FUDMA Journal of Accounting and Finance Research, 4(1). ISSN: 2992-4693 (Online); 2992-2704 (Print)

Integrating digital forensics and machine learning for fraud detection in Nigerian deposit money banks: a PLS-SEM and artificial neural network approach

Ridwan Adebisi Sanusi[1], Ibraheem Sanusi[2]*, D. O. B Briggs[3]
[1,3]Department of Accounting, Nasarawa State University, Keffi, Nigeria
[2]Department of Statistics, University of Ibadan, Nigeria
**Corresponding author: sanusi.adebisi1726@gmail.com*

https://doi.org/10.33003/fujafr-2026.v4i1.286.53-69

Abstract

Purpose: This study examines the association between digital forensic capabilities and fraud detection effectiveness in Nigeria's five largest deposit money banks—United Bank for Africa Plc, Zenith Bank Plc, Access Bank Plc, First Bank Nigeria Limited, and Guaranty Trust Bank Plc. Specifically, it evaluates the relative contributions of network forensics, cloud forensics, mobile forensics, and Internet of Things (IoT) forensics to fraud detection effectiveness.
Methodology: A cross-sectional survey design was adopted, with data collected through structured questionnaires administered to staff of the selected banks. Of the 306 questionnaires distributed, 243 valid responses were obtained, representing a 79% response rate. Data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) to test hypothesized relationships and Artificial Neural Network (ANN) analysis to assess predictive importance. PLS-SEM analysis was conducted using JASP version 0.95.3, while ANN estimation employed a multilayer perceptron model in SPSS version 27.
Results and conclusion: The PLS-SEM results indicate that digital forensic capabilities jointly explain a substantial proportion of variance in fraud detection effectiveness with all $R^2 > 0.75$. Cloud forensics ($\beta = 0.515$) and network forensics ($\beta = 0.500$) exhibit the strongest associations, followed by IoT forensics ($\beta = 0.456$) and mobile forensics ($\beta = 0.449$). ANN results corroborate these findings, ranking cloud forensics as the most important predictor (normalized importance = 100%), closely followed by network forensics (99.7%), mobile forensics (85.3%), and IoT forensics (79.8%).
Implication of findings: The study implies that bank management should prioritize investment in cloud and network forensic infrastructures, complemented by targeted training and process integration, to enhance fraud detection performance. However, the cross-sectional and self-reported nature of the data limits causal inference, indicating the need for future longitudinal studies using objective fraud performance indicators.

Keywords: Cloud forensic, Fraud detection, IoT forensic, Mobile forensic, Network forensic.

1. Introduction

International financial institutions operate in an increasingly complex and highly digitalized environment, making them particularly vulnerable to sophisticated, dynamic fraud schemes that continually evolve with technological advancements. As financial crimes become more complex, traditional detection systems alone are insufficient, necessitating more advanced technical solutions. In this context, digital forensics, which formally captures, identifies, extracts, and analyzes digital evidence, has emerged as a cornerstone for effective fraud detection and investigative processes, especially within legal and regulatory investigations (Dalwadi, 2023). Digital transformation across Nigeria's banking sector, particularly among Deposit Money Banks (DMBs), has improved accessibility and operational efficiency, yet simultaneously expanded the reach and sophistication of fraud schemes such as insider fraud, identity theft, and unauthorized transactions.

According to the 2023 Nigeria Inter-Bank Settlement System (NIBSS) Annual Fraud Landscape Report, the annual fraud count more than doubled from 44,947 cases in 2019 to 95,620 in 2023 (a 112% increase), while actual losses surged from ₦2.9 billion to ₦17.67 billion (a 496% increase) over the same period highlighting both the rapidly escalating fraud challenge and the inadequacy of traditional detection systems in the face of digital payment growth (NIBSS, 2023). Under operational pressures, many

Nigerian banks have begun adopting digital forensics methodologies designed to strengthen early fraud detection and provide evidence-based insights. However, the practical application of these techniques remains constrained by evolving cyber threats, limited technological infrastructure, and shortages of trained practitioners. In related research, forensic accounting techniques have been shown to improve corruption detection and litigation support in the public sector, implying potential benefits when extended to digital forensic practices in banking contexts. For instance, Akpootu & Yusuf (2025) demonstrated that forensic accounting significantly enhances corruption detection, suggesting the value of forensic capabilities in Nigerian financial systems.

Additionally, Osunwole et al. (2024) found that forensic accounting influences investigative objectivity, reinforcing the relevance of rigorous forensic processes within financial investigations. Though not banking-specific, these studies from FUJAFR underscore the broader impact of forensic methods in strengthening detection and accountability across Nigerian financial contexts. Theoretically, this study adopts a capability model framing: digital forensic capability—comprising sub-capabilities in network, cloud, mobile, and IoT forensics—enhances fraud detection capability (through improved detection speed, coverage, and quality of evidence), which in turn increases overall fraud detection effectiveness. This framework advances current literature by articulating how specific forensic sub-capabilities contribute to measurable detection outcomes, linking these to operational realities within Nigerian DMBs (a context under-researched in prior studies).

Prior work has largely focused on fraud detection in non-banking sectors or international settings (e.g., Griffiths & Pretorius, 2021; Baroto et al., 2020 in Indonesia; Ojukwu et al., 2020 in Nigeria's public sector), without rigorous empirical analysis of Nigerian DMBs or employing hybrid analytic techniques that capture both linear and nonlinear relationships. This study addresses these gaps by applying a hybrid PLS-SEM and Artificial Neural Network (ANN) methodology to assess the influence of digital forensics on fraud detection effectiveness in Nigeria's largest deposit money banks.

2. Literature review

Fraud diamond theory

The Fraud Diamond Theory advanced by Wolfe and Hermanson extends the traditional fraud triangle by introducing capability as a critical enabler of fraudulent behaviour. While pressure, opportunity, and rationalization explain the motivation and justification for fraud, capability accounts for the offender's technical competence, positional authority, system knowledge, and confidence to exploit control weaknesses and evade detection (Peprah, 2018; Adams, 2020). In contemporary banking environments characterized by digitalized operations, fraud capability increasingly manifests through technological sophistication rather than solely managerial authority. As such, digital forensic technologies represent institutional counter-capabilities that directly constrain offenders' ability to conceal fraudulent activities. This study draws on the Fraud Diamond Theory by conceptualizing digital forensics as an organizational capability that weakens the capability dimension of fraud, thereby increasing detection likelihood.

Anomie theory

Anomie Theory, proposed by Merton and Chinoy (1957), explains deviant behaviour because of structural strain arising from a misalignment between socially prescribed goals and legitimate means of attainment (Lau, 2020; Ugwu, 2021). In contexts where material success is emphasized and access to legitimate economic opportunities is constrained, individuals may resort to illicit practices such as fraud. Within the Nigerian banking sector, rapid digital transformation, performance pressures, and exposure to high-value financial transactions may intensify such strain. While Anomie Theory explains the motivational foundation of fraud, it does not address detection outcomes. This gap reinforces the importance of institutional mechanisms—such as digital forensic capabilities—that limit the translation of deviant motivation into undetected fraudulent outcomes.

Socio-technical systems perspective

The socio-technical systems theory (Trist & Bamforth, 1951) posits that organizational effectiveness depends on the alignment of technological systems with human actors, organizational processes, and governance structures. Applied to fraud detection, this perspective suggests that digital forensic tools do not operate independently but derive effectiveness from their integration into investigative workflows, staff competencies, and institutional policies. Network, cloud, mobile, and IoT forensics therefore function as interrelated technical subsystems that enhance fraud detection only when embedded within coherent organizational practices. This study adopts the socio-technical perspective to justify treating digital forensics as a multidimensional capability influencing fraud detection effectiveness through improved investigative processes and evidential quality.

Conceptualization of digital forensic capability

This study conceptualizes digital forensic capability as a latent organizational construct reflecting the extent to which digital forensic tools are deployed, operationalized, and embedded within fraud detection and investigation processes of deposit money banks. Rather than measuring mere technological availability, the construct captures functional application in detecting, analyzing, and preserving digital evidence. This capability-based conceptualization aligns with contemporary forensic and auditing literature, which emphasizes process integration and investigative utility as determinants of fraud detection effectiveness. Tagang et al., (2024) highlighted that effective information management practices significantly influence the containment of financial crimes by enhancing data quality, accessibility, security, and governance, which are essential precursors to timely detection and forensic investigation. Moreover, Chukwuma et al., (2025) demonstrated that corporate governance attributes such as independent directors and audit committee financial expertise significantly reduce the likelihood of financial statement fraud in listed deposit money banks, suggesting that governance complements technical forensic capabilities in strengthening fraud oversight.

Network forensics

Network forensics enhances fraud detection by enabling continuous monitoring, traffic reconstruction, and anomaly identification within banking networks. Through the analysis of packet flows, access logs, and intrusion trails, network forensics increases the probability of identifying unauthorized activities and reduces the time required to detect fraudulent transactions. Empirical evidence supports this mechanism. Adeniyi and Shola (2024) found network forensics to exert a statistically significant influence on fraud detection using PLS-SEM, while Naz and Khan (2024) reported similar outcomes in organizational settings. In Nigerian deposit money banks, where electronic payment platforms and real-time transaction processing dominate, network forensics constrains offenders' ability to conceal fraudulent actions across interconnected systems. This mechanism provides the empirical and theoretical basis for H1, which posits that network forensics significantly influences fraud detection.

Cloud computing forensics

Cloud computing forensics strengthens fraud detection by facilitating centralized evidence collection, scalable log analysis, and cross-system traceability of transactions stored within virtualized infrastructures. By enabling investigators to preserve volatile data, recover deleted records, and reconstruct transaction histories across distributed platforms, cloud forensics improves both detection accuracy and evidential admissibility. Onamusi et al. (2024) demonstrated that cloud computing forensics significantly enhances fraud detection in Nigerian deposit money banks, while Pham and Vu (2024) reported consistent findings using PLS-SEM among Vietnamese SMEs. Given the increasing reliance of Nigerian banks on cloud-based applications and data storage, cloud forensics reduces informational asymmetry and strengthens investigative depth, thereby justifying H2, which predicts a significant effect of cloud computing forensics on fraud detection.

Mobile device forensics

Mobile device forensics contributes to fraud detection by enabling the extraction and analysis of communication records, authentication credentials, transaction alerts, and application data from mobile devices used in banking transactions. This capability directly links fraudulent activities to user behaviour, thereby improving attribution and reducing detection latency. Garba (2024) found that mobile device forensics significantly improves fraud detection in Nigerian deposit money institutions, while Onyema et al. (2024) reported similar positive effects using regression and ANOVA analyses. As mobile banking fraud continues to rise in Nigeria, mobile device forensics serves as a critical investigative mechanism that enhances detection probability and evidential clarity. These empirical and contextual considerations underpin H3, which posits that mobile device forensics has a significant effect on fraud detection.

Internet of things (IoT) forensics

IoT forensics improves fraud detection by enabling the analysis of data generated from interconnected devices such as ATMs, POS terminals, biometric access systems, and surveillance infrastructure. By correlating device-level logs with transactional data, IoT forensics enhances detection coverage and strengthens evidential triangulation in complex fraud cases. Nentawe and Tumba (2024) documented a strong positive relationship between IoT forensics and fraud detection in Nigerian deposit money banks, while Ahmad and Lee (2024) reported comparable findings in Malaysian commercial banks. In digitally interconnected banking environments, IoT forensics limits offenders' ability to exploit device-based vulnerabilities without detection. This mechanism provides the empirical foundation for H4, which asserts that IoT forensics significantly influences fraud detection.

3. Methodology

The survey research design adopted in this study is based on a positivist theory which considers the researcher to be a neutral information collector. As the survey design looks at a population sample one time and observes its behavior but does not intervene, the results are generalizable. It explores causation by investigating variables, including their interrelations with people, events, decisions, or systems through various means. Such exploration is useful in obtaining appropriate data along with demographics and respondent views.

The population of the study comprised 1,305 internal control, senior, and managerial staff drawn from Nigeria's five largest internationally authorized deposit money banks—United Bank for Africa Plc (UBA), Zenith Bank Plc, Access Bank Plc, First Bank of Nigeria Limited, and Guarantee Trust Bank Plc (GTBank). The population figure was constructed based on staff records and regulatory disclosures covering the 2019–2023 operational period, focusing specifically on personnel directly involved in financial reporting, transaction processing, risk management, information technology, audit, and internal control functions. These categories were selected because of their operational proximity to digital banking systems and fraud detection processes, making them information-rich for the objectives of the study.

The five banks were purposively selected due to their extensive domestic and international operations, advanced digital banking infrastructure, and higher exposure to sophisticated and technology-driven fraud risks relative to smaller or regionally focused banks. Within each bank, the target respondents included accountants, internal and external auditors, IT and cybersecurity professionals, economists, internal control officers, and senior management staff who possess relevant knowledge of digital forensic practices and fraud detection mechanisms. Sample size was determined using Taro Yamane's (1967) formula:

$$n = \frac{N}{1 + N(e)^2}$$

Where n = sample size
N = Population Size (1305)
e = level of significance at 5% (0.05)

$$n = \frac{1305}{1 + 1305(0.05)^2}$$

$$n = \frac{1305}{1 + 3.2625}$$

$$n = \frac{1305}{4.2625}$$

$$n = 306$$

Table 1: Population and sample distribution of respondents across selected deposit money banks

Deposit Money Bank	Estimated Population of Relevant Staff	Proportion of Total Population (%)	Questionnaires Distributed	Valid Responses Retrieved
United Bank for Africa Plc (UBA)	275	21.1	65	52
Zenith Bank Plc	290	22.2	68	55
Access Bank Plc	310	23.8	73	59
First Bank of Nigeria Ltd	260	19.9	61	47
Guarantee Trust Bank Plc (GTBank)	170	13	39	30
Total	1,305	100	306	243

A proportionate stratified sampling technique was adopted to ensure adequate representation of each bank in line with its share of the total population. Consequently, questionnaires were allocated proportionately across the five banks based on staff strength within the defined categories, rather than using equal allocation, to minimize sampling bias and improve external validity. A total of 306 questionnaires were distributed accordingly. Out of the distributed questionnaires, 243 were correctly completed and returned, yielding an effective response rate of 79%. The high response rate was largely attributable to the researcher's physical administration of the instrument and follow-up visits. To assess potential non-response bias, an early–late respondent comparison was conducted by examining mean differences in key constructs; no statistically significant differences were observed, suggesting that non-response bias was unlikely to materially affect the study's findings.

Methods of data collection

Primary data were collected using a structured questionnaire designed to obtain direct and reliable information from respondents for hypothesis testing. The questionnaire was divided into six sections.

- Section A captured respondents' demographic information (gender, age, educational qualification, position, and department).
- Sections B–F contained items measuring the study's constructs: Fraud Detection, Network Forensics, Cloud Computing Forensics, Mobile Device Forensics, and Internet of Things (IoT) Forensics.

Each construct included five items adapted from validated scales (e.g., Ahmad & Lee, 2023; Ibrahim & Musa, 2022) to suit Nigerian Deposit Money Banks, ensuring contextual relevance and conceptual equivalence. Items were rated on a 5-point Likert scale (5 = Strongly Agree to 1 = Strongly Disagree), chosen for its flexibility in measuring opinion intensity and enabling statistical analysis.

Validity and reliability

The initial questionnaire was reviewed by five experts (three forensic accounting academics and two banking risk managers) for content validity, clarity, and relevance, leading to minor revisions. A pilot study with 20 respondents from one deposit money bank (excluded from the main sample) tested reliability and validity. Cronbach's alpha results showed all constructs had strong internal consistency above 0.7 (Network Forensic = 0.91; Cloud Forensic = 0.89; Mobile Forensic = 0.87; IoT Forensic = 0.88; Fraud Detection = 0.85), confirming the questionnaire's reliability for the main study.

Ethical consideration

The ethical considerations of this study followed human research. Participants were made aware of the study's purpose and informed of its voluntary nature and the right to refuse to participate without penalty. Consent was acquired, responses were de-identified, and confidentiality was guaranteed by anonymizing information and limiting data access. There was no coercion, deception and the study avoided unnecessary personal data. All data were restricted to academic purposes and are stored in password-protected files. The study received ethical approval from the institutional review committee prior to the study.

Techniques for data analysis and model specification

Data were analyzed descriptively (mean, median, standard deviation) and hypotheses were tested using PLS-SEM (Partial Least Squares Structural Equation Modeling) at a 0.05 significance level. PLS-SEM, developed by Wold (1982), is a non-parametric technique that utilizes weight vector regressions coupled with bootstrapping to evaluate path coefficients, Cronbach's alpha, R^2, and Variance Inflation Factor (VIF). The analysis started with outer loadings of indicators, where a cutoff of 0.7 indicates over 50% variance explained and construct reliability. Internal consistency using Jöreskog's Composite Reliability criteria of 0.60–0.70 is acceptable for exploratory research and 0.70–0.90 is adequate to good. When using Cronbach's alpha, which is computed assuming equal contribution of indicators and generally below Composite Reliability, a value above 0.7 is considered reliable. Average Variance Extracted (AVE) of ≥0.50 represents a construct explaining at least half the variance of its indicators. VIF checks for the presence of collinearity: a value above 5 indicates severe collinearity. R^2 shows in-sample predictive power, from 0 to 1, where 0.75, 0.50, and 0.25 indicate substantial, moderate, and weak explanatory power, respectively.

In this study, digital forensic capability constructs comprising network, cloud, mobile, and IoT forensics—were operationalized reflectively because each set of indicators is conceptualized as a manifestation of the underlying latent capability rather than as independent components. Reflective models assume that the latent construct causes the observed indicators, such that conceptual changes in the construct would lead to corresponding changes in all its indicators. Under reflective measurement, indicators are expected to be highly correlated and interchangeable, such that omission of a single indicator does not alter the conceptual meaning of the underlying construct. This is consistent with psychometric guidelines indicating that reflective indicators share a common underlying cause and covary as a result (i.e., latent variable → indicators), and internal consistency reliability assessments are appropriate (e.g., Cronbach's alpha and Composite Reliability) for reflective constructs (Hanafiah, 2020).

Artificial Neural Network

Artificial Neural Network (ANN) is a machine learning algorithm modeling human neurons based on how they work. It aims to detect correlations and help individuals to become better decision makers (Goel, Goel & Kumar, 2023). ANN is most beneficial in the accounting and financial systems as it enhances predictive analytics, anomaly detection, and data security (Sarker, 2023). They are often used for the identification, prediction, and classification of complicated trends. This allows them to be used for financial data analysis in environments as diverse as cloud-hosted accounting security and risk evaluation. An ANN has an input layer, one or more hidden layers, and an output layer. Each layer is made up of interconnected nodes (neurons) in which each neuron receives inputs that have been weighted and will output as an activation function, which will then trigger the transmission of the output to the next layer. For predicting data, a backpropagation algorithm is used to minimize the error between the predicted and observed values.

4. Results and discussion

Table 2 shows that 57.6% of respondents were male, 42.4% female. Most participants (42%) were aged 30–39, followed by under 30 (26.7%), 40–49 (22.6%), and 50+ (8.6%). Educationally, 49.4% held a B.Sc. or B.A., 25.1% an MBA/Master's, 17.3% an ND/HND, and 4.1% a PhD or other qualifications. Nearly half worked in key operational areas: Internal Audit (26.7%), Finance/Accounting (24.7%), ICT (22.6%), and Risk Management (19.8%), with 6.2% in other departments. This reflects a diverse, experienced workforce occupying vital compliance and control roles.

Table 2: Demographic information

Variables	Options	Frequency (n)	Percentage (%)
Gender	Male	140	57.60%
	Female	103	42.40%
Age	Less than 30 years	65	26.70%
	30–39 years	102	42.00%
	40–49 years	55	22.60%
	50 years and above	21	8.60%
Educational Qualification	ND/HND	42	17.30%
	B.Sc./B.A.	120	49.40%
	M.Sc./MBA	61	25.10%
	PhD	10	4.10%
	Others	10	4.10%
Department/Unit	Internal Audit	65	26.70%
	ICT	55	22.60%
	Risk Management	48	19.80%
	Finance/Accounting	60	24.70%
	Others	15	6.20%

Partial least square structural equation model

Table 3: Reliability measure and average variance extracted

Latent Variable	Cronbach's α	Jöreskog's ρ	Dijkstra-Henseler's ρ	AVE
Network Forensic	0.955	0.955	0.958	0.559
Cloud Forensic	0.959	0.959	0.96	0.811
Mobile Forensic	0.947	0.947	0.95	0.826
IoT Forensic	0.949	0.949	0.951	0.784
Fraud Detection	0.863	0.863	0.863	0.789

Table 3 shows reliability measures for each latent variable. These measures indicate how consistent the indicators are with one another. Among them are Cronbach's alpha, Jöreskog's rho and Dijkstra-Henseler's rho. All the constructs exhibit reliability coefficients well above the recommended threshold of 0.70 (Hair et al., 2021), indicating strong internal consistency among their measurement items. The Average Variance Extracted (AVE) values for each latent variable in the model illustrate the proportion of variance captured by the construct as opposed to variance resulting from measurement errors. The indicators have good convergent validity and accurately measure their underlying construct when the AVE value is greater than 0.50. Every construct in this study exceeded this threshold. This indicates that the indicators accurately reflect the construct.

Table 4: Factor loading estimate

Construct	Indicator	Estimate	R^2	Total R^2
Network Forensic	NF1	0.83	0.8	0.81
	NF2	0.91	0.796	
	NF3	0.978	0.822	
	NF4	0.919	0.827	
	NF5	0.854	0.805	
Cloud Forensic	CF1	0.859	0.81	0.826
	CF2	0.955	0.823	
	CF3	0.901	0.84	
	CF4	0.913	0.833	
	CF5	0.912	0.822	
Mobile Forensic	MF1	0.886	0.806	0.783
	MF2	0.934	0.825	
	MF3	0.851	0.794	
	MF4	0.939	0.773	
	MF5	0.805	0.717	
IoT Forensic	IF1	0.872	0.764	0.788
	IF2	0.856	0.766	
	IF3	0.964	0.793	
	IF4	0.836	0.796	
	IF5	0.904	0.823	

Table 4 shows factor loadings for each construct and its indicators, all exceeding the 0.70 threshold), indicating significant contributions to their constructs. These strong loadings confirm the measurement model’s convergent validity and indicator reliability (Hair et al., 2021). The R^2 values, representing variance explained by latent variables, all exceed 0.75, demonstrating strong explanatory power (Shmueli et al., 2016).

Table 5: Fornell-Larcker matrix

Latent Variable	Network Forensic	Cloud Forensic	Mobile Forensic	IoT Forensic	Fraud Detection
Network Forensic	**0.748**				
Cloud Forensic	<.001	**0.901**			
Mobile Forensic	0.046	0.085	**0.909**		
IoT Forensic	0.01	0.068	0.784	**0.885**	
Fraud Detection	0.494	0.554	0.556	0.535	**0.888**

The Fornell–Larcker matrix indicates that discriminant validity is adequately established among the latent constructs in the model as shown in table 5. The square roots of the Average Variance Extracted (AVE), shown on the diagonal, are relatively high for all constructs—Network Forensic (0.748), Cloud Forensic (0.901), Mobile Forensic (0.909), IoT Forensic (0.885), and Fraud Detection (0.888)—demonstrating strong convergent validity. Importantly, for each construct, the diagonal value exceeds its correlations with other constructs, satisfying the Fornell–Larcker criterion.

Table 6: Heterotrait–Monotrait ratio (HTMT)

Latent Variable	Network Forensic	Cloud Forensic	Mobile Forensic	IoT Forensic
Network Forensic				
Cloud Forensic	0.62			
Mobile Forensic	0.58	0.64		
IoT Forensic	0.55	0.61	0.79	
Fraud Detection	0.69	0.74	0.75	0.72

Discriminant validity was also assessed using the Heterotrait–Monotrait (HTMT) ratio as shown in Table 6. The HTMT values were all below the 0.90 threshold (Henseler, Ringle, & Sarstedt, 2015). These results confirm that all constructs are empirically distinct and measure unique theoretical concepts.

Table 7: PLS-SEM model fit

Model Fit Indices	Value
Q^2 (Predictive Relevance, Blindfolding)	0.683
Bootstrapping Resamples	5,000
P-value	< .001
Measurement Model Type	Reflective

Source: JASP Output, 2026.

Table 7 presents the model fit indices for the Partial Least Squares Structural Equation Model (PLS-SEM) used in this study. The Q^2 predictive relevance value (0.683) obtained through blindfolding procedures further demonstrates the model's strong out-of-sample predictive accuracy. The results from 5,000 bootstrap resamples show that all path coefficients were statistically significant ($p < .001$), validating the robustness of the model.

Table 8: PLS-SEM total effect estimates

Outcome	Predictor	Estimate	f²	z-value	p-value	95% CI (LL, UL)	VIF
Fraud Detection	Network Forensic	0.500	0.26	8.42	<0.001	(0.38, 0.61)	1.006
	Cloud Forensic	0.515	0.29	8.97	<0.001	(0.40, 0.63)	1.015
	Mobile Forensic	0.449	0.21	7.65	<0.001	(0.32, 0.57)	1.017
	IoT Forensic	0.456	0.22	7.88	<0.001	(0.33, 0.58)	1.011

Table 8 presents PLS-SEM total effect estimates showing all predictors positively and significantly impact Fraud Detection: Cloud Forensic (0.515), Network Forensic (0.500), IoT Forensic (0.456), and Mobile Forensic (0.449). These values indicate that all predictors have substantial positive effects on Fraud Detection which implies that enhancing any forensic capability boosts fraud detection. Among the predictors, cloud forensic exhibits the strongest effect, as reflected by the highest estimate and effect size ($f^2 = 0.29$), followed by network forensic ($f^2 = 0.26$), IoT forensic ($f^2 = 0.22$), and mobile forensic ($f^2 = 0.21$), indicating moderate to substantial practical significance Low VIF values (1.006–1.017) confirm no multicollinearity and unique contributions from each construct..The path diagram is shown in Figure 1.

Artificial neural network

The Artificial Neural Network (ANN) analysis was conducted using the Multilayer Perceptron (MLP) algorithm in SPSS to complement the structural equation modeling (SEM) results. Prior to model estimation, the data were preprocessed to enhance model performance. All predictor variables were standardized using z-score normalization to ensure comparability and to prevent variables with larger scales from disproportionately influencing the learning process. The dataset contained no missing values, as incomplete responses were screened and removed during the data-cleaning stage. While SEM provides theory-driven explanations of causal relationships and hypothesis testing, ANN enhances predictive accuracy and allows for ranking the relative importance of predictors in a non-parametric manner. This complementary SEM–ANN approach has been widely adopted in prior studies to combine explanatory and predictive strengths in complex behavioral and technological research contexts (e.g., Xu et al., 2024; Yan et al., 2022).

Table 9: Case Processing Summary

		N	Percent
Sample	Training	168	69.10%
	Testing	75	30.90%

No of unit=4, Rescaling Method for Covariates=Standardized, Number of hidden layer=1, Number of Units in Hidden Layer 1=3, Number of Units in output layer = 1.

Table 9 shows the Artificial Neural Network (ANN) case processing summary, with 243 valid responses split into 168 (69.1%) for training and 75 (30.9%) for testing, following standard machine learning practice to balance model training and evaluation. The ANN has one hidden layer with three neurons to capture nonlinear relationships and an output layer with one neuron using an identity activation function for the continuous dependent variable. The network diagram is shown in Figure 3.

Table 10: Model summary

Training	Sum of Squares Error	12.07
	Relative Error	0.145
Testing	Sum of Squares Error	7.167
	Relative Error	0.152

Table 10 summarizes the Artificial Neural Network (ANN) model's performance, showing sum of squares error (SSE) of 12.07 for training and 7.167 for testing, indicating low prediction errors. Relative errors of 0.145 (training) and 0.152 (testing) demonstrate stable predictive accuracy and good generalization to unseen data.

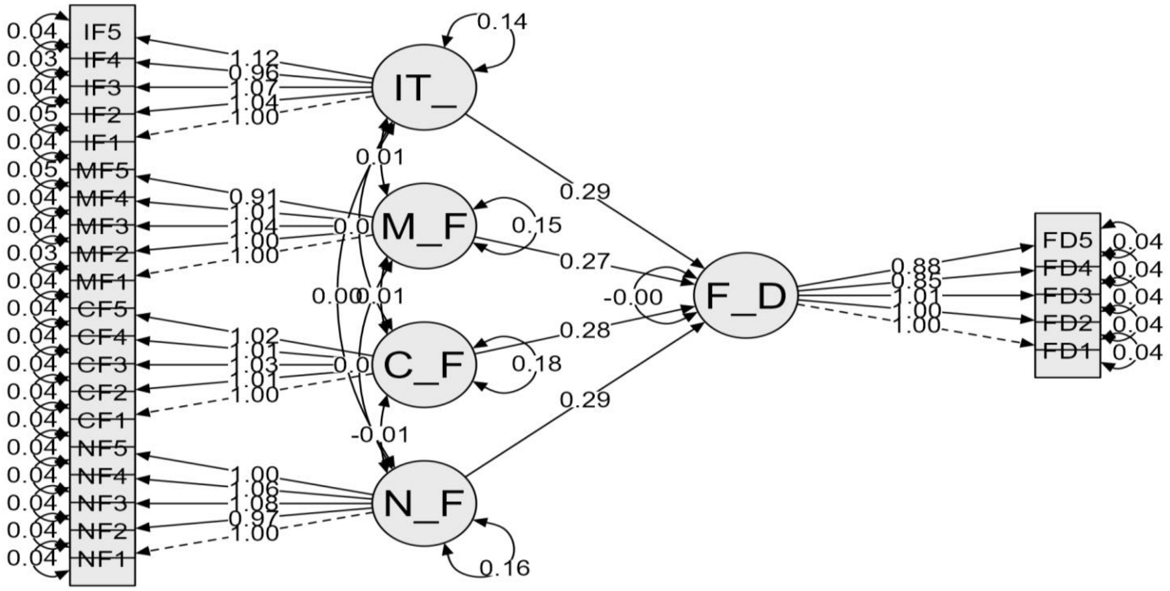

Figure 1: PLS-SEM Path Diagram
Source: JASP Output

Table 11: Independent variable importance

Variables	Importance	Normalized Importance
Network Forensic	0.273	99.7%
Cloud Forensic	0.274	100%
Mobile Forensic	0.234	85.3%
IoT Forensic	0.219	79.8%

Table 11 presents the relative importance of each independent variable in predicting Fraud Detection within the Artificial Neural Network (ANN) model. Among the predictors, Cloud Forensic exhibits the highest influence with an importance score of 0.274 and a normalized importance of 100%, indicating that it contributes most significantly to the model's predictive accuracy. Network Forensic follows closely with a normalized importance of 99.7%, suggesting an almost equivalent predictive strength in improving fraud detection outcomes. Mobile Forensic (85.3%) and IoT Forensic (79.8%) also make substantial contributions, highlighting their complementary roles in strengthening the fraud detection framework of deposit money banks.

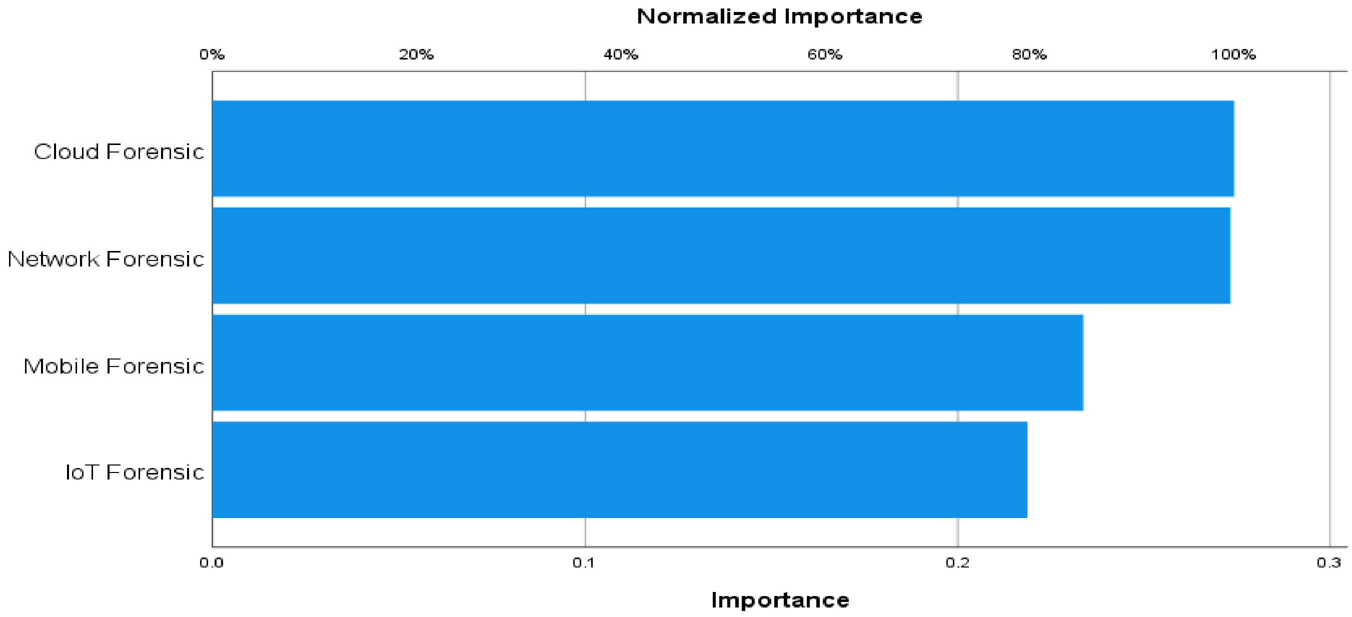

Figure 2: Variable importance plot
Source: SPSS Output

Figure 2 shows the variable importance plot of the ANN model which is in support of the figures in table 8.

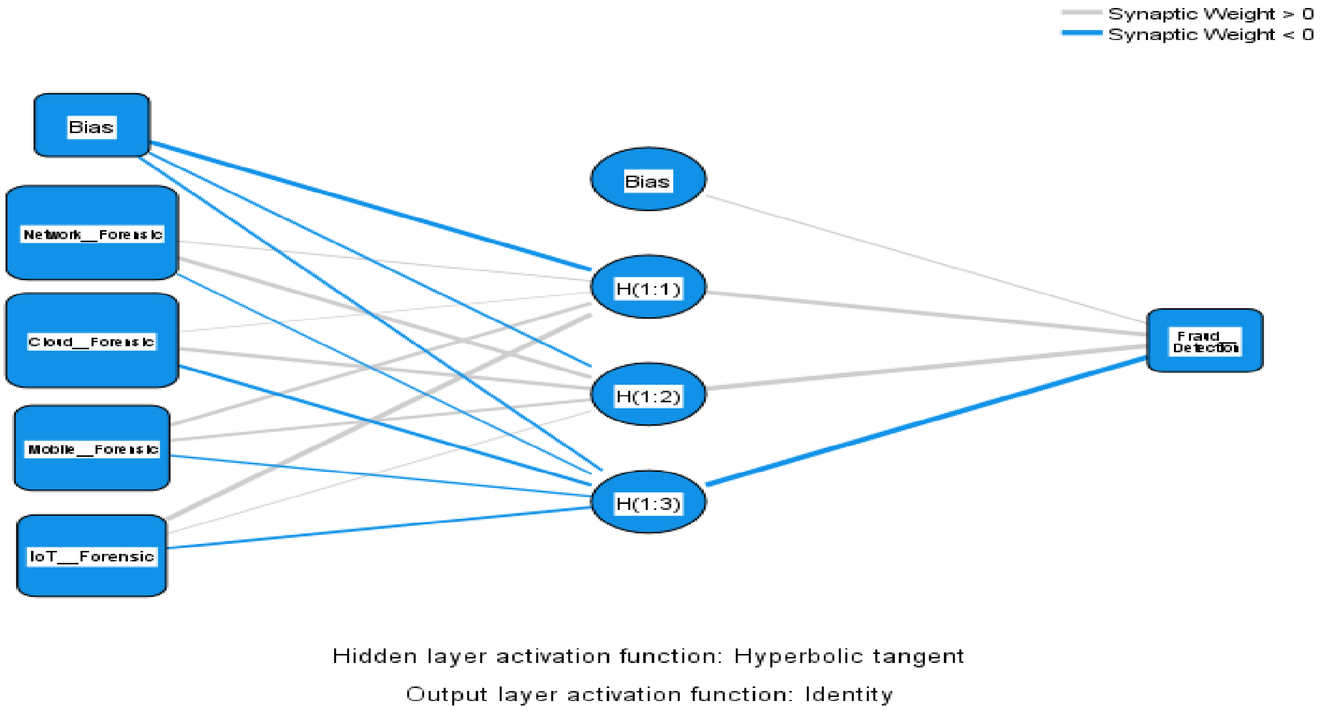

Figure 3: Network Diagram
Source: SPSS Output

Discussion of findings

The findings indicate that not all digital forensic capabilities are equally associated with fraud detection effectiveness in Nigerian deposit money banks, with cloud forensic capability emerging as the most influential, followed by network forensics, while mobile and IoT forensics play comparatively smaller but complementary roles. The ANN ranking suggests that capabilities embedded within core banking infrastructures matter most, reflecting operational realities in which transaction processing, audit trails, and fraud monitoring systems are increasingly cloud-based and network-dependent, thereby making forensic visibility at these levels more strongly associated with effective detection. The effect sizes observed are moderate to substantial for cloud and network forensics, indicating that these associations are not merely statistically detectable but practically meaningful, whereas the smaller effect sizes for mobile and IoT forensics imply diminishing marginal returns when these capabilities are developed in isolation. From a budgeting perspective, the results imply that fraud detection effectiveness is more closely associated with strategic investment in centralized forensic platforms, network analytics, and staff competence to interpret forensic outputs than with the acquisition of standalone tools alone, underscoring the importance of balancing technology spending with training and process integration.
Theoretically, the findings refine the study's framework by extending fraud and socio-technical theories to show that institutional forensic counter-capabilities are hierarchical rather than uniform, with those most tightly coupled to core banking systems exhibiting stronger associations with detection outcomes, thereby moving beyond a generalized technology–performance linkage. However, future longitudinal research is needed to establish temporal and causal ordering among forensic capability development and fraud detection effectiveness. These results are consistent with prior studies that emphasize the centrality of infrastructure-level analytics and centralized forensic platforms in enhancing financial fraud monitoring (e.g., Adeniyi and Shola, 2024), as well as research highlighting the growing role of cloud-based audit technologies in strengthening continuous assurance and fraud detection in financial institutions (Onamusi et al., 2024; Pham and Vu, 2024).

5. Conclusion

According to the study, digital forensics, including network forensics, cloud forensics, mobile forensics, and Internet of Things (IoT) forensics, has a robust and positive relationship with fraudulent activity detection in Nigeria's largest deposit money banks. PLS-SEM and Artificial Neural Network analyses show that cloud and network forensics have the most impact on enhancing fraud detection systems. This points to the fact that Nigerian banks can be significantly improved in regard to their internal control systems and fraud detection mechanisms if strong forensic tools and analytics are incorporated in this area. The results thus also emphasize the increasing relevance of digital forensic integration in the financial institutions' business strategy to foster transparency, data integrity, and accountability.

Based on the results, several practical recommendations are provided:

i. It is imperative that banks create centralized network monitoring systems that can retain forensic logs for a minimum of twelve months, integrating these with Security Information and Event Management (SIEM) platforms to enhance data forensic surveillance online.
ii. Implementation of cloud forensics procedures must be standardized utilizing detailed operational playbooks supported by vendor agreements that facilitate timely access to stored data.
iii. For at least one staff member, banks should purchase new mobile forensic tools and offer professional certification training for everyone hundred employees.
iv. Cross-functional forensic response teams must also be established to coordinate investigations and to run regular drills to gauge readiness. On a policy level, the Central Bank of Nigeria (CBN)

should also enhance its own regulatory framework to provide guidelines for the retention of forensic records, the reporting of incidents, and competency standards for digital forensic units.

Notwithstanding these contributions, the study is subject to several limitations. First, reliance on self-reported perceptual measures raises the possibility of common method bias and subjective assessment of fraud detection effectiveness. Additionally, the cross-sectional research design restricts causal inference, limiting the ability to observe dynamic capability development over time. Future research should address these limitations by incorporating objective fraud detection key performance indicators, such as fraud loss ratios, detection latency, and false-positive rates. Longitudinal studies examining the evolution of digital forensic capability adoption would further enhance causal understanding, while mixed methods approaches combining surveys, interviews, and forensic audit case analyses could provide richer contextual insights into how digital forensics is operationalized within banking environments.

Reference

Adams, A. (2020). *Effect of forensic auditing on deposit bank frauds in Nigeria* (Doctoral Dissertation, Salem University, Lokoja, Kogi State).

Adeniyi, E. O., & Shola, A. J. (2024). Forensic accounting services as a tool for fraud mitigation in selected Kwara State-owned tertiary institutions in Nigeria. *Nexus International University Journal of Social Sciences, 10*(1), 57–67.

Ahmad, M., & Lee, K. (2024). Impact of internet of things forensic on financial fraud detection and prevention in Malaysian commercial banks. *Journal of Financial Services Research*, *8*(3), 97-114.

Baroto, W., Agung, O.I. & Darajat, F. (2020). Digital Forensic Readiness for Micro, Small, and Medium Enterprise in Indonesia, *International Journal of Management and Applied Science*, *2* (2), 20-31.

Dalwadi, P. (2023). Uncovering financial fraud: The role of forensic accounting in preventing and detecting fraud in India. *International Journal of Management, Public Policy and Research, 2*(2), 1–5.

Garba, A. (2024). Impact of forensic accounting on fraud detection in Nigerian deposit money banks. *Journal of Advance Research in Business, Management and Accounting,* 10(2), 16–30.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., & Danks, N. P. (2021). Partial least squares structural equation modeling (PLS-SEM) using R: A workbook. *Springer Nature*. https://doi.org/10.1007/978-3-030-80519-7

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

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.

Goel, A., Goel, A. K., & Kumar, A. (2023). The role of artificial neural network and machine learning in utilizing spatial information. *Spatial Information Research*, *31*(3), 275-285. https://doi.org/10.1007/s41324-022-00494-x

Griffiths, L., & Pretorius, H. W. (2021). Implementing robotic process automation for auditing and fraud control. In Society 5.0: First International Conference, Society 5.0 2021, Virtual Event, June 22–24, 2021, Revised Selected Papers 1 (pp. 26-36). *Springer International Publishing.*

Ibrahim, K. M., & Musa, S. J. (2022). Effect of corporate governance on risk management of selected deposit money banks in Nigeria. *International Journal of Health Sciences, 6*(S6), 6193–6203.

Lau, T. F. T. (2020). The Concept of Anomie in explaining crime. *Bellarmine Law Society Review*, *11*(1). https://ejournals.bc.edu/index.php/blsr/article/view/12829

Naz, I., & Khan, S. N. (2024). Impact of forensic accounting on fraud detection and prevention: A case of firms in Pakistan. *Journal of Financial Crime, 1*(3), 43–54.

Nentawe, D. N., & Tumba, F. N. (2024). Effects of forensic accounting and fraud detection in Nigerian deposit money banks. *Journal of Accounting*, *3*(11), 88–98.

Ojukwu, S. E., Ubi, J. J., Olugbemi, K. O., Olugbemi, M. D., & Emefiele, C. C. (2020). Forensic accounting and fraud detection in Nigerian universities: A study of Cross River University of Technology. *Journal of Accounting and Financial Management, 6*(4), 61–72.

Onyema, C. C., Ojo-Agbodu, A. A., & Adebayo, M. A. (2024). Impact of forensic accounting on fraud management: An examination of some selected deposit money banks in Nigeria. *International Journal of Research and Innovation in Social Science, 8*(4), 1648–1661.

Peprah, W. K. (2018). Predictive relationships among the elements of the fraud diamond theory: The perspective of accountants. *International Journal of Academic Research in Accounting, Finance and Management Services*, *8*(3), 141-148. http://dx.doi.org/10.6007/IJARAFMS/v8-i3/4547

Pham, Q. H., & Vu, K. P. (2024). Insight into how digital forensic accounting and metaverse circular business model innovation contribute to accelerated internationalization: evidence from Vietnam-based SMEs. *Cogent Business & Management*, *11*(1), 88-91.

Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science*, *10*(6), 1473-1498. https://doi.org/10.1007/s40745-022-00444-2

Ugwu, J. I. (2021). Forensic accounting and fraud control in Nigeria: A critical review. *Research Journal of Finance and Accounting*, *12*(10), 112-120.

Akpootu, E. J., & Yusuf, Y. (2025). Forensic accounting litigation support and detection of public sector corruption in Nigeria. *FUDMA Journal of Accounting and Finance Research [FUJAFR]*, *3*(4), 221–238. https://doi.org/10.33003/fujafr-2025.v3i4.253.221-238

Osunwole, O. O., Adewumi, A. A., Adeyemi, O. A., & Adekanye, T. (2024). Influence of Forensic Accounting on Litigation Support and Engagement in Nigeria. *FUDMA Journal of Accounting and Finance Research [FUJAFR]*, *2*(3), 63–72. https://doi.org/10.33003/fujafr-2024.v2i3.109.63-72

Tagang, J. D., Ahmed, A., I. Ningi, S., & Shittu, I. O. (2024). An Assessment of Information Management Practices and the Containment of Financial Crimes in Nigeria. *FUDMA Journal of Accounting and Finance Research [FUJAFR]*, *2*(4), 82–90. https://doi.org/10.33003/fujafr-2024.v2i4.143.82-90

Chukwuma, O. E., Abdulkarim, S. A., & Abdullahi, M. A. (2025). Corporate Governance Attributes and the Likelihood of Fraud on Financial Statements of Listed Deposit Money Banks in Nigeria . *FUDMA Journal of Accounting and Finance Research [FUJAFR]*, *3*(2), 138–153. https://doi.org/10.33003/fujafr-2025.v3i2.174.138-153

Hanafiah, M. H. (2020). Formative vs. reflective measurement model: Guidelines for structural equation modeling research. *International Journal of Analysis and Applications*, *18*(5), 876-889. https://doi.org/10.28924/2291-8639

Yan, C., Siddik, A. B., Yong, L., Dong, Q., Zheng, G. W., & Rahman, M. N. (2022). A two-staged SEM-artificial neural network approach to analyze the impact of FinTech adoption on the sustainability performance of banking firms: the mediating effect of green finance and innovation. *Systems*, *10*(5), 148. https://doi.org/10.3390/systems10050148

Xu, S., Wang, Y., & Luo, W. (2024). Hybrid SEM-ANN model for predicting undergraduates'e-learning continuance intention based on perceived educational and emotional support. *PloS one, 19*(12), e0308630. https://doi.org/10.1371/journal.pone.0308630

Appendix
RESEARCH QUESTIONNAIRE

Instruction: Please tick as appropriate

SECTION A: Demographic Information

Please tick (✓) the most appropriate option.

1. Gender:

☐ Male ☐ Female

2. Age:

☐ Less than 30 years ☐ 30–39 years ☐ 40–49 years ☐ 50 years and above

3. Educational Qualification:

☐ ND/HND ☐ B.Sc./B.A. ☐ M.Sc./MBA ☐ PhD ☐ Others (specify): ___________

4. Current Position:

☐ Officer ☐ Senior Officer ☐ Manager ☐ Executive/Director

5. Department/Unit:

☐ Internal Audit ☐ ICT ☐ Risk Management ☐ Finance/Accounting ☐ Others: ___________

SECTION B: Network Forensics

Please indicate your level of agreement with each statement using the following scale:

1 - Strongly Disagree, 2 – Disagree, 3 – Neutral, 4 – Agree, 5 - Strongly Agree

S/N	Statements	5	4	3	2	1
1	Network forensics provides real-time alerts for potentially fraudulent activities					
2	The evidence gathered through network forensics is reliable and useful for legal proceedings					
3	The organization provides sufficient training on network forensic tools and techniques					
4	The integration of network forensics with other security tools improves the detection of fraud					
5	Network forensics has reduced the occurrence of fraud incidents in the organization					

SECTION C: Cloud Computing Forensics

S/N	Statements	5	4	3	2	1
1	We can detect tampering of cloud forensic evidence					
2	We can recover deleted data from cloud environments					
3	We maintain data integrity during cloud forensic investigations					
4	Cloud forensics enables better tracking of digital evidence in fraud cases					
5	We effectively identify and collect relevant data across different cloud service models					

SECTION D: Mobile Device Forensics

S/N	Statements	5	4	3	2	1
1	Implementation of mobile forensics has improved our fraud detection success rate					
2	The organization has sufficient expertise to utilize mobile forensics effectively					
3	Privacy regulations are effectively addressed in mobile forensics procedures					
4	Mobile device forensics helps identify patterns and connections in complex fraud schemes					
5	Digital evidence recovered through mobile forensics is reliable for fraud case prosecution					

SECTION E: Internet of Things (IoT) Forensics

S/N	Statements	5	4	3	2	1
1	Our forensic tools can effectively collect data from diverse IoT devices					
2	We can effectively analyze encrypted IoT communications					
3	Staff can effectively utilize IoT forensics for fraud detection					
4	Our IoT forensic procedures protect user privacy					
5	IoT forensics has improved our fraud detection success rate					

SECTION F: Fraud Detection

S/N	Statements	5	4	3	2	1
1	We can quickly respond to identified fraud attempts					
2	Our tools can detect new and emerging fraud patterns					
3	Our automated alert systems effectively flag potential fraud cases					
4	Fraudulent activities are detected in real-time and with minimal delay					
5	Our fraud detection systems effectively identify suspicious activities					