MRS Journal of Multidisciplinary Research and Studies
*Abbreviate Title- MRS J Mul Res Stud*
ISSN *(Online) 3049-1398*
Vol-2, Iss-9(September-2025)

OPEN ACCESS

# EFFECT OF ARTIFICIAL INTELLIGENCE (AI) ON FRAUD PREVENTION OF LISTED DEPOSIT MONEY BANKS IN NIGERIA

**Musa, Success Jibrin[1*], Success Blessing Ejur[2], Ibrahim Karimu Moses[3], Success, Dominion Uchubiyojo[4] & Yusuf, Ismaila[5]**

[*1] Department of Accounting, Veritas University Abuja

[2] Department of Finance, Veritas University Abuja

[3] Department of Accounting, Confluence University of Science and Technology, Osara, Kogi

[4] Department of Computer Science, Phoenix University, Awada

[5] Department of Accounting, Federal University, Dutsin- Ma

***Corresponding Author*** **Musa, Success Jibrin** (Department of Accounting, Veritas University Abuja)

**Article History**: Received: 13 / 08 / 2025:, Accepted: 26 / 08 / 2025:, Published: 01 / 09 / 2025

**Abstract:** Fraud remains a significant challenge for the global financial sector, with substantial financial losses and eroded trust in banking systems. In Nigeria, Deposit Money Banks (DMBs) have been severely impacted by rising fraud activities, including identity theft, account takeovers, and cybercrimes. With the expansion of digital banking and online services, fraud has become more sophisticated, prompting the need for advanced fraud prevention methods. This study explores the effect of Artificial Intelligence (AI) on fraud prevention in Listed DMBs. This study adopts a survey research design, which is considered appropriate due to the nature of the research objectives and the methodology employed. A survey research design is particularly well-suited for collecting data from a large group of individuals to gain insights into their perceptions, experiences, and attitudes on a particular topic. The population for this study consists 100 Hundred of the staff and management of the 14 listed deposit money banks operating in Nigeria as of December 31, 2024. The regression analysis shows that ADS accounts for approximately 29.8% of the variation in FFP, indicating a strong and meaningful relationship between the two. As ADS improves, so does the effectiveness of fraud prevention, with each increase in ADS leading to a notable improvement in FFP. However, the model also suggests that there are other important factors contributing to FFP, as evidenced by the 70% of variability not explained by ADS alone. While ADS proves to be a valuable predictor, it is clear that a comprehensive fraud prevention strategy should integrate ADS with other methods, such as human oversight, user behavior analytics, and rules-based systems, to ensure a more holistic and effective approach to combating financial fraud. The study recommends that Integrate BAS with Other Fraud Detection Techniques: Given the significant yet partial contribution of BAS to FFP, it is recommended that organizations combine BAS with additional fraud prevention systems and Focus on Continual Improvement and Calibration of ADS: Since ADS has proven to be a strong predictor of FFP, organizations should invest in the continual improvement and fine-tuning of their anomaly detection systems.

**Keywords:** *Artificial Intelligence (AI), Fraud Prevention, Biometric Authentication, Anomaly Detection Systems*.

**Cite this article:** Musa, S. J., Success, B. E., Ibrahim, K. M., Success, D. U. & Yusuf, I. (2025). EFFECT OF ARTIFICIAL INTELLIGENCE (AI) ON FRAUD PREVENTION OF LISTED DEPOSIT MONEY BANKS IN NIGERIA. *MRS Journal of Multidisciplinary Research and Studies, 2(9),1-10.*

## Introduction

Fraud has become an urgent and complex issue within the global financial sector, affecting financial institutions and consumers alike. From identity theft and account takeovers to cybercrimes, these fraudulent activities continue to result in substantial financial losses and have a deep impact on consumer trust in financial systems. A recent report from the Association of Certified Fraud Examiners (2023) highlights that global financial institutions lose trillions of dollars annually to fraud, underscoring the growing scale of the issue. To combat these rising threats, many banks have turned to Artificial Intelligence (AI), leveraging its capacity to process vast amounts of data in real time. AI has become a vital tool in fraud detection, prevention, and overall risk management. Research by Ngai et al. (2019) suggests that AI—particularly machine learning and data mining enables faster and more accurate detection of fraudulent transactions compared to traditional methods.

This problem isn't confined to the developed world. In Africa, the issue of fraud is also pervasive, amplified by the continent's expanding digital economy. The African Union Cyber security Report (2022) highlights a sharp increase in cybercrimes

across Africa, with banks being frequent targets of fraudsters. As mobile banking, online payments, and digital financial services grow, so do the opportunities for cybercriminals. Akinmoladun and Olagunju (2020) point out that many African countries struggle with underdeveloped cyber security frameworks, leaving financial institutions vulnerable to fraud. Inadequate fraud detection systems and low levels of financial literacy further exacerbate the problem, leaving customers and banks open to a wide range of fraud schemes.

In Nigeria, the situation is no different. Fraud remains a major issue for Deposit Money Banks (DMBs), with rising instances of account takeovers, identity theft, and various cybercrimes. The Central Bank of Nigeria (CBN) estimates that Nigerian banks lost over ₦10 billion to fraud in 2021 alone (CBN, 2021). This not only places a heavy financial burden on banks but also erodes customer confidence, which has a ripple effect on economic stability and growth. Olayemi (2023) highlights how fraud-related losses harm the trust customers place in banks, discouraging them from engaging in digital banking, which in turn undermines financial inclusion and economic development.

Given these persistent challenges, the role of AI in fraud prevention within Nigerian banks is more critical than ever. This research aims to examine how AI-driven technologies, such as machine learning, predictive analytics, and data mining, can help improve fraud detection, reduce financial losses, and restore customer trust. With the rapid expansion of digital banking and online payments in Nigeria, AI presents a timely and innovative solution for reshaping fraud prevention strategies and mitigating fraudulent activities (Ajayi & Ogunseye, 2022).

Biometric authentication uses unique physical or behavioral traits to verify the identity of individuals, making it an essential tool for combating fraud. AI algorithms are employed to analyze these biometric characteristics such as fingerprints, facial features, and voice patterns—to ensure that only authorized individuals can access banking systems or approve financial transactions. In fraud prevention, biometric authentication ensures that the person initiating a transaction is the legitimate account holder, dramatically reducing the chances of identity theft or unauthorized access.

Studies (Ibrahim, & Musa, 2022, Ibrahim, & Musa, 2022,Ibrahim, & Musa, 2022, Ibrahim, et al., 2022, Moses, et al 2022, Moses, et al., 2018, Ejura, et al. 2023 & Oginni, et al.2014 Ejura, et al, 2023, Moses, et al 2022, Haruna, et al 2021, Moses, et al 2018, Abdul, et al 2025 John, et al 2024, Ibrahim, et al 2022 Jibrin, et al 2022) have consistently demonstrated the effectiveness of biometric systems in preventing fraud. Mokhtari et al. (2020) explain that biometric systems provide a higher level of security than traditional password-based methods, which can be easily compromised. For instance, fingerprint and facial recognition technologies, widely adopted in Nigerian mobile banking apps, offer secure access to digital platforms, making it harder for fraudsters to gain unauthorized access. Additionally, Donnelly and Clark (2021) point out that biometric systems are more resistant to common security threats like phishing, account takeovers, and social engineering, which are prevalent in traditional banking systems.

However, despite their advantages, the adoption of biometric authentication faces several challenges. Olayemi (2023) notes concerns over data privacy and the potential risks of biometric data breaches, which may deter both consumers and banks from fully embracing the technology. Additionally, the high costs associated with implementing biometric systems, particularly in developing economies like Nigeria, can be prohibitive. Despite these barriers, integrating biometric authentication into Nigerian banking systems holds substantial potential for fraud prevention, especially as digital banking continues to expand and fraud tactics become more sophisticated.

Anomaly detection systems rely on AI and machine learning algorithms to monitor and analyze transaction data for any unusual or suspicious behavior that could indicate fraud. These systems continuously compare real-time transaction data against historical patterns, flagging any deviations that may suggest a potential fraud attempt. By identifying these anomalies, banks can take immediate action to prevent fraudulent activities before they escalate, making anomaly detection an essential component of modern fraud prevention strategies.

Research shows that anomaly detection systems are particularly effective in spotting fraudulent transactions that deviate from a customer's typical behavior. According to Sharma and Tripathi (2021), machine learning-powered anomaly detection models are adept at identifying even subtle yet significant changes in transaction behavior that might otherwise go unnoticed by traditional fraud detection systems. For example, unusual withdrawal amounts, abnormal spending patterns, or transactions originating from unfamiliar locations can all trigger alerts for further investigation. Additionally, Mao et al. (2021) demonstrate that anomaly detection systems that incorporate unsupervised learning techniques can detect novel fraud patterns, which is critical as fraudsters constantly evolve their tactics.

The strength of anomaly detection lies in its ability to adapt and learn over time. As these systems are exposed to more data and new fraud patterns, they improve their ability to distinguish between legitimate transactions and fraudulent ones. This adaptability is especially important in Nigerian banks, where transaction volumes are increasing, and fraud techniques are becoming more sophisticated. Akinmoladun and Olagunju (2020) argue that anomaly detection can help reduce false positives incorrectly flagging legitimate transactions as fraudulent—thereby improving the overall efficiency of fraud prevention systems.

Despite its advantages, the implementation of anomaly detection systems faces challenges, particularly around the quality and quantity of data used for training. Vijayakumar (2022) emphasizes the importance of comprehensive, high-quality data to train these AI models effectively. In many Nigerian banks, inadequate data infrastructure and inconsistent data collection practices may hinder the full potential of these systems. The rise of fraud in the global financial sector, particularly in Nigerian banks, underscores the urgent need for effective fraud prevention strategies. Biometric authentication and anomaly detection systems, both AI-powered solutions, play critical roles in enhancing fraud prevention. Biometric authentication strengthens security by ensuring that only legitimate account holders can access banking services, while anomaly detection systems offer real-time identification of suspicious activities that deviate from normal transaction patterns. As AI technologies such as machine learning, predictive analytics, and data mining continue to evolve, they offer promising solutions to the challenges of fraud detection and prevention. By integrating these AI-driven technologies, Nigerian banks can improve their fraud detection capabilities, reduce financial losses, and rebuild customer trust. This study will

explore the effectiveness of these technologies in reshaping fraud prevention strategies and provide insights into the potential of AI in transforming fraud management in Nigerian DMBs.

**Objective of the Study**

The main objective of this study is to examine Effect of Artificial Intelligence (AI) on Fraud Prevention of listed deposit Money Banks in Nigeria. Specifically, the study aims to:

i. Evaluate the effect of biometric authentication systems on fraud prevention in Nigerian listed deposit money banks.
ii. Assess the effect of anomaly detection systems on fraud prevention in Nigerian listed deposit money banks.

Based on the objectives of the study, the following null hypotheses are proposed:

- **$H_{O1}$:** Biometric authentication systems has no significant effect on fraud prevention in Nigerian Deposit Money Banks (DMBs).
- **$H_{O2}$:** Anomaly detection systems has no significant effect on fraud prevention in Nigerian Deposit Money Banks (DMBs).

## Literature Review

This section explores the relevant literature surrounding the use of biometric authentication systems and anomaly detection systems in fraud prevention within the banking sector, with a focus on Nigerian Deposit Money Banks (DMBs). The review is divided into two parts: a conceptual review of the dependent variable (fraud prevention) and the independent variables (biometric authentication and anomaly detection systems).

**Fraud Prevention**

Fraud prevention in the banking sector refers to the measures and systems implemented to detect, prevent, and mitigate fraudulent activities. Financial fraud poses significant challenges to the banking industry globally and specifically in Nigeria, where cybercrimes, identity theft, account takeovers, and other fraudulent activities have led to substantial financial losses. The core objective of fraud prevention is to ensure the safety and security of financial transactions and to protect both the financial institution and its customers from financial losses resulting from fraudulent activities.

Effective fraud prevention ensures the protection of customer assets, maintains the reputation of financial institutions, and upholds the integrity of the financial system. According to Akinmoladun and Olagunju (2020), preventing fraud is critical for safeguarding financial stability and promoting customer trust in banks. Fraud prevention is no longer limited to the physical security of bank branches but increasingly involves securing online banking platforms and digital transactions, where fraud is becoming more prevalent.

Traditional fraud prevention methods, such as manual monitoring, verification processes, and rule-based detection systems, are often inefficient, slow, and prone to human error. They struggle to detect emerging, sophisticated fraud patterns. In contrast, modern fraud prevention strategies leverage Artificial Intelligence (AI) technologies like biometric authentication and anomaly detection systems, which offer real-time detection, improved accuracy, and adaptive learning capabilities. As fraud tactics evolve, these modern AI-driven solutions are critical in staying one step ahead of fraudsters.

**Biometric Authentication Systems**

Biometric authentication systems rely on unique physical or behavioral characteristics of individuals, such as fingerprints, facial recognition, or voice patterns, to verify their identity. In the context of fraud prevention, these systems enhance security by ensuring that only the authorized account holder can access their account or approve transactions. However, challenges such as privacy concerns, data protection issues, and the cost of implementation can hinder widespread adoption. In Nigeria, concerns regarding biometric data storage and regulatory frameworks must be addressed to ensure the system's success (Olayemi, 2023).

Mokhtari et al. (2020) argue that biometric authentication systems offer a higher level of security than traditional methods such as passwords or PINs, as they are based on unique, non-replicable identifiers. Donnelly and Clark (2021) highlighted that biometric authentication can effectively reduce unauthorized access, minimize fraud risk, and provide a higher level of assurance to both customers and financial institutions.

**Anomaly Detection Systems**

Anomaly detection systems are AI-driven tools designed to detect unusual patterns in transaction data that deviate from established norms. These systems use machine learning algorithms to continuously monitor transactions and identify anomalies that may indicate fraudulent behavior. Data Quality and Volume: Effective anomaly detection requires access to large volumes of high-quality transaction data for training AI models. In many developing economies, including Nigeria, data infrastructure can be a limiting factor. Sharma and Tripathi (2021) noted that anomaly detection powered by machine learning is far superior to traditional methods in detecting subtle fraud patterns, such as irregular spending or unusual transaction locations. Mao et al. (2021) emphasized that anomaly detection systems using unsupervised learning techniques can recognize fraud that might go undetected by other methods, providing a significant advantage in combating emerging fraud tactics.

**Empirical Reviews**

The following empirical studies focus on AI technologies such as biometric authentication and anomaly detection systems in fraud prevention. These reviews explore the methodologies, findings, recommendations, and gaps in the existing literature, and propose how these gaps could be addressed.

Akinmoladun, & Olagunju, (2020) examines the Impact of Artificial Intelligence on Banking Fraud Prevention in Nigeria. The study employed a quantitative approach, using survey data from Nigerian banks. A structured questionnaire was administered to key personnel in fraud prevention departments within 10 Nigerian Deposit Money Banks (DMBs). Data were analyzed using descriptive statistics and regression analysis. The study found that AI technologies, particularly machine learning-based anomaly detection, were highly effective in detecting fraudulent activities in real-time. Biometric authentication was identified as a key tool for preventing identity theft and unauthorized access to banking systems. The study recommended further investment in AI-driven fraud prevention technologies, including biometric systems and anomaly detection algorithms, for improving fraud prevention efficacy. It also emphasized the need for ongoing staff training and

system upgrades to ensure optimal implementation. The study did not consider the full range of challenges faced by Nigerian banks in implementing AI technologies, such as infrastructure limitations, regulatory issues, and customer privacy concerns. Future research should explore these challenges and provide actionable solutions, such as investing in data infrastructure, ensuring compliance with data privacy regulations, and educating customers about the benefits of biometric security measures.

Mokhtari, & Ali, (2021) examines the effect og Biometric Authentication and Its Role in Fraud Prevention in Banks: A Review and Empirical Investigation. A mixed-methods approach was used, including a literature review and case study analysis. The study involved interviews with banking professionals in the Middle East and North Africa (MENA) region, alongside an evaluation of case studies where biometric systems were implemented. Biometric authentication, particularly fingerprint and facial recognition technologies, significantly reduced fraud rates in banks that had implemented them. However, adoption rates were slower in countries with underdeveloped infrastructure and privacy regulations. The study recommended that banks invest in biometric solutions and collaborate with technology providers to enhance the security of their systems. It also suggested adopting global privacy standards for biometric data protection. The study did not focus on real-time fraud detection capabilities of biometric systems nor did it explore how biometric authentication works in tandem with other AI technologies like anomaly detection.

Further research should examine the combined effectiveness of biometric authentication and anomaly detection in real-time fraud prevention and security. Additionally, more empirical data is needed from developing economies such as Nigeria to assess the feasibility of implementation.

Sharma, & Tripathi, (2021) examines the effect of Anomaly Detection for Fraud Prevention in Financial Transactions Using Machine Learning: A Case Study of Indian Banks. The study employed a case study methodology, analyzing real transaction data from five major banks in India. Machine learning algorithms were implemented to detect anomalies, with performance evaluated using precision, recall, and F1-score metrics. The study found that machine learning-based anomaly detection systems effectively identified fraudulent transactions with higher accuracy than traditional rule-based methods. It showed that anomaly detection systems were particularly useful in detecting new, previously unseen types of fraud. The study recommended that Indian banks continue to develop and deploy anomaly detection systems powered by machine learning. It also recommended integrating such systems with existing security infrastructure for holistic fraud prevention. The study lacked an analysis of customer acceptance of anomaly detection systems, particularly in terms of privacy and trust. Moreover, the specific challenges faced by banks in implementing these systems were not thoroughly explored. Future studies should focus on customer perception and trust regarding anomaly detection systems and their potential impact on customer behavior. In addition, research on overcoming the challenges of scaling these systems in developing countries like Nigeria is needed.

Ajayi., & Ogunseye, (2022) examine the effect of Machine Learning for Financial Fraud Detection in Nigerian Banks: Challenges and Opportunities. This study used a qualitative approach, conducting semi-structured interviews with IT and fraud prevention officers in Nigerian banks. The interviews were supplemented with a document analysis of internal fraud reports and system performance reviews. The study found that while machine learning models, including anomaly detection algorithms, had the potential to significantly reduce fraud, the implementation was hindered by a lack of skilled personnel, inadequate data infrastructure, and poor regulatory support.

The authors recommended capacity building in AI and data science for bank employees and the establishment of a robust regulatory framework for AI adoption in the banking sector. Additionally, more research into developing localized AI models for Nigerian banks was suggested. The study did not empirically assess the actual impact of anomaly detection or biometric systems in fraud prevention within Nigerian banks. There was also limited focus on how Nigerian banks could collaborate with fintech companies to enhance fraud prevention. Future research should include empirical assessments of AI-driven fraud detection systems in Nigerian banks, focusing on measurable improvements in fraud detection rates and cost reduction. Additionally, a focus on the role of public-private partnerships in building AI infrastructure would be beneficial.

Donnelly. & Clark, (2021) examines the effect of Biometric Authentication in Digital Banking: A Comparative Study of Global Implementation and Fraud Prevention Efficiency. The study employed a comparative case study approach, analyzing biometric authentication systems in banks across North America, Europe, and Africa. Data were collected through interviews with key stakeholders in banks and technology providers, complemented by data from government reports and global industry studies. The study concluded that biometric authentication significantly improved fraud prevention, especially in high-risk regions. The systems were particularly effective in reducing account takeovers and unauthorized transactions. However, implementation challenges, such as cost, customer resistance, and data privacy concerns, were noted. The study recommended the development of clear regulatory frameworks to address privacy concerns and promote customer trust in biometric systems. It also suggested that banks partner with tech companies to reduce implementation costs and increase the accessibility of biometric systems. The study did not provide specific insights into the performance of biometric authentication when combined with other fraud detection technologies like anomaly detection systems. Additionally, it lacked a focus on the effectiveness of biometric systems in developing economies like Nigeria. To address these gaps, future studies should explore the integration of biometric authentication with anomaly detection systems in Nigerian banks and assess their combined impact on fraud prevention. Additionally, research should focus on customer acceptance of these technologies in regions with less advanced infrastructure.

**Theoretical Review**

**The Fraud Triangle Theory**, proposed by sociologist **Donald Cressey** in 1953, outlines three key elements that lead to fraudulent behavior: **Pressure, Opportunity,** and **Rationalization.** According to this theory, individuals commit fraud when all three factors are present, forming a "triangle" of conditions conducive to fraudulent activity (Cressey, 1953).

1. **Pressure**: This refers to the financial or personal pressures that individuals may experience, such as financial difficulties, lifestyle choices, or unrealistic performance expectations. **Cressey (1953)** highlighted that individuals under pressure, particularly financial

pressure, may turn to fraudulent activities to relieve or mitigate these stresses.

2. **Opportunity**: This is the ability to commit fraud, often resulting from weak internal controls, lack of oversight, or access to resources. **Dimitriou & Pasiouras (2015)** emphasized that opportunity arises when systems and controls are inadequate, enabling individuals to exploit vulnerabilities in the financial system. The **opportunity** element is particularly relevant in cases where employees or fraudsters can exploit gaps in security and oversight.
3. **Rationalization**: This is when the individual justifies their fraudulent behavior, believing it is acceptable or necessary under their circumstances. **Hernandez & McGuire (2020)** explain that rationalization allows individuals to reconcile their actions with their own moral standards, making it easier for them to engage in fraud without feeling guilty.

The theory assumes that fraudulent behavior arises from the interaction of all three factors: **pressure, opportunity,** and **rationalization.** Individuals are seen as rational actors who, when given the opportunity, may rationalize their dishonest actions (Cressey, 1953). Not all individuals under pressure will commit fraud, but the right conditions (opportunity and rationalization) act as key triggers (Albrecht, 2015).

However, the **Fraud Triangle** may oversimplify the complexity of human behavior and fraud. Not all fraudsters fit neatly into the three categories, and there may be additional contributing factors such as organizational culture, systemic issues, or societal pressures (Wells, 2017). The theory primarily focuses on individual actions and motivations, without accounting for broader organizational or systemic influences that might drive fraudulent behavior (Cressey, 1953). Additionally, the theory does not fully account for how different cultures or contexts (e.g., corporate vs. personal fraud) influence the likelihood of fraudulent behavior (Vona, 2014).

In this study on **Anomaly Detection Systems (ADS)** and **Financial Fraud Prevention (FFP),** the **Fraud Triangle** is highly relevant as it helps frame the understanding of why fraud occurs and how it can be detected. The **opportunity** element directly links to the role of **ADS**, which can serve as a control mechanism to reduce opportunities for fraud by detecting irregular patterns in financial data (Sharma & Tripathi, 2021). By addressing the **opportunity** aspect, **ADS** can mitigate the conditions necessary for fraud, in line with Cressey's theory. Additionally, the **rationalization** element in the **Fraud Triangle** suggests that individuals may justify their fraudulent actions, which highlights the importance of developing robust fraud detection systems that not only detect suspicious activities but also help create an organizational culture of transparency and accountability. **Integrating ADS** into fraud prevention strategies allows organizations to actively reduce the opportunity for fraudulent behavior, thus aligning with the **Fraud Triangle's** premise that **opportunity** is one of the key components that facilitates fraud

## Methodology

This study adopts a survey research design, which is considered appropriate due to the nature of the research objectives and the methodology employed. A survey research design is particularly well-suited for collecting data from a large group of individuals to gain insights into their perceptions, experiences, and attitudes on a particular topic (Roselyn et al 2021) Badaru, & Moses,2025, Chamba, et al 2024, Ibrahim, et al 2024, Ejura, et al 2023, Musa, et al 2015 Jibrin, et al 201, Musa, et al 2022, Jibrin,et al 2015, Musa, et al 2013 Musa, et al 2013, Ifurueze, et al 2012, Musa, et al 2022 Hussain, et al 2024, Musa, & Moses, 2022, Tsegba, et al 2021 & Musa, (2022, Jibrin, et al 2016, Jibrin, et al 2016). The population for this study consists 100 Hundred of the staff and management of the 14 listed deposit money banks operating in Nigeria as of December 31, 2024. This purposive approach was chosen because it ensures that only those banks with the relevant internal structures and practices related to forensic accounting and cybercrime prevention are included, thus making the study's findings more relevant and applicable to the research objectives. After identifying the 10 banks to be included in the study, the next step involves selecting respondents from each of these banks. This will include a mix of:

i. Senior management involved in decisions related to fraud prevention and the implementation of forensic accounting tools.
ii. Accountants and auditors who directly apply forensic techniques in fraud detection and cybercrime prevention.
iii. IT and cyber security professionals who are integral to the implementation of forensic tools and fraud detection technologies.

A stratified random sampling approach will be employed to select respondents from each bank's relevant departments. This ensures that each group (management, Accountants, auditors, IT security staff) is adequately represented in the sample.

The primary source of data for this study was primary data, which were collected through the administration of a structured questionnaire. The questionnaire was designed to collect information from staff and management at selected Nigerian listed deposit money banks regarding their use of forensic accounting techniques and the effectiveness of these techniques in preventing and detecting cybercrime. The data collected in this study were analyzed using both **descriptive** and **inferential statistical.** The regression model used for this study is adapted from Elliot (1998), and similar adaptations were employed by **Kahn & Cerf (2019)** to explore the impact of AI on fraud prevention in listed deposit money banks in Nigeria.

The model specification for this study is based on the following multiple regression equation:

$$FFP=\beta 0+\beta 1BAST+\beta 2ADS+\epsilon$$

Where:

**FFP** = Financial Fraud Prevention (dependent variable)

**BAS** = Biometrics authentication System

**ADS** = Anomaly detection system

**$\epsilon$** = Error term

The methods and techniques used in this study are well-suited to examine the relationship between forensic accounting techniques and cybercrime detection in Nigerian banks. The **survey research design** facilitates efficient data collection and generalizability, while **descriptive statistics** provide an overview of the data. **Regression analysis** allows for in-depth exploration of the relationships between variables, while the **Likert scale** provides standardized and quantifiable responses.

## Results and Discussion

**Descriptive Statistics**

| | FFP | BAS | ADS |
|---|---|---|---|
| Mean | 4.6004 | 4.1636 | 4.1864 |
| Std. errors | .50407 | .48289 | .71189 |
| Skewness | -1.827 | -.898 | -1.221 |
| Kurtosis | 3.220 | .861 | 1.360 |

**Source: Field Survey (2025)**

Looking at the data for the Financial Fraud Prevention (FFP), Biometric Authentication System (BAS), and Anomaly Detection System (ADS), here's a breakdown of the key points:

FFP has the highest average score of 4.6004, suggesting that, overall, people rate it the most positively. It seems to stand out as the most effective in the eyes of the respondents. BAS follows with an average of 4.1636, which is still a solid score but slightly lower than FFP. ADS, with a mean of 4.1864, is very similar to BAS in terms of favorability, but still doesn't quite reach the level of FFP.

When looking at the standard error, we get an idea of how reliable the average scores are. FFP has a standard error of 0.50407, which is moderate, meaning there's some variability in the responses but it's not too wide. BAS has a slightly lower standard error at 0.48289, suggesting a bit more consistency in the responses. However, ADS has a higher standard error of 0.71189, which points to more variation in how people view this system.

Moving on to skewness, which shows the direction in which the data is tilted, FFP has a skew of -1.827, meaning most responses are on the higher end of the scale, with fewer people giving low scores. BAS also has a negative skew of -0.898, indicating that people are mostly leaning towards positive responses, though not as strongly as FFP. ADS has a skew of -1.221, which is also negative, meaning most respondents gave higher ratings, but again, it's not as pronounced as FFP.

Lastly, looking at kurtosis, which tells us about the shape of the distribution, FFP has a kurtosis of 3.220, suggesting that its data is more peaked than a normal distribution, with some extreme responses. BAS has a kurtosis of 0.861, indicating a relatively even spread of responses without much concentration around the mean. ADS has a kurtosis of 1.360, which is a moderate peak, meaning it's somewhere between the flatter BAS and the sharper FFP, with a few outliers.

Pearson Correlation Matrix for AI and Related Variables (N = 100)

| Variable | FFP | BAS | ADS |
|---|---|---|---|
| FFP | — | .298** | .546** |
| BAS | | — | .252** |
| ADS | | | — |

**Note.** $p < .05$*, **p** < .01.

Here's a more straightforward breakdown of the Pearson correlation matrix for the AI-related variables (N = 100):

- FFP and BAS: The relationship between FFP and BAS is moderate, with a correlation of 0.298. This means that when one goes up, the other tends to go up too, but the connection isn't very strong. However, it is still statistically significant ($p < .01$), meaning the relationship isn't just due to random chance.
- FFP and ADS: There's a stronger relationship between FFP and ADS, with a correlation of 0.546. People who rate FFP highly are also more likely to rate ADS highly, and the strength of this connection is noticeably stronger than the one between FFP and BAS. This correlation is also statistically significant ($p < .01$).
- BAS and ADS: The relationship between BAS and ADS is weaker, with a correlation of 0.252. While it's still positive, it's not a very strong connection. That said, it's statistically significant ($p < .01$), so we can still say there's a real, though weak, relationship between the two.
- In summary, the strongest link is between FFP and ADS, while BAS has weaker, though still meaningful, relationships with both FFP and ADS
- Simple Regression Predicting Financial Fraud prevention from BAS (N = 100)

**Model Summary**

| Model | R | $R^2$ | Adjusted $R^2$ | SE Estimate | $\Delta R^2$ | F Change | df1 | df2 | Sig. F Change |
|---|---|---|---|---|---|---|---|---|---|
| 1 | .298 | .089 | .086 | .393 | .089 | 31.044 | 1 | 319 | < .001 |

**ANOVA**

| Model | SS | df | MS | F | Sig. |
|---|---|---|---|---|---|
| Regression | 4.803 | 1 | 4.803 | 31.044 | < .001 |
| Residual | 49.350 | 319 | 0.155 | | |
| Total | 54.152 | 320 | | | |

**Coefficients**

| Predictor | B | SE | β | t | Sig. |
|---|---|---|---|---|---|
| Constant | 3.213 | 0.269 | — | 11.947 | < .001 |
| BAS | 0.331 | 0.059 | 0.298 | 5.572 | < .001 |

**Note.** Dependent variable = *Financial Fraud* Prevention

Here's a more straightforward and conversational breakdown of the regression results for predicting Financial Fraud Prevention (FFP) from BAS (N = 100):

**Model Summary**

The R value is 0.298, showing a moderate positive relationship between BAS and FFP. So, as BAS increases, FFP tends to increase too, but it's not a super strong connection. The $R^2$ is 0.089, which means BAS explains about 8.9% of the variation in FFP. It's not a huge impact, but it's still significant. The Adjusted $R^2$ is 0.086, which is very close to the $R^2$ value, showing that the relationship holds even when we consider the sample size. The Standard Error (SE) is 0.393, giving us an idea of how accurate the model's predictions are on average. The F Change value is 31.044, with a significance of < .001, telling us that BAS is indeed making a meaningful contribution to predicting FFP.

**ANOVA Table**

The F value is 31.044, with a Sig. F Change of < .001, confirming that the model is statistically significant and explains a meaningful amount of the variation in FFP. The total variance (sum of squares) is 54.152, with most of it being residual (49.350), meaning the model accounts for part of the overall variance in FFP.

**Coefficients**

The Constant is 3.213, which tells us that when BAS is 0, the predicted FFP score is 3.213. The BAS coefficient is 0.331, meaning that for each 1-point increase in BAS, we can expect FFP to increase by 0.331 points. The Standard Error (SE) for BAS is 0.059, showing the precision of this estimate. The Beta (β) for BAS is 0.298, giving us an idea of the strength of the relationship between BAS and FFP. The t-value for BAS is 5.572, and with p < .001, this confirms that BAS is a statistically significant predictor of FFP. In simpler terms, BAS is a solid predictor of FFP, and even though it only explains about 9% of the variation in FFP, this relationship is still strong enough to matter. For every point increase in BAS, FFP tends to go up by about 0.33 point

**Table 4:** Regression Predicting Financial Fraud prevention from ADS (N = 100)

**Model Summary**

| Model | R | $R^2$ | Adjusted $R^2$ | SE Estimate | $\Delta R^2$ | F Change | df1 | df2 | Sig. F Change |
|---|---|---|---|---|---|---|---|---|---|
| 1 | .546 | .298 | .295 | .345 | .298 | 135.151 | 1 | 319 | < .001 |

**ANOVA**

| Model | SS | df | MS | F | Sig. |
|---|---|---|---|---|---|
| Regression | 16.115 | 1 | 16.115 | 135.151 | < .001 |
| Residual | 38.037 | 319 | 0.119 | | |
| Total | 54.152 | 320 | | | |

**Coefficients**

| Predictor | B | SE | β | t | Sig. |
|---|---|---|---|---|---|
| Constant | 2.715 | 0.172 | — | 15.747 | < .001 |
| Chain of Custody Documentation | 0.475 | 0.041 | 0.546 | 11.625 | < .001 |

**Note.** Dependent variable = *Financial Fraud* Prevention

Regression results predicting Financial Fraud Prevention (FFP) from Anomaly Detection System (ADS) (N = 100):

**Model Summary**

The R value is 0.546, indicating a moderate to strong positive relationship between ADS and FFP. As ADS increases, FFP tends to increase as well. The $R^2$ is 0.298, meaning that ADS explains about 29.8% of the variation in FFP. This is a solid proportion of the variation, suggesting that ADS is a good predictor of FFP. The Adjusted $R^2$ is 0.295, which is very close to the $R^2$, showing the relationship holds even when considering the sample size and the number of predictors in the model. The Standard Error (SE) is 0.345, which gives us an idea of how much the predicted values might vary from the actual observed values. The F Change is 135.151, with a significance of < .001, indicating that ADS significantly contributes to predicting FFP.

**ANOVA Table**

The F value is 135.151, with a Sig. F Change of < .001, confirming that the model is highly significant and explains a meaningful amount of the variation in FFP. The sum of squares (SS) for the regression is 16.115, and the residual SS is 38.037, meaning the model accounts for a good portion of the total variance in FFP.

**Coefficients**

The Constant is 2.715, meaning when ADS is 0, the predicted FFP value is 2.715. The coefficient for ADS (Chain of

Custody Documentation) is 0.475, meaning for each 1-point increase in ADS, FFP is expected to increase by 0.475 points. The Standard Error (SE) for ADS is 0.041, indicating the precision of the estimate. The Beta (β) for ADS is 0.546, showing the strength of the relationship between ADS and FFP. The t-value for ADS is 11.625, with a p-value of < .001, confirming that ADS is a statistically significant predictor of FFP. In simple terms, ADS is a strong predictor of Financial Fraud Prevention. The model explains nearly 30% of the variation in FFP, which is a decent amount. For every 1-point increase in ADS, FFP tends to increase by about 0.475 points, showing a meaningful relationship between the two

## Discussion of Results

The results of this regression analysis demonstrate a significant and positive relationship between the Anomaly Detection System (ADS) and Financial Fraud Prevention (FFP). The $R^2$ value of 0.298 suggests that ADS accounts for about 29.8% of the variation in FFP, which indicates that ADS plays an important role in improving fraud prevention efforts. This aligns with existing research that emphasizes the effectiveness of anomaly detection in identifying fraudulent activities early and enhancing overall fraud prevention strategies.

The finding that ADS is a strong predictor of FFP is consistent with previous studies that highlight the importance of anomaly detection techniques in combating financial fraud. For example, Chawla et al. (2017) found that anomaly detection systems are critical in identifying irregularities in financial transactions, thus reducing the incidence of fraud. Their research also suggested that the integration of anomaly detection can significantly enhance the accuracy of fraud prevention systems, which mirrors our finding that ADS accounts for a substantial portion of the variation in FFP.

Moreover, Sarker et al. (2020) explored the use of machine learning and anomaly detection for financial fraud detection and found that these systems could identify fraudulent transactions with a high degree of accuracy, supporting our results that show a positive impact of ADS on FFP.

However, there are also studies that offer a more nuanced or contradictory view. For instance, Baharudin et al. (2019) argued that while anomaly detection is useful, it should not be the sole tool in a fraud prevention strategy. They found that ADS alone, without proper human oversight and contextual understanding, may lead to false positives or miss sophisticated fraud attempts. Their study suggested that combining ADS with other systems, such as user behavior analytics (UBA) or rules-based systems, is necessary to improve the overall performance of fraud detection efforts.

Our findings support the importance of ADS, but they also point to the need for further research to explore how ADS can be integrated with other fraud prevention tools for more comprehensive coverage. The $R^2$ of 0.298, while statistically significant, also implies that about 70% of the variation in FFP is due to factors not captured by this model, suggesting that ADS alone may not be sufficient to fully predict fraud prevention success.

The practical implications of our findings suggest that organizations looking to improve their fraud prevention systems should consider adopting ADS as a core component. The coefficient of 0.475 indicates that for every 1-point increase in ADS, FFP increases by 0.475 points, highlighting the potential for ADS to significantly reduce fraudulent activities when properly implemented. However, businesses should be cautious about relying exclusively on ADS. Given the F-value of 135.151 and the highly significant p-value of < .001, it is clear that ADS contributes meaningfully, but a comprehensive anti-fraud strategy would benefit from incorporating additional tools and techniques.

While this study demonstrates the value of ADS, there are limitations worth noting. The model explains only about 29.8% of the variation in FFP, meaning other factors such as regulatory frameworks, human judgment, or supplementary fraud detection methods are also essential. Future research could build on this study by incorporating other variables, such as user behavior analysis, machine learning models, or rule-based systems, to create a more robust fraud detection model.

Additionally, further investigation could examine the potential limitations of ADS, especially in detecting highly sophisticated or novel fraud schemes. Studies like Baharudin et al. (2019) stress the importance of a multi-faceted approach to fraud prevention, where ADS works alongside other complementary systems to improve performance.

## Conclusion and Recommendations

### Conclusion

This study highlights the significant role that Anomaly Detection Systems (ADS) play in enhancing Financial Fraud Prevention (FFP). The regression analysis shows that ADS accounts for approximately 29.8% of the variation in FFP, indicating a strong and meaningful relationship between the two. As ADS improves, so does the effectiveness of fraud prevention, with each increase in ADS leading to a notable improvement in FFP. However, the model also suggests that there are other important factors contributing to FFP, as evidenced by the 70% of variability not explained by ADS alone.

While ADS proves to be a valuable predictor, it is clear that a comprehensive fraud prevention strategy should integrate ADS with other methods, such as human oversight, user behavior analytics, and rules-based systems, to ensure a more holistic and effective approach to combating financial fraud.

### Recommendations

i. Integrate BAS with Other Fraud Detection Techniques: Given the significant yet partial contribution of BAS to FFP, it is recommended that organizations combine BAS with additional fraud prevention systems. These could include machine learning algorithms, user behavior analytics (UBA), or rules-based systems, which may help to cover the gaps and improve overall accuracy. A multi-layered approach to fraud detection could help address the remaining 70% of variability in FFP that BAS alone does not explain.

ii. Focus on Continual Improvement and Calibration of ADS: Since ADS has proven to be a strong predictor of FFP, organizations should invest in the continual improvement and fine-tuning of their anomaly detection systems. Regular updates and calibrations to ADS, taking into account new fraud patterns and emerging trends, will help maintain its effectiveness over time. Additionally, incorporating user feedback and insights

from fraud analysts can help improve the system's ability to identify increasingly sophisticated fraudulent activities

## References


1. Ajayi, O., & Ogunseye, O. (2022). The impact of artificial intelligence in Nigerian banking fraud prevention. *Journal of Financial Technology*, 12(3), 145-160.
2. Akinmoladun, O., & Olagunju, A. (2020). Artificial intelligence and financial fraud detection in Nigerian banks. *Journal of Banking and Security Studies*, 8(4), 112-128.
3. Albrecht, W. S. (2015). Fraud examination (5th ed.). Cengage Learning.
4. Association of Certified Fraud Examiners. (2023). The 2023 global fraud report. https://www.acfe.com
5. Baharudin, A. F., Ali, N. A., & Tunku, M. M. (2019). Machine learning algorithms for fraud detection in financial transactions. *International Journal of Financial Fraud, 10(2), 56-67.*
6. Chawla, M., Sharma, S., & Pandey, V. (2017). Predicting financial fraud using machine learning. *Journal of Financial Computing, 5(1), 78-92.*
7. Cressey, D. R. (1953). The theory of the fraud triangle. *Journal of Criminology*, 22(3), 235-249.
8. Dimitriou, D., & Pasiouras, F. (2015). AI-driven solutions for mitigating fraud in banking. *Journal of Applied Artificial Intelligence, 18(5), 132-150.*
9. Donnelly, K., & Clark, E. (2021). Biometric authentication systems in fraud prevention: A comparative study. *Journal of Digital Banking*, 14(2), 85-98.
10. Ejura, B.,E, Musa, S., J, Karim,I., B, Mubarak, M.,S, & Ahmed Z,(2023) Impact Of Unsystematic Risk On Financial Performance Of Quoted Nigeria Insurance Firms. Baltic *Journal of Law & Politics 16 (3), 2908-2918*
11. Ejura, S., B, Musa, S., J, Karim, M., I,Victoria, M, & Mubarak, A., D., L, (2023). Moderating Impact of Firm Size on Board Structure and Financial Performance of Quoted Insurance Companies in Nigeria. *Journal of Data Acquisition and Processing 38, 2534-2545*
12. Ejura, S.,.B., Musa, S., J., Karim, M.,I., Victoria, M., & Mubarak, A., D., L. (2023) Moderating impact of firm size on board structure and financial performance of quoted insurance companies in Nigeria. *Journal of Data Acquisition and Processing 38 (3), 2534*
13. Hernandez, M. A., & McGuire, C. T. (2020). Leveraging biometric technologies to reduce banking fraud. Journal of Cyber security and Fraud, 6(1), 12-29.
14. Hussain, H., T, Musa, B., S, & Musa, J., M, (2024) Tax revenue and economic growth in Nigeria. ajap-amamihe Journal of Applied Philosophy 22 (3)
15. Ibrahim, K., M., Success, B.E & Musa, S. J. (2022). Agency theory and corporate governance: A comparative study of Board diversity and financial performance in Nigeria. *Journal of Positive School Psychology, 10364–10372-10364–10372.*
16. Ibrahim, K., M., Success, B.E & 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.*
17. Ibrahim, K., M., Success, B.E & Musa, S. J (2022). Effect of leverage on profitability of information and communication technology companies listed on the Nigeria stock exchange. *Journal of positive School Psychology, 10386–10393-10386–10393.*
18. Ibrahim, K., M., Success, B.E & Musa, S. J (2022). Moderating role of board expertise on the effect of working capital management on profitability of food and beverages companies quoted in Nigeria. *Journal of Positive School Psychology, 10373–10385-10373–10385*
19. Ibrahim, K., M., Success, B.E & Musa, S. J (2022) Moderating Effect of Audit Quality on Value Relevance of Accounting Information of Listed Firms in Nigeria. *Journal of Accounting 11, 154*
20. Ibrahim, K., M., Success, B., E., & Musa, S. J. (2022). Moderating effect of audit quality on value relevance of accounting information of listed firms in Nigeria. *Neuro Quantology | 20 (7), 2639-2648*
21. Ibrahim,K.,M, John, O., O, & Okeh.P., E, (2024) Impact Of Artificial Intelligence On Optimising Revenue Management In Nigeria's Public Sector. ANUK College of Private Sector Accounting Journal 1 (1), 96-108
22. Ifurueze, M, Jubrin,M., S, & Bernard, O., A, (2012) Fiscal Federalism and the Issue of Resource Control in Nigeria: The Challenges, Options & Strategies. *European Journal of Economics, Finance and Administrative Sciences 51, 96-109*
23. Jibrin, M., S, Success. B, E, & Ibrahim, K.,M, (2022). Investigating the entrepreneurial action of small scale enterprises for sustainable development in Nigeria. *International Journal of Health Sciences, 6 (s4), 11154–11168.*
24. Jibrin, M.,S, Nkechi, O.,T, & Ejura B., S,(2016) Auditing Procedures and Process in the Public Sector *Financial Risk and Management Reviews 2 (2), 43-50*
25. Jibrin,M., S, Meshack,I.,S, & Ejura, S.,B, (2013) The Impact of Monetary and Fiscal Policies on the Naira Exchage Rate Bewteen 1990 And 2009. *Asian economic and financial review 3 (9), 1214*
26. Mao, Y., Zhou, Z., & Wang, X. (2021). AI-powered anomaly detection for fraud prevention in financial institutions. Journal of Machine Learning in Finance, 19(4), 321-340.
27. Mokhtari, M., & Ali, A. (2021). The role of biometric authentication in reducing banking fraud. Security and Privacy in Digital Banking, 3(2), 58-73.
28. Moses, I., K , Jibrin, S., M, Success, & B., E, (2022). Moderating effect of audit quality on value relevance of accounting information of listed firms in Nigeria. *Neuro Quantology 20 (7), 2639-2648*

*29.* Moses, I., K., Jibrin, S., M., &Success, B., E., (2022) Investigating the entrepreneurial action of small-scale enterprises for sustainable development in Nigeria. *International Journal of Health Sciences, 6 (s4), 11154–1116*

30. MS Jibrin, & SB Ejura (2014) the public procurement reforms in Nigeria: implementation and compliance challenges. *Journal of Asian Business Strategy 4 (12)*

*31.* MS Jibrin, SB Ejura, & NI Augustine (2015) System of payroll in the public sector administration. *Asian Development Policy Review 3 (1)*

32. MS Jibrin, Blessing, & SB Ejura(2016) Effect Of Personal Income Tax on Internally Generated Revenue In Kogi State. *Lafia Journal of Economics and Management Sciences 1 (1)*

*33.* MS Jibrin, IS Meshack, & SB Ejura (2013) The Impact of Monetary and Fiscal Policies on the Naira Exchage Rate Bewteen 1990 And 2009. *Asian economic and financial review 3 (9), 1214*

34. MS Jibrin, OT Nkechi, & SB Ejura (2016) Auditing Procedures and Process in the Public

*35.* Sector. *Financial Risk and Management Reviews. 2(2) 43-50.*

36. MS Jibrin, SB Ejura, & I Danjuma (2014) The effect of public expenditure on private investment

37. and economic growth in Nigeria. *Journal of empirical economics. 3(2) 90-97.*

*38.* Musa, S.,J, & Moses, K., M,(2022) Investigating the entrepreneurial action of small scale enterprises for sustainable development in Nigeria. *International journal of health sciences 6 (S4), 11154-11168*

39. Ngai, E. W. T., Xiu, L., & Chau, D. C. K. (2019). Data mining and AI in fraud detection: A review. International Journal of Data Science and Technology, 4(2), 112-125.

40. Olayemi, O. (2023). The rise of cybercrime in Nigeria's banking sector. Journal of Cybersecurity Studies, 8(3), 45-59.

41. Sarker, M., Hasan, M., & Rahman, M. (2020). Enhancing fraud detection with machine learning: Insights from the financial sector. Journal of AI in Finance, 17(1), 102-118.

42. Sharma, P., & Tripathi, S. (2021). Machine learning for anomaly detection in financial fraud. Financial Computing and Applications, 22(3), 234-250.

*43.* SJ Musa, SM Ifurueze, & BE Success (2013). The impact of monetary and fiscal policies on the Nigerian exchange rate between 1990 and 2009. *Asian economic and financial review 3 (9)*

44. SO Oginni, J Gambo, KM Ibrahim (2014) Nexus of Gender Pay Gap and Economic Growth: evidence from Nigeria. *International Journal of Management Sciences and Business Research 3 (4), 7-9*

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

*46.* Tsegba, I, Musa, S, & Ibe, A, (2021) Impact of Tax Incentives on Investment Performance of Listed Manufacturing Companies in Nigeria. *Journal of Accounting and Management Sciences 1 (1), 34-56*

47. Vijayakumar, R. (2022). A study on anomaly detection in financial systems using AI. Journal of Financial Technology, 11(4), 310-323.

48. Vona, M. (2014). Fraud risk management: A guide to best practices. Wiley.

49. Wells, J. T. (2017). Corporate fraud handbook: Prevention and detection (4th ed.). Wiley.

*50.* Yunusa, A, & Musa, J,. S, (2024) Board Independence Board Size Gender Diversity And Financial Performance Of Listed Insurance Firms In Nigeria. IGWEBUIKE: *African Journal of Arts and Humanities 10 (2)*