVERALL CONCLUSION

The study examined the effectiveness of AI-driven banking technologies in improving fraud detection mechanisms in digital banking services. The Likert scale findings show that respondents generally held favourable perceptions across all five constructs, namely transaction monitoring, real-time fraud alerts, suspicious activity identification, accuracy and efficiency, and customer trust. The overall effectiveness mean score of 3.73 indicates that respondents' perceptions were above the neutral level, suggesting that AI-based banking technologies are viewed as useful in strengthening fraud detection practices in digital banking.

The hypothesis results further support this empirical direction. The one sample t test showed that respondents' overall perception significantly differed from the neutral test value, leading to the rejection of H_{01}. The ANOVA result also indicated significant differences across age groups, leading to the rejection of H_{02}. Younger respondents, particularly those aged 26 to 35 years and 18 to 25 years, reported more favourable perceptions than older respondents. Overall, the study contributes to understanding how digital banking users perceive AI-driven fraud detection and highlights the relevance of age based differences in the acceptance and evaluation of such technologies.

SUGGESTIONS BASED ON FINDINGS

1. Banks should strengthen AI-based transaction monitoring systems because respondents showed favourable perceptions regarding the role of AI in monitoring digital banking transactions and identifying unusual transaction patterns.
2. Digital banking platforms should improve real-time fraud alert systems, as respondents reported comparatively strong agreement regarding the usefulness of AI-based alerts in improving the speed of fraud detection.
3. Banks should ensure that AI-enabled alert mechanisms are linked with timely internal response systems so that suspicious transactions can be examined quickly and effectively.

4. Financial institutions should improve customer awareness regarding how AI-based systems identify suspicious activities, as this may help increase confidence in fraud detection processes.
5. Banks should communicate the benefits of AI-driven fraud detection in simple language so that customers understand how such systems support transaction safety.
6. AI-based fraud detection systems should be regularly reviewed to improve accuracy and reduce delays in identifying fraudulent transactions, as accuracy and efficiency emerged as important areas of respondent agreement.
7. Digital banking service providers should focus on building trust among customers by explaining the security role of AI-enabled fraud detection mechanisms.
8. Since younger respondents showed more favourable perceptions, banks should design separate awareness strategies for older age groups to improve their understanding and acceptance of AI-driven banking technologies.
9. Customer education programmes should be introduced for users above 46 years of age, as their mean perception scores were lower than those of younger respondents.
10. Banks should provide clear guidance through mobile banking applications, websites, and customer support channels about the role of AI in fraud detection.
11. AI-driven fraud detection mechanisms should be supported by human verification in sensitive cases so that customers feel more secure and system decisions remain accountable.
12. Banks should use customer feedback to identify areas where users still feel uncertain about AI-based monitoring, alerts, suspicious activity detection, and digital banking security.
13. Digital banking platforms should avoid presenting AI fraud detection as a fully automatic solution and should instead communicate it as a support mechanism for safer banking.
14. Banks should improve transparency in fraud alert messages by making alerts clear, timely, and easy for customers to act upon.
15. Financial institutions should conduct periodic perception studies across age groups to understand whether customer confidence in AI-driven fraud detection improves over time.
16. Banks should integrate AI-based fraud detection with customer trust building measures, such as secure authentication, immediate alerts, complaint support, and transparent reporting.
17. Policymakers and banking regulators may encourage banks to adopt customer-centric AI fraud detection practices that balance technological efficiency with user awareness, fairness, and trust.

REFERENCES:

1. AbouGrad, H., & Sankuru, L. (2025). Online banking fraud detection model: Decentralized machine learning framework to enhance effectiveness and compliance with data privacy regulations. Mathematics, 13(13), 2110. doi: 10.3390/math13132110
2. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. Applied Sciences, 12(19), 9637. doi: 10.3390/app12199637
3. Aljunaid, S. K., Almheiri, S. J., Dawood, H., & Khan, M. A. (2025). Secure and transparent banking: Explainable AI-driven federated learning model for financial fraud detection. Journal of Risk and Financial Management, 18(4), 179. doi: 10.3390/jrfm18040179
4. Boulieris, P., Pavlopoulos, J., Xenos, A., & Vassalos, V. (2024). Fraud detection with natural language processing. Machine Learning, 113(8), 5087–5108. doi: 10.1007/s10994-023-06354-5
5. Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep learning in financial fraud detection: Innovations, challenges, and applications. Data Science and Management. doi: 10.1016/j.dsm.2025.08.002

6. Detthamrong, U., Chansanam, W., Boongoen, T., & Iam-On, N. (2024). Enhancing fraud detection in banking using advanced machine learning techniques. International Journal of Economics and Financial Issues, 14(5), 177–184. doi: 10.32479/ijefi.16613
7. Dichev, A., Zarkova, S., & Angelov, P. (2025). Machine learning as a tool for assessment and management of fraud risk in banking transactions. Journal of Risk and Financial Management, 18(3), 130. doi: 10.3390/jrfm18030130
8. Nobel, S. M. N., Sultana, S., Singha, S. P., Chaki, S., Mahi, M. J. N., Jan, T., Barros, A., & Whaiduzzaman, M. (2024). Unmasking banking fraud: Unleashing the power of machine learning and explainable AI on imbalanced data. Information, 15(6), 298. doi: 10.3390/info15060298
9. Patil, A., Mahajan, S., & Menpara, J. (2024). Enhancing fraud detection in banking by integration of graph databases with machine learning. MethodsX, 12, 102683. doi: 10.1016/j.mex.2024.102683
10. Yaseen, H., & Al-Amarneh, A. (2025). Adoption of artificial intelligence-driven fraud detection in banking: The role of trust, transparency, and fairness perception in financial institutions in the United Arab Emirates and Qatar. Journal of Risk and Financial Management, 18(4), 217. doi: 10.3390/jrfm18040217