ICFB-UCB-2026-053

Artificial Intelligence and Fraud Detection Efficiency in Commercial Banks in Nigeria: Evidence from Calabar Metropolis, Cross River State

Mendie Enyieokpon[1], Samuel, Onyeka Bright[1] and Ofem Okpoloku Bassey[1]

[1]Department of Banking and Finance, University of Calabar, Calabar, Nigeria
Corresponding Author: mendieenyieokponsamuel@unical.edu.ng

Abstract

This study investigated the effect of Artificial Intelligence (AI) on the efficiency of fraud detection in commercial banks in Nigeria, focusing on the Calabar Metropolis, Cross River State. A descriptive survey design with a quantitative approach was adopted, and primary data were collected from 124 valid banking professionals across Fraud Forensics, IT/Cybersecurity, Risk Management, and Digital Banking Operations departments using the AI and Fraud Detection Survey (AIFDS) questionnaire. Four AI dimensions, machine learning algorithms, deep learning systems, AI-driven operational processes, and IT infrastructure quality, served as independent variables, with fraud detection efficiency as the dependent variable. Data were analyzed using descriptive statistics, Pearson correlation, simple linear regression, and multiple regression via SPSS Version 29. Findings revealed that all four AI dimensions have significant positive effects on fraud detection efficiency: machine learning algorithms ($\beta = 0.647$, $R^2 = 0.419$, $p < 0.01$) emerged as the strongest individual predictor, followed by AI-driven operational processes ($\beta = 0.638$, $R^2 = 0.407$, $p < 0.01$), deep learning systems ($\beta = 0.619$, $R^2 = 0.383$, $p < 0.01$), and IT infrastructure quality ($\beta = 0.573$, $R^2 = 0.328$, $p < 0.01$). All four null hypotheses were rejected at the 0.01 significance level. Jointly, the four dimensions explained 58.4% of the variance in fraud detection efficiency (Adjusted $R^2 = 0.571$, $F(4,119) = 41.77$, $p < 0.01$), with the regression equation $FDE = 0.384 + 0.271(MLA) + 0.238(DLS) + 0.254(AID) + 0.196(ITF)$. The study concludes that AI is a statistically significant and strategically indispensable determinant of fraud-detection efficiency in Nigerian commercial banking, and recommends that banks adopt an integrated, multi-dimensional AI strategy, prioritize IT infrastructure investment, and institutionalize real-time, AI-powered transaction monitoring to curtail escalating financial fraud.

Keywords: Artificial Intelligence; Machine Learning; Deep Learning; Fraud Detection Efficiency; Nigerian Commercial Banks; IT Infrastructure; Calabar Metropolis

INTRODUCTION

The digital transformation of the Nigerian banking sector has fundamentally altered the landscape of financial services, moving from brick-and-mortar dependency to a hyper-connected, real-time ecosystem. However, this evolution has been shadowed by a sophisticated and relentless surge in cyber-malfeasance. As of 2026, the Nigerian financial industry finds itself at a critical juncture where traditional rule-based defence mechanisms have become dangerously obsolete. In their place, Artificial Intelligence (AI) has emerged not merely as a technological upgrade, but as

the foundational pillar of modern fraud detection and institutional resilience (Aljunaid et al., 2025; Ononiwu, 2024).

The scale of the crisis is documented in staggering detail by recent industry reports. According to the Nigeria Inter-Bank Settlement System (NIBSS, 2025), losses attributed to digital fraud soared to ₦52.26 billion in 2024, representing a nearly 200% year-on-year increase from the ₦17.67 billion recorded in 2023. The Financial Institutions Training Centre (FITC, 2025) further noted that fraud incidents involving web-based platforms and mobile apps grew by over 360% in the first half of 2025. These figures underscore a sobering reality: as banks innovate to provide seamless customer experiences, cyber-syndicates are innovating with equal or greater velocity to exploit the structural vulnerabilities of the digital trust economy.

Traditional rule-based systems, which operate on static if-then logic, are fundamentally reactive and incapable of detecting modern fraud typologies including social engineering, account takeover (ATO), and SIM-swapping tactics that mimic legitimate user behaviour. These systems suffer from high False Positive Rates (FPR), customer friction, and critical detection latency — often identifying fraud only after funds have been cleared and exited the system (Aljunaid et al., 2025). AI, encompassing Machine Learning (ML), Deep Learning (DL), and Anomaly Detection, offers a paradigmatic shift from reactive to predictive and proactive defence architecture. Unlike human-coded rules, AI algorithms learn from vast historical datasets, identifying subtle, non-linear correlations that human auditors cannot perceive, assigning real-time risk scores to every transaction (Akinnagbe & Akintayo, 2025).

Despite the clear strategic imperative, the adoption of AI in Nigerian commercial banking remains fragmented and constrained by an infrastructure-capability gap, a technical brain drain, and data quality limitations (NITDA, 2025; Ibrahim & Yusuf, 2025). The Central Bank of Nigeria's 2024 Risk-Based Cybersecurity Framework mandates real-time AI-driven monitoring across all electronic channels, yet empirical evidence on the differential effectiveness of specific AI dimensions remains scarce, particularly in geographically underrepresented commercial centres such as Calabar Metropolis.

This study addresses that gap by empirically investigating the effect of four AI dimensions — machine learning algorithms, deep learning systems, AI-driven operational processes, and IT infrastructure quality — on fraud detection efficiency in commercial banks in Calabar Metropolis, Cross River State. The paper is structured as follows: Section 2 presents the theoretical frameworks; Section 3 reviews the conceptual and empirical literature; Section 4 outlines the methodology; Section 5 presents findings and discussion; and Section 6 provides conclusions and recommendations.

2. THEORETICAL FRAMEWORK

2.1 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), originally proposed by Davis (1989), posits that technology adoption is driven by Perceived Usefulness (PU) — the degree to which a system enhances job performance — and Perceived Ease of Use (PEOU) — the degree to which the system is free from effort. In the AI fraud detection context, banking professionals are more likely to accept and optimise AI systems when they perceive these systems as genuinely effective at reducing fraud losses and as operationally manageable without prohibitive complexity. TAM has evolved through TAM2 (Venkatesh & Davis, 2000), TAM3 (Venkatesh & Bala, 2008), and the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003), each incorporating additional contextual determinants relevant to institutional technology adoption.

2.2 Fraud Diamond Theory

The Fraud Diamond Theory (Wolfe & Hermanson, 2004) extends the classic Fraud Triangle by adding a fourth element — Capability — to the existing triad of Pressure, Opportunity, and Rationalisation. In the Nigerian banking context, the capability element is particularly significant: modern fraud perpetrators demonstrate technical sophistication, positional access, and advanced concealment abilities that legacy detection systems cannot address. AI directly counters the capability element by deploying deep learning architectures capable of detecting multi-layered concealment strategies, adversarial transaction patterns, and synthetic identity constructs that exceed the discriminative capacity of shallower models (Hussaini et al., 2024).

2.3 Resource-Based View (RBV)

The Resource-Based View (Barney, 1991; Wernerfelt, 1984) posits that firms achieve sustained competitive advantage through internal resources that are Valuable, Rare, Imperfectly Imitable, and Organised (VRIO). Applied to AI fraud detection, proprietary ML models trained on bank-specific historical transaction data, integrated AI operational capabilities, and high-quality IT infrastructure constitute VRIO-compliant strategic assets. Banks that develop and protect these resources achieve superior fraud detection performance that competitors cannot readily replicate, generating durable competitive advantage in the banking sector's trust economy (Oladapo, 2024).

3. CONCEPTUAL FRAMEWORK AND LITERATURE REVIEW

3.1 Conceptual Framework

The conceptual framework posits direct causal relationships between four AI dimensions (independent variables) and fraud detection efficiency (dependent variable) in Nigerian commercial banks. The framework integrates TAM's adoption logic, the Fraud Diamond's perpetrator capability dynamics, and the RBV's strategic resource perspective into a unified predictive model.

Independent Variables (AI Dimensions)	Direction	Dependent Variable
Machine Learning Algorithms (MLA)	→	
Deep Learning Systems (DLS)	→	Fraud Detection Efficiency (FDE)
AI-Driven Operational Processes (AID)	→	(Fraud Loss Reduction • Real-Time Detection • False Positive Reduction)
IT Infrastructure Quality (ITF)	→	

Figure 1. Conceptual Framework: AI Dimensions and Fraud Detection Efficiency. Source: Author's compilation (2025).

Model Equation: $FDE = \beta_0 + \beta_1(MLA) + \beta_2(DLS) + \beta_3(AID) + \beta_4(ITF) + \varepsilon$

3.2 Machine Learning Algorithms

Machine learning algorithms have emerged as the primary defence against transactional fraud in Nigerian banks. Supervised models including Random Forest, Logistic Regression, and Gradient Boosting analyse historical transaction data to classify activities as legitimate or fraudulent, while unsupervised anomaly detection algorithms establish behavioural baselines and flag deviations in real time (Okeowo & Olaniyi, 2022; Adebayo & Ogunleye, 2024). Studies document fraud detection accuracy rates of 85–97% for ML systems, substantially exceeding the 60–75% typical of rule-based alternatives, with loss reductions of 40–68% in the first year of deployment (Adebayo & Ogunleye, 2024).

3.3 Deep Learning Systems

Deep neural networks, characterised by multi-layer architectures capable of processing unstructured data, have proven particularly effective for detecting complex fraud typologies including synthetic identity fraud, adversarial payment manipulation, and deepfake-enabled account takeover. Ibrahim and Yusuf (2025) documented a 25% improvement in cross-border money laundering detection in Tier-1 Nigerian banks integrating deep learning. The Fraud Diamond's capability element — which encompasses sophisticated concealment abilities — is directly countered by deep learning's capacity to cross-reference multiple data streams and detect the artefacts of AI-generated synthetic fraud (Eze et al., 2025).

3.4 AI-Driven Operational Processes

The operational embedding of AI in banking functions — real-time transaction monitoring, AI-powered KYC, AML screening, behavioural biometrics, and automated fraud case prioritisation — transforms algorithmic capability into institutional fraud detection performance. Ngozi and Chidiebere (2024) demonstrated that AI-driven AML monitoring reduced false positive rates from 94.7% (rule-based) to 78.3% (AI-driven) while increasing genuine suspicious transaction identification by 23.4% in Nigerian commercial banks. From an RBV perspective, AI-embedded operational capabilities constitute dynamic, hard-to-imitate organisational competencies that generate sustained competitive advantage (Barney, 1991).

3.5 IT Infrastructure Quality

The robustness, scalability, and reliability of IT infrastructure — encompassing server capacity, network bandwidth, cloud computing access, and integrated data environments — constitutes the foundational prerequisite for AI model performance. The Nigerian banking sector confronts a documented infrastructure-capability gap: high cloud computing costs, data silo fragmentation, inadequate compute power, and erratic power supply constrain AI model training quality and operational uptime (NITDA, 2025; Nnaomah et al., 2024). Research demonstrates that data quality improvements alone can enhance AI detection performance by 30–50% without algorithmic changes, confirming infrastructure as the highest-yield investment opportunity in the AI fraud detection ecosystem (Kayode & Mojisola, 2024).

3.6 Research Gap

Despite the substantial body of evidence on AI fraud detection effectiveness in Nigerian banking, critical gaps persist: no published study has simultaneously examined all four AI dimensions in an integrated regression framework targeting banking professionals in Cross River State; the Calabar Metropolis context remains empirically underrepresented; and no study captures

the post-2019 Finance Act and 2024 CBN Cybersecurity Framework reform environment with its associated digital compliance obligations. This study addresses all three gaps.

4. METHODOLOGY

4.1 Research Design and Study Area

The study adopted a descriptive survey research design with a quantitative approach, appropriate for objectively examining relationships among study variables without experimental manipulation (Kothari, 2004). The study area is Calabar Metropolis — the administrative capital of Cross River State, Nigeria — a significant regional financial hub hosting concentrated commercial bank branches along Ndidem Usang Iso (Marian) Road, Calabar Road, and the Calabar Free Trade Zone.

4.2 Population and Sampling

The target population comprised specialised banking professionals in the 24 licensed commercial banks operating in Calabar Metropolis, specifically staff in Fraud Forensics and Internal Audit, IT and Cybersecurity, Risk Management and Compliance, and Digital Banking Operations — estimated at 210 personnel. Purposive sampling was applied to ensure only professionals with direct knowledge of AI-driven fraud systems were included. The Taro Yamane (1967) formula ($n = N / [1 + N(e)^2]$, where $e = 0.05$) yielded a minimum sample of 138, to which 10% was added for non-response, producing a final administered sample of 138 questionnaires.

4.3 Instrument and Data Collection

Primary data were collected using the AI and Fraud Detection Survey (AIFDS), a structured questionnaire comprising two sections: Section A (demographic profile) and Section B (30 Likert-scale items, 6 per construct, scored 1–5 from Strongly Disagree to Strongly Agree). Content validity was established through expert review by academics in Banking and Finance and alignment with the 2024 CBN Risk-Based Cybersecurity Framework. Reliability was confirmed via pilot test Cronbach's Alpha coefficients of $\alpha = 0.82$ (MLA), 0.84 (DLS), 0.80 (AID), 0.78 (ITF), and 0.86 (FDE) — all exceeding the 0.70 minimum threshold (Nunnally, 1978).

4.4 Data Analysis

Data were analysed using SPSS Version 29 employing: (i) descriptive statistics (means and standard deviations) to characterise variable distributions; (ii) Pearson Product-Moment Correlation to examine bivariate relationships and assess multicollinearity; (iii) simple linear regression for individual hypothesis testing of each AI dimension; and (iv) multiple linear regression for joint model estimation. All hypotheses were tested at the $\alpha = 0.05$ significance level, with null hypotheses rejected where $p < 0.05$.

5. RESULTS AND DISCUSSION

5.1 Response Rate and Demographic Profile

Of the 138 questionnaires administered, 131 were returned (94.9% response rate) and 124 were valid for analysis (effective valid response rate of 89.9%), exceeding the 70% minimum threshold recommended by Oluwadare et al. (2025). The sample was dominated by male respondents (62.9%), mid-career professionals aged 26–35 years (41.1%), postgraduate degree holders (49.2%), and IT/Cybersecurity specialists (30.6%). Tier-1 bank staff constituted 51.6% of the sample, ensuring representation of institutions with the most advanced AI fraud detection infrastructure.

Table 1: Demographic Profile of Respondents (N = 124)

Variable	Category	Frequency (n)	% (%)
Gender	Male	78	62.9
	Female	46	37.1
Age Group	18–25 years	18	14.5
	26–35 years	51	41.1
	36–45 years	42	33.9
	46 years & above	13	10.5
Education	HND/B.Sc.	43	34.7
	Postgraduate (M.Sc./MBA)	61	49.2
	Professional (ACIB/CISA)	20	16.1
Department	Fraud Forensics/Internal Audit	34	27.4
	IT/Cybersecurity	38	30.6
	Risk Management/Compliance	31	25.0
	Digital Banking Operations	21	16.9
Experience	< 2 years	15	12.1
	2–5 years	38	30.6
	6–10 years	46	37.1
	> 10 years	25	20.2
Bank Tier	Tier-1 Bank	64	51.6
	Tier-2 Bank	43	34.7
	Other Commercial Bank	17	13.7

Source: Field Survey, 2026.

5.2 Reliability Analysis

Table 2: Cronbach's Alpha Reliability Coefficients

Construct	No. of Items	Cronbach's α	Decision
Machine Learning Algorithms (MLA)	6	0.82	Reliable
Deep Learning Systems (DLS)	6	0.84	Reliable
AI-Driven Operational Processes (AID)	6	0.80	Reliable
IT Infrastructure Quality (ITF)	6	0.78	Reliable
Fraud Detection Efficiency (FDE)	**6**	**0.86**	**Reliable**

Note: Minimum acceptable threshold α ≥ 0.70 (Nunnally, 1978). Source: Field Survey, 2026.

5.3 Descriptive Statistics

Table 3: Descriptive Statistics for Key Variables (N = 124)

Variable	N	Min	Max	Mean	Std. Dev.	Interpretation
Machine Learning Algorithms (MLA)	124	1.00	5.00	3.94	0.73	Positive – High adoption
Deep Learning Systems (DLS)	124	1.00	5.00	3.71	0.82	Positive – Moderate-High
AI-Driven Operational Processes (AID)	124	1.00	5.00	3.83	0.77	Positive – High integration
IT Infrastructure Quality (ITF)	124	1.00	5.00	3.47	0.91	Moderate – Gap identified
Fraud Detection Efficiency (FDE)	124	1.00	5.00	**3.78**	0.80	Positive – Effective
Reduction in Fraud Losses	124	1.00	5.00	3.86	0.79	Strongest FDE dimension
Real-Time Detection Capability	124	1.00	5.00	3.82	0.81	High effectiveness
False Positive Rate Reduction	124	1.00	5.00	3.65	0.84	Lowest FDE sub-dimension

Note: 5-point Likert scale (1 = Strongly Disagree; 5 = Strongly Agree). Source: Field Survey, 2026.

Machine learning algorithms recorded the highest mean (Mean = 3.94, SD = 0.73), indicating robust adoption and perceived effectiveness. AI-driven operational processes followed (Mean = 3.83), then deep learning systems (Mean = 3.71). IT infrastructure quality recorded the

lowest mean (Mean = 3.47, SD = 0.91), reflecting the persistent infrastructure-capability gap documented in Nigerian banking literature (NITDA, 2025; Ibrahim & Yusuf, 2025). The composite Fraud Detection Efficiency variable recorded a mean of 3.78 (SD = 0.80), with fraud loss reduction as the highest-scoring dimension (Mean = 3.86) and false positive rate reduction as the lowest (Mean = 3.65).

5.4 Pearson Correlation Analysis

Table 4: Pearson Correlation Matrix (N = 124)

Variable	MLA	DLS	AID	ITF	FDE
Machine Learning Algorithms (MLA)	1.000	0.623**	0.591**	0.488**	0.647**
Deep Learning Systems (DLS)	0.623**	1.000	0.574**	0.463**	0.619**
AI-Driven Operational Processes (AID)	0.591**	0.574**	1.000	0.512**	0.638**
IT Infrastructure Quality (ITF)	0.488**	0.463**	0.512**	1.000	0.573**
Fraud Detection Efficiency (FDE)	**0.647****	**0.619****	**0.638****	**0.573****	**1.000**

*** Correlation significant at the 0.01 level (2-tailed). Source: Field Survey, 2026.*

All four AI dimensions are significantly and positively correlated with fraud detection efficiency at the 0.01 level. Machine learning algorithms recorded the strongest bivariate correlation (r = 0.647), followed by AI-driven operational processes (r = 0.638), deep learning systems (r = 0.619), and IT infrastructure quality (r = 0.573). Inter-correlations among predictors range from 0.463 to 0.623, none exceeding the 0.70 multicollinearity threshold, confirming all variables are suitable for simultaneous multiple regression entry.

5.5 Hypothesis Testing: Individual Regression Results

Table 5 presents the simple regression results for each of the four null hypotheses. All hypotheses were tested at the $\alpha = 0.05$ significance level using the decision rule: reject H_0 if $p < 0.05$.

Table 5: Simple Linear Regression Results — Individual AI Dimensions on Fraud Detection Efficiency (N = 124)

Hypothesis	Predictor	R	R^2	β	t	F	p-value	Decision
H_{o1}	Machine Learning Algorithms (MLA)	0.647	0.419	0.647	9.413	88.60	0.000**	**Rejected**

Hypothesis	Predictor	R	R^2	β	t	F	p-value	Decision
Ho_2	Deep Learning Systems (DLS)	0.619	0.383	0.619	8.738	76.35	0.000**	**Rejected**
Ho_3	AI-Driven Operational Processes (AID)	0.638	0.407	0.638	9.183	84.33	0.000**	**Rejected**
Ho_4	IT Infrastructure Quality (ITF)	0.573	0.328	0.573	7.744	59.97	0.000**	**Rejected**

*** p < 0.01. Dependent Variable: Fraud Detection Efficiency (FDE). Source: Field Survey, 2026.*

5.6 Joint Multiple Regression Model

Table 6: Multiple Regression — Joint Effect of AI Dimensions on Fraud Detection Efficiency (N = 124)

Predictor Variable	Std. Beta (β)	Std. Error	t-value	p-value	VIF
(Constant)	0.384	0.201	1.910	0.058	—
Machine Learning Algorithms (MLA)	0.271	0.067	4.045	0.000**	1.68
Deep Learning Systems (DLS)	0.238	0.071	3.352	0.001**	1.72
AI-Driven Operational Processes (AID)	0.254	0.068	3.735	0.000**	1.64
IT Infrastructure Quality (ITF)	0.196	0.073	2.685	0.008**	1.48

Model Summary: R = 0.764 | R^2 = 0.584 | Adjusted R^2 = 0.571 | F(4,119) = 41.77 | p = 0.000 | All VIF values < 2.0 (no multicollinearity)**

*** p < 0.01. Dependent Variable: Fraud Detection Efficiency. Source: Field Survey, 2026.*

The joint multiple regression model is statistically significant ($F(4,119) = 41.77$, $p < 0.01$). The four AI dimensions collectively explain 58.4% of the variance in fraud detection efficiency (Adjusted $R^2 = 0.571$). The derived regression equation is:

$$FDE = 0.384 + 0.271(MLA) + 0.238(DLS) + 0.254(AID) + 0.196(ITF) + \varepsilon$$

Machine learning algorithms emerged as the strongest joint predictor ($\beta = 0.271$, $t = 4.045$, $p < 0.01$), followed closely by AI-driven operational processes ($\beta = 0.254$), deep learning systems

(β = 0.238), and IT infrastructure quality (β = 0.196). All VIF values are below 2.0, confirming the absence of problematic multicollinearity. The integrated model explains 14.9 additional percentage points of variance beyond the best single predictor (MLA, $R^2 = 0.419$), confirming that a holistic, multi-dimensional AI strategy generates substantially superior fraud detection outcomes than any single-component approach.

5.7 Discussion of Findings

The finding that machine learning algorithms exert the strongest effect on fraud detection efficiency (β = 0.647 simple; β = 0.271 joint) is consistent with TAM's prediction that perceived usefulness drives adoption and performance outcomes (Davis, 1989) and corroborates Adebayo and Ogunleye's (2024) documentation of 40–68% fraud loss reductions in Nigerian banks with mature ML deployments. The high explanatory power ($R^2 = 0.419$) reflects ML's position as the most widely operationalised AI fraud detection component in Nigerian Tier-1 and Tier-2 institutions.

The significant positive effect of deep learning systems (β = 0.619, $R^2 = 0.383$) validates the Fraud Diamond Theory's capability element: neural network architectures directly counter sophisticated fraud perpetrators by detecting the multi-layered concealment strategies — synthetic identities, adversarial transaction patterns, deepfake biometrics — that evade shallower algorithmic approaches (Wolfe & Hermanson, 2004; Ibrahim & Yusuf, 2025). The lower mean score for DLS (Mean = 3.71) relative to MLA (Mean = 3.94) reflects the higher implementation complexity of deep architectures, which smaller Nigerian banks have yet to fully operationalise.

The near-equivalent explanatory power of AI-driven operational processes (β = 0.638, $R^2 = 0.407$) and machine learning algorithms is a particularly instructive finding. It challenges the widespread misconception that deploying AI software equates to achieving fraud detection outcomes: how AI is embedded across operational workflows determines performance as decisively as algorithmic sophistication itself. This result validates the RBV's proposition that AI-embedded operational capabilities constitute hard-to-imitate organisational resources that generate sustained competitive advantage (Barney, 1991).

The significant positive effect of IT infrastructure quality (β = 0.573, $R^2 = 0.328$), despite recording the lowest mean (Mean = 3.47) and lowest individual explanatory power, constitutes the most policy-relevant finding of this study. It implies that improvements in infrastructure in banks currently constrained by data silos, inadequate compute, and unreliable connectivity would generate substantial fraud detection efficiency gains — confirming IT infrastructure as the highest-yield investment opportunity for improving AI fraud detection in Nigerian commercial banking (NITDA, 2025; Kayode & Mojisola, 2024).

6.1 Conclusions

This study provides robust empirical evidence that Artificial Intelligence — operationalised across machine learning algorithms, deep learning systems, AI-driven operational processes, and IT infrastructure quality — is a statistically significant and strategically indispensable determinant of fraud detection efficiency in commercial banks in Nigeria. All four null hypotheses were rejected at the 1% significance level. The four AI dimensions collectively explain 58.4% of variance in fraud detection efficiency (Adjusted $R^2 = 0.571$), confirming that the transition from rule-based to AI-driven fraud defence represents a quantifiable operational necessity for Nigerian commercial banks confronting the ₦52.26 billion annual fraud crisis (NIBSS, 2025).

The study theoretically validates the Technology Acceptance Model in the Nigerian AI adoption context, establishes the Fraud Diamond's capability element as directly addressable through deep learning and operational AI, and confirms the Resource-Based View's prediction that AI infrastructure and operational capabilities constitute VRIO-compliant strategic assets. These findings advance the nascent empirical literature on AI fraud detection in Global South banking contexts and provide the first purposive empirical investigation of this relationship in Calabar Metropolis.

6.2 Recommendations

- **Machine Learning Governance:** Nigerian commercial banks should accelerate investment in mature machine learning frameworks, implementing quarterly retraining schedules, adversarial robustness testing, and automated performance degradation monitoring to sustain detection accuracy against adaptive fraud syndicates.
- **Deep Learning Integration:** Tier-1 and Tier-2 banks should progressively integrate deep learning architectures — particularly graph neural networks for fraud ring detection and transformer-based models for KYC verification. Smaller banks should explore vendor-provided cloud-based deep learning platforms and transfer learning arrangements.
- **Operational AI Embedding:** Bank management should treat AI-driven operational process integration as a strategic priority equal to algorithm procurement, embedding AI in every fraud-relevant function: real-time transaction monitoring, KYC, AML screening, behavioural biometrics authentication, and automated case prioritisation.
- **Infrastructure Investment Policy:** The CBN, NDPC, and NITDA should jointly develop an IT infrastructure development framework specifically targeting the structural constraints degrading AI fraud detection performance, including Sovereign Cloud incentives, mandatory data silo dismantlement standards, and edge computing subsidies.
- **Human Capital Development:** Banks should establish in-house AI talent development programmes in partnership with universities, offering competitive remuneration for AI/ML specialists and investing in upskilling programmes for existing forensics and IT personnel.

6.3 Contribution to Knowledge

This study contributes to knowledge in four ways: (i) it provides the first purposive empirical investigation of AI fraud detection specifically targeting banking professionals in Calabar Metropolis, filling a geographic gap in the Nigerian literature; (ii) it operationalises AI as a four-dimensional construct and quantifies the differential weights of each dimension in predicting fraud detection efficiency, offering greater practical precision than composite adoption indices; (iii) it advances the joint application of TAM, Fraud Diamond Theory, and RBV in an integrated multi-theoretical framework for the AI fraud detection context; and (iv) it provides a validated AIFDS instrument (Cronbach's Alpha 0.78–0.86) replicable across Nigerian states and other African banking markets.

6.4 Limitations and Future Research Directions

The study is limited by its cross-sectional design, reliance on self-reported perceptions rather than audited financial performance data, and geographic restriction to Calabar Metropolis. Future research should: (i) conduct longitudinal panel studies tracking actual fraud detection performance over time as AI investment changes; (ii) investigate the moderating role of bank size

(Tier-1 vs. Tier-2 vs. microfinance); (iii) examine adversarial ML robustness against deliberate evasion attempts; (iv) test the mediating role of Explainable AI (XAI) between AI adoption and regulatory compliance outcomes; and (v) extend comparative investigation across West African banking markets to assess whether the infrastructure-capability gap is a Nigeria-specific or pan-African constraint.

REFERENCES

Adebayo, F., & Ogunleye, T. (2024). Machine learning adoption and fraud loss reduction in Nigerian commercial banks: A four-year longitudinal analysis. *Journal of Financial Crime*, 31(3), 441–459. https://doi.org/10.1108/JFC-08-2023-0214

Akinnagbe, C., & Akintayo, M. (2025). Real-time risk scoring and AI fraud detection in Nigerian electronic payment systems. *Journal of Financial Technology*, 4(1), 22–39.

Aljunaid, M., Rahman, A., & Hassan, K. (2025). Detection latency and adversarial machine learning in banking fraud prevention systems. *Journal of Financial Intermediation*, 61, Article 101009. https://doi.org/10.1016/j.jfi.2024.101009

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. https://doi.org/10.1177/014920639101700108

Central Bank of Nigeria. (2025). Risk-based cybersecurity framework and guidelines for deposit money banks: 2024 revised edition. CBN. https://www.cbn.gov.ng

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

Eze, C., Nwosu, P., & Okafor, B. (2025). AI-verified biometric overrides and audit trail integrity in Nigerian commercial bank operations. *Journal of Banking and Finance Technology*, 8(1), 14–31.

Financial Institutions Training Centre. (2025). Fraud and forgeries in the Nigerian banking sector: Report for H1 2025. FITC Research Division. https://www.fitc-ng.com

Hussaini, M., Abubakar, S., & Idris, R. (2024). Fraud diamond theory and AI countermeasures in Nigerian banking: A conceptual integration. Nigerian Journal of Forensic Accounting, 6(1), 22–39.

Ibrahim, O., & Yusuf, A. (2025). Artificial intelligence and cross-border money laundering detection in Nigerian Tier-1 commercial banks. Journal of Financial Crime, 32(1), 88–105. https://doi.org/10.1108/JFC-07-2024-0201

Kayode, A., & Mojisola, R. (2024). Graph neural networks and fraud ring detection in Nigerian commercial banking. Journal of Financial Crime, 31(4), 901–919. https://doi.org/10.1108/JFC-09-2023-0267

Kothari, C. R. (2004). Research methodology: Methods and techniques (2nd rev. ed.). New Age International Publishers.

Ngozi, A., & Chidiebere, O. (2024). AI transaction monitoring and anti-money laundering compliance in Nigerian commercial banks: A comparative experimental study. Journal of Money Laundering Control, 27(3), 441–459. https://doi.org/10.1108/JMLC-04-2023-0058

Nigeria Information Technology Development Agency. (2025). Artificial intelligence adoption in Nigeria's financial services sector: Infrastructure readiness and capability gaps. NITDA. https://www.nitda.gov.ng

Nigeria Inter-Bank Settlement System. (2025). NIBSS fraud landscape report 2024: Annual industry statistics on electronic payment fraud. NIBSS. https://www.nibss-plc.com.ng

Nnaomah, C., Oguike, T., & Eze, P. (2024). Data quality constraints and AI model performance in Nigerian banking: A systematic analysis. African Journal of Information Systems, 16(1), 33–51.

Nunnally, J. C. (1978). Psychometric theory (2nd ed.). McGraw-Hill.

Oladapo, F. (2024). Machine learning fraud detection accuracy and false positive management in Nigerian commercial banks. African Journal of Information Technology, 16(2), 55–73.

Oluwadare, O., Abiodun, R., & Eze, C. (2025). Research methodology for quantitative banking studies in Nigeria: A practitioner guide. University of Lagos Press.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Wernerfelt, B. (1984). A resource-based view of the firm. Strategic Management Journal, 5(2), 171–180. https://doi.org/10.1002/smj.4250050207

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. The CPA Journal, 74(12), 38–42.

Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). Harper and Row.