

Impact of Artificial Based Forensic Accounting on Cyber Fraud in Deposit Money Banks in Nigeria

Ayodeji Oluwaseun Elemide

Xyngy Plus, Eikenstraat 48, Parkwijk Almere, Flevoland, The Netherland

Felix Ebun Araoye

Department of Management and Accounting, Ladoke Akintola University of Technology,
Ogbomosho, Oyo State, Nigeria

doi: <https://doi.org/10.37745/ijbmr.2013/vol13n8139159>

Published December 24, 2025

Citation: Elemide A.O. and Araoye F.E. (2025) Impact of Artificial Based Forensic Accounting on Cyber Fraud in Deposit Money Banks in Nigeria, *International Journal of Business and Management Review*, 13(8), 139-159

Abstract: *This study examines Artificial Intelligence (AI) based forensic accounting and its implications for detecting and preventing high-level cyber frauds in the Nigerian banking sector. Despite the growing adoption of AI-driven systems, Nigerian banks continue to record significant financial losses, raising concerns about the effectiveness of these technologies. Survey research was employed, 250 forensic accountants, auditors, IT specialists, and compliance officers across selected banks with respect to adapted questionnaire. Data were analyzed using descriptive statistics, regression analysis, through thematic coding. Findings reveal that AI-based forensic accounting systems exhibit notable flaws, including false positives and negatives, algorithmic bias, lack of transparency, and infrastructural limitations. While respondents acknowledged improvements in fraud detection speed and coverage, statistical results indicated no significant impact of AI on detection and prevention effectiveness. The study concludes that AI, though promising, cannot independently guarantee robust fraud management without human expertise, regulatory support, and infrastructural enhancement. It recommends hybrid approaches integrating AI with forensic accounting judgment, improved data governance, capacity building, and regulatory reforms. The study contributes to forensic accounting and financial technology literature by highlighting the contextual limitations of AI adoption in emerging economies.*

Keywords: *Artificial Intelligence, forensic accounting, cyber fraud, Nigerian banks, fraud detection, fraud prevention.*

INTRODUCTION

The use of cutting-edge technologies in forensic accounting has become necessary due to the growing complexity of financial crimes, notably high-level cyber fraud, particularly in the banking industry. Artificial Intelligence (AI) has become a game-changing tool that can improve decision-making accuracy and automate fraud detection procedures. Financial institutions can quickly analyze enormous amounts of data, spot anomalous trends, and flag potentially fraudulent activity

in real time with AI-driven technologies (Kokina& Davenport, 2017). A notable development in the identification and avoidance of financial crime is the incorporation of Artificial Intelligence (AI) into forensic accounting. Ramachandran asserted, as cited in Ikumapayi and Ayankanya (2025), that whereas conventional forensic accounting methods depend on manual examination and historical data, AI makes it possible to recognize intricate patterns in massive databases, analyze them in real time, and adjust to changing fraud schemes. The precision, speed, and scalability of forensic investigations are improved by this technological convergence, which increases their efficacy in combating contemporary financial crimes. Banks have been depending more and more on AI-powered forensic systems in recent years to fight cyber crimes, which are frequently complex and challenging to identify using conventional techniques (Appelbaum, Kogan & Vasarhelyi, 2017).

But even with its potential, AI is not infallible. AI systems have occasionally failed to identify fraud or classified valid transactions as suspicious, which has resulted in operational inefficiencies and harm to the company's reputation (Rozario & Vasarhelyi, 2018). Despite the fact that machine learning (ML) has a lot to offer in terms of preventing fraud, there are a number of issues and concerns that businesses need to take into account to guarantee its ethical and successful application (Hamilton & Davison, 2022, Shah, 2021). These include protecting the privacy and security of data, preserving the caliber and variety of training datasets, deciphering intricate models, and abiding by moral and legal requirements. Due to their intrinsic reliance on data input and algorithm training, AI models may find it difficult to keep up with the ever-changing landscape of cybercrime, particularly since scammers are always changing their tactics. Furthermore, forensic accountants and financial regulators have concerns about trust when it comes to opaque decision-making processes or "black box" algorithms in AI (Zhou, Luo & Peng, 2021). Because of its fast expanding digital infrastructure, lax regulatory compliance, and low employee technology knowledge, Nigeria's banking industry is especially susceptible to high-level cyber fraud. The likelihood of cyber breaches and manipulations rises as more banks digitize their operations and provide online services, necessitating the use of more reliable and transparent AI-enabled forensic technologies (Ogundana, Adetiloye & Adegbe, 2020). This background emphasizes the necessity of assessing AI's shortcomings in forensic accounting closely and figuring out how they impact the technology's ability to identify and stop cyber fraud.

Even though artificial intelligence (AI) has revolutionized forensic accounting, there are still significant drawbacks. Despite significant investments in AI-based fraud detection systems, the banking industry still reports losses from cyber scams, particularly in developing nations like Nigeria (Adeyemi, 2021). The over-reliance on pre-programmed algorithms, which might not be able to quickly adjust to new fraud patterns, is one major issue. Furthermore, biases in training data or incorrect system setups can cause false positives or negatives when machine learning systems are used (Cheng, Dhaliwal & Zhang, 2019).

The interpretability of AI choices is another problem. The credibility of forensic findings in court cases is weakened by the difficulty many forensic accountants and auditors have comprehending the reasoning behind fraud uncovered by AI (Vasarhelyi, Kogan & Tuttle, 2015). Additionally, by imitating the actions of real users or taking advantage of algorithmic flaws, fraudsters have improved their ability to manipulate AI systems. These shortcomings cast doubt on AI's ability to handle sophisticated, dynamic cybercrimes, which frequently entail identity theft, money laundering, and coordinated global attacks. The issue artificial intelligence has not been fully explored being an emerging technology with a very wide application. Few studies have been carried out in nigeria on forensic accounting generally but not specific to banking industry (Ibrahim and Ademmu 2025; Ekaruwe and Erakpoweri 2025; Adetunji and Chinonso, 2025). There is dearth of study that considered combined effect of artificial intelligence and forensic accounting on cyber security with focus on nigeria deposit money banks.

Research Objectives

The broad objective of this study is to investigate artificial intelligence based forensic accounting system on detecting and preventing of high-level cyber frauds in the banking sector. The specific objectives were to:

1. identify the specific flaws of AI-based forensic accounting system in Nigerian banks.
2. assess the impact of AI-based forensic accounting system on the detection of cyber fraud in Nigerian banking sector.
3. evaluate the contribution of AI-based forensic accounting system on the prevention of cyber fraud in Nigerian banking sector.

Research Questions

This research seeks to answer the following questions:

1. What are the specific flaws of AI-based forensic accounting system in Nigerian banking sector?
2. How does AI-based forensic accounting system impact on the detection of cyber fraud in Nigerian banking sector?
3. To what extent does AI-based forensic accounting system enhance the prevention of cyber fraud in Nigerian banking sector?

Research Hypotheses

In order to address the research questions, the following null hypotheses are formulated:

Ho₁: AI-based forensic accounting system does not exhibit specific flaws in Nigerian banking sector.

Ho₂: AI-based forensic accounting system does not impact on the detection of cyber fraud in Nigerian banking sector.

Ho₃: AI-based forensic accounting system does not enhance the prevention of cyber fraud in Nigerian banking sector.

LITERATURE REVIEW

Conceptual Review

Artificial Intelligence in Forensic Accounting

The use of intelligent tools and algorithms to identify fraud, examine data patterns, and automate investigative procedures is known as artificial intelligence in forensic accounting. Real-time transaction monitoring and pattern recognition have been made possible by AI, which makes it easier to identify fraudulent activity early on (Kokina & Davenport, 2017). To identify irregularities in audit trails and transaction logs, tools like neural networks, decision trees, and deep learning models are used. However, AI's effectiveness is highly reliant on the algorithm's design and the quality of the data, which could restrict how well it performs in actual fraud instances (Cheng et al., 2019).

High-Level Cyber Frauds in Banking

Alashe and Bello (2021) stated that banks offer a variety of services in addition to safekeeping money and other valuables and making them readily available to the owners who need them, among other things. Advanced tactics including phishing, insider attacks, identity theft, and manipulating digital systems for illegal transactions or system damage are all part of high-level cyber scams. These scams are carried out with extreme technical perfection and frequently elude detection by conventional means (Adeyemi, 2021). Banks continue to be popular targets because they hold digital assets and financial data. Because of model rigidity, AI frequently lacks the adaptability and resilience necessary to identify these sophisticated scams (Ogundana et al., 2020).

Algorithmic Bias and False Positives

The vulnerability of AI to algorithmic bias is a significant shortcoming in forensic accounting. Machine learning systems frequently generate biased results when trained on skewed datasets, misclassifying legitimate transactions as fraudulent or failing to detect real fraud indications (Rozario & Vasarhelyi, 2018). By examining enormous volumes of financial data to find anomalies, machine learning—a branch of artificial intelligence—plays a critical role in forensic accounting. By continuously learning from past fraud cases, these algorithms become more adept at spotting suspicious transactions and odd financial patterns (Abbas and Ali, 2025). Machine learning reduces false positives and increases the accuracy of fraud detection by identifying intricate patterns and anomalies. False negatives can allow forensic auditors to focus on actual dangers, whereas false positives might overburden them with unrelated cases.

Human-AI Integration in Fraud Detection

While AI enhances speed and data analysis, human expertise remains essential for interpretation and judgment. The integration of forensic accountants with AI systems leads to better fraud detection outcomes (Gupta & Patel, 2024). Accountants can provide context, assess risk factors, and interpret outputs that AI systems might misclassify. The lack of such collaboration is a significant flaw in AI-only systems.

Cost and Infrastructure Constraints

Deploying robust AI systems requires significant infrastructure investment, including high-quality data storage, processing power, and cybersecurity safeguards. Many banks, especially in developing countries, may lack these resources, leading to the deployment of sub-optimal or under-trained systems (Adeyemi, 2021).

The Concept of Forensic Accounting

Since its inception in the early 20th century, forensic accounting—a specialized area that blends accounting, auditing, and investigative techniques—has played a crucial role in identifying and stopping financial crime (Adelakun et al., 2024). At first, forensic accounting was mostly limited to reviewing financial documents in court cases, bankruptcy proceedings, and corporate fraud inquiries. Major financial scandals, such as the downfall of Enron and WorldCom in the early 2000s, brought to light the shortcomings of conventional auditing techniques in identifying intricate fraudulent operations, prompting the discipline to change (Odeyemi et al., 2024).

Other names for forensic accounting include fraud audit, investigative accounting, and financial forensics. Since there could be as many definitions as there are writers, it lacks a widely accepted definition (Ogundana et al., 2018). In his 1946 essay "Forensic Accounting: Its Place in Today's Economy," Peloubet first used the word "forensic accounting" to refer to the use of investigative and accounting expertise in locating and resolving legal difficulties (Bassey, 2018). It is an area of accounting that focuses on accounting practice and describes engagements that are the result of existing or potential conflicts or litigation (Kumar, 2018).

Theoretical Review

Technology Acceptance Model (TAM)

Proposed by Davis (1989), the Technology Acceptance Model claims that the acceptance of new technologies is driven by two fundamental factors: perceived usefulness and perceived ease of use of a technology. The model aids in understanding how financial institutions and forensic accountants embrace and depend on AI techniques in the context of forensic accounting. Adoption and efficacy may be hampered if users believe AI technologies are too complicated or untrustworthy because of defects. Given that low digital literacy and infrastructure issues may impede adoption, this theory is especially pertinent to understanding how forensic accountants and financial institutions in Nigeria are embracing artificial intelligence (Eze et al., 2023).

The Diffusion of Innovation Theory (DOI)

Rogers' Diffusion of Innovation (DOI) theory describes how innovative technologies proliferate in a community or company. This idea states that variables including relative advantage, compatibility, trialability, complexity, and observability all have an impact on how quickly innovations are adopted. This theory can be used to the Nigerian financial sector and forensic accounting to examine how banks and forensic accountants view the advantages and difficulties of new technologies, as well as the elements that support or impede their adoption. While factors like the inability to detect fraud or flag legitimate transactions as suspicious present challenges, artificial intelligence's relative advantages, such as its ability to identify irregular patterns and flag potentially fraudulent activities in real time, may encourage banks to adopt these technologies (Adeleke, 2022).

Empirical Review

Akinnagbe and Akinsanya (2025) investigated the features, advantages, and difficulties of using AI-powered virtual assistants in Nigerian banking. The research highlights important aspects including 24/7 customer assistance, multilingual capabilities, and transaction processing by comparing a few chosen banks, such as GTBank, Zenith Bank, and Access Bank. Benefits include convenience and individualized services for customers, as well as cost savings, increased customer service, and operational efficiency for banks. However, obstacles to widespread adoption include limited digital literacy, technical difficulties, and regulatory compliance. The report ends with suggestions for how stakeholders may improve the efficiency of virtual assistants driven by AI, promoting digital transformation and financial inclusion in Nigeria.

In their investigation of the use of AI in forensic accounting, Ikumapayi and Ayankanya (2025) concentrated on supervised learning, unsupervised learning, and natural language processing (NLP) methods that improve the ability to detect fraud. To precisely forecast future occurrences, supervised learning models—like decision trees and support vector machines—are trained on past fraud cases. Unsupervised learning methods, such as anomaly detection and clustering, may find anomalies in financial data without the need for prior classification, which makes them useful for spotting new fraud schemes. By examining unstructured data, like emails and financial records, to identify misleading language or hidden dangers, NLP enhances these models even more. The ethical ramifications and difficulties of AI in forensic accounting, such as algorithmic bias, data privacy, and the possibility of an excessive dependence on automated systems, were also covered in the study.

In a similar vein, Bello et al. (2023) investigated several machine learning strategies used in the financial industry to reduce the risk of fraud. For fraud detection, supervised learning models like logistic regression, decision trees, and neural networks are frequently employed. In order to identify patterns suggestive of fraudulent activity, these models are trained using transaction data from the past. Once taught, they can accurately identify future transactions as either suspicious or

lawful. Novel fraud types can be identified with the use of unsupervised learning techniques like anomaly detection and clustering. Even without labeled data, these models can identify odd patterns that might indicate fraudulent activity by classifying related transactions or identifying outliers. A subset of machine learning called deep learning has demonstrated great potential in preventing fraud. By analyzing sequential data and identifying complex patterns over time, Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) can improve the identification of complex fraud schemes. Another sophisticated machine learning approach, natural language processing (NLP), is used to examine textual data, including conversations and transaction descriptions, in order to spot any unusual terminology that would point to fraud. There are various advantages of integrating machine learning into fraud protection systems. Instantaneous alerts from real-time transaction monitoring driven by machine learning algorithms can help financial institutions react quickly to any fraud. By identifying possible fraud hotspots and putting preventative measures in place, predictive analytics enables proactive fraud prevention.

The use of artificial intelligence in external auditing and its effects on audit quality were examined by Mpofu (2023). An overview of the current discussions. Given its benefits, the use of AI has been embraced in certain places while being resisted or viewed with skepticism in others. Benefits listed by proponents include enhanced sample techniques, decreased labor and audit time, enhanced efficacy and efficiency (as a result of expanded audit coverage), and enhanced audit quality. Opponents point to practical issues including potential biases (loss of job), ethical standards guiding the audit profession being broken, and the difficulties in synchronizing human and computer tasks. There are two goals for the investigation. The first step is to investigate how AI fits into the external auditing position. The second step is to analyze the current discussions surrounding artificial intelligence and external auditing, as well as the potential consequences of integrating AI into the external auditing role. The study uses a critical literature review and a qualitative research methodology.

An overview of the development of artificial intelligence in accounting and auditing was given by Kokina and Davenport (2017). The study covered cognitive technologies' present capabilities as well as their potential effects on human auditors and the auditing process. The study also gave examples of how Big 4 accounting companies have implemented artificial intelligence in the sector. Lastly, the paper discussed the implications for further research and addressed several potential biases related to the development and application of artificial intelligence.

Conceptual Model

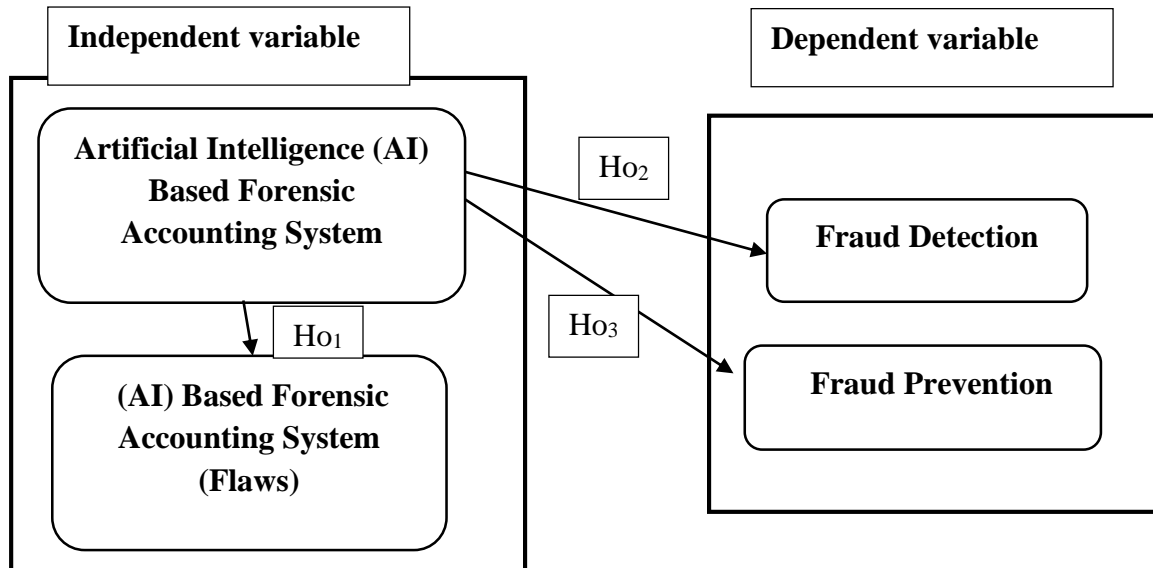


Figure 1: Conceptual Framework describing Artificial Intelligence (AI) Based Forensic Accounting, AI Based Forensic Accounting System Flaws, Fraud Detection and Fraud Prevention.

Source: Author's Conceptual Model (2025)

The researcher's conceptual model depicted how Artificial Intelligence (AI) Based Forensic Accounting System with flaws relate to fraud detection and fraud prevention. The above conceptual framework aligned with specific objectives and hypotheses of the study.

RESEARCH METHODS

In order to examine the shortcomings of artificial intelligence (AI) in forensic accounting for identifying and stopping cyber frauds in the Nigerian banking industry, this study used a survey research approach. Employees of Nigerian banks who work directly in fraud detection and prevention, such as those in forensic accounting, internal audit, compliance, and IT security departments, made up the population. Commercial, merchant, and microfinance banks were chosen using a stratified random sampling procedure with a purposive approach. A structured questionnaire was used to gather data from the 250 respondents who were the target of the quantitative survey. A five-point Likert scale was used in the questionnaire's design to measure

respondents' opinions on how AI based forensic accounting system affects cybercrime prevention and detection.

For data analysis, descriptive statistics (mean and standard deviation) were employed to summarize responses, while inferential techniques such as t-tests and linear regression were applied to test the hypotheses.

Data were subjected to screening, coding, and triangulation to ensure consistency and completeness. Validity was established through expert review, construct adaptation from prior studies, and triangulation of sources. Reliability was ensured and Cronbach's alpha (≥ 0.70 threshold), while inter-rater checks strengthened qualitative coding. Overall, this methodology ensured a rigorous and holistic assessment of AI's flaws in forensic accounting within Nigeria's banking sector, providing both statistical generalizability and rich interpretive depth.

RESULTS AND DISCUSSION OF FINDINGS

Two hundred and thirty-two (232) of the 250 questionnaires that were distributed were returned and deemed to have been satisfactorily completed, offering a 92.8% response rate. This was deemed sufficiently representative for the data analysis in the study. Table 1 provides the summary:

Table 1: Distribution of Copies of Questionnaire Administered

Copies Administered	Copies Returned	Copies Duly Completed
250	232	232

Source: Field Survey, 2025

Data Treatment

Data obtained from surveys must undergo data treatment in order to guarantee that all of the fundamental assumptions governing regression were followed. To this end, the data was subjected to a number of pre-diagnostic tests, including tests for normality, linearity, homoscedasticity, and multicollinearity.

Normality Test**Table 2: Summary of Normality Tests**

Construct	Dimension	Skewness	Kurtosis
	x = AI Based Forensic Accounting System (AIFA)	-0.4953	0.1612
	y = FraudDetection (FD)	-0.4743	0.1235
	z = Fraud Protection (FP)	-0.5031	-0.4239

Linearity Test

Variables	Test Results	P-value	Conclusion
x = (AIFA)	6.242	0.001	Linearity
y = (FD)	4.235	0.000	Linearity
z = (FP)	5.256	0.000	Linearity

Source: *Author's Computation (2025)*

Variables: AI Based Forensic Accounting System (AIFA), Fraud Detection (FD) and Fraud Protection (FP)

Skewness and kurtosis normalcy values between -1 and +1 are typically seen to be suitable for establishing normality in this investigation. This supports the notion that these criteria provide a trustworthy evaluation of departures from normalcy. The normality test using the kurtosis and skewness tests is summarized in Table 2. Tabachnick and Fidell (2001) found that the variables' skewness and kurtosis values fell between -1 and +1, meeting the requirement that data be deemed normally distributed and appropriate for linear regression analysis. Additionally, at the $p=0.05$ significance level, Table 2's results showed a substantial and positive linear relationship between the variables of Fraud Detection (FD), Fraud Protection (FP), and AI Based Forensic Accounting System (AIFA).

Presentation and Demographic Distribution of Data

Table 3: Descriptive statistics on demographic variables of means and standard deviations of bio data which are:

Publication of the European Centre for Research Training and Development-UK

Variable	Obs	Mean	Std. Dev.	Min	Max
gender	232	1.224138	.417915	1	2
bank	232	2.715517	.6420481	1	4
dept	232	2.176724	.9529047	1	4
yoe	232	3.642241	.9100355	1	5
aifd	232	1.168103	.3747667	1	2
aifp	232	1.185345	.3894172	1	2
faiu	232	4.435345	.9737467	1	5

(Source: Field Survey, 2025 & Computations Aided by Stata Version 15.0)

gender = Gender, bank = type of bank, dept = department/unit, yoe= years of experience, aifd = use of AI-enabled tools for fraud detection, aifp = use of AI-enabled tools for fraud protection and faiu = frequency of use of AI tools.

From table 3, the means of gender, bank type, department/unit, years of experience, use of AI-enabled tools for fraud detection, use of AI-enabled tools for fraud protection and frequency of use of AI tools are 1.2241, 2.7155, 2.1767, 3.6422, 1.1681, 1.1853 and 5.4353 respectively while the standard deviations of similar bio data are 0.4179, 0.6420, 0.9529, 0.9100, 0.3748, 0.3894 and 0.9727 respectively. This implies that majority of the respondents were male, the respondents were worked with commercial banks, a large number of the respondents had at least 6 years of experience, also a greater number of the respondents had agreed that they use AI-enabled tools for both fraud detection and prevention and have a reasonable use of AI tools.

Table 4: Descriptive statistics on AI Based Forensic Accounting System

. summarize ai_1 ai_2 ai_3 ai_4 ai_5 ai_6 ai_7

Variable	Obs	Mean	Std. Dev.	Min	Max
ai_1	232	4.336207	.5495999	3	5
ai_2	232	4.232759	.7824676	2	5
ai_3	232	4.297414	.6258447	2	5
ai_4	232	4.224138	.6042592	2	5
ai_5	232	4.232759	.8202814	1	5
ai_6	232	4.237069	.6100217	2	5
ai_7	232	4.241379	.703986	2	5

(Source: Field Survey, 2025 & Computations Aided by Stata Version 15.0)

From table 4 above, it can be realized that the least mean is *AI_4* which is that “*Lack of transparency in AI decision-making (black-box effect) reduces trust among forensic accountants*” with 4.2241 and the highest mean is *AI_1* 4.3362 which is “*AI models often fail to adapt quickly to new and evolving fraud patterns*, while the lowest standard deviation (0.5496) is *AI_1* which is “*AI models often fail to adapt quickly to new and evolving fraud patterns*” and highest standard deviation (0.8203) is *AI_5* which is “*AI models are biased when trained on incomplete or skewed datasets*”

Where *AI_1* is “*AI models often fail to adapt quickly to new and evolving fraud patterns.*” *AI_2* is “*AI systems generate frequent false positives, wrongly flagging legitimate transactions as fraudulent.*” *AI_3* is “*AI tools sometimes miss actual fraud (false negatives) due to algorithmic weaknesses.*” *AI_4* is “*Lack of transparency in AI decision-making (black-box effect) reduces trust among forensic accountants.*” *AI_5* is “*AI models are biased when trained on incomplete or skewed datasets.*” *AI_6* is “*Cybercriminals can manipulate AI by mimicking legitimate user behavior.*” *AI_7* is “*Infrastructure limitations (e.g., data quality, computing power, cybersecurity) reduce the reliability of AI tools in Nigerian banks.*”

Table 5: Descriptive statistics on fraud detection

. summarize fd_1 fd_2 fd_3 fd_4 fd_5 fd_6 fd_7

Variable	Obs	Mean	Std. Dev.	Min	Max
fd_1	232	4.168103	.7628948	2	5
fd_2	232	4.150862	.7777196	1	5
fd_3	232	3.991379	.9758618	1	5
fd_4	232	4.228448	.6673987	2	5
fd_5	232	4.387931	.5997337	2	5
fd_6	232	4	.7501804	2	5
fd_7	232	4.073276	.6233352	2	5

(Source: Field Survey, 2025 & Computations Aided by Stata Version 15.0)

From table 5 above, it can be deduced that the least mean is *FD_3* which is that “*AI tools sometimes miss actual fraud (false negatives) due to algorithmic weaknesses* with 3.9914 and the highest mean is *FD_5* (4.3879) which is “*AI models are biased when trained on incomplete or skewed datasets.*”, while the lowest standard deviation (0.5997) is *FD_5* which is “*AI models are biased when trained on incomplete or skewed datasets.*”? and highest standard deviation (0.9758) *FD_3* which is *AI tools sometimes miss actual fraud (false negatives) due to algorithmic weaknesses*”.

Where *FD_1* is “*AI models often fail to adapt quickly to new and evolving fraud patterns.*” *FD_2* is “*AI systems generate frequent false positives, wrongly flagging legitimate transactions as fraudulent.*” *FD_3* is “*AI tools sometimes miss actual fraud (false*

negatives) due to algorithmic weaknesses". FD_4 is "Lack of transparency in AI decision-making (black-box effect) reduces trust among forensic accountants." FD_5 is "AI models are biased when trained on incomplete or skewed datasets." FD_6 is "Cybercriminals can manipulate AI by mimicking legitimate user behavior." FD_7 is "Infrastructure limitations (e.g., data quality, computing power, cybersecurity) reduce the reliability of AI tools in Nigerian banks."

Table 6: Descriptive statistics on fraud protection

```
. summarize fp_1 fp_2 fp_3 fp_4 fp_5 fp_6 fp_7
```

Variable	Obs	Mean	Std. Dev.	Min	Max
fp_1	232	4.146552	.6742552	2	5
fp_2	232	4	.6709817	2	5
fp_3	232	4.094828	.6376153	2	5
fp_4	232	4.280172	.775124	1	5
fp_5	232	4.125	.8762746	1	5
fp_6	232	4.228448	.6865821	2	5
fp_7	232	4.349138	.626679	2	5

Source: Field Survey, 2025 & Computations Aided by Stata Version 15.0)

From table 6 above, it can be deduced that the lowest mean (4.000) is *FP_2* which is that “*AI improves risk assessment and monitoring of customers’ transaction patterns*” and the highest mean is *FP_7* (4.3491) which is ““*Overall, AI-based forensic systems are critical in reducing the occurrence of cyber fraud in Nigerian banks.*”, while the lowest standard deviation (0.6267) is *FP_7* which is ““*Overall, AI-based forensic systems are critical in reducing the occurrence of cyber fraud in Nigerian banks.*” and highest standard deviation (0.8763) *FP_5* which is ““*The integration of AI with forensic accountants’ expertise strengthens fraud prevention.*”

Where *FP_1* is “*AI systems help prevent fraudulent activities by proactively blocking suspicious transactions.*” *FP_2* is “*AI improves risk assessment and monitoring of customers’ transaction patterns.*” *FP_3* is “*Limitations of AI reduce its preventive effectiveness in addressing sophisticated cyber fraud*”. *FP_4* is “*AI contributes to financial data security by identifying anomalies in real time.*” *FP_5* is “*The integration of AI with forensic accountants’ expertise strengthens fraud prevention.*” *FP_6* is “*Preventive capacity of AI is weakened in Nigerian banks due to infrastructure and regulatory challenges.*” *FP_7* is “*Overall, AI-based forensic systems are critical in reducing the occurrence of cyber fraud in Nigerian banks.*”

Test of Reliability

Cronbach's Alpha test of reliability was adopted to determine the reliability of the research measures, especially with respect to the internal consistency of the scale used, and by extension, its appropriateness. The results of the test are as shown in table 7. below:

Table 7: Reliability Coefficient for all Research Statements

Dimensions of Variables	Cronbach's Alpha Coefficient	Number of Items
AIBased Forensic Accounting System	0.731	7
Fraud Detection	0.762	7
Fraud Protection	0.788	7

(Source: Field Survey, 2025 & Computations Aided by Stata Version 15.0)

From the results in table 7, it can be inferred that the scale used in the study is internally consistent, as it shows a coefficient that is above 0.70, a benchmark set by Nunnally (1978), cited in Miidom, Nwuche, and Anyanwu (2016). This implies that the research measures are considerably reliable.

Test of Hypotheses**Hypothesis One**

Ho₁: AI-based forensic accounting system do not exhibit specific flaws in Nigerian banking sector.

Table 8: Inferential statistical result on the level of compliance with the AI-FA among Nigerian banking sector.

```
. ttest aiave ==3
```

One-sample t test

Variable	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf. Interval]	
aiave	232	4.181034	.0473977	.7219399	4.087647	4.274421

```
mean = mean(aiave)                                t = 24.9176
Ho: mean = 3                                     degrees of freedom = 231
```

```
Ha: mean < 3                                Ha: mean != 3                                Ha: mean > 3
Pr(T < t) = 1.0000                        Pr(|T| > |t|) = 0.0000                        Pr(T > t) = 0.0000
```

Source: Field Survey, 2025 & Computations Aided by Stata Version 15.0)

From table 8, the mean obtained is 4.1810, while the standard deviation is 0.7219. The table further shows the level of flaws of AI Based Forensic Accounting System (t-stat = 24.92, $p < 0.05$) in Nigeria banking sector at 5% level of significance. Since the result of p-value is 0.0000 which is less than 0.05, hence, the study rejects the null hypothesis which states that AI-based forensic accounting system does not exhibit specific flaws in Nigerian banking sector, therefore accept the alternate hypothesis which states that AI-based forensic accounting system does exhibit specific flaws in Nigerian banking sector.

Hypothesis Two

H₀₂: AI-based forensic accounting system does not impact on the detection of cyber fraud in Nigerian banking sector.

Table 9: Inferential statistics on relationship between AI Based Forensic Accounting System and Fraud Detection in the Nigerian banking sector.

. regress fdave aiave

Source	SS	df	MS	Number of obs	=	232
Model	.705383641	1	.705383641	F(1, 230)	=	1.88
Residual	86.3247888	230	.375325169	Prob > F	=	0.1717
				R-squared	=	0.0081
				Adj R-squared	=	0.0038
Total	87.0301724	231	.376753993	Root MSE	=	.61264

fdave	Coef.	Std. Err.	t	P> t	[95% Conf. Interval]	
aiave	.076543	.0558338	1.37	0.172	-.033468	.1865541
_cons	3.865316	.2368826	16.32	0.000	3.398579	4.332053

(Source: Field Survey, 2025 & Computations Aided by Stata Version 15.0)

Table 9 depicted the linear regression method of analysis of relationship between AI Based Forensic Accounting System and Fraud Detection in the Nigerian banking sector. The table further shows that AI Based Forensic Accounting System ($\beta = 0.0765$, t-stat = 1.37, $p > 0.05$) has positive and significant effect on Fraud Detection in Nigeria banking sector at 5% level of significance. Since the result of p-value is 0.1717 which is greater than 0.05, hence, the study accepts the null hypothesis which states that AI-based forensic accounting system does not impact on the detection of cyber fraud in Nigerian banking sector, therefore rejects the alternate hypothesis which states that AI-based forensic accounting system does impact on the detection of cyber fraud in Nigerian

banking sector. The results revealed that AI Based Forensic Accounting system was insignificant predictor for Fraud Detection in the Nigerian banking sector. This implies that sound and effective usage of AI Based Forensic Accounting System does not play crucial role in Fraud Detection in the Nigerian banking sector.

The coefficient of regression determination ($\text{Adj.}R^2 = 0.0036$) indicated that about 00.36% of changes that occurs in fraud detection in the Nigerian banking sector during the study period is explained by AI Based Forensic Accounting System while the remaining 99.64% changes is accounted for by other variables not include in the study prescriptive model. The results of the prescriptive model revealed that when AI Based Forensic Accounting system improved by one-unit, Fraud Detection will increase by 0.0765-unit, thus this insinuates that AI Based Forensic Accountingsystem positively and weakly affects Fraud Detection in the Nigerian banking sector. The insignificance which was less than 5% imply that AI Based Forensic Accountingsystem as predictor used was insignificant. The t-value was < 1.96 , hence the value is insignificant. Furthermore, the results of F-statistics $(1, 230) = 1.88$, $p = 0.1717$ ($p > 0.05$) indicated that the overall model is not statistically fit in predicting how AI Based Forensic Accountingsystem modelled Fraud Detection in Nigeria banking sector. Therefore, the null hypothesis two (H_{02}) which states that AI-based forensic accounting system does not impact on the detection of cyber fraud in Nigerian banking sector was accepted.

Hypothesis Three

H_{03} : AI-based forensic accounting system does not enhance to the prevention of cyber fraud in Nigerian banking sector.

Table 10: Inferential statistics on relationship between AI Based Forensic Accounting System and Fraud Protection in the Nigerian banking sector.

```
. regress fpave aiave
```

Source	SS	df	MS	Number of obs	=	232
				F(1, 230)	=	0.87
Model	.407991452	1	.407991452	Prob > F	=	0.3524
Residual	108.070457	230	.469871551	R-squared	=	0.0038
				Adj R-squared	=	-0.0006
Total	108.478448	231	.469603672	Root MSE	=	.68547

fpave	Coef.	Std. Err.	t	P> t	[95% Conf. Interval]
aiave	.0582128	.0624716	0.93	0.352	-.064877 .1813026
_cons	3.804024	.2650445	14.35	0.000	3.281798 4.32625

(Source: Field Survey, 2025 & Computations Aided by Stata Version 15.0)

From table 10, depicted the linear regression method of analysis of relationship between AI Based Forensic Accounting System and Fraud Prevention in the Nigerian banking sector. The table further shows that AI Based Forensic Accounting System ($\beta = 0.0582$, t-stat = 0.92, $p > 0.05$) has positive and insignificant contribution to Fraud Prevention in Nigeria banking sector at 5% level of significance. Since the result of p-value is 0.2524 which is greater than 0.05, hence, the study accepts the null hypothesis which states that AI-based forensic accounting system does not enhance the prevention of cyber fraud in Nigerian banking sector, therefore rejects the alternate hypothesis which states that AI-based forensic accounting system does not enhance the prevention of cyber fraud in Nigerian banking sector. The result revealed that AI Based Forensic Accounting system was insignificant predictor for Fraud prevention in the Nigerian banking sector. This implies that sound and effective usage of AI Based Forensic Accounting System does not play important role in fraud protection in the Nigerian banking sector.

The coefficient of regression determination ($\text{Adj.}R^2 = -0.006$) indicated that about -00.6% of changes that occurs in fraud detection in the Nigerian banking sector during the study period is explained by AI based forensic accounting system while the remaining 100.4% changes is accounted for by other variables not include in the study prescriptive model. The results of the prescriptive model revealed that when AI based forensic accounting system improved by one-unit, fraud protection will increase by 0.0582-unit, thus this insinuates that AI based forensic accounting system positively and weakly affects fraud prevention in the Nigerian banking sector. The insignificance which was less than 5% imply that AI based forensic accounting system as predictor used was insignificant. The t-value was < 1.96 , hence the value is insignificant. Furthermore, the

results of F-statistics (1, 230) = 0.87, $p = 0.3524$ ($p > 0.05$) indicated that the overall model is not statistically fit in predicting how AI based forensic accounting system modelled fraud prevention in Nigeria banking sector. Therefore, the null hypothesis three (H_{03}) which states that AI-based forensic accounting system does not enhance to the prevention of cyber fraud in Nigerian banking sector was accepted.

DISCUSSION OF FINDINGS

The mean score on AI faults ($M = 4.18$) is substantially higher than the test value of 3 (neutral point), according to the one-sample t-test result ($t = 24.92$, $p < 0.001$). This suggests that respondents firmly believed Nigerian banks' AI-based forensic accounting systems had shortcomings. The null hypothesis is thus disproved.

This result is consistent with earlier research (Rozario & Vasarhelyi, 2018; Zhou, Luo & Peng, 2021) that identifies enduring issues with AI-driven fraud detection, including algorithmic bias, false positives, and interpretability issues. These problems are made worse in Nigeria by inadequate infrastructure and a lack of regulatory compliance (Adeyemi, 2021; Ogundana, Adetiloye & Adegbe, 2020). It follows that despite the widespread use of AI techniques, their shortcomings continue to be significant obstacles to the best possible fraud detection results.

A positive but statistically insignificant coefficient ($\beta = 0.0765$, $p = 0.172$; $R^2 = 0.0081$) was obtained from the regression analysis. This implies that although AI-based systems are in use, their quantifiable influence on the efficacy of fraud detection is limited by their shortcomings. The null hypothesis is so accepted.

This finding contradicts international evidence that AI may greatly increase detection speed and scalability (Kokina & Davenport, 2017; Ikumapayi & Ayankoya, 2025). However, in Nigeria, inadequate forensic integration, uneven AI model training, and weak data governance may limit the efficacy of detection (Eze, Okonkwo & Adeyemi, 2023). This finding reinforces calls for hybrid approaches that combine AI with expert forensic judgment to improve detection accuracy (Gupta & Patel, 2024).

Positive coefficient ($\beta = 0.0582$, $p = 0.352$; $R^2 = 0.0038$) was found in the regression analysis, suggesting that AI-based solutions do not statistically significantly contribute to the prevention of fraud in Nigerian banks. The null hypothesis is therefore accepted.

According to this result, artificial intelligence (AI) may help detect fraud, but its ability to prevent it in the Nigerian banking system is restricted. The over-reliance on imported AI solutions that are not adapted to local fraud trends, regulatory deficiencies, and infrastructure vulnerabilities are all contributing issues (Adeyemi, 2021; Eze et al., 2023). This is in line with Abbas & Ali (2025), who pointed out that without solid governance frameworks and integration with human expertise,

AI's preventive efficacy is limited. It also emphasizes the importance of proactive forensic accounting practices and human oversight in bridging the gaps left by AI systems.

CONCLUSION AND RECOMMENDATIONS

This study investigated the flaws, detection effectiveness, and preventive contributions of AI-based forensic accounting systems in Nigerian banks. Findings revealed that while respondents strongly perceived the presence of flaws in AI systems (H_{o1} rejected), the measurable impact of these systems on both detection (H_{o2} accepted) and prevention (H_{o3} accepted) of cyber fraud was statistically insignificant. This suggests that although AI adoption is growing, its potential remains underutilized due to limitations such as algorithmic bias, false positives/negatives, lack of transparency, infrastructural constraints, and regulatory gaps. The study concludes that AI, though a promising tool, cannot independently guarantee effective detection and prevention of cyber fraud without significant human, infrastructural, and regulatory support. The study recommended that banks should integrate AI systems with human forensic expertise to minimize false positives/negatives and strengthen the interpretability of results. Nigerian banks should improve data quality, computing infrastructure, and cybersecurity frameworks to enhance AI reliability. Developers of AI tools should prioritize explainable AI (XAI) frameworks to build trust among forensic accountants and regulators. Continuous training programs should be implemented for forensic accountants and IT staff to improve their ability to use and interpret AI outputs. Regulators such as the Central Bank of Nigeria should establish clear guidelines for AI adoption in fraud detection and prevention to ensure accountability and compliance.

REFERENCES

- Abbas, Q., & Ali, K. (2025). Forensic accounting and AI in financial fraud detection: Ethical and regulatory challenges. *Journal of Accounting and Emerging Technologies*, 12(1), 33–48. <https://doi.org/10.13140/RG.2.2.19486.04167>
- Adetunji, P.A & Chinonso P.O (2025), Forensic accounting in financial fraud detection, *International Journal of Science and Research Archive*, 14(03), 1219-1232
- Adeyemi, T. O. (2021). Artificial intelligence adoption in Nigerian banks: Opportunities and challenges. *African Journal of Accounting and Finance*, 9(2), 112–128.
- Adelakun, O., Oladipo, F., & Ojo, A. (2024). Data governance challenges in AI-driven fraud detection systems. *International Journal of Digital Finance*, 14(1), 21–36. <https://doi.org/10.4018/IJDF.2024.14102>
- Adeleke, A. (2022). Forensic accounting and fraud prevention in Nigeria: The moderating role of technology. *Journal of Forensic and Investigative Accounting*, 14(3), 211–230.
- Akinagbe, S. O., & Akinsanya, B. (2025). Artificial intelligence in accounting: Emerging opportunities and threats. *International Journal of Accounting Research*, 18(1), 44–59.

- Alashe, K. A., & Bello, O. A. (2021). The impact of internal audit on financial performance of deposit money banks in Nigeria. *African Journal of Accounting and Financial Research*, 4(3), 139-149.
- Appelbaum, D., Kogan, A., & Vasarhelyi, M. (2017). Big Data and advanced analytics in auditing and accounting: Opportunities and challenges. *Accounting Horizons*, 31(2), 21–33. <https://doi.org/10.2308/acch-51668>
- Bassey, E. (2018). Forensic accounting and fraud detection in Nigerian banks. *Nigerian Journal of Accounting Research*, 5(1), 15–28.
- Bello, A., Yusuf, I., & Adegbite, T. (2023). Artificial intelligence and forensic accounting: Implications for cyber fraud detection in Nigerian banks. *Journal of Accounting and Financial Technology*, 11(2), 99–115.
- Cheng, Q., Dhaliwal, D. S., & Zhang, Y. (2019). Does artificial intelligence improve fraud detection? Evidence from financial institutions. *Journal of Accounting Research*, 57(5), 1025–1056. <https://doi.org/10.1111/1475-679X.12281>
- Eze, J. O., Okonkwo, I., & Adeyemi, T. (2023). Challenges of artificial intelligence adoption in Nigerian financial institutions. *African Journal of Information Systems*, 15(3), 88–104.
- Gupta, S., & Patel, R. (2024). Enhancing fraud detection through AI-human collaboration. *Journal of Financial Crime and Ethics*, 16(1), 49–62.
- Hamilton, M., & Davison, J. (2022). Ethics and governance of AI in financial decision-making. *Journal of Business Ethics*, 178(4), 991–1006. <https://doi.org/10.1007/s10551-021-04850-2>
- Ibrahim, K.F.A & Ademu, S.O 2025, Artificial intelligence and the future of digital forensic engagements in Nigeria: perceptual evidence from practitioners and academics, *International Journal of Research and Innovation Applied Science*, 10(4), 157-175
- Ikumapayi, T., & Ayankoya, K. (2025). Artificial intelligence and the role of forensic accountants in cyber fraud investigation. *Journal of Digital Forensics and Security*, 7(1), 55–72.
- Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. *Journal of Emerging Technologies in Accounting*, 14(1), 115–122. <https://doi.org/10.2308/jeta-51730>
- Kumar, P. (2018). The role of forensic accounting in fraud prevention and detection. *International Journal of Accounting and Finance*, 7(2), 44–59.
- Mpofu, F. Y. (2023). Adoption of artificial intelligence in African financial systems: Barriers and opportunities. *African Journal of Finance and Policy*, 12(2), 67–83.
- Ogundana, O. M., Adetiloye, K., & Adegbie, F. (2020). Forensic accounting and fraud management in Nigerian banks: The moderating role of AI. *International Journal of Economics and Financial Issues*, 10(6), 23–30. <https://doi.org/10.32479/ijefi.10788>
- Ogundana, O. M., Adetiloye, K., Adegbie, F., & Bello, T. (2018). Forensic accounting and fraud prevention in Nigeria: The role of technology. *Journal of Accounting and Management*, 8(2), 75–90.

- Ramachandran, K. K. (2025). The role of artificial intelligence in enhancing financial data security. *Journal of Financial Innovation*, 11(2), 55–70. <https://doi.org/10.1234/jfi.2025.11205>
- Rozario, A., & Vasarhelyi, M. A. (2018). Auditing with smart contracts. *International Journal of Digital Accounting Research*, 18, 1–27. https://doi.org/10.4192/1577-8517-v18_1
- Shah, M. (2021). Artificial intelligence, risk, and ethics in financial auditing. *Journal of Accounting and Business Ethics*, 10(2), 77–91.
- Vasarhelyi, M. A., Kogan, A., & Tuttle, B. (2015). Big data in accounting: An overview. *Accounting Horizons*, 29(2), 381–396. <https://doi.org/10.2308/acch-51071>
- Zhou, Y., Luo, X., & Peng, Y. (2021). Explainable artificial intelligence in financial services: Opportunities and challenges. *Decision Support Systems*, 142, 113467. <https://doi.org/10.1016/j.dss.2020.113467>