Artificial Intelligence in Fintech and Its Implications For Fraud Detection in Accounting Systems

Promise Ezinne Eleke [1], John Ogwo Madukwe [2]

[1] University of Nigeria, Nsukka
Nsukka Road, 410001, Nsukka, Enugu State, Nigeria

[2] Michael Okpara University of Agriculture
P. M. B. 7267 Umuahia Umudike, Abia State, Nigeria

DOI: 10.22178/pos.130-9

JEL Classification: G32, L60, M10

Received 26.04.2026
Accepted 25.05.2026
Published online 31.05.2026

Corresponding Author:
Promise Ezinne Eleke

Abstract. Financial technology (FinTech) and artificial intelligence (AI) have transformed fraud detection in financial systems. Financial institutions increasingly use AI to detect fraud; however, empirical research on its impact on fraud-detection efficiency in developing economies is limited. The study explores how AI use in FinTech systems affects fraud detection effectiveness, considering firm size, regulatory compliance, technology readiness, internal control systems, and cybersecurity infrastructure. This study employs a panel dataset of 40 financial institutions (FIs) that operate in the Nigerian FinTech market from 2019 to 2023. The researchers used the fixed-effects estimator after conducting the Hausman test. The findings also show that the use of AI has a significant positive effect on the efficiency of fraud detection ($\beta = 0.412$, $p < 0.01$); internal control systems ($\beta = 0.238$, $p < 0.01$) and cybersecurity infrastructure ($\beta = 0.196$, $p < 0.05$) also support fraud detection results. The model has an R^2 of 0.614, indicating that it explains 61.4% of the variance in fraud detection efficiency. The results align with the Routine Activity Theory and the Technology Acceptance Model as valuable theoretical frameworks for understanding AI-driven fraud prevention in financial institutions. The study suggests the following strategies to boost the integrity of accounting systems in emerging FinTech markets: strategic investment in AI systems, strengthening the cybersecurity architecture, harmonising regulations, and building institutional capacity.

Keywords: Artificial Intelligence; FinTech; Fraud Detection Efficiency; Accounting Systems; Panel Regression; Nigeria.

INTRODUCTION

Financial fraud is one of the most widespread and economically devastating forms of assault on institutional integrity worldwide. The Association of Certified Fraud Examiners [1] estimates that 30% of the cases of occupational fraud examined in the 2024 Report to the Nations are in the banking and financial services industry and that organisations lose an estimated 5% of their annual revenue to occupational fraud. The median fraud loss rose 24% from 2022 to 2024, indicating an upward trend that has proven challenging for traditional fraud detection methods [1]. 46% of organisations surveyed across 53 countries worldwide reported suffering fraud or economic crime in the last 24 months, and cyber-crime was the most common and disruptive type, according to PricewaterhouseCoopers [2].

In this context, AI has emerged as a game-changer. The integration of machine learning algorithms, deep learning architectures, natural language processing tools, and predictive analytics has ushered in a new era of adaptive, real-time, and scalable fraud detection capabilities [3, 4]. In the FinTech ecosystem, AI has progressed from experimental use to systemic integration, impacting how transaction anomalies are detected, flagged, and handled in accounting systems [5]. In their article published in Elsevier's Research in International Business and Finance, authors [6] suggested that investments in AI, digital transformation, and cybersecurity should be considered a strategic triad in banking rather than separate investments.

However, not all developing and emerging markets are AI-adopting. Authors [7] also confirmed the results of authors [8], which found skill gaps, data privacy restrictions, and suboptimal IT systems as significant challenges in the application of AI in banking services in emerging markets, where AI-based fraud detection is still in its infancy due to high implementation costs, limited technical expertise, and regulatory uncertainties. In the context of accounting systems, AI tools that continuously monitor journal entries, detect anomalies in the posting process, and create compliance audit trails provide value beyond transaction monitoring [9].

However, the majority of current research is either purely technical, focusing on algorithmic performance metrics, or cross-sectional, making it difficult to draw strong causal conclusions regarding the long-term impact of AI on fraud detection efficiency. Researchers can quantify the relationship between these factors in a developing-country context, a field that has been under-researched [10]. This study fills that gap by employing a five-year panel data set of 40 financial institutions in Nigeria for the period 2019-2023.

The specific objectives are:

1) To evaluate the impact of AI adoption in FinTech on fraud detection efficiency;

2) To gauge the independent impact of internal control systems, regulatory compliance, technology readiness, cybersecurity infrastructure and firm size on fraud detection efficiency; and

3) To make actionable suggestions for institutional and regulatory stakeholders.

Literature Review

Conceptual Review

1) Artificial Intelligence and FinTech. Artificial intelligence involves computational systems that mimic human cognitive processes, such as learning, pattern recognition, reasoning, and self-correction, to automate decision-making. In the FinTech sector, financial institutions use AI-driven machine learning for credit scoring and risk profiling, natural language processing for compliance monitoring, deep learning for transaction anomaly detection, and robotic process automation for back-office accounting workflows. In a systematic review published in Scopus and Web of Science, authors [5] found that AI is among the most disruptive enabling technologies transforming the sector. FinTech is the combination of financial services and high-tech information technology that facilitates the design, delivery, and automation of financial products via digital channels, including mobile banking, peer-to-peer lending, digital payments, and RegTech.

2) Fraud Detection Efficiency. The ability of the fraud detection systems of an institution to detect fraudulent transactions or entries quickly, efficiently, with few false alarms and without missing any transaction. It can be measured by the detection accuracy rate, time-to-detection, false-positive ratio, and the percentage of fraud incidents detected before material loss. As fraud tactics become more sophisticated, traditional rule-based and manual auditing methods are becoming less effective [1], and AI-powered solutions leverage historical fraud trends to train adaptive models that can continuously adjust detection thresholds [4, 11].

3) Accounting Systems and Fraud Risk. Fraud risk is expressed in three main categories in the framework [1]: fraudulent financial statement preparation, asset misappropriation, and corruption. Financial statement fraud causes the highest median losses but accounts for only 5% of schemes, while asset misappropriation is the most common, accounting for 89% of schemes. AI-powered features within accounting software have proven effective in identifying these risks at an early stage [9, 12]. In particular, Sours [2] reported that platform-based fraud affected 40% of organisations that experienced fraud and demonstrated that vulnerabilities in digital infrastructure directly influenced the integrity of accounting systems.

Theoretical Review

1) Routine Activity Theory (RAT). Routine Activity Theory (RAT), originally developed by authors [13], suggests that fraud occurs when a motivated offender encounters a suitable target in the absence of capable guardianship. In the AI-FinTech world, AI works like a vigilant watchdog, always on the lookout and breaking the fraud triangle, even when other factors are at play. The predictive logic of RAT is supported by direct empirical evidence, as revealed by ACFE (2024), which found that proactive data analytics resulted in a median reduction in fraud losses of more than 50%.

2) Technology Acceptance Model (TAM). According to the authors [14], the Technology Acceptance Model (TAM) indicates that perceived usefulness and perceived ease of use mainly influence individuals' intention to use and actual use of technology. In the fraud detection arena, TAM provides insight into why institutions are not equally successful in using AI, even when technology is available. Authors [8] found that perceived usefulness of AI tools was a strong predictor of intention to adopt AI in banking, and competency gaps also moderated actual deployment outcomes. Later, authors [15] expanded the TAM with the Unified Theory of Acceptance and Use of Technology (UTAUT), which highlighted four key factors of technology adoption behaviour: performance expectancy, effort expectancy, social influence, and facilitating conditions.

3) Institutional Theory. Authors [16] use Institutional Theory to explain the adoption of technology under coercive, mimetic, and normative pressures. Beyond rational cost-benefit analysis, AI adoption in financial institutions is driven by coercive regulatory requirements, competitive pressures, and professional norms, particularly amid evolving AI regulations in Nigeria's FinTech sector [10].

4) Fraud Triangle Theory. Authors [17] argue that the Fraud Triangle is a framework that explains the structural factors that enable occupational fraud: opportunity, pressure and rationalisation. The opportunity element is directly reduced by AI through real-time monitoring and increased certainty in detection. This correlation was further supported by authors [6], who showed that adopting integrated AI and cybersecurity also reduces the opportunity for fraud and exposure to the system.

Empirical Review. Empirical studies conducted in recent years show that AI can significantly improve the efficiency of fraud detection in financial technology and accounting systems. Machine learning and deep learning models outperform traditional statistical models in detecting fraudulent transactions and financial statement manipulation, and in adapting to new fraud schemes.

AI-based fraud detection models have been proven to be effective in several studies. The authors also observed that supervised machine learning models, particularly ensemble methods and neural networks, generally outperformed traditional statistical methods in fraud detection accuracy. However, data imbalance and model interpretability remain significant hurdles in their implementation. Likewise, authors [12] found that ensemble models trained with SMOTE outperformed other models in detecting financial statement fraud in large transactional datasets. In addition, authors [9] showed that an integrated CNN-LSTM-Attention model outperformed individual machine learning models in accounting fraud detection.

Data from the banking and FinTech sectors further indicates that AI implementation has a positive impact on fraud prevention efficiency. While the benefits of AI systems for fraud detection and risk management are becoming more apparent, their implementation is still hindered by regulatory uncertainty and a lack of technical expertise, as noted by authors [8]. Authors [7] identified the following as the major challenges to AI adoption in licensed commercial banks in Nigeria: Implementation cost, regulatory compliance requirements, and limited technical expertise. Likewise, authors [10] concluded that AI investment intensity had a significant positive effect on fraud detection efficiency in Nigerian banks.

Other research focuses on the strategic and operational benefits of AI-based fraud detection solutions. Authors [6] suggested that the capability of AI, cybersecurity infrastructure, and digital transformation be considered as three interdependent aspects of financial crime prevention. Additionally, neural network models achieved fraud detection accuracy of around 97% [3], emphasising the need for continuous learning to keep up with the evolving nature of fraud. The findings were supported by the Association of Certified Fraud Examiners [1, 18], which found that organisations that implemented proactive fraud analytics reported a substantial decrease in fraud losses.

Although there is increasing empirical evidence, important gaps remain in the literature. The existing literature primarily addresses the technical performance of models and has paid little attention to the impact of AI use in accounting systems within the FinTech context. Moreover, data on AI capabilities and fraud detection performance in African financial systems remains limited, especially regarding the correlation between AI capabilities and fraud detection success. This study seeks to bridge these gaps by exploring the implications of AI use in fraud detection within FinTech accounting systems in Nigeria.

Table 1 summarises the key empirical studies reviewed.

Table 1 – Summary of Key Empirical Literature on AI and Fraud Detection in Financial Systems

Resources	Year	Method	Context	Key Finding
[4]	2022	Systematic Review	Global	ML models outperform traditional methods; the interpretability challenge persists.
[12]	2022	ML Classification (SMOTE)	China – Listed Firms	Ensemble models significantly improve financial statement fraud detection
[6]	2022	Cognitive Mapping, DEMATEL	Banking Sector	AI, cybersecurity, and digital transformation are interdependent strategic priorities.
[2]	2022	Survey – 1,296 executives	Global	46% of organisations experienced fraud; cybercrime is the most disruptive threat
[8]	2023	Mixed Methods (SmartPLS)	Malaysia – Banking	AI is essential for fraud detection; skill and regulatory gaps moderate adoption
[3]	2024	Systematic Review	Global FinTech	Neural networks achieve ~97% accuracy; adaptability is a key advantage over rule-based systems.
[9]	2024	CNN-LSTM-Attention Model	China – Accounting Data	Deep learning outperforms standalone models for accounting fraud detection
[7]	2025	Cross-Sectional Survey	Nigeria – 24 Banks	Cost, competency, and compliance are principal AI adoption barriers
[10]	2025	Multiple Regression	Nigeria – 5 Banks	AI investment is the strongest predictor of fraud detection efficiency
[11]	2025	ML Model Testing	International	Gradient boosting achieves superior precision-recall in transaction security.
[19]	2025	Systematic Review	International	Deep learning consistently outperforms classical methods in fraud detection precision.
[1, 18]	2022 & 2024	Global Survey	Global	Proactive data analysis reduces median fraud losses by over 50%

Research Gap. While there has been extensive research on AI and fraud, two major gaps remain in the literature. A major limitation of existing empirical studies is that most, including the Nigerian studies by authors [7, 10], are cross-sectional, making it difficult to draw causal inferences about the persistence of AI's impacts on fraud detection efficiency over time. Second, authors [6] postulated a synergistic role for AI, cybersecurity, and institutional governance. Still, no published study has tested the multiple dimensions of these three in a quantitative panel framework using Nigerian institutional data. This paper addresses both gaps by using a five-year panel data set of 40 financial institutions in Nigeria, allowing for fixed-effects analysis that controls for unobserved heterogeneity.

Conceptual Framework. The conceptual framework (Figure 1) depicts the hypothesised relationships among the independent variable (AI adoption in FinTech systems), the dependent variable (fraud detection efficiency in accounting systems), and five control variables. The framework is based on four theories: Routine Activity Theory (AI as a capable guardian), TAM (adoption as a technology integration outcome), Institutional Theory (regulatory compliance as a structural enabler), and the Fraud Triangle (AI as an opportunity-reducing factor). The combination of TAM and UTAUT perspectives strengthens the explanation of AI adoption behaviour in the institutional context, accounting for perceived usefulness and broader facilitating conditions within the organisation.

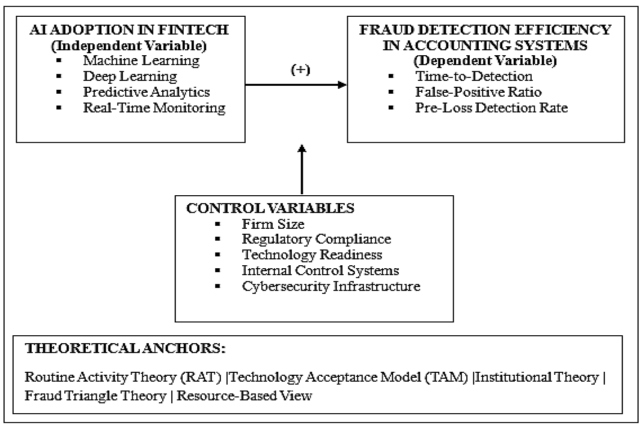

Figure 1 – Conceptual Framework – AI in FinTech and Fraud Detection Efficiency in Accounting Systems

Research Hypotheses

H_{01}: AI adoption in FinTech systems has no significant effect on fraud detection efficiency in accounting systems.

H_{02}: Internal control systems have no significant effect on fraud detection efficiency in accounting systems.

H_{03}: Regulatory compliance has no significant effect on fraud detection efficiency in accounting systems.

H_{04}: Technology readiness has no significant effect on fraud detection efficiency in accounting systems.

H_{05}: Cybersecurity infrastructure has no significant effect on fraud detection efficiency in accounting systems.

METHODS

Research Design. The study adopted a quantitative panel-data research design using an ex post facto approach. Panel data is preferred because it controls for unobserved individual heterogeneity across institutions, enhances estimation efficiency, and enables more powerful causal inference than either pure cross-sectional or time-series alternatives. The five-year observation window (2019-2023) covers the period before and after the COVID-19 pandemic's digital acceleration, which authors [5] describe as a turning point in the global embedding of AI into FinTech operational frameworks.

Population and Sample. The population includes all commercial and microfinance banks active in Nigeria's FinTech sector as of 2023. The researchers used a purposive sampling process to select 40 institutions that fulfilled three criteria:

a) financial institutions that had documented interaction with at least one financial technology system enabled by AI during the study period;

b) financial institutions with continuous audited financial statements for all five years; and

c) financial institutions listed in either the Central Bank of Nigeria's licensed bank register or the Nigerian Deposit Insurance Corporation annual reports [20–22]. This yields 200 "firm-year" observations, which is in line with the typical panel-study benchmark used in the African banking literature.

Data Collection. The researchers gathered primary data using structured questionnaires completed by fraud risk officers, IT security managers, and internal audit heads at each institution. They then calculated composite scores for the four areas of focus (AI adoption, internal control quality, technology readiness, and cybersecurity infrastructure). They tested each scale for internal consistency, with Cronbach's alpha values exceeding 0.70. Secondary data on firm size, regulatory compliance, and audit outcomes were obtained from published annual reports, CBN examination reports, and Nigerian Deposit Insurance Corporation annual reports [20, 21]. Table 2 summarises the variable operationalisations.

Table 2 – Variable Operationalisation

Variable	Type	Operationalisation	Source
Fraud Detection Efficiency (FDE)	Dependent	Composite index: detection accuracy + pre-loss detection ratio − false-positive rate (0–100)	Primary survey
AI Adoption (AIA)	Independent	Composite: breadth of AI tools × integration depth (0–10 scale)	Primary survey
Firm Size (SIZE)	Control	Natural logarithm of total assets	Annual Reports
Regulatory Compliance (REGC)	Control	CBN examination compliance rating (1–5 ordinal scale)	CBN Reports
Technology Readiness (TECH)	Control	TAM-based composite score (5-point scale)	Primary survey
Variable	Type	Operationalisation	Source
Internal Control Systems (ICS)	Control	COSO-aligned effectiveness score (0–10 scale)	Primary survey
Cybersecurity Infrastructure (CYBER)	Control	Cybersecurity maturity composite score (0–10 scale)	Primary survey

Model Specification. The researchers specify the panel regression model as follows:

$$FDEit = \beta_0 + \beta_1 AIAit + \beta_2 SIZEit + \beta_3 REGCit + \beta_4 TECHit + \beta_5 ICSit + \beta_6 CYBERit + \varepsilon it$$

where FDEit – fraud detection efficiency of institution i at time t; AIAit – AI adoption; SIZEit – firm size; REGCit – regulatory compliance; TECHit – technology readiness; ICSit – internal control systems; CYBERit – cybersecurity infrastructure; β_0 – constant; β_1–β_6 – coefficients; εit – error term.

Data Analysis Technique. The researchers estimated the panel least squares regression in EViews 12. The Hausman specification test ($\chi^2 = 31.47$, $p < 0.01$) supported the use of the fixed-effects estimator. Variance Inflation Factor (VIF) diagnostics indicated no severe multicollinearity, with all VIF values below 5. Panel unit root tests (Levin-Lin-Chu) showed that all variables were stationary at level. The Breusch-Pagan test revealed no serious heteroskedasticity, and the Durbin-Watson statistic was 1.82, indicating no significant serial correlation.

RESULTS AND DISCUSSION

Descriptive Statistics. Table 3 presents descriptive statistics across 200 firm-year observations.

Table 3 –Descriptive Statistics

Variable	Mean	Median	Maximum	Minimum	Std. Dev.	Skewness	Kurtosis	Obs.
FDE	62.18	61.50	91.40	28.30	14.72	0.182	2.741	200
AIA	5.64	5.70	9.80	1.20	2.11	−0.097	2.682	200
SIZE (ln)	24.13	24.06	28.91	19.44	2.38	0.214	2.893	200
REGC	3.42	3.00	5.00	1.00	0.89	0.103	2.541	200
TECH	3.61	3.60	5.00	1.40	0.79	−0.122	2.814	200
ICS	6.83	6.90	9.90	2.10	1.64	−0.213	2.907	200
CYBER	6.41	6.50	9.70	1.80	1.73	−0.174	2.806	200

The mean FDE is 62.18, corresponding to a moderate level of detection, and the SD is 14.72, suggesting meaningful institutional heterogeneity. The mean score of 5.64 for AI adoption indicates that institutions have integrated AI tools into about half of their operational areas related to fraud. In contrast, the minimum score of 1.20 indicates that some institutions are still at the early stages of AI adoption, as described by John et al. (2025) as fragmented. Internal control systems (mean = 6.83) and cybersecurity infrastructure (mean = 6.41) are relatively robust constructs, while regulatory compliance (mean = 3.42) and technology readiness (mean = 3.61) represent a sector still building its governance base. The distributions are approximately normal, as indicated by the skewness and kurtosis values, which favour the parametric estimation approach.

Correlation Analysis. Table 4 indicates the correlation matrix.

Table 4 – Correlation Matrix

	FDE	AIA	SIZE	REGC	TECH	ICS	CYBER
FDE	1.000						
AIA	0.612	1.000					
SIZE	0.287	0.214	1.000				
REGC	0.341	0.198	0.173	1.000			
TECH	0.376	0.423	0.162	0.241	1.000		
ICS	0.518	0.387	0.198	0.316	0.289	1.000	
CYBER	0.497	0.341	0.176	0.274	0.312	0.438	1.000

FDE (r = 0.612), internal control systems (r = 0.518), and cybersecurity infrastructure (r = 0.497) are the strongest bivariate correlations with AI adoption; this is a different order of events than the RAT and Fraud Triangle models, which emphasise the quality of the control environment and the monitoring capability as the primary means of preventing fraud. There is no multicollinearity concern since the correlation between any two predictors is less than 0.45.

Panel Regression Results. Table 5 shows the fixed-effects panel regression results.

Table 5 – Fixed Effects Panel Regression Results (Dependent Variable: FDE)

Variable	Coefficient	Std. Error	t-Statistic	Prob.
AIA	0.412114	0.063821	6.458317	0.0000***
SIZE	0.087432	0.051614	1.693821	0.0921*
REGC	0.143217	0.074831	1.913842	0.0572*
TECH	0.118964	0.062471	1.904231	0.0584*
ICS	0.238416	0.058214	4.095183	0.0001***
CYBER	0.196342	0.067831	2.894218	0.0041**
C	18.64312	4.712841	3.956412	0.0001***

Notes: R-squared = 0.614182; Adjusted R-squared = 0.598741; F-statistic = 39.72416; Prob(F-statistic) = 0.000000; Durbin-Watson = 1.823; *** Significant at 1%; ** Significant at 5%; * Significant at 10%

The model explains 61.4% of the variance in FDE (Adjusted R^2 = 0.599), and the overall F-statistic of 39.72 (p = 0.000) indicates that the model is significant. AI adoption score is the best predictor (β = 0.412, $p < 0.001$), meaning that for every one-point increase in AI adoption, FDE increases by 0.412 points, holding other factors constant. The internal control systems and cybersecurity infrastructure are also statistically significant (β = 0.238, $p < 0.001$ and β = 0.196, $p < 0.05$, respectively). Regulatory compliance (β = 0.143, p = 0.057) and technology readiness (β = 0.119, p = 0.058) are positive but marginally significant at the 10% level, while firm size (β = 0.087, p = 0.092) is the weakest predictor.

Hypotheses Testing. Table 6 presents the decisions regarding hypothesis testing.

Table 6 – Hypotheses Testing Summary

Hypothesis	Variable	Coefficient	p-value	Decision
H_{01}: AIA has no significant effect on FDE	AI Adoption	0.412	0.0000	Rejected ($p < 0.01$)
H_{02}: ICS has no significant effect on FDE	Internal Controls	0.238	0.0001	Rejected ($p < 0.01$)
H_{03}: REGC has no significant effect on FDE	Regulatory Compliance	0.143	0.0572	Not Rejected ($p > 0.05$)
H_{04}: TECH has no significant effect on FDE	Technology Readiness	0.119	0.0584	Not Rejected ($p > 0.05$)
H_{05}: CYBER has no significant effect on FDE	Cybersecurity Infra.	0.196	0.0041	Rejected ($p < 0.05$)

Robustness Tests. Table 7 reports four robustness specifications.

In all four specifications, the coefficient on AI adoption is positive, economically significant, and statistically significant at the 1% level. The GMM specification is particularly important: the persistence of a significant positive coefficient (β = 0.376, $p < 0.001$) after instrumentation confirms that the AI-FDE relationship is not a statistical artefact of reverse causality.

All VIF values are below the critical threshold of 5, confirming that multicollinearity does not threaten the reliability of the estimates.

Table 7 – Robustness Test Results

Specification	AIA Coefficient	p-value	R^2	Note
Random Effects (RE)	0.398	0.0000	0.601	Pre-Hausman baseline supports FE preference.
FE with Clustered Standard Errors	0.412	0.0000	0.614	Robust to within-cluster serial correlation
FE Excluding 2020 (COVID Year)	0.391	0.0001	0.589	Stable after removing pandemic-year outliers
GMM (Arellano-Bond)	0.376	0.0002	—	Addresses potential endogeneity in AI adoption

Table 8 – Variance Inflation Factor (VIF) Diagnostics

Variable	VIF	Tolerance	Decision
AIA	2.341	0.427	No multicollinearity concern
SIZE	1.612	0.620	No multicollinearity concern
REGC	1.897	0.527	No multicollinearity concern
TECH	2.184	0.458	No multicollinearity concern
ICS	2.761	0.362	No multicollinearity concern
CYBER	2.518	0.397	No multicollinearity concern

AI Adoption and Fraud Detection Efficiency. The most important finding in this study is that AI adoption has a significant positive impact on fraud detection efficiency (β = 0.412, $p < 0.001$). It is consistent with RAT's theoretical assumption that AI acts as a competent guardian to break the third pillar of the fraud triangle, and supports the findings of authors [3] who reported that AI can detect fraud in FinTech applications with an accuracy of around 97%, and authors [10] who found that AI investment is the most significant determinant of the efficiency of fraud detection in Nigerian banks. The size of the coefficient is economically significant: a high-adopter institution will see FDE scores about 6 to 8 points higher than a low-adopter institution, ceteris paribus; this is a significant institutional capability gap relative to the sample mean FDE of 62.18 out of 100, with direct implications for financial loss prevention.

This coefficient is also robust to excluding the COVID-year (β = 0.391, $p < 0.001$) and is estimated using GMM, which addresses endogeneity (β = 0.376, $p < 0.001$), further supporting causal interpretation. The results of the present study are consistent with the population-level findings of ACFE (2024) that proactive data analysis can cut fraud losses by more than 50% at the median; the institutional-level regression findings in the present study complement and elaborate on the population-level findings of ACFE (2024) with panel-based precision [18].

Internal Control Systems and Cybersecurity Infrastructure. Internal control systems (β = 0.238, $p < 0.001$) and cybersecurity infrastructure (β = 0.196, $p < 0.05$) were the second- and third-strongest predictors of FDE, respectively. This discovery aligns with the authors [6], who suggest that the effectiveness of AI in financial institutions depends on the cybersecurity and control architecture in which AI tools are used. The takeaway is significant: AI investments without parallel investments in internal controls and cybersecurity will yield suboptimal fraud detection. AI acts as a monitoring guardian, and strong internal controls complement this role by limiting the opportunity element of fraud, thereby further constraining the fraud opportunity space when both are in place. This complementarity is confirmed by source [18], which shows that organisations that integrated internal audit roles with proactive data analysis controls achieved the best overall fraud-prevention results.

Regulatory Compliance and Technology Readiness. Positive and marginally significant coefficients were obtained for regulatory compliance (β = 0.143, $p = 0.057$) and technology readiness (β = 0.119, $p = 0.058$). According to Institutional Theory, the greater the regulatory pressure, the more likely it is that technology will be adopted and the process improved. In contrast, TAM suggests that the higher the technology readiness level, the more effective AI use will be [8]. The marginal significance may be due to the AI governance frameworks established by CBN for fraud detection still being developed during

2019-2023, so regulatory pressure was not uniform across the board, as noted by the authors [7] in their study on bank adoption in Nigeria. Technology readiness scores derived from TAM-based self-report instruments can also capture intent and perception rather than deployment quality, potentially leading to measurement attenuation.

Firm Size. The coefficient for firm size was positive and weakly significant ($\beta = 0.087$, $p = 0.092$), indicating that the quality of AI deployment and internal control design is more important than firm size in determining fraud detection capability in the Nigerian FinTech banking sector. The size gap in financial resources for investing in AI and the complexity of compliance functions are not enough to offset the gap in detection efficiency between high AI adopters and low AI adopters at the same size.

CONCLUSIONS

The study analysed how the use of Artificial Intelligence (AI) in FinTech systems affects the efficiency of fraud detection in accounting systems, using panel data from 40 financial institutions in Nigeria from 2019 to 2023. A key finding that strengthens the use of machine learning and deep learning tools in institutional fraud risk management is empirical evidence that AI can significantly and robustly improve the efficiency of fraud detection. The internal control systems and cybersecurity infrastructure are validated as independent factors with a significant impact, akin to the integrated AI-cybersecurity-governance framework proposed by the authors [6]. Regulatory compliance and technology readiness have positive yet contextually moderated impacts, indicating the dynamic regulatory and institutional readiness environment within the Nigerian FinTech sector. All major findings are consistent across various estimation methods, including the GMM specification, and the model accounts for around 61% of the variance in FDE. Theoretically, the results support the validity of the RAT, the Fraud Triangle, the TAM, and Institutional Theory as frameworks for mitigating fraud in AI-enabled FinTech markets.

Recommendations

1) Executives of financial institutions should focus on strategic investment in AI for accounting and transaction monitoring processes, while also investing in internal control frameworks and cybersecurity infrastructure to achieve the complementary multiplier effect observed in this study.

2) The Central Bank of Nigeria and NDIC should expedite the formulation of clear, enforceable AI governance guidelines for anti-fraud applications. Enforcement of more consistent, stringent regulations, such as minimum capital requirements reforms that have led to banking consolidation, could have a major impact on the level of adoption of sectoral AI and its potential to prevent fraud.

3) Small FinTech institutions with lower scores on the AI adoption distribution should begin by incrementally integrating tools for real-time transaction anomaly detection and journal entry monitoring. In sum, both authors [3, 4] confirm that even partial implementation of AI can yield substantial improvements in detection efficiency over rule-based solutions.

4) Future research should build on this study by: a) Using longer panel periods to explore long-run AI capability-building trajectories; b) Comparing AI adoption across sub-Saharan African FinTech markets; and c) Exploring the moderating effect of the explainability dimension of AI adoption on the trust and compliance dimension of fraud detection effectiveness.

Limitations. The institutional officer self-reports for the AI adoption and internal control constructs may lead to response bias. The five-year panel may not be sufficient to capture the long-term nature of the capability-building process. The researchers cannot directly generalise the findings from the Nigerian sample to other emerging-market contexts.

REFERENCES

1. ACFE. (2024). *Occupational Fraud 2024: A Report to the Nations.* Retrieved from https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

2. PWC. (2022). PwC's Global Economic Crime and Fraud Survey 2022. Retrieved from https://www.pwc.com/gx/en/services/forensics/economic-crime-survey/2022.html

3. Shoetan, P. O., & Familoni, B. T. (2024). Transforming Fintech Fraud Detection with Advanced Artificial Intelligence Algorithms. *Finance & Accounting Research Journal, 6*(4), 602–625. doi: 10.51594/farj.v6i4.1036

4. Ali, A., Razak, S. A., 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

5. Barroso, M., & Laborda, J. (2022). Digital transformation and the emergence of the Fintech sector: Systematic literature review. *Digital Business, 2*(2), 100028. doi: 10.1016/j.digbus.2022.100028

6. Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance, 60*, 101616. doi: 10.1016/j.ribaf.2022.101616

7. John, S. A., Shonubi, J. A., Azuikpe, P. F., & Ologun, V. O. (2025). Adoption of AI-Driven Fraud Detection System in the Nigerian Banking Sector: An analysis of cost, compliance, and competency. *ArXiv.org.* doi: 10.48550/arxiv.2511.00061

8. Rahman, M., Ming, T. H., Baigh, T. A., & Sarker, M. (2021). Adoption of artificial intelligence in banking services: an empirical analysis. *International Journal of Emerging Markets, 18*(10), 4270–4300. doi: 10.1108/ijoem-06-2020-0724

9. Wu, P., & Chen, Y. (2024). Enhanced detection of accounting fraud using a CNN-LSTM-Attention model optimised by Sparrow search. *PeerJ Computer Science, 10*, 2532. doi: 10.7717/peerj-cs.2532

10. Oluwadare, O. E., Adekanmbi, J. A., & Omodara, B. E. (2025). Artificial Intelligence and Fraud Prevention in Nigerian Deposit Money Banks (DMBs). *Acta Universitatis Danubius. Economica, 21*(3), 128-150

11. Fariha, N., Khan, M. N. M., Hossain, M. I., Reza, S. A., Bortty, J. C., Sultana, K. S., Jawad, M. S. I., Safat, S., Ahad, M. A., & Begum, M. (2025). Advanced fraud detection using machine learning models: enhancing financial transaction security. *International Journal of Accounting and Economics Studies, 12*(2), 85–104. doi: 10.14419/c73kcb17

12. Zhao, Z., & Bai, T. (2022). Financial fraud detection and prediction in listed companies using SMOTE and machine learning algorithms. *Entropy, 24*(8), 1157. doi: 10.3390/e24081157

13. Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity approach. *American Sociological Review, 44*(4), 588. doi: 10.2307/2094589

14. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. doi: 10.2307/249008

15. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of Information Technology: toward a unified view. *MIS Quarterly, 27*(3), 425–478. doi: 10.2307/30036540

16. DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage revisited: institutional isomorphism and collective rationality in organisational fields. *American Sociological Review, 48*(2), 147. doi: 10.2307/2095101

17. Cressey, D. R. (1950). The criminal violation of financial trust. *American Sociological Review, 15*(6), 738. doi: 10.2307/2086606

18. ACFE. (2022). *Occupational Fraud 2022: A Report to the Nations*. Retrieved from https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

19. Hafez, I. Y., Hafez, A. Y., Saleh, A., El-Mageed, A. a. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data, 12*(1). doi: 10.1186/s40537-024-01048-8

20. NDIC. (2022). *Annual Report & Statement of Accounts*. Retrieved from https://ndic.gov.ng/wp-content/uploads/2024/08/2022-Annual-Report.pdf

21. NDIC. (2023). *Audited Financial Statements for the Year Ended 31 December 2023*. Retrieved from https://ndic.gov.ng/wp-content/uploads/2024/05/NDIC-2023-Signed-Audited-Financial-Statement.pdf

22. Central Bank of Nigeria. (n. d.). Financial Stability Reports. Retrieved from https://www.cbn.gov.ng/documents/financialstabilityreport.html