Article

JOURNAL OF MANAGEMENT SCIENCES
2025, Vol. 10(1), 217-232
©The Authors 2025

DIGITAL INNOVATIONS AND FRAUD DETECTION AND PREVENTION IN FINANCIAL INSTITUTIONS IN NIGERIA

[1]Nnam, Hilary Ikechukwu, [1]Okorieocha, Onyedikachi Chikezie and [2]Anyalor, Chichi Maureen

[1]Department of Accounting, Alex Ekwueme Federal University, Ndufu-Alike, Ikwo
[2]Department of Business Administration, Alex Ekwueme Federal University, Ndufu-Alike, Ikwo.

Abstract

The study focused on digital innovations and fraud detection and prevention in financial institutions in Nigeria. Digital innovation was measured using machine learning, blockchain technology, multifactor authentication and identification and data analytics. However, fraud detection and prevention was used as the dependent variables. The population of the study is made up of 200 staff of the 10 selected deposit money banks in Nigeria selected from 10 banks. However, the sample size of 147 staff was derived using convenience sampling. The data collected were analyzed using ordinary least multiple regression analysis. The result revealed that Machine learning, blockchain technology and multifactor authentication and identification all have significant effect on fraud detection and prevention in deposit money banks in Nigeria, while data analytics has no significant effect on fraud detection and prevention in deposit money banks in Nigeria. Based on the findings, the study concludes that digital innovation positively affects fraud detection and prevention in financial institutions in Nigeria. Therefore, the following recommendations were made; to enhance the security of customer transactions and prevent unauthorized access, Nigeria deposit money banks should consider integrating advanced authentication mechanisms, including biometric identification and multi-factor authentication. These measures are crucial in mitigating the risk of identity theft and unauthorized financial transactions. Investing in and implementing real-time fraud monitoring systems is essential for the proactive detection of anomalous transaction patterns. Such systems empower banks to swiftly identify and respond to suspicious activities, thereby reducing the impact of fraudulent incidents.

Keywords: Digital innovation, Machine learning, Blockchain technology, Multifactor authentication and identification, Data analytics and Fraud detection and prevention.

Introduction

In the dynamic landscape of the financial sector, Nigeria Deposit Money Banks (DMBs) are confronted with the formidable challenge of combating fraud, a pervasive issue that poses a significant threat to the integrity of financial systems. As the nation strives to foster a robust and secure banking environment, the role of technological innovation emerges as a pivotal catalyst in fortifying fraud prevention measures. This study delves into the intricate relationship between technological innovation and its transformative impact on enhancing the resilience of Nigeria's Deposit Money Banks against fraudulent activities. The imperative to address fraud in the banking sector cannot be overstated, considering its detrimental effects on financial institutions, customers, and the overall economy. As noted by Anyanwu (2019), fraud not only erodes public trust but also hampers economic growth by diverting resources that could otherwise be channeled into productive ventures. Consequently, there exists an urgent need for innovative and sophisticated approaches to bolster fraud prevention strategies within Nigeria's banking sector. Technological innovation has emerged as a beacon of hope in this endeavor, offering advanced tools and solutions that can effectively thwart fraudulent activities. The integration of cutting-edge technologies such as artificial intelligence (AI), machine learning, biometrics, and blockchain into the operational frameworks of Deposit Money Banks has the potential to revolutionize the landscape of fraud prevention. According to Smith and Jones (2021), the implementation of AI-powered algorithms can detect anomalous patterns and behaviors, enabling banks to proactively identify and mitigate fraudulent transactions in real-time. Furthermore, the utilization of biometric authentication methods, as endorsed by Okonkwo et al. (2020), provides an additional layer of security by ensuring that access to financial systems is contingent upon the unique physiological or behavioral characteristics of individuals. This not only mitigates the risk of unauthorized access but also safeguards customer identities, fostering a more secure banking environment.

In the context of Nigeria's banking sector, the adoption of blockchain technology holds significant promise for enhancing transparency and traceability in financial transactions. Ojo and Akinbode (2018) argue that the decentralized and immutable nature of blockchain can create an incorruptible ledger, reducing the vulnerability of banks to fraudulent activities such as identity theft and unauthorized fund transfers. As we navigate through this study, each section will scrutinize specific technological innovations and their individual contributions to fraud prevention, providing a comprehensive understanding of their synergistic effects within the context of Nigeria Deposit Money Banks. By critically examining these advancements and their implementation challenges, this research aims to offer valuable insights for policymakers, bank executives, and industry stakeholders seeking to fortify the resilience of Nigeria's financial sector against the ever-evolving landscape of fraud. Fraud remains a persistent challenge for Nigeria's Deposit Money Banks (DMBs), threatening financial stability and eroding public trust. The intricate nature of fraudulent activities necessitates a paradigm shift toward leveraging technological innovation as a proactive strategy for fraud prevention within the banking sector. This introduction will elucidate the multifaceted landscape of fraud in Nigerian DMBs, emphasizing the pivotal role of technological advancements in fortifying defenses against fraudulent activities. Nigeria's financial sector, experiencing substantial growth, has concurrently witnessed an alarming surge in sophisticated fraudulent activities. From identity theft and phishing attacks to intricate financial manipulations, the dynamic nature of fraud necessitates a nuanced and adaptive response. Traditional methods of fraud prevention, such as manual auditing and routine checks, have proven insufficient in countering the evolving tactics employed by fraudsters. Therefore, there is a compelling need to integrate cutting-edge technological solutions to address this escalating issue.

The Central Bank of Nigeria (CBN) and other regulatory bodies have implemented stringent measures to curb fraud, but the evolving tactics of perpetrators demand a more sophisticated and anticipatory approach. The integration of artificial intelligence (AI), block chain, biometrics, and data analytics emerges as a transformative strategy for fortifying the defences of DMBs against the ever-evolving landscape of fraudulent activities. Artificial intelligence, a powerful technological innovation, offers predictive analytics capabilities that empower banks to identify patterns indicative of fraudulent behaviour. Machine learning algorithms, integral to AI, continuously evolve to adapt to new types of fraud, providing a dynamic defence mechanism. These AI-driven solutions enhance the accuracy and efficiency of fraud detection, reducing the occurrence of false positives and negatives (Smith & Jones, 2019). Block chain technology, characterized by its decentralized and tamper-resistant nature, introduces a paradigm of security in financial transactions. The establishment of an immutable ledger minimizes the risk of data manipulation and unauthorized access, providing a secure foundation for banking operations (Nakamoto, 2008). The implementation of block chain in payment systems and transaction verification adds an extra layer of security, creating a formidable barrier against fraudulent activities. Biometric authentication, another innovative approach, has gained prominence in strengthening the security of financial transactions. Fingerprint recognition, facial recognition, and voice authentication are now standard features in digital banking applications. These biometric measures not only offer a secure means of user identification but also mitigate the risk of identity theft, a prevalent form of fraud in the Nigerian banking landscape (Johnson et al., 2020). Data analytics, powered by big data technologies, allows banks to scrutinize vast amounts of transactional data in real-time. This enables the detection of anomalies and irregularities that may indicate fraudulent activities. A proactive approach facilitated by advanced analytics allows for immediate intervention and mitigation, preventing potential financial losses (Chen et al., 2018). While the adoption of these technological innovations aligns with the global trend of digitization in the financial sector, challenges such as the cost of technology integration, cyber security concerns, and the need for skilled personnel must be addressed to fully harness their benefits in fraud prevention. The subsequent sections of this study will delve into the specific applications, challenges, and future prospects of these innovative technologies in the context of fraud prevention within Nigeria's Deposit Money Banks. The contemporary financial landscape in Nigeria is marred by a persistent and escalating challenge fraud within Deposit Money Banks (DMBs).

Despite concerted efforts to curb fraudulent activities, the intricate nature of financial fraud remains a formidable hurdle for the country's banking sector. As noted by Onuoha and Ugochukwu (2017), the escalating sophistication of fraudulent schemes coupled with the evolving landscape of technology necessitate an urgent re-evaluation of existing fraud prevention strategies within Nigeria's Deposit Money Banks. The proliferation of technology in banking operations, while enhancing efficiency and accessibility, concurrently exposes the sector to new and sophisticated forms of fraud (Anyanwu, 2019). The pervasive use of digital channels and online platforms has created an environment where fraudsters exploit vulnerabilities, necessitating an immediate examination of the role of technological innovation as a potential catalyst for fortifying fraud prevention measures. The gravity of the issue is underscored by the far-reaching consequences of financial fraud, affecting not only the stability of individual banks but also eroding public confidence in the broader financial system (Ojo & Akinbode, 2018). Instances of identity theft, unauthorized transactions, and cyber-attacks pose significant threats to both the financial institutions and the customers they serve. Therefore, there is a critical need to explore how technological innovations can serve as a catalyst for preventing and mitigating fraud within the specific context of Nigeria's Deposit Money Banks. Thus, the main objective of the study is to examine the effect of digital innovations on fraud detection and prevention in financial institutions in Nigeria. The specific objectives are:

(i) To examine the effect machine learning on fraud detection and prevention in deposit money banks.

(ii) To determine the effect blockchain technology on fraud detection and prevention in deposit money banks.

(iii) To assess the effect multifactor authentication and identification on fraud detection and prevention in deposit money banks.

(iv) To examine the effect data analytics on fraud detection and prevention in deposit money banks.

REVIEW OF RELATED LITERATURE

Conceptual Framework

Digital innovation

The advent of technological innovation has not only revolutionized the way financial institutions operate but has also become instrumental in fortifying the defenses of Nigeria's Deposit Money Banks against the ever-evolving landscape of fraud. Technological solutions, ranging from advanced analytics to artificial intelligence, present a transformative potential in pre-emptively detecting and mitigating fraudulent activities. As we embark on an exploration of this intersection between technology and fraud prevention, it is imperative to appreciate the pivotal role these innovations play in safeguarding the integrity of financial institutions. The significance of technological innovation in fraud prevention within Nigerian DMBs cannot be overstated. As custodians of public trust and economic stability, these banks are tasked with protecting both individual and institutional assets from an array of sophisticated fraudulent schemes. Identity theft, cyber intrusions, and financial scams pose not only financial risks but also erode the trust that underpins the entire banking sector. Therefore, the integration of innovative technological solutions assumes paramount importance in establishing a robust defense against these threats, ensuring the resilience and sustainability of the banking sector. The relevance of this exploration extends beyond the individual banks to the very fabric of the Nigerian banking sector. The economic stability and growth of the nation hinge upon the trust and confidence of its populace in the banking system. The proactive adoption of technological innovations for fraud prevention is not merely a strategic choice for individual banks but a collective imperative for the entire sector. The continued evolution of banking practices necessitates a corresponding evolution in security measures, making technological innovation an indispensable component in securing the foundations of the nation's economic infrastructure. The primary purpose of this literature review is to conduct a rigorous examination of existing scholarly work, reports, and studies that elucidate the multifaceted relationship between technological innovation and fraud prevention in Nigerian DMBs. By synthesizing this body of knowledge, we aim to discern patterns, identify gaps, and draw insights that can inform future strategies in leveraging technology for fraud prevention. This review is not merely an academic exercise but a strategic initiative to guide stakeholders in optimizing their approach to technological solutions, thus contributing to the resilience and trustworthiness of Nigeria's banking sector.

Overview of Fraud in Nigeria's DMBs in Nigeria

Fraud within Nigeria's Deposit Money Banks (DMBs) constitutes a complex and pervasive challenge that demands rigorous scrutiny. Studies by Afolabi and Oke (2017) underscore the prevalence of fraudulent activities, revealing the multifaceted nature of this phenomenon in the Nigerian banking sector. Understanding the intricacies of fraud within DMBs is imperative for implementing effective prevention strategies (Afolabi & Oke, 2017). The landscape of fraud in Nigerian DMBs encompasses various forms, including identity theft, cyber fraud, and financial misappropriation. Adepoju et al. (2019) delve into the nuanced dimensions of identity theft, shedding light on the sophisticated tactics employed by fraudsters to compromise personal information. This research is instrumental in comprehending the evolving nature of identity-related fraud (Adepoju et al., 2019). Moreover, cyber fraud poses a significant threat to the integrity of Nigeria's banking system. Research by Ogunlade and Oludare (2018) explores the methods employed in cyber fraud within DMBs, emphasizing the need for robust cybersecurity measures to safeguard against unauthorized access and data breaches. This empirical evidence informs the urgency of technological fortifications against cyber threats (Ogunlade & Oludare, 2018).

Financial misappropriation, another facet of fraud within DMBs, has been investigated by Odusote et al. (2020). Their research delves into the mechanisms through which internal and external actors manipulate financial processes, highlighting the necessity for stringent internal controls to mitigate the risk of misappropriation (Odusote et al., 2020). The landscape of fraud prevention in Nigeria Deposit Money Banks (DMBs) has undergone a transformative shift with the infusion of technological innovations. This literature review examines the rich tapestry of scholarly works that explore the multifaceted impact of technological advancements on fortifying fraud prevention mechanisms within the Nigerian banking sector. Cressey's Fraud Triangle (1953) laid the groundwork for understanding the psychological and situational factors that converge to facilitate fraud. This conceptual framework identifies pressure, opportunity, and rationalization as critical elements contributing to fraudulent activities. In the dynamic Nigerian banking environment, this foundational work serves as a backdrop to the evolving strategies employed to address fraud challenges (Cressey, 1953).

Technological Solutions and Fraud Prevention

Fawcett and Provost's seminal work in 1997 introduced machine learning as a powerful tool in fraud detection. Their research establishes a theoretical foundation for the application of algorithms in identifying patterns indicative of fraudulent behavior, providing empirical evidence supporting the efficacy of these technologies (Fawcett & Provost, 1997). The landscape of fraud prevention underwent a transformative evolution with the seminal work of Fawcett and Provost in 1997, which introduced machine learning as a potent tool in the detection of fraudulent activities. This groundbreaking research not only established a theoretical foundation for the application of algorithms but also provided compelling empirical evidence attesting to the efficacy of these technological solutions (Fawcett & Provost, 1997). Machine learning, as conceptualized by Fawcett and Provost, represents a paradigm shift in fraud detection methodologies. The theoretical framework laid out in their work revolutionized the way financial institutions approached the challenge of identifying patterns indicative of fraudulent behavior. Their research demonstrated that algorithms, when trained on vast datasets, could discern intricate patterns and anomalies, enabling proactive detection of fraudulent activities.

The practical implications of Fawcett and Provost's research are profound. The integration of machine learning into fraud prevention strategies empowers financial institutions to move beyond traditional rule-based approaches. The adaptability and self-learning capabilities of machine learning algorithms enhance the accuracy of fraud identification over time, creating a dynamic and responsive defense against evolving fraud tactics. This seminal work not only underscores the potential of machine learning in mitigating fraud risks but also serves as a catalyst for continuous innovation within the field of fraud prevention. Financial institutions worldwide have since embraced machine learning technologies, further validating the enduring impact of Fawcett and Provost's pioneering research. Fawcett and Provost's 1997 work remains a cornerstone in the realm of technological solutions for fraud prevention. Their contribution not only laid the groundwork for leveraging machine learning in the fight against fraud but also set the stage for ongoing advancements that continue to redefine the landscape of fraud prevention in contemporary finance.

Security Measures and Cyber Fraud Prevention

Lee and Patel's empirical study (2019) delves into the significance of robust encryption and cybersecurity protocols in preventing cyber fraud and unauthorized access within Nigerian DMBs. The findings underscore the crucial role of these security measures in mitigating risks associated with unauthorized access and data breaches (Lee & Patel, 2019). In the ever-evolving landscape of cyber threats, Lee and Patel's empirical study in 2019 serves as a beacon, shedding light on the indispensable role of robust encryption and cybersecurity protocols in preventing cyber fraud and unauthorized access within Nigerian Deposit Money Banks (DMBs) (Lee & Patel, 2019). The research conducted by Lee and Patel delves deep into the intricate world of cybersecurity, unveiling the significance of two critical components: robust encryption and advanced cybersecurity protocols. In the face of escalating cyber threats, their empirical findings emphasize the paramount importance of these security measures in mitigating risks associated with unauthorized access and data breaches. The study underscores the pivotal role of robust encryption as a formidable defense mechanism against cyber fraud. By encoding sensitive information in transit and at rest, encryption serves as a barrier those adversaries find challenging to breach. Lee and Patel's research empirically substantiates the efficacy of encryption in safeguarding critical data within the operational frameworks of Nigerian DMBs, contributing to the overall resilience against cyber threats. Furthermore, the empirical evidence presented by Lee and Patel sheds light on the critical role played by advanced cybersecurity protocols. These protocols act as a dynamic shield, continuously adapting to emerging threats and vulnerabilities. By implementing proactive measures, such as intrusion detection systems and realtime monitoring, Nigerian DMBs can fortify their defenses, mitigating the risks associated with unauthorized access and potential data breaches. Lee and Patel's study stands as a cornerstone in the realm of cybersecurity for Nigerian DMBs. Their research not only accentuates the criticality of robust encryption and advanced cybersecurity protocols but also provides actionable insights for financial institutions seeking to establish resilient defenses against the ever-persistent threat of cyber fraud.

Theoretical Review

Technological innovation has emerged as a pivotal force in reshaping fraud prevention strategies within the banking sector, particularly in the context of Nigeria Deposit Money Banks. This theoretical review aims to delve into key theoretical frameworks that underpin the integration of advanced technologies as catalysts for fortifying fraud prevention mechanisms.

Innovation Diffusion Theory

Rogers' Innovation Diffusion Theory provides a valuable lens for understanding the adoption and diffusion of technological innovations. In the realm of Nigeria DMBs, this theory helps illuminate the process through which novel fraud prevention technologies are introduced, accepted, and integrated into the operational landscape. Rogers' Innovation Diffusion Theory (1962) stands as a seminal framework shaping our understanding of the intricate process of adopting and disseminating technological innovations. In the context of Nigeria Deposit Money Banks (DMBs), this theory serves as an invaluable lens, offering profound insights into the dynamic journey of integrating novel fraud prevention technologies into the operational landscape. The foundational work of Rogers (1962) guides us through the stages of innovation adoption, presenting a systematic approach to comprehend how these advancements are introduced, accepted, and assimilated within the unique context of Nigeria DMBs. This theoretical lens provides a structured framework, elucidating the complexities inherent in the adoption and diffusion of technological innovations (Rogers, 1962). As the financial sector in Nigeria constantly evolves, Rogers' theory becomes particularly crucial in navigating the challenges surrounding the introduction of fraud prevention technologies. It delineates the process from the initial exposure and awareness to the pivotal decision-making phase, where stakeholders evaluate the compatibility and benefits of integrating these technologies (Rogers, 1962). Moreover, in the ever-changing landscape of Nigeria DMBs, the theory emphasizes the collaborative efforts and strategic considerations essential in ensuring the seamless integration of fraud prevention technologies into daily operations (Rogers, 1962). It underscores the importance of a systematic approach to not only introduce these innovations but also to facilitate their acceptance and utilization among stakeholders within the banking sector. In essence, Rogers' Innovation Diffusion Theory acts as a beacon, guiding the strategic integration of novel fraud prevention technologies within Nigeria DMBs. By acknowledging and embracing the principles embedded in this theoretical framework, stakeholders can navigate the complexities of technology adoption, fostering a resilient and technologically advanced operational landscape in the realm of Nigeria's banking sector.

Technology Acceptance Model

The Technology Acceptance Model (TAM) is instrumental in examining stakeholders' perceptions and attitudes towards technological innovations. Specifically, TAM assesses factors such as perceived ease of use and perceived usefulness. In the context of Nigeria DMBs, understanding how end-users perceive and embrace these innovations is essential for successful implementation. Davis' Technology Acceptance Model (TAM), introduced in 1989, stands as a seminal framework for understanding the dynamics of technological adoption by assessing end-users' perceptions and attitudes. This model delves into crucial factors, including perceived ease of use and perceived usefulness, offering insights into the acceptance of technological innovations within the unique context of Nigeria Deposit Money Banks (DMBs). Davis (1989) presents TAM as an instrumental tool, providing a systematic approach to gauge stakeholders' inclinations toward technological advancements. Particularly in the setting of Nigeria DMBs, where the financial landscape is rapidly evolving, understanding how end-users perceive and embrace these innovations becomes imperative for ensuring their successful implementation. The crux of TAM lies in its assessment of perceived ease of use, reflecting on the simplicity associated with incorporating new technologies, and perceived usefulness, gauging the perceived value and benefits of these innovations to end-users (Davis, 1989). In the intricate milieu of Nigeria DMBs, where end-users play a pivotal role in the dayto- day operations, their attitudes toward technological advancements profoundly influence the success or failure of implementation endeavors. As financial institutions grapple with the challenges of staying technologically relevant, TAM offers a strategic lens to comprehend the subjective experiences and reactions of end-users. By acknowledging the importance of perceived ease of use and perceived usefulness, stakeholders in Nigerian DMBs can tailor their implementation strategies to align with the expectations and needs of the end-users, fostering a harmonious integration of technological innovations. Davis' Technology Acceptance Model (1989) serves as an indispensable guide, offering nuanced insights into the intricate interplay between end-users and technological innovations within Nigerian DMBs. By applying TAM's principles, stakeholders can navigate the complexities of implementation, ensuring a seamless and user-centric adoption of technologies that are pivotal for the continual evolution of the banking sector.

Empirical Review

Anzor, et al. (2024) examined the impact of artificial intelligence (AI), specifically computer vision and robotic process automation (RPA), on fraud detection in Deposit Money Banks in Southeast Nigeria. AI technologies offer innovative solutions to combat rising fraud threats by enabling real-time monitoring, anomaly detection, and process automation. The study’s objectives include assessing the effectiveness of computer vision in detecting insider fraud and evaluating the role of RPA in monitoring card fraud activities. Using a descriptive survey design, data was collected from employees within various banking institutions in Southeast Nigeria via questionnaire to assess the effectiveness, challenges, and potential improvements AI technologies bring to fraud detection practices. A total population of 1101 staff were selected from the studied organizations. Sample size of two hundred and eighty four (284) was determined using Freund and William's statistic formula at 5 percent margin of error. Data was presented and analyzed using Likert Scale and the hypotheses using Z - test. The findings indicate that Computer Vision had significant positive effect on insider fraud detection, Z = 6.561< 8.639, P. <, 05. Robotics had significant positive effect on card fraud monitoring in money deposit bank in Southeast, Nigeria, Z = 7.649 < 9.987, P. <,05. The study underscores the importance of a comprehensive AI-integrated fraud detection system and recommends further exploration into cost-effective implementations tailored to the context of smaller banking institutions. Addressing these challenges can foster an improved security landscape in Nigeria’s banking sector, enhancing trust and operational resilience.

Another study, conducted by Okwudire and Afolabi (2022) and titled “Effectiveness of Computer Vision Technology in Detecting Internal Fraud within Financial Institutions,” focuses on evaluating the accuracy of computer vision in identifying fraudulent actions, as well as its cost-effectiveness and associated limitations. This case study survey involved a sample of 50 fraud prevention experts and IT personnel drawn from a population of 1,200 employees across ten banks. Qualitative data were collected through semi-structured interviews, and quantitative data related to accuracy and costs were analyzed using statistical methods. The study found that computer vision systems demonstrated a high accuracy rate in detecting insider fraud; however, significant implementation costs and operational challenges, such as the need for regular system maintenance, were noted. The conclusion drawn was that while computer vision is an effective tool for insider fraud detection, its high costs may limit its adoption among some financial institutions. The researchers recommended a phased implementation approach, conducting cost-benefit analyses to justify investments, and establishing partnerships with technology providers to manage financial constraints.

Ohwo, Dada and Ogundajo (2022) conducted a study a study on the effect of Information Technology Control on Fraud Risk Detection in Deposit Money Banks (DMBs) in Nigeria. The study employed the survey research design with a study population of 1,030 which comprised staff in the Internal Control, Internal Audit and Information Technology departments of all Deposit Money Banks (DMBs) in Nigeria as contained on the CBN website. The 13 listed banks were used as samples for the study and the Taro Yamane formula was used to obtain a sample size of 288. The purposive sampling technique was subsequently used in administering the questionnaire to the respondents. The reliability of Cronbach-alpha coefficients ranged from 0.864 to 0.952. Descriptive and inferential statistics were used to analyze the data. Similarly, the study showed that IT control has a significant effect on fraud risk detection in Deposit Money Banks (DMBs) in Nigeria with F287=30.690, Df = 3 & 265, adj. R2 =0.209, p-value=0.000< 0.05. The study, therefore, concluded that IT Controls have a significant effect on fraud risk detection in DMBs in Nigeria. The study, therefore, recommended that Banks should give priority to the implementation of information technology controls across all their digital channels or platforms as this will help to promote adequate fraud risk detection on the platforms and boost customers’ confidence in the banking sector.

Adebayo and Ige (2022), conducted a study titled “Automating Card Fraud Detection: Insights from Robotic Process Automation in Banking,” focused on analyzing the effectiveness of RPA in automating card fraud detection processes, assessing its return on investment (ROI), and exploring its future potential in enhancing fraud detection capabilities. Conducted as a case study analysis, the study included 75 banking professionals and IT specialists from a population of 800 banking staff across various departments. Data were collected through qualitative interviews, and performance metrics of RPA implementations were analyzed thematically. The study found that RPA significantly reduced manual workloads and increased fraud detection efficiency, leading to substantial ROI for banks that adopted these technologies. The conclusion was that RPA serves as a viable solution for automating card fraud detection, enabling notable operational improvements. The authors recommended continuous investment in RPA technology, regular evaluations of performance against fraud detection metrics, and collaborative efforts to identify additional areas where RPA could provide benefits.

Another important study by Nwankwo and Eze (2021), titled “Role of Artificial Intelligence and Computer Vision in Minimizing Insider Fraud in Nigerian Banks,” aims to assess the effectiveness of computer vision in reducing insider fraud and to explore employee perceptions of AI-based monitoring systems. The researchers also sought to identify limitations in implementing this technology within the banking sector. This cross-sectional survey involved a sample of 200 employees from a population of 1,000 across three Nigerian banks. Data collection was carried out through structured questionnaires and interviews, which were analyzed using thematic analysis and descriptive statistics. The findings indicated that while computer vision effectively identified suspicious behaviors among employees, privacy concerns were significant, as many staff felt uncomfortable with continuous monitoring. The study concluded that AI-driven computer vision can help mitigate insider fraud but warned that resistance from employees due to privacy issues could hinder its widespread adoption. The researchers recommended that banks develop transparent policies regarding AI monitoring to foster employee trust and ensure the ethical deployment of technology.

Another good study conducted by Chukwuma and Okwuosa (2021). titled “Evaluating the Impact of Robotics on Card Fraud Prevention in Financial Services,” aimed to evaluate the impact of robotics on card fraud prevention strategies, analyze customer perceptions of automated fraud detection, and identify technological challenges related to implementing robotic systems. This research utilized a cross-sectional survey design, collecting data from a sample of 250 customers and fraud analysts, selected from a population of 1,500 customers across multiple banks. Online surveys and focus group discussions were employed for data collection, with the analysis carried out using statistical methods. The findings suggested that robotics enhanced fraud detection rates and improved customer satisfaction due to faster response times. The study concluded that while robotics offers significant benefits in card fraud monitoring, technological barriers still need to be overcome. Recommendations included improving customer communication about the advantages of robotics and investing in infrastructure upgrades to facilitate better system compatibility.

Oduro and Mensah (2020) investigated “Robotic Process Automation in Banking: A Study on Card Fraud Detection.” The study aimed to assess the effectiveness of robotic process automation (RPA) in detecting card fraud within banks, explore its integration with existing fraud detection systems, and identify the challenges faced by banks in implementing RPA for fraud monitoring. A descriptive survey design was employed, with data collected from 100 employees involved in fraud detection across ten banks, chosen from a population of 600 employees. Structured questionnaires were utilized to gather data, which was then analyzed using both qualitative and quantitative methods. The findings indicated that RPA significantly improved the speed and accuracy of card fraud detection by enabling real-time analysis of transaction patterns and the identification of unusual activities. The study concluded that RPA provides a robust solution for combating card fraud in banks but noted that challenges related to employee training and system integration need to be addressed. Consequently, the authors recommended that banks invest in employee training and ensure seamless integration of RPA systems with other fraud detection processes.

A study by Johnson and Okeke (2020), titled “Application of Computer Vision for Insider Threat Detection in Financial Institutions,” investigates the effectiveness of computer vision in detecting insider threats within financial institutions. The primary objectives of the study were to assess how real-time video surveillance could impact fraud reduction and to evaluate the operational challenges associated with implementing computer vision systems in banks. Employing a descriptive survey design, the researchers collected data from a sample of 150 employees and managers from a population of 500 employees across five major banks. The data was gathered using structured questionnaires and analyzed using descriptive statistics, supplemented by interviews with security personnel. The findings revealed that computer vision significantly reduces insider fraud, particularly when integrated with machine learning algorithms for real-time analysis. However, challenges related to data privacy and technical limitations were highlighted. The study concluded that computer vision is a potent tool for identifying suspicious behaviors indicative of insider fraud and recommended that banks invest in real-time systems in high-risk areas, prioritize employee training on data privacy, and continuously update AI algorithms to enhance detection accuracy.

Bhasin (2016) conducted a study on the role of technology in combatting bank frauds: perspectives and prospects. As part of the study, a questionnaire-based survey was conducted in 2013-14 among 345 bank employees to know their perception towards bank frauds and evaluate the factors that influence the degree of their compliance level. This study provides a frank discussion of the attitudes, strategies and technology that specialists will need to combat frauds in banks. In the modern era, there is “no silver bullet for fraud protection; the doubleedged sword of technology is getting sharper, day-in-day-out.” The use of neural network-based behavior models in real-time has changed the face of fraud management all over the world. Banks that can leverage advances in technology and analytics to improve fraud prevention will reduce their fraud losses. Recently, forensic accounting has come into limelight due to rapid increase in financial frauds or white-collar crimes.

METHODOLOGY

Research design

The research design used for this study is the survey research design. This design is deemed most suitable as it allowed seeking the opinions of well-informed individuals on the impact of digital innovation on fraud detection and prevention in financial institutions in Nigeria, which provided comprehensive thoughts from the number of individual cases.

Population of the study

The population of this study is made up of all the fifteen (14) deposit money banks listed in Nigeria Exchange Group as at December, 2023. They include; Access Bank Plc, Eco Bank of Nigeria, Fidelity Bank Plc, First Bank of Nigeria, First City Monument Bank, Guaranty Trust Bank, Stanbic IBTC Bank, Sterling Bank Plc, Union Bank of Nigeria Plc, United Bank for Africa Plc, Unity Bank Plc, Wema Bank Plc, Zenith Bank Plc and Jaiz bank.

3.3 Sample size/sampling techniques of the study

The study adopted purposive sampling technique. The purposive sampling was used to select only deposit money banks that were able to give information relating to big data analytics. Based on that, ten (10) deposit money banks with 200 employees were purposively selected as the sample size of the study. These deposit money are; Access Bank Plc, Eco bank, Fidelity Bank Plc, First Bank of Nigeria, First City Monument Bank, Guaranty Trust Bank, Stanbic IBTC Bank, Sterling Bank Plc, United Bank for Africa Plc, and Union bank Plc. The study was carried out for the period of 10 years ranging from 2014-2023.

3.4 Data collection and research variables

The study used a descriptive field survey research design and adapted questionnaire as a research instrument. The questionnaire consists of three sections, sections; A, B, C and D. Section A focused on machine learning. Section B focused on blockchain technology. Section C focused on multifactor authentication and identification. And section D focused on data analytics. The instrument was structured using the four point rating Likert scale comprising of Strongly Agree (SA), Agree (A), Disagree (D), and Strongly Disagree (SD) from which the respondent specified their level of agreement.

3.5 Data analysis technique

Multiple regression analysis was used to determine the cause-effect of the independent variables on the dependent variable. Analysis was done with the aid of Statistical Package for Social Sciences (SPSS 23.0).

3.6 Model Specification

The regression equations are given as:

$$FDP = \beta_0+\beta_1 ML+\beta_2 BCT+ \beta_3 AUID+\beta_4 DA+\mu$$

Where:
FDP = Fraud detection and prevention
ML = Machine Learning
BCT = Blockchain Technology
AUID = Multi-factor authentication and identification
DA = Data Analytics
β= regression parameter, which measures the coefficient.
μi= error term or stochastic variable.

DATA ANALYSIS, RESULT AND DISCUSSIONS

Data Presentation

The analysis focused on digital innovation and fraud detection and prevention in financial institutions in Nigeria. Technological innovation represents the independent variable of the study and was measured using machine learning (ML), blockchain technology (BCT), Multi-factor authentication and identification (AUID) and data analytics (DA). However, fraud detection and prevention (FDP) represents the dependent variable of the study. 200 questionnaires were distributed to the staff and management of the firms, 147 representing 70% were correctly filled and returned while 53 questionnaires representing 30% were null and void.

.

Data Analysis.

The data were analysed using both descriptive statistics and multiple regression analysis

Descriptive Statistics

Table 4.1 Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
MACHINE LEARNING	147	1.00	4.00	3.2721	.94040
BLOCKCHAIN TECHNOLOGY	147	1.00	4.00	3.3810	.77046
MULTI-FACTOR AUTHENTICATION AND IDENTIFICATION	147	1.00	4.00	3.5034	.72503
DATA ANALYTICS	147	1.00	4.00	3.5034	.64505
FRAUD DETECTION AND PREVENTION	147	1.00	4.00	3.1973	.91890
Valid N (listwise)	147				

Source: SPSS result extracted from appendix 1A

Table 4.1 shows that descriptive statistics of the variables. It is important to note that all the variables have the minimum of 1 and maximum of 4. Table 4.1 reveals that the mean values of machine learning (ML), blockchain technology (BCT), Multi-factor authentication and identification (AUID), data analytics (DA) and fraud detection and prevention (FDP) are 3.2721, 3.3810, 3.5034, 3.5034 and 3.1973 respectively for the period covered by the study, indicating that the average value of machine learning of the series is 3.27%, that of blockchain technology is 3.38%, Multi-factor authentication is 3.50%, Data analytics is 3.50% while that of fraud detection and prevention is approximately 3.20%. The standard deviation (Std. Dev.) indicates the dispersion from or spread of the series from their mean values. Machine learning has the highest dispersion of 0.94040, followed by fraud dection and prevention with the dispersion of 0.91890. Blockchain technology and Multi-factor authentication have standard deviation of 0.77046 and 0.72503 respectively. However, data analytics has the lowest dispersion of 0.64505.

Table 4.2, presents the regression result on the effect of technological innovation (ML, BCT, AUID and DA) on fraud detection and prevention (FDP). From the model summary table above, the following information can be distilled. The R^2 which measure the level of variation of the dependent variable caused by the independent variables stood at 0.922. The R^2 otherwise known as the coefficient of determination shows the percentage of the total variation of the dependent variable (FDP) that can be explained by the independent or explanatory variables (ML, BCT, AUID and DA). Thus the R^2 value of approximately 0.922 indicates that 92.2% of the variation in the RA of Big 4 auditing firms can be explained by a variation in the in the use of artificial intelligence while the remaining 7.8% (i.e. 100-R^2) could be accounted by other factors not included in this model. The adjusted R^2 of approximately 0.920 indicates that if other factors are considered in the model, this result will deviate from it by only 0.002 (i.e. 0.922 – 0.920). This result shows that there will be a further deviation of the variation caused by the independent factors to be included by 0.002%.

Regression Analysis

Parameters	**Coefficient**	**Std Error**	**T-statistics**	**P-value**
Constant	0.170	0.138	1.237	0.218
ML	0.914	0.073	12.495	0.000
BCT	1.075	0.094	11.436	0.000
AUID	1.052	0.089	11.820	0.000
DA	-0.114	0.105	-1.088	0.278
R-Square	0.922			
Adjusted R-Square	0.920			
F-statistics	421.107			
P-value	0.0000			

Source: SPSS result extracted from appendix 1B

The regression result as presented in table 4.2 determines the relationship between ML, BCT, AUID & DA and FDP shows that when all the independent variables are held stationary; the FDP variable is estimated at 0.170. This simply implies that when all independent variables are held constant, there will be an increase in the FDP of deposit money banks up to the tune of 1.170% occasioned by factors not incorporated in this study. Thus, a unit increase in ML will lead to an increase in FDP by 0.914%. For BCT, a unit increase in BCT will lead to an increase in FDP by 1.075%. For AUID, a unit increase in AUID will lead to an increase in FDP by 1.052%. Finally, a unit increase in DA will lead to a decrease in FDP by 0.114%. Finally, the result shows that there is a significant variation of Fisher's statistics (421.107) has the probability value of 0.0000 which means the model as a whole is statistically significant at 5% level.

Test of Hypothesis

Hypothesis one

HO$_1$*:* Machine learning has no significant effect on fraud detection and prevention in deposit money banks in Nigeria.

Since the calculated probability value 0.000 is less than the accepted probability value of 0.05. The null hypothesis is rejected and the alternative accepted thus; Machine learning has a significant effect on fraud detection and prevention in deposit money banks in Nigeria.

Hypothesis two

HO$_2$*:* Blockchain technology has no significant effect on fraud detection and prevention in deposit money banks in Nigeria.

Since the calculated probability value 0.000 is less than the accepted probability value of 0.05. The null hypothesis is rejected and the alternative accepted thus; blockchain technology has a significant effect on fraud detection and prevention in deposit money banks in Nigeria

.

Hypothesis three

HO$_3$*:* Multi-factor authentication and identification have no significant effect on fraud detection and prevention in deposit money banks in Nigeria.

Since the calculated probability value 0.000 is less than the accepted probability value of 0.05. The null hypothesis is rejected and the alternative accepted thus; Multi-factor authentication and identification have a significant effect on fraud detection and prevention in deposit money banks in Nigeria.

Hypothesis four

HO₃*:* Data analytics has no significant effect on reporting accuracy of accounting professionals.
Since the calculated probability value 0.278 is greater than the accepted probability value of 0.05. The null hypothesis is accepted and the alternative hypothesis rejected thus; data analytics has no significant effect on reporting accuracy of accounting professionals.

Summary of Findings

The following findings were summarized thus:

(i) Machine learning has a significant effect on fraud detection and prevention in deposit money banks in Nigeria.

(ii) Blockchain technology has a significant effect on fraud detection and prevention in deposit money banks in Nigeria.

(iii) Multi-factor authentication and identification have a significant effect on fraud detection and prevention in deposit money banks in Nigeria.

(iv) Data analytics has no significant effect on fraud detection and prevention in deposit money banks in Nigeria.

Conclusion

The emergence of technological advancements has significantly revolutionized fraud prevention strategies within Nigeria Deposit Money Banks. Innovative technological solutions such as biometric authentication, artificial intelligence-based algorithms and blockchain technology have been pivotal in fortifying the resilience of the banking sector against fraudulent activities. The implementation of these cutting-edge technologies has not only bolstered security measures but has also streamlined operational efficiency within NDMBs. By harnessing realtime data analytics and machine learning algorithms, banks have been able to proactively identify, assess, and mitigate potential risks associated with fraudulent behavior, thereby safeguarding the interests of both customers and financial institutions alike. The integration of robust cybersecurity frameworks alongside continuous advancements in technological infrastructure has ensured a resilient defense mechanism against evolving fraud tactics.
Technological innovation stands as an indispensable catalyst for fortifying the defense mechanisms of Nigeria Deposit Money Banks against fraud. The seamless integration of advanced technologies not only enhances security measures but also fosters a more robust, efficient, and resilient banking system, thereby mitigating risks and fostering sustainable growth in the financial sector. Technological innovation has proven to be an indispensable catalyst for fraud prevention in Nigeria deposit money banks. Through the implementation of advanced technological solutions, (i.e. biometric identification systems, machine learning algorithms, and blockchain technology), Nigerian banks have significantly improved their ability to detect and prevent fraudulent activities. These innovations have allowed for greater accuracy in risk profiling, enhanced realtime monitoring of transactions, and more secure customer authentication processes.

Recommendations

Based on the comprehensive analysis conducted in this study, the following recommendations were made:

1. Integration of Advanced Authentication Mechanisms: To enhance the security of customer transactions and prevent unauthorized access, Nigeria deposit money banks should consider integrating advanced authentication mechanisms, including biometric identification and multi-factor authentication. These measures are crucial in mitigating the risk of identity theft and unauthorized financial transactions.

2. Implementation of Real-time Fraud Monitoring Systems: Investing in and implementing real-time fraud monitoring systems is essential for the proactive detection of anomalous transaction patterns. Such systems empower banks to swiftly identify and respond to suspicious activities, thereby reducing the impact of fraudulent incidents.

3. Continuous Staff Training on Cyber security: Recognizing the human factor in fraud prevention, it is recommended that Nigeria deposit money banks prioritize continuous training programs for their staff. These programs should cover the latest cybersecurity threats, attack vectors, and preventive measures, ensuring that bank employees are well-equipped to safeguard against evolving fraud tactics.

4. Collaboration with Fintech Innovators: Active collaboration with fintech innovators is crucial for Nigeria DMBs to stay at the forefront of technological advancements. By embracing emerging technologies through collaboration, banks can harness innovative solutions that provide robust defenses against everevolving fraud schemes.

5. Regular Security Audits and Assessments: To identify and address potential vulnerabilities in the banking system, it is recommended that Nigeria DMBs conduct regular security audits and assessments. This proactive approach ensures that the security infrastructure remains resilient in the face of emerging threats.

References

Adams, J., & Williams, R. (2018). Collaboration with Fintech Innovators: A Strategic Imperative for Banking Security. *J Financ Technol*. 12(3): 45-58.

Adams, L., & Williams, R. (2018). Blockchain Technology in Nigerian Deposit Money Banks: Enhancing Traceability and Transparency. *J Bank Innov*. 12(3): 45-62.

Adebayo, A., & Ige, A. (2022). Automating Card Fraud Detection: Insights From Robotic Process Automation In Banking. *International Journal Of Banking Technology*, 15(3), 45-62.

Adepoju, MI. (2019). Identity Theft and Banking Sector: Evidence from Nigeria. Int J Cyber Criminol. 13(1): 33-48.

Adeyemo K & Obafemi FJ (2024). Technological innovation as a catalyst for fraud prevention in Nigeria deposit money banks. JRIBM. 11: 007.

Afolabi, A., & Oke, M.O. (2017). Fraud in the Nigerian Banking Sector: An Empirical Investigation. *J Financ Crime*. 24(3): 475-489.

Anyanwu, JC. (2019). Banking Sector Reforms, Economic Performance and Financial Inclusion in Nigeria. *Central Bank of Nigeria Economic and Financial Review*. 57(2): 1-29.

Anzor E, Okilie, J, Ode, I., Mba, B., Onyeka-Udeh, V., Obayi, P., Nwankwo, P., Anukwe, G. and Eze, J. (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), 15-2.*

Bhasin, M. (2016). Role of technology in combatting bank frauds: perspectives and prospects. *International Journal of Accounting and Finance*, 5(2), 200-2012.

Brown, A., & Davis, C. (2018). Blockchain Technology in Enhancing Traceability and Transparency of Financial Transactions. *J bank financ technol,* 7(2), 112-129.

Brown, A., Davis, C., & Smith, R. (2019). Advancements in Fraud Prevention: A Survey of Nigerian DMBs. J Bank Financ Res. 12(3): 112-130.

Brown, A., Davis, C., & White, S. (2019). Real-Time Monitoring Systems and Artificial Intelligence: A Survey of Their Effectiveness in Fraud Prevention in Nigerian Deposit Money Banks. *Int J Bank Sec*. 8(1): 23-41.

Brown, M., Jones, P., Clark, S., & Davis, C. (2019). Real-time Fraud Monitoring Systems: A Crucial Element in Bolstering Fraud Prevention Measures. *J Financl Sec*. 15(4): 189-204.

Chen, L., Garcia, M., Nguyen, Q., & Patel, S. (2022). Technological Innovations in Nigeria Deposit Money Banks: A Comprehensive Analysis. *J Bank Technol*. 18(1): 30-47.

Chukwuma, C., & Okwuosa, E. (2021). Evaluating The Impact Of Robotics On Card Fraud Prevention In Financial Services. *Journal Of Financial Fraud Detection*, 10(2), 28-39

Cressey, DR. (1953). Other people's money; a study of the social psychology of embezzlement.

Davis, FD. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. 319-340.

Fawcett, T., & Provost, F. (1997). Adaptive fraud detection. Data Min Knowl Discov. 1(3): 291-316.

Garcia, M., & Nguyen, Q. (2020). Machine Learning Algorithms for Proactive Fraud Detection: A Case Study in Nigerian Banks. *Int J Financ Anal Bank*. 9(2): 78-95.

Johnson, E., & Williams, F. (2021). Continuous Staff Training on Cybersecurity: Empowering Bank Employees Against Evolving Fraud Tactics. *J Cybersecur Edu*. 25(3): 112-127.

Johnson, M. (2021). Empirical Analysis of Multi-factor Authentication in Nigerian Banks. Cybersecur Stud. 8(2): 45-62.

Johnson, A., & Okeke, C. (2020). Application Of Computer Vision For Insider Threat Detection In Financial Institutions. *Journal Of Cybersecurity In Finance*, 12(4), 77-89.

Jones, R., & Clark, S. (2017). Real-time Data Analytics: A Key Player in Proactive Fraud Prevention. *J Financ Anal*. 14(1): 55-70.

Lee, A., & Patel, S. (2019). Robust Cybersecurity Frameworks: Safeguarding Nigeria Deposit Money Banks Against Cyber Fraud. *Int J Cybersecur Res*. 8(4): 210-225.

Lee, J., & Patel, P. (2019). Cybersecurity Protocols and Unauthorized Access Prevention in Nigerian Deposit Money Banks. *J Cybersecur*. 6(4): 178-195.

Lee, S., & Patel, K. (2019). Cybersecurity Measures and Fraud Prevention in Nigeria Deposit Money Banks. *International Jo Info Sec*. 16(4): 345-362.

Nwankwo, S., & Eze, E. (2021). Role Of Artificial Intelligence And Computer Vision In Minimizing Insider Fraud In Nigerian Banks. *African Journal Of Information Systems*, 13(1), 115-130.

Odusote, B. (2020). Financial Misappropriation and Internal Controls in Nigerian Banks. Int J Financ Bank Res. 6(2): 17-32.

Oduro, M., & Mensah, K. (2020). Robotic Process Automation In Banking: A Study On Card Fraud Detection. *Journal Of Banking Innovation*, 7(2), 33-50.

Ohwo, O., Dada, S. and Ogundajo, G. (2022), Information technology control and fraud risk detection in deposit money banks (dmbs) in Nigeria. *International Journal of Accounting and Finance*, 11(4), 7-18

Ogunlade, O., & Oludare, AA. (2018). Cyber Fraud and Financial Institutions in Nigeria. J. Internet Bank Commer. 23(3), 1-18.

Ojo, O., & Akinbode, O. (2018). Blockchain Technology in Financial Services: A Panacea for Fraud Prevention in Nigeria. *Int j adv res comput sci*. 9(3): 71-75.

Okwudire, O., & Afolabi, J. (2022). Effectiveness Of Computer Vision Technology In Detecting Internal Fraud Within Financial Institutions. *Journal Of Financial Technology*, 9(1), 15-30.

Okonkwo, U., Eze, UC., & Ufoma, N. (2020). Biometrics and Banking Security in Nigeria: A Study of Selected Banks in Anambra State. *Int J Comput Appl*. 177(7): 5-10.

Onuoha, B., & Ugochukwu, LI. (2017). Cybersecurity Challenges in Nigeria: Underlying Factors to the Incidence of Cybercrimes. *J econ sustain Dev*. 8(2): 63-74.

Robinson, J., & White, B. (2021). Technological Advancements and Fraud Prevention in Nigeria Deposit Money Banks. *J Financ Sec*. 16(3): 134-148.

Rogers, EM. (1962). Diffusion of Innovations.

Smith, A., & Jones, B. (2020). Advanced Data Analytics and Machine Learning in Early Fraud Detection: Evidence from Nigerian Deposit Money Banks. *J Financ Technol*. 15(2): 87-104.

Smith, A., & Jones, B. (2021). Artificial Intelligence in Fraud Detection: A Comprehensive Review. *J Financ Crime*. 28(1): 180-196.

Smith, J. (2020). The Impact of Technological Advancements on Fraud Prevention Strategies: A Case Study of Nigeria Deposit Money Banks. *J Financ Technol*. 11(2): 89-104.

Smith, J., & Jones, L. (2020). The Impact of Data Analytics and Machine Learning on Fraud Prevention in Nigerian Banking. *J Financ Technol*. 5(1): 78-94.

Smith, J., & Jones, P. (2020). Integration of Advanced Authentication Mechanisms in Nigeria Deposit Money Banks. *Int J Bank Sec*. 6(1): 28-41.

Taylor, K. (2017). Regular Security Audits and Assessments: A Proactive Approach to Identifying and Addressing Vulnerabilities. *J Bank Sec*. 13(4): 176-191.

Wilson, A. (2016). The Role of Technological Innovation in Fortifying the Defense Mechanisms of Nigeria Deposit Money Banks. *J Financ Innov*. 9(3): 112-127.