KASU Journal of Accounting Research and Practice (KAJARAP)

Volume 10, Number 2, December, 2025 ISSN: 2360-8889
https://journals.kasu.edu.ng/index.php/accounting

FORENSIC ACCOUNTING TECHNIQUES AND ELECTRONIC TRANSACTIONS FRAUD DETECTION OF LISTED SYSTEMATICALLY IMPORTANT BANKS IN NIGERIA

Oseh Anthony[1], Dr. Haruna Dadda'u[2], Dr. Saifullahi Abdullahi Mazadu[3]

[1,2,3,] Kaduna State University, Kaduna, Kaduna State, Nigeria,

Corresponding Author(s)' email/mobile:osehtony6@gmail.com/08036767599[1],
harunadaddau@kasu.edu.ng/08037006042[2],
hunan4dad@gmail.com/08033581343[3]

Abstract

This study explores forensic accounting techniques and electronic transactions fraud detection of listed systematically important banks (SIBs) in Nigeria. The study constructs are digital forensic technique, data mining, blockchain technology and fraud triangle as the exogenous constructs with electronic transactions fraud detection as the endogenous construct. The theories that underpinned the study are the fraud triangle theory, general strain theory, diffusion of innovation theory and big data analytics theory. The study employed a primary source of data collection through the use of a well-structured questionnaire. The population of the study is all 14 listed deposit money in Nigeria with the Nigeria Exchange Group (NGX). The study administered structured questionnaires to obtain data while both SPSS v25 and SmartPLS 4.0 (PLS-SEM) were utilised for the analysis of the data of the study. SPSS was used for preliminary analyses, while SmartPLS was used for the main data analysis. The study findings indicate that digital forensic technique has a positive and significant relationship with electronic transactions fraud detection in SIBS in Nigeria; while data mining, blockchain technology and fraud triangle have positive but no relationships with SIBs electronic transactions fraud detection drive. From the findings, the study recommends that institutionalising digital forensic units in all systematically important banks will yield good outcomes in the banking revolution; also, investing in data mining infrastructure and promoting analytical culture among internal auditors, adopting blockchain technology for real-time transaction monitoring and audit transparency, and more training would be required for the banks' staff in the area of forensic.

Keywords: forensic accounting, electronic transactions, fraud, systematically important banks, Nigeria

1. Introduction

Electronic transactions have become the backbone of modern banking operations, offering unprecedented efficiency, convenience, and speed in the delivery of financial services. As digitalisation expands, financial institutions increasingly rely on internet banking, mobile payments, point-of-sale systems, and blockchain-enabled transfers to

support customer transactions and enhance financial inclusion (Laudon & Traver, 2021; Demirgüç-Kunt et al., 2018). However, this rapid shift toward digital platforms has also intensified vulnerabilities to electronic transaction fraud, manifesting in identity theft, unauthorised transfers, data breaches, and social engineering attacks (Ngai et al., 2011; ACFE, 2020).

Globally, banks lose billions annually to electronic fraud, and the threat is especially severe in developing economies where detection systems are less sophisticated (Demirgüç-Kunt et al., 2018). In Nigeria, the proliferation of digital channels has magnified fraud risk, making electronic fraud detection a critical concern for regulators, financial institutions, and banking customers. A growing body of empirical research has examined fraud in digital financial environments, highlighting the importance of forensic accounting techniques, such as digital forensics, data mining, and blockchain analysis, for detecting irregularities in electronic transactions (Adejumo & Ogburie, 2025; Ali et al., 2024).

Earlier studies, however, often focus on general banking fraud, traditional audit mechanisms, or isolated techniques rather than integrated forensic approaches applicable to systematically important banks (SIBs). Prior works also emphasise challenges such as weak internal controls, inadequate fraud detection infrastructure, increasing cyber sophistication, and insider collusion as key drivers of electronic fraud (Nwobia et al., 2021; Olaleye & Fashina, 2019; Ibrahim & Musa, 2022). Despite these insights, research often provides empirical evidence on how combinations of forensic accounting techniques can strengthen electronic fraud detection in high-risk, high-volume financial institutions like Nigeria's SIBs, which handle the majority of digital transactions nationwide (Proshare, 2025).

The Nigerian banking sector is currently experiencing an unprecedented surge in fraud incidents, with reported financial losses arising from ₦9.4 billion in 2023 to over ₦53.4 billion in the first nine months of 2024 (FITC, 2024; NIBSS, 2024). Fraud cases involving web channels, mobile transactions, POS terminals, and internal system manipulation continue to escalate (Jaiyeola, 2023; Ijeseun, 2023).

Incidents of insider collaboration, cyberattacks on system infrastructure, and large-scale breaches such as the ₦40 billion First Bank fraud and the ₦9.3 billion Union Bank electronic system compromise underscore the systemic vulnerability of Nigerian banks (Augie, 2024; Olajide, 2025). Yet existing research remains fragmented, with limited methodological rigor, inadequate sector-specific focus on SIBs, and a lack of integrated frameworks combining digital forensic tools, data mining, blockchain analysis, and behavioural fraud models such as the fraud triangle. This gap necessitates a comprehensive, empirically grounded study capable of assessing the effectiveness of forensic accounting techniques in combating electronic fraud in Nigeria's most critical banks.

This study seeks to fill these gaps by empirically examining the impact of four key forensic accounting techniques: digital forensic technique, data mining, blockchain, and fraud triangle on electronic transaction fraud detection in Nigeria's listed systematically important banks. Using a quantitative research design, data were collected from officers within the SIBs and analysed using SPSS and Partial Least Squares Structural Equation

Modeling (PLS-SEM), enabling robust assessment of construct reliability, validity, and predictive relationships.

By integrating technological, behavioural, and analytical forensic approaches, this research provides one of the most comprehensive investigations into electronic fraud detection in Nigerian SIBs. The findings would contribute to the literature by offering evidence-based insights into which forensic techniques significantly improve fraud detection, thereby guiding regulators, policymakers, and banking institutions in strengthening fraud-resistant digital banking ecosystems.

More so, the study seek to answer the question to what extent does digital forensic technique impact on the electronic transactions fraud detection of systematically important Banks in Nigeria, in what way does data mining impact on electronic transactions fraud detection of systematically important Banks in Nigeria, what is the extent to which blockchain impacts on electronic transactions fraud detection of systematically important Banks in Nigeria, and how does fraud triangle impact on electronic transactions fraud detection of systematically important Banks in Nigeria?

The main objective of this study is to investigate the impact of forensic accounting techniques on electronic transactions fraud detection of systematically important Banks in Nigeria, with specific objectives to examine the impact of digital forensic technique on electronic transactions fraud detection of systematically important Banks in Nigeria, to evaluate the impact of data mining on electronic transactions fraud detection of systematically important Banks in Nigeria, to determine the impact of blockchain technology on electronic transactions fraud detection of systematically important Banks in Nigeria, and to assess the impact of fraud triangle on electronic transactions fraud detection of systematically important Banks in Nigeria.

To achieve the objectives of this study, the hypotheses would be formulated in the null form. Therefore, a study on the application of forensic accounting techniques and electronic transactions fraud detection of systemically important banks in Nigeria is desirable to focus more on electronic fraud detection.

2. Literature Review

Conceptual Framework

The framework in figure 1 explains the relationship between forensic accounting techniques application and electronic transactions fraud detection of systematically important banks in Nigeria. The framework depicts the study conceptual framework of the relationship between Forensic accounting techniques and its representations, and Electronic Transactions Fraud Detection.

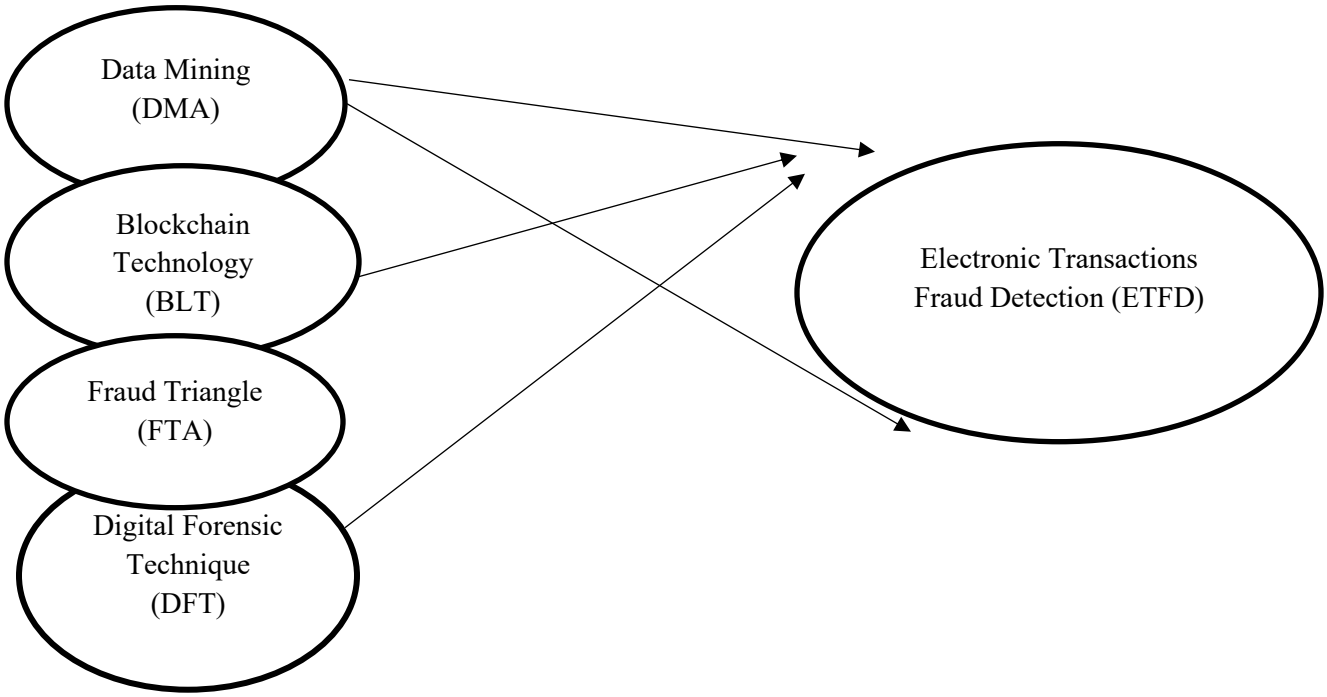


Figure 1: Conceptual Framework
Source: Author's idea, 2025.

Electronic Transactions Fraud Detection

Electronic transactions fraud refers to unauthorised, illegal, or deceptive activities committed through digital banking channels such as mobile transactions, internet banking, POS systems, ATMs, and web-based transfers (Ede, 2023; Ochieng & Kamaara, 2023; Manocha et al., 2024; Kasowaki & Faris, 2024). As digital adoption increases, fraudsters exploit system vulnerabilities, weak authentication protocols, and insider collusion to perpetrate fraudulent activities (Taherdoost, 2023; Radenkovic et al., 2023; Lin et al., 2023).

Effective detection requires analytical, technological, and forensic tools capable of identifying anomalies, tracking transaction trails, and preventing financial losses (Vivek et al., 2024). Nigerian banks, especially those with high transaction volumes such as Systemically Important Banks (SIBs), face increasing incidents of electronic fraud and rising financial losses.

Forensic Accounting Techniques

Forensic accounting techniques involve specialised investigative tools applied within digital financial environments. They combine accounting, auditing, criminology, and digital technology to uncover fraud patterns and reconstruct electronic financial trails (Tally, 2022). In electronic banking, core forensic techniques include digital forensics, data mining analytics, blockchain analysis, and behavioural fraud assessment, all of which support the identification of hidden irregularities, the analysis of large transaction datasets, and the validation of electronic records **(**Musa & Zahrah, 2024; Onamusi et al., 2024**)**

Digital Forensic Technique

Digital forensics is the process of collecting, preserving, analysing, and presenting electronic evidence extracted from devices, servers, networks, and transaction logs (Musa & Zahrah, 2024). In the banking sector, digital forensics helps identify system breaches, spoofed identities, unauthorised login attempts, malware intrusions, and manipulation of transaction databases. Techniques such as forensic imaging, log correlation, IP tracking, and traceability analysis allow financial institutions to reconstruct fraud incidents and pinpoint weaknesses in their digital infrastructure.

Data Mining

Data mining refers to computational methods that extract hidden patterns from large datasets using classification, clustering, anomaly detection, regression, and predictive modelling (Ngai et al., 2011; Kumar & Sriganga, 2014; Hassani et al., 2016). In fraud detection, data mining enables banks to identify outlier transactions, suspicious behavioural trends, abnormal transfer sequences, and inconsistent digital footprints. As a high-volume analytical tool, data mining automates pattern recognition and strengthens real-time fraud detection in electronic banking.

Blockchain Technology

Blockchain technology is a decentralized digital ledger that records transactions in an immutable and transparent manner (Nakamoto, 2008). In fraud detection, blockchain enhances traceability, cryptographic security, and tamper-resistant audit trails. Banks employing blockchain-based analytis can monitor transaction authenticity, detect double spending, trace digital signatures, and ensure integrity of digital records. Its immutable structure makes blockchain a powerful instrument for forensic auditing and electronic transaction verification.

Empirical Review

Digital Forensic Technique and Electronic Transactions Fraud Detection

Oluyide (2025) study was on the impact of Forensic Accounting Techniques in Mitigating Electronic Fraud in Nigeria's Deposit Money Banks. A quantitative approach through an online survey was employed with a positivist paradigm for the study. A stratified random sampling method was employed to select a sample of 95 respondents, representing eight 'best-fit' groups, including staff from operations, Information Technology, and Electronic Channel departments of five participating Deposit Money Banks, as well as accountants, auditors, representatives from bank regulators, professional accounting bodies, and law enforcement agencies in Nigeria. The result showed that digital forensics was not statistically significant in mitigating electronic fraud. It is suggested that if the scope of data analytics were expanded, it could help mitigate e-fraud, as it shows significance at a 10% level. The study reveals a need to employ specialists known as forensic accountants in the daily operational activities of banks. These professionals could collaborate with the bank's information technology department to implement precautionary measures to reduce e-fraud in deposit money banks. In the body of the study, there were 148 respondents from bank staff, as stated in the abstract, which noted 95 respondents.

In contrast, a study conducted by Mabior and Wanyama (2024) on the role of forensic investigations in reducing financial fraud among commercial banks in South Sudan. The study used a primary data collection approach, including questionnaires, interviews, and focus groups. The study employed the mixed-method approach and explanatory research design. The population was 119 respondents, and from 9 commercial

banks in South Sudan, a census sampling technique was employed for the 119 staff of the banks for the study. The collected data were analysed using both descriptive and regression analyses. Both the fraud triangle and agency theories were used to underpin the study. The study's findings reveal a strong positive and significant relationship between forensic accounting techniques and fraud reduction, which was harnessed with the use of digital technologies. The study also recommended the implementation of forensic techniques in banks to curb fraud cases. However, the study does not cover many forensic accounting technique variables, and hence, the findings cannot be applicable in Nigeria.

Similarly, Ogunwole and Jimoh (2024) investigated Forensic Accounting Services as a tool for Fraud Mitigation in Selected Kwara State-owned Tertiary Institutions in Nigeria. The study adopted a survey research design. The population for the study comprised principal officers, bursary, and account/audit staff of the six selected tertiary institutions in Kwara State. Stratified Random Sampling was used, comprising 157 staff of the selected institutions. Data were collected using a structured questionnaire. The data collected were analysed using Partial Least Squares and Structural Equation Model (PLS-SEM). With a path coefficient of 0.592and 0747 respectively, findings revealed that investigation service and digital forensic service of forensic accountants have a statistically significant negative impact on fraud. It was concluded that forensic accounting services have a significant impact on fraud in tertiary institutions in Kwara State. The study recommended, amongst others, that tertiary institutions should adopt a comprehensive anti-fraud strategy that combines fraud prevention, detection and prompt response measures. It was also recommended that tertiary institutions should engage the services of forensic accountants at the early stage of a suspected fraud case.

Data Mining and Electronic Transactions Fraud Detection

Uduehe et al. (2024) study was on Forensic Accounting Techniques and Fraud Management of Commercial Banks in Awka-South, Anambra State. The study used data mining as a proxy for the independent variable to explain fraud detection. The primary source of data collection was used. The descriptive survey research design was employed for the study, a structured questionnaire was used to obtain the responses of the targeted respondents, with a population of 758 staff from 13 (thirteen) commercial banks in Awka, while a sample size of 262 was selected for the study. The descriptive as well as frequency analysis, with a regression analysis. In their study, they used the fraud triangle as a theory. The findings of the study show that there is a significant positive relationship between data mining and fraud management. However, the study was conducted using only the banks within Awka, which may not give a better picture than having more branches outside Anambra state to have a generalised view.

Similarly, Thomas (2024) investigated the Applications of Data Mining Techniques in Detecting Occupational Fraud: A Qualitative Review of Forensic Accounting Practices. The study employed the use of a qualitative research design. The fraud triangle theory was used to underpin the study. The study utilised interpretivism philosophy and an inductive approach in conducting the investigation. The primary method of gathering data was through the use of semi-structured interviews. The study population consisted of 10 participants, selected through a purposive method for the investigation, with the researcher employing thematic analysis to analyse the data collected for the study. The study's

findings reveal that most respondents agreed that data mining analysis can detect and prevent fraud. The study population, however, is not adequate to provide a comprehensive outcome for a study of this nature. A validity test was not conducted on the data to ascertain whether there is bias or not in the data.

In line with similarly study, Ewa (2022) study was on forensic accounting techniques and fraud management in public sector Ministries, Departments and Agencies in Nigeria. The study employed a survey research design and multiple regression analysis technique (OLS). The study uses fraud diamond and fraud triangle theories to underpin it. A primary data collection method was used through the extraction from questionnaires distributed to the population. The population is drawn from among professionals working in the south-south geopolitical zone of the Nigerian public service; there are 350. Purposive sampling was adopted to ensure that only knowledgeable respondents were recruited in the study. The findings of the study suggest that Data mining, ratio analysis and trend analysis techniques have a strong positive relationship and significant impact on fraud detection in fraud management. The domain may not be adequate, hence the decision to use systematically important banks.

Also, Oyedokun (2022) carried out a study on the determinants of forensic accounting techniques and theories: An Empirical Investigation. The data analysed in this study were gathered from both primary and secondary sources. Data were collected with the use of electronically using an online questionnaire through Google Form, while the secondary data were from existing information. The study used the fraud triangle to underpin the study. A population of 120 respondents, purposively selected. The findings of the study show that data mining emerged as the most appropriate technique for fraud investigation; however, the combination of two or more techniques is advised for forensic accountants, forensic legal practitioners, and all other similar parties.

Blockchain Technology and Electronic Transactions Fraud Detection

In Indonesia, Ananda and Yanti (2024) did a study on the impact of knowledge of blockchain towards fraud detection skills throught readiness technology as an intervening variable. The study supports the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT). The research employs a quantitative approach, gathering data from an auditor. From the population of auditors, the research sample was selected through purposive sampling. The criteria for the sample include internal and external auditors with experience in using technology as a tool for fraud detection. Data were collected by distributing a questionnaire link through email to 97 respondents. Upon data collection, validity and reliability tests were conducted, followed by processing using descriptive statistical methods, including R-Square analysis, path coefficient testing, specific indirect effects testing, and F-Square table analysis. The findings indicate a positive relationship between knowledge of Blockchain and fraud detection capabilities.

Ali et al. (2024) carried out a study on forensic accounting and fraud detection emerging trends and techniques. This study explores how artificial intelligence (AI), blockchain technology and data analytics can improve forensic accounting techniques. A variety of techniques, including regression analysis, Beneish M-Score, and Benford's Law, were used in a comprehensive methodology to assess the effectiveness of forensic accounting on 100 companies, which was the study population. The study sample was 50 companies which employed blockchain technology to examine it effect on detecting fraud.

The results of the regression analysis show that both data analytics (β=0.35) and AI (β=0.30) have a substantial positive impact on improving fraud detection effectiveness. Also, from the analysis, the utilisation of advanced technologies like AI, blockchain technology, and data analytics significantly enhances the efficiency of forensic accounting in detecting and preventing fraud. The study recommended that a significant amount of funds must be invested in infrastructure and training to achieve successful implementation.

In India, Singh et al. (2023) investigated the effectiveness of blockchain applications in fraud detection using a systematic literature review approach. The study applied the secondary method of data collection from various literature. The study covered the period from 2015-2022 as it covered financial domains in India. The findings of the research explored different types of business domains using blockchains in detecting fraud. They examined their effectiveness in other sectors such as insurance, banks, online transactions, real estate, and credit card usage. Again, the findings indicated that real-life applications of blockchain technology to secure the gateway for online transactions; people from diverse backgrounds with different business objectives can strongly rely on blockchains to prevent fraud. The study was not elaborate enough, as no theory or specific population was used in their work.

Fraud Triangle and Electronic Transactions Fraud Detection

Rahman and Jie (2024) study was on Fraud detection using fraud triangle theory: evidence from China. Data sets were collected from 16,063 listed companies in the Shanghai and Shenzhen market, from 2010 to 2020. The quantitative research design method was used, with analysis conducted using regression to handle five (5) variables for the study. The research finding indicates that the fraud triangle positively affects fraud detection. With the robustness of the study, it fails to mention the theories used for the study.

Djatnicka et al. (2023) The study utilized the Fraud Triangle perspective to detect financial statement fraud in property and real estate companies using the Beneish M-Score model. It was conducted on listed property and real estate firms on the Indonesia Stock Exchange. The analysis employed logistic regression, where financial statement fraud was the dependent variable, represented by the M-Score. The independent variables included financial stability, proxied by changes in assets; external pressure, measured by the leverage ratio; and financial targets, represented by return on assets. The findings revealed that financial stability and financial targets had a positive impact on fraudulent financial statements, while external pressure did not significantly influence financial fraud. The study also indicated that lower leverage reduces the likelihood of a firm violating credit agreements, thereby decreasing the probability of fraudulent financial reporting. The study did not mention population and theory in their study.

Renata and Marlinah (2022) the study investigated the influence of the Fraud Triangle Theory in detecting fraudulent financial statements among manufacturing companies listed on the Indonesia Stock Exchange (IDX) from 2019 to 2021. The research employed logistic regression analysis to test the data. The dependent variable, financial statement fraud, was measured using the Beneish M-Score Model. The independent variables were based on fraud triangle components and additional corporate governance factors, including: Financial stability, proxied by asset change, Personal financial needs,

proxied by managerial ownership, External pressure, measured by leverage ratio, Financial target, represented by return on assets, Nature of the industry, measured by the ratio of accounts receivable, Ineffective monitoring, proxied by the proportion of independent commissioners, Quality of external auditors, represented by affiliation with a Big Four auditing firm (BIG-4), Auditor changes, Auditor opinion. The findings revealed that financial stability, personal financial needs, the nature of the industry, and the quality of external auditors significantly influenced financial statement fraud. However, external pressure, financial targets, ineffective monitoring, auditor changes, and auditor opinions did not have a significant impact on fraudulent financial reporting.

Theoretical Review

This study is anchored on: fraud triangle, general strain theory, diffusion of innovation and big data analytics. The Fraud Triangle Theory (Cressey, 1953) proposes that fraud occurs when three conditions, pressure, opportunity, and rationalisation, converge (Wells, 2005). Weak internal controls, personal pressures, and moral justification all contribute to fraudulent acts in financial institutions. Despite criticisms that the model oversimplifies fraud and pays insufficient attention to systemic and cultural factors, it remains a foundational framework for understanding fraud dynamics in forensic accounting. The theory supports the fraud-triangle construct of this study by explaining behavioural drivers of electronic transaction fraud.

Agnew (1992) argues that strain or stress increases the likelihood of deviant behaviour as individuals seek maladaptive coping mechanisms. In banking, financial pressures, job-related frustration, or unmet performance expectations may push employees toward fraudulent activities. GST provides behavioural insight into why internal actors may engage in electronic fraud, complementing the fraud triangle's focus on opportunity structures.

Rogers' (2003) Diffusion of Innovation Theory explains how technological innovations are adopted within organizations. Constructs such as relative advantage, compatibility, and complexity determine the adoption of forensic tools such as digital forensics and blockchain. The theory underpins the study's assumption that banks' willingness to adopt innovative forensic technologies influences fraud detection outcomes.

Big Data Analytics Theory (Diebold, 2012; Laney, 2001) emphasises the importance of analysing large, diverse, and real-time datasets to generate insights (Laney, 2001; Manyika et al., 2011). As electronic transactions generate high-volume, high-velocity, and high-variety data, BDAT explains how data mining and analytics support fraud detection. The theory justifies the inclusion of data mining as a key construct in the study model.

3. Methodology

This study employed a descriptive survey research design to obtain firsthand reports and perceptions on forensic accounting techniques and electronic transaction fraud detection in Nigeria's systematically important banks (SIBs). The research philosophy is stated as interpretivism, reflecting emphasis on respondents' subjective experiences and insights regarding the adoption and effectiveness of forensic techniques.

The study population began with all 14 deposit money banks listed on the Nigeria Exchange Group (NGX) as of 31 December 2024, but the population was adjusted to focus on the subset of systematically important banks (SIBs). The six SIBs used as the study

domain are: First HoldCo Plc, UBA Plc, Guaranty Trust Holding Company Plc (GTCO), Access Holdings Plc, Zenith Bank Plc and Ecobank Transnational Incorporated (ETI). The adjustment was justified because these Tier-1 banks dominate transaction volumes and are reported to account for the majority of electronic transaction activity and related fraud exposure, making them a relevant benchmark for the study.

Data were collected from bank officers with experience or knowledge of fraud detection and controls (compliance officers, internal control officers, risk analysts, accountants, and heads of operations). The questionnaires were distributed across 20 branches × 10 officers per bank for the six SIBs to ensure coverage of branch-level operations and functional lines involved in fraud controls. The instrument targeted staff who are knowledgeable about the application of forensic techniques in their institutions.

The study used primary data collected via a structured, closed-ended questionnaire. The questionnaire comprised six parts: Part A (respondent demographics); Part B (Electronic Transactions Fraud Detection dependent construct); Part C (Digital Forensic Techniques); Part D (Data Mining); Part E (Blockchain Technology); and Part F (Fraud Triangle). All construct items were measured on a five-point Likert scale (1 = strongly disagree to 5 = strongly agree). The scale and item format were adapted from existing validated instruments and relevant literatures.

The structural equation model was adopted for this study as outlined below, consists of four independent constructs [digital forensic technique (DFT), data mining (DMA), blockchain technology (BLT) and fraud triangle (FTA)] and the dependent construct (electronic transactions fraud detection- ETFD), all of which were integrated. The model specifies this:

$y=\Lambda y\eta + \varepsilon$ ……..(i)

(Where Λy is the factor loading matrix and ε measurement errors)

Structural model:

$ETFD=\beta 1DFT +\beta 2DMA + \beta 3BLT + \beta 3BLT + \zeta$ ……(ii)

$\beta 1, \beta 2, \beta 3, \beta 4>0$ (higher forensic capability increases ETFD). ζ is a structural disturbance. Where: ETFD = Electronic transactions fraud detection; $\beta 0$ = Constant; β_1 to β_4 = Coefficients of independent variables 1 and 4; DFT = Digital Forensic Technique; DMA= Data Mining; BLA= Blockchain Technology; FTA= Fraud Triangle.

A pilot test was conducted before the main data collection to ensure instrument clarity and internal consistency. Pilot data show item and construct statistics used to evaluate initial measurement properties. Reliability and validity testing procedures planned include Cronbach's alpha for internal consistency, and subsequent construct validity checks during PLS-SEM analysis (see next subsections). The paper reports pilot descriptive and distribution checks (kurtosis/skewness) and used the pilot to refine items before final administration as well as the reliability which all are within the threshold.

4. Results and Discussion

Respondents Demographic Bio-Data

Table 1

Respondents Demographic Information

Category		Frequency (N=182)	% (Total =100)
Gender			
	Male	106	58.24
	Female	76	41.76
		56	30.78
		48	26.37
		46	25.27
		32	17.58
		2	1.09
		85	46.70
		95	52.21
		27	14.84
		69	37.91
		13	7.14
		17	9.34
		56	30.77
		62	34.07
		54	29.67
		66	36.26

Source: Questionnaire extraction, 2025.

Data analysis procedure

A two-stage analytical approach was implemented: Preliminary analysis (SPSS v25): Data cleaning, non-response bias assessment, descriptive statistics, normality checks (kurtosis/skewness), and multicollinearity diagnostics. These steps ensure the dataset meets assumptions and helps detect problematic responses before modelling. The table below show a summary of preliminary analysis:

Table 2

Data Analytic Result

Constructs	Levene's test for equality of variance (Non-bias) –Sig.	Mean	Multicollinearity VIF	Tolerance Value	Cronbach's Alpha
ETFD	0.877	3.7121	-	-	
DFT	0.766	3.3714	1.275	0.785	
DMA	0.800	3.6747	1.757	0.576	
BLT	0.723	3.4703	1.505	0.664	
FTA	0.971	4.0659	1.296	0.772	
					0.775

Source: SPSSV25 Output (2025)

The above results show that the questionnaires returned behind acceptable time for retrieval were determined through the use of levene's test for equality of variance, where the six (6) questionnaires retrieved as late responses were seen to be insignificance and therefore fit to be part of data analyses.

The responses mean of respondents was determined with the use of a descriptive statistics, with results showing a moderate acceptance of questions by respondents. To confirm if independent constructs were correlated with each other, by way of multicollinerarity. The results show no multicollinerarity exist. The reliability test was also down, as the cronbach's Alpha outcome shows to be within the threshold of 0.7 to state that the data collection has internal consistency.

Results

The Measurement, Outer Model

Some scholar's likes as Anderson and Gerbing (1988) recommend that the convergent validity and reliability should be assessed before hypothesis testing. In the same vein, Hair, Ringle and Sarsted (2013) further suggested that discriminant validity needs to be examined in order to satisfy the average variance extracted (AVE). Therefore, AVE for each construct should be greater than the minimum benchmark of 0.5 (Fornell & Larcker, 1981; Hair et al., 2013).

Convergent Validity

This measures the extent to which multiple items that measure the same conceptions are in agreement. Hair et al. (2010) recommended the use of factor loadings, composite reliability and average variance extracted to appraise convergent validity. The loadings for each item should be above the threshold of 0.5 (Hair et al., 2013; 2007).

Composite reliability values (Table 2) represent the composite reliability values for the constructs which exceed the threshold of 0.7, and all values of AVEs are more than 0.5, hence it's in line with the outer measurement. All measurements show a sufficient degree of convergent validity, and all valid measures of their respective constructs are based on their parameter estimates and statistical significance (Chow & Chan, 2008).

The PLS algorithm was used in the study investigation to assess the reliability of individual items and other measurement model components. The outer factor loadings of each construct's individual items are used to calculate the measurement model's individual item reliability (Duarte & Raposo, 2010; Hair et al., 2012; Hulland, 1999).

The outer factor loadings of DFT2, BLT1, FTA1, ETFD1 and 3 are below the threshold of 0.40; therefore, they were removed to improve convergent reliability of the constructs. The outcome of the results is stated in Table 3.

Table 3

AVE and CR Before and After Deletion of DFT2, BLT1, FTA1, ETFD1 and ETFD3

Affected Constructs	AVE Before Removal	AVE After Removal	Improvement	CR Before Removal	CR After Removal	Improvement
DFT	0.405	0.489	0.084	0.754	0.747	-0.007
BLT	0.321	0.390	0.069	0.499	0.715	0.216
FTA	0.305	0.369	0.064	0.442	0.697	0.275
ETFD	0.257	0.423	0.166	0.463	0.669	0.206

Source: PLS-SEM 4.0, 2025

From Table 4 below, all indicators have loadings of 0.70 or higher; however, with Hair et al. (2007) claims, some above 0.40 were retained for the loadings.

Table 4

Adjusted Measurement Model (Reliability and Convergent Validity)

Construct	Item	Loadings	Cronbach's Alpha	AVE	CR
ETFD	ETFD 2	0.885	0.357	0.423	0.669
DFT	DFT 1	0.894	0.583	0.489	0.777
	DFT 3	0.858			
	DFT 4	0.481			
DMA	DMA 1	0.720	0.888	0.376	0.747
	DMA 2	0.659			
	DMA 3	0.636			
	DMA 4	0.448			
	DMA 5	0.568			
BLT	BLT 2	0.610	0.499	0.390	0.715
	BLT 3	0.738			
	BLT 4	0.636			
	BLT 5	0.490			
FTA	FTA 2	0.564	0.454	0.369	0.697
	FTA 3	0.657			
	FTA 4	0.704			
	FTA 5	0.481			

Source: PLS-SEM 4.0, 2025

The result of the study measurement model as show in Table 4, where the values of composite reliability (CR) and Cronbach's Alpha coefficient. It is recommended by Hair

et al. (2014) to use composite reliability to assess internal consistency reliability, because it considers certain indicators of outer factor loadings. This will evaluate the internal consistency with the use of composite reliability. According to Hair et al. (2014), a latent construct should have a composite reliability value (CR) of at least 0.70 to be considered reliable. From table 4.5, all the constructs are within the acceptable threshold except for FTA and ETFD, 0.697 and 0.669 even within range, are acceptable.

Although the composite reliability (CR) values for some constructs in this study (0.669 and 0.697) fall slightly below the recommended 0.70 threshold, they are considered acceptable based on the exploratory nature of the research. According to Bagozzi and Yi (1988), and Hair et al. (2019), CR values above 0.60 are deemed adequate in early-stage research or where constructs are contextually novel. Therefore, given the complexity and emerging nature of forensic accounting techniques in the Nigerian banking context, the CR values obtained still indicate satisfactory internal consistency and reliability.

Discriminant Validity

Discriminant Validity ascertains how distinct one construct is from another construct contained within the same model (Durate & Roposo, 2010; Hair et al., 2014). The square root of the extracted construct average variance must be higher than its correlation with any other constructs in the same model, Fornell-Lacker criterion claims so (Fornell & Lacker, 1981). The criterion utilised the square root of the AVE for a particular latent construct is bigger than its correlations with other latent constructs, and this particular latent construct shares more variance with its related items than with any other latent constructs in the model.

Table 5

Discriminant Validity (Fornell-Lacker Criterion)

	BLT	DMA	DFT	ETFD	FTA
BLT	**0.625**				
DMA	0.552	**0.613**			
DFT	0.425	0.508	**0.864**		
ETFD	0.444	0.512	0.699	**0.651**	
FTA	0.382	0.517	0.371	0.406	**0.608**

Source: PLS-SEM 4.0, 2025

The bolded diagonal values correspond to the square root of AVE of the constructs (n=182)

Furthermore, the discriminant validity of the study's constructs was established using the Heterotrait-Monotrait Ratio (HTMT). Values of the HTMT near 1 signify a lack of discriminant validity. HTMT values were below the threshold for most pairs but showed high values for some pairs (e.g., Data Mining--Fraud Triangle = 0.994; ETFD—Fraud Triangle = 0.961). The thesis notes that, given theoretical and operational overlap among forensic constructs, some HTMT elevation may reflect conceptual complementarity rather than measurement redundancy

Assessment of Structural Model

For the structural model, the bootstrap approaches for analysis were utilized. Bootstrap is a non-parametric procedure that can be used to test statistical significance

PLS-SEM results and a path coefficient, R^2, F^2 values. To confirm the relationship between the exogenous constructs and endogenous construct, Frazier et al. (2004**)** and Hair et al. (2014) suggest the use of bootstrap in analyzing the data.

Hypotheses Testing for Constructs Relationship

The model displays the findings of the study's direct relationship of constructs, which is represented by the four hypotheses stated in the introduction:

H_{01} Digital forensic technique has no significant impact on electronic transaction fraud detection of systematically important Banks in Nigeria.

H_{02} Data mining has no significant impact on electronic transactions fraud detection of systematically important Banks in Nigeria.

H_{03} Blockchain technology has no significant impact on electronic transactions fraud detection of systematically important Banks in Nigeria.

H_{04} Fraud triangle has no significant impact on electronic transactions fraud detection of systematically important Banks in Nigeria.

Structural Model of Latent Constructs of Direct Relationship

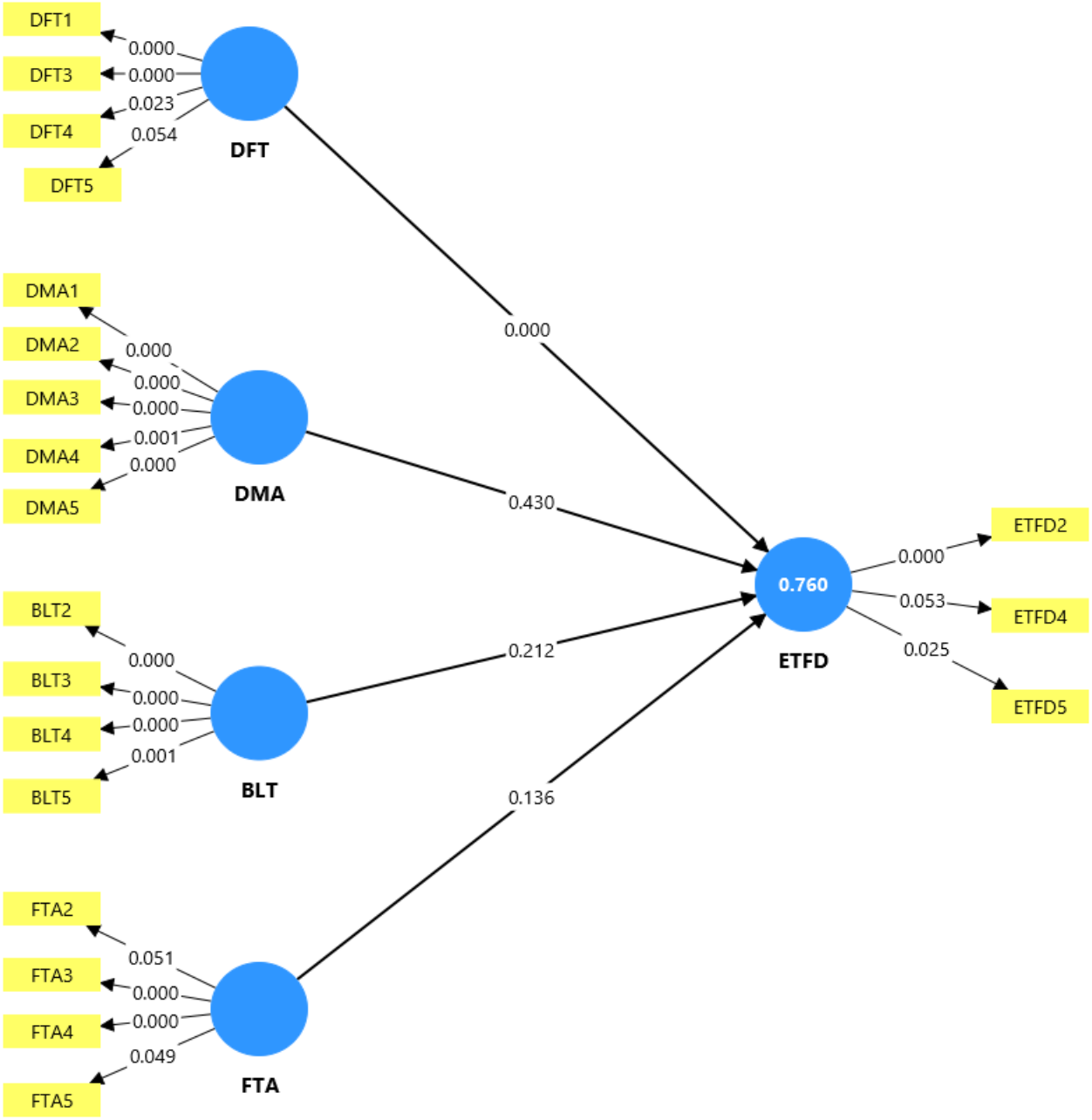


Figure 2: **Structural Model of Latent Constructs of Direct Relationship**

Table 6

Structural Model: Test of Significance for Direct Relationship

Hypotheses	Relationship	B	Std. Error	T	p	Decision
$H0_1$	DFT>ETFD	0.792	0.070	11.253	0.000*	Reject
$H0_2$	DMA>ETFD	0.042	0.053	0.789	0.430**	Fail to reject
$H0_3$	BLT>ETFD	0.058	0.047	1.249	0.212**	Fail to reject
$H0_4$	FTA>ETFD	0.069	0.046	1.490	0.136**	Fail to reject

Note: β= Beta coefficient, Std. error=Standard error, t=T-statistics, p=Probability value, *relationship significant, **relationship not significant

Source: PLS-SEM 4.0, 2025

The study demonstrates that digital forensic technique (DFT) has a strong and statistically significant effect on electronic transaction fraud detection (ETFD) among Nigeria's systematically important banks (SIBs). Results from Table 6 reveal a high positive coefficient (β = 0.792) and a t-value of 11.253, significant at the 1% level, indicating that a 1% increase in DFT leads to a 79.2% improvement in ETFD.

Consequently, the null hypothesis is rejected. The finding aligns with the Diffusion of Innovation theory, which explains how the adoption of new technological innovations enhances fraud detection capabilities by improving investigative efficiency and system responsiveness. This result is consistent with the findings of Mabior and Wanyama (2024), Ogunwole and Jimoh (2024), and Gerald (2022), but contradicts the report of Oludide (2025).

The hypothesis that data mining has no significant effect on electronic transaction fraud detection is supported by the study's results. Table 6 reports a positive but insignificant coefficient (β = 0.042), t-value of 0.789, and p-value of 0.430 at the 5% significance level, showing that while data mining may improve ETFD by 4.2% for every 1% increase, this effect is not statistically meaningful.

The finding is interpreted through Big Data Analytics theory, which highlights the role of data-driven insights in managing complex datasets but acknowledges challenges when tools are insufficiently developed or underexploited. Supporting literature suggests that limited research and application of data mining in management fraud detection weaken its predictive power (Calderon & Cheh, 2002; Koskivaara, 2004; Kirkos & Manolopoulos, 2004). The study's results contradict empirical evidence from Uduehe et al. (2024), Thomas (2024), Ndubuisi et al. (2017), and Ewa (2022).

The study also finds that blockchain technology does not significantly influence electronic transaction fraud detection in Nigeria's SIBs. Table 6 indicates a positive but insignificant coefficient (β = 0.058), t-value of 1.249, and p-value of 0.212, showing that although an increase in blockchain adoption may enhance ETFD by 5.8%, the effect is statistically insignificant at the 5% level.

While blockchain offers decentralisation, immutability, and traceable audit trails that theoretically support fraud detection, its practical application remains insufficiently developed within Nigerian banks. Interpreted through the Diffusion of Innovation theory,

the findings suggest that blockchain remains in an early adoption phase, limiting its measurable impact. This result contradicts prior studies by Celestin and Vanitha (2019); Singh et al. (2023); and Ali et al. (2024), which reported stronger relationships.

Findings further reveal that the fraud triangle has no significant impact on electronic transaction fraud detection in SIBs. Table 6 shows a positive coefficient (β = 0.069), t-value of 1.490, and p-value of 0.136 at the 5% level, indicating that although a 1% increase in fraud triangle elements (pressure, rationalisation, opportunity) corresponds to a 6.9% rise in ETFD, this effect is statistically insignificant.

The fraud triangle theory proposes that individuals commit fraud when faced with pressure, opportunity, and rationalization; however, these behavioural mechanisms alone appear inadequate for driving significant detection outcomes in technologically complex financial environments. The study's finding contradicts the conclusions of Rahman and Jie (2019); Renata and Marlinah (2022), and Hakimi and Rahmat (2019), though it aligns with the contrasting evidence provided by Amir et al. (2022).

Coefficient of Determination for Construct Relationships

The ability of a model to predict outcomes is measured by its coefficient of determination or R-square (R^2). According to Hair et al. (2010, 2014), the R-square of a research study indicates the combined effects of exogenous latent constructs on changes in the endogenous latent construct.

Hair et al. (2014), Hair et al. (2011), Reinartz et al. (2009) recommended a general rule of thumb as an acceptable R^2 value. In their research, the R2 values are 0.75, 0.50, and 0.25, respectively, for substantial, moderate, and weak, while Chin (1998) offered R2 values of 0.67, 0.33, and 0.19 to represent substantial, moderate, and weak, respectively, in PLS-SEM modeling.

Table 7

Coefficient of determination for Direct Relationship (R^2)

Construct	R-Square	P-value
Electronic Transactions Fraud Detection (ETFD)	0.760	0.000

Source: PLS-SEM 4.0, 2025

According to the result in Table 7, variations in the endogenous latent construct (Electronic Transactions Fraud Detection for systematically important banks in Nigeria) are explained by the exogenous latent constructs of this study. These include digital forensic technique, data mining, blockchain technology and fraud triangle to the extent that 76% of changes are explained by these constructs, with a p-value of 0.000 to specify that the model is good. This indicates a substantial relationship between the endogenous constructs and the exogenous constructs.

5. Conclusion and Recommendations

The study investigated the impact of forensic accounting techniques (digital forensic technique, data mining, blockchain technology, and fraud triangle) on electronic transaction fraud detection in systematically important banks (SIBs) in Nigeria. The empirical findings show that digital forensic technique significantly enhance fraud

detection capacity, affirming their effectiveness in identifying access breaches, reconstructing transaction trails, and resolving electronic fraud cases within large-scale banking systems.

This demonstrates that digital forensics is the most mature and impactful fraud detection mechanism currently adopted by Nigerian SIBs, aligning with prior assertions that advanced forensic tools contribute substantially to fraud mitigation in technologically dynamic environments. The results, therefore, underscore the need for institutional investment in digital forensic infrastructure to strengthen early-warning systems and improve investigative accuracy.

Conversely, data mining, blockchain technology, and fraud triangle constructs displayed positive but statistically insignificant effects on electronic transaction fraud detection. These findings suggest that although the tools possess inherent potential, they remain under-utilised, weakly institutionalised, or insufficiently integrated into the operational workflow of Nigerian SIBs. The insignificant outcomes reflect limited analytical culture, inadequate staff training, and suboptimal adoption of emerging technologies such as blockchain and predictive analytics within the Nigerian banking sector.

Overall, the study concludes that while forensic accounting innovations exist, their operational impact depends on greater organisational commitment, capacity building, and technological diffusion across SIBs.

To strengthen fraud detection systems in Nigeria's systematically important banks, the study recommends institutionalising digital forensic units across all deposit money banks, especially SIBs under CBN regulatory oversight. Establishing dedicated units will enhance the capacity for real-time monitoring, forensic imaging, and incident reconstruction, thereby improving fraud response efficiency.

The study emphasises that banks should invest heavily in digital forensic infrastructure, including forensic software, log-analysis systems, and specialised cybersecurity tools, to achieve deeper system digitalisation and mitigate electronic fraud risks effectively.

In addition, banks should strengthen the adoption of data-driven and technology-based fraud detection frameworks. This includes investing in data mining platforms, developing an internal analytics culture among auditors, and training staff in advanced fraud detection algorithms.

Similarly, the adoption of blockchain technology for real-time transaction validation, immutable audit trails, and enhanced transparency is strongly recommended. To address behavioural dimensions of fraud, banks should integrate fraud triangle principles into ethics training, compliance programs, and staff behaviour monitoring systems to reduce opportunities, pressures, and rationalisations that encourage fraudulent behaviour. Collectively, these measures will improve institutional resilience and ensure that forensic accounting techniques translate into stronger fraud detection outcomes in Nigerian SIBs

References

Adejumo, P., & Ogburie, C. (2025). Forensic accounting in financial fraud detection: Trends and challenges. *International Journal of Science and Research Archive, 14*(03), 1219-1232.

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47–87. https://doi.org/10.1111/j.1745-9125.1992.tb01093.x

Ali, A. M., Futaih, R. F., Shukur, M., & Al-Orfali, A. K. (2024). Forensic accounting and fraud detection: Emerging trends and techniques. *Journal of Ecohumanism, 3*(5), 525–542. https://doi.org/10.62754/joe.v3i5.3921

Ananda, R., & Yanti, H. B. (2024). Analysis impact knowledge of blockchain towards fraud detection skill throught readiness technology as intervening variable

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin*, *103*(3), 411.

Augie, B. (2023, December 19). UBA, GTCO, Zenith, most capitalised lenders in Nigeria. *MoneyCentral*. https://moneycentral.com.ng

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74–94. https://doi.org/10.1007/BF02723327

Chow, W. S., & Chan, L. S. (2008). Social network, social trust and shared goals in organizational knowledge sharing. *Information & management*, *45*(7), 458-465.

Cressey, D. R. (1953). *Other people's money: a study in the social psychology of embezzlement* Glencoe, IL: The Free Press

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). *The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution.* The World Bank

Diebold, F. X. (2012). *On the origin(s) and development of the term 'Big Data'*. PIER Working Paper No. 12-037. University of Pennsylvania. https://ssrn.com/abstract=2152421

Djatnicka, E. W., Purba, S. S., & Wulandari, D. (2023). Fraud Triangle Perspective: Detecting financial statement fraud using the Beneish M-Score model in property and real estate companies listed on the Indonesia Stock Exchange. *East Asian Journal of Multidisciplinary Research, 2*(7), 3113–3130. https://doi.org/10.34007/eajmr.v2i7.4894

Duarte, P. A. O., & Raposo, M. L. B. (2010). A PLS model to study brand preference: An application to the mobile market. In Handbook of Partial Least Squares. Springer.

Ede, T. E. (2023). E-business management practices and the performance of small-scale entrepreneurs (SSEs) in Ebonyi State. *EBSU Journal of Social Sciences and Humanities*, *13*(3).

Ewa, U. E. (2022). Forensic accounting and fraud management in Nigeria. *Journal of Accounting, Business and Finance Research*, *14*(1), 19-29.

Financial Institutions Training Centre (FITC). (2024). *Reports on Frauds and Forgeries in Nigerian Banks: Quarterly Report*. FITC Publications.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Frazier, P. A., Tix, A. P., & Barron, K. E. (2004). Testing moderator and mediator effects in counseling psychology research. *Journal of counseling psychology*, *51*(1), 115.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning

Hair, J. F., Money, A. H., Samuel, P., & Page, M. (2007). Research methods for business. John Wiley & sons Ltd.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2013). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139-152

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least square structural equation modeling in marketing research. *Journal of the Academy of Marketing science, 40*(3), 414-433

Hair, J.F. Hult, G. T. M, Ringle, C.M., & Sarstedt, M (2014). A primer on partial least squares structural equation modelling (PLS-SEM). Thousand Oaks CA: Sage Publications.

Hair, J.F., Black, J. W., Babin, B. J., & Anderson, E. R (2010). Multivariate data Analysis (Seventh). Pearson Education Limited.

Hassani, H., Huang, X., Silva, E. S., & Ghodsi, M. (2016). A review of data mining applications in crime. *Statistical Analysis and Data Mining: The ASA Data Science Journal*, *9*(3), 139-154.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic management journal*, *20*(2), 195-204.

Ijeseun D. (2023, August 21). Nigeria's banking sector loses ₦9.5 billion to electronic fraud.

Jaiyeola, T (2023, September 10). Punch Newspaper. 78,584 e-payment fraud cases recorded in one year. https://punchng.com/78584-e-payment-fruad-cases-recorded-in-one-year-report/

Kasowaki, L., & Faris, I. (2024). *Elevating transactions: the role of internet banking in revolutionizing e-commerce experiences*. EasyChair, Tech. Rep.

Kumar, V., & Sriganga, B. K. (2014). A review on data mining techniques to detect insider fraud in banks. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(12), 370-380.

Laney, D. (2001). *3D data management: Controlling data volume, velocity, and variety*. META Group Research Note

Laudon, K. C., & Traver, C. G. (2021). *E-Commerce 2021: Business, Technology, Society.* Pearson

Mabior, M. M., & Wanyama, K. W. (2024). Role of forensic investigations in reduction of financial fraud among commercial banks in South Sudan. *International Journal of Finance and Accounting, 3*(1), 1–14. https://doi.org/10.11648/j.ijfa.20240301.11

Manocha, T., Sharma, R., Sharma, V., & Kumar, H. (2024, November). Blockchain in E-Commerce: Assessing Key Factors, Consumer Perceptions, and Implementation Challenges. In *2024 International Conference on Intelligent & Innovative Practices in Engineering & Management (IIPEM)* (pp. 1-6). IEEE.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). *Big data: The next frontier for innovation, competition, and productivity*. McKinsey Global Institute. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation

Musa, A. S., Awan, I. U., & Zahrah, F. (2024). The case for validating ADDIE model as a digital forensic model for peer-to-peer network investigation. *Information Systems Frontiers*, *26*(6), 2305-2321.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision support systems*, *50*(3), 559-569.

Nigeria Inter-Bank Settlement System (NIBSS). (2021). *NIBSS Industry Fraud Report 2019–2021*. NIBSS Publications.

Nwaobia, A.W., Omotayo, I.I., & Ajibade, A. (2021). Internal audit and fraud detection in selected banks listed in Nigeria. *IOSR Journal of economics and Finance, 12*(1), 51-65

Ochieng'Oyugi, G. J., & Kamaara, M. (2023). E-procurement practices and procurement performance in Kenya's state enterprises. *International Journal of Management and Business Research*, *5*(2), 383-395.

Ogunwole, A. E., & Jimoh, S. A. (2024). Forensic Accounting Services as a tool for Fraud Mitigation in Selected Kwara State owned Tertiary Institutions in Nigeria. *NIU Journal of Social Sciences*, *10*(1), 57-67.

Olajide R. (2025, April 22). Afripost Newspaper. Union Bank faces ₦9.3 billion fraud scandal linked to system breach. https://afripost.ng/2025/04/22/union-bank-faces-%E2%82%A69-3-billion-fraud-scandal-linked-to-system-breach/#:~:text=Union%20Bank%20of%20Nigeria%

Olaoye, C. O., & Dada, R. A. (2017). The roles of auditors in fraud detection and Prevention in Nigeria deposit money banks: Evidence from southwest. *European Scientific Journal, 13*(31), 290-306

Oluyide, S. E. (2025). The Impact of Forensic Accounting Techniques in Mitigating Electronic Fraud in Nigeria's Deposit Money Banks. *The Journal of Forensic Accounting Profession*, *5*(1), 43-63.

Onamusi, G. E., Farouk, M. A., Uyagu, B. D., & Ekele, J. S. (2024). Effect of digital forensic accounting technological tools on cyber financial fraud detection among quoted deposit money banks in Nigeria. *International Journal of Capacity Building in Education and Management*, *6*(5), 45-57.

Oyedokun, G. E. (2020). Forensic accounting investigation and fraud prevention in Nigeria. *Journal of Accounting Research, 6*(2), 120–134.

Proshare. (2025). *Getting Bigger, Braver, and Dominant – The Class of 2025: Proshare Bank Strength Index Report*. Proshare

Radenković, B., Despotović-Zrakić, M., & Labus, A. (2023). Digital payment systems: state and perspectives. In *Digital Transformation of the Financial Industry: Approaches and Applications* (pp. 203-216). Cham: Springer International Publishing

Rahman, M. J., & Jie, X. (2024). Fraud detection using fraud triangle theory: evidence from China. *Journal of Financial Crime*, *31*(1), 101-118.

Renata, F., & Marlinah, A. (2022). Theoretical Analysis Fraud Diamond in Detecting Financial statement

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.

Singh, S., Singh, S., & Kajla, T. (2023). Checking the effectiveness of blockchain application in fraud detection with a systematic literature review approach. *Contemporary Studies of Risks in Emerging Technology, Part B*, 57-86

Taherdoost, H. (2023). *Smart Contracts in Blockchain Technology: A Critical Review. Information 2023, 14, 117*.

Tally, G. (2022). Forensic accounting technique. https://tallysolutions.com/us/accounting/what-is-forensic-accounting-and-techniques/#gref. Received 21/03/2023

Thomas, N. S. (2024). *The Applications of Data Mining Techniques in Detecting Occupational Fraud: A Qualitative Review of Forensic Accounting Practices* (Doctoral dissertation, Dublin Business School).

Uduehe, E. M., Okoye, E. I., & Amahalu, N. N. (2024). Forensic accounting techniques and fraud management of commercial banks in Awka-South Anambra State. *Journal of Global Accounting*, *10*(2), 307-346.

Vivek, Y., Ravi, V., Mane, A., & Naidu, L. R. (2024, October). Explainable artificial intelligence and causal inference based atm fraud detection. In *2024 IEEE Symposium on Computational Intelligence for Financial Engineering and Economics (CIFEr)* (pp. 1-7). IEEE.

Wells, A. (2005). Detached mindfulness in cognitive therapy: A metacognitive analysis and ten techniques. *Journal of rational-emotive and cognitive-behavior therapy*, *23*, 337-355.