IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Impact of digitalisation of banking operations on fraud practices in the Nigerian banking sector

Louis Eziokwubundu Odom[1], Taiwo Adewale Muritala[2], Nnanna P. Azu[3*]

[1,2]Department of Business Administration, Nile University of Nigeria, Abuja, Nigeria.
[3]Department of Economics, Air Force Institute of Technology, Kaduna, Nigeria.

Corresponding author: Nnanna P. Azu (*Email: phil4azu@yahoo.com*)

Abstract

This study investigates the impact of digitalisation of banking operations on fraud practices in the Nigerian banking sector. Specifically, it assesses how digital channels—Internet banking, mobile banking, Automated Teller Machines (ATM), Point of Sale (POS), and Unstructured Supplementary Service Data (USSD)—influence the incidence and severity of fraud across commercial banks. The research adopts a quantitative ex-post facto design, utilising secondary data from thirteen quoted Nigerian banks over ten years (2014–2023), sourced from the Nigerian Exchange Group (NGX) and related institutional reports. Analytical techniques include one-step difference Generalised Method of Moments (GMM) to address endogeneity and dynamic panel effects, and Dumitrescu–Hurlin panel Granger non-causality tests to examine directional relationships between digitalisation and fraud. The results indicate that mobile banking, ATMs, and POS usage significantly increase fraud-related losses, while Internet banking and USSD are associated with lower fraud incidence, likely due to enhanced authentication and encryption protocols. Granger causality tests reveal that adoption of digital channels—particularly mobile banking, POS, ATM, and USSD—predicts fraud occurrences, whereas past fraud does not significantly drive digital adoption. The study concludes that digitalisation has heterogeneous effects on fraud in Nigerian banks, with some channels exacerbating risks and others mitigating them. The findings underscore the importance of channel-specific security measures and proactive regulatory oversight to balance innovation with risk management. To mitigate fraud, banks should implement tailored controls for vulnerable channels, enhance monitoring and regulatory compliance, conduct continuous forensic audits, and provide targeted customer education. These measures will help ensure that the benefits of digital banking are realised while safeguarding the integrity and stability of the financial system.

Keywords: ATM, Digitalisation, Fraud, Internet banking, Mobile banking, POS.

DOI: 10.53894/ijirss.v8i6.10363
Funding: This study received no specific financial support.
History: Received: 24 July 2025 / **Revised:** 28 August 2025 / **Accepted:** 01 September 2025 / **Published:** 29 September 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

Digital banking has changed how financial services are delivered around the world. In Nigeria, the adoption of digital systems has transformed the way businesses interact with customers, streamlined operational workflows, and enhanced access to financial services for the unbanked population [1, 2]. Focused initiatives, including the Cashless Nigeria Project spearheaded by the Central Bank of Nigeria (CBN) in 2012, and the Bank Verification Number (BVN) System rolled out in 2014, have enabled enhanced operational efficiencies and streamlined identity management systems [3, 4]. Over the last decade, innovations in internet banking, mobile banking, and USSD platforms have made financial services more accessible to previously marginalised populations, thereby advancing financial inclusion in Nigeria [5].

Emerging technologies, such as artificial intelligence, blockchain, and big data analytics, enable efficient and transparent ways to enhance customer experience [6, 7]. Digital tools have fostered the formation of ecosystems around seamless transactions, broadened access to, and enhanced the personalisation of financial services. Reduced transaction costs and hyper-connected services through mobile and digital platforms result in rapid service delivery [8]. As such, digital transformation in Nigeria's banking sector extends beyond responding to global technological trends, serving as a means of economic and financial empowerment.

On the downside, fraud cases stemming from an alarming technological advancement and the ease of conducting mobile and Internet banking, such as mobile wallets, USSD, ATMs, and POS systems, among others, have and continue to vex the Nigerian banking industry. Losses to fraud cases, as captured by the NIBSS, stood at an eye-watering and possibly the highest value witnessed in the banking industry, at ₦42.6 billion in the second quarter of 2024 alone, and in the entire financial year of 2023, the projection never hit the industry's total benchmark. Such nefarious actions include, but are not limited to, identity theft, phishing, SIM swaps, insider collusion, and skimming cards [4]. The muddling loss of public confidence due to rising incidences of fraud, as highlighted, sheds distinct light on the country's financial inaccessibility and infrastructural fragility. The relentless advancement in technology, coupled with an increasing number of proliferating fraud cases, necessitates investigations to assess the relationship between digitalisation and fraud in Nigerian banking systems.

Digitalisation indeed increased access and efficiency. However, it has also created vulnerabilities that fraudsters are increasingly able to exploit. Weak encryption, customer ignorance, and internal abuses of secrecy increase risks to clients and financial institutions, as discussed in Pandey, et al. [7]. Smaller banks, especially in rural regions, are struggling with the implementation of robust cybersecurity frameworks. This aligns with other developing regions where delayed digital adoption has become a tool for exposing clients to fraud, as discussed in Bueno, et al. [9]. In the case of Nigeria, the unregulated exposure of such weaknesses risks negating the gains of the digital transformation. It also undercuts the public confidence in the electronic banking services being offered.

Fraudulent schemes evolve rapidly, often outpacing defensive measures implemented by banks. With the rise of mobile and USSD transactions, fraud typologies such as SIM swap, phishing, and malware attacks have grown more prevalent [6]. Insider-led fraud and delayed adoption of advanced cybersecurity systems further weaken institutional defences [10]. Although frameworks such as the BVN and cashless policy were intended to curb fraud, inconsistent implementation has limited their effectiveness [4]. There is, therefore, a pressing need for comprehensive research to evaluate how digitalisation contributes to fraud risks and how institutions can respond with resilient, adaptive security strategies.

The main objective of this study is to examine the impact of digitalisation on fraud practices in Nigerian banks. Specifically, the study seeks to: (i) assess the relationship between internet banking and total fraud cases; (ii) evaluate the effect of USSD usage on fraud; (iii) examine how ATMs contribute to fraud risks; (iv) analyse the influence of mobile banking on fraud; and (v) determine the extent to which POS usage is linked to fraud incidents. These objectives aim to provide an integrated understanding of how various digital channels impact fraud in the Nigerian banking sector.

The scope of the study is limited to thirteen quoted commercial banks actively engaged in digital banking services: Access Bank, Ecobank, Fidelity Bank, First Bank, FCMB, GTB, Stanbic IBTC, Sterling Bank, Union Bank, UBA, Unity Bank, Wema Bank, and Zenith Bank. The temporal coverage spans the last decade (2014–2023), a period marked by significant digital growth and a rise in fraud cases. The justification for this research lies in its potential to inform banking practice, regulatory frameworks, and customer education. By identifying vulnerabilities and assessing the effectiveness of current measures, the study contributes to the design of robust, evidence-based strategies to combat fraud while supporting a safe digital transformation in the Nigerian financial sector.

This study contributes to the existing literature by examining the nexus between digitisation and fraud in the Nigerian banking system. While there have been comprehensive studies on the impact of digitisation on financial systems [9] the relationship between the individual channels of digital banking and the risk of fraud is limited, particularly in Nigeria. This study aims to bridge the gap by analysing the role of internet banking, mobile banking, POS, ATMs, USSD, and mobile wallets in preventing fraudulent activities in Nigerian banks. Additionally, while the bulk of the literature has focused on advanced economies, this study provides novel evidence on the impact of digital banking channels on fraud in a low-income country, a context where the level of technology and regulatory environment differ significantly. This study, by including control variables such as the number of employees and productivity, provides a better understanding of how organisational factors, including size and operational efficiency, affect the incidence of fraud. This research makes a novel empirical contribution by employing the GMM and Granger causality tests to address issues of endogeneity and dynamic interrelationships in the context of fraud and digital banking. It thereby provides a comprehensive, yet robust framework for subsequent research in the area of digital banking and fraud.

Additionally, the outcomes of this study hold immense relevance for policymakers and bank regulators in Nigeria. These results suggest the need for customised strategies for fraud prevention that deal with the specific vulnerabilities of each channel. For example, this study reveals that mobile banking, ATMs, and POS systems are more susceptible to fraud, and therefore, more stringent security controls are necessary to mitigate the risk. On the other hand, this study finds that internet banking and USSD platforms can be safe, providing a platform for the Central Bank of Nigeria and relevant authorities to strengthen policy formulation for digital banking. This research also emphasises the need to develop advanced tools for fraud detection and prevention using machine learning and Artificial Intelligence, thereby deepening the existing literature on technological innovations, rather than relying on "merely spraying and praying" fraud detection mechanisms.

2. Literature Review

This study builds on the FTT-Fraud Triangle Theory and TAM-Technology Acceptance Model to provide a nuanced analysis of the current state of the banking sector in Nigeria, specifically in relation to fraud. The Fraud Triangle advanced by Cressey [11] traces the conditions of fraud to pressure, opportunity, and rationalisation. Pressures can come from the economy and the level of performance expected, as well as opportunities from controls and supervision. Rationalisation deals with the moral justifications individuals provide for unethical and fraudulent behaviour [4, 12, 13]. A substantial body of research in finance employs the model as a framework for understanding the systemic and behavioural aspects of fraud. Nigeria is a country that has, to a large extent, witnessed the technological and insider collusion associated with an increase in fraudulent activities. The FTT model helps identify gaps in defence against fraud and in constructing anti-fraud models that focus on the root causes of fraud, rather than merely addressing its symptoms.

In relation to this behavioural perspective, the Technology Acceptance Model (TAM) by Davis [14] describes the adoption of digital tools used in fraud detection and prevention. According to the model, users' propensity to accept technologies is dependent on the adoption of perceived usefulness (PU) and perceived ease of use (PEOU) of these technologies. In banking, these technologies are AI systems, blockchain, and machine learning for real-time fraud detection [15, 16]. The adoption outcomes are also impacted by organisational support, user training, and compliance with regulations as described by Winasis, et al. [3] and Fundira, et al. [17]. This research integrates TAM in the analysis to assess how banks not only implement anti-fraud technologies, but also how employees and customers use and interact with them. FTT and TAM together provide an integrated approach that explains the context of fraud and the corresponding conditions that enhance the success of technologies designed for fraud prevention.

Evidence from empirical research in Nigeria suggests that certain forms of targeted identity controls can help mitigate common types of fraud. In a survey of bank managers, Nnachi, et al. [4] noted that the Bank Verification Number used for identity management systems and identity theft significantly enhanced depositor protection. On the supervisory side, Odukoya and Samsudin [18] found that higher regulatory capability, supported by forensic expertise, is associated with fewer incidents in Deposit Money Banks. Regional evidence from East Africa suggests that manipulation risks persist where enforcement gaps remain, even when overall manipulation flags are low, underscoring the importance of credible oversight [19]. Sectoral monitoring reports also document ongoing losses in digital channels, indicating that operational and analytical controls must complement identification measures [4].

A growing body of studies links digital transformation to new control possibilities, particularly through the use of distributed ledgers and data-driven operations. Rahman, et al. [20] identified and mapped four thematic areas within the blockchain-and-banking scholarship that intersect with artificial intelligence, as well as Industry 4.0, and argued that these streams could transform compliance and audit trails. Syntheses of digitalisation in finance also emphasise that, for advanced analytics and platform architectures in the financial services sector to function effectively, institutional preparedness and transparent governance are essential [21, 22]. Reviews of digital financial services further connect technology adoption to human development outcomes through inclusion, skills, and literacy, which are relevant for both customer protection and fraud resilience [8, 23].

Machine-learning studies provide evidence that model choice, feature engineering, and imbalance handling materially affect fraud detection performance. Using genetic algorithms for feature selection, Ileberi, et al. [24] reported accuracy gains across random forest, neural networks, and logistic regression. Kasasbeh, et al. [25] showed that multilayer perceptrons improved precision and sensitivity relative to conventional classifiers. Nguyen, et al. [15] demonstrated that segmenting users into "new" and "old" cohorts and pairing CatBoost with deep networks raised area-under-curve performance. An ensemble of LSTM with AdaBoost achieved very high sensitivity and specificity on imbalanced card data [16]. Complementary work with discriminant analysis and support vector machines confirmed that preprocessing and choice of algorithm jointly determine out-of-sample detection rates [26].

Evidence on organisational and behavioural defences highlights the value of culture, governance, and specialist functions. Survey data from Indonesian regional banks suggest that an ethical culture weakens the link between pressure, opportunity, and occupational fraud, consistent with fraud theory predictions [27]. In South Africa, integrating forensic accounting with big data tools yielded high classification accuracy and practical clustering of red flags, suggesting a complementary approach to human analytics [12, 13]. Studies of insider cyber fraud in India stressed the importance of rapid detection and structured pre- and post-incident controls, supported by machine-learning triage [10]. Nigerian evidence further shows that embedding forensic accountants within supervisory routines strengthens prevention at the system level [18].

Adoption studies indicate that organisational capabilities are a binding constraint on the effective use of anti-fraud technologies. In Indian banking, the adoption of digital tools is associated with improved performance, with workforce agility mediating the gains from technology adoption [28]. Public-sector analyses in Korea suggest that both ICT adoption and administrative discretion foster innovative mindsets, which are crucial for sustained digital transformation [29]. Broader evidence suggests that leadership, communication, and an enabling climate influence intentions to adopt digital systems; however, organisational support often falls short of what is required for durable transformation [15, 30, 31].

Comparative work on digital transformation highlights structural and capacity barriers that can limit the effectiveness of fraud-control payoffs. Mixed-methods evidence from Indonesia catalogued internal and external obstacles to digital uptake, including funding and skill deficits that mirror constraints observed in many Nigerian institutions [12, 13, 18]. Case studies of e-government adoption in Rwanda and Afghanistan identified infrastructure, inclusion, and trust as persistent hurdles, and recommended public-private partnerships to close capability gaps [32, 33]. Reviews of public-sector IT adoption and blockchain use in government have noted that success requires more than just tools; it also requires strategies, governance, and legal frameworks that translate technologies into credible processes [34, 35].

Ultimately, multi-industry studies confirm that digitalisation enhances performance when aligned with strategy, investment, and learning, which has direct implications for banking fraud control. Research in European process industries has found that digital adoption supports radical product innovation, while efficiency gains depend on the sector context and the matching of capabilities [36]. Conceptual and empirical work on digital transformation stresses the progression from digitisation to full transformation and the organisational resources required at each stage [22, 37]. Evidence from firm studies confirms that digital innovation raises productivity and competitiveness when supported by governance and location-specific policies [38]. Together with inclusion-oriented reviews, these results suggest that Nigerian banks will derive more substantial benefits from fraud mitigation when technology deployment is combined with culture, skills, and oversight [22, 23].

3. Methodology

3.1. Model Specification

In evaluating the influence of digital banking on fraud practices and prevention, Nnachi, et al. [4], Akinbowale, et al. [13] and Akinbowale, et al. [12] proxied the elements of digitalisation to include Internet banking (INB), mobile banking (MBK), automated teller machines (ATM), Point-of-Sale (POS) systems and Unstructured Supplementary Service Data (USS). They presented these elements of digitalisation as the independent variables and fraud prevention as the dependent variable. The model was given as follows:

$$FRD_i = \beta_0 + \beta_1 INB_i + \beta_2 MBT_i + \beta_3 ATM_i + \beta_4 POS_i + \beta_4 USS_i + \mu_i \qquad 1$$

Where;

FRD_i represent the Total number of Fraud Cases, INB_i is internet banking, USS_i represents Unstructured Supplementary Service Data (USS), ICT_i stands for automated teller machines (ATM), MOB_i is the mobile banking (MOB) POS_i is the Point-of-Sale (POS) systems, β_1 to β_5 are the parameters to be estimated. α_0 is the constant. μ_i is the white noise.

The inclusion of employees (EMP) and productivity (PDT) as control variables is justified because both factors significantly influence fraud dynamics and the effectiveness of digitalisation in banking. A larger workforce may increase fraud risks through insider involvement, weak monitoring, or collusion, as noted in studies emphasising the role of organisational behaviour in fraud occurrence [18, 27]. Productivity, measured as net income relative to total assets, captures managerial efficiency and resource utilisation, which can shape both the capacity to invest in fraud-prevention technologies and the incentive structures that create pressure for fraudulent practices [9, 12, 13]. By controlling for EMP and PDT, the model accounts for organisational and performance-related factors that could bias estimates, ensuring that the observed relationships between digital channels (INB, MBK, ATM, POS, and USS) and fraud reflect the actual impact of digitalisation rather than confounding influences of internal workforce dynamics and financial efficiency [4]. Therefore:

$$FRD_i = \beta_0 + \beta_1 INB_i + \beta_2 MBT_i + \beta_3 ATM_i + \beta_4 POS_i + \beta_4 USS_i + \beta_4 EMP_i + \beta_4 PDT_i + \mu_i \qquad 2$$

3.2. Estimation Technique

Relating the methodological discussion to the topic "Impact of Digitalisation of Banking Operations on Fraud Practices in the Nigerian Banking Sector" and the study's objectives, the choice of the one-step difference GMM and the Dumitrescu–Hurlin panel Granger causality test is both methodologically sound and directly relevant. The one-step difference GMM estimator, introduced by Arellano and Bond [39] and extended by Arellano and Bover [40] and Blundell and Bond [41] is particularly suitable for dynamic panel models where lagged dependent variables are correlated with the error term. It corrects for endogeneity, measurement error, and unobserved heterogeneity, ensuring more reliable results than pooled OLS or fixed effects, which are prone to bias [42]. By applying GMM, this study accounts for the dynamic nature of fraud losses and the adoption of digital banking. The inclusion of control variables, such as employees (EMP) and productivity (PDT), further reduces omitted variable bias.

The Dumitrescu and Hurlin [43] Panel Granger causality test complements the GMM estimation by explicitly addressing the direction of causality between fraud and digital channels. While GMM estimates the magnitude and significance of the impact, the Granger test reveals whether digital adoption drives fraud or vice versa. This dual approach is consistent with best practices in empirical finance and banking research, where magnitude and causality must both be established for policy relevance [44] and Bowsher [45]. In this study, the Granger results indicate that mobile banking, POS, ATMs, and USSD transactions Granger-cause fraud, while fraud does not predict digital adoption. This highlights that fraud risks are primarily consequences of digital expansion. Thus, combining GMM and Granger techniques ensures robust, policy-relevant evidence for Nigerian banks and regulators. Given a hypothetical GMM model:

$$lnY_{it} = \varphi lnY_{it-1} + \gamma Z'_{it} + \beta X'_{it} + d_t + \varepsilon_{it} \qquad 3$$

Where Z is the control variable, X is the explanatory variable.

4. Results and Discussion

The descriptive statistics in Panel A reveal that fraud losses (lnFRD) have an average of 7.31 with moderate variability (std. dev. = 0.74), suggesting relative stability in fraud magnitudes across banks and years. Among the digital channels, mobile banking (lnMBT, mean = 7.42) and mobile wallets (lnMWT, mean = 8.77) show wider dispersion (std. dev. = 1.80 and 2.10, respectively), indicating rapid growth and uneven adoption across institutions. By contrast, internet banking (lnINB, mean = 8.13, std. dev. = 0.35), ATMs (lnATM, mean = 6.75, std. dev. = 0.31), and POS (lnPOS, mean = 6.71, std. dev. = 0.25) are more stable, reflecting mature usage. Employment size (lnEMP, mean = 8.78) also varies substantially across banks, while productivity (PDT) remains relatively small (mean = 0.048) with narrow variation, underscoring low but steady efficiency growth.

Table 1.
Descriptive Statistics and Correlation Matrix.

Panel A: Descriptive Statistics								
Variable	**lnFRD**	**lnINB**	**lnMBT**	**lnATM**	**lnPOS**	**lnUSS**	**lnEMP**	**PDT**
Obs	130	130	130	130	130	130	130	130
Mean	7.312	8.125	7.416	6.748	6.707	4.162	8.779	0.048
Std. dev.	0.744	0.349	1.797	0.312	0.249	1.430	0.751	0.029
Min	5.366	7.257	3.401	6.299	6.238	1.098	7.689	0.011
Max	8.800	8.491	10.238	7.284	7.088	6.444	10.240	0.099
Panel B: Correlation Matrix								
Variable	lnFRD	lnINB	lnMBT	lnATM	lnPOS	lnUSS	lnEMP	PDT
lnFRD	1							
lnINB	0.033	1						
lnMBT	0.747	0.079	1					
lnATM	0.067	0.163	0.141	1				
lnPOS	-0.019	-0.177	-0.003	0.385	1			
lnUSS	0.757	0.071	0.992	0.131	-0.005	1		
lnEMP	0.611	-0.003	0.319	-0.121	-0.046	0.359	1	
PDT	-0.057	0.215	-0.126	0.327	-0.038	-0.119	0.148	1

Panel B shows strong correlations between fraud losses and some digital channels. Fraud is highly and positively correlated with mobile banking (0.747***), mobile wallets (0.738***), and USSD (0.757***), suggesting that rising use of these platforms strongly coincides with higher fraud incidences. By contrast, fraud is weakly related to internet banking (0.0326) and negatively associated with POS (–0.0186), implying little or no connection. Employment size (0.611***) is also positively associated with fraud, consistent with insider risks discussed in prior studies. Notably, multicollinearity is evident, as mobile banking, mobile wallets, and USSD exhibit near-perfect correlations (r = 0.988–0.992***), highlighting overlapping adoption trends across these channels. These patterns suggest that while digital platforms expand access, they also intensify fraud risks, particularly in mobile-based systems.

4.1. Determination of the GMM Technique

The choice of the one-step difference GMM estimator is justified by its consistency, efficiency, and robustness in handling the dynamic nature of the dataset. Compared to pooled OLS and fixed effects, which yield biased estimates in the presence of endogeneity and autocorrelation, difference GMM corrects for these issues by using internal instruments derived from lagged variables (See Table 2). While the two-step estimators often provide asymptotically efficient estimates, they are sensitive to small-sample bias and downward-biased standard errors, which is a concern given the modest sample of 13 banks over 10 years. The one-step difference GMM produces a stable and significant coefficient for the lagged dependent variable (0.999***), aligning closely with theoretical expectations and outperforming the inconsistent two-step difference result (0.0287). This makes it the most reliable choice for estimating the dynamic relationship between digitalisation and fraud practices in Nigerian banks.

Table 2.
Summary: Difference or System GMM.

Estimators	**Coefficients (of L.lnFRD)**
Pooled OLS	0.998***
Fixed Effects	0.696***
One-Step Diff. GMM	0.999***
Two-Step Diff. GMM	0.0287
One-Step Syst. GMM	0.998***
Two-Step Syst. GMM	0.991***

4.2. Impact of Digital Banking on Fraud Practices

The one-step difference GMM results in Table 3 show that digitalisation channels exert mixed effects on fraud-related losses in Nigerian banks. The negative and significant coefficient of the lagged dependent variable (L.lnFRD = –0.9996) indicates mean reversion in fraud losses, suggesting that high fraud levels in one period are likely to be corrected in subsequent periods, consistent with adaptive security responses. Among the digital channels, mobile banking (0.295), ATM usage (0.000906), and POS transactions (0.00212) are positively and significantly associated with higher fraud losses, implying that greater reliance on these platforms may increase exposure to fraudulent activities. Conversely, internet banking (–0.000177) and USSD transactions (–0.104) exhibit negative relationships with fraud, with the latter significant at the 10% level, suggesting that these channels, possibly due to stronger authentication protocols, may mitigate fraud risks.

Table 3.
One-Step Difference GMM on the impact of Digitalisation on Fraud Practices in Quoted Nigerian Banks.

Variables	Coefficients
L.lnFRD	-0.9996***
	(0.671)
lnINB	-0.000177*
	(0.00725)
lnMBK	0.295**
	(0.136)
lnATM	0.000906**
	(0.00664)
lnPOS	0.00212**
	(0.00802)
lnUSS	-0.104*
	(0.0957)
lnEMP	1.007*
	(0.505)
PDT	0.0383
	(0.0758)
AR(1)	0.015
AR(2)	0.400
Sagan Test	0.000
Hansen Test	0.427
Observations	104
Instruments (i)	12
Number of countries (n)	13
Instrumental Ratio (n/i)	1.125
Year Dummies	Yes

Note: Robust options used; t-statistics in parentheses; *** p < 0.01, ** p < 0.05, * p < 0.1 indicate significance at 1%, 5% and 10% respectively. Estimations are done using the xtabond2 routine in Stata 18.

The number of employees (1.007) shows a positive and significant effect, indicating that larger workforce sizes might inadvertently increase fraud vulnerability through insider threats or weak internal controls. The GMM results suggest that productivity (PDT = 0.0383) has a positive but statistically insignificant effect on fraud losses. Diagnostic tests confirm the validity of the model: the AR (1) test is significant as expected, AR(2) is insignificant (0.400), ruling out serial correlation, and the Hansen test (0.427) confirms instrument validity despite the Sargan rejection, consistent with robust specifications. Overall, the findings highlight that while digitalisation drives efficiency, specific platforms—especially mobile banking and POS—are more susceptible to fraud, requiring targeted regulatory oversight and improved security infrastructure.

4.3. Granger Causality Tests

The Dumitrescu–Hurlin panel Granger causality test in Table 4 provides evidence of asymmetric causal relationships between digital channels and fraud in Nigerian banks. The results show that fraud does not Granger-cause internet banking, mobile banking, ATMs, POS, or USSD transactions, as indicated by the statistically insignificant p-values in those directions. This suggests that past fraud levels do not significantly explain future movements in digital banking usage. However, the reverse causality is observed in several channels: internet banking weakly predicts fraud at the 10% level, while mobile banking, ATM usage, and USSD transactions strongly Granger-cause fraud with p-values of 0.000, indicating that increases in these digital activities precede higher fraud incidences.

Table 4.
Dumitrescu and Hurlin [43] Granger non-causality test results.

	W-bar	Z-bar	Z-bar tilde

Fraud → Internet Banking	0.7491	-0.6398(0.5223)	-0.8072(0.4195)
Internet Banking → Fraud	1.6524	1.6634 (0.0962)	0.1639 (0.8698)
Fraud →Mobile Banking	1.3657	0.9323 (0.3512)	-0.1444 (0.8852)
Mobile Banking → Fraud	22.6403	55.1723 (0.0000)	22.7252 (0.0000)
Fraud → ATM	0.9106	-0.2280 (0.8196)	-0.6336 (0.5263)
ATM → Fraud	5.8017	12.2421 (0.0000)	4.6242 (0.0000)
Fraud → POS	1.7195	1.8344 (0.0666)	0.2359 (0.8135)
POS → Fraud	3.0874	5.3220 (0.0000)	1.7064 (0.0879)
Fraud → USSD	0.6764	-0.8249 (0.4094)	-0.8853 (0.3760)
USSD → Fraud	0.8175	11.8341 (0.0000)	4.4522 (0.0000)

Note: P-Value in Parenthesis.

For POS transactions, the results suggest a bidirectional but asymmetric relationship: fraud weakly Granger-causes POS transactions (p = 0.0666), while POS usage Granger-causes fraud (p = 0.0000 for Z-bar, 0.0879 for Z-bar tilde). This implies that fraud incidents can influence POS adoption patterns, but more importantly, increased POS usage tends to predict future fraud risks. Overall, the evidence highlights that fraud in Nigerian banks is largely a consequence of the growth in digital platforms rather than a driver of their adoption. These findings emphasise the need for banks to strengthen security frameworks, particularly in mobile banking, ATM, POS, and USSD channels, where fraud risks are most responsive to digital activity.

4.4. Discussion of Findings

The GMM results align with existing literature, which highlights that digitalisation exerts both enabling and constraining effects on fraud. The positive associations of mobile banking, ATMs, and POS channels with fraud are consistent with earlier findings that rapid digital uptake without proportionate safeguards often amplifies vulnerabilities [4, 16, 24, 25]. In contrast, the mitigating role of internet banking and USSD suggests that stronger authentication and encryption mechanisms embedded in these systems provide relatively safer avenues, echoing the arguments of Rahman, et al. [20] and Al-Emran and Griffy-Brown [22] who argue that governance and system design critically shape risk outcomes. These mixed effects strengthen the claim that fraud prevention should focus on channel-specific vulnerabilities, rather than applying standard solutions across the board [18, 19].

How Granger causality works, namely that the use of mobile banking, ATMs, POS, and USSD greatly forecasts future fraud losses, shows that fraud is fundamentally a result of digital expansion rather than a cause of it. This is consistent with the global literature, which shows that the use of technology is often associated with an increase in fraudulent activities due to vulnerabilities in the system or poorly managed oversight [10, 12, 13, 23, 27]. The absence of evidence that fraud predicts future use of digital channels also highlights the notion that customers gravitate towards convenience, irrespective of the apparent risks. This also supports the observations of Twizeyimana, et al. [32] who found that users in developing contexts tend to adopt digital tools despite the presence of operational constraints or risks, as the need is too great. Thus, the primary direction of causality is from digitalisation to fraud, which points to the need for governance frameworks to mitigate the unintended consequences of technology expansion [34, 35].

The fraud adoption paradox, as observed in POS transactions, equally demonstrates the multi-layered complexities underlying user behaviour and fraud risks. As fraud schemes targeting POS terminals become more prevalent, the adoption of POS systems widens, and the association of POS use and trust is user perception and behaviour shifts become more pronounced. This dynamic is consistent with Blichfeldt and Faullant [36] and Akinbowale, et al. [12] who state that the sectoral context and responsive strategising for which the benefits of digital adoption are ravenously argued are bifurcated. Furthermore, Huang, et al. [38] and Li, et al. [37] argue that the ever-sustained and consistent performance improvements that come from digital innovation are results of further, extra, and additional investments in culture, domain, conduct, and expertise oversight. These authors' findings in the Nigerian context does mean that banks must not only and merely secure the POS systems, but also, and more so, construct an active customer fraud trust and reporting management system with constant monitoring, which resonates with the more digital inclusion and fraud resilience position [22, 23].

The findings of this study strongly align with the dual perspectives of the Fraud Triangle Theory (FTT) and the Technology Acceptance Model (TAM). The positive association of mobile banking, ATMs, and POS with fraud underscores the "opportunity" element of FTT, as weak internal controls and rapid digital adoption create avenues for exploitation [4, 12]. Similarly, the mitigating role of Internet banking and USSD reflects how stronger control mechanisms can reduce opportunities for fraudulent acts, thereby weakening one of the legs of the fraud triangle. At the same time, the evidence that digital adoption predicts fraud rather than the reverse demonstrates TAM's relevance: although technologies are perceived as valuable and easy to use, their adoption without parallel security reinforcement introduces vulnerabilities [3, 15-17]. Thus, while FTT explains the behavioural and systemic conditions that foster fraud, TAM contextualises how the acceptance of digital tools—shaped by perceived benefits and usability—can unintentionally increase fraud risks. Together, these theories emphasise that fraud mitigation requires both strengthening institutional controls and ensuring that fraud-prevention technologies are fully embraced and effectively deployed.

5. Conclusions

This study demonstrates that digitalisation has a dual effect on fraud practices in Nigerian banks. While mobile banking, ATMs, and POS channels are strongly associated with increased fraud risks, internet banking and USSD appear to mitigate losses, reflecting the importance of authentication and control mechanisms. Granger causality results confirm that digital adoption predominantly drives fraud, rather than the reverse, with POS transactions exhibiting a bidirectional, though asymmetric, relationship. Overall, these findings underscore that digital expansion, if not matched with robust oversight and technology-driven safeguards, can exacerbate systemic vulnerabilities in the banking sector.

To address these challenges, banks should strengthen fraud management systems with advanced analytics, biometric authentication, and real-time monitoring tailored to high-risk channels such as mobile banking, ATMs, and POS. Regulatory authorities, notably the Central Bank of Nigeria, must enforce stricter compliance with cybersecurity standards and promote sector-wide collaboration on sharing fraud intelligence. Investing in forensic accounting, machine learning–based detection tools, and continuous employee training is essential for enhancing resilience. Furthermore, customer education campaigns are crucial for reducing exposure to phishing, SIM swapping, and other types of fraud. A channel-specific security strategy, supported by policy consistency and organisational culture, will enable Nigerian banks to reap the benefits of digitalisation while minimising fraud risks.

References

[1] H. Al-Dmour, F. Asfour, R. Al-Dmour, and A. Al-Dmour, "Validation of the impact of marketing knowledge management on business performance via digital financial innovation as a mediating factor," *VINE Journal of Information and Knowledge Management Systems*, vol. 52, no. 1, pp. 33-56, 2022. https://doi.org/10.1108/VJIKMS-05-2020-0085

[2] A. Chhaidar, M. Abdelhedi, and I. Abdelkafi, "The effect of financial technology investment level on European banks' profitability," *Journal of the Knowledge Economy*, vol. 14, pp. 2959-2981, 2023. https://doi.org/10.1007/s13132-022-00992-1

[3] S. Winasis, U. Wildan, and A. H. Sutawidjaya, "Impact of digital transformation on employee engagement influenced by work stress on Indonesian private banking sector," in *Proceedings of the 5th NA International Conference on Industrial Engineering and Operations Management*, 2020.

[4] R. A. Nnachi *et al.*, "Effect of bank verification number on fraud management of selected commercial banks in Ebonyi state, Nigeria," *International Journal of Engineering Research and Technology*, vol. 13, no. 6, pp. 1165-1172, 2020.

[5] V. Singh, S.-S. Chen, M. Singhania, B. Nanavati, and A. Gupta, "How are reinforcement learning and deep learning algorithms used for big data based decision making in financial industries–A review and research agenda," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100094, 2022. https://doi.org/10.1016/j.jjimei.2022.100094

[6] R. Zaib and O. Ourabah, "Large scale data using K-Means," *Mesopotamian Journal of Big Data*, vol. 2023, pp. 36-45, 2023. https://doi.org/10.58496/MJBD/2023/006

[7] M. K. Pandey, M. Mittal, and K. Subbiah, "Optimal balancing & efficient feature ranking approach to minimize credit risk," *International Journal of Information Management Data Insights*, vol. 1, no. 2, p. 100037, 2021. https://doi.org/10.1016/j.jjimei.2021.100037

[8] P. G. Pio *et al.*, "Complaint management: Comparison between traditional and digital banks and the benefits of using management systems for improvement," *International Journal of Productivity and Performance Management*, vol. 73, no. 4, pp. 1050-1070, 2024. https://doi.org/10.1108/IJPPM-08-2022-0430

[9] L. A. Bueno, T. F. Sigahi, I. S. Rampasso, W. Leal Filho, and R. Anholon, "Impacts of digitization on operational efficiency in the banking sector: Thematic analysis and research agenda proposal," *International Journal of Information Management Data Insights*, vol. 4, no. 1, p. 100230, 2024. https://doi.org/10.1016/j.jjimei.2024.100230

[10] N. C. Roy and S. Prabhakaran, "Insider employee-led cyber fraud (IECF) in Indian banks: From identification to sustainable mitigation planning," *Behaviour & Information Technology*, vol. 43, no. 5, pp. 876-906, 2024. https://doi.org/10.1080/0144929X.2023.2191748

[11] D. R. Cressey, *Other people's money: A study of the social psychology of embezzlement*. Glencoe, IL: Free Press, 1953.

[12] O. E. Akinbowale, P. Mashigo, and M. F. Zerihun, "The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry," *Cogent Business & Management*, vol. 10, no. 1, p. 2163560, 2023. https://doi.org/10.1080/23311975.2022.2163560

[13] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation," *Cogent Economics & Finance*, vol. 11, no. 1, p. 2153412, 2023. https://doi.org/10.1080/23322039.2022.2153412

[14] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, vol. 13, no. 3, pp. 319-340, 1989. https://doi.org/10.2307/249008

[15] N. Nguyen *et al.*, "A proposed model for card fraud detection based on Catboost and deep neural network," *IEEE Access*, vol. 10, pp. 96852-96861, 2022. https://doi.org/10.1109/ACCESS.2022.3205416

[16] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," *IEEE Access*, vol. 10, pp. 16400-16407, 2022. https://doi.org/10.1109/ACCESS.2022.3148298

[17] M. Fundira, E. I. Edoun, A. Pradhan, and C. Mbohwa, "Assessing digital competencies and AI ethics awareness among customers in the banking sector," *African Journal of Science, Technology, Innovation and Development*, vol. 16, no. 6, pp. 792-807, 2024.

[18] O. O. Odukoya and R. S. Samsudin, "Knowledge capability and fraud risk assessment in Nigeria deposit money banks: The mediating effect of problem representation," *Cogent Business & Management*, vol. 8, no. 1, p. 1899450, 2021. https://doi.org/10.1080/23311975.2021.1899450

[19] S. Nyakarimi, "Probable earning manipulation and fraud in banking sector. Empirical study from East Africa," *Cogent Economics & Finance*, vol. 10, no. 1, p. 2083477, 2022. https://doi.org/10.1080/23322039.2022.2083477

[20] S. M. M. Rahman, K.-J. Yii, E. K. Masli, and M. L. Voon, "The blockchain in the banking industry: A systematic review and bibliometric analysis," *Cogent Business & Management*, vol. 11, no. 1, p. 2407681, 2024. https://doi.org/10.1080/23311975.2024.2407681

[21] S. K. Sia, P. Weill, and N. Zhang, "Designing a future-ready enterprise: The digital transformation of DBS bank," *California Management Review*, vol. 63, no. 3, pp. 35-57, 2021. https://doi.org/10.1177/0008125621992583

[22] M. Al-Emran and C. Griffy-Brown, "The role of technology adoption in sustainable development: Overview, opportunities, challenges, and future research agendas," *Technology in Society,* vol. 73, p. 102240, 2023. https://doi.org/10.1016/j.techsoc.2023.102240

[23] H. Sharma and A. Díaz Andrade, "Digital financial services and human development: Current landscape and research prospects," *Information Technology for Development,* vol. 29, no. 4, pp. 582-606, 2023. https://doi.org/10.1080/02681102.2023.2199189

[24] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," *Journal of Big Data,* vol. 9, p. 24, 2022. https://doi.org/10.1186/s40537-022-00573-8

[25] B. Kasasbeh, B. Aldabaybah, and H. Ahmad, "Multilayer perceptron artificial neural networks-based model for credit card fraud detection," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 26, no. 1, pp. 362-373, 2022.

[26] J. Chaquet-Ulldemolins, F.-J. Gimeno-Blanes, S. Moral-Rubio, S. Muñoz-Romero, and J.-L. Rojo-Álvarez, "On the black-box challenge for fraud detection using machine learning (I): Linear models and informative feature selection," *Applied Sciences,* vol. 12, no. 7, p. 3328, 2022. https://doi.org/10.3390/app12073328

[27] D. Ratmono and Frendy, "Examining the fraud diamond theory through ethical culture variables: A study of regional development banks in Indonesia," *Cogent Business & Management,* vol. 9, no. 1, p. 2117161, 2022. https://doi.org/10.1080/23311975.2022.2117161

[28] A. Muduli and A. Choudhury, "Digital technology adoption, workforce agility and digital technology outcomes in the context of the banking industry of India," *Journal of Science and Technology Policy Management,* 2024. https://doi.org/10.1108/JSTPM-01-2024-0018

[29] K. Lee and J. Yeo, "Information and communication technology adoption, administrative discretion, and innovative mindsets in public organizations," *Public Personnel Management,* vol. 54, no. 1, pp. 72-98, 2025. https://doi.org/10.1177/00910260241276200

[30] A. David *et al.*, "Understanding local government digital technology adoption strategies: A PRISMA review," *Sustainability,* vol. 15, no. 12, p. 9645, 2023. https://doi.org/10.3390/su15129645

[31] R. Gholami, N. Singh, P. Agrawal, K. Espinosa, and D. Bamufleh, "Information technology/systems adoption in the public sector: Evidence from the Illinois Department of Transportation," *Journal of Global Information Management,* vol. 29, no. 4, p. 23, 2021. https://doi.org/10.4018/JGIM.20210701.oa8

[32] J. D. Twizeyimana, H. Larsson, and Å. Grönlund, "E-government in Rwanda: Implementation, challenges and reflections," *Electronic Journal of E-government,* vol. 16, no. 1, pp. pp19-31-pp19-31, 2018.

[33] A. M. Samsor, "Challenges and prospects of e-government implementation in Afghanistan," *International Trade, Politics and Development,* vol. 5, no. 1, pp. 51-70, 2021. https://doi.org/10.1108/ITPD-01-2020-0001

[34] M. B. Rehouma and S. Hofmann, "Government employees' adoption of information technology: A literature review," in *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 2018.

[35] F. R. Batubara, J. Ubacht, and M. Janssen, "Challenges of blockchain technology adoption for e-government: A systematic literature review," in *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 2018.

[36] H. Blichfeldt and R. Faullant, "Performance effects of digital technology adoption and product & service innovation–A process-industry perspective," *Technovation,* vol. 105, p. 102275, 2021. https://doi.org/10.1016/j.technovation.2021.102275

[37] S. Li, L. Gao, C. Han, B. Gupta, W. Alhalabi, and S. Almakdi, "Exploring the effect of digital transformation on Firms' innovation performance," *Journal of Innovation & Knowledge,* vol. 8, no. 1, p. 100317, 2023. https://doi.org/10.1016/j.jik.2023.100317

[38] Q. Huang, C. Xu, X. Xue, and H. Zhu, "Can digital innovation improve firm performance: Evidence from digital patents of Chinese listed firms," *International Review of Financial Analysis,* vol. 89, p. 102810, 2023. https://doi.org/10.1016/j.irfa.2023.102810

[39] M. Arellano and S. Bond, "Some tests of specification for panel data: Monte Carlo evidence and an application to employment equations," *The Review of Economic Studies,* vol. 58, no. 2, pp. 277-297, 1991. https://doi.org/10.2307/2297968

[40] M. Arellano and O. Bover, "Another look at the instrumental variable estimation of error-components models," *Journal of Econometrics*, Vol. 68, no. 1, pp. 29-51, 1995. https://doi.org/10.1016/0304-4076(94)01642-D

[41] R. Blundell and S. Bond, "Initial conditions and moment restrictions in dynamic panel data models," *Journal of Econometrics,* vol. 87, no. 1, pp. 115-143, 1998. https://doi.org/10.1016/S0304-4076(98)00009-8

[42] B. Shepherd, *The gravity model of international trade: A user guide*. New York, USA: United Nations ESCAP, 2013.

[43] E.-I. Dumitrescu and C. Hurlin, "Testing for Granger non-causality in heterogeneous panels," *Economic Modelling,* vol. 29, no. 4, pp. 1450-1460, 2012. https://doi.org/10.1016/j.econmod.2012.02.014

[44] S. Bond, A. Hoeffler, and J. Temple, "GMM estimation of empirical growth models," CEPR Discussion Paper No. 3048, 2001.

[45] C. G. Bowsher, "On testing overidentifying restrictions in dynamic panel data models," *Economics Letters,* vol. 77, no. 2, pp. 211-220, 2002. https://doi.org/10.1016/S0165-1765(02)00130-1