FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 2, January, 2026, pp 175 – 183
DOI: https://doi.org/10.33003/fjs-2026-1002-4491

STRENGTHENING FINANCIAL INTEGRITY: THE ROLE OF CYBERSECURITY IN MITIGATING FINANCIAL FRAUD IN NIGERIA'S BANKING SECTOR

***[1]Folasade Mercy Okikiola, [2]Taiwo Shukurat Arogundade, [3]Isaac Onadokun, [4]Olasunkanmi Esther Oladiboye and [5]Adetunji Kazeem Sodiq**

[1,3,4,] Computer Technology Department, Yaba College of Technology, Nigeria.
[5]Computer Engineering Department, Yaba College of Technology, Nigeria
[2]Computer Science Department, Federal University Oye-Ekiti, Nigeria

*Corresponding authors' email: sade.mercy@yahoo.com

ABSTRACT

In the era of digital transformation, cybersecurity has become crucial to the banking industry, particularly in safeguarding financial institutions against the escalating threats of fraud and cybercrime. This study examines the role of cybersecurity in mitigating financial fraud in Nigeria's banking sector, with a specific focus on three major commercial banks: UBA, GT Bank, and Access Bank. Employing a descriptive research design, data were collected from 109 staff members across different departments through structured questionnaires. The collected data were analyzed using SPSS for quantitative analysis and NVivo for thematic content analysis. Findings from the study reveal that Nigerian banks have taken significant steps to enhance cybersecurity. Key practices identified include the implementation of multi-factor authentication, routine system, software updates, continuous staff training, and the use of firewalls and encryption technologies. These measures have proven effective in reducing internal threats and unauthorized system access. However, the study also highlights persistent challenges. Low customer cybersecurity awareness contributes significantly to phishing and social engineering attacks. Inadequate real-time monitoring systems hinder rapid threat detection and response. The study concludes that while progress has been made, a more integrated and proactive approach is required to further secure Nigeria's financial ecosystem.

Keywords: Cybersecurity, Cyber threat, Financial Fraud, Nigerian Banks, Digital Banking

INTRODUCTION

In recent years, technological advancements have presented both unprecedented opportunities and challenges, particularly in the realm of cybersecurity. The advent of digital banking has led to a higher transactional volume within Nigeria's financial sector, increasing fraud incidents. Significantly, Nigerian banks incurred losses over N42.6 billion due to fraud and forgeries in the second quarter of 2024, exceeding the entire fraud losses recorded in 2023 (Naira metrics, 2024) In the increasingly digital landscape of the 21st century, cybersecurity has become a vital component in safeguarding the integrity, confidentiality, and availability of financial data within the global financial sector. Effective cybersecurity measures are essential in defending against various cyber threats that financial institutions encounter, including data breaches, financial fraud, ransomware attacks, and more. These threats not only pose significant financial risks but also damage customer trust and the overall stability of the global financial system (Abrahams et al., 2024). Fraud is a scourge that has profoundly affected Nigeria's financial sector and the economy at large. Nugraha & Bayunitri (2020) define fraud as the deliberate conduct by one or more persons within management, personnel, or third parties that may lead to the misrepresentation of financial statements. Manipulation, fabrication, or modification of supporting documentation; misappropriation of assets; fraudulent activities, including the concealment or omission of transaction consequences from records or documents; transaction documentation lacking substance; and distorted accounting standards (Badejo,2018). Fraud prevention entails the identification of dubious transactions within the banking sector and the mitigation of potential financial or reputational damage to clients or other financial institutions. As online and mobile banking continue to grow, and financial institutions increasingly digitize their services, having a robust fraud protection plan becomes essential. The banking sector, in particular, has greatly benefited from the rapid advancements and results-oriented nature of information technology. This technology has a profound impact, continually influencing human activities across various fields and eras. Digital technologies and the Internet of Things are at the center of this planned revolution. As the Internet became more widely used for commercial purposes, the quantity and variety of computer crimes grew. Although one aspect of a crime may have been conducted via an electronic device, in certain instances, the majority of crimes are perpetrated online or through technological processes. According to (Ahmed,2020), cybercrime refers to crimes that take place in the internet's cybernetic community, commonly known as cyberspace. These rising levels of fraud and crime forced the development of cybersecurity, which aims to reduce, eliminate cyber-fraud and other related crimes in today's ever-changing human society. Cybersecurity is a crucial pillar in Nigeria's National Digital Economy Policy and Strategy, which outlines a vision for diversifying the country's economy (National Digital Economy Policy and Strategy,2020). The importance of cybersecurity is illustrated in Figure 1.

Figure 1: Importance of Cybersecurity

The 2021 Nigerian National Cybersecurity Policy and Strategy specify the banking, finance, and insurance industry as one of its thirteen important information infrastructure sectors and outlines the Nigerian government's strategy for safeguarding key information infrastructure. The NCPS seeks to defend Nigeria's digital economy by enhancing the legal and regulatory environment and aligning laws concerning e-business and online consumer rights, among other issues. CBN created the Consumer Protection Department in April 2012 to formulate and execute a robust consumer protection framework and enhance consumer trust in the financial system. The department executes three principal functions: complaints handling, market conduct and development, and consumer education and financial literacy. The banking sector is currently adopting cloud computing for several applications. According to Gartner, he projected that the global public cloud market would expand by 23.1 percent in 2021, indicating a high frequency of utilisation for these services. From 2019 to 2021, most enterprises transitioned to cloud-based transactions for their operations. IT professionals exhibit reluctance to increase migration due to the security, management, and compliance challenges linked to cloud-based data and application storage. They fear that highly confidential firms may accidentally disclose information about individuals and organisations, potentially leading to the disclosure of financial data and intellectual property. Ahmed et al. (2020) report that 95% of hackers distribute spyware by establishing trust with individuals, therefore persuading them to visit a website, provide login credentials, or download a malicious file while impersonating a friend, cashier, or manager. Banks may empower their workers to identify the indicative signs of online fraud, such as emails prompting customers to access the website or pop-up advertisements proposing free items in return for completing a personal survey. Contemporary fraudsters use advanced strategies and technologies to execute their nefarious actions effectively. Despite substantial advancements in fraud protection technologies, ongoing vigilance is essential. A data breach occurs when a fraudster infiltrates a firm's network and extracts data from a database. Fraudsters often seek customers' data, credit card information, and other personally identifying details. Subsequent to the data acquisition, it is disseminated on the Dark Web. The methods used by a fraudster may differ, but the outcome is often same. Moreover, assailants often modify their methodologies. The following are several popular kinds of fraud that persist today. The purpose of a denial of service (DoS) assault is to deplete a website's computational resources, resulting in a crash. A fraudster may control a botnet including hundreds or thousands of compromised machines to do regular activities like form completion.

Malware, an abbreviation for "malicious software," encompasses a wide range of dangerous programs, including viruses, ransomware, and spyware. The Creeper virus, first detected in the 1970s, has been a threat to individuals and organisations. Phishing is a technique used to get valuable information from workers inside an organisation. The phishing communication will use an email, text message, phone call, or other forms of contact to mislead the victim into revealing personal information or permitting malware installation on their device. Ransomware encrypts data on the compromised device and solicits a ransom (Zheng,2020). The fraudster will submit a compensation claim to get the encryption key necessary for regaining access to your data. Cyber fraud is a persistent concern that jeopardises both human existence and the infrastructure of nation-states (Antonucci, 2017). Countries are implementing substantial measures to safeguard their cyberspace from threats and vulnerabilities that may result in billions of dollars in property damage, financial theft, and breakdowns in essential national infrastructure. These initiatives seek to protect against cyberattacks and cybercrime (Ahmed et al.,2020). Cybercrime is on the rise globally (Buchanan, 2016), resulting in billions of dollars in damage for individuals, businesses, organisations, and governments (Antonucci,2017). The Nigerian banking system has seen a notable increase in financial fraud, including identity theft, phishing, unauthorised access, and electronic payment diversion. As financial services become more digitized, banks have emerged as primary targets for hackers aiming to exploit system flaws. Despite measures to enforce security protocols, the prevalence and complexity of cyberattacks persistently increase, eroding consumer confidence and financial stability. A significant issue is the apparent gap between current cybersecurity systems and their efficacy in proactively identifying and alleviating fraudulent actions. Numerous financial organisations contend with outdated infrastructure, inadequate cybersecurity proficiency, and an absence of thorough regulatory enforcement. As a consequence, fraudsters often evade security mechanisms, leading to significant financial losses. This scenario raises important enquiries on the sufficiency of existing cybersecurity measures in Nigerian banks and their effectiveness in mitigating fraud. It is essential to investigate the role of cybersecurity in mitigating these risks and to develop solutions for enhancing digital defences to maintain the integrity and dependability of banking operations in Nigeria. The specific objectives are: To assess the current

cybersecurity measures implemented by Nigerian banks in preventing financial fraud, to evaluate the impact of cyber threats and vulnerabilities on the financial performance and reputation of Nigerian banks, and to identify the challenges and limitations faced by banks in implementing effective cybersecurity strategies.

MATERIALS AND METHODS

Literature Review

The increasing reliance on digital technologies in the Nigerian banking sector has brought about significant improvements in service delivery and financial inclusion. However, it has also led to a surge in financial fraud, posing a serious threat to both financial institutions and consumers. Cybersecurity threats, especially in the financial service sector, are now associated with the use of sophisticated technologies to exploit the vulnerabilities of computer servers to carry out cybercrime or fraud (Bromwich, J. E., 2016). The related studies on this research have been summarized in the table below (Table 1), which provides the research methodologies along with the findings.

Table 1: Overview of Related Studies

Author(s)	Title	Methodology	Findings
Nte *et al*. (2022)	An Evaluation of the Challenges of Mainstreaming Cybersecurity Laws and Privacy Protection in Nigeria	Qualitative research using legal and policy document analysis.	Qualitative review of Nigerian cybersecurity laws; highlights privacy rights, regulatory gaps, and recommendations for stronger legal frameworks.
Rjoub *et al*.(2023)	A survey on explainable artificial intelligence for cybersecurity	Systematic literature review (SLR) of XAI applications.	Reviews XAI techniques in network cybersecurity, focusing on interpretability, current challenges, and future directions to enhance trust in ML-based defenses
Becher & Torka (2024).	Exploring AI-Enabled Cybersecurity Frameworks: Deep-Learning Techniques, GPU Support, and Future Enhancements	Empirical analysis of real-world frameworks with case studies.	Assesses real-world AI-based cybersecurity frameworks, focusing on deep learning models and the importance of GPU support in detecting dynamic threats.
Obi et al. (2024)	Comprehensive review on cybersecurity: modern threats and advanced defense strategies.	Comprehensive literature review of modern threats	Analyzed contemporary cybersecurity threats (APTs, phishing), and defense strategies.
Abdulkareem (2025)	The role of cybersecurity awareness in safeguarding digital systems in institution of higher learning.	A descriptive survey design was employed.	Survey-based study in Kontagora, Nigeria; emphasizes training and continuous awareness to combat phishing & malware.
Ogunyemi (2024)	Cyber Risks and the Nigerian Business Sector: A Critical Analysis of the Emerging Cyber Insurance Market in Nigeria	Mixed-methods research design, the study integrates descriptive analysis, correlation, and regression techniques.	Explored the growing threat of cyber risk exposure and its implications for Nigerian businesses, focusing on how these threats affect financial security, operational continuity, profitability, and demand for cyber insurance.
Okoroiwu et al. (2024)	Financial Institutions Cyber Security Incidents and Economic Growth of Nigeria.	An ex-post facto research design and time series data analysis were used.	Investigated the impact of cybersecurity incidents on Nigeria's economic growth, focusing on the banking sector from 2002 to 2022.
Olaniyan et al. (2021)	Forensic accounting as an instrument for fraud detection and prevention in the public sector: moderating on ministries, departments and agencies in Nigeria	A cross sectional Survey design was adopted	Examined the use of forensic accounting in Nigeria as a tool for fraud detection and prevention, they discovered, using original data spanning ten (10) years, from 2010 to 2020, that financial analysis is useful and advantageous in preventing fraud, even though foreign currencies cannot control fraud.
Akintoye et al. (2022)	Cyber security and financial innovation of selected deposit money banks in Nigeria	Survey research design	Explored how cybersecurity affects financial innovation in Nigerian Deposit Money Banks.
Garba et al. (2022)	An assessment of cybersecurity awareness level among Northeastern University students in Nigeria	Survey-based quantitative study among university students.	Assessed the cybersecurity awareness level among students in Northeastern University. The study highlights the need for awareness programs to increase students' cybersecurity knowledge, particularly in the Northeastern region of Nigeria

Author(s)	Title	Methodology	Findings
Kolade (2022)	Cybersecurity in Nigeria's financial industry: Enhancing consumer trust and security	Comparative case study across six African countries.	Kolade (2022) highlighted the importance of cybersecurity in Nigeria's financial industry, emphasizing the need to enhance consumer trust and security. The study explored six country case studies, including Nigeria, to capture the diversity of financial markets on the African continent

An in-depth analysis of the related studies reveals the need for interdisciplinary and context-specific strategies to address cybersecurity risks. The studies collectively highlight the evolving nature of cyber threats, the dual-use potential of AI, and the urgent need for integrated approaches that combine technology, policy, education, and financial safeguards to build resilient digital systems.

Research Methodology

Research design

This study has employed a descriptive research design to gather necessary data. Descriptive research aims to depict situations, individuals, or events, revealing natural relationships. It serves as an all-inclusive approach that connects viable empirical research with conceptual research queries.

Participants

The intended population includes all employees working in commercial banks. Out of 21 commercial banks in Lagos State, U.B.A, GT Bank and Access Bank were selected by stratified random selection. A total of 150 workers were chosen at random from the three commercial banks to which made up the sample size of 109 using the Slovin formula, n = N/(1+Ne2), which was invented by Robert Slovin (1960, p.2), where n = Sample Size, N = Total Population = 150 e = Margin of error at 5% 1 = Constant. The sample size for this study was calculated from a population of one hundred and fifty (150) employees in the three banks.

Therefore, substituting it into the formulae, we obtained:

n = 150

1+150 (0.05)2

n = 150

1.375

n = 109

Instruments

A closed-ended questionnaire was the main tool employed in this investigation. 24 items was included in the questionnaire, using Likert scales to collect responses from the 109 respondents who were chosen to make up the sample size. Four sections—Sections A, B, C, and D made up the questionnaire. Section A comprises the respondent's biographical information, including age, sex, qualifications, company name, and years of experience. Sections B, C, and D were constructed using a Likert four-point rating scale and were represented in the table column using its shortened words.

RESULTS AND DISCUSSION

Demographic Characteristics of the Respondents

Table 2: Demographic Analysis

	Frequency	Percent	Valid Percent	Cumulative Percent
Gender				
Male	59	54.1	54.1	54.1
Female	50	45.9	45.9	100.0
Age Range				
20-30	61	56.0	56.0	56.0
31-40	43	39.4	39.4	95.4
41-others	5	4.6	4.6	100.0
Bank				
GT Bank	38	34.9	34.9	34.9
U.B.A	44	40.4	40.4	75.2
Access	27	24.8	24.8	100.0
Department				
Information Technology	65	59.6	59.6	59.6
Operation	20	18.3	18.3	78.0
Customer Service	9	8.3	8.3	86.2
Compliance	15	13.8	13.8	100.0

The demographic characteristics of the respondents as obtained from the filled and returned structured questionnaire were presented and analyzed in Table 2. The gender distribution analysis indicates that out of a total of 109 respondents, 59 (54.1%) are male, while 50 (45.9%) are female. This shows a slightly higher representation of males compared to females in the study population. The valid per cent and cumulative per cent confirm the accuracy of the data, with no missing values. This distribution suggests that both genders are fairly represented, enabling meaningful comparisons and generalizations. The age distribution analysis shows that the majority of respondents fall within the 20–30 age range, accounting for 61 individuals or 56% of the total sample. This is followed by the 31–40 age group, which comprises 43 respondents or 39.4%. Only 5 participants (4.6%) fall into the 41 and above category. This suggests that the sample is predominantly young adults, with fewer middle-aged or older participants. The bank distribution analysis indicates that among the 109 respondents, the majority (44 individuals or 40.4%) use UBA. GT Bank follows closely

with 38 respondents (34.9%), while Access Bank is used by 27 participants, representing 24.8% of the sample. This suggests that the major respondents are from UBA, followed by GT Bank, with Access Bank being the least used. The data may reflect brand preference, accessibility, or customer satisfaction among users of these banks. The analysis of departmental distribution among 109 respondents shows that the majority, 65 individuals (59.6%), are from the Information Technology department, indicating a strong IT presence in the study. Operations follows with 20 respondents (18.3%), while Compliance has 15 respondents (13.8%). Customer Service is the least represented, with only 9 respondents (8.3%). This suggests a strong representation from the IT department, reflecting the nature or focus of the organisation or study.

Data Presentation

Table 3: Cybersecurity Indicator: Measures Implemented

Descriptive Statistics Variables	N	Minimum	Maximum	Mean	Std. Deviation
Nigerian banks have a strong firewalls and network security systems to prevent unauthorized access	109	2	5	4.17	.462
Banks in Nigeria make use of multi-factor authentication (e.g. OTPs, Biometrics) for online transactions.	109	4	5	4.67	.472
My bank regularly updates its cybersecurity software to protect against new threats.	109	3	5	4.09	.632
Employees in Nigerian banks are regularly trained on cybersecurity awareness and fraud prevention	109	3	5	4.40	.511
There are dedicated cybersecurity teams in Nigerian banks responsible for monitoring and responding to threats.	109	2	5	3.71	1.039
Valid N (listwise)	109				

Source: Researcher's Field Survey

The analysis in Table 3 provides insights into the current cybersecurity measures implemented by Nigerian banks to prevent financial fraud based on the respondents' views. The data reveals a generally positive outlook, with high mean scores across most variables, indicating strong cybersecurity practices within the sector. The highest-rated measure is the use of multi-factor authentication (MFA), with a mean score of 4.67 and a relatively low standard deviation of 0.472. This suggests a widespread and consistent implementation of OTPs, biometrics, and similar tools across Nigerian banks, enhancing the security of online transactions. Following this is employee training, with a mean of 4.40, indicating that banks prioritise continuous staff education on cybersecurity awareness and fraud prevention, an essential component in reducing internal vulnerabilities. To safeguard an organisation from any attack, staff training and engagement are significant in constructing awareness among workers and inspiring them to give attention to cyber threats (Bada et al., 2014; Al-Bassam, 2018). Firewalls and network security systems also received a strong rating (mean = 4.17), reflecting strong infrastructure to prevent unauthorised access. Regular software updates (mean = 4.09) further emphasize banks' commitment to staying ahead of evolving cyber threats, although the slightly higher standard deviation (0.632) suggests some variability among institutions in this regard. The analysis demonstrates that Nigerian banks have implemented several effective cybersecurity strategies, particularly in authentication, training, and infrastructure. However, disparities in certain areas, such as dedicated security teams, highlight the need for more uniform adoption of best practices to ensure protection against financial fraud across the banking sector.

Table 4: Financial Performance and Reputation

Descriptive Statistics Variables	N	Minimum	Maximum	Mean	Std. Deviation
Frequent cybersecurity breaches negatively affect customers' trust in Nigerian banks	109	4	5	4.61	.489
Cyber threats negatively influence investor confidence in Nigerian banks.	109	2	5	3.90	1.154
Public disclosure of cyberattacks results in negative media attention and reputation damage.	109	2	5	3.55	.887
Cybersecurity vulnerabilities can result in lawsuits and legal liabilities for banks.	109	3	5	3.98	.272
Reputation damage from cyber breaches takes a long time to rebuild.	109	3	5	4.16	.655
Valid N (listwise)	109				

Source: Researcher's Field Survey

The analysis reveals that cyber threats and vulnerabilities have significant implications for both the financial performance and reputation of Nigerian banks. The data shows that respondents strongly agree that frequent cybersecurity breaches affect customers' trust, with a very high mean score of 4.61 and a low standard deviation of 0.489, indicating a strong agreement. When customers lose trust, they may reduce their interactions with the bank, leading to lower transaction volumes and potential revenue loss. Similarly, the perception that cyber threats negatively affect investor confidence is reflected in a moderately high mean of 3.90, although the higher standard deviation of 1.154 suggests varied opinions. However, reduced investor confidence can lead to declining investments, affecting a bank's market value and ability to raise capital. The public disclosure of cyberattacks, averaging 3.55, highlights how media coverage

can amplify reputational damage. Media attention from cyber incidents can affect public trust, harm brand image, and cause customers and investors to question the bank's reliability. Furthermore, cybersecurity vulnerabilities leading to lawsuits and legal liabilities (mean = 3.98) highlight the financial implications. Legal battles and regulatory fines damage organisational credibility. The relatively low standard deviation (0.272) indicates a strong agreement on this risk. The belief that reputation damage takes a long time to repair (mean = 4.16) highlights the lasting consequences. A tarnished reputation can affect new customers and partners, impacting long-term profitability. Strengthening cybersecurity frameworks is essential for safeguarding trust, ensuring regulatory compliance, and maintaining competitive performance.

Table 5: Cybersecurity Implementation: Challenges and Limitations

Descriptive Statistics Variables	N	Minimum	Maximum	Mean	Std. Deviation
High implementation costs are a major barrier to adopting advanced cybersecurity solutions.	109	1	5	3.47	1.561
There is a shortage of skilled cybersecurity professionals within the Nigerian banking sector.	109	2	5	3.20	.900
A lack of real time monitoring tools limits the effectiveness of incident response.	109	2	5	3.66	1.278
Employees' negligence contributes significantly to cybersecurity breaches.	109	2	5	3.71	.737
Cybersecurity awareness among customers is low, increasing overall risk.	109	2	5	4.52	1.042
Valid N (listwise)	109				

Source: Researcher's Field Survey

The descriptive statistics presented reveal several significant challenges and limitations faced by Nigerian banks in implementing effective cybersecurity strategies. These challenges stem from financial, technical, human, and operational constraints, as reflected in the responses of 109 participants. One of the most critical barriers is the low level of cybersecurity awareness among customers, which has the highest mean score of 4.52. This suggests that respondents agree that customer ignorance increases cybersecurity risks, making them vulnerable to phishing, social engineering, and other cyber threats. Closely related is the role of employees' negligence, with a mean of 3.71, indicating that internal human error remains a considerable risk factor in bank cybersecurity breaches. This emphasizes the urgent need for continuous staff training and stronger internal policies to mitigate insider threats. Another major concern is the lack of real-time monitoring tools (mean = 3.66), which limits the effectiveness of incident response. Without timely detection systems, banks struggle to respond swiftly to cyberattacks, allowing more damage to occur. In addition, the high cost of implementing advanced cybersecurity solutions (mean of 3.47) is a substantial financial challenge. This implies that while banks recognize the need for strong systems, budgetary constraints delay or prevent adoption. Furthermore, the shortage of skilled cybersecurity professionals (mean = 3.20) reflects a talent gap in the sector. With cyber threats becoming increasingly complex, the lack of expertise affects the effectiveness of cybersecurity frameworks in banks. Nigerian banks face multifaceted challenges in implementing effective cybersecurity strategies. These include limited customer awareness, inadequate real-time tools, financial constraints, and a shortage of skilled personnel. Addressing these issues involves investment in training, technology, and public education to strengthen the overall cybersecurity posture of the banking sector.

Table 6: Correlation Analysis

Correlations Variables		Cybersecurity	Financial Integrity	Financial Fraud
Cybersecurity	Pearson Correlation	1	.684**	.750**
	Sig. (2-tailed)		.000	.000
	N	109	109	109
Financial integrity	Pearson Correlation	.684**	1	.610**
	Sig. (2-tailed)	.000		.000
	N	109	109	109

** Correlation is significant at the 0.01 level (2-tailed).

The Pearson correlation coefficient between cybersecurity and financial integrity is 0.684, which is both positive and statistically significant at the 0.01 level. This suggests a strong association: as cybersecurity measures improve, financial integrity within the banking system also increases. This implies that well-implemented cybersecurity frameworks contribute significantly to upholding transparency, accountability, and trustworthiness in financial institutions.

NVivo Analysis

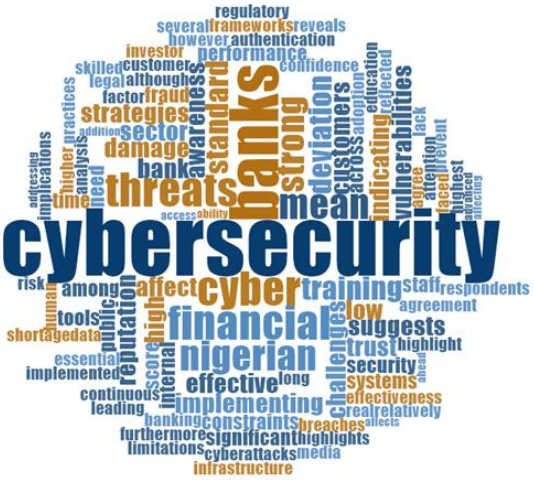

Figure 2: Visual Representation of the Responses

The NVivo word cloud diagram visually represents the dominant themes derived from the study's data. At the center of the cloud is the most prominent term, "cybersecurity," which highlights its essential role in protecting financial institutions from evolving threats. Other significant terms, such as "banks," "threats," "training," and "financial," reveal key areas of concern. "Banks" appear both as subjects and objects in discussions about cybersecurity. The word "threats" emphasises the continuous risks of fraud and data breaches, while "training" emphasises the need to build staff capacity to detect, prevent, and respond to cyber incidents. Additionally, terms like "trust," "reputation," and "public" illustrate that cybersecurity extends beyond technical aspects; it also profoundly impacts public perception and institutional credibility. Once financial institutions face a breach, regaining customer trust can be both costly and time-consuming. The inclusion of words such as "standard," "regulatory," "implementation," and "strategies" shows the need for consistent policies, frameworks, and actionable plans to mitigate cyber risks and enhance system integrity. Challenges represented by terms like "constraints," "limitations," and "infrastructure" highlight the obstacles banks encounter in establishing strong cybersecurity systems, which range from financial constraints to outdated infrastructure and skill shortages. The diagram shows that ensuring financial integrity in Nigeria's banking sector requires a multifaceted approach, involving regulation, technology, customer awareness, and continuous investment in both human and digital resources to effectively combat financial fraud.

Discussion

The findings from the analysis reveal that Nigerian banks have made commendable progress in implementing cybersecurity measures to safeguard against financial fraud. A key strength identified is the widespread use of multi-factor authentication. This includes the deployment of tools like one-time passwords (OTPs), biometric verification, and other layered security systems to protect customer transactions and data. These practices greatly enhance security by making unauthorized access more difficult, especially for online and mobile banking platforms. (Johnson, 2021) Findings suggest that the adoption of MFA goes beyond meeting regulatory requirements; it is a strategic imperative for fortifying the security framework of Nigerian banks. The study highlights the specific role of multi-factor authentication in mitigating risks associated with identity theft. Another significant area of strength is employee training on cybersecurity practices. The results suggest that banks invest in continuous awareness and capacity-building programs for their staff. This approach is crucial, as it empowers employees to identify potential cyber threats, follow best practices, and avoid negligent behaviors that could expose the system to attacks. Well-trained staff are better equipped to follow established protocols, respond to incidents quickly, and contribute to building a culture of security within the institution. Employees who are unaware of their cybersecurity obligations are more likely to disregard applicable policies and procedures, leading to unintended data exposure or successful cyber-attacks (Badejo,2018).

The study also indicates that Nigerian banks maintain strong technical infrastructure, such as firewalls and network security systems. These tools play a vital role in detecting and blocking unauthorized access attempts and defending against external threats. Similarly, regular updates of software systems are practiced to address known vulnerabilities and adapt to evolving threats, although there may be some inconsistencies in how uniformly this is done across the sector. Despite these efforts, several challenges persist. One major concern is the lack of awareness among bank customers regarding cybersecurity. This makes them easy targets for fraud schemes such as phishing and social engineering. When customers unknowingly compromise on their own security, it creates weaknesses that banks must then manage. Additionally, internal factors such as employee negligence continue to pose a significant risk. Mistakes like clicking on malicious links or failing to follow protocols can lead to severe breaches. There is also a pressing need for real-time monitoring systems to detect and respond to threats promptly. Without such tools, incidents may go unnoticed until considerable damage has been done. Financial limitations are another obstacle. Implementing and maintaining advanced cybersecurity systems requires significant investment, which may not be feasible for all banks. Furthermore, the shortage of qualified cybersecurity professionals in the country limits the capacity of banks to build and manage sophisticated security frameworks. This is supported by Fatoki, 2023 findings, which showed that the challenges impeding the effort to stop cyber fraud in Nigeria's banking system included a lack of standards and national central control, a lack of infrastructure, the internet's vulnerability, a lack of national

functional databases, and inadequate awareness by bank customers.

CONCLUSION

This study concluded that cybersecurity plays a crucial role in protecting Nigeria's banking sector against the ever-evolving threat of financial fraud. As financial services continue to digitise, the risks associated with cybercrime ranging from phishing and identity theft to ransomware and insider fraud have intensified, posing significant challenges to banks, customers, and the broader economy. Through the analysis of primary data collected from staff across three major Nigerian banks (GTBank, UBA, and Access Bank), it is evident that banks are making commendable efforts to adopt modern cybersecurity measures, including multi-factor authentication, real-time system updates, employee training, and network firewalls. However, the study also revealed several critical vulnerabilities that still persist. Among the most pressing are low cybersecurity awareness among customers, employee negligence, inadequate real-time monitoring tools, high implementation costs, and a shortage of skilled cybersecurity professionals. These gaps have continued to undermine the effectiveness of existing strategies and expose banks to reputational damage, financial losses, and regulatory sanctions.

RECOMMENDATIONS

To strengthen cybersecurity in Nigeria's banking sector, banks must launch nationwide awareness campaigns in partnership with CBN, NDIC, and telecoms, using media and mobile apps to teach safe practices like avoiding phishing, fake apps, and OTP sharing. Investments in modern threat detection tools (SIEM, XDR) will ensure real-time monitoring and automated responses. Internally, banks should enforce strong policies, role-based access, and staff training to reduce insider risks. Addressing talent gaps through certifications, bootcamps, and academies is vital. Finally, banks must collaborate with regulators to update policies, conduct vulnerability assessments, share intelligence, and enforce compliance for stronger sector-wide resilience.

ACKNOWLEDGEMENT

Special appreciation goes to professionals within Nigeria's banking sector who shared their perspectives and experiences, which greatly enriched the quality of the research. The constructive feedback from colleagues and peers also contributed to strengthening the clarity and relevance of this work.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are openly available in [repository name e.g "figshare"] at http://doi.org/[doi].

AUTHOR CONTRIBUTION STATEMENT

Folasade M. Okikiola conceptualized the study, designed the research framework, and initiated the project. Taiwo S. Arogundade carried out the data collection, performed the analysis, and interpreted the findings. Olasunkanmi E. Oladiboye, critically reviewed the manuscript, contributed to intellectual refinement, and validated the overall results. All authors contributed to the writing, read, and approved the final manuscript.

REFERENCES

Abdulkareem, S. (2025). The role of cybersecurity awareness in safeguarding digital systems in institution of higher learning. Kontagora journal of intellectual discourse, 3(1), 280-292

Abrahams, T.O., Ewuga, S.K., Dawodu, S.O., Adegbite, A.O., & Hassan, A.O. (2024). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, 5(1), 1-25

Ahmed, A. A., Al-Khater, W. A., Al-Maadeed, S., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive Review of Cybercrime Detection Techniques

Akintoye, R., Ogunode, O., Ajayi, M. and Joshua, A.A. (2022). Cyber security and financial innovation of selected deposit money banks in Nigeria. Universal Journal of Accounting and Finance, 10(3), 643-652

Antonucci, D. (2017). The cyber risk handbook: Creating and measuring effective cybersecurity capabilities: John Wiley & Sons

Badejo, B., Okuneye, B., & Taiwo, M. (2018). Fraud detection in the banking system in Nigeria: Challenges and prospects. Shirkah: Journal of Economics and Business, 2(3)

Becher, T., & Torka, S. (2024). Exploring AI-Enabled Cybersecurity Frameworks: Deep-Learning Techniques, GPU Support, and Future Enhancements. arXiv preprint arXiv:2412.12648

Bromwich, J. E., (2016). "Protecting your digital life in 7 easysteps". New York Times, p. B4

Buchanan, B. (2016). The cybersecurity dilemma: Hacking, trust, and fear between nations: Oxford University Press

Fatoki, J. O. (2023). The influence of cyber security on financial fraud in the Nigerian banking industry. International Journal of Science and Research Archive, 9(2), 503-515

Garba, A.A., Siraj, M.M., and Othman, S.H., 2022. An assessment of cybersecurity awareness level among northeastern university students in nigeria. International Journal of Electrical and Computer Engineering (IJECE), 12 (1), Pp. 572
. https://doi.org/10.11591/ijece.v12i1.pp572-584

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

Kolade, E. (2022). Cybersecurity in Nigeria's Financial Industry: Enhancing Consumer Trust and Security

Naira metrics, 2024. https://nairametrics.com/2024/09/14/breaking-nigerian-banks-lose-n42-6-billion-to-fraud-in-q2-2024-surpassing-full-year-2023-record/

National Cybersecurity Policy and Strategy, Nigerian Government, (2021). https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf

National Digital Economy Policy and Strategy (2020) Nigerian Federal Ministry of Communications and Digital Economy, https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/883-national-digital-economy-policy-and-strategy/file.

Nte, N. D., Enoke, B. K., & Omolara, J. A. (2022). An evaluation of the challenges of mainstreaming cybersecurity laws and privacy protection in Nigeria. Journal of Law and Legal Reform, 3(2), 243-266

Nugraha, R., & Bayunitri, B. I. (2020). The influence of internal control on fraud prevention (Case study at Bank BRI of Cimahi City). International journal of Financial, Accounting, and Management, 2(3), 199-211

Obi, O. C., Akagha, O. V., Dawodu, S. O., Anyanwu, A. C., Onwusinkwue, S., & Ahmad, I. A. I. (2024). Comprehensive review on cybersecurity: modern threats and advanced defense strategies. Computer Science & IT Research Journal, 5(2), 293-310

Ogunyemi, A. A. (2024). Cyber Risks and the Nigerian Business Sector: A Critical Analysis of the Emerging Cyber Insurance Market in Nigeria. ACU Journal of Social Sciences, 3(1)

Okoroiwu, K. L., Okoyeuzu, C. R., & Ukpere, W. I. (2024). Financial Institutions Cyber Security Incidents and Economic Growth of Nigeria

Olaniyan, N. O., Ekundayo, A. T., Oluwadare, O. E., & Omolade Bamisaye, T. (2021). Forensic accounting as an instrument for fraud detection and prevention in the public sector: moderating on ministries, departments and agencies in Nigeria. Acta Scientiarum Polonorum. Oeconomia, 20(1), 49-59

Rjoub, G., Bentahar, J., Wahab, O. A., Mizouni, R., Song, A., Cohen, R., ... & Mourad, A. (2023). A survey on explainable artificial intelligence for cybersecurity. IEEE Transactions on Network and Service Management, 20(4), 5115-5140

Zheng, Y., Pal, A., Abuadbba, S., Pokhrel, S. R., Nepal, S., & Janicke, H. (2020). Towards IoT Security Automation and Orchestration. Paper presented at the 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)