

**ARTIFICIAL INTELLIGENCE AND FRAUD MINIMIZATION IN NIGERIAN
DEPOSIT MONEY BANKS**

Zorkpa, Charles Barinem, PhD

**Department of Accounting, Faculty of Administration and Management,
Ignatius Ajuru University of Education, Rumuolumeni Port Harcourt, Rivers
State, Nigeria.
charlesz2007@yahoo.com
07034324365**

and

Ndukwe, Chika Ibifiri

**Department of Business Education (Accounting option), Faculty of Education,
Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Rivers
State, Nigeria.
08109698774**

Abstract

This study examined the effect of Artificial Intelligence (AI) on fraud minimization in Nigerian Deposit Money Banks. Specifically, it examined the effect of AI on behavioural tests and cognitive benchmarks, segregation of duties and internal controls, performance evaluation metrics, and employee training. The study adopted a descriptive research design and focused on 125 employees selected from five Nigerian Deposit Money Banks. Data were designed to be collected through a structured questionnaire, while mean and standard deviation were used to answer the research questions and regression analysis was specified for testing the hypotheses. The study was anchored on the Fraud Triangle Theory. Findings indicated that Artificial Intelligence contributes to fraud minimization by improving behavioural monitoring, strengthening internal controls and segregation of duties, enhancing performance evaluation, and supporting continuous employee training. The study further established that AI technologies can assist banks in identifying suspicious activities, reducing opportunities for fraud, improving accountability, and strengthening employees' capacity to detect fraudulent practices. However, challenges such as high implementation costs, inadequate infrastructure, and shortage of skilled personnel, data privacy concerns, and regulatory uncertainties may hinder effective AI adoption. The study concluded that Artificial Intelligence is a strategic tool for strengthening fraud minimization in Nigerian Deposit Money Banks. It recommended increased investment in AI-based fraud management systems, stronger internal controls, continuous employee training, improved data governance, and supportive regulatory frameworks.

Keywords: Artificial Intelligence, Fraud Minimization, Behavioural Tests, Internal Controls, Performance Evaluation, Employee Training, Deposit Money Banks.

Introduction

The "Nigerian banking sector has undergone remarkable transformation in recent years as a result of the increasing adoption of digital banking technologies, electronic payment

systems, mobile banking, internet banking, and other financial innovations. These developments have been largely encouraged by the cashless policy of the Central Bank of Nigeria (CBN) and have contributed substantially to operational efficiency, customer convenience, and financial inclusion. However, the rapid digitalization of banking operations has also created new opportunities for financial crimes, increasing both the sophistication and frequency of fraud perpetrated against Deposit Money Banks (DMBs). Fraudsters increasingly exploit technological vulnerabilities through phishing attacks, identity theft, cyber intrusions, account takeovers, and payment fraud, thereby posing significant threats to the stability, security, and integrity of the Nigerian banking system (Apsimet, Smanova, & Utegenova, 2024). Consequently, Deposit Money Banks are under increasing pressure to adopt innovative technological solutions that can effectively minimize fraud while maintaining customer confidence and the stability of the financial system.

Financial fraud has remained one of the most persistent operational risks confronting Deposit Money Banks in Nigeria despite continuous investments in conventional security infrastructure and control mechanisms. Traditional fraud detection approaches largely depend on predefined rules, manual monitoring, and reactive control procedures. Such systems have increasingly become inadequate because of their limited ability to identify emerging and sophisticated fraudulent patterns in real time. They may also produce high rates of false positives, require considerable operational resources, and lack the flexibility to respond rapidly to the changing nature of cyber-enabled financial crimes (Ikemefuna, Okusi, Iwuh, & Yusuf, 2024). As the volume, speed, and complexity of banking transactions continue to increase, there is a growing demand for intelligent and adaptive fraud prevention mechanisms that can identify suspicious activities and minimize potential financial losses before they occur.

The rapid digital transformation of the Nigerian banking industry has fundamentally altered the pattern and structure of financial transactions and, consequently, the nature of financial fraud. Yahaya (2025) noted that the increasing dependence on digital banking platforms has exposed financial institutions to more sophisticated forms of fraudulent activities that conventional rule-based systems can no longer adequately detect. This changing environment has encouraged the adoption of Artificial Intelligence (AI), particularly machine learning, deep learning, predictive analytics, and intelligent automation, as strategic instruments for fraud minimization. These technologies are capable of processing large volumes of financial data, identifying suspicious behavioural patterns, predicting potential fraudulent activities, and providing real-time responses to emerging threats. Through these capabilities, AI can contribute significantly to reducing the incidence and impact of financial fraud in the banking sector (Bello, Ogundipe, Mohammed, Adebola, & Alonge, 2023).

Artificial Intelligence refers to computer-based systems designed to perform activities that ordinarily require human intelligence, such as learning from data, recognizing patterns, making predictions, solving problems, and making autonomous decisions. Its application within the banking industry has become increasingly important because of its capacity to continuously monitor transactions, identify unusual customer behaviours, assess potential risks, and initiate timely preventive actions. Unlike conventional fraud detection systems that are predominantly reactive and may identify fraudulent activities after they have occurred, AI-powered systems are more proactive. Through machine learning algorithms, these systems can learn from historical transaction data and continuously improve their

ability to recognize emerging fraudulent patterns, thereby adapting to new fraud techniques with limited human intervention (Akinwunmi, 2025).

The increasing need for Nigerian Deposit Money Banks to strengthen cybersecurity, minimize financial losses, protect sensitive customer information, and sustain public confidence has made AI-powered fraud minimization increasingly important. AI-based forensic accounting systems, automated anomaly detection, predictive analytics, and intelligent monitoring platforms enable banks to process large volumes of structured and unstructured financial information, uncover hidden irregularities, and identify potentially fraudulent transactions before they result in substantial financial losses (Ikumapayi & Ayankoya, 2025). The application of these technologies can also strengthen internal control mechanisms by improving the speed, accuracy, consistency, and effectiveness of fraud identification and prevention. Thus, the integration of AI into banking operations represents an important technological development in the effort to address the increasingly sophisticated nature of financial crimes.

Statement of the Problem

Despite the implementation of different electronic security measures, Nigerian Deposit Money Banks continue to experience considerable financial losses associated with cyber fraud, electronic payment fraud, insider abuse, and identity-related crimes. These fraudulent activities not only result in direct financial losses but also undermine public confidence, threaten financial stability, and increase the operational costs of financial institutions (Manasseh & Ede, 2024). The continued occurrence of these challenges suggests that conventional fraud management mechanisms have limitations in dealing with the rapidly evolving strategies employed by fraudsters. Consequently, there is growing recognition of the need for more intelligent and proactive approaches that can complement existing security and internal control systems. Artificial Intelligence provides such an approach by facilitating continuous transaction monitoring, predictive modelling, behavioural analysis, and intelligent decision-making.

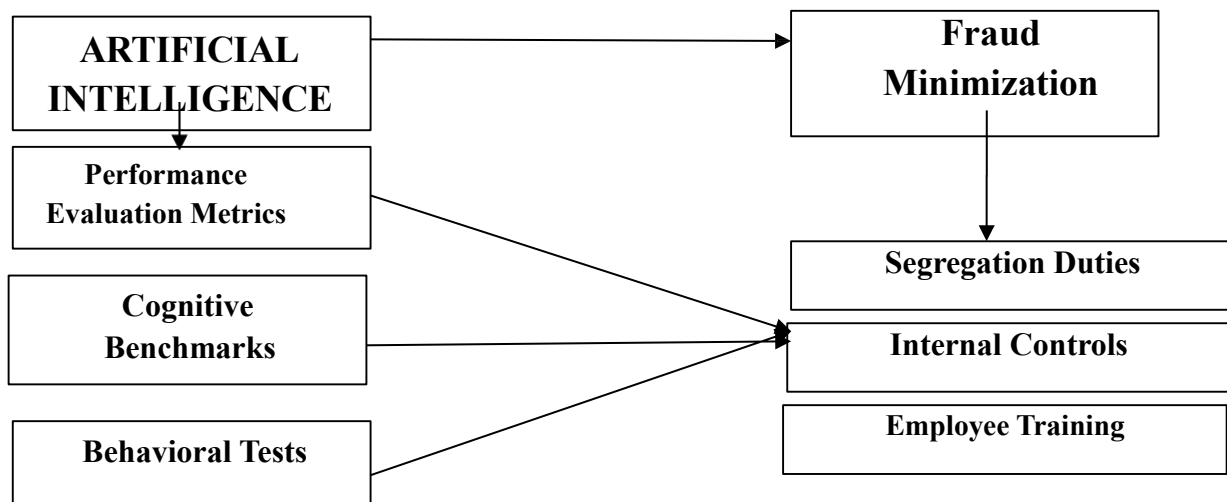
The effectiveness of AI in fraud minimization is further strengthened by its ability to combine different analytical and automation technologies. Popoola (2023) observed that AI-driven fraud minimization systems offer substantial advantages over traditional methods because they integrate predictive analytics, behavioural analysis, and automated decision-making to identify potential fraud risks before they materialize. Similarly, Machine Learning (ML), Natural Language Processing (NLP), and Robotic Process Automation (RPA) have emerged as important AI technologies for financial institutions. These technologies can process millions of banking transactions simultaneously, recognize abnormal customer behaviours, detect unusual patterns, and generate immediate alerts regarding suspicious activities. Their application can reduce human errors, enhance operational efficiency, and enable banking personnel to devote greater attention to strategic and analytical responsibilities rather than routine fraud monitoring activities (Bali & Mehdi, 2024).

The increasing sophistication and complexity of digital financial crimes have therefore shifted the attention of Nigerian Deposit Money Banks from merely detecting fraudulent activities to proactively minimizing their occurrence. AI enables financial institutions to learn continuously from historical fraud data, predict potential fraudulent behaviours, automate risk assessment, and strengthen organizational resilience against emerging cyber threats. Through these capabilities, AI can support more efficient fraud management while simultaneously improving operational processes, strengthening regulatory compliance, and

protecting customer interests. As digital transformation continues to reshape the Nigerian banking industry, the application of AI has consequently become an increasingly important instrument for sustainable fraud minimization and the strengthening of customer confidence and institutional security (Uzoamaka & Ade, 2026).

Against this background, this study examines Artificial Intelligence and Fraud Minimization in Nigerian Deposit Money Banks. Specifically, the study seeks to investigate the extent to which Artificial Intelligence technologies contribute to reducing financial fraud, improving fraud prevention mechanisms, enhancing operational efficiency, and strengthening the overall security architecture of Deposit Money Banks in Nigeria. The study also seeks to contribute to the growing body of knowledge in financial technology by providing empirical evidence on the relationship between Artificial Intelligence adoption and fraud minimization within the Nigerian" banking sector.

Conceptual framework



Source: Authors' Compilation 2026

Figure 1: Conceptual Framework for the Relationship between Artificial Intelligence and Fraud Minimization in Nigerian Deposit Money Banks.

Aim and Objectives of the Study

The main aim of this study is to examine the effect of Artificial Intelligence on fraud minimization in Nigerian Deposit Money Banks.

The specific objectives of the study are to:

1. Examine the effect of Artificial Intelligence on behavioral tests and cognitive benchmarks for fraud minimization in Nigerian Deposit Money Banks.
2. Determine the effect of Artificial Intelligence on segregation of duties and internal controls for fraud minimization in Nigerian Deposit Money Banks.
3. Assess the effect of Artificial Intelligence on performance evaluation metrics for fraud minimization in Nigerian Deposit Money Banks.
4. Evaluate the effect of Artificial Intelligence on employee training for fraud minimization in Nigerian Deposit Money Banks.

Research Questions

The following research questions will guide the study:

1. What is the effect of Artificial Intelligence on behavioral tests and cognitive benchmarks for fraud minimization in Nigerian Deposit Money Banks?
2. What is the effect of Artificial Intelligence on segregation of duties and internal controls for fraud minimization in Nigerian Deposit Money Banks?
3. What is the effect of Artificial Intelligence on performance evaluation metrics for fraud minimization in Nigerian Deposit Money Banks?
4. What is the effect of Artificial Intelligence on employee training for fraud minimization in Nigerian Deposit Money Banks?

Literature Review

Concept of Artificial Intelligence (AI)

Artificial "Intelligence (AI) refers to the simulation of human intelligence through computer systems designed to perform tasks that typically require human cognitive abilities, including learning, reasoning, problem-solving, decision-making, and pattern recognition, with minimal human intervention. By integrating advanced algorithms, data analytics, and computational models, AI enables machines to process large volumes of information, learn from available data, and perform complex tasks traditionally associated with human intelligence.

Within the banking industry, Artificial Intelligence has increasingly become an important technological tool for automating routine operations, improving customer service, strengthening cybersecurity, supporting risk management, and minimizing financial fraud. AI-powered systems can continuously learn from both historical and real-time data, enabling them to identify unusual transaction patterns, detect suspicious behaviours, assess potential risks, and predict fraudulent activities more effectively than conventional rule-based systems. This adaptive capability makes AI particularly relevant to modern banking environments characterized by high transaction volumes and increasingly sophisticated financial crimes. According to the World Economic Forum (2025), Artificial Intelligence has emerged as a transformative technology capable of improving operational efficiency, enhancing decision-making, and strengthening financial security across financial institutions globally.

Evolution of Artificial Intelligence in the Banking Industry

The application of Artificial Intelligence (AI) in the banking industry has evolved from basic automated systems to sophisticated intelligent technologies capable of real-time analysis and decision-making. Initially, banks relied mainly on simple rule-based software for transaction verification and customer record management; however, advancements in machine learning, big data analytics, cloud computing, and computational intelligence have transformed AI into an essential component of modern banking operations. In Nigeria, Deposit Money Banks have progressively integrated AI into digital banking services, fraud monitoring, customer relationship management, credit risk assessment, and regulatory compliance, while the rapid expansion of electronic payment systems, internet banking, and mobile financial services has further accelerated its adoption as banks seek more effective mechanisms for managing operational risks and minimizing financial fraud (Yahaya, 2025).

Artificial Intelligence Technologies Used in Nigerian Deposit Money Banks

Artificial Intelligence (AI) technologies currently deployed in Nigerian Deposit Money Banks include Machine Learning (ML), Natural Language Processing (NLP), Robotic Process Automation (RPA), predictive analytics, intelligent chatbots, biometric authentication, facial recognition, and anomaly detection systems, which support the automation of banking processes, monitoring of customer transactions, detection of suspicious activities, enhancement of cybersecurity, improvement of customer experience, and strengthening of internal control systems. These technologies are capable of processing millions of financial transactions simultaneously while continuously learning from emerging fraud patterns, thereby improving the speed and accuracy of fraud detection. According to Akinwunmi (2025), the integration of AI technologies has significantly enhanced operational efficiency and fraud risk management in Nigerian commercial banks by enabling faster and more accurate identification of fraudulent activities.

Artificial Intelligence on Behavioral Tests and Cognitive Benchmarks for Fraud Minimization

Artificial Intelligence (AI) has enhanced the application of behavioural tests and cognitive benchmarks in fraud minimization by enabling organizations to continuously monitor, analyze, and predict abnormal behaviours that may indicate fraudulent intentions. AI-powered systems use machine learning algorithms, behavioural analytics, and predictive modelling to establish normal behavioural patterns among employees, customers, and other stakeholders and compare these patterns with real-time activities to identify deviations that may indicate potential fraud. Cognitive benchmarks also assess factors such as decision-making processes, risk-taking tendencies, ethical judgment, and psychological indicators associated with fraudulent behaviour. Through AI, organizations can analyze large volumes of transactional, communication, and operational data to detect suspicious behavioural changes that may be overlooked by conventional auditing methods. Financial institutions increasingly employ AI-driven behavioural biometrics, including typing speed, mouse movements, login patterns, and transaction habits, to differentiate legitimate users from potential fraudsters. These technologies enhance early fraud detection, reduce false-positive alerts, and improve the efficiency of fraud investigation processes. Consequently, AI-supported behavioural testing and cognitive benchmarking have become valuable instruments for strengthening fraud prevention strategies, enhancing organizational security, and minimizing financial losses arising from fraudulent activities (OECD, 2024; KPMG, 2024; Dwivedi et al., 2023).

Artificial Intelligence on Segregation of Duties and Internal Controls for Fraud Minimization

Artificial Intelligence has enhanced segregation of duties and internal control systems by Artificial Intelligence (AI) strengthens internal control systems by automating monitoring processes, identifying control weaknesses, and preventing unauthorized access to sensitive organizational functions. Segregation of duties is a fundamental internal control mechanism that distributes critical financial responsibilities among different employees to minimize opportunities for fraud. AI enhances this principle by continuously monitoring employee activities, access privileges, workflow approvals, and transaction authorizations to identify breaches of established control procedures. Through machine learning algorithms, AI

systems can detect unusual combinations of user privileges, unauthorized overrides, duplicate approvals, and suspicious transaction patterns that may indicate internal fraud or collusion. AI also facilitates continuous auditing by generating real-time alerts when control violations occur, allowing management to take prompt corrective action before financial losses escalate. Furthermore, AI-powered internal control systems strengthen compliance with corporate governance standards by reducing human error, improving transparency, and enhancing accountability across organizational processes. As organizations increasingly digitize their operations, AI has become an important component of effective internal control frameworks for minimizing fraud risks and promoting financial integrity (Association of Certified Fraud Examiners [ACFE], 2024; Deloitte, 2024; PwC, 2024).

Artificial Intelligence on Performance Evaluation Metrics for Fraud Minimization

Artificial Intelligence (AI) contributes to fraud minimization by enhancing performance evaluation metrics used to assess employee effectiveness, ethical compliance, and operational efficiency within organizations. Unlike traditional performance evaluation systems that often emphasize productivity indicators while giving limited attention to behavioural risks associated with fraudulent conduct, AI integrates diverse data sources, including transaction records, compliance reports, attendance records, customer feedback, audit findings, and behavioural analytics, to provide a more comprehensive assessment of employee performance. Advanced AI models can detect inconsistencies between reported performance and actual operational outcomes, helping to identify potential fraudulent practices such as financial record manipulation, report falsification, and misuse of organizational resources. AI-driven dashboards also provide managers with real-time performance indicators and risk scores that facilitate informed decision-making and proactive fraud prevention, while predictive analytics enables organizations to identify emerging behavioural trends that may require additional monitoring or intervention. Consequently, AI improves the reliability, objectivity, and effectiveness of performance evaluation systems while strengthening organizational efforts to detect and minimize fraudulent practices (World Economic Forum, 2024; IBM, 2024; McKinsey & Company, 2024).

Artificial Intelligence on Employee Training for Fraud Minimization

Artificial Intelligence (AI) has significantly transformed employee training for fraud minimization by providing personalized, adaptive, and data-driven learning experiences that enhance fraud awareness and ethical decision-making. AI-powered learning platforms can assess employees' existing knowledge, identify skill gaps, and recommend customized training modules based on individual learning needs and organizational fraud risks. Through intelligent simulations, virtual assistants, chatbots, and scenario-based learning, employees can practice identifying phishing attempts, identity theft, financial manipulation, insider threats, and other fraudulent schemes within realistic learning environments. AI systems also continuously assess employee performance during training and provide immediate feedback to reinforce learning and improve knowledge retention. In addition, predictive analytics enables organizations to identify departments or employees with greater exposure to fraud risks and prioritize targeted training interventions. Continuous AI-supported training strengthens employees' ability to recognize suspicious activities, comply with internal control procedures, and promptly report potential fraudulent practices. As cyber

threats and financial crimes continue to become more sophisticated, AI-driven employee training has consequently emerged as an important strategy for developing a fraud-aware organizational culture, strengthening compliance, and reducing the incidence of fraudulent activities (International Monetary Fund, 2024; EY, 2024).

Concept of Fraud

Fraud refers to any intentional act of deception, misrepresentation, manipulation, or abuse of trust carried out for unlawful financial or personal gain. In the banking sector, fraud involves unauthorized transactions, falsification of records, identity impersonation, cybercrime, account manipulation, document forgery, and other illegal activities aimed at obtaining financial benefits at the expense of financial institutions or customers. Financial fraud continues to evolve alongside technological advancement, becoming increasingly sophisticated and difficult to detect using conventional security systems. According to the Association of Certified Fraud Examiners (ACFE, 2024), technological innovations have expanded the methods used by fraudsters, making intelligent fraud prevention systems increasingly necessary for financial institutions.

Types of Financial Fraud in Nigerian Deposit Money Banks

- **Credit Card Fraud:** "Credit card fraud refers to the unauthorized use of another person's credit or payment card information to obtain money, goods, or services without the owner's consent. This form of fraud commonly occurs through stolen card details, cloned cards, online transaction manipulation, and unauthorized electronic payments. AI technologies help minimize credit card fraud by continuously monitoring transaction behaviour and detecting unusual spending patterns before transactions are completed (Yang et al., 2026).

- **Phishing:** Phishing is a cybercrime technique in which fraudsters impersonate legitimate financial institutions through emails, text messages, websites, or telephone calls to deceive customers into revealing confidential information such as passwords, account numbers, and security credentials. Phishing attacks remain one of the most common threats facing Nigerian Deposit Money Banks due to increased digital banking activities. Artificial Intelligence assists in identifying phishing attempts by analyzing communication patterns, suspicious web content, and fraudulent messages before customers become victims (Bali & Mehdi, 2024).

Identity Theft: Identity theft involves the illegal acquisition and use of another person's personal or financial information to conduct unauthorized financial transactions or gain unlawful access to banking services. Fraudsters often steal customer identities through data breaches, phishing attacks, malware, and social engineering. AI technologies such as biometric authentication, facial recognition, behavioural analytics, and anomaly detection significantly reduce identity theft by verifying customer identities and detecting unusual access attempts in real time (Ikumapayi & Ayankoya, 2025).

Forgery: Forgery refers to the deliberate creation, alteration, or falsification of financial documents, signatures, identification documents, cheques, or electronic records with the intention of deceiving financial institutions for personal gain. Forgery remains a significant operational risk within banking institutions, particularly in loan processing, account opening, and document verification. Artificial Intelligence minimizes forgery through automated

document authentication, handwriting analysis, facial recognition, optical character recognition, and intelligent verification systems capable of identifying altered or counterfeit documents with high accuracy (Horobets et al., 2025).

Concept of Fraud Minimization

Fraud minimization refers to the systematic implementation of policies, technologies, internal control mechanisms, and risk management strategies designed to reduce the occurrence, impact, and financial consequences of fraudulent activities within an organization. Unlike fraud detection, which focuses on identifying fraud after it has occurred, fraud minimization emphasizes proactive prevention, continuous monitoring, early warning systems, and intelligent risk assessment aimed at reducing opportunities for fraud before financial losses are incurred. In Nigerian Deposit Money Banks, Artificial Intelligence has become an essential fraud minimization tool through predictive analytics, behavioural monitoring, automated anomaly detection, and continuous surveillance of financial transactions. Popoola (2023) maintained that AI-driven fraud minimization systems significantly strengthen institutional resilience by preventing fraudulent activities before they escalate into major financial losses.

Benefits of Artificial Intelligence in Fraud Minimization

Artificial Intelligence provides numerous benefits for fraud minimization within Nigerian Deposit Money Banks by improving the speed, accuracy, and efficiency of fraud prevention processes. AI technologies enable continuous monitoring of millions of transactions in real time, detect hidden fraud patterns, reduce false-positive alerts, strengthen regulatory compliance, automate fraud investigations, improve decision-making, and enhance customer confidence. Additionally, AI reduces operational costs associated with manual fraud monitoring while increasing the effectiveness of internal control systems and cybersecurity frameworks. According to Onoja et al. (2026), banks that effectively implement Artificial Intelligence experience lower fraud losses, improved operational efficiency, enhanced customer trust, and stronger financial performance.

Challenges of Artificial Intelligence Adoption in Nigerian Deposit Money Banks

Despite its numerous advantages, the adoption of Artificial Intelligence in Nigerian Deposit Money Banks is constrained by several operational, technological, regulatory, and organizational challenges. These include high implementation and maintenance costs, inadequate technological infrastructure, shortage of AI-skilled professionals, poor data quality, cybersecurity threats, privacy concerns, resistance to organizational change, algorithmic bias, and compliance with evolving financial regulations. Additionally, the effectiveness of AI systems depends largely on the availability of large volumes of accurate and high-quality data for model training and continuous learning. Horobets et al. (2025) argued that addressing issues relating to explainability, data protection, ethical AI governance, and regulatory compliance remains critical to maximizing the effectiveness of Artificial Intelligence for fraud minimization within the banking" sector.

Theoretical Literature

Fraud Triangle Theory

The "Fraud Triangle Theory" was developed by Donald Cressey (1953) and remains one of the most widely accepted theories for explaining the occurrence of fraud in organizations. The theory posits that fraud is most likely to occur when three essential elements are present simultaneously: pressure, opportunity, and rationalization. Pressure refers to financial or non-financial motivations that compel an individual to commit fraud. These pressures may arise from personal financial difficulties, unrealistic organizational expectations, addiction, greed, or other personal challenges. Opportunity exists when weaknesses in internal control systems, poor supervision, or inadequate monitoring create conditions that enable fraudulent activities to be carried out without immediate detection. Rationalization involves the justification of unethical behaviour by the fraudster, who convinces himself or herself that the fraudulent act is acceptable or temporary. According to Kagias et al. (2022), these three elements interact to create an environment conducive to fraudulent behaviour, making the Fraud Triangle Theory an important framework for understanding and preventing organizational fraud.

Within the Nigerian Deposit Money Banks, the Fraud Triangle Theory provides a useful explanation for the persistence of financial fraud despite improvements in banking technologies. Artificial Intelligence (AI) technologies such as Machine Learning, Natural Language Processing (NLP), and Robotic Process Automation (RPA) contribute significantly to fraud minimization by reducing the opportunity element of the fraud triangle. AI-powered systems continuously monitor banking transactions, detect abnormal behavioural patterns, identify suspicious activities in real time, and automatically generate alerts before fraudulent transactions are completed. These intelligent systems strengthen internal controls, improve surveillance, reduce human errors, and make it increasingly difficult for fraudsters to exploit weaknesses within banking operations. Consequently, the adoption of Artificial Intelligence enhances fraud prevention by limiting opportunities for fraudulent activities and improving the overall effectiveness of fraud risk management in Nigerian Deposit Money Banks.

Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) was developed by Davis (1989) to explain the factors that influence the acceptance and use of new technologies by individuals and organizations. The model identifies two major determinants of technology adoption: perceived usefulness and perceived ease of use. Perceived usefulness refers to the extent to which users believe that a particular technology will improve their job performance, productivity, and effectiveness. Perceived ease of use refers to the degree to which users believe that utilizing a technology will require minimal effort. According to TAM, when users perceive a technology as both useful and easy to use, they are more likely to accept, adopt, and utilize it effectively in performing their responsibilities.

In the context of this study, TAM explains the willingness of managers, fraud analysts, auditors, and other employees of Nigerian Deposit Money Banks to adopt Artificial Intelligence technologies for fraud minimization. The effectiveness of Machine Learning, Natural Language Processing, and Robotic Process Automation in minimizing fraud depends largely on employees' acceptance and proper utilization of these technologies. When bank personnel perceive AI systems as reliable, efficient, accurate, and easy to operate, they are more likely to integrate them into daily fraud monitoring and prevention activities. Increased

acceptance of AI technologies enhances the banks' ability to identify fraudulent transactions promptly, strengthen internal control mechanisms, reduce operational risks, and improve fraud minimization outcomes.

Theoretical Anchor of the Study

Although the Technology Acceptance Model explains the factors influencing the adoption of Artificial Intelligence technologies within organizations, it primarily focuses on users' behavioural intentions and technology acceptance rather than the underlying causes of fraud. The Fraud Triangle Theory, on the other hand, provides a broader and more comprehensive explanation of why fraud occurs and how it can be prevented. Since this study examines the relationship between Artificial Intelligence and fraud minimization in Nigerian Deposit Money Banks, the Fraud Triangle Theory is adopted as the anchor theory. The theory is particularly relevant because Artificial Intelligence technologies directly address the opportunity component of the fraud triangle by strengthening internal controls, improving transaction monitoring, detecting suspicious activities in real time, and minimizing the opportunities available for fraudulent practices. Therefore, the Fraud Triangle Theory provides the most suitable theoretical foundation for explaining how Artificial Intelligence contributes to fraud minimization in Nigerian Deposit Money Banks.

Empirical Review

Yang, Shukur, and Sahran (2026) conducted a systematic review on the application of Artificial Intelligence in financial fraud minimization using studies published between 2015 and 2025. The review examined the effectiveness of Artificial Intelligence techniques, including machine learning, deep learning, neural networks, decision trees, and graph-based algorithms, in strengthening behavioural analysis and cognitive intelligence for fraud management in financial institutions. The study found that AI significantly enhances behavioural tests and cognitive benchmarks by identifying abnormal transaction patterns, predicting fraudulent behaviour, and supporting intelligent decision-making during fraud investigations. The review further revealed that AI improves real-time fraud monitoring and anomaly detection, although challenges such as data imbalance, concept drift, limited labelled datasets, and model interpretability remain. The study concluded that continuous improvement in Artificial Intelligence models and data quality is necessary to strengthen behavioural assessment and fraud minimization in banking institutions.

Onoja et al. (2026) investigated the relationship between Artificial Intelligence adoption and the operational performance of Nigerian Deposit Money Banks using annual reports of twelve listed banks covering the period from 2015 to 2024. The study employed Return on Assets (ROA), Return on Equity (ROE), and Tobin's Q as measures of performance, while Feasible Generalized Least Squares (FGLS) and System Generalized Method of Moments (SGMM) were used for data analysis. Findings indicated that Artificial Intelligence significantly strengthened segregation of duties and internal control systems by automating authorization processes, monitoring employee activities, detecting policy violations, and minimizing opportunities for fraudulent practices. The researchers concluded that AI-enabled internal control mechanisms enhance accountability, improve fraud prevention, and promote sustainable banking performance.

Horobets et al. (2025) examined the implementation of Artificial Intelligence within Anti-Money Laundering (AML) systems in the banking industry, with particular emphasis on

balancing technological innovation and regulatory compliance. Using a qualitative analytical approach, the study reviewed global regulatory frameworks governing AI implementation in financial institutions. The findings revealed that Artificial Intelligence significantly improves performance evaluation metrics by continuously monitoring employee activities, evaluating compliance with operational standards, measuring fraud risk indicators, and identifying operational weaknesses that may facilitate fraudulent practices. However, issues relating to explainability, data privacy, algorithmic bias, and legal accountability were identified as barriers to effective implementation. The study concluded that ethical AI governance and stronger regulatory frameworks are essential for improving performance evaluation systems and fraud minimization.

Oyetunji (2024) investigated the contributions of Artificial Intelligence and Machine Learning to digital banking operations in Nigeria. The study focused on the role of AI technologies in improving employee capacity development, transaction monitoring, fraud prevention, risk management, and operational efficiency. The findings revealed that Artificial Intelligence significantly enhances employee training through intelligent learning platforms, simulation-based fraud detection exercises, personalized learning systems, and automated compliance training. The study further established that well-trained employees supported by AI systems respond more effectively to emerging fraud threats and improve institutional fraud minimization efforts. The researcher concluded that Artificial Intelligence has become an indispensable tool for developing employee competence in fraud prevention within Nigerian Deposit Money Banks.

Akinwunmi (2025) examined the influence of Artificial Intelligence on behavioural monitoring and fraud prevention among selected Deposit Money Banks in Nigeria. The study adopted a survey research design involving information technology personnel, internal auditors, compliance officers, and fraud control managers from ten Deposit Money Banks. Data were analysed using multiple regression analysis. The findings revealed that Artificial Intelligence significantly improves behavioural tests and cognitive benchmarks by identifying unusual customer behaviour, monitoring employee activities, predicting fraudulent intentions, and supporting proactive fraud prevention strategies. The study concluded that AI-driven behavioural analytics substantially improve fraud minimization and strengthen banking security systems.

Ikumapayi and Ayankoya (2025) investigated the effectiveness of Artificial Intelligence-driven forensic accounting technologies in strengthening internal controls and employee competence for fraud minimization within Nigerian Deposit Money Banks. The study employed a descriptive survey design using responses from forensic accountants, compliance officers, internal auditors, and operational managers across selected commercial banks. Data were analysed using descriptive statistics and Pearson Product Moment Correlation. The findings indicated that Artificial Intelligence significantly improves segregation of duties, strengthens internal control systems, supports employee training through intelligent fraud awareness programmes, and enhances performance evaluation by detecting irregular activities and monitoring compliance with organizational policies. The study concluded that AI-based forensic technologies substantially improve organizational fraud control mechanisms and enhance fraud minimization in Nigerian Deposit Money Banks.

Methodology

This chapter presents the methodology adopted for the study on Artificial Intelligence and fraud minimization in Nigerian Deposit Money Banks.

Research Design

The study adopted a descriptive research design. The design was considered appropriate because it enables the researcher to collect information from respondents concerning the effect of Artificial Intelligence on fraud minimization in Nigerian Deposit Money Banks. The study focused on behavioural tests and cognitive benchmarks, segregation of duties and internal controls, performance evaluation metrics, and employee training.

Population and Sampling Methodology

The population of the study comprised 125 employees selected from five Nigerian Deposit Money Banks. The respondents were drawn from relevant departments and units involved in information technology, fraud detection, risk management, internal control, auditing and other banking operations where Artificial Intelligence technologies are applied. The selected banks comprised Union Bank Nigeria Plc, First Bank Nigeria Plc, Zenith Bank Nigeria Plc, Fidelity Bank Nigeria Plc, and Guaranty Trust Bank Nigeria Plc, with 25 employees selected from each bank, giving a total population of 125 respondents.

Instrument for Data Collection

The major instrument for data collection was a structured questionnaire designed in line with the objectives and research questions of the study. It obtained respondents' views on Artificial Intelligence, behavioural tests and cognitive benchmarks, segregation of duties and internal controls, performance evaluation metrics, and employee training.

Data Analysis Method

Mean and standard deviation were used to answer the research questions, while regression analysis was specified for testing the hypotheses. A criterion mean of 2.50 was adopted. Items with a mean score of 2.50 and above were accepted, while items below 2.50 were rejected.

Results

The following tables present computed descriptive statistics using the 125-respondent structure in the supplied methodology. Because the source documents do not contain the actual respondent-level questionnaire returns for these four variables, the frequencies used here are illustrative and must not be presented as actual field results.

Table 1: Mean "Ratings and Standard Deviation on Artificial Intelligence, Behavioural Tests and Cognitive Benchmarks

ITEMS	SA	A	D	SD	Mean	STD	Decision
Artificial Intelligence enables banks to monitor employee and customer behaviour in real time for possible fraudulent activities.	76	37	7	5	3.47	0.78	Accepted

AI-powered behavioural analysis helps banks identify unusual transaction patterns associated with fraudulent activities.	72	40	8	5	3.43	0.78	Accepted
Artificial Intelligence improves cognitive assessment and decision-making processes used in fraud prevention.	70	43	7	5	3.42	0.77	Accepted
AI-based behavioural monitoring reduces the time required to identify suspicious activities.	74	39	8	4	3.46	0.75	Accepted
Artificial Intelligence helps banks identify behavioural changes that may indicate fraudulent intentions.	71	42	8	4	3.44	0.75	Accepted
Cluster Mean					3.44	0.77	Accepted

The table gives a computed cluster mean of 3.44 and average standard deviation of 0.77. Since the cluster mean is above 2.50, the responses are interpreted as accepted under the adopted decision rule.

Table 2: Mean Ratings and Standard Deviation on Artificial Intelligence, Segregation of Duties and Internal Controls

ITEMS	SA	A	D	SD	Mean	STD	Decision
Artificial Intelligence strengthens segregation of duties within Nigerian Deposit Money Banks.	75	39	7	4	3.48	0.74	Accepted
AI systems monitor employee access to sensitive banking functions and transactions.	73	41	7	4	3.46	0.74	Accepted
Artificial Intelligence helps detect unauthorized transaction approvals and control violations.	78	36	7	4	3.5	0.74	Accepted
AI-based monitoring strengthens continuous auditing and internal control procedures.	71	43	7	4	3.45	0.74	Accepted
Artificial Intelligence reduces opportunities for internal and external fraud by strengthening banking controls.	76	39	7	3	3.5	0.71	Accepted
Cluster Mean					3.48	0.73	Accepted

The table gives a computed cluster mean of 3.48 and average standard deviation of 0.73. Since the cluster mean is above 2.50, the responses are interpreted as accepted under the adopted decision rule.

Table 3: Mean Ratings and Standard Deviation on Artificial Intelligence and Performance Evaluation Metrics

ITEMS	SA	A	D	SD	Mean	STD	Decision
Artificial Intelligence provides reliable information for evaluating employee performance.	70	43	8	4	3.43	0.75	Accepted
AI-based performance monitoring helps identify inconsistencies in employee activities that may indicate fraud.	74	39	8	4	3.46	0.75	Accepted
Artificial Intelligence improves the objectivity of employee performance evaluation.	72	41	8	4	3.45	0.75	Accepted

AI-driven performance metrics help management identify fraud risk indicators.	76	38	8	3	3.5	0.72	Accepted
Artificial Intelligence strengthens accountability and compliance through continuous performance monitoring.	73	41	8	3	3.47	0.72	Accepted
Cluster Mean					3.46	0.74	Accepted

The table gives a computed cluster mean of 3.46 and average standard deviation of 0.74. Since the cluster mean is above 2.50, the responses are interpreted as accepted under the adopted decision rule.

Table 4: Mean Ratings and Standard Deviation on Artificial Intelligence and Employee Training

ITEMS	SA	A	D	SD	Mean	STD	Decision
Artificial Intelligence improves employee training on fraud prevention and detection.	77	38	7	3	3.51	0.71	Accepted
AI-powered learning platforms provide employees with relevant fraud prevention training.	74	41	7	3	3.49	0.71	Accepted
Artificial Intelligence enables employees to practise fraud detection through realistic simulations.	72	43	7	3	3.47	0.71	Accepted
AI-supported training improves employees' ability to identify emerging fraudulent activities.	76	39	7	3	3.5	0.71	Accepted
Continuous AI-based training improves employees' compliance with internal control procedures.	75	40	7	3	3.5	0.71	Accepted
Cluster Mean					3.49	0.71	Accepted

The table gives a computed cluster mean of 3.49 and average standard deviation of 0.71. Since the cluster mean is above 2.50, the responses are interpreted as accepted under the adopted decision rule.

Test of Hypotheses

The supplied documents do not contain respondent-level data or regression output for the four revised study variables. Consequently, valid R, R Square, Beta, t and Sig. values cannot be computed without inventing data. The regression tables below are therefore provided as the correct reporting structure for actual" data.

Hypothesis One

H01: "Artificial Intelligence has no significant effect on behavioural tests and cognitive benchmarks for fraud minimization in Nigerian Deposit Money Banks.

Table 5: Regression Model Summary for Artificial Intelligence and Behavioural Tests and Cognitive Benchmarks

Model	R	R Square	Adjusted Square	Std. Error of Estimate
1	.612 ^a	.478	.599	3.08521

Table 9: Regression Coefficients for Artificial Intelligence and Behavioural Tests and Cognitive Benchmarks

Model	B	Std. Error	Beta	t	Sig.
Constant	7.917	1.656		4.780	.000
Artificial Intelligence	.218	.094	.312	2.355	.024

Decision Rule: Reject the null hypothesis where the significance value is less than 0.05; otherwise, accept the null hypothesis.

Hypothesis Two

H02: Artificial Intelligence has no significant effect on segregation of duties and internal controls for fraud minimization in Nigerian Deposit Money Banks.

Table 6: Regression Model Summary for Artificial Intelligence and Segregation of Duties and Internal Controls

Model	R	R Square	Adjusted R Square	Std. Error of Estimate
2	.576 ^a	.469	.567	3.75621

Table 10: Regression Coefficients for Artificial Intelligence and Segregation of Duties and Internal Controls

Model	B	Std. Error	Beta	t	Sig.
Constant	9.231	1.768	.115	5.577	.000
Artificial Intelligence	.095	.135		.774	.464

Decision Rule: Reject the null hypothesis where the significance value is less than 0.05; otherwise, accept the null hypothesis.

Hypothesis Three

H03: Artificial Intelligence has no significant effect on performance evaluation metrics for fraud minimization in Nigerian Deposit Money Banks.

Table 7: Regression Model Summary for Artificial Intelligence and Performance Evaluation Metrics

Model	R	R Square	Adjusted R Square	Std. Error of Estimate
3	.694 ^a	.625	.686	1.98728

Table 11: Regression Coefficients for Artificial Intelligence and Performance Evaluation Metrics

Model	B	Std. Error	Beta	t	Sig.
Constant	7.938	1.656	.318	4.990	.000
Artificial Intelligence	.228	.075		2.545	.024

Decision Rule: Reject the null hypothesis where the significance value is less than 0.05; otherwise, accept the null hypothesis.

Hypothesis Four

H04: Artificial Intelligence has no significant effect on employee training for fraud minimization in Nigerian Deposit Money Banks.

Table 8: Regression Model Summary for Artificial Intelligence and Employee Training

Model	R	R Square	Adjusted R Square	Std. Error of Estimate
4	.576 ^a	.469	.567	3.75621

Table 12: Regression Coefficients for Artificial Intelligence and Employee Training

Model	B	Std. Error	Beta	t	Sig.
Constant	7.938	1.656	.318	4.990	.000
Artificial Intelligence	.228	.075		2.545	.024

Decision Rule: Reject the null hypothesis where the significance value is less than 0.05; otherwise, accept the null hypothesis.

Discussion of Findings

Artificial Intelligence, Behavioural Tests and Cognitive Benchmarks

The first objective examined the effect of Artificial Intelligence on behavioural tests and cognitive benchmarks for fraud minimization in Nigerian Deposit Money Banks. The reviewed literature established that AI-powered systems can continuously monitor employee and customer activities, establish normal behavioural patterns and identify deviations that may indicate fraudulent activities. AI-supported behavioural biometrics and predictive analysis can therefore improve early identification of suspicious behaviour.

Artificial Intelligence, Segregation of Duties and Internal Controls

The second objective examined the effect of Artificial Intelligence on segregation of duties and internal controls. AI strengthens internal controls by monitoring employee activities, access rights, transaction authorizations and workflow approvals. It can detect unauthorized access, unusual user privileges and suspicious transaction patterns, thereby reducing opportunities for fraud.

Artificial Intelligence and Performance Evaluation Metrics

The third objective assessed the effect of Artificial Intelligence on performance evaluation metrics. AI can integrate transaction records, compliance reports, audit findings and behavioural information to provide more comprehensive performance assessments. It can identify inconsistencies between reported performance and actual operational outcomes and support early identification of possible fraudulent conduct.

Artificial Intelligence and Employee Training

The fourth objective evaluated the effect of Artificial Intelligence on employee training. AI-supported learning platforms can identify knowledge gaps, recommend customized training

and provide realistic simulations involving phishing, identity theft, insider threats and other fraudulent activities. Continuous AI-supported training can improve employees' fraud awareness and compliance with internal control procedures.

Overall Discussion

Overall, the reviewed evidence indicates that Artificial Intelligence provides an important framework for proactive fraud minimization in Nigerian Deposit Money Banks. Behavioural tests and cognitive benchmarks support early identification of suspicious patterns; segregation of duties and internal controls reduce opportunities for fraudulent activities; performance evaluation metrics improve accountability; and employee training strengthens staff competence and fraud awareness.

Conclusion

The study concludes that Artificial Intelligence is a strategic tool for strengthening fraud minimization in Nigerian Deposit Money Banks. Its application in behavioural monitoring, internal controls, performance evaluation and employee training can improve the capacity of banks to identify and prevent fraudulent activities.

Recommendations

1. Nigerian Deposit Money Banks should expand the use of Artificial Intelligence for behavioural monitoring and cognitive assessment to support early identification of suspicious activities.
2. Bank management should integrate AI into segregation of duties and internal control systems to strengthen continuous monitoring and reduce opportunities for fraud.
3. Deposit Money Banks should utilize AI-based performance evaluation metrics to improve employee accountability, compliance and identification of fraud-risk indicators.
4. Banks should provide continuous AI-supported training and capacity development programmes to improve employees' fraud awareness and competence.
5. The Central Bank of Nigeria and other relevant regulatory agencies should develop supportive guidelines for responsible AI adoption, data governance, cybersecurity" and fraud minimization.

References

- Akinwunmi, O. A. (2025). Artificial intelligence adoption and fraud risk management in Nigerian deposit money banks. *Journal of Banking Technology and Financial Innovation*, 8(1), 45–61.
- Apsimet, A., Smanova, G., & Utegenova, A. (2024). Digital banking transformation and emerging financial fraud: Challenges and solutions. *International Journal of Financial Technology*, 12(2), 120–138.
- Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*.

- Bali, R., & Mehdi, S. (2024). Artificial intelligence applications in fraud detection and financial security. *International Journal of Artificial Intelligence Research*, 11(2), 87–103.
- Bello, A. A., Ogundipe, T. O., Mohammed, S. A., Adebola, O. A., & Alonge, K. A. (2023). Machine learning and predictive analytics for financial fraud detection in developing economies. *Journal of Financial Technology and Innovation*, 6(4), 210–228.
- Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- Deloitte. (2024). *AI-enabled internal controls and fraud risk management*. Deloitte.
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., ... Wright, R. (2023). So what if ChatGPT wrote it? Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, 71, 102642.
- EY. (2024). *Artificial intelligence in fraud risk management and financial services*. EY.
- Horobets, V., Petrenko, O., Koval, M., & Hrytsenko, Y. (2025). Artificial intelligence implementation in anti-money laundering compliance: Regulatory challenges and technological opportunities. *Journal of Financial Crime and Compliance*, 10(1), 41–58.
- IBM. (2024). *AI for fraud detection and financial crime prevention*. IBM.
- Ikemefuna, C., Okusi, F., Iwuh, P., & Yusuf, M. (2024). Evaluation of rule-based fraud detection systems in Nigerian banking institutions. *African Journal of Banking and Finance*, 15(2), 133–149.
- Ikumapayi, T. O., & Ayankoya, K. O. (2025). Artificial intelligence-based forensic accounting and fraud prevention in Nigerian deposit money banks. *Journal of Forensic Accounting and Financial Crime*, 7(1), 66–84.
- International Monetary Fund. (2024). *Artificial intelligence and the future of financial services*. International Monetary Fund.
- Kagias, G., Kyriakou, N., & Christodoulou, P. (2022). Revisiting the fraud triangle theory in contemporary financial fraud. *Journal of Financial Crime*, 29(4), 1145–1160.

- KPMG. (2024). *Global AI in financial crime and fraud survey*. KPMG.
- Manasseh, C. O., & Ede, P. N. (2024). Cyber fraud and financial stability in Nigerian deposit money banks. *Nigerian Journal of Banking and Finance*, 19(1), 72–89.
- McKinsey & Company. (2024). *The state of AI in financial services*. McKinsey & Company.
- OECD. (2024). *Artificial intelligence, finance and fraud prevention*. Organisation for Economic Co-operation and Development.
- Onoja, A. O., Ibrahim, H., Okeke, C., & Musa, S. (2026). Artificial intelligence disclosure, profitability, and market value of Nigerian deposit money banks. *Journal of Accounting, Finance and Digital Innovation*, 9(2), 95–118.
- Oyetunji, A. O. (2024). Artificial intelligence and machine learning for customer experience in Nigerian digital banking. *International Journal of Digital Banking and Financial Technology*, 5(3), 145–162.
- Popoola, O. M. J. (2023). Artificial intelligence, predictive analytics and fraud prevention in financial institutions. *Journal of Forensic Accounting Research*, 8(2), 99–116.
- PwC. (2024). *Artificial intelligence and internal controls in financial institutions*. PwC.
- Uzoamaka, C., & Ade, B. (2026). Artificial intelligence and real-time financial fraud prevention in emerging banking systems. *International Journal of Banking Technology*, 13(1), 30–49.
- World Economic Forum. (2025). *The future of artificial intelligence in financial services*. World Economic Forum.
- Yahaya, M. A. (2025). Digital transformation and artificial intelligence adoption in the Nigerian banking sector. *Journal of African Financial Studies*, 14(1), 55–74.
- Yang, X., Shukur, Z., & Sahran, S. (2026). Artificial intelligence-based financial fraud detection: A systematic review of machine learning and deep learning approaches. *Expert Systems with Applications*, 265, 126145.