THE NEXUS BETWEEN CYBER RESILIENCE, AI-DRIVEN THREAT DETECTION AND FRAUD PREVENTION AMONGST DMBS IN BENIN CITY, NIGERIA

[1]Marley Osayande Iyamu
marleyosayande@gmail.com

&
[2]Rosemary Obasi, PhD
Orcid: 0000-0000-7768-0858, obasi@biu.edu.ng

[1&2]Department of Accounting, Faculty of Social and Management Sciences,
Benson Idahosa University, Edo State, Nigeria

Abstract

This study investigated the nexus between cyber resilience, Artificial Intelligence (AI)-driven threat detection, and fraud detection and prevention among Deposit Money Banks in, Nigeria. The study used descriptive research design to collect primary data through the administration of structured questionnaires to 141 respondents among Deposit Money Banks in Benin City and analysed using descriptive statistics and robust least square regression technique. The findings indicate that while institutions heavily rely on authentication protocols and the results revealed that AI-driven threat detection has a positive and significant relationship with fraud detection and prevention among DMBs in Nigeria at p-value < 0.05 level of significance. Cyber resilience has a negative and insignificant relationship with fraud detection and prevention among DMBs in Nigeria at p-value > 0.05 level of significance. The study recommended that DMBs in Nigeria should explore AI-driven threat detection as a cyber-security measure for detecting and preventing fraudulent activities in banking industry in Nigeria.

Keywords: Artificial Intelligence Driven Threat Detection, Cyber Resilience, Fraud Detection and Prevention, Technology Acceptance Model, and Theory of Anomaly Detection theory.

Introduction

The emergence of innovative technology exposed financial institutions, accounting firms and other sectors to fraudulent activities. Naz and Khan (2024) and Chukwuma, et al., (2025) argued that the process of underscoring the need for more effective tools to detect and prevent fraudulent activities resulted in fundamental issues witnessed in the auditing process as experienced by the high-profile corporate scandals in Brooge Energy and Tingo Group in U.S. Bello (2024) affirmed that financial institutions in Nigeria have taken it as a priority for the integration of Artificial Intelligence (AI) into fraud detection and prevention. Financial institutions have to create a road map for robust defense mechanisms in the area of adversarial training, model assembling, and an anomaly detection technique which is aimed at improving resilience of fraud detection systems against cyber-attacks. The intergration of artificial intelligence into threat detection and fraud prevention strategies is transforming how these institutions safeguard their operations and customer's data. However, the collaboration with AI developers and financial institutions make it easy for cyber resilience, so as to mitigate fraud detection thereby strengthening the operational efficiency and effectiveness of the banking sector in Nigeria.

Grimm, et al. (2021) maintained that fraud detection and prevention has become less easy through the process of AI and machine learning (ML) approach. By leveraging on AI capabilities, financial institutions, accounting professionals and other sectors can enhance their ability to identify and respond to cyber threat in real time, automate the detection of fraudulent activities and adapt to emerging patterns of cybercrime. Hatzivasilis, et al., (2020) argued that fairness, accountability, and transparency in fraud detection systems are hindered by the interpretability of AI models as a major problem. The presence of innovation and technology among financial institutions have greatly promoted the prevention and detection of fraud through big data analytics, blockchain-enabled predictive analytical model, alluring realm of AI, ML, and deep learning, etc. Real-time fraud detection is now an industry norm based on the corporate governance reforms to reshape the culture and methods of doing business in the era of globalization (Ayinla, et al, 2024). The exploration of cyber resilience highlights the essential role of AI in fortifying financial institutions, accounting firms and other sectors against potential risk, ensuring both operational stability and customer trust in a technology-driven world.

The digital transformation of financial services has fundamentally altered the threat landscape, expanded the attack surface and created new vulnerabilities for cybercriminals to exploit. Traditional reactive security measures, characterized by signature-based detection and manual response, have proven inadequate against rapidly evolving threats like AI-controlled phishing and advanced persistent threats (APTs). In the Nigerian context, the urgency for advanced mechanisms is underscored by the fact that banks Fraud losses across digital channels jumped from ₦17.67 billion in 2023 to over ₦52 billion in 2024, with POS platforms accounting for over a quarter of reported cases (Ogundipe, 2025). Consequently, the transition to proactive, AI-driven frameworks is no longer an option but a mandatory requirement for maintaining public trust. In the current era of globalization and digitalization, commercial banks in Nigeria are increasingly exposed to sophisticated cyber threats that jeopardize the integrity of financial data. While traditional, rule-based internal controls are widely used, they often struggle to keep pace with the high-velocity data streams of modern banking, leading to delayed detection and increased financial losses.

The core of the problem lies in several critical gaps such as data vulnerabilities. The presence of missing or incomplete datasets creates "blind spots" that facilitate fraudulent activities and result in biased, poorly performing AI models (Bello, et al., 2023). Bhattacharjeeet al. (2022) posits that, Cybercriminals now use adversarial techniques to manipulate data inputs or exploit algorithmic vulnerabilities, allowing them to bypass standard security measures. Persistent financial recklessness and internal fraudulent activities by personnel remain a significant challenge for corporate organizations (Kankpang, et al., 2024). Despite the potential of AI, banks face substantial hurdles in implementation, most notably regulatory compliance (cited by 68.1% of respondents) and the need for specialized technical expertise. This exploratory study focuses on understanding cyber resilience and assessing how it enhances threat detection and fraud prevention among financial institutions in Benin City. Specifically, the research addresses the following salient questions: This objective focuses on how AI technologies are used to identify and stop fraudulent activities and to explore how AI-driven threat detection systems can enhance cyber resilience in banks. This objective examines the capacity of AI to help banks resist, respond to, and recover from cyber-attacks.

Without addressing these challenges through robust AI-driven cyber resilience frameworks, financial institutions risk substantial reputational damage and operational instability. This study therefore explores how AI-driven threat detection can bridge these gaps to fortify both fraud prevention and institutional resilience.

Literature Review and Hypothesis Development

Fraud Prevention and Detection

Fraud detection is the process of monitoring the activities of users of digital transactions in order to estimate, predict and avoid objectionable behaviour. Fraud detection among financial transactions remains a dominant factor in advanced detection mechanisms. Fraud detection is a new phenomenon that began through manual review of online transactions which is rule-based systems in the present-day era (Ogude, et al., 2022). However, financial institutions have to implement several corporate governance reforms to detect and prevent fraud due to the fact that fraud is a very relevant problem that demands attention. Fraud is an intentional act by one or more individuals among management that are charged with governance, and employees or third parties applying the use of deception to obtain an unjust and illegal advantage (Bello et al., 2023). Fraud detection is defined as the process of identifying suspicious activity of criminal element in relation to money theft (Handoko & Rosita, 2022). The presence of fraud detection within the realm of accounting has undergone a profound metamorphosis given the level of technological progress in the domain of data analytics as a means of preventing fraudulent activities (Ayinla, et al., 2024). According to the Nigerian Interbank Settlement System (NIBSZS) report of 2019, there are various kinds of fraud committed by people such as mobile telecommunication fraud, payment fraud, insurance fraud and cyber- crime fraud without due diligence to corporate governance code of conduct. Hence, fraud is a fundamental concept that deals with deceitfulness or deliberately practiced in order to gain some advantages dishonestly (Takon, et al., 2023). Alshari and Gawali (2021) stated that there are three basic approaches to fraud detection such as the traditional or rule-based approach, data mining approach and ensemble (hybrid) approach. The advent of big data analytics and AI-driven tools created through the digitalization of business transactions aid fraud detection (Handoko & Rosita, 2022).

Relationship between AI-Driven Threat Detection and Fraud Detection and Prevention

The field of accounting profession has been driven by the presence of fraud detection through the integration of data analytics (Ayinla, et al, 2024). The financial environment has experienced several cyber risk associated with data digitalisation process. AI threat detection is a cyber-security approach that utilizes artificial intelligent (AI), and Machine Learning (ML) to identify, analysed and respond to potential security threat in real time (Daniel & Andreas, 2022; Ukoba et al., 2023). Nyre-Yu et al. (2022) defined AI-driven threat detection as the analysis of vast amounts of data and detecting potential security threats through the usage of artificial intelligence and machine learning algorithms. Meanwhile, the emergence of AI-driven threat detection has caused a shift from traditional and analog processing to real-time analytics, by commanding huge investments in infrastructure capable of handling high-velocity data streams and AI powered system for curbing cyber-attacks. Vivek, et al. (2023) re-affirmed that cyber criminals are becoming more sophisticated as the drive for digitalisation continued. Aftabi, et al. (2023) argued that financial institution should channel more effort in leveraging on Machine Learning and other AI tools toward the detection of fraud in order to improve accuracy and operational efficiency among financial institution in Nigeria, the use of AI threat detection strategy and AI-powered systems should be adopted for minimising fraudulent activities. Faccia (2023) added that financial institutions should be more conscious of fraud detection by complying with ethical use of data analytics and adhere to principles of data privacy and fairness. Sontan and Samuel (2024) opined that red-flagged transactions were the rule-based systems explored by organisations to detect fraudulent activities.

Ayinla, et al. (2024) in his study title "Transformative Implications of Technology on Accounting Practices" used exploratory and case studies research to investigate and analyse the practical application, challenges, and implications of advanced technologies in fraud detection in Nigeria. Their findings revealed that the integration of data analytics, ML, AI powered system and

big data is very instrumental in fraud detection. Adhikari, et al. (2024) conducted study on the effectiveness of AI-based techniques in financial fraud detection. The study adopted deep learning and ML to assess the performance of AI-driven fraud detection systems. The study revealed that AI-based tools strongly contribute to real-time fraud detection and adaptability. Also, ethical concerns, algorithmic bias, data privacy issues and system vulnerabilities were the main challenges of AI-based fraud detection systems. Aashima, et al. (2023) in their study evaluated the significance of forensic accounting in fraud detection in India Banking" they established that the integration of AI powered tools along with traditional accounting knowledge improved the ability of the banking sector to detect financial frauds. Aftabi, et al. (2023) examined detecting fraud in financial statements by exploring data mining and Generative Adversarial Network (GAN) models. The study established that the usage of both ML and AI by financial institution would strongly curb fraud detection. Bello, et al. (2023) used the application of AI for real-time fraud detection in US financial transactions. The analysis of the case studies revealed that financial institutions effectiveness is driven by AI-powered techniques for curbing financial fraud and improving fraud detection capabilities thereby enhance operational efficiency.

H1: There is positive relationship between AI-driven threat detection and fraud detection and prevention among deposit money banks in Nigeria.

Relationship between Cyber Resilience and Fraud Detection and Prevention

Cyber resilience is a new phenomenon that has characterized public domain with significant recognition of the critical component of cyber security strategy (Tzavara & Vassiliadis, 2024). Financial institutions commit huge investment in the area of AI-driven cybersecurity nowadays to forestall the resilience of fraud detection systems (Nair, et al., 2024). Al-Dosari, et al. (2024) affirmed that the usage of AI-driven tools by financial institutions to identify potential vulnerabilities in real-time in the prevention of cyber-attacks. The presence of cyber security among AI-based fraud detection systems entails trust from the financial system in protecting customer data from financial losses (Xu, et al., 2024).

Fundamental elements of cyber-security in the financial sector serve as building blocks for designing and implementation of cyber-security strategy and operating framework. The cyber-security strategy includes eight basic elements which are: cyber-security strategy and framework; governance; risk and Control Assessment; monitoring; response timely to cyber incident; information sharing, and continuous Learning. The emergence of cyber-threats lead to lost of confidentiality and integrity of financial data and caused a substantial risk to the stability and reputation of innovative driven business organisations (Reis, et al., 2024). Kaushik et al. (2024) conducted a study on ethical consideration in AI-based cyber security in Singapore. They established that privacy, data security and algorithmic bias were the ethical considerations of AI-based cyber-security in fraud detection and prevention. Mishra (2023) in his work titled **"**Exploring the impact of AI based Cyber Security and Financial Sector Management" he affirmed that the integration of AI in network security systems like Enhanced Encryption Standard (EES) and K-Nearest Neighbor (KNN) improved financial sector management against cyber-attacks and threats. The following hypothesis is proposed.

H2: There is positive relationship between cyber resilience and fraud detection and prevention among deposit money banks in Nigeria.

Theoretical Review

The relevant theories of the study were theory of Technology Acceptance Model (TAM) and theory of Anomaly/Outlier detection theory.

Technology Acceptance Model (TAM)

The usage of AI is likened to the theory of Technology Acceptance Model (TAM) which was proposed by Fred Davis (1989) on the usefulness and practicality of AI by financial

institutions, accounting firms and auditing firms in Nigeria. The underlying principle of the theory is that it is designed to predict user's acceptance of information technology usage. The theory anchors the usage of information technology on two major perceptual factors such as the perceived usefulness and the perceived ease of use and attitude towards using it. The perceived usefulness is seen as the degree to which a person believes that using a particular system would enhance the operation of the financial institution in Nigeria in the area of fraud prevention and detection (Hubert, et al., 2018).

The Theory of Anomaly/Outlier Detection

The use of AI is also likened to the theory of Anomaly/Outlier detection theory proposed by Dorothy Demining in 1986. This theory is based on the premise that fraudulent activities often deviate from the normal norm, and AI can efficiently flag this deviation in real time. Zanke (2023), in his comparative study of fraud detection across banking, insurance, accounting firms and healthcare emphasized how AI-driven fraud detection systems leverage anomaly detection to identify irregularities in transaction patterns.

Methodology

This study adopted an exploratory research design using a cross-sectional survey approach. Primary data were gathered through structured questionnaires administered to staff in various commercial banks operating within the Benin City Metropolis, Edo State, Nigeria.

The total population consisted of staff from commercial banks in Benin City. A stratified sampling technique was used to select 141 respondents from 19 commercial banks in Benin City. The sample included IT professionals, cyber security experts, senior staff, and management staff. A total of 190 questionnaires were distributed, out of which 141 were returned and found usable for the analysis. Data were processed using SPSS, focusing on descriptive statistics to identify trends in AI implementation and perceived resilience.

The questionnaire would be constructed on 5-point Likert scale: Strong disagree (1), Disagree (2), Undecided (3), Agree (4) and Strong agree (5). Therefore, reliability of the questionnaire is tested using Cronbach's Alpha, which is the default statistical procedure for reliability analysis. However, any value > or equal to 0.70 justify the reliability of the research instrument. In verifying the reliability of the research instrument data, a Cronbach Alpha test was carried. The result obtained was presented in the table below.

Table 3.1: Reliability Test

Variable	Cronbach's Alpha	No of Items
Fraud detection and prevention	0.706	3
AI-driven threat detection	0.752	2
Cyber resilience	0.784	3

Source: Author's Computation, 2026

It was observed from table 3.1 above that fraud detection and prevention has a coefficient value of 0.706, AI-driven threat detection has a Cronbach's Alpha coefficient value of 0.752 and cyber resilience has a Cronbach's Alpha coefficient value of 0.784. This means that the Cronbach's Alpha for all the variables is more than 0.70. This indicates that the variable is considered to be good for internal alpha which is between 0 and 1. This means scales in this reliability analysis were well-established and the result was acceptable.

Data Presentation and Analysis

The demographic characteristics of 92 out of the 141 respondents were analysed using descriptive statistics to provide insights into the sample's professional background and cybersecurity experience.

Table 4.1: The demographic profiles of the respondents are presented.

Variable	Category	Frequency	%
Sex	Male	41	44.6
	Female	47	51.1
Age	0-25 years old	2	2.2
	26-30 years old	24	26.1
	31-40 years old	32	34.8
	41-50 years old	21	22.8
	Above 51 years old	4	4.3
Marital Status	Single	1	1.1
	Married	44	47.8
	Divorced	32	34.8
	Widowed	2	2.2
Educational Qualification	HND/BSc	60	65.2
	MSc	21	22.8
Cyber-security Experience	0-3 years	19	20.7
	4-6 years	29	31.5
	7-10 years	11	12.0
	11 years & above	26	28.3
Staff Role	IT professional/cyber security experts	21	22.8
	Senior	23	25.0
	Management	45	48.9

Source: Authors Compilation (2026)

Descriptive Statistics of Study Constructs

The descriptive statistics for the constructs—Fraud Prevention, AI-Driven Threat Detection, and Cyber Resilience—reveal important patterns in institutional capability

Table 2: Descriptive statistics for the constructs

Construct	Mean (M)	Std. Deviation (SD)	Skewness (S)	Kurtosis (K)
Fraud prevention	2.7971	0.43631	-2.988	17.525
AI-driven threat detection	2.4647	0.47257	-1.359	6.899
Cyber resilience	2.8116	0.54370	-1.570	6.975

Source: Authors compilation (2026)

The distribution characteristics reveal a strong negative skewness across all constructs. In social science research, skewness values beyond -1.0 or -2.0 suggest substantial non-normality.14 The kurtosis value for fraud prevention (K = 17.525) is extremely high; while some scholars use a threshold of ±7.0, an absolute value exceeding 10 indicates a heavily peaked (leptokurtic) distribution with heavy tails.

Regression Results

In order to test the individual significance of the variables, a multiple regression techniques was adopted and the result is presented in table 4.3 below:

Table 4.3: Regression Results

Variable	OLS Model	Robust OLS Model
C	2.7999	2.9732
	(5.0689)	(3.6212)
	{0.0000}	{0.0003}
ATD	0.1742	0.4452
	(1.4651)	(2.5188)
	{0.1464}	{0.0118}
CBR	0.0818	-0.2560
	(0.7807)	(-1.6426)
	{0.4370}	{0.1005}
R-squared/ Rw-squared	0.036718	0.049794
Adjusted R^2	0.015071	0.028441
F-statistic/ Rn-statistic	1.696220	7.633038
Prob(F-stat.)	0.189249	0.022004

Source: Authors compilation (2026)

The regression result revealed that R^2 value of 0.036718 implies that about 4% of the proportion of variations in the dependent variable was explained by independent variables. The F-statistic value of 1.696220 with probability value (0.189249) > 0.05 showed that the regression result is not valid and unacceptable for investigating the relationship between the variables. Hence, the non-linear relationship of the OLS result is corrected by running the robust OLS as shown in Table 4.3 above. The robust OLS result with Rw^2 value of 0.049794 indicates that about 5% of the proportion of variations in fraud detection and prevention explained by AI-driven threat detection and cyber resilience. The Rn-statistic value of 7.633038 with probability value (0.00) < 0.05 showed that there is a significant relationship between the variables.

Specifically, AI-driven threat detection (ATD) has a positive coefficient (0.4452) and significant (0.0118) relationship with fraud detection and prevention among DMBs in Nigeria (FDT) at p-value < 0.05 level of significance. This implies that AI-driven threat detection would strongly influence fraud detection and prevention among DMBs in Nigeria. Cyber resilience (CBR) has a negative coefficient (-0.2560) and insignificant (0.1005) relationship with fraud detection and prevention among DMBs in Nigeria (FDT) at p-value > 0.05 level of significance. This implies that cyber resilience would adversely influence fraud detection and prevention among DMBs in Nigeria overtime.

Discussion of Findings

The results revealed that AI-driven threat detection has a positive and significant relationship with fraud detection and prevention among DMBs in Nigeria at p-value < 0.05 level of significance. The result aligns with the findings of Ayinla, et al. (2024) that the integration of data analytics, ML, AI powered system and big data is very instrumental in fraud detection. The result also supports the findings of Adhikari, et al. (2024) and Aftabi, et al. (2023) that AI-based tools strongly contribute to real-time fraud detection. Cyber resilience has a negative and insignificant relationship with fraud detection and prevention among DMBs in Nigeria at p-value > 0.05 level of significance. The result negates the findings of Kaushik et al. (2024) data security and algorithmic bias were the ethical considerations of AI-based cyber-security in fraud detection and prevention. The result also differs with the findings of Bello, et al. (2023) that financial institution effectiveness is driven by AI-powered techniques in the area of cyber resilience for curbing financial fraud in Nigeria.

Conclusion and Recommendations

The study focused on cyber resilience, AI-driven threat detection and fraud detection and prevention among DMBs in Nigeria. Financial institutions have to create a road map for robust defense mechanisms in the area of adversarial training, model assembling, and an anomaly detection technique which is aimed at improving resilience of fraud detection systems against cyber-attacks. The effective usage of AI by financial institution in Nigeria toward the detection of fraud helps to improve in operational efficiency. The results revealed that AI-driven threat detection has a positive and significant relationship with fraud detection and prevention among DMBs in Nigeria at p-value < 0.05 level of significance. Cyber resilience has a negative and insignificant relationship with fraud detection and prevention among DMBs in Nigeria at p-value > 0.05 level of significance.

Recommendations

The study recommended that:

1. DMBs in Nigeria should explore AI-driven threat detection as a cyber-security measure for detecting and preventing fraudulent activities in banking industry in Nigeria.
2. To improve on cyber resilience by investing in enabling technology, including user interface and incorporating collaborative learning approaches for detecting and preventing fraud among DMBs in Nigeria in the long-run.
3. To improve resilience, institutions should invest in scalable, cost-effective technologies like cloud-based AI platforms.

References

Aashima, M. B., & Kedia, N. (2023). Evaluating the significance of forensic accounting in fraud detection in the Indian banking sector: A systematic literature review. *Gurukul Business Review, 19*(10), 145–160.

Adhikari, P., Hamal, P., & Baidoo Jnr, F. (2024). Artificial intelligence in fraud detection: Revolutionising financial security. *International Journal of Science and Research Archive, 13*(1), 1457–1472

Aftabi, S. Z., Ahmadi, A., & Farzi, S. (2023). Fraud detection in financial statements using data mining and GAN models. *Expert Systems with Applications*, 227, 120-144.

Alshari, E.A., & Gawali, B.W. (2021). Development of classification system for LULC using remote sensing and GIS. *Global Transitions Proceedings, 2*(1), 8-17.

Ayinla, B.S., Asuzu, O.F., Ndubuisi, N.L., Ike, C.U., Atadoga, A, & Adeleye, R.A. (2024). Utilising data analytics for fraud detection in accounting: A review and case studies. *International Journal of Science and Research Archive, 11*(1), 1348–1363.

Bello, H.O. (2024). Developing predictive financial fraud models using ai-driven analytics within cybercrime-resilient security ecosystems. *International Journal of Research Publication and Reviews, 6*(1), 5055-5069.

Bello, O.A., Ogundipe, A., Mohammed, D., Folorunso A., & Alonge, O.A. (2023). AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities. *European Journal of Computer Science and Information Technology*, *121*(6), 88-106.

Bhattacharjee, S., Islam, M. J., & Abedzadeh, S. (2022). Robust anomaly based attack detection in smart grids under data poisoning attacks. In Proceedings of the 8th ACM on Cyber-Physical System Security Workshop, 3-14.

Chukwuma, O.E., Abdulkarim, S.A., & Abdullahi, M.A. (2025). Corporate governance attributes and the likelihood of fraud on financial statements of listed deposit money

banks in Nigeria. *Fudma Journal of Accounting and Finance Research [FUJAFR], 3*(2), 138-153.

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13* (3), 319-340.

Faccia, A. (2023). National payment switches and the power of cognitive computing against fintech fraud. *Big Data and Cognitive Computing*, *7*(2), 76.

Grimm, S., Schwaar, S., & Holzer, P. (2021). Federated learning for fraud detection in accounting and auditing. *ERCIM NEWS*, 30.

Handoko, B.L., & Rosita, A. (2022). The effect of skepticism, big data analytics to financial fraud detection moderated by forensic accounting. 2022 6th International Conference on E-Commerce, E-Business and E-Government. https://doi.org/10.1145/3537693.3537703.

Hatzivasilis, G., Ioanidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., & Koshutanski, H. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences, 10*(16), 5702.

Kankpang, K.A., Ogar-Abang, O.J., & Animpuye, C. (2024). Forensic accounting and fraud prevention and detection in commercial banks in Nigeria. *Aksu Journal Of Management Sciences (AKSUJOMAS), 9*(1), 106-128.

Kaushik, K., Khan, A., Kumari, A., Sharma, I., & Dubey, R. (2024). Ethical considerations in AI-based cybersecurity. In next-generation cybersecurity: *AI, ML, and Blockchain*, 437-470. Singapore: Springer Nature Singapore.

Naz, I., & Khan, S.N. (2024). Impact of forensic accounting on fraud detection and prevention: a case of firms in Pakistan. *Journal of Financial Crime*. *Journal of Financial Analysis and Investigation, 23*(1), 98-115.

Nyre-Yu, M., Morris, E., Moss, B. C., Smutz, C., & Smith, M. (2022). Explainable AI in cybersecurity operations: Lessons learned from xAI tool deployment. In Proceedings of the Usable Security and Privacy (USEC) Symposium, San Diego, CA, USA, 28.

Ogude, U.C., Nwohiri, A.M., & Ugbaja, G.U. (2022). Review of fraud detection methods and development of a data mining technique for real-time financial fraud detection. *Bayero Journal of Engineering and Technology (BJET), 17*(1), 1-11.

Reis, O., Oliha, J.S., Osasona, F., & Obi, O.C. (2024). Cybersecurity dynamics in Nigerian banking: Trends and strategies. *Review Computer Science & IT Research Journal, 5*(2), 336-364.

Takon, S.M., Mboto, H.W., Obo, E.B., Ogar, G.W., Bekom, A.O., Nkamare, S.E., & Emefiele, C.C. (2023). Effect of fraud on commercial banks' performance in Nigeria. *Paradigm Academic Press Frontiers in Management Science, 2*(2), 69-78.

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security, 23*, 1695–1719.

Vivek, Y., Ravi, V., Mane, A. A., & Naidu, L.R. (2023). ATM fraud detection using streaming data analytics. *arXiv preprint arXiv:2303.04946*.

Xu, J., Yang, T., Zhuang, S., Li, H., & Lu, W. (2024). AI-based financial transaction monitoring and fraud prevention with behaviour prediction.