Yamtara-Wala Journal of Arts, Management and Social Sciences (YAJAMSS)
Volume 8 Issue 3 June, 2026

AI-DRIVEN FRAUD DETECTION AND CYBER FRAUD MITIGATION IN NIGERIAN DEPOSIT MONEY BANKS

[1]Abubakar Ado Adamu, [2]Mohammed Nura Ibrahim Naala and [3]Abubakar Umar

[1]Kaduna State University, KASU, Kaduna
[2]Ahmadu Bello University, Zaria
[3]Al-Qalam University, Katsina
wadadanlami@gmail.com abubakar.ado@kasu.edu.ng

Abstract

This study examines the role of AI-driven fraud detection systems in mitigating cyber fraud in Nigerian deposit money banks. Specifically, the study investigates the effects of AI fraud detection capability, predictive analytics capability, automated transaction monitoring systems, and FinTech digital infrastructure on cyber fraud mitigation. The study adopted a survey research design and collected data from banking professionals working in fraud risk management, internal control, digital banking operations, and information technology security departments of selected deposit money banks in Nigeria. A total of 123 questionnaires were distributed, out of which 102 were properly completed and used for analysis, representing a response rate of 82.6%. The data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The model explained 73.2% of the variance in cyber fraud mitigation, indicating strong predictive power. The findings revealed that AI fraud detection capability had a significant positive effect on cyber fraud mitigation. Predictive analytics capability also significantly influenced cyber fraud mitigation. Similarly, automated transaction monitoring systems had a significant positive effect on cyber fraud mitigation. FinTech digital infrastructure recorded the strongest effect on cyber fraud mitigation. The study concludes that AI technologies, predictive analytics, automated monitoring systems, and robust FinTech infrastructure significantly enhance banks' capacity to detect, prevent, and manage cyber fraud in digital banking environments. The study recommends increased investment in AI-based fraud detection systems, improved FinTech infrastructure, automated transaction monitoring, and stronger cybersecurity frameworks.

Keywords: Artificial Intelligence, Fraud Detection Systems, Digital Banking, Deposit Money Banks, Nigeria.

1.0 Introduction

The global financial system has experienced significant transformation in recent years due to the rapid development of financial technology (FinTech), which integrates advanced digital technologies into traditional financial services. FinTech innovations such as mobile banking, digital payment systems, blockchain platforms, and artificial intelligence (AI) have fundamentally reshaped the way financial services are delivered and accessed (Hasan et al., 2024; Yamsani et al., 2025; Wembe, 2025). These technologies have improved financial efficiency, expanded financial inclusion, and enhanced transaction speed across global financial markets. The integration of AI and predictive analytics

into financial systems has further enabled banks to automate operational processes, analyze large volumes of financial data, and improve decision-making capabilities (Dodda, 2025; Hamdouni, 2025). Consequently, FinTech has emerged as a major driver of financial sector modernization and economic development in both developed and emerging economies (Hasan et al., 2024; Dodda, 2025; Chuang & Shrestha, 2025; Shahid et al., 2025).

Despite the numerous benefits associated with FinTech adoption, the rapid digitalization of financial services has also increased exposure to cyber threats and financial fraud. As banking operations increasingly migrate to online platforms, cybercriminals have developed more sophisticated techniques for exploiting vulnerabilities within digital financial systems (Onwuegbuchi et al., 2023; Khatiwada, 2024). Cyber fraud has therefore become one of the most critical challenges confronting modern banking institutions worldwide. Fraudulent activities such as phishing attacks, identity theft, unauthorized transactions, card fraud, and digital payment manipulation continue to undermine the security of online financial systems and pose significant risks to financial institutions and customers (Akinwale et al., 2022; Folami et al., 2024). These emerging threats highlight the limitations of conventional fraud detection mechanisms that rely primarily on manual monitoring and rule-based systems (Ali et al., 2022; Khatib, 2024; Onwuegbuchi et al., 2023).

In developing economies such as Nigeria, the expansion of digital banking and FinTech services has increased rapidly due to growing internet penetration, mobile technology adoption, and government initiatives aimed at promoting financial inclusion. Nigerian deposit money banks have invested heavily in digital banking platforms such as mobile banking applications, internet banking services, automated teller machines, and electronic payment channels (Adeyemo & Obafemi, 2024; Agbeyinka, 2025). These technologies have significantly improved banking accessibility and transaction convenience for customers (Wembe, 2025; Yamsani et al., 2025). However, the rapid growth of digital financial services has also exposed the Nigerian banking system to increasing cyber fraud incidents, including electronic payment fraud, ATM fraud, online banking fraud, and digital identity theft. Reports indicate that cyber fraud remains a major threat to financial system stability and continues to cause significant financial losses to banks and customers in Nigeria (Adeyemo & Obafemi, 2024; Agbeyinka, 2025; Folami et al., 2024; Imade & Evbayiro-Osagie, 2025).

In response to the increasing complexity of digital financial crimes, financial institutions are adopting advanced technological solutions to strengthen fraud detection and cybersecurity frameworks. Artificial intelligence has become a key technological innovation in modern fraud detection systems due to its ability to analyze large volumes of transactional data and detect suspicious patterns in real time (Abi, 2025; Alahmad et al., 2026). AI-driven fraud detection systems utilize machine learning algorithms, predictive analytics, and anomaly detection techniques to identify irregular transaction behavior and prevent fraudulent activities before they occur (Islam et al., 2025; Kokogho et al., 2025). These technologies enable financial institutions to improve fraud monitoring accuracy, reduce response time, and enhance risk management capabilities in digital banking environments. Recent studies

emphasize that AI-based financial monitoring systems significantly outperform traditional fraud detection mechanisms in terms of efficiency, scalability, and predictive capabilities (Abi, 2025; Islam et al., 2025; Kokogho et al., 2025; Mazumder, 2025).

The rapid expansion of FinTech-enabled digital banking has significantly improved the efficiency and accessibility of financial services worldwide. Digital financial technologies such as mobile banking, internet banking, and electronic payment systems have allowed financial institutions to deliver faster and more convenient services to customers (Hasan et al., 2024; Wembe, 2025; Yamsani et al., 2025). Globally, the adoption of digital financial services has grown rapidly, with the World Bank reporting that over 76% of adults worldwide now have access to digital financial accounts, compared to 51% in 2011, reflecting the transformative role of FinTech in financial inclusion and economic development (World Bank, 2022).

However, the increasing reliance on digital financial platforms has simultaneously created new opportunities for cybercriminal activities. Cyber fraud has emerged as one of the most critical challenges confronting modern banking institutions, as fraudsters exploit vulnerabilities within digital financial systems to gain unauthorized access to financial accounts and manipulate electronic transactions (Onwuegbuchi et al., 2023; Khatiwada, 2024). The growing sophistication of cyber threats has made it increasingly difficult for traditional fraud detection systems to effectively identify and prevent fraudulent activities in real time (Onwuegbuchi et al., 2023; Khatiwada, 2024; Shahid et al., 2025). According to the International Monetary Fund, financial institutions globally lose billions of dollars annually to cyber-related financial crimes, highlighting the growing urgency of strengthening cybersecurity frameworks in digital banking environments (IMF, 2023).

In Nigeria, the rapid adoption of digital banking technologies has significantly increased the exposure of deposit money banks to cyber fraud risks. Financial institutions in the country have experienced rising incidents of online banking fraud, electronic payment manipulation, phishing attacks, and unauthorized electronic fund transfers (Adeyemo & Obafemi, 2024; Folami et al., 2024; Yahaya, 2025). Data from the Nigeria Inter-Bank Settlement System indicates that the value of electronic transactions in Nigeria exceeded ₦600 trillion in 2023 which is equivalent to $440.6 billion USD, reflecting the massive growth in digital financial activities across the country (NIBSS, 2024). While this growth demonstrates the increasing acceptance of digital financial services, it has also increased the vulnerability of banking systems to cyber fraud. These fraudulent activities not only result in substantial financial losses but also undermine public confidence in the security of digital financial systems. Although banks have implemented various internal control mechanisms and cybersecurity strategies to address fraud risks, the increasing complexity of cyber threats has revealed significant limitations in conventional fraud detection systems that rely heavily on manual monitoring and rule-based fraud detection mechanisms (Akinwale et al., 2022; Agbeyinka, 2025; Imade & Evbayiro-Osagie, 2025).

Recent technological developments suggest that artificial intelligence-driven fraud detection systems may provide more effective solutions for combating cyber fraud in FinTech-enabled banking

environments (Abi, 2025; Alahmad et al., 2026). AI technologies such as machine learning, predictive analytics, and behavioral pattern recognition enable financial institutions to analyze large volumes of transactional data and identify suspicious activities with greater accuracy and speed. These technologies allow banks to detect abnormal transaction patterns, prevent unauthorized financial activities, and respond to cyber threats in real time. Despite the increasing adoption of AI technologies in global banking systems, empirical studies examining the effectiveness of AI-driven fraud detection systems in mitigating cyber fraud within Nigerian deposit money banks remain limited (Islam et al., 2025; Mazumder, 2025). This lack of empirical evidence creates a significant research gap that necessitates further investigation into how AI-based fraud detection technologies can enhance cybersecurity and reduce cyber fraud in Nigeria's rapidly evolving FinTech ecosystem (Abi, 2025; Alahmad et al., 2026; Kokogho et al., 2025).

Given the increasing reliance on digital banking systems, strengthening cybersecurity frameworks and fraud detection mechanisms has become a strategic priority for financial institutions. AI-driven fraud detection technologies provide a promising solution for improving fraud monitoring, as according to Ali et al. (2022), machine learning-based fraud detection systems significantly enhance transaction monitoring capabilities by identifying anomalous patterns in financial data and improving detection accuracy. These technologies enable financial institutions to proactively detect cyber threats, analyze fraudulent behavior patterns, and respond rapidly to potential financial crimes within digital banking systems. Understanding the effectiveness of AI-based fraud detection technologies in mitigating cyber fraud is therefore essential for improving the security, resilience, and sustainability of FinTech-enabled banking systems. This study therefore examines the role of AI-driven fraud detection systems in mitigating cyber fraud in FinTech-enabled digital banking among Nigerian deposit money banks, contributing to the growing literature on FinTech innovation, cybersecurity, and digital financial risk management (Alahmad et al., 2026; Hamdouni, 2025; Yamsani et al., 2025).

Based on the growing adoption of financial technology (FinTech) and artificial intelligence (AI) in modern banking systems, this study seeks to examine how AI-driven fraud detection systems contribute to cyber fraud mitigation in FinTech-enabled digital banking among Nigerian deposit money banks. The integration of AI technologies such as machine learning, predictive analytics, and behavioral pattern recognition has significantly improved banks' capacity to monitor financial transactions, detect anomalies, and prevent fraudulent activities in real time. Previous studies suggest that AI-based fraud detection systems enhance cybersecurity frameworks, improve fraud detection accuracy, and reduce the incidence of financial crimes in digital banking environments (Abi, 2025; Alahmad et al., 2026; Kokogho et al., 2025). In addition, the expansion of FinTech-enabled banking platforms has created both opportunities for improved financial service delivery and new vulnerabilities for cyber fraud activities. Consequently, this study proposes the following hypotheses to empirically examine the relationship between AI-driven fraud detection systems and cyber fraud mitigation in Nigerian deposit money banks.

H_{01}: AI-driven fraud detection capability has no significant effect on cyber fraud mitigation in Nigerian deposit money banks.
H_{02}: Predictive analytics capability has no significant effect on cyber fraud mitigation in Nigerian deposit money banks.
H_{03}: Automated transaction monitoring systems have no significant effect on cyber fraud mitigation in Nigerian deposit money banks.
H_{04}: FinTech digital banking infrastructure has no significant effect on cyber fraud mitigation in Nigerian deposit money banks.

Literature Review

Cyber Fraud Mitigation

Cyber fraud mitigation refers to the strategic, technological, and procedural measures adopted by financial institutions to prevent, detect, control, and reduce fraudulent activities conducted through digital banking platforms. In deposit money banks, cyber fraud mitigation involves protecting customers' accounts, securing electronic transactions, detecting unauthorized access, preventing identity theft, and reducing losses arising from online banking fraud, phishing, card fraud, malware attacks, and electronic payment manipulation (Onwuegbuchi et al., 2023; Khatiwada, 2024). As digital banking expands, cyber fraud mitigation has become central to financial stability, customer trust, and the integrity of banking operations (Akinwale et al., 2022; Folami et al., 2024). Effective mitigation requires the integration of cybersecurity frameworks, internal control systems, digital authentication mechanisms, real-time transaction monitoring, and AI-enabled fraud detection tools (Adeyemo & Obafemi, 2024; Imade & Evbayiro-Osagie, 2025). In this study, cyber fraud mitigation is treated as the dependent variable because it represents the expected outcome of banks' investment in AI fraud detection capability, predictive analytics capability, automated transaction monitoring systems, and FinTech digital infrastructure.

AI Fraud Detection Capability

AI fraud detection capability refers to the ability of deposit money banks to use artificial intelligence technologies to identify, analyze, and prevent fraudulent transactions within digital banking systems. It involves the deployment of machine learning algorithms, anomaly detection systems, neural networks, behavioural analytics, and intelligent monitoring tools to detect unusual transaction patterns and suspicious customer behaviour (Abi, 2025; Islam et al., 2025). Unlike traditional fraud detection systems that depend mainly on fixed rules and manual review, AI-based systems can learn from historical transaction data, adapt to emerging fraud patterns, and generate alerts in real time (Ali et al., 2022; Mazumder, 2025). This capability improves the speed, accuracy, and efficiency of fraud detection by enabling banks to process large volumes of digital transactions and identify risks that may not be easily detected through conventional methods (Kokogho et al., 2025; Alahmad et al., 2026). In this study, AI fraud detection capability is conceptualized as a technological capability that strengthens cyber fraud mitigation by improving banks' ability to detect and respond to fraudulent activities promptly.

Predictive Analytics Capability

Predictive analytics capability refers to the ability of banks to use data analytics, statistical models, machine learning techniques, and historical transaction data to forecast possible fraud risks before they occur. It enables financial institutions to move from reactive fraud control to proactive fraud prevention by identifying patterns, trends, and behavioural signals associated with fraudulent activities

(Yoshikuni et al., 2023; Kokogho et al., 2025). In digital banking, predictive analytics helps banks assess transaction risk, identify high-risk customers or channels, forecast suspicious activities, and support evidence-based cybersecurity decisions (Islam et al., 2025; Alahmad et al., 2026). This capability is particularly important because cyber fraud is dynamic and constantly evolving, requiring banks to anticipate fraud patterns rather than merely respond after losses have occurred (Bolton & Hand, 2002; Mazumder, 2025). In this study, predictive analytics capability is viewed as a key dimension of AI-driven fraud detection because it supports early warning, risk prediction, fraud prevention, and improved decision-making in cyber fraud mitigation.

Automated Transaction Monitoring System

Automated transaction monitoring system refers to technology-enabled systems used by banks to continuously track, screen, and evaluate digital transactions for suspicious or abnormal activities. These systems monitor transactions across digital channels such as mobile banking, internet banking, ATM services, electronic transfers, and payment platforms (Oztas et al., 2023). Automated transaction monitoring systems reduce dependence on manual review by applying predefined risk rules, behavioural indicators, and automated alerts to detect potentially fraudulent transactions in real time (Adeyemo & Obafemi, 2024; Akinbowale et al., 2024). They support fraud investigation by flagging unusual transaction frequency, abnormal transfer amounts, suspicious locations, unauthorized access attempts, and irregular customer behaviour (Rahman & Anwar, 2014; Yamani et al., 2025). In this study, automated transaction monitoring system is conceptualized as an operational fraud control mechanism that enhances cyber fraud mitigation by improving transaction surveillance, increasing detection speed, reducing response delays, and strengthening banks' capacity to prevent financial losses.

FinTech Digital Infrastructure

FinTech digital infrastructure refers to the technological foundation that supports secure and efficient digital banking operations. It includes mobile banking platforms, internet banking systems, electronic payment networks, cloud-based banking solutions, cybersecurity architecture, encryption systems, digital authentication tools, databases, and secure transaction processing platforms (Durak et al., 2024; Hasan et al., 2024). A strong FinTech digital infrastructure enables banks to deliver digital financial services while maintaining system reliability, transaction security, and protection against cyber threats (Chuang & Shrestha, 2025; Shahid et al., 2025). Without adequate digital infrastructure, AI-based fraud detection systems, predictive analytics tools, and automated transaction monitoring systems may not function effectively (Agbeyinka, 2025; Sanusi et al., 2026). In this study, FinTech digital infrastructure is conceptualized as a foundational technological resource that supports cyber fraud mitigation by strengthening digital transaction security, improving system resilience, enabling secure data processing, and facilitating the deployment of advanced fraud detection technologies in Nigerian deposit money banks.

Theoretical Framework

The theoretical framework provides the foundational perspectives that explain the occurrence of fraud and the mechanisms through which financial institutions can mitigate fraudulent activities within digital

banking environments. In the context of FinTech-enabled banking systems, fraud detection and prevention are closely linked to behavioral, technological, and organizational factors that influence financial crimes. Several theoretical perspectives have been developed to explain the motivations and opportunities associated with fraud, particularly within financial institutions. Among the most widely applied theories in fraud and financial crime research are the Fraud Triangle Theory, Fraud Diamond Theory, Fraud Scale Theory, and Fraud Pentagon Theory. These theories provide useful insights into the drivers of fraudulent behavior and help explain how technological innovations such as artificial intelligence can be used to detect and mitigate cyber fraud in digital banking systems.

Fraud Triangle Theory

The Fraud Triangle Theory was developed by Donald Cressey in 1953 to explain the factors that motivate individuals to commit fraud. According to this theory, fraud occurs when three conditions are present: pressure, opportunity, and rationalization. Pressure refers to the financial or personal stress that motivates an individual to commit fraudulent activities. Opportunity arises when weaknesses in internal control systems allow individuals to exploit organizational resources without detection. Rationalization occurs when individuals justify their fraudulent actions by convincing themselves that their behavior is acceptable or temporary (Chukwuekwu, 2024).

In the context of digital banking systems, the rapid expansion of FinTech platforms may create opportunities for cybercriminals to exploit vulnerabilities in financial technologies. Weak cybersecurity frameworks, inadequate monitoring systems, and poor internal controls can increase opportunities for fraudulent activities. The integration of AI-driven fraud detection systems can significantly reduce these opportunities by strengthening transaction monitoring, identifying suspicious patterns, and improving fraud detection accuracy in digital financial systems.

Fraud Diamond Theory

The Fraud Diamond Theory was proposed by David T. Wolfe and Dana R. Hermanson in 2004 as an extension of the Fraud Triangle Theory. The theory introduced a fourth element known as capability, which represents the skills, knowledge, and technical abilities required for an individual to successfully commit fraud. According to this theory, even when pressure, opportunity, and rationalization exist, fraud may not occur unless the individual possesses the capability to exploit the system.

In modern digital banking environments, cybercriminals often possess advanced technological skills that enable them to bypass traditional security mechanisms and manipulate digital financial systems. As financial transactions increasingly occur through digital platforms, fraudsters utilize sophisticated technological tools to execute cyber fraud. AI-driven fraud detection systems therefore play a critical role in addressing the capability element of fraud by strengthening digital monitoring systems and detecting technologically sophisticated fraudulent activities in real time (Abi, 2025; Kokogho et al., 2025). Previous studies have also emphasized that the use of intelligent fraud detection technologies significantly improves banks' ability to monitor digital transactions, identify anomalies, and respond promptly to emerging cyber threats within financial systems (Ezu, 2020; Hossain, 2022). Furthermore, recent research highlights that the integration of artificial intelligence and advanced data

analytics into banking cybersecurity frameworks enhances financial institutions' capacity to combat increasingly complex cyber fraud schemes and protect digital banking infrastructure (Faisal et al., 2024; George et al., 2025).

Fraud Scale Theory

The Fraud Scale Theory was developed by W. Steve Albrecht and his colleagues to provide an alternative explanation for fraudulent behavior within organizations. The theory suggests that fraud is influenced by three key factors: situational pressure, perceived opportunity, and personal integrity. Unlike the Fraud Triangle Theory, the Fraud Scale Theory replaces rationalization with personal integrity, emphasizing the ethical character of individuals as a key determinant of fraudulent behavior.

According to this theory, individuals with low levels of integrity are more likely to engage in fraudulent activities when they experience financial pressure and perceive opportunities within organizational systems. In the context of FinTech-enabled digital banking systems, weak regulatory oversight, inadequate monitoring systems, and poor cybersecurity frameworks may increase opportunities for fraud. AI-driven fraud detection systems can therefore help mitigate cyber fraud by improving transaction transparency, strengthening monitoring systems, and reducing opportunities for fraudulent activities within digital banking environments (Ali et al., 2022; Mazumder, 2025).

Fraud Pentagon Theory

The Fraud Pentagon Theory was developed by Jonathan Marks and expanded the Fraud Triangle Theory by adding two additional elements: competence and arrogance. According to this theory, fraud occurs when five elements are present: pressure, opportunity, rationalization, competence, and arrogance. Competence refers to an individual's ability to manipulate financial systems or exploit internal control weaknesses, while arrogance refers to the belief that one can successfully commit fraud without being detected.

In digital banking environments, cybercriminals often demonstrate high levels of technical competence and confidence in exploiting digital financial systems. The increasing complexity of FinTech platforms has created new opportunities for technologically skilled fraudsters to manipulate financial transactions and bypass security controls. AI-driven fraud detection systems therefore play a critical role in addressing these risks by strengthening cybersecurity frameworks, improving transaction monitoring systems, and enabling financial institutions to detect fraudulent activities in real time (Islam et al., 2025; Alahmad et al., 2026).

Empirical Review

Relationship between AI Fraud Detection Capability and Cyber Fraud Mitigation

Empirical studies have shown that artificial intelligence fraud detection capability plays a critical role in reducing cyber fraud in digital banking environments. AI fraud detection capability refers to the ability of banks to deploy intelligent systems such as machine learning algorithms, anomaly detection tools, neural networks, and behavioural analytics to identify suspicious transaction patterns and prevent fraudulent financial activities. Abi (2025) examined AI-driven fraud detection systems within FinTech platforms using hybrid supervised and unsupervised learning architectures. The study found that AI-based systems significantly improved fraud detection accuracy by analyzing large volumes of transaction data and identifying unusual

financial behaviour. The study concluded that machine learning algorithms enhance the ability of financial institutions to detect cyber fraud in real time and reduce financial losses associated with digital banking fraud.

Similarly, Anzor et al. (2024) investigated the effect of artificial intelligence on fraud detection in deposit money banks in South-East Nigeria. Using a quantitative research approach, the study revealed that AI-driven fraud detection systems significantly improved banks' ability to detect fraudulent financial transactions and strengthen cybersecurity frameworks. The findings indicated that financial institutions that adopted AI-based monitoring technologies experienced improved fraud detection efficiency and reduced losses from fraudulent activities. In a related systematic review, Ali et al. (2022) found that machine learning techniques improve financial fraud detection by identifying irregular transaction patterns more efficiently than conventional rule-based systems. Earlier, Bolton and Hand (2002) emphasized the relevance of statistical fraud detection models in identifying abnormal financial behaviour, thereby providing a foundation for later AI-based fraud detection systems. These studies suggest that AI fraud detection capability is important for enhancing cyber fraud mitigation because it improves speed, accuracy, adaptability, and real-time fraud response in digital banking systems.

Relationship between Predictive Analytics Capability and Cyber Fraud Mitigation

Predictive analytics capability has also been identified as a major technological tool for mitigating cyber fraud in banking institutions. Predictive analytics involves the use of historical data, statistical models, machine learning tools, and behavioural pattern analysis to forecast potential fraud risks before they occur. Yoshikuni et al. (2023) developed and validated scales on big data and business analytics-enabled capabilities, showing that analytics capability improves organizational innovation, responsiveness, and decision-making. Applied to fraud detection, this implies that banks with strong predictive analytics capability are better positioned to identify fraud tendencies, forecast suspicious transaction patterns, and implement preventive measures before cyber fraud causes financial loss.

Islam et al. (2025) reviewed emerging AI technologies used in banking fraud detection and found that machine learning-based predictive systems outperform traditional rule-based systems because of their ability to learn from historical transaction data and adapt to evolving fraud patterns. The study concluded that predictive AI technologies play a crucial role in strengthening cybersecurity systems and improving fraud detection efficiency in digital banking environments. Similarly, Kokogho et al. (2025) investigated the role of advanced analytics and machine learning in enhancing cybersecurity risk management within FinTech ecosystems. Their findings revealed that analytics-driven fraud detection systems improve financial institutions' ability to identify abnormal transaction patterns and strengthen cybersecurity monitoring. These findings are consistent with Alahmad et al. (2026), who argued that the synergy between AI and FinTech strengthens financial stability by improving predictive monitoring, fraud detection, and risk management in both Islamic and conventional banking systems. Therefore, predictive analytics capability contributes to cyber fraud mitigation by enabling banks to shift from reactive fraud detection to proactive fraud prevention.

Relationship between Automated Transaction Monitoring System and Cyber Fraud Mitigation

Automated transaction monitoring systems are essential for detecting and preventing cyber fraud in digital banking because they allow banks to continuously monitor electronic transactions and flag suspicious activities in real time. Oztas et al. (2023) emphasized the importance of transaction monitoring systems in anti-money laundering and financial crime detection by developing a synthetic transaction monitoring dataset that supports fraud detection modelling. Their study highlights the relevance of automated monitoring systems in detecting suspicious patterns within large-scale financial transactions. In digital banking, automated monitoring systems reduce the limitations of manual fraud detection by improving surveillance speed, consistency, and accuracy.

Adeyemo and Obafemi (2024) examined the role of technological innovation in preventing fraud in Nigerian deposit money banks. The study employed a survey research design involving banking professionals and found that technologies such as automated transaction monitoring systems, digital authentication mechanisms, and electronic surveillance tools significantly improved fraud detection and prevention in Nigerian banks. Similarly, Rahman and Anwar (2014) found that fraud prevention and detection techniques are effective when financial institutions adopt technology-driven monitoring mechanisms and strengthen internal control systems. Akinbowale et al. (2024) also investigated anti-fraud technologies in the banking industry and found that technology-based fraud detection tools are important in strengthening cyber fraud mitigation. These studies indicate that automated transaction monitoring systems enhance cyber fraud mitigation by supporting continuous surveillance, rapid detection of unusual transactions, timely fraud alerts, and improved investigation processes.

Relationship between FinTech Digital Infrastructure and Cyber Fraud Mitigation

FinTech digital infrastructure refers to the technological foundation that supports secure digital banking operations, including mobile banking platforms, internet banking systems, payment gateways, cybersecurity architecture, cloud systems, encryption technologies, and secure authentication mechanisms. Strong FinTech digital infrastructure is critical for cyber fraud mitigation because AI fraud detection systems, predictive analytics tools, and automated monitoring platforms depend on secure and reliable digital systems to function effectively. Durak et al. (2024) developed a FinTech adoption scale and showed that digital financial technology adoption depends on infrastructure, usability, trust, security, and system reliability. This suggests that banks with stronger FinTech infrastructure are more likely to achieve effective fraud prevention and digital transaction security.

Agbeyinka (2025) examined the effects of information and communication technology and fraud detection systems on the performance of deposit money banks in Nigeria. The study found that advanced technological systems significantly improved fraud monitoring capabilities and reduced electronic banking fraud. Similarly, Imade and Evbayiro-Osagie (2025) analyzed the relationship between electronic banking services and fraud incidence in Nigerian deposit money banks. Their findings revealed that while the expansion of digital banking increases exposure to cyber fraud

risks, the adoption of advanced fraud detection technologies helps mitigate such risks. Furthermore, Adeyemo and Obafemi (2024) confirmed that digital security systems and technological innovation play a critical role in reducing cyber fraud in Nigerian banks. Sanusi et al. (2026) further demonstrated that integrating digital forensics and machine learning improves fraud detection capability in Nigerian deposit money banks. These findings suggest that FinTech digital infrastructure provides the operational foundation for cyber fraud mitigation by improving system security, transaction monitoring, data protection, and resilience against cyber threats.

Model Specification

To empirically examine the effect of artificial intelligence-driven fraud detection systems on cyber fraud mitigation in FinTech-enabled digital banking among Nigerian deposit money banks, this study specifies a structural model that captures the relationship between AI-based fraud detection capabilities and cyber fraud mitigation. The model is formulated based on the assumption that the adoption of advanced AI technologies such as machine learning algorithms, predictive analytics, automated transaction monitoring systems, and anomaly detection tools significantly enhances the ability of financial institutions to detect and prevent fraudulent activities within digital banking environments.

In line with the study objectives, cyber fraud mitigation (CFM) is specified as the dependent variable, while AI fraud detection capability (AIFD), predictive analytics capability (PAC), automated transaction monitoring systems (ATMS), and FinTech digital infrastructure (FDI) are treated as independent variables. These constructs represent key technological components of AI-driven fraud detection systems that enhance fraud monitoring, detection accuracy, and real-time response capabilities in digital banking platforms. The model therefore assumes that improvements in these technological capabilities will significantly reduce cyber fraud incidents in deposit money banks.

The structural model for the study is expressed mathematically as follows:

$$CFM=\beta 0+\beta 1AIFD+\beta 2PAC+\beta 3ATMS+\beta 4FDI+\varepsilon$$

Where:

CFM = Cyber Fraud Mitigation

AIFD = AI Fraud Detection Capability

PAC = Predictive Analytics Capability

ATMS = Automated Transaction Monitoring Systems

FDI = FinTech Digital Infrastructure

β_0 = Constant term

$\beta_1 – \beta_4$ = Coefficients of the independent variables

ε = Error term

The model is estimated using Partial Least Squares Structural Equation Modeling (PLS-SEM), which allows simultaneous evaluation of the measurement model and structural model. PLS-SEM is particularly suitable for this study because it enables the analysis of latent constructs, handles complex predictive relationships, and is appropriate for studies with relatively small sample sizes. The structural relationships between the constructs are assessed using path coefficients, coefficient of determination (R^2), and statistical significance tests to determine the influence of AI-driven fraud detection systems on cyber fraud mitigation in Nigerian deposit money banks.

Methodology

This study adopts a survey research approach to examine the role of artificial intelligence-driven fraud detection systems

in mitigating cyber fraud within FinTech-enabled digital banking among Nigerian deposit money banks. A cross-sectional survey research design is employed because it enables the researcher to collect data from respondents at a single point in time and analyze the relationships between variables using statistical techniques. This research design is appropriate for the study because it allows the researcher to obtain empirical evidence from banking professionals who are directly involved in digital banking operations, cybersecurity management, and fraud monitoring activities within financial institutions.

The estimated population of 123 respondents was arrived at through a scientific enumeration of employees occupying fraud-sensitive and technology-related positions in the selected deposit money banks. Specifically, the study first identified the relevant functional departments directly connected with AI-driven fraud detection and cyber fraud mitigation, namely internal control, IT security, risk management, digital banking operations, and branch management. Staff nominal rolls and departmental records from the selected banks were then used to determine the actual number of employees occupying these roles, which produced a total accessible population of 123 banking professionals. Since this population was relatively small and manageable, the study adopted a census sampling technique, meaning that all the 123 eligible respondents were included rather than selecting a fraction of them. This method is scientifically appropriate because it eliminates sampling error, improves representativeness, and ensures that the views of all relevant professionals with direct knowledge of fraud detection systems and cybersecurity practices are captured. Although the study is based on selected deposit money banks, the findings can be reasonably generalized to similar banking institutions in Nigeria because the respondents were drawn from standardized banking functions that exist across deposit money banks, and the issues investigated AI-driven fraud detection, cyber fraud mitigation, risk management, and digital banking security—are common operational concerns across the Nigerian banking sector.

Data for the study were collected using a structured questionnaire designed on a five-point Likert scale ranging from strongly disagree (1) to strongly agree (5). The questionnaire measures key constructs such as AI-driven fraud detection capability and cyber fraud mitigation in digital banking systems. Prior to the main data collection, the instrument is subjected to validity and reliability checks to ensure the accuracy and consistency of the measurement items. The collected data are analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) because it is suitable for analyzing complex relationships between latent constructs and is widely used in FinTech, cybersecurity, and information systems research. The analysis includes reliability tests such as Cronbach's alpha and composite reliability, validity assessments using convergent and discriminant validity, and hypothesis testing through path analysis to determine the effect of AI-driven fraud detection systems on cyber fraud mitigation in Nigerian deposit money banks.

Measurements of the Study Variables

The measurement of the study variables was based on validated scales adapted from prior empirical studies and modified to suit the context of AI-driven fraud detection and cyber fraud mitigation in Nigerian deposit money banks. AI Fraud Detection Capability was measured using items adapted from

Miri-Lavassani et al. (2009), focusing on the ability of AI systems to detect suspicious transactions, improve fraud detection speed, enhance accuracy, and support real-time monitoring. Cyber Fraud Mitigation was measured using items adapted from Ghazali et al. (2023), emphasizing the extent to which banks prevent, detect, and reduce cyber fraud through technology-enabled security practices. Predictive Analytics Capability was measured from Yoshikuni et al. (2023), capturing the use of predictive models, data analytics, and algorithmic tools to identify fraud risks and forecast suspicious transaction patterns. Automated Transaction Monitoring System was measured using items adapted from Oztas et al. (2023), Yamani et al. (2025), and Thomas et al. (2013), focusing on continuous transaction surveillance, automatic flagging of suspicious activities, and the effectiveness of monitoring systems in fraud investigation. FinTech Digital Infrastructure was measured using items adapted from Durak et al. (2024), reflecting the availability of secure digital banking platforms, cybersecurity infrastructure, upgraded FinTech systems, and digital transaction security. All constructs were measured using a five-point Likert scale ranging from strongly disagree to strongly agree, and the measurement model later confirmed acceptable item loadings for the constructs as shown in the study's measurement model section.

Results and Discussion

A total of 123 questionnaires were distributed to banking professionals working in fraud risk management, digital banking operations, internal control, and information technology security units of deposit money banks. Out of these, 102 questionnaires were properly completed and returned, representing a response rate of 82.6%, which is considered adequate for statistical analysis.

Demographic Characteristics of the Respondents

The demographic characteristics of the respondents indicate that 63.7% were male while 36.3% were female, suggesting that male respondents slightly dominated the sample. In terms of age distribution, 21.6% of the respondents were between 21–30 years, 42.2% were between 31–40 years, 25.5% were between 41–50 years, while 10.7% were above 50 years, indicating that most respondents were within the active working age group of the banking sector. Regarding educational qualifications, 18.6% held a bachelor's degree, 54.9% possessed a master's degree, and 26.5% had professional certifications or postgraduate qualifications, reflecting a highly educated workforce. With respect to job positions, 27.5% were internal control staff, 31.4% were IT/risk management officers, 22.5% were branch managers, and 18.6% occupied other managerial roles within the banks. In terms of work experience, 19.6% had less than five years of experience, 34.3% had between 6–10 years, 28.4% had between 11–15 years, while 17.7% had over 15 years of experience, indicating that most respondents possessed significant experience in banking operations and fraud monitoring activities. These demographic characteristics demonstrate that the respondents possess adequate professional knowledge and experience relevant to the study on AI-driven fraud detection systems and cyber fraud mitigation in Nigerian deposit money banks.

Assessment of the Measurement Model

The assessment of the measurement model focused on indicator loadings, internal consistency reliability, and discriminant validity to ensure the adequacy of the

constructs used in the analysis. The results indicate that all factor loadings exceeded the recommended threshold of 0.70, confirming that the measurement items adequately represent their respective constructs, while internal consistency reliability assessed through Composite Reliability and Cronbach's Alpha values surpassed the acceptable benchmark of 0.70. Furthermore, the Heterotrait–Monotrait ratio (HTMT) and Average Variance Extracted (AVE) results confirm that the constructs demonstrate satisfactory convergent and discriminant validity, indicating that the measurement model is reliable and suitable for structural model evaluation using PLS-SEM.

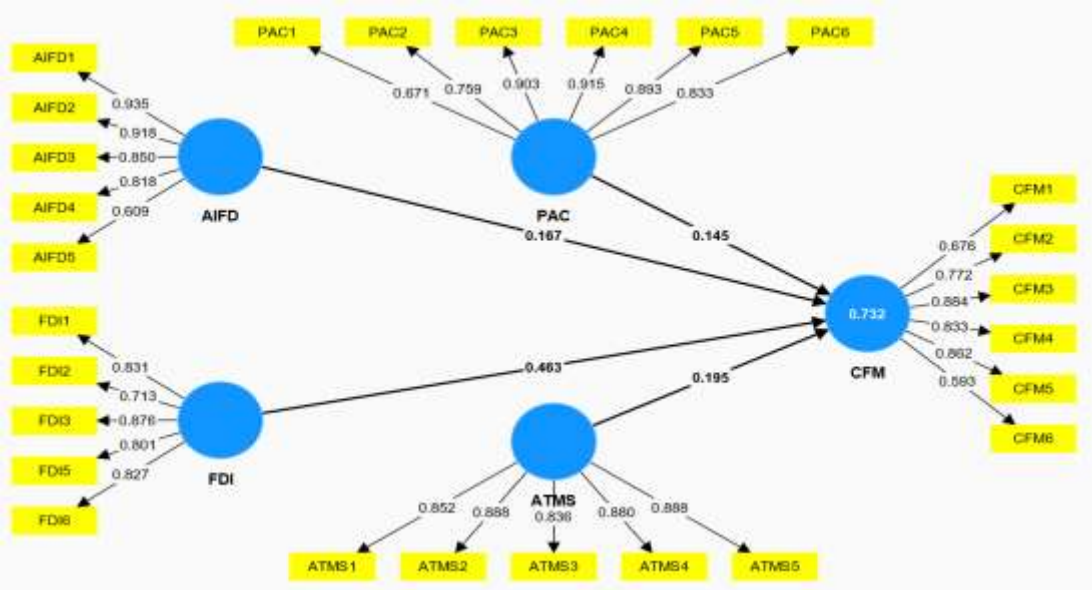

Figure 1: Measurement Model

The items are designed in figure 1 (AI Fraud Detection Capability, Predictive Analytics Capability, Transaction Monitoring Systems, FinTech Digital Infrastructure, and Cyber Fraud Mitigation).

Table 1. Measurement Model: Item Statements and Factor Loadings

Construct	Code	Measurement Items	Factor Loadings
AI Fraud Detection Capability (AIFD)	AIFD1	Our bank uses AI systems to automatically detect suspicious transactions.	0.812
	AIFD2	Artificial intelligence improves the speed of fraud detection in our bank.	0.847
	AIFD3	AI-based systems enhance the accuracy of identifying fraudulent transactions.	0.865
	AIFD4	AI technologies enable real-time monitoring of digital banking transactions.	0.834
Predictive Analytics Capability (PAC)	PAC1	Predictive analytics tools help identify potential fraud risks in digital banking transactions.	0.801
	PAC2	Our bank uses predictive models to forecast fraudulent transaction patterns.	0.842
	PAC3	Predictive analytics improves fraud risk assessment in digital banking systems.	0.816

Automated Transaction Monitoring Systems (ATMS)	PAC4	Predictive analytics supports proactive fraud prevention strategies in our bank.	0.853
	ATMS1	Our bank has automated systems for monitoring digital transactions continuously.	0.829
	ATMS2	Automated monitoring systems quickly flag suspicious transactions.	0.871
	ATMS3	Automated systems improve the effectiveness of fraud detection processes.	0.854
	ATMS4	Transaction monitoring systems enhance fraud investigation processes.	0.818
FinTech Digital Infrastructure (FDI)	FDI1	Our bank has a well-developed digital banking infrastructure.	0.803
	FDI2	FinTech platforms in our bank improve digital transaction security.	0.847
	FDI3	Digital banking technologies enhance the monitoring of financial transactions.	0.832
	FDI4	Our bank continuously upgrades its FinTech infrastructure to improve cybersecurity.	0.865
Cyber Fraud Mitigation (CFM)	CFM1	AI-based fraud detection systems reduce the incidence of cyber fraud in our bank.	0.882
	CFM2	Fraud detection technologies improve the prevention of digital banking fraud.	0.861
	CFM3	Our bank is able to detect cyber fraud quickly due to advanced monitoring systems.	0.847
	CFM4	AI-driven fraud monitoring enhances the security of digital banking transactions.	0.873

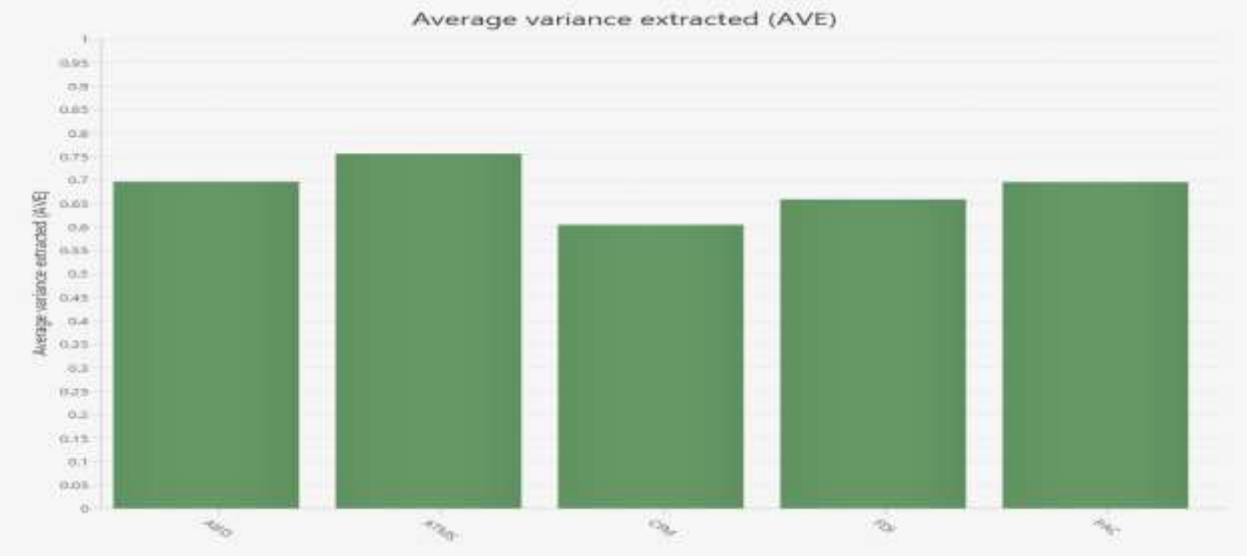

Figure 2: Average Variance Extracted

The results presented in the Average Variance Extracted (AVE) chart indicate that all the constructs in the model meet the recommended threshold for convergent validity in PLS-SEM analysis. Specifically, Automated Transaction Monitoring Systems (ATMS) recorded the highest AVE value of approximately 0.756, indicating that the

construct explains a substantial proportion of the variance of its indicators. This is followed by Predictive Analytics Capability (PAC) and AI Fraud Detection Capability (AIFD) with AVE values of about 0.695 and 0.698 respectively, suggesting that these constructs adequately capture the underlying variance of their measurement items. Similarly, FinTech Digital Infrastructure (FDI) achieved an AVE value of approximately 0.661, while Cyber Fraud Mitigation (CFM) recorded an AVE value of about 0.606. Since all AVE values exceed the recommended minimum threshold of 0.50, the results confirm that the constructs demonstrate satisfactory convergent validity, indicating that the measurement items adequately represent their respective latent constructs and that the model is appropriate for further structural analysis using PLS-SEM.

The Heterotrait–Monotrait Ratio (HTMT) results presented in the figure were used to assess the discriminant validity of the constructs included in the model. The results indicate that most of the HTMT values fall below the recommended threshold of 0.90, suggesting that the constructs are sufficiently distinct from one another and measure different conceptual phenomena. Specifically, the HTMT values for relationships such as ATMS–AIFD (0.81), CFM–AIFD (0.82), CFM–ATMS (0.79), FDI–AIFD (0.78), FDI–ATMS (0.69), PAC–AIFD (0.75), PAC–CFM (0.77), and PAC–FDI (0.70) are within acceptable limits, confirming adequate discriminant validity among these constructs. However, two relationships—FDI–CFM (0.91) and PAC–ATMS (0.88)—appear relatively high, with the former slightly exceeding the recommended threshold, suggesting a potential overlap between FinTech Digital Infrastructure and Cyber Fraud Mitigation. Despite this minor concern, the overall HTMT results generally support the discriminant validity of the measurement model, indicating that the constructs used in the study are empirically distinct and appropriate for further structural model evaluation in the PLS-SEM analysis.

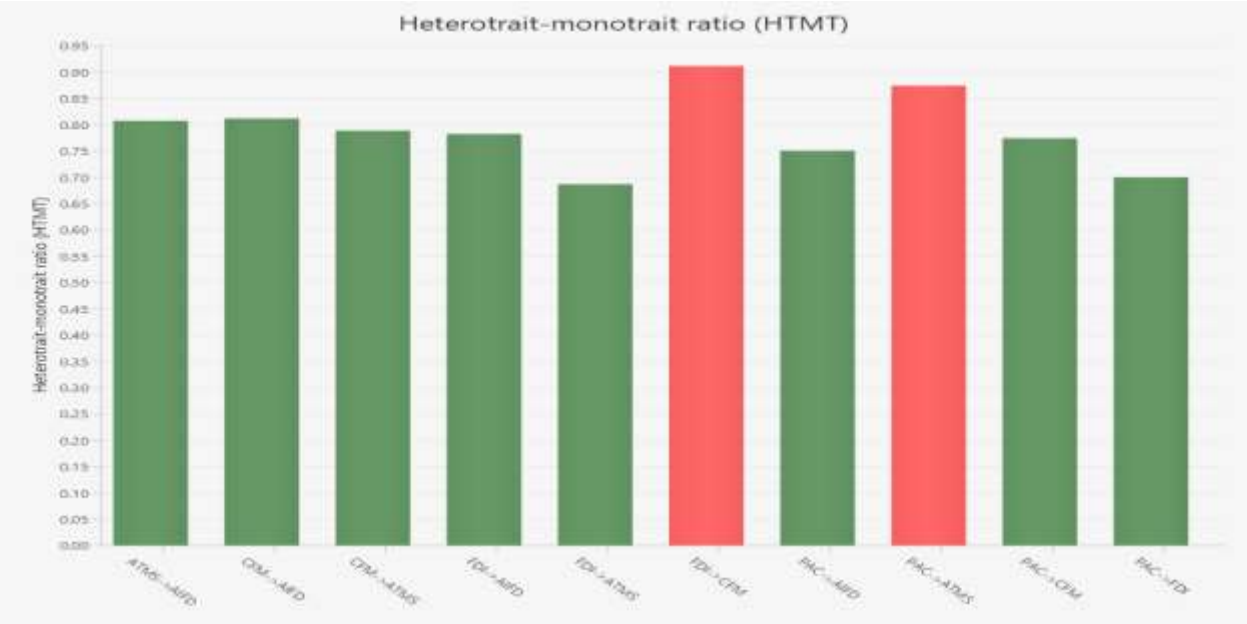

Figure 3: HTMT

Structural Model Assessment and Hypotheses Testing

The structural model results presented in Table 2 were used to evaluate the hypothesized relationships between the independent variables and Cyber Fraud Mitigation (CFM). The results indicate that all the proposed hypotheses are statistically significant, as their t-statistics exceed the recommended threshold of 1.96 and the p-values are below 0.05, suggesting strong empirical support for the relationships in the model. Furthermore, the R^2 value of 0.732 indicates that the predictor variables collectively explain 73.2% of the variance in cyber fraud mitigation, demonstrating that AI-driven fraud detection technologies significantly contribute to reducing cyber fraud in Nigerian deposit money banks.

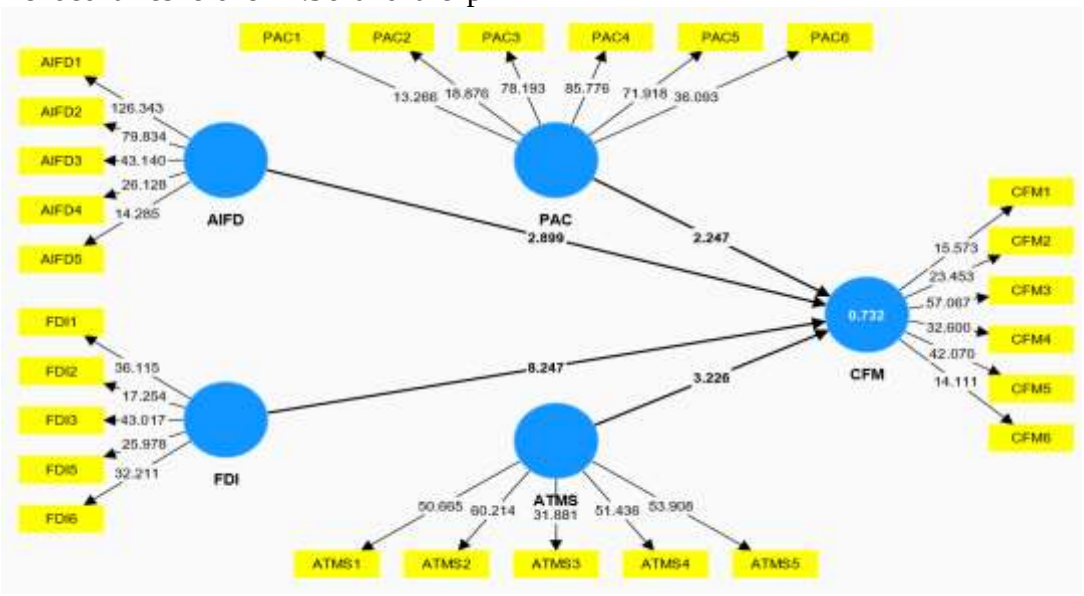

Figure 4: Structural Model

Table 2: Test of Hypotheses

	Beta	Mean	STDEV	T stat	P values	Decision
AIFD -> CFM	0.167	0.169	0.058	2.899	0.004	Reject
PAC -> CFM	0.145	0.145	0.065	2.247	0.025	Reject
ATMS -> CFM	0.195	0.194	0.061	3.226	0.001	Reject
FDI -> CFM	0.463	0.463	0.056	8.247	0.000	Reject

R^2-0.732

Hypothesis 1 examined the effect of AI Fraud Detection Capability (AIFD) on Cyber Fraud Mitigation (CFM). The results show a beta coefficient of 0.167, t-statistic of 2.899, and p-value of 0.004, indicating a positive and statistically significant relationship between AIFD and CFM. This implies that improved deployment of artificial intelligence technologies such as machine learning algorithms and intelligent fraud detection tools enhances the ability of banks to detect and mitigate cyber fraud in digital banking environments. Since the relationship is statistically significant, the null hypothesis is rejected, confirming that AI fraud detection capability significantly contributes to cyber fraud mitigation.

Hypothesis 2 assessed the influence of Predictive Analytics Capability (PAC) on Cyber Fraud Mitigation (CFM). The results reveal a beta coefficient of 0.145, t-statistic of 2.247, and p-value of 0.025, indicating a statistically significant positive effect. This suggests that predictive analytics systems enable banks to analyze transactional data patterns, identify suspicious activities, and anticipate potential cyber threats before they occur. Consequently, the null hypothesis is rejected, implying that predictive analytics capability plays a significant role in strengthening fraud prevention mechanisms within Nigerian digital banking systems.

Hypothesis 3 evaluated the effect of Automated Transaction Monitoring Systems (ATMS) on Cyber Fraud Mitigation (CFM). The results indicate a beta value of 0.195, t-statistic of 3.226, and p-value of 0.001, demonstrating a significant positive relationship between ATMS and cyber fraud mitigation. This finding suggests that automated monitoring systems improve real-time transaction surveillance and enable financial institutions to quickly detect abnormal transaction behaviors. Based on the statistical significance of the relationship, the null hypothesis is rejected, confirming that automated transaction monitoring systems significantly enhance cyber fraud mitigation in Nigerian deposit money banks.

Hypothesis 4 examined the effect of FinTech Digital Infrastructure (FDI) on Cyber Fraud Mitigation (CFM). The results show the strongest relationship among the variables, with a beta coefficient of 0.463, t-statistic of 8.247, and p-value of 0.000. This indicates that robust digital banking infrastructure, including secure platforms, advanced cybersecurity frameworks, and integrated financial technologies, plays a critical role in preventing cyber fraud. Consequently, the null hypothesis is rejected, confirming that FinTech digital infrastructure significantly improves cyber fraud mitigation within the Nigerian banking sector.

Discussion of Findings

The findings of this study reveal that AI Fraud Detection Capability (AIFD) has a significant positive effect on cyber fraud mitigation in Nigerian deposit money banks. This suggests that the deployment of artificial intelligence technologies such as machine learning algorithms, pattern recognition systems, and automated anomaly detection tools enhances banks' ability to detect fraudulent transactions in real time and prevent financial losses. AI-driven fraud detection systems are capable of processing large volumes of transaction data and identifying suspicious patterns that may not be easily detected through traditional fraud monitoring techniques. This finding aligns with previous studies which indicate that artificial intelligence improves fraud detection accuracy, reduces response time to cyber threats, and strengthens digital banking security frameworks (Adeyemo & Obafemi, 2024; AbouGrad & Sankuru, 2025). Similarly, Kokogho et al. (2025) emphasized that AI-enabled fraud monitoring systems significantly enhance the resilience of banking institutions against cyber-attacks by enabling proactive identification and mitigation of fraudulent activities.

The study also finds that Predictive Analytics Capability (PAC) significantly influences cyber fraud mitigation in Nigerian deposit money banks. Predictive analytics systems utilize historical data, behavioral analytics, and algorithmic modeling to forecast potential fraudulent activities before they occur. By analyzing transactional patterns and user behavior, predictive analytics tools enable banks to

anticipate fraud risks and implement preventive security measures. This proactive approach strengthens the overall cybersecurity architecture of financial institutions and minimizes exposure to cyber fraud. The result is consistent with earlier studies which report that predictive analytics enhances fraud risk management by enabling early detection of anomalies and improving fraud investigation processes in digital banking systems (Adeyemo & Okoronkwo, 2024; Alahmad et al., 2026). Furthermore, research by Li et al. (2023) suggests that predictive fraud detection models significantly improve the operational efficiency of banking security systems by enabling real-time fraud risk assessment.

The findings further demonstrate that Automated Transaction Monitoring Systems (ATMS) have a significant effect on cyber fraud mitigation. Automated transaction monitoring systems continuously track digital banking transactions and flag suspicious activities based on predefined risk parameters and behavioral analytics models. This capability allows banks to detect abnormal transaction patterns quickly and respond promptly to potential cyber threats. The effectiveness of automated monitoring systems in preventing cyber fraud has been widely acknowledged in financial technology research. For example, Adeyemo and Obafemi (2024) argue that automated fraud detection systems significantly strengthen financial institutions' cybersecurity frameworks by enabling continuous transaction surveillance. Similarly, Song et al. (2023) noted that real-time transaction monitoring technologies improve fraud detection efficiency and reduce financial losses associated with cyber fraud in digital banking environments.

Finally, the results indicate that FinTech Digital Infrastructure (FDI) has the strongest positive influence on cyber fraud mitigation among the variables examined in the study. This finding suggests that a robust digital banking infrastructure including secure payment platforms, advanced encryption technologies, secure cloud computing environments, and integrated cybersecurity systems plays a critical role in preventing cyber fraud. Strong FinTech infrastructure enhances system resilience, improves data protection mechanisms, and supports the effective deployment of AI-based fraud detection technologies. This result is consistent with previous research indicating that advanced digital infrastructure strengthens financial system security and enhances fraud prevention capabilities in modern banking systems (Kumar et al., 2024; Nugraha et al., 2022). In addition, Effiom and Edet (2022) reported that the adoption of advanced financial technologies significantly improves operational security and reduces vulnerability to cyber fraud in digital banking environments.

Conclusion

This study examined the role of AI-driven fraud detection systems in mitigating cyber fraud in Nigerian deposit money banks, focusing on the influence of AI fraud detection capability, predictive analytics capability, automated transaction monitoring systems, and FinTech digital infrastructure on cyber fraud mitigation. The findings indicate that all the technological capabilities examined significantly contribute to improving cyber fraud mitigation within the digital banking environment. The results further reveal that FinTech digital infrastructure has the strongest influence on cyber fraud mitigation, suggesting that a robust digital ecosystem provides the foundation for

effective implementation of advanced fraud detection technologies. In addition, AI-based fraud detection systems, predictive analytics, and automated monitoring technologies significantly enhance banks' ability to detect suspicious activities, monitor transactions in real time, and prevent cyber threats. The high explanatory power of the model (R^2 = 0.732) further confirms that these technological capabilities collectively play a substantial role in strengthening fraud prevention strategies in Nigerian deposit money banks. Therefore, the study concludes that the integration of advanced financial technologies and artificial intelligence systems is critical for improving cybersecurity resilience and reducing cyber fraud risks in modern digital banking systems.

Recommendations

1. Deposit money banks should invest more in artificial intelligence-based fraud detection systems to improve the accuracy and speed of identifying suspicious transactions and reducing cyber fraud incidents in digital banking operations.
2. Banks should strengthen the adoption of predictive analytics technologies that analyze historical transaction data and behavioral patterns to forecast potential fraud risks and support proactive fraud prevention strategies.
3. Financial institutions should enhance automated transaction monitoring systems to ensure continuous real-time monitoring of digital banking transactions and rapid detection of abnormal transaction patterns.
4. Nigerian deposit money banks should invest in upgrading their FinTech digital infrastructure, including secure cloud computing platforms, advanced encryption technologies, and integrated cybersecurity frameworks to strengthen digital banking security.
5. The Central Bank of Nigeria (CBN) should develop stronger regulatory frameworks and cybersecurity guidelines to support the adoption of advanced fraud detection technologies in the banking sector.
6. Banks should provide continuous training for IT security personnel and fraud risk management teams to enhance their ability to manage AI-driven fraud detection systems effectively.
7. Financial institutions should promote collaboration with FinTech firms and cybersecurity experts to develop innovative fraud detection solutions and strengthen digital banking security systems.
8. Banks should adopt integrated fraud management systems that combine AI, predictive analytics, and automated monitoring technologies to create a comprehensive cyber fraud mitigation framework within the Nigerian banking sector.

References

Abi, R. (2025). AI-Driven Fraud Detection Systems in Fintech Using Hybrid Supervised and Unsupervised Learning Architectures. *Int. J. Research Publication and Reviews*, *6*(6), 4375-4394.

AbouGrad, H., & Sankuru, L. (2025). Online banking fraud detection model: Decentralized machine learning framework to enhance effectiveness and compliance with data privacy regulations. *Mathematics*, *13*(13), 2110.

Adeyemo, K., & Obafemi, F. J. (2024). A survey on the role of technological innovation in Nigerian deposit money bank fraud prevention. *South Asian Journal of Social Studies and Economics*, *21*(3), 133-150.

Adeyemo, F. S., & Okoronkwo, G. (2024). Artificial intelligence and operational efficiency of deposit money banks in Lagos State, Nigeria. *Koozakar Festschrift*, *4*, 4-15.

Agbeyinka, I. (2025). Effects of ict and fraud detection on performance of deposit money banks in Nigeria. *International Journal of Social and Educational Innovation (IJSEIro)*, *12*(24), 531-551.

Akinwale, F. F., Ailemen, I. O., & Areghan, I. (2022). Electronic fraud: an emerging cause of bank failure in Nigerian deposit money banks. *Journal of Money Laundering Control*, *25*(1), 249-263.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2024). Investigating the level of effectiveness of the anti-fraud technologies employed by the South African banking industry for cyberfraud mitigation. *Journal of Financial Crime*, *31*(1), 201-225.

Alahmad, F. A., Ghouse, G., & Bhatti, M. I. (2026). AI and Fintech Synergy: Strengthening Financial Stability in Islamic and Conventional Banks. *Journal of Risk and Financial Management*, *19*(1), 21.

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. *Applied Sciences*, *12*(19), 9637.

Anzor, E. D., Okolie, J. I., Udeh, I. E., Mbah, P. C., Onyeka-Udeh, V., Obayi, P. M., ... & Eze, J. O. (2024). Effect of artificial intelligence (AI) on fraud detection in deposits money banks in South East, Nigeria. *IOSR Journal of Humanities and Social Science*, *29*(11), 15-27.

Bhasin, M. L. (2016). The fight against bank frauds: Current scenario and future challenges. *Ciencia e Tecnica Vitivinicola Journal*, *31*(2), 56-85.

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical science*, *17*(3), 235-255.

Chuang, M. Y., & Shrestha, S. K. (2025). Fintech converges with investment and risk: A bibliometric review. *Journal of Risk and Financial Management*, *18*(9), 517.

Chukwuekwu, O. (2024). Fraud and performance of listed deposit money banks in Nigeria: Exploring the combined effects of fraud triangle and fraud diamond theories. *Journal of Business and Econometrics Studies*, *1*(3), 1-8.

Dodda, A. (2025). *Artificial intelligence and financial transformation: Unlocking the power of fintech, predictive analytics, and public governance in the next era of economic intelligence*. Deep Science Publishing.

Durak, İ., Cise, S. N., & Yazıcı, S. (2024). Developing a financial technology (FinTech) adoption scale: A validity and reliability study. *Research in International Business and Finance*, *70*, 102344.

Ezu, G. (2020). Electronic fraud and performance of deposit money banks in Nigeria: 2008-2018. *International Journal of Business and Management*, *15*(6).

Faisal, N. A., Nahar, J., Sultana, N., & Mintoo, A. A. (2024). Fraud detection in banking leveraging AI to identify and prevent fraudulent activities in real-time. *Journal of Machine Learning, Data Engineering and Data Science*, *1*(01), 181-197.

Folami, R. A., Yinusa, G. O., & Toriola, A. K. (2024). Digital payment fraud and bank fragility: Evidence from deposit money banks in Nigeria. *African Journal of Economic Review*, *12*(4), 21.

George, M. Z. H., Alam, M. K., & Hasan, M. T. (2025). Machine learning for fraud detection in digital banking: a systematic literature review REVIEW. *arXiv preprint arXiv:2510.05167*.

Ghazali, N. N., Hassan, S., & Ahmad, R. (2023). Fortifying against cyber fraud: instrument development with the protection motivation theory. *International Journal of Advanced Computer Science and Applications*, *14*(10).

Hamdouni, A. (2025). From ESG to Financial Stability: Unpacking the Multi-Dimensional Impact of AI-Driven FinTech-Related Technology Adoption on Bank Performance. *International Journal of Financial Studies*, *13*(4), 234.

Hasan, M. H., Hossain, M. Z., Hasan, L., & Dewan, M. A. (2024). FinTech and sustainable finance: how is FinTech shaping the future of sustainable finance? *European Journal of Management, Economics and Business*, *1*(3), 100-115.

Hossain, M. N. (2022). Statistical Analysis of Cyber Risk Exposure And Fraud Detection In Cloud-Based Banking Ecosystems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 289-331.

Imade, O. O., & Evbayiro-Osagie, E. I. (2025). The Impact of Electronic Banking Services on Fraud Incidence in Nigerian Deposit Money Banks: An Empirical Analysis. *International Journal of Finance, Accounting and Management Studies*, *1*(9), 27-42.

International Monetary Fund (IMF). (2023). *Global financial stability report: Safeguarding financial stability amid high inflation and geopolitical risks*. IMF.

Islam, I., Chowdhury, S. A., Hoque, A., & Hasan, M. M. (2025). The Future of Banking Fraud Detection: Emerging AI Technologies and Trends. *Well Testing Journal*, *34*(S3), 102-120.

Khatiwada, S. (2024). *FINANCIAL TECHNOLOGY AND CYBERSECURITY IN COMMERCIAL BANK IN NEPAL* (Doctoral dissertation, Shanker Dev Campus).

Khatib, S. (2024). The Application of Machine Learning Models in Fraud Detection and Prevention Across Digital Banking Channels and Payment Platforms. *International Journal of Advanced Computational Methodologies and Emerging Technologies*, *14*(9), 1-7.

Kokogho, E., Okon, R., Omowole, B. M., Ewim, C. P. M., & Onwuzulike, O. C. (2025). Enhancing cybersecurity risk management in fintech through

advanced analytics and machine learning. *International Journal of Frontiers in Science and Technology Research*, *8*(1), 001-023.

Mazumder, P. T. (2025). Harnessing Fintech Innovations for Anti-Money Laundering: A Data-Driven Approach. *Available at SSRN 5259084*.

Miri-Lavassani, K., Kumar, V., Movahedi, B., & Kumar, U. (2009). Developing an identity fraud measurement model: a factor analysis approach. *Journal of Financial crime*, *16*(4), 364-386.

Nigeria Inter-Bank Settlement System (NIBSS). (2024). *Annual payment system statistics report*. Lagos: NIBSS.

Onwuegbuchi, O., Ibiyeye, A. O., Okolo, J. N., & Adeniji, S. A. (2023). Cybersecurity risks in the fintech ecosystem: Regulatory and technological perspectives. *Communication in Physical Sciences*, *9*(4), 9547-967.

Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Dogan, H., & Aksu, G. (2023, November). Enhancing anti-money laundering: Development of a synthetic transaction monitoring dataset. In *2023 IEEE International Conference on e-Business Engineering (ICEBE)* (pp. 47-54). IEEE.

PK, R., Khaparde, A., Bendre, V., & Katti, J. (2025). Fraud detection and prevention by face recognition with and without mask for banking application. *Multimedia Tools and Applications*, *84*(2), 781-804.

Rahman, R. A., & Anwar, I. S. K. (2014). Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. *Procedia-Social and Behavioral Sciences*, *145*, 97-102.

Sanusi, R. A., Sanusi, I., & Briggs, D. O. B. (2026). Integrating digital forensics and machine learning for fraud detection in Nigerian deposit money banks: a PLS-SEM and artificial neural network approach: A PLS-SEM and Artificial Neural Network Approach. *FUDMA Journal of Accounting and Finance Research [FUJAFR]*, *4*(1), 53-69.

Shahid, M., Alam, M., Noman, R., & Ahmad, F. (2025, April). Enabling FinTech in the Banking System: An Overview, Challenges and Future Opportunities. In *2025 12th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1-6). IEEE.

Thomas, E. A., Zumr, Z., Graf, J., Wick, C. A., McCellan, J. H., Imam, Z., ... & Fleming, M. (2013). Remotely accessible instrumented monitoring of global development programs: Technology development and validation. *Sustainability*, *5*(8), 3288-3301.

Wembe, P. (2025, April). Bridging Economic Divides: The Role of Fintech Payment Systems in Developing Countries. In *Global Conference Alliance Inc*.

World Bank. (2022). *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. Washington, DC: World Bank.

Wu, E., & Emefederalun, I. (2025). Digital Innovations and Fraud Detection and Prevention in Financial Institutions in Nigeria. *Journal of*

Management Sciences, *10*(1), 217-232.

Yahaya, O. A. (2025). Digital transformation and internal control effectiveness of listed deposit money banks in Nigeria. *Journal of Business and Management Studies*, *27*(12), 1-31.

Yamsani, N., Kant, V., Sarasu, P., Khan, S., Kaur, B., & Bhoyar, M. (2025, February). Data-Driven Financial Services: Advancing Payment Systems Through Fintech Innovations. In *2025 International Conference on Technology Enabled Economic Changes (InTech)* (pp. 1506-1509). IEEE.

Yamani, Y., Long, S. K., Sato, T., Braitman, A. L., Politowicz, M. S., & Chancey, E. T. (2025). Multilevel confirmatory factor analysis reveals two distinct human–automation trust constructs. *Human Factors*, *67*(2), 166-180.

Yoshikuni, A. C., Dwivedi, R., Zhou, D., & Wamba, S. F. (2023). Big data and business analytics enabled innovation and dynamic capabilities in organizations: Developing and validating scale. *International Journal of Information Management Data Insights*, *3*(2), 100206.