Journal of Contemporary Accounting and Finance
pISSN: 3115-6606; eISSN: 3156-2809
Affiliated with
Department of Accounting, Federal University Dutsin-Ma, Katsina State, Nigeria

How to Cite this Article: Andortan, A. S., Oboh, J. O., Ofem, D. W., & Obi, O. B. (2026). Effect of Artificial Intelligence on Cybercrime Rate in the Nigeria Banking Sector. *Journal of Contemporary Accounting and Finance (JOCAF)*. 1(1), 32-41. https://doi.org/10.33003/jocaf-2026.v1i1.4.32-41

Effect of Artificial Intelligence on Cybercrime Rate in the Nigeria Banking Sector

ANDORTAN, SOLOMON ANDORTAN[1]*, OBOH, JOHN OGENYI[2], OFEM, DEAN WILLIAM[3] and OBI, OBI BISONG[4]
[1,2,3,4]Department of Accounting, Faculty of Administration and Management Sciences, University of Calabar, Calabar, Cross River State, Nigeria

*Corresponding author: donsolas@gmail.com

ABSTRACT
This study investigates the effect of artificial intelligence on cybercrime in the Nigerian banking sector. Specifically, the study examines the influence of user authentication, transaction monitoring, and secure communication channels on cybercrime in the Nigerian banking sector. The study is anchored on the Technology Acceptance Model (TAM3) and the Fraud Diamond Theory. A survey research design was adopted, and data were collected through structured questionnaires administered to staff of selected deposit money banks in Nigeria. The study employed descriptive statistics and multiple regression analysis to analyze the data. The empirical findings revealed that user authentication, transaction monitoring, and secure communication channels have significant negative effects on cybercrime in the Nigerian banking sector. The study concludes that artificial intelligence plays a crucial role in strengthening cybersecurity frameworks and enhancing fraud-prevention mechanisms within the Nigerian banking sector. Based on the findings, the study recommends that deposit money banks should increase investment in artificial intelligence technologies, strengthen authentication mechanisms, and adopt advanced transaction monitoring systems to mitigate cybercrime threats and protect financial transactions effectively.

Keywords
Artificial Intelligence, Cybercrime Rate, Secure Communication, Transaction Monitoring, User Authentication

1. Introduction

The increasing adoption of digital technologies has transformed the banking sector, leading to significant improvements in financial service delivery through internet banking, mobile banking, electronic payments, and other digital platforms. While these innovations have enhanced operational efficiency and customer convenience, they have also increased financial institutions' vulnerability to cyber threats. Cyber fraud, phishing attacks, identity theft, unauthorized transactions, and other forms of cybercrime have emerged as major challenges for banks worldwide (Humayun et al., 2020).

Nigeria's banking sector has seen a significant rise in cybercrime incidents amid growing reliance on digital financial services. According to the Nigeria Inter-Bank Settlement System (NIBSS, 2023), a total of 95,620 fraud cases were reported in 2023, affecting over 80,000 customers and resulting in financial losses estimated at ₦17.67 billion. Similarly, the Africa Cyber Threat Assessment Report estimated that cyber fraud costs African economies over $4 billion annually, highlighting the growing threat of cybercrime across the continent (African Intelligence, 2024). The increasing sophistication of cybercriminals has exposed the limitations of conventional security approaches, thereby necessitating the adoption of advanced technologies for fraud detection and prevention.

Artificial Intelligence (AI) has emerged as a promising technological solution to strengthen cybersecurity in the banking industry. Through machine learning algorithms, predictive analytics, biometric authentication, and real-time transaction monitoring, AI enables financial institutions to detect suspicious activities, identify emerging threats, and respond more effectively to cyber-attacks (Zhang et al., 2021; Ononokpono et al., 2023). Consequently,

many banks are increasingly integrating AI-driven systems into their cybersecurity frameworks to enhance the security of digital transactions and reduce cybercrime incidents.

Despite the growing adoption of AI technologies in banking operations, cyber fraud remains a persistent challenge within the Nigerian financial sector. Existing studies have largely focused on the opportunities, benefits, and challenges associated with AI adoption (Montasari & Hill, 2019; Becue et al., 2021; Meraj et al., 2022), with limited empirical evidence on the extent to which AI reduces cybercrime in the Nigerian banking sector. This gap necessitates further investigation. Therefore, this study examines the influence of Artificial Intelligence on cybercrime rates in the Nigerian banking sector.

2. Review of literature and hypothesis development

User Authentication and Cybercrime

User authentication is the process of verifying an individual's identity before granting access to a computer system, network, application, or digital platform. It is a critical component of cybersecurity that ensures only authorized users can access sensitive information and perform specific transactions (Stallings, 2022). In the banking sector, user authentication serves as a frontline defence against unauthorized access, financial fraud, identity theft, and other cybercrimes.

Traditionally, authentication relied primarily on usernames and passwords. However, the increasing sophistication of cybercriminals has exposed the weaknesses of password-based systems through phishing, credential theft, malware, and social engineering. Consequently, organizations have adopted stronger authentication mechanisms such as Multi-Factor Authentication (MFA), One-Time Passwords (OTP), biometric authentication, and token-based verification systems (Aloul, 2023).

Authentication methods are generally categorized into three factors: knowledge factors (something the user knows, such as a password), possession factors (something the user has, such as a token or mobile device), and inherence factors (something the user is, such as fingerprints or facial recognition). Modern banking institutions increasingly combine these factors to provide layered security and reduce vulnerabilities to cyber-attacks.

The emergence of Artificial Intelligence (AI) has further enhanced authentication systems through behavioral analytics, adaptive authentication, and anomaly detection. AI-powered authentication solutions can analyze user behaviour patterns, detect suspicious login attempts, and trigger additional verification steps when unusual activity is detected. This capability strengthens cybersecurity frameworks and significantly reduces cybercrime rates in financial institutions (Kumar & Singh, 2024).

Therefore, effective user authentication remains an essential cybersecurity mechanism for protecting digital assets, safeguarding customer information, maintaining trust in online banking services, and reducing cybercrime incidents within the financial sector.

Kumar and Singh (2024) examined the effectiveness of AI-driven multi-factor authentication systems in reducing cyber fraud among commercial banks in India. Using survey data from 215 cybersecurity professionals and Structural Equation Modelling (SEM), the study found that AI-powered authentication systems significantly reduced unauthorized access and account compromise incidents. The study concluded that advanced authentication mechanisms improve cybersecurity performance and fraud prevention.

Hassan et al. (2024) investigated the relationship between biometric authentication and cyber fraud prevention in African financial institutions. The study used panel data from 42 banks across five African countries and analyzed them using fixed-effects regression. Findings revealed that banks adopting biometric authentication recorded significantly lower rates of identity theft and unauthorized account access than institutions relying solely on password-based authentication.

The impact of multi-factor authentication on cybersecurity resilience in digital banking platforms has been examined in China (*Chen et al., 2023*). Data were collected from 180 commercial banks and analyzed using logistic regression. The results showed that the implementation of multi-factor authentication significantly reduced successful cyber intrusion attempts and improved overall transaction security.

Adeyemi and Oladipo (2022) examined the influence of user authentication technologies on electronic banking fraud in Nigeria. Using data obtained from selected deposit money banks and employing Ordinary Least Squares

(OLS) regression analysis, the study found that stronger authentication controls, particularly OTP and biometric verification systems, significantly reduced electronic fraud incidents. The authors recommended increased investment in advanced authentication technologies.

Alshamrani and Alghamdi (2021) investigated the effectiveness of multi-factor authentication in mitigating cyber threats within financial institutions in Saudi Arabia. Using a quantitative research design and survey responses from information security managers, the study found that institutions implementing multi-factor authentication experienced fewer cybersecurity breaches than those relying on traditional password systems.

Ho1. There is no significant relationship between user authentication and cyber crime rate in Nigeria banking sector.

Transaction monitoring and cybercrime

Transaction monitoring is the continuous process of tracking, analyzing, and evaluating financial transactions to identify suspicious, fraudulent, or unusual activities that may indicate cybercrime, money laundering, or other financial misconduct. It is a critical component of cybersecurity and risk management frameworks within financial institutions. Transaction monitoring enables banks and other financial service providers to detect irregular transaction patterns, unauthorized account activities, and potential security breaches in real time (Basel Committee on Banking Supervision, 2023).

Traditionally, transaction monitoring relied on rule-based systems that flagged transactions exceeding predefined thresholds. However, the increasing sophistication of cybercriminals and the growing volume of digital transactions have limited the effectiveness of conventional monitoring systems. Consequently, financial institutions now employ Artificial Intelligence (AI), machine learning, and data analytics technologies to improve the accuracy and speed of fraud detection (Kiron & Unruh, 2023).

AI-powered transaction monitoring systems analyze large volumes of transactional data and customer behaviour patterns to identify anomalies that may indicate fraudulent activity. These systems can detect suspicious behaviors such as unusual fund transfers, rapid transaction sequences, multiple login attempts, and transactions originating from unfamiliar locations. Once detected, alerts are generated for further investigation or immediate intervention (Gupta & Sharma, 2024).

In the banking sector, effective transaction monitoring contributes significantly to fraud prevention, regulatory compliance, anti-money laundering (AML) efforts, and cybersecurity enhancement. By identifying threats before substantial damage occurs, transaction monitoring helps reduce cybercrime rates, protect customer assets, and maintain confidence in digital financial services. Consequently, it has become one of the most important AI-enabled security mechanisms in modern banking operations.

Gupta and Sharma (2024) investigated the effectiveness of AI-powered transaction-monitoring systems in detecting financial fraud in commercial banks in India. Using data from 35 banks and applying logistic regression analysis, the study found that AI-based monitoring systems significantly improved fraud detection accuracy and reduced fraudulent transaction losses. The study concluded that transaction monitoring enhances cybersecurity effectiveness in financial institutions.

Mohammed et al. (2024) examined the influence of real-time transaction monitoring on cyber fraud prevention in Middle Eastern banks. Using survey data collected from 210 information security professionals and analyzing responses using Structural Equation Modelling (SEM), the study found that real-time monitoring significantly improved early fraud detection and reduced successful cyberattacks on banking platforms.

Li et al. (2023) assessed the impact of machine-learning-based transaction-monitoring systems on cybersecurity performance in Chinese digital banking institutions. Using panel data from 120 financial institutions, the study found that advanced transaction-monitoring technologies significantly reduced unauthorized electronic transactions and strengthened fraud control mechanisms.

Adewale and Okonkwo (2022) investigated the relationship between transaction monitoring systems and electronic fraud prevention in Nigerian deposit money banks. Using Ordinary Least Squares (OLS) regression analysis, the study found that effective transaction monitoring significantly reduced online banking fraud and

improved the security of electronic payment systems. The researchers recommended greater investment in automated monitoring technologies.

Redhead (2021) examined the role of automated transaction monitoring in combating cybercrime within financial institutions in the United Kingdom. The study adopted a quantitative research design and analyzed data from 75 commercial banks. Findings indicated that institutions using advanced transaction monitoring tools experienced significantly lower fraud rates and faster response times to suspicious activity than banks relying on traditional monitoring systems.

Ho2. There is no significant relationship between transaction monitoring and cyber crime rate in Nigeria banking sector.

Secure Communication and Cybercrime

Secure communication is the process of transmitting information between parties in a manner that protects the confidentiality, integrity, and authenticity of the data from unauthorized access, interception, modification, or disclosure. It is a fundamental component of cybersecurity that ensures sensitive information remains protected while being transmitted across digital networks. Secure communication is achieved through various security mechanisms, including encryption, cryptographic protocols, Secure Sockets Layer (SSL), Transport Layer Security (TLS), virtual private networks (VPNs), and end-to-end encryption technologies.

In the banking sector, secure communication is critical for safeguarding customer information, financial transactions, login credentials, and other confidential data exchanged over digital channels. As cybercriminals increasingly target online banking systems through phishing, man-in-the-middle, and data-interception attacks, and through malware, financial institutions have strengthened their communication infrastructure with advanced encryption and secure communication protocols.

The advancement of Artificial Intelligence (AI) and modern cryptographic technologies has further enhanced secure communication systems by enabling real-time threat detection, adaptive encryption, intrusion prevention, and secure data transmission. These technologies help organizations identify vulnerabilities, prevent unauthorized access, and maintain the integrity of digital communications. Consequently, secure communication has become an essential mechanism for reducing cybercrime, protecting customer trust, ensuring regulatory compliance, and maintaining the security of digital financial services.

Khan et al. (2024) developed the FinSafeNet framework to enhance the security of financial transactions through optimized deep learning techniques. Using experimental analysis and financial transaction datasets, the study found that secure communication systems integrated with advanced encryption and intelligent threat detection significantly improved transaction security and reduced cyber fraud incidents. The study concluded that secure communication infrastructure is vital for financial cybersecurity.

Fauziyah et al. (2024) examined the effectiveness of a multilayered cryptographic protocol in enhancing secure communication systems. Using simulation experiments and cybersecurity performance testing, the study found that multilayered encryption significantly improved data confidentiality, integrity, and resistance to cyber-attacks. The researchers concluded that secure communication protocols strengthen organizational cybersecurity frameworks.

Melo et al. (2024) investigated a visual two-factor authorization protocol for secure electronic banking communication. Using experimental evaluation within internet banking environments, the study found that secure communication channels combined with strong authentication mechanisms significantly reduced unauthorized access and transaction manipulation. The authors concluded that secure communication is essential for protecting digital banking systems from cyber threats.

Gounari et al. (2024) analyzed secure communication standards and cybersecurity compliance within the European open banking framework. Using regulatory and institutional data, the study found that financial institutions implementing strong encryption and secure communication protocols experienced fewer cybersecurity incidents and improved customer trust. The study emphasized the importance of secure communication in modern banking operations.

Ali et al. (2024) examined advanced graph-based encryption algorithms for secure communication in digital environments. Using experimental cryptographic analysis, the study revealed that enhanced encryption techniques improved data confidentiality and protected communication channels against interception and cyber-attacks. The study concluded that robust secure communication mechanisms are effective tools for reducing cybersecurity vulnerabilities.

Ho3. There is no significant relationship between secure communication and the cybercrime rate in Nigeria's banking sector.

Theoretical Framework

Technology Acceptance Model

The Technology Acceptance Model 3 by Venkatesh and Bala in 2008, an extension of the original Technology Acceptance Model (TAM) developed by Davis in (1989). It was later updated to TAM2 by Viswanath Venkatesh and Fred Davis in 2000, and then further extended to TAM3 by Venkatesh and Bala in 2008. The theory explains how users form attitudes and intentions towards adopting and using new technologies, such as Artificial Intelligence (AI). It proposes that users' behavioral intentions are influenced by six key factors: Perceived Usefulness, Perceived Ease of Use, Social Influence, Facilitating Conditions, Individual Differences, and System Characteristics. These factors interact to shape users' attitudes, intentions, and ultimately, their actual use of the technology. TAM 3 is relevant to this study by helping to understand how bank employees and customers perceive the usefulness and ease of AI-driven systems reducing cyber crime rate in the banking sector.

3. Methodology

This study adopted a survey research design to examine the effect of artificial intelligence on cybercrime rate in the Nigerian banking sector. The study was conducted among staff of fourteen deposit money banks operating in Calabar (Table 1), Cross River State, Nigeria, namely Access Bank Plc, First Bank of Nigeria Plc, Guaranty Trust Bank Plc, United Bank for Africa (UBA) Plc, Zenith Bank Plc, Fidelity Bank Plc, First City Monument Bank (FCMB), Keystone Bank Plc, Stanbic IBTC Bank Plc, Union Bank of Nigeria Plc, Sterling Bank Plc, Wema Bank Plc, Polaris Bank Plc, and Ecobank Nigeria Plc. The population of the study comprised 880 bank employees. The sample size of 275 respondents was determined using the Taro Yamane formula and proportionately allocated to the selected banks using Bowley's proportional allocation technique (Table 2). Data were collected through a structured questionnaire designed to measure the study variables: user authentication, transaction monitoring, secure communication, and cybercrime rate.

The instrument's validity was established through expert review, and reliability was assessed using Cronbach's Alpha, with a coefficient threshold of 0.70 considered acceptable. Data were analyzed using descriptive statistics, including frequencies, percentages, means, and standard deviations, and the hypotheses were tested using multiple regression analysis. The model specified cybercrime rate as the dependent variable and user authentication, transaction monitoring, and secure communication as the explanatory variables.

The sample size for this study was determined using the Taro Yamane formula for finite populations:

$n = N/ 1+N(e)^2$

Where N = population (880)

n = Sample Size

e = 0.05

$n = 880 /1+ 880 (0.05)^2$

$n = 880 /1+ 880 (0.0025)$

$n = 880 /1+2.2$

$n = 880/3.2$

$n= 275$

Therefore, the study's sample size is 275 respondents.

Table 1: Population Distribution of Staff in Selected Deposit Money Banks in Calabar

S/N	Bank	Staff Population
1	Access Bank Plc	95
2	First Bank of Nigeria Plc	110
3	Guaranty Trust Bank Plc	85
4	United Bank for Africa Plc	80
5	Zenith Bank Plc	90
6	Fidelity Bank Plc	60
7	First City Monument Bank (FCMB)	55
8	Keystone Bank Plc	40
9	Stanbic IBTC Bank Plc	45
10	Union Bank of Nigeria Plc	50
11	Sterling Bank Plc	35
12	Wema Bank Plc	30
13	Polaris Bank Plc	45
14	Ecobank Nigeria Plc	60
Total	880	

Source: Field Survey (2026).

Table 2: Proportionate Allocation of Sample Size

S/N	Bank	Population	Sample Allocation
1	Access Bank Plc	95	30
2	First Bank of Nigeria Plc	110	34
3	Guaranty Trust Bank Plc	85	27
4	United Bank for Africa Plc	80	25
5	Zenith Bank Plc	90	28
6	Fidelity Bank Plc	60	19
7	FCMB	55	17
8	Keystone Bank Plc	40	13
9	Stanbic IBTC Bank Plc	45	14
10	Union Bank Plc	50	16
11	Sterling Bank Plc	35	11
12	Wema Bank Plc	30	9
13	Polaris Bank Plc	45	14
14	Ecobank Nigeria Plc	60	18
Total	880	275	

Source: Researcher's computation (2026) using Bowley's 1926 formula

The model specification for this study is based on the following multiple regression equation: $CC=\beta0+\beta1UA+\beta2TM+ \beta3SCC+ \epsilon$

Where:

CC = cybercrime rate (dependent variable)
UA = User authentication
TM = Transaction monitoring
SCC = Secure communication channel
ϵ = Error term

4. Results

The descriptive statistics (Table 3) present the distribution of responses regarding Artificial Intelligence dimensions and cybercrime rate among staff of selected deposit money banks in Calabar. The mean score for User Authentication (3.76) indicates that respondents generally perceive authentication mechanisms such as biometric verification, one-time passwords (OTP), and multi-factor authentication as widely used in the banking sector. Transaction Monitoring recorded a mean value of 3.68, suggesting that banks employ monitoring systems to detect

suspicious transactions and fraudulent activities. Similarly, Secure Communication recorded a mean score of 3.59, indicating a moderate to high implementation of encrypted communication channels and secure data transmission systems.

Table 3: Descriptive Statistics

Variable	N	Minimum	Maximum	M	SD
Cybercrime Rate (CR)	275	1.00	5.00	3.12	0.84
User Authentication (UA)	275	1.00	5.00	3.76	0.71
Transaction Monitoring (TM)	275	1.00	5.00	3.68	0.75
Secure Communication (SC)	275	1.00	5.00	3.59	0.79

Source: Researcher Computation from SPSS, 2026

The mean value for Cybercrime Rate (3.12) suggests that cybercrime remains a concern despite the adoption of AI-driven security mechanisms. The standard deviation values, which range from 0.71 to 0.84, indicate a moderate level of variation in respondents' opinions. Overall, the findings suggest that AI-enabled security measures are widely implemented across the selected deposit money banks and are perceived as important tools for mitigating cybercrime.

Table 4: Regression results

Variable	β	SE	*t*	*p*
Constant	1.245	0.384	3.24	.002
User Authentication (UA)	-0.312	0.087	-3.59	< .001
Transaction Monitoring (TM)	-0.276	0.094	-2.94	.004
Secure Communication Channel (SCC)	-0.241	0.089	-2.71	.008

Source: Researcher Computation from SPSS, 2026

H_{01}: There is no significant relationship between user authentication and cybercrime rate in the Nigerian banking sector.

The regression result (Table 4) revealed that user authentication has a coefficient of **β = -0.312** and a **p-value of 0.000**, which is less than the 0.05 level of significance. This indicates that user authentication has a significant negative effect on the cybercrime rate in the Nigerian banking sector. The negative coefficient implies that improvements in authentication mechanisms lead to a reduction in cybercrime incidents. Therefore, the null hypothesis is rejected.

This finding is consistent with the empirical evidence reviewed in the literature. Specifically, Chen et al. (2023) found that implementing multi-factor authentication significantly reduced successful cyber intrusion attempts and enhanced transaction security on Chinese digital banking platforms. Similarly, Kumar and Singh (2024) reported that AI-driven multi-factor authentication systems significantly reduced unauthorized access and account compromise incidents among commercial banks in India. The result also corroborates the findings of Hassan et al. (2024), who observed that banks adopting biometric authentication experienced lower levels of identity theft and unauthorized account access. Within the Nigerian context, the finding aligns with Adeyemi and Oladipo (2022), who found that stronger authentication controls, such as one-time passwords (OTP) and biometric verification, significantly reduced electronic banking fraud. The result further supports the study of Alshamrani and Alghamdi (2021), which established that institutions enhanced transaction security on Chinese digital banking platforms. Therefore, the present study confirms that effective user authentication is a critical cybersecurity mechanism for reducing cybercrime in the Nigerian banking sector.

H_{02}: There is no significant relationship between transaction monitoring and cybercrime rate in the Nigerian banking sector.

The regression analysis showed that transaction monitoring has a coefficient of **β = -0.276** and a **p-value of 0.004**, which is below the 0.05 significance threshold. This indicates that transaction monitoring significantly and negatively affects the cybercrime rate in the Nigerian banking sector. Consequently, the null hypothesis is rejected.

This finding is in line with prior empirical studies reviewed in Chapter Two. For instance, Gupta and Sharma (2024) found that AI-powered transaction monitoring systems significantly improved fraud detection accuracy

and reduced fraudulent transaction losses in commercial banks. Likewise, Mohammed et al. (2024) reported that real-time transaction monitoring enhanced early fraud detection and reduced successful cyberattacks on banking platforms. The finding also aligns with Li et al. (2023), who found that machine-learning-based transaction-monitoring systems significantly reduced unauthorized electronic transactions and strengthened fraud control mechanisms in Chinese banking institutions. In Nigeria, Adewale and Okonkwo (2022) established that effective transaction monitoring significantly reduced online banking fraud and improved the security of electronic payment systems. Similarly, Redhead (2021) found that financial institutions utilizing advanced transaction monitoring tools experienced lower fraud rates and faster responses to suspicious activities. Therefore, the present study reinforces the argument that transaction monitoring is an effective mechanism for detecting and preventing cybercrime in the banking sector.

H_{03}: There is no significant relationship between secure communication channels and cybercrime rate in the Nigerian banking sector.

The regression result revealed that secure communication channels have a coefficient of **β = -0.241** and a **p-value of 0.008**, which is less than the 0.05 significance level. This indicates that secure communication channels significantly reduce cybercrime rate in the Nigerian banking sector. Accordingly, the null hypothesis is rejected.

This finding is consistent with several empirical studies reviewed in the literature. Khan et al. (2024) found that secure communication systems integrated with advanced encryption technologies significantly improved transaction security and reduced cyber fraud incidents. Similarly, Fauziyah et al. (2024) reported that multilayered cryptographic protocols enhanced data confidentiality, integrity, and resistance to cyberattacks. The finding also supports the study of Melo et al. (2024), which found that secure communication channels combined with strong authentication mechanisms significantly reduced unauthorized access and transaction manipulation in electronic banking environments. Furthermore, Gounari et al. (2024) established that financial institutions implementing strong encryption and secure communication protocols experienced fewer cybersecurity incidents and improved customer trust. The result is also consistent with Ali et al. (2024), who found that advanced encryption algorithms enhanced data confidentiality and protected communication channels from cyberattacks. Therefore, the present study confirms that secure communication infrastructure is an important tool for reducing cybercrime and strengthening cybersecurity within the Nigerian banking sector.

5. Conclusion

This study examined the effect of artificial intelligence on cybercrime rate in the Nigerian banking sector using user authentication, transaction monitoring, and secure communication channels as proxies for AI-driven security mechanisms. The findings revealed that all three variables have significant negative effects on cybercrime rate, indicating that enhanced authentication systems, effective transaction monitoring, and secure communication infrastructures contribute substantially to reducing cybercrime incidents in the banking sector. The study therefore concludes that the adoption and effective implementation of artificial intelligence-enabled security mechanisms play a crucial role in strengthening cybersecurity and mitigating cybercrime in Nigerian banks.

Recommendations

Based on the findings, the study recommends that banks strengthen user authentication by adopting advanced technologies, such as biometric verification, one-time passwords, and multi-factor authentication. Financial institutions should also invest in artificial intelligence-powered transaction monitoring systems to facilitate real-time detection and prevention of fraudulent activities. Additionally, banks should enhance their secure communication infrastructure by implementing robust encryption technologies and secure communication protocols to protect sensitive financial information and reduce exposure to cyber threats. These measures will collectively improve cybersecurity resilience and further reduce cybercrime in the Nigerian banking sector.

References

Adewale, T. O., & Okonkwo, C. J. (2022). Transaction monitoring systems and electronic fraud prevention in Nigerian banks. *Journal of Financial Crime*, 29(3), 821-837.

Adeyemi, T. A., & Oladipo, A. O. (2022). User authentication technologies and electronic banking fraud prevention in Nigeria. *Journal of Financial Crime*, 29(4), 1158-1173.

African Intelligence. (2024). *Africa cyber threat assessment report*. Interpol African Cybercrime Operations Desk.

Ali, N., Sadiqa, A., Shahzad, M. A., Qureshi, M. I., Siddiqui, H. M. A., Abdallah, S. A. O., & Abd El-Gawaad, N. S. (2024). Secure communication in the digital age: A new paradigm with graph-based encryption algorithms. *Frontiers in Computer Science*, 6, Article 1454094. [Crossref]

Aloul, F. (2023). Multi-factor authentication and cybersecurity enhancement in digital systems. *International Journal of Information Security*, 22(3), 421-435.

Alshamrani, A., & Alghamdi, F. (2021). The role of multi-factor authentication in reducing cyber threats in financial institutions. *Journal of Cyber Security Technology*, 5(2), 89-104.

Basel Committee on Banking Supervision. (2023). *Principles for operational resilience and risk monitoring in banking institutions*. Bank for International Settlements.

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, 54(5), 3849-3886. [Crossref]

Chen, Y., Wang, H., & Liu, X. (2023). Multi-factor authentication and cybersecurity resilience in digital banking platforms. *Computers & Security*, 126, Article 103051.

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

Fauziyah, Wang, Z., & Tabassum, M. (2024). A holistic secure communication mechanism using a multilayered cryptographic protocol to enhance security. *Computers, Materials & Continua*, 78(3), 4417-4452. [Crossref]

Gounari, M., Stergiopoulos, G., Pipyros, K., & Gritzalis, D. (2024). Harmonizing open banking in the European Union: An analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards. *International Cybersecurity Law Review*, 5(1), 79-120. [Crossref]

Gupta, R., & Sharma, P. (2024). Artificial intelligence-based transaction monitoring and fraud detection in commercial banks. *Journal of Information Security and Applications*, 79, Article 103642.

Hassan, M., Ibrahim, S., & Ahmed, K. (2024). Biometric authentication and cyber fraud prevention in African financial institutions. *African Journal of Information Systems*, 16(1), 44-61.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering*, 45(5), 3171-3189. [Crossref]

Khan, A. R., Ahamad, S. S., Mishra, S., Khan, M. A. R., Sharma, S. K., AlEnizi, A., & Kumar, M. (2024). FinSafeNet: Securing digital transactions using optimized deep learning and multi-kernel PCA with Nyström approximation. *Scientific Reports*, 14, Article 26853. [Crossref]

Kiron, D., & Unruh, G. (2023). Artificial intelligence and financial fraud detection: Emerging trends in transaction monitoring. *MIT Sloan Management Review*, 64(2), 45-52.

Kumar, R., & Singh, P. (2024). Artificial intelligence-driven authentication systems and cyber fraud reduction in commercial banks. *Journal of Information Security and Applications*, 78, Article 103617.

Li, J., Chen, Y., & Wang, X. (2023). Machine learning-driven transaction monitoring and cybersecurity performance in digital banking. *Computers & Security*, 125, Article 103016.

Melo, L. P., Amaral, D. M., Albuquerque, R. O., Sousa Júnior, R. T., Orozco, A. L. S., & García Villalba, L. J. (2024). A secure approach out-of-band for e-banking with visual two-factor authorization protocol. *Cryptography*, 8(4), Article 51. [Crossref]

Meraj, F., Ansari, M. F., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cyber security: A literature review. *International Journal of Advanced Research in Computer and Communication Engineering*, 11(9), 1-8. [Crossref]

Mohammed, S., Hassan, M., & Ali, A. (2024). Real-time transaction monitoring and cyber fraud prevention in banking institutions. *International Journal of Information Management Data Insights*, 4(1), Article 100245.

Montasari, R., & Hill, R. (2019). *Cybercrime and digital forensics: An introduction*. Routledge.

Nigeria Inter-Bank Settlement System. (2023). *Annual fraud landscape report*. NIBSS.

Ononokpono, D., Effiong, E., & Okon, A. (2023). Artificial intelligence milieu: Implications for corporate performance in the Nigerian banking industry. *International Journal of Research and Innovation in Applied Science*, 8(5), 34-44. [Crossref]

Redhead, M. (2021). The future of transaction monitoring: Better ways to detect and disrupt financial crimes. Royal United services institute. SSRN Working Paper.

Stallings, W. (2022). *Network security essentials: Applications and standards* (7th ed.). Pearson.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, 39(2), 273-315. [Crossref]

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186-204. [Crossref]

Zhang, P., Haenlein, M., Kaplan, A., & Tan, C. W. (2019). Artificial intelligence (AI) and management analytics. *Journal of Management Analytics*, 6(4), 341-343. [Crossref]