International Journal of Intellectual Discourse (IJID)
ISSN: 2636-4832 Volume 8, Issue 4. December, 2025

Artificial Intelligence and Digital Fraud Mitigation: A Proposed Framework

*Ibrahim Adamu Abubakar, Muhammad Halliru Beri, Badariyya Ahmad, and Nura Idris

Department of Accountancy, School of Management Studies, Kano State Polytechnic, Nigeria.

*Corresponding Author: ibrahimadamu999@gmail.com

Abstract

Nigerian financial institutions specifically listed deposit money banks are experiencing maximum number of digital frauds in very recent years. Therefore, this study examines the impact of artificial intelligence to mitigate digital fraud in Nigerian listed deposit money banks. Hence, the moniTARs (monitoring insider trading and outsider) system frame work which includes genetic algorithms and neutral nets for analyzing digital fraud were used to identify digital fraud. The authors summarized prior studies, synthesize contemporary thought and other relevant literature that established negative relationship between variables and proposed future research directions. The finding of this study served as a wakeup call to policy makers and any other relevant authorities to get better policies that can protect myopic behavior of fraudsters. Regulatory authorities (CBN, NDIC, and NCC) should develop advance machine learning for banks only to detect and prevent patterns of any digital fraud in banking industry. It is suggested that further research should focused on listed insurance firms using any sophisticated algorithms software to prevent myopic behavior of unauthorized people.

Keywords: Artificial Intelligence, Digital Fraud, DMBs.

1. Introduction

In recent years of the world, large digital frauds uncovered in the giant companies as the result of the existence of ethical failures and the issue of transparency and reliability of the financial information provided to regulatory authorities and other stake holders (Omijeh, 2023). The regulatory authorities' response to financial scandals to take measures to protect relevant information, mitigate conflicts of interest and loss of confidence of the quality of financial statement, all in order to protect the investors interest and increase the confidence of participants in capital market (Ayeni, et al., 2024). A weak storage of relevant information may provide an opportunity for fraudsters to engage in digital fraud which is a strong indication of a collapse of company or deterioration of quality of financial report (Pianoschi & Mierlita, 2025)

Despite the fact that, artificial intelligence has the capacity to mitigate digital fraud and ensure digital activities efficiency not only in banks, but in financial institutions as a whole. Available statistics indicate that an alarming rate of rise in digital frauds has disclose one hundred and eighty seven thousand, eight hundred and seventy cases (187,870 cases) or 88.74% of total fraud cases with the actual loss of four billion and ninety seven million naira only (₦4.97 billion) representing 69.10% of total Nigerian banks losses for 2021 (Igwe & Toby, 2021). The commission distinguished that the ways and instrument used for digital fraud include digital and web-based platforms such as e-commerce,

point of sales (POS) and mobile banking etc. In addition, Nigerian banks lose nine billion and five hundred million naira (₦9.5 billion) to e-fraud in 2023 which lead to the Nigerian electronic fraud forum called for new measures and enhanced collaboration to mitigate the rising trend of digital fraud (Kanu et al., 2023).

Digital fraud is increasing on a daily basis with new approaches for extracting illegal fund from financial institutions specifically banks, the increase of constant vigilance of banks and their customers have meant that perpetrators seems to be one step ahead at all times. To prevent or to bring to an end digital fraud before it can happen in digital based daily transaction because of the smartness of the players with advances technological approaches. The call for an urgent solution through, modern technology which is AI. Therefore, AI can be used to provide more efficient and reliable solution to digital fraud in banks. In addition, AI is the current strength of any computing system of today. This point out that regulatory agency policies and strategies on preventing digital fraud is not working as envisaged. Even though, some empirical studies have been conducted on the AI and digital fraud (Elyassami, et al., 2022) some others studies on AI of banks (Igwe, et al., 2021). Never the less, digital fraud is under investigation, despite the fact that, several studies have highlighted the effectiveness of Machine learning algorithms such as neutral networks, decision trees, and supports victor machine have been applied on large volume of data and identify few fraudulent patterns in service industry (Priya & Saradha., 2021).Secondly and more importantly, increase in the number of digital fraud in a firm probably support the notion in increasing the problem of performance and other studies evidences have been established that financial constrained of some financial institutions to provide proactive measure may lead to fraudulent people to engage in digital fraud

The study contributes to the related literature on digital fraud in the banking industry (Musa, 2023; Anzor, et al., 2024; Ekolama., et al.,2022) by focusing on previous literature that usually explained on the relationship between AI and fraud (Ayeni., et al.,2024). The current study not only present further evidences but also consider as many AI technique as possible for the comprehensiveness and examine which techniques have significant explanatory power for bank's digital fraud.

The remainder of the paper is organized as follows, the first section gives introduction, and the second section is to review related literature, followed by the empirical studies, and next, the main results are discussed, finally, conclusion is provided.

This study examines the impact of artificial intelligence to mitigate digital fraud in Nigerian listed deposit money banks

2. Literature Review

2.1 Conceptual framework

This subsection explains the concept of AI and its attributes as well as seminaries between AI and human intelligence. Further consider the concept of digital fraud and its attributes.

2.1.1 Concept of artificial intelligence

Artificial intelligence in accounting refers to the application of AI technologies and techniques to automate and enhance various accounting processes and tasks (Khaled & Al-Sartawi, 2022). AI in accounting leverage machine learning, natural language processing, data analytics and other AI capacities to streamline accounting operation, improve accuracy and provide valuable insight.

Davitaia (2025) viewed AI as the creation of intelligence by machines that are programmed to take decisions and think like human being, who is not real intelligence but created by human being

through machines using programming language that is known as artificial intelligence. The most important component of artificial intelligence is machine learning which means specific program can be adapted to any new data or information that entered the system and configures and learns from it without any dealings by human being. Mohanty Mishra (2023) affirmed that artificial intelligence is the fourth industrial revolution as programmers build machines to learn from past experiences, adapt new data, act and perform like human intelligence.

2.1.2 AI in Accounting Practice

Some of the key aspect of AI in accounting as mentioned by accounting and finance researcher (Firdaus, et al., 2022; Gupta, 2023 & Singh et al., 2025) which includes the following

- Automation of Routine Tasks: can automate repetitive and time-consuming tasks in accounting, such as data entry, invoice processing and reconciliation. By using optical character recognition (OCR) and machine learning algorithms, AI system can extract information from source documents, classify transactions, and update accounting records automatically.
- Data Analysis and predictive Analytics: AI enables accountants to analyze vast amount of financial data quickly and accurately. Machine learning algorithms can identify the patterns, trends and anomalies in financial data, enabling more accurate financial forecasting, fraud detection and risk assessment. AI can also perform predictive analytics to help businesses make data driven decisions and optimize financial performance.
- Natural Language Processing (NLP): NLP allows AI systems to understand and interpret human language, enabling communication between accountants and AI powered accounting systems NLP can facilitate tasks such as voice-based data entry, generating financial reports, and answering accounting related queries.
- Financial Reporting and compliance: AI can assist in generating financial reports, ensuring compliances with accounting standards, and regulatory requirements. AI-based system can analyze financial data, identify discrepancies and automatically generate accurate financial statements and reports, reducing the risk of errors and ensuring compliance.

2.1.4 Artificial intelligence and human intelligence.

AI and human intelligences (HI) have distinct characteristics and capabilities when it comes to monitoring digital fraud in banks. Here are some of the major differences between the two;

a) Processing power and speed: AI systems can process and analyze vast amount of data at a much faster rate than humans. They can quickly identify patterns, anomalies, and trends in real- time, enabling rapid detection of potential fraudulent activities. Human intelligence, on the other hand, may be limited by the amount of information that can be processed and the time required analyzing it.

b) Scalability: AI systems can be easily scaled to handle large volumes of data and transactions, making them suitable for monitoring fraud in banks with high transactions volumes. Human intelligence, on the other hand, ma struggle to keep up with the sheer volume of data and may be more prone to errors or oversight.

c) Pattern recognition: Ai systems excel at identifying a complex pattern and correction in data, allowing them to detect subtle indicators of fraud. They can learn from historical data and adapt to evolving fraud patterns, improving their accuracy over time. Human intelligence may rely on experience and intuition to identify potential fraud but may be in recognizing intricate pattern or detecting emerging fraud trends.

d) Contextual understanding: human intelligence has the advantage of contextual understanding and ability to interpret complex situations. Humans can consider various factors, such as social, economic and psychological aspects, which may influence fraudulent activities. AI systems although capable of analyzing data, may lack the ability to fully comprehend the context and nuances of fraud situations.

e) Ethical and moral judgment: human intelligence possesses ethical and moral judgment, allowing individual to consider the broader implications and ethical consideration when dealing with fraud. Humans can assess the intentions and motivations behind fraudulent activities, which may not easily capture by AI systems. Ethical decision-making and considerations are crucial in fraud detection and prevention, requiring human intelligence to ensure fairness, transparency, and accountability.

f) Adaptability and creativity: human intelligence is highly adaptable and creative, enabling individuals to think outside the box and come up with innovative solutions to combat fraud. Humans can leverage their knowledge, experience and critical thinking skill.

In summary, AI and HI differ are processing power, scalability, pattern recognition abilities, contextual understanding,

2.1.3 The concept of digital fraud

Defining digital fraud is a special task, there is no definite and precise rule can be laid down as a general preposition in defining digital fraud as it includes surprise, on line trick, wiliness and unfair approach or using electronically to cheat (Louati, et al., 2024).

Digital fraud is the use of trickery and deception principally carried out using electronic devices through the internet, to gain or steal anything of value from unsuspecting victims. The digital fraud varies greatly and appears in many forms (Sinha, 2021). Digital fraud in banking sector entails the use of phishing emails, phony websites, fake mobile apps, bogus social media profile of authentic institutions and other mechanisms to illegally obtain information and defraud customers and businesses (Mohanty & Mishra, 2023).

2.1.4 Fraud detection and risk management

AI can play a crucial role in detecting fraudulent activities and managing financial activities. By analyzing historical data and identifying patterns, AI system can flag suspicious transactions, anomalies, or potential fraud indicators. This helps accountants and practicing auditors in identifying and mitigating financial risks more effectively.

2.1.5 Virtual assistants and chat bots:

AI-powered virtual assistants and chat bots can provide real-time support to accountants and users. These assistants can answer accounting related queries, provide guidelines on accounting standards, and offer support in financial decision-making processes.

In accounting field, AI streamlines processes, improves accuracy, enhances decision making, reduce the burden of manual tasks and identifying patterns of fraudulent activities by leveraging AI technologies.

2.1.6 Digital Banking Fraud in an emerging economy

a. Insider fraud; this is type of fraud is exclusively executed by members staff in the banking system, who exploited the strategies position, the held I the system ad their grasp f HW it works victims f this fraud which involve bank ad their customers.

b. Outsider fraud this is one the type of fraud which involves perpetrators are external to the banking system, they thrived on their internet skills and sometimes on their understanding of the

victims, routine and identity, for instance the perpetrators send bank's customer false email asking for their bank verification details.

c. Collaborative fraud this involved collaboration between bank staff and fraudsters outside the banking system, bank staff could provide account details of customers to the collaborative fraudster.

d. Weak internal corporate governance is another type of digital fraud which bank executive reported mechanism will minimize incidence of digital fraud, when unauthorized person sending out information to customers' who subscribed to electronic alerts. Through this, integration of AI can contact and send anti fraud massages to their customers automatically while perpetrators continue to design new ways of working o customers vulnerabilities, Nigeria board banks need to integrate AI to the cybercrime Act to trace ad prosecute as a way to boost confidence t their customers.

2.2 Theoretical framework

2.2.1 Theory of fraud triangle

Theory that under pins this study is the fraud triangle theory, theory derived from the sociology of crime which is profound by Donald R. Cressey (1970). A fraud triangle theory is explained why people committed fraud and determined their responses based on three fundamental elements which include the following: pressure, opportunity and rationalization. This theory further explained that, these elements occur consecutively to provoke the desire to commit fraud. The first necessary component is perceived pressure which is related to the motivation and drive behind the fraudulent action of individuals. This motivation frequently occurs in people who are under some forms of financial pressure, second component is known as perceived opportunity, it's nothing more than the action of persons. This motivation often occurs in people who are under some forms behind the crime and the ability to commit it. Lastly, the third component known as rationalization has to do with the idea the individuals can rationalize their dishonest acts, making their illegal action seem justified and acceptable (Homer, 2020). Despite, the theory of fraud triangle and other theories, there is still a track for a deeper understanding of what drives a person to fraud in digital era. It may bring the level of confidence and certainty rested in the financial statement by users.

2.3 Empirical review

In recent years, the rise of digital technology has led to an increase in fraudulent activities conducted through the platform. (Halbouni, 2016; Button & Cross, 2012). As fraudulent become more sophisticated, the traditional techniques of fraud detection and prevention have proven to be insufficient (Ekolama et al., 2022; Bello & Olufemi, 2024; Pianoschi & Mierlita, 2025). This has prompted the exploration and integration of AI technologies to enhance fraud detection and prevention capabilities.

Some existing studies have scrutinized the use of AI in various fields such as accounting, finance, management and cyber security (Ekolama, et al., 2022; Ajayi et al., 2025). However, there are appear to be in a literature gap regarding to specific application of AI in accounting is detecting and preventing digital fraud such as using POS, ATM, transfer through USSD code or mobile application, and hacking cyber site.

While, some researchers have touched upon the AI and digital fraud variables of the study, there is a need for further research to explore the potential of AI in identifying patterns, anomalies and trends associated digital fraud (Ayeni, et al., 2024; Ezu & Nwoba, 2025). This could involve the development of machine learning algorithms that can analyses large number of data specifically for banks, detect fraudulent patterns and make life

time decisions to prevent fraudulent activities (Priya & Saradha., 2021). A lot of researchers investigate the impact of machine learning on financial fraud, conventional techniques such as manual verification and inspection are imprecise, costly and time consuming for identifying fraudulent activities with advent of AI, machine learning based approaches can be used intelligently to detect fraudulent transactions by analyzing a large number of data. The empirical reviewed reveal that support vector machine (SVM) and artificial neural network (ANN) are popular ML algorithms used for fraud detection and credit card fraud is the most popular fraud type address using ML techniques (Priya & Saradha., 2021; Ezu & Nwobia, 2025).in addition, ethical consideration and the integration of AI with existing fraud prevention measure are not sufficient to enhance the security measure to protect the interest of investors and other stakeholders.

The link between AI and digital fraud is identifying with modern technique which is used to detect and expose digital fraud. As prior studies mentioned that, the AI plays a significant role in identify sophisticated technique of digital banking fraud.

3. Methodology

The focus of this study is to examine the relationship between AI and digital fraud of listed deposit money banks in Nigeria. Therefore, data was collected from top management and other staffs with relevant knowledge on the current study. The instrument of data collection was questionnaire. The research design of this study is correlation research design; the design predicted the relationship between variables under investigation as at 2022, the population of the study consist of 15 banks in Nigeria stock exchange. The sample size of the study consists of fourteen (14) banks as the result of availability of relevant data. The prior studies were used to examine impact of independent variable and dependent variable under investigation.

3.1 Model Specification and Variables Measurement

The variables for the current study classified in to independent and dependent variables. The empirical model is presented blow.

$$ML_{it} = \beta 0 + \beta_1 APP_{it} + \beta 2TRF_{it} + \beta 3HWS_{it}\ 4 + \beta 4HEM_{it} + €_{it} \quad \ldots\ldots\ldots\ldots\ldots (1)$$

$$NA_{it} = \beta 0\ \beta 0 + \beta_1 APP_{it} + \beta 2TRF_{it} + \beta 3HWS_{it}\ 4 + \beta 4HEM_{it} + €_{it} \quad \ldots\ldots\ldots\ldots\ldots (2)$$

Where ML represent machine learning, NA is represent neutral algorithms, APP is represent mobile application, TRF is represent USSD transfer, HWS is represent hacking company's website, HEM is represent hacking emails .€ stand for error term, β0 is the intercept, β1, β2,β3, and β4 represent the model parameters respectively. i represent firm and t is the time.

Digital Fraud Model

There are numerous mathematical models developed by scholars for detecting digital fraud, often employing statistical methods and machine learning algorithms. One prominent model in financial fraud detection, specifically for identifying digital fraud in financial transaction is;

Leverage Index (LVGI**)** is the **o**riginal concept to measures the ratio of total debt to total assets. A LVGI > 1 indicates increasing leverage, which can be a motivator for digital fraud to meet debt covenants.

Formula: LVGit = (Current Liabilitiest-1+Long-Term Debt t-1)/Total Assets t-1)**/**
(Current Liabilitiest+Long-Term Debtt)/Total Assetst

Total Accruals to Total Assets (TATA): is a measure the extent to which corporate manager uses discretionary accounting policies to boost earnings. High accruals can indicate earnings manipulation or digital fraud.

*Digital Adaptation**:** Could monitor a digital entity's credit lines or borrowed digital assets against its current digital assets or revenue. High and rapidly increasing digital borrowing without corresponding growth might signal financial distress leading to fraudulent activities. It could be analyzed non-cash adjustments or deferred revenue/expenses in digital accounting. Unusually high non-cash components relative to actual cash flow in digital transactions might be a sign of aggressive revenue recognition or expense deferral.

Formula**:**

TATAt = Total Assetst (Income From Continuing Operationst − Cash From Operationst)

3.2 The variables and measurement

Table 1 provides a summary of the variable measurements.

Variable	**Acronym**	**Definition**	**Source**
AI (Machine learning and neural algorithms)	MLA/NLA	Machine learning and neural algorithms	Gupta, 2023;Davitala, 2025
Mobile App	APP	Fraud through mobile banking application	Balogun, et al, 2012
USSD Code transfer	TRF	Fraud using USSD Code transfer	Bello and Olufemi, 2024; Anzor, et al, 2024
Hacking website	HWS	Hacking bank's website by fraudsters	Ajayi, et al, 2025
Hacking email/msg	HEM	Hacking individual email by fraudster	Odufasan et al, 2025

5. Conclusion

Utilizing machine learning to detect or prevent digital fraud is promising and growing research field. The study carefully understands the critical challenge of digital fraud in financial institutions specifically banks. The concepts of algorithms allow banks and other financial institutions to monitor suspicious transactions which may lead to comprehensive analysis rather than sampling and faster remediation.

The discoveries are potentially important for the literature of artificial intelligence for banks. On the other hand, this is one of the front works to analyze how AI considers by the bank to detect and prevent digital fraud, on analysis that might be useful for subsequent studies. In addition, the evidence found is also of interest of banks as it shows that, banks should not only concern about detecting digital fraud but also concerned about how this digital fraud is eliminated and avert possible collapse of listed banks in Nigeria. The study of artificial intelligence significantly mitigates the myopic behavior of unauthorized people to practice digital fraud and explain to the stakeholders the method of digital fraud in banks.

It is suggested that further research should be conducted using empirical investigation on listed banks or insurance firms. Financial analysts look at an artificial intelligence as a device to mitigate the digital fraud and provide healthy environment of all digital financial transactions to shareholders and other

stakeholders. The study also present useful recommendation to policy makers and regulatory agencies (Central Bank of Nigeria, Nigerian Communication Commission) such as periodic review of the policy to iron out grey areas and expose new technique of digital fraud.

References

Ajayi, A. J., Joseph, S., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The impact of artificial intelligence on cyber security in digital currency transactions. *Available at SSRN 5137847*.

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.

Ayeni, T. J., Durotoye, E. O., & Eriabie, S. (2024, April). Adoption of artificial intelligence for fraud detection in deposit money banks in Nigeria. In *2024, international conference on science, engineering and business for driving sustainable development goals (SEB4SDG)* (pp. 1-5). IEEE.

Balogun, E. D., Ogunsola, K. O., & Samuel, A. D. E. B. A. N. J. I. (2021). A risk intelligence framework for detecting and preventing financial fraud in digital marketplaces. *Iconic Research and Engineering Journals*, *4*(08), 134-149.

Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer science & IT research journal*, *5*(6), 1505-1520.

Button, M. (2012). Cross-border fraud and the case for an "Interfraud". *Policing: An International Journal of Police Strategies & Management*, *35*(2), 285-303.

Celestin, M., & Vanitha, N. (2019). Uncovering fraud in the digital era: Innovative techniques for auditors. *Indo American Journal of Multidisciplinary Research and Review*, *3*(2), 31-37.

Davitaia, A. (2025). Artificial Intelligence and machine learning in fraud detection for digital payments. *International Journal of Science and Research Archive*, *15*(3), 714-719.

Ekolama, S. M., Orike, S., & Elechi, P. (2022). Preventing cyber-fraud in Nigeria's banking system using fraudaeck-AI. *European Journal of Electrical Engineering and Computer Science*, *6*(6), 55-63.

Elyassami, S., Nasir Humaid, H., Ali Alhosani, A., & Taher Alawadhi, H. (2021). Artificial intelligence-based digital financial fraud detection. In *International Conference on Intelligent and Fuzzy Systems* (pp. 214-221). Cham: Springer International Publishing.

Ezu, G. K., & Nwobia, C. E. (2025). Nigeria Deposit Insurance Corporation as a Panacea for stabilizing Nigeria Banking Industry. *International Journal of Finance, Accounting and Management Studies*, *1*(2), 101-114.

Firdaus, R., Xue, Y., Gang, L., & Sibt e Ali, M. (2022). Artificial intelligence and human psychology in online transaction

fraud. *Frontiers in psychology*, *13*, 947234.

Gupta, P. (2023). Leveraging machine learning and artificial intelligence for fraud prevention. *SSRG International Journal of Computer Science and Engineering*, *10*(5), 47-52.

Halbouni, S. S., Obeid, N., & Garbou, A. (2016). Corporate governance and information technology in fraud prevention and detection: Evidence from the UAE. *Managerial Auditing Journal*, *31*(6/7), 589-628.

Homer, E. M. (2020). Testing the fraud triangle: a systematic review. *Journal of Financial Crime*, *27*(1), 172-187.

Igwe, E. I., & Toby, A. J. (2021). Deposit insurance and credit risk of Nigeria banking system: a time series analysis. *Journal of Global Economics and Business*, *2*(6), 1-30.

Kanu, C., Nnam, M. U., Ugwu, J. N., Achilike, N., Adama, L., Uwajumogu, N., & Obidike, P. (2023). Frauds and forgeries in banking industry in Africa: a content analyses of Nigeria Deposit Insurance Corporation annual crime report. *Security journal*, *36*(4), 671-692.

Khaled AlKoheji, A., & Al-Sartawi, A. (2022). Artificial intelligence and its impact on accounting systems. In *European, Asian, Middle Eastern, North African Conference on Management & Information Systems* (pp. 647-655). Cham: Springer International Publishing.

Louati, H., Louati, A., Almekhlafi, A., ElSaka, M., Alharbi, M., Kariri, E., & Altherwy, Y. N. (2024). Adopting artificial intelligence to strengthen legal safeguards in blockchain smart contracts: a strategy to mitigate fraud and enhance digital transaction security. *Journal of Theoretical and Applied Electronic Commerce Research*, *19*(3), 2139-2156.

Malik, H., & Mustafa, K. (2025). AI and Financial Risk Management: Preventing Fraud and Securing Digital Transactions.

Mohanty, B., & Mishra, S. (2023). Role of artificial intelligence in financial fraud detection. *Academy of Marketing Studies Journal*, *27*(S4).

Musa, S. J., Ejur, S. B., Moses, I. K., & Yusuf, I. (2024) Effect Of Artificial Intelligence (Ai) on Fraud Prevention of Listed Deposit Money Banks in Nigeria.

Odufisan, O. I., Abhulimen, O. V., & Ogunti, E. O. (2025). Harnessing Artificial Intelligence and Machine Learning for Fraud Detection and Prevention in Nigeria. *Journal of Economic Criminology*, 100127.

Oluwadare, O. E., Adekanmbi, J. A., & Omodara, B. E. (2025). Artificial Intelligence and Fraud Prevention in Nigerian Deposit Money Banks (DMBs). *Acta Universitatis Danubius. Œconomica*, *21*(3), 128-150.

Omijeh, B. O. (2023). The Effect of Online Fraud on the Adoption of Digital Economy in Nigeria: A Review. *African Journal of Management and Business Research*, *10*(1), 26-33.

Pianoschi, A., & Mierlita, S. (2025). Revising ISA240 in a digital world: the sociomaterial perspective on fraud, technology, and stakeholder influence. *Digital Finance*, 1-27.

Priya, G. J., & Saradha, S. (2021, February). Fraud detection and prevention using machine learning algorithms: a review. *7th International Conference on*

Electrical Energy Systems (ICEES). 564-568.

Singh, N., Jain, N., & Jain, S. (2025). AI and IoT in digital payments: Enhancing security and efficiency with smart devices and intelligent fraud detection. *International Research Journal of Modernization in Engineering Technology and Science*, *6*(12), 982-991.

Uzomah, M. M., & Eruetemu, P. O. (2024). Artificial intelligence and digital economy and the economic state of Nigerians. *Journal of Emerging Technologies*, *4*(1), 26-35.