

Determinants of Artificial Intelligence Adoption for Cybersecurity in Nigeria's Banking Sector: Evidence from Survey and Thematic Analysis

Dr. Roberts Ndukwe Eke 

Independent Researcher, Port Harcourt, Rivers State, Nigeria.

Corresponding author: robeken@yahoo.co.uk

DOI: <https://doi.org/10.62154/ajmbr.2025.021.01022>

Abstract

The Nigerian banking sector is increasingly exposed to cyber threats due to rapid digital transformation and expanding online financial services. This study investigates the determinants driving the adoption of Artificial Intelligence (AI)-enabled cybersecurity solutions in Nigerian deposit money banks and evaluates perceived readiness for implementation. A structured questionnaire was administered to information technology and cybersecurity-related personnel across selected Nigerian banks, producing 97 valid responses. Quantitative data were analysed using descriptive statistics, while open-ended responses were analysed using thematic analysis to identify dominant threat channels and perceptions. Findings indicate that a substantial proportion of respondents reported the deployment of AI for cybersecurity in their institutions, and many agreed that AI can improve banking security and service availability. However, evidence also suggests limited workforce readiness, constraints in access to appropriate AI tools, and infrastructural challenges that hinder broader adoption. The thematic analysis revealed that social media platforms, particularly Facebook and Instagram, were frequently associated with cyber threat exposure, suggesting the need for stronger customer-facing security awareness and fraud prevention measures. The study concludes that while AI adoption is emerging within Nigerian banks, scaling its cybersecurity benefits requires investment in digital infrastructure, targeted capacity development, and stronger governance frameworks for AI deployment. It is recommended that bank management prioritise cybersecurity funding, workforce upskilling, and cross-sector collaboration to improve AI implementation outcomes.

Keywords: AI-Driven Cybersecurity, Cybersecurity Challenges, Digital Transformation in Banking, Banking Sector, Nigeria.

Introduction

The Nigerian banking sector has experienced accelerated digital transformation driven by the adoption of mobile banking, internet banking, agent banking, and fintech integration. While these innovations improve service delivery and financial inclusion, they also expand the cyber-attack surface and intensify exposure to threats such as phishing, credential theft, malware infections, ransomware, and distributed denial-of-service attacks. Cybersecurity risks in banking are particularly critical because breaches can result in financial loss, operational disruption, regulatory sanctions, and reputational damage. Recent studies have emphasised that cyber threats in Nigeria's banking environment are

shaped by internal control weaknesses, insider risks, low customer security awareness, and evolving attacker sophistication (Ama et al., 2024; Ojeka et al., 2017; Reis et al., 2024).

Artificial intelligence (AI), including machine learning and predictive analytics, is increasingly applied in cybersecurity to enhance anomaly detection, automate threat triage, and improve incident response. In banking contexts, AI can support fraud detection, behavioural analytics, and real-time monitoring of transaction anomalies. However, organisational adoption depends on technology readiness, organisational capacity, and environmental/regulatory pressures, as explained by established technology adoption frameworks such as the Technology Acceptance Model (TAM) and the Technology–Organisation–Environment (TOE) framework (Bryan & Zuva, 2021; Qin et al., 2020). AI adoption in cybersecurity is often examined through technology adoption frameworks. TAM explains adoption using perceived usefulness and perceived ease of use as predictors of behavioural intention and actual system usage (Bryan & Zuva, 2021). TOE expands this by integrating organisational and environmental drivers such as infrastructure readiness, top management support, competitive pressure, and regulatory influence (Qin et al., 2020). In banking, these factors influence AI adoption decisions because cybersecurity investments require technical capability, governance maturity, and risk management alignment (Kedarya & Elalouf, 2023).

Empirical evidence indicates that financial institutions increasingly deploy AI for threat detection, fraud monitoring, and automated response, but implementation barriers persist, including skills shortages, data quality limitations, high costs, and ethical concerns around privacy and bias (Uzoka et al., 2024). In Nigeria, banking cybersecurity challenges have been linked to insider threats, weak controls, and limited customer security awareness (Ama et al., 2024; Ojeka et al., 2017). These conditions make AI adoption both necessary and complex, especially when institutions face constraints in funding, infrastructure, and specialist workforce capacity.

Despite the growing relevance of AI-driven cybersecurity, empirical evidence on adoption drivers and readiness constraints in Nigeria's banking sector remains limited. Existing research tends to focus on general cybersecurity challenges or digital banking risks, with fewer studies assessing the practical determinants of AI-based cybersecurity adoption from the perspective of bank cybersecurity stakeholders. Therefore, this study investigates the drivers and constraints influencing AI-powered cybersecurity adoption in Nigerian banks and provides recommendations for strengthening AI implementation through improved infrastructure, capacity development, and institutional support.

Literature Review

Significant advantages have resulted from Nigeria's financial services' quick digitisation, including increased operational effectiveness and consumer satisfaction (Lottu et al., 2023). At the same time, it has made banks more vulnerable to ransomware attacks, DDoS attacks, phishing scams, and insider threats (Reis et al., 2024). The introduction of

computers reduced many banking-related problems, but it also introduced new ways for consumers to become victim to different types of cyberattacks (Oyewole et al., 2024).

In Abiodun (2023), it is highlighted that the sharp increase in cybercrimes in recent years is one of the largest problems facing financial institutions in the twenty-first century. In fact, Nigeria has suffered from the reputation of being a haven of cyber-enabled fraudulent activities (Ebenezer et al., 2016; Ojedokun & Eraye, 2012). These include the notorious 419 scam that spread around the world from the 1980s onwards as in Arewa (2018), and more recently 'online advanced fee fraud' (Osho & Onoja, 2015). Although there has been the introduction of Nigeria's Cybercrimes Law, Tambawal (2024) notes it has not addressed bank clients' susceptibility to cybercrimes. Additionally in 2021, the Nigerian National Cybersecurity Policy and Strategy (NCPS) was unveiled to tackle the cybersecurity threat in the banking, finance, and insurance sectors. The aim of the above policy is to strengthen the cybersecurity framework. Yet, Nigerian cybercrime is itself in constant transformation, with more sophisticated and organized attacks been launched (Hinchliffe, 2017) Gulyas and Kiss (2022) states that 2021 was again another "worst year ever" for financial industry cyberattacks, underscoring the dramatic increase in these attacks. They emphasised that these attacks have a disproportionately negative effect on the industry, as evidenced by the dramatic increase in virus infections and blackmail. Given the likelihood of increasingly sophisticated attacks on the financial sector in the future, the authors contend that cybersecurity ought to be a primary priority. It highlights how important it is to become informed on the latest threat trends, tools, and tactics in order to maximise protection against malicious attacks.

The dangers of internet banking were accentuated by Arora et al. (2022), they also stressed the necessity of strong cybersecurity measures. The study highlights the cybersecurity issues of different nations while reviewing different risk kinds and user authentication and security techniques. It implies that different nations need varying degrees of security goals and that banks must have strong cybersecurity systems. Kedarya and Elalouf (2023) examined cybersecurity risks as well as developments in the worldwide banking industry. Their report highlights changes in company strategies and the need for new business models to address these issues. It is based on interviews with officials of significant national banks in Israel. The findings highlight the value of an integrated strategy to risk management, which can benefit banks all over the world.

Furthermore, Reis et al. (2024) gave insights into technology changes and trends in e-banking, which are relevant for understanding potential cybersecurity threats.

AI-Driven Cybersecurity Adoption: Theoretical and Empirical Foundations

AI adoption in cybersecurity is often examined through technology adoption frameworks. TAM explains adoption using perceived usefulness and perceived ease of use as predictors of behavioural intention and actual system usage (Bryan & Zuva, 2021). TOE expands this by integrating organisational and environmental drivers such as infrastructure readiness,

top management support, competitive pressure, and regulatory influence (Qin et al., 2020). In banking, these factors influence AI adoption decisions because cybersecurity investments require technical capability, governance maturity, and risk management alignment (Kedarya & Elalouf, 2023).

Empirical evidence indicates that financial institutions increasingly deploy AI for threat detection, fraud monitoring, and automated response, but implementation barriers persist, including skills shortages, data quality limitations, high costs, and ethical concerns around privacy and bias (Uzoka et al., 2024). In Nigeria, banking cybersecurity challenges have been linked to insider threats, weak controls, and limited customer security awareness (Ama et al., 2024; Ojeka et al., 2017). These conditions make AI adoption both necessary and complex, especially when institutions face constraints in funding, infrastructure, and specialist workforce capacity.

Research Design and Methodology

Research Design

The research design for evaluating the factors driving adaptation of AI-driven cybersecurity in Nigerian banking sector employed mixed-methods approach, combining both qualitative and quantitative methods (Dawadi et al., 2021). The research design was based on a descriptive and exploratory study, which aims to describe the current state of AI-driven cybersecurity adoption in Nigerian banks and explore the factors influencing its adaptation.

Methodology

Data Collection

The study employed a survey research design, where a web-based questionnaire was administered to IT professionals and cybersecurity experts in Nigerian banks. The survey focused on quantifiable metrics like perceived ease of use of AI solutions which is intended to provide deeper insights into challenges and strategies for implementation. The population of the bank is comprised of all the thirty-three (33) deposit money banks in Nigeria (Ama et al., 2024). The researcher adopted a purposive sampling technique to select the prominent in in Nigeria. These banks include First Bank of Nigeria, Zenith Bank Nig. Plc, Fidelity Bank Nigeria Plc, Access Bank Nig. Plc and Guarantee Trust Bank. These banks broadly reflect Tier 1 commercial banks based on scale, market footprint, and systemic importance within Nigeria's banking ecosystem.

Instrumentation

A structured questionnaire was developed based on validated scales from prior studies on technology adoption like the TAM-TOE models. The TAM is a commonly used model for understanding the IT adoption and usage process (Bryan & Zuva, 2021). Its popularity stems from the model's ability to clarify variables such as behavioral intent (BI) relevant to IT acquisition and use across a wide range of situations. The model's primary factors for system utilization are perceived utility (PU) and perceived ease of use (PEOU). Similarly, the

T-O-E framework is a prominent concept for three factors influencing organisational adoption: technology, organisation, and environment (Qin et al., 2020). This model has been used by Gholami et al. (2018), Qin et al. (2020) and (Bryan & Zuva, 2021). The questionnaire includes Likert-scale items to measure perceptions about the current state of AI-driven cybersecurity adoption in Nigerian banks, factors influencing the adaptation of AI-driven cybersecurity and challenges faced in implementing AI-driven cybersecurity. To achieve the aim of this study, primary data was primarily from the questionnaires that were given out. The researcher implemented self-administered questionnaire via E-mail. A five-point Likert-scale such as "Strongly Agree", "Agree", "Undecided", "Disagree", "Strongly Disagree" was used for the questionnaire design. Since, the present research paper is focused on banking sector it reflects a purposive study.

Sampling Technique

A stratified random sampling method will be used to ensure representation across different categories of banks (commercial banks). This ensures that insights are gathered from diverse perspectives within Nigeria's banking ecosystem. The questionnaire was designed to collect both qualitative and quantitative data, including closed-ended and open-ended questions. Therefore, the questionnaire was administered to bank staff via e-mails especially the members of information technology (IT) team because they will be more knowledgeable about cyber-attacks. The questionnaire was divided into sections, including:

- i. Demographic information of respondents
- ii. Current state of AI-driven cybersecurity adoption in Nigerian banks
- iii. Factors influencing the adaptation of AI-driven cybersecurity
- iv. Challenges faced in implementing AI-driven cybersecurity
- v. Benefits of AI-driven cybersecurity adoption

Population Definition, Sample Selection

The target population includes all licensed banks operating in Nigeria under the regulation of the Central Bank of Nigeria (CBN). This includes commercial banks offering banking services. These banks are categorized based on their scope of authorization, including international, national, regional licenses, non-interest banking, merchant banking, and financial holding companies. The study will target a sample size of 100 IT professionals and cybersecurity experts from 20 Nigerian banks. The sample was selected using random sampling technique.

Sample Size Determination

Determining an adequate sample size is essential to ensure statistical validity while maintaining feasibility within resource constraints. The sample size formula for quantitative surveys using Cochran's formula for sample size calculation:

$$n_0 = \frac{Z^2 \cdot p \cdot (1 - p)}{e^2} \quad (1)$$

where:

Z : Z-score corresponding to confidence level (1.96 for 95% confidence).

p : Estimated proportion of success (assume 50%).

e : Margin of error (5% or 0.05).

Substituting values:

$$n_0 = \frac{(1.96)^2 \cdot 0.5 \cdot (1 - 0.5)}{(0.05)^2} = 384 \quad (2)$$

Adjusting for Finite Population Size: Since there are approximately 40 licensed banks in Nigeria as per CBN data:

Adjusted Sample Size (n_f):

$$n_f = \frac{n_0}{1 + \left(\frac{n_0 - 1}{N}\right)} \quad (3)$$

where $N = 33 \div$ (total population):

substituting values:

$$n_f = \frac{384}{1 + \left(\frac{384 - 1}{40}\right)} = 34 \quad (4)$$

Reliability of Instrument

Table I contains the result of the reliability test conducted.

Table I: Cronbach Alpha reliability test result.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	Number of Items
0.712	0.221	20

The Table I above addresses the qualities of measurement scales and the things that comprise them. Ideally, an alpha number less than 0.6 is deemed unacceptable, however an alpha value more than 0.6 indicates that the result (questionnaire) is acceptable. The Cronbach coefficient for the study performs admirably, with a value of 0.712 indicating that the scales and items of the research instrument have a high degree of internal consistency.

Data Analysis

Quantitative responses from the Likert-scale items were analysed using descriptive statistics (frequencies and percentages) to summarise perceptions of AI cybersecurity adoption and readiness. Qualitative responses from open-ended questions were analysed using thematic analysis to identify recurring cyber threat sources and contextual drivers. NVivo 11 was used strictly for organising and coding qualitative responses and generating

word frequency and cluster outputs, consistent with qualitative research practice (Braun & Clarke, 2012; Zamawe, 2015).

Results and Discussion

Results

Demographic Data Analysis

Demographic data analysis involves the systematic examination of data related to the characteristics of populations. This analysis is crucial for understanding trends, making informed decisions in policy-making, marketing, and social services, and addressing various societal issues. Figure 1 presents the percentage of gender respondents. It was observed that about 59.79% of respondents are male while 40.21% are female. Figure 2 indicates the respondents age range and Figure 3 shows the respondents location.

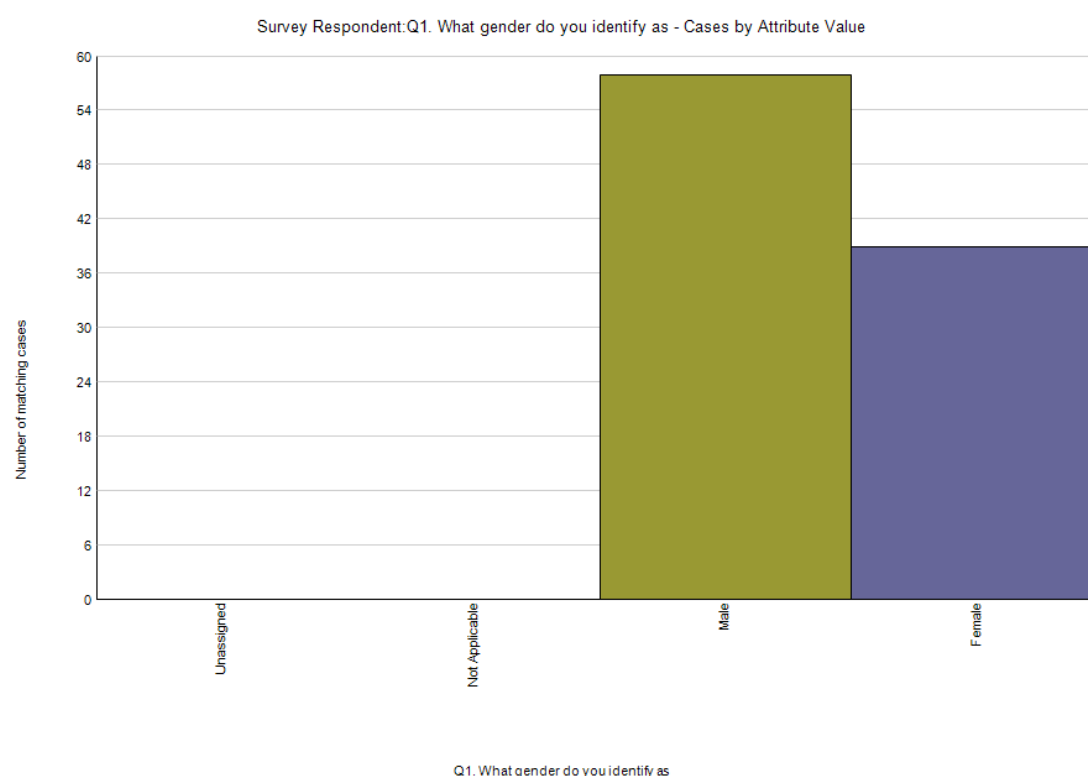


Figure 1: Percentage Gender respondents

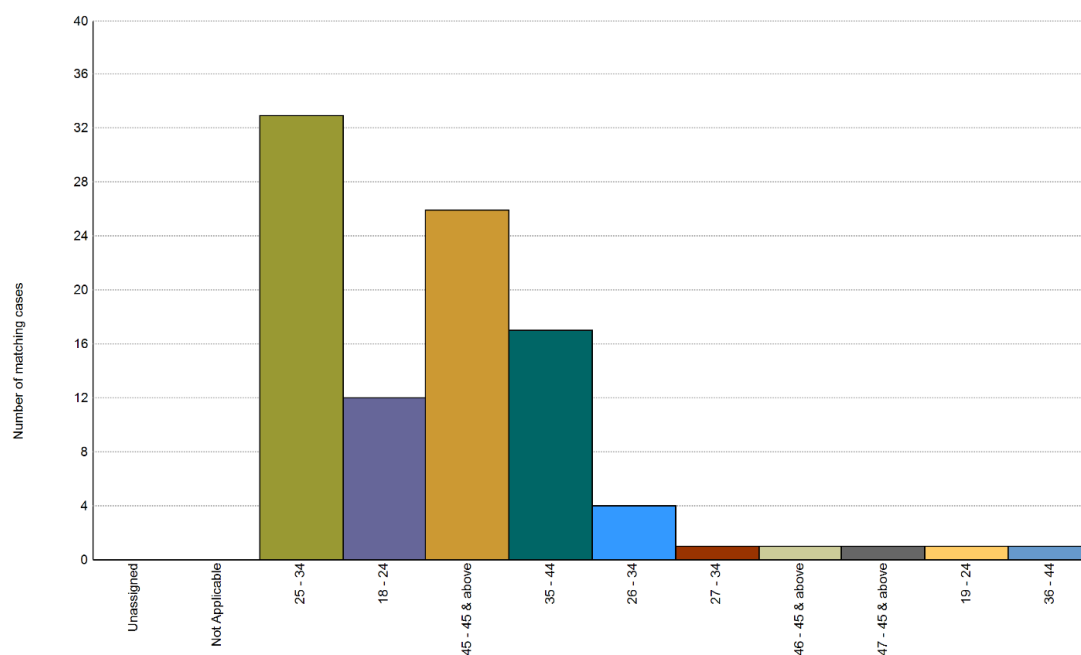


Figure 2: Respondents age range

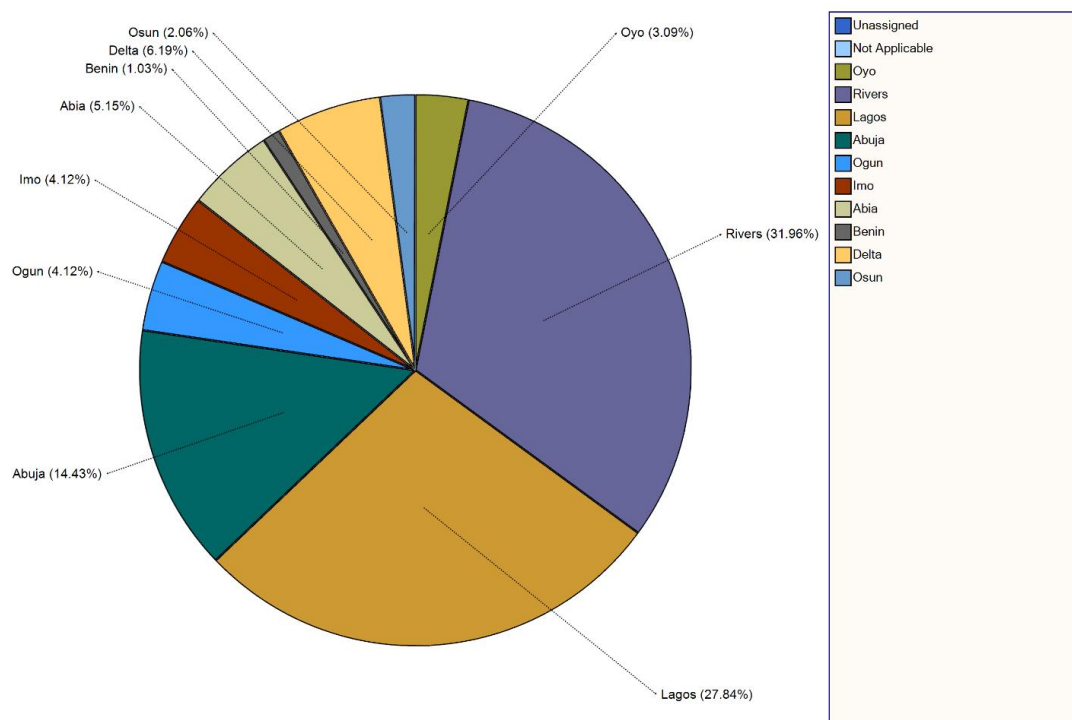


Figure 3: Interviewee residence location

Q5. Has your bank been attacked cyber-wise in the last 3 years and for how long was the outage?

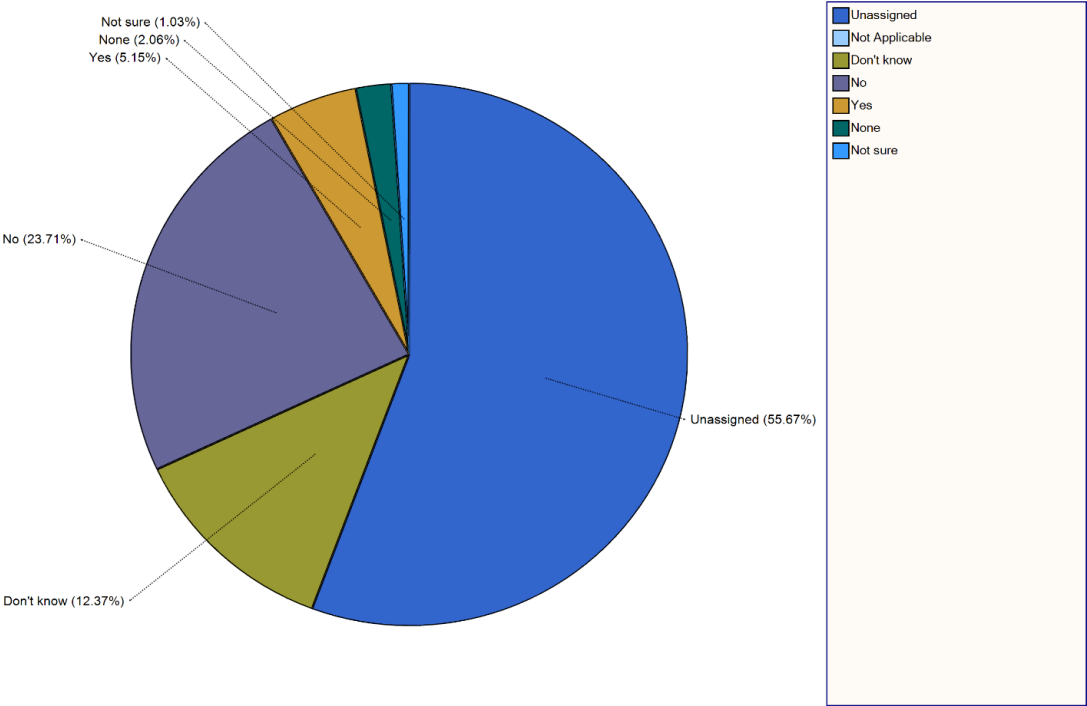


Figure 4: Response on cyber-attack in Nigerian banks (Source: Field Survey 2025)

To investigate factors driving slow adaptation of AI-driven cybersecurity in the banking sector.

Q6. Is AI deployed in your bank for cybersecurity?

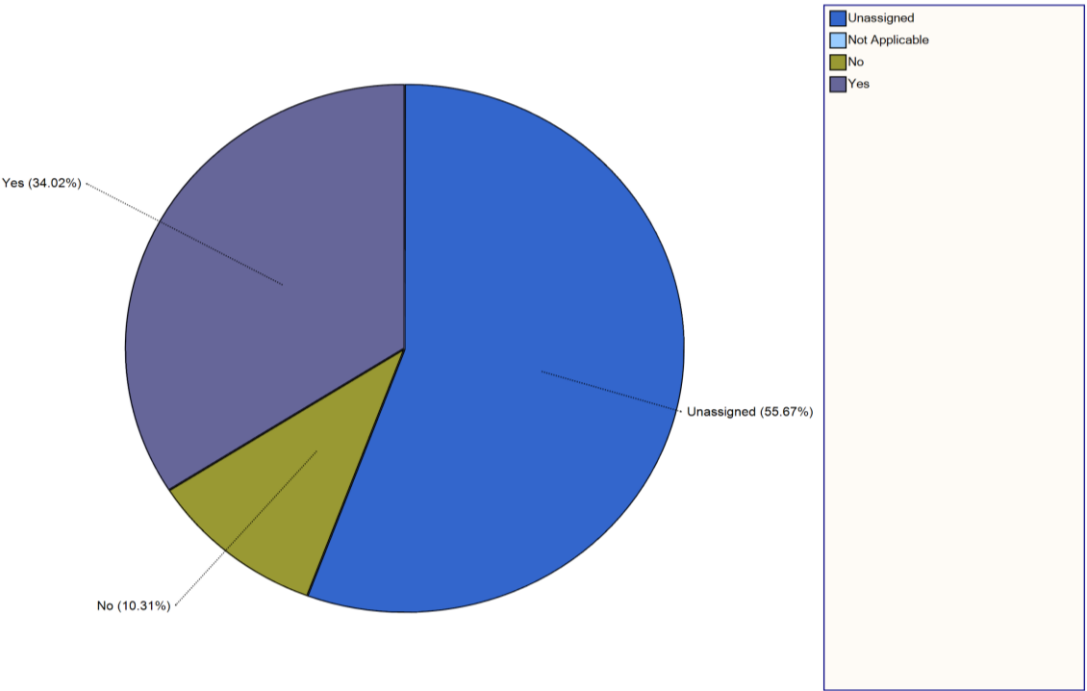


Figure 5: Nigerian banks AI deployment

Q.7. Do you believe that AI-driven cybersecurity can improve the security of the Nigerian Banking sector?

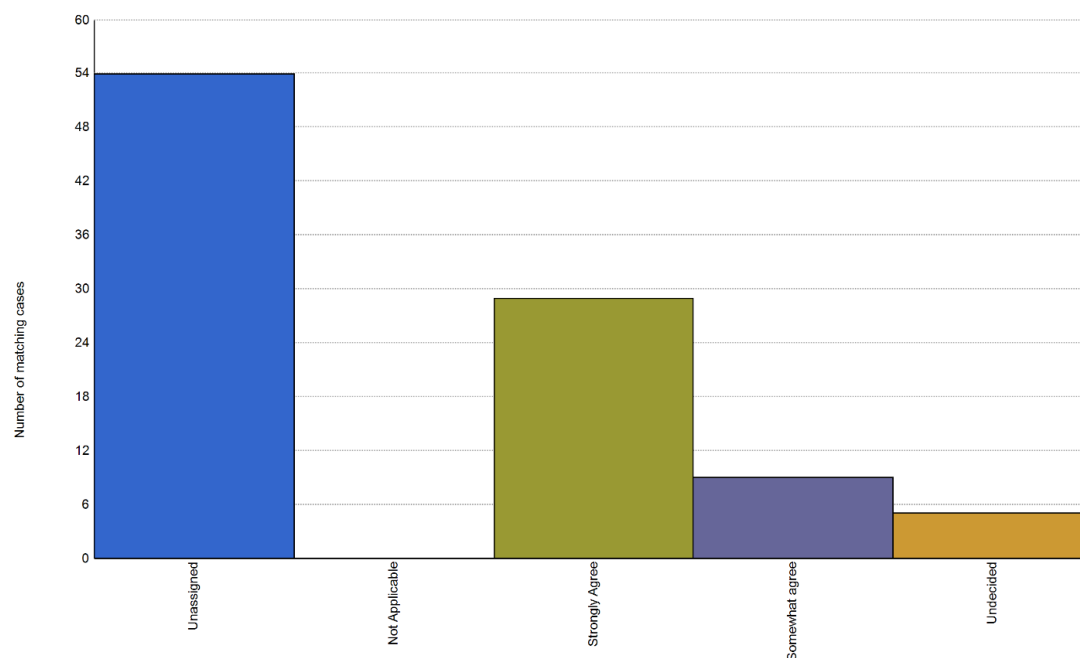


Figure 6: Response on improvement of cyber security in Nigeria banks using AI

Q.8. Does AI-driven cyber system affect service availability positively for the Nigerian Banking sector?

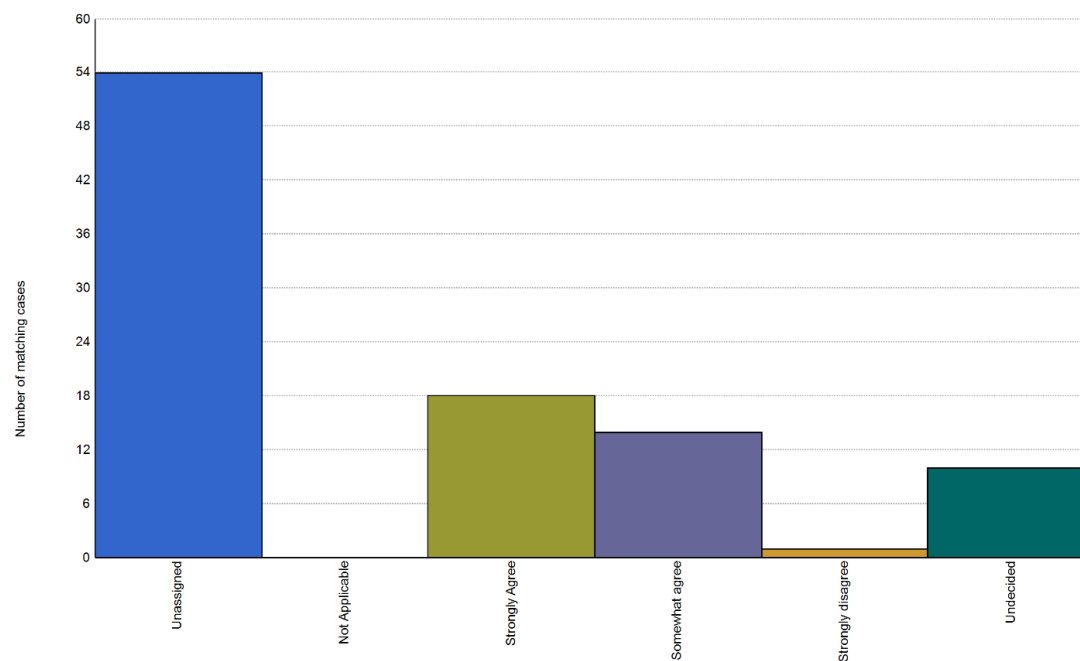


Figure 7: Effect of AI-driven cyber system on Nigerian Banking sector service availability

Q.9. Do you have any experience working with AI?

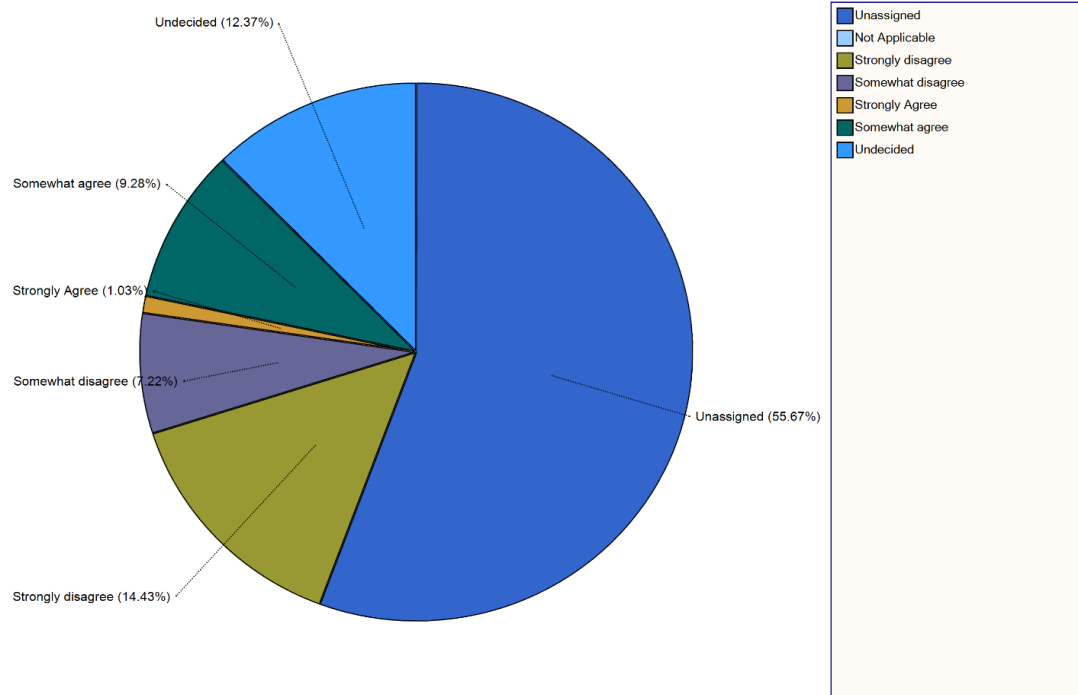


Figure 8: Experience working with AI

Q.10. Do you have the required skills to implement AI?

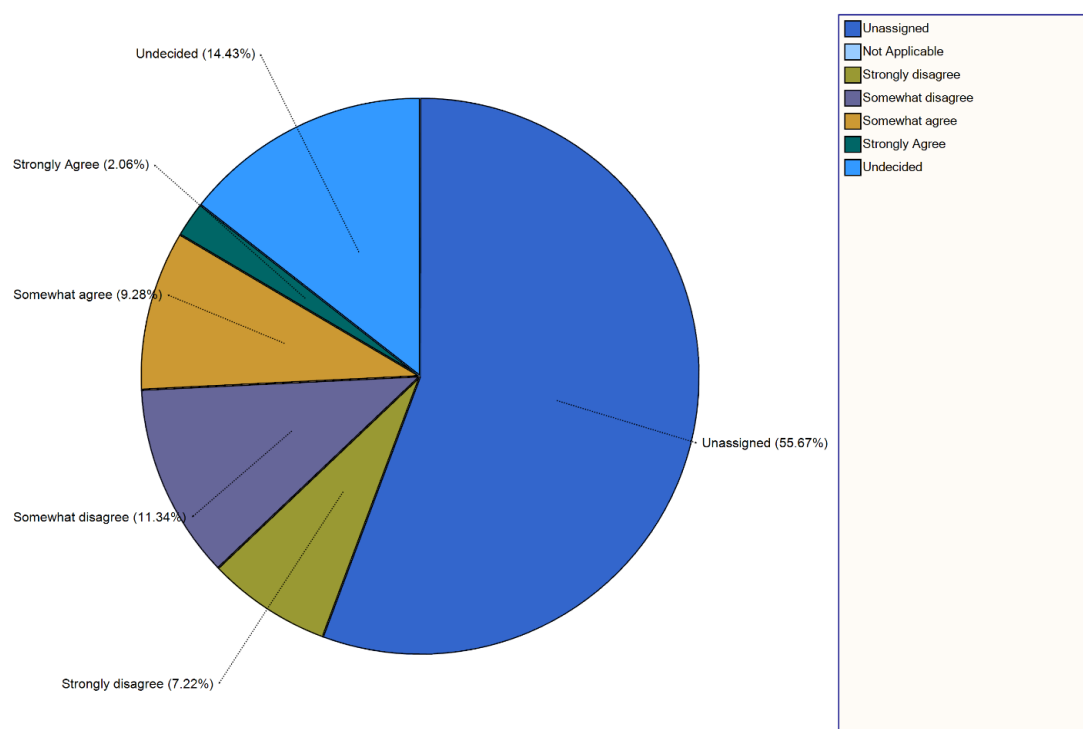


Figure 9: Having required skills to implement AI

Q.11. Do you have the right tools to implement AI?

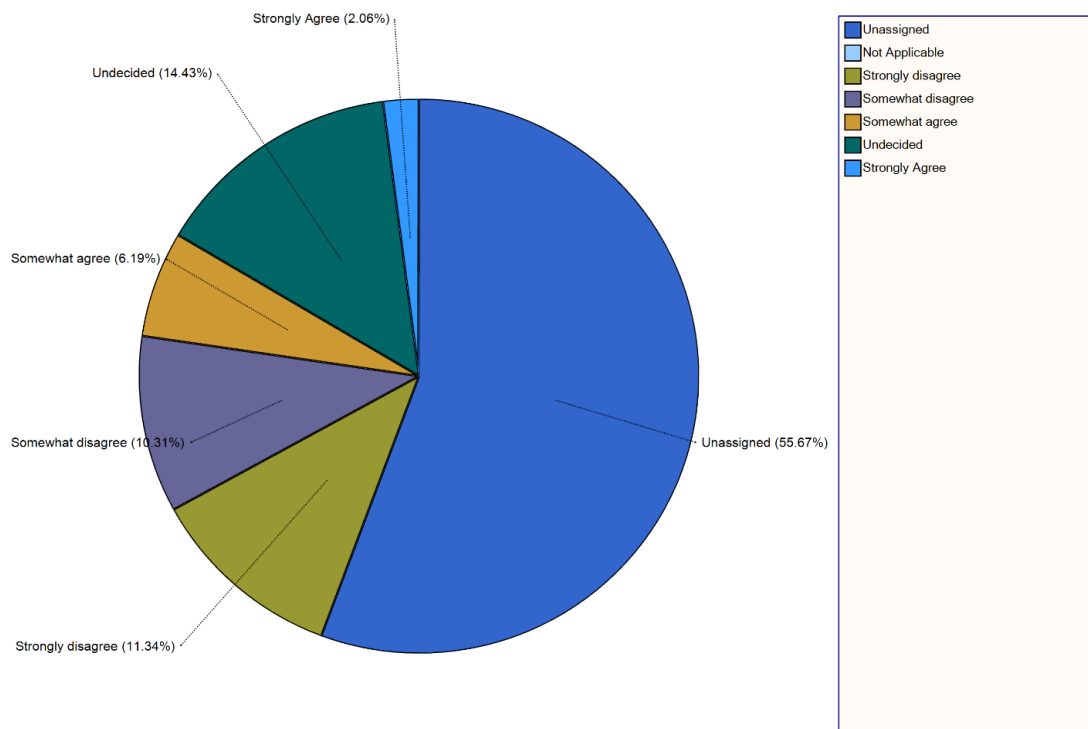


Figure 10: Having right tools for AI implementation

Q.12. Is there lack of adequate funding by management for AI deployment?

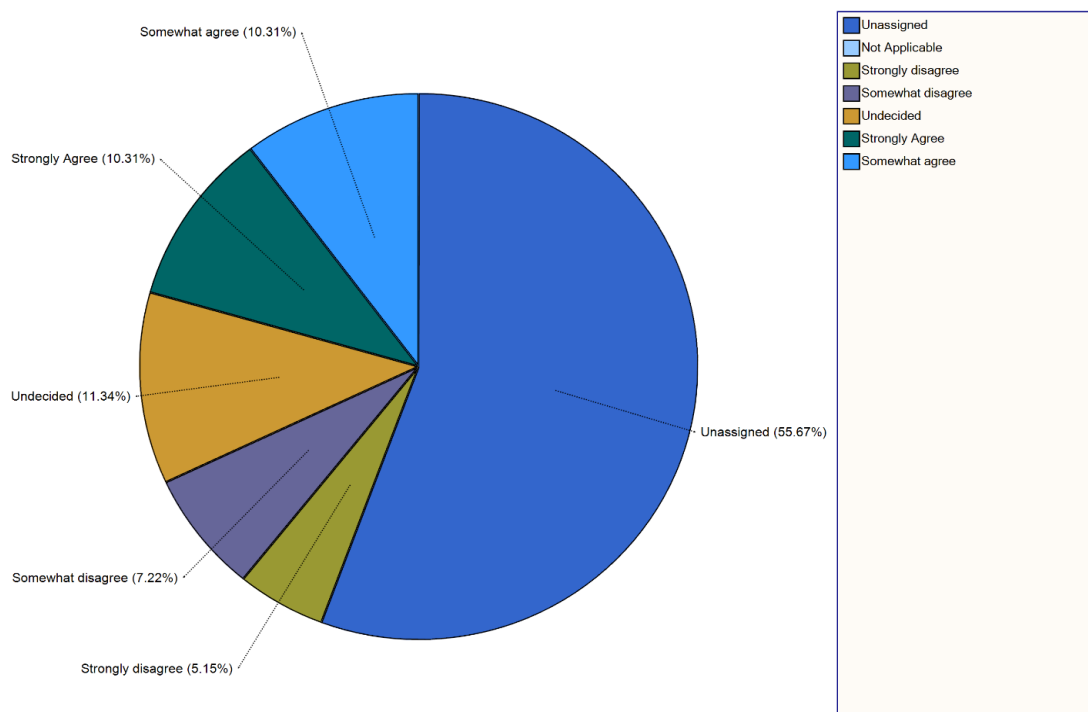


Figure 11: Lack of adequate funding by management for AI deployment

Q.13. The cost of AI deployment & implementation is prohibitive

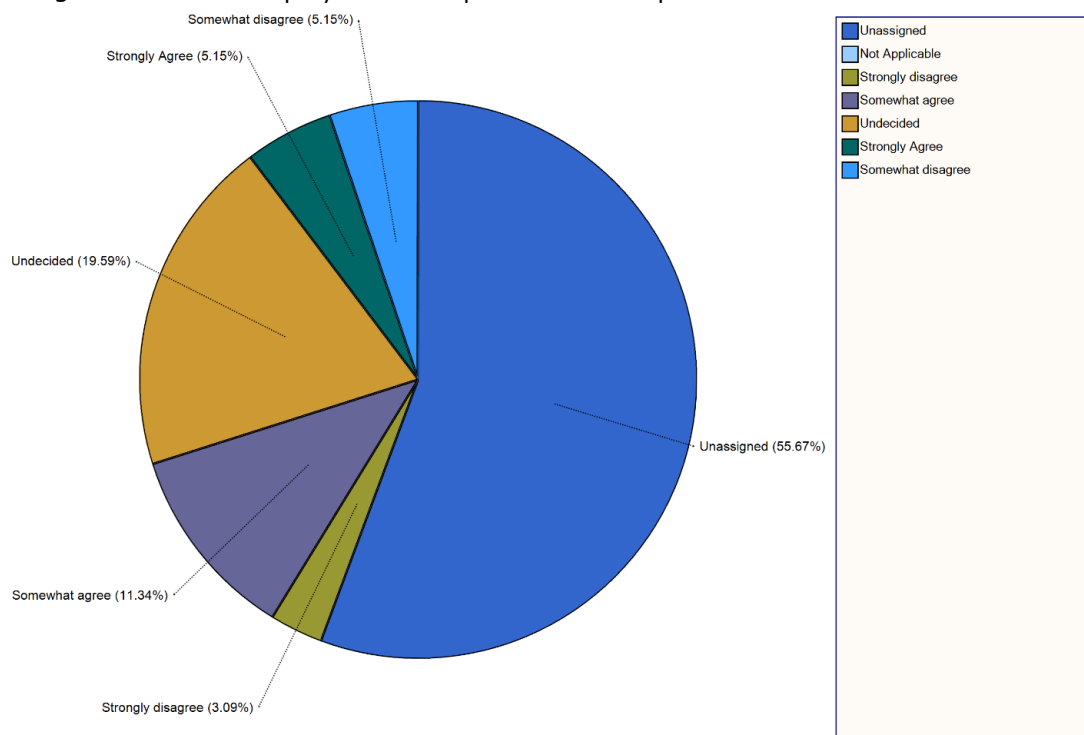


Figure 12: Prohibitive cost of AI deployment & execution

Q.14. Lack of proper in-country technological infrastructure

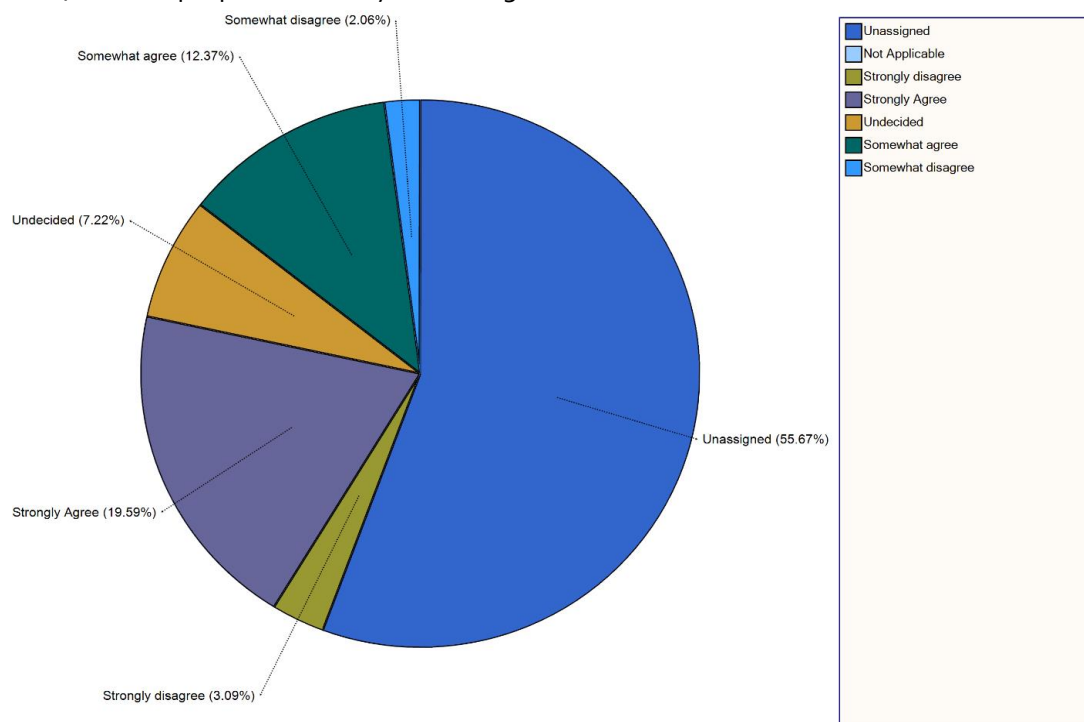


Figure 13: Responses on lack of proper in-country technological infrastructure

Q.14. If there are other factors or elements in play? please specify:

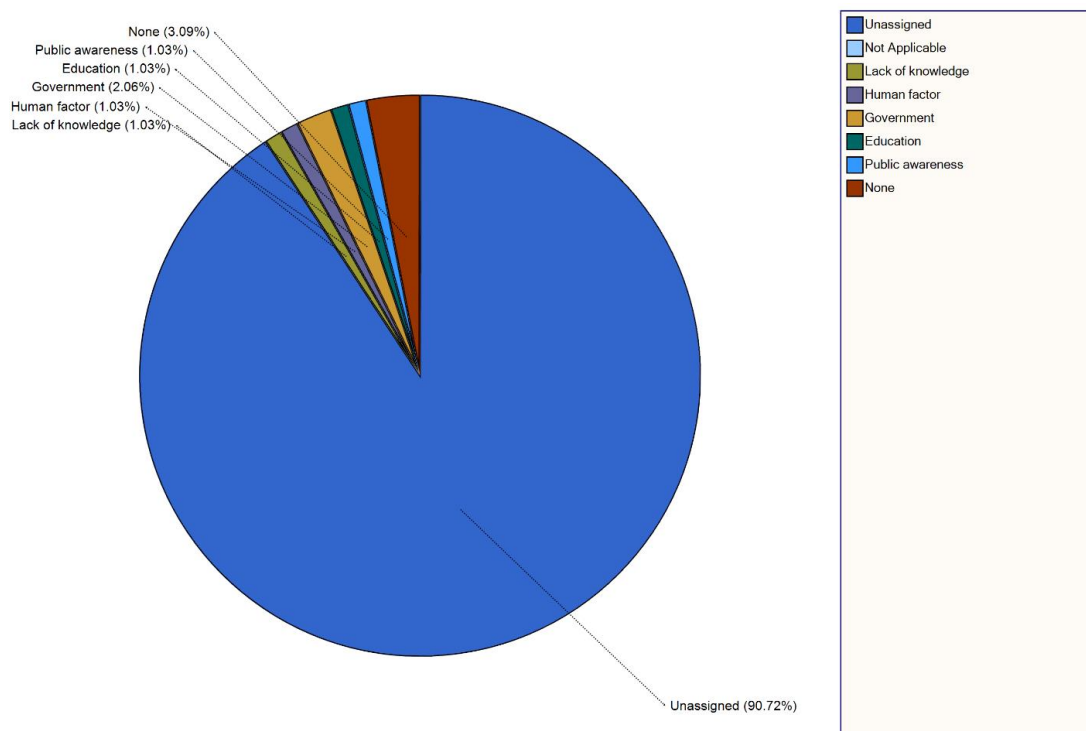


Figure 14: Other factors or elements that affect AI application in banks

Discussion of Findings

Analysis of Participants Demographics

Out of 97 surveys male participants are the majority 59.79% with compared to female participants 40.21% which is expected. According to World Bank report (2023) male working force is 64% whereas female working force is 36% (Available from: <https://data.worldbank.org/indicator/SL.TLF.CACT.FE.ZS>). Thus, male participants are more accessible than female participants. Also, studies by Grameenphone, in collaboration with Brac (2023) found that male and young generations dominate the internet usage (Available from: <https://www.grameenphone.com/about/media-center/press-release/grameenphone-and-brac-expand-safe-internet-awareness-among-students>, accessed 8th June, 2023). This study also reflected the above findings. Out of 97 participants age-group 25 – 34 is the majority 34.02%. The rest of the participants are in the age-groups: 45 – 45 and above (26.80%), 35 – 44 (17.53%), and 18 – 24 (12.37%). The participants are dispersed across Rivers (31.96%), Lagos (27.84%), Abuja (14.43%), Delta (6.19%), Abia (5.15%), Imo and Ogun (4.12%) whereas, Benin (2.06%), and Osun (1.03%) respectively (Figure 3). The participants of this survey are well educated, 54% had Bachelor and 45% are of higher Degree. People from financial institutions had participated in this survey.

Sampling and Study Context

The study focused on selected Nigerian deposit money banks with significant market presence and operational scale. The banks included First Bank of Nigeria, Zenith Bank Plc,

Fidelity Bank Plc, Access Bank Plc, and Guaranty Trust Bank (GTBank). These banks broadly reflect Tier 1 commercial banks based on scale, market footprint, and systemic importance within Nigeria's banking ecosystem. Respondents were primarily IT and cybersecurity-related staff recruited through purposive sampling due to their operational knowledge of cybersecurity systems. A total of 97 valid responses were obtained and analysed.

Analysis on Cyberthreat Awareness

People are informed and updated about cyberthreat by both online sources. According to the population that said "No" (23.71%), Don't know (12.37%), Yes (5.15%), None (2.06%), Not sure (1.03%), and unassigned (55.57%). Based on the percentage of response, it showed that most participants answered "no" to their banks being attacked. Meanwhile 12.37% of participants says they don't know, so we can infer that many people in Nigeria are not aware of cyberthreat (Figure 4). Although, the participants have different opinions about cyber threat awareness.

Implementation of AI-Driven Cyber Security Issues

Out of 97 respondents that participated in the survey, 34.02% said "Yes", 10.31% said "No" and 55.57% is unassigned (Figure 5). This indicates that AI is deployed in Nigerian banks. The term "Unassigned" attribute value label: the label that will be used for the system-created 'Unassigned' attribute value in any new projects that was created. The majority of the participants (29.90%) "Strongly Agree", 9.28% "Somewhat Agree", Undecided participants (5.15%) and 55.67% are unassigned (Figure 6). This shows that the respondents believe that AI-driven cybersecurity can improve the security of the Nigerian Banking sector. Out of the total, (18.56%) "Strongly Agree" that AI-driven cyber system positively affects the service availability for Nigerian banks, (14.43%) Somewhat Agree, 10.31% are undecided, and 1.03% Strongly Disagree. The unassigned response is 55.67%, it can be deduced that AI-driven cyber system affects service availability positively for the Nigerian Banking (Figure 7).

Out of the total population, 14.43% Strongly Disagreed that they have experience working with AI, meanwhile 12.37% respondents are Undecided, 9.28% Somewhat Agrees, then 7.22% Somewhat Disagrees, 1.03% Strongly Agrees, and 55.67% is Unassigned. This indicates that there is lack of experience in working with AI in Nigerian banks, greater percentage (14.43%) of the response strongly disagrees (Figure 8). The response showed that 14.43% are Undecided that they have the required skill to implement AI, meanwhile 11.34% respondents Somewhat Disagree, 9.28% Somewhat Agrees, then 7.22% Strongly Disagrees, 2.06% Strongly Agrees, and 55.67% is Unassigned. A higher percentage is undecided while 11.34% Somewhat disagrees, it is not clear whether the required skills to implement AI in Nigerian banks is available (Figure 9). Out of the total population that participated in the study, it was observed that 14.43% are Undecided, 11.34% Strongly Disagree that they have the right tools to implement AI, meanwhile 10.31% respondents

Somewhat Disagree, 6.19% Somewhat Agrees, then 2.06% Strongly Agrees, and 55.67% is Unassigned. A higher percentage (14.43%) is undecided while 11.34% strongly disagrees, this is a clear indication that the right tools to implement AI in Nigerian banks is not available (Figure 10).

The response in this section showed that 11.34% are Undecided, 5.15% Strongly Disagree that their lack of adequate funding by management for AI deployment, meanwhile 7.22% respondents Somewhat Disagree, 14.43% Somewhat Agrees, then 10.31% Strongly Agrees, and 55.67% is Unassigned. A higher percentage (14.43%) somewhat agrees, 10.31% strongly agrees, which shows that their lack of adequate funding by management for AI deployment (Figure 11). From the population that participated in questionnaire, about 19.59% are Undecided, 3.09% Strongly Disagree that the cost of AI deployment & implementation is prohibitive, meanwhile 5.15% respondents Somewhat Disagree, 11.34% Somewhat Agrees, then 5.15% Strongly Agrees, and 55.67% is Unassigned. Since, the higher percentage (19.59%) is undecided while 11.34% somewhat agrees, this is not a very clear indication that the cost of AI deployment & implementation is prohibitive (Figure 12). Approximately 7.22% of those who responded to the survey are undecided, 3.09% strongly disagree that there is lack of proper in-country technological infrastructure, 2.06% somewhat disagree, 12.37% somewhat agree, 19.59% strongly agree, and 55.67% are unassigned. Considering the majority (19.59%) strongly agreed, this strongly indicates that there is lack of proper in-country technological infrastructure (Figure 13).

About 90.72% of respondents are unassigned, meanwhile the other factors include "None" (3.09%), "Government" (2.06%), "Lack of knowledge" (1.03%), "Human factor" (1.03%), "Education" (1.03%), and "Public awareness" (1.03%). However, the "None" factor has the percentage (3.09) followed by the Government (Figure 14). Therefore, the government has a key role to play in the country technological infrastructure to boost the implementation of AI.

Thematic Analysis

A thematic analysis was conducted on the open-ended questions such as: "Q4. If you have experience any of the above, please provide all websites, apps or games involved". The result showed that "Facebook" and "Instagram" with 12 words each which has the highest word count in the word frequency analysis as presented in Figure 15. A cluster analysis was used to further examine the source of the most experienced cyber threat. Figure 16 indicates that "Facebook" and "banking" are in the same cluster. In hierarchical analysis, the clustering of "Facebook" and "banking" reveals a notable overlap in the ways that users encounter and interpret cyberthreats from these sources. It emphasizes the necessity of all-encompassing cybersecurity plans that tackle flaws shared by financial services and social media. This shows that Facebook has been associated with various cyber threats in the banking industry.



Figure 15: Thematic observation of websites with highest cyber threat experience via word cloud.

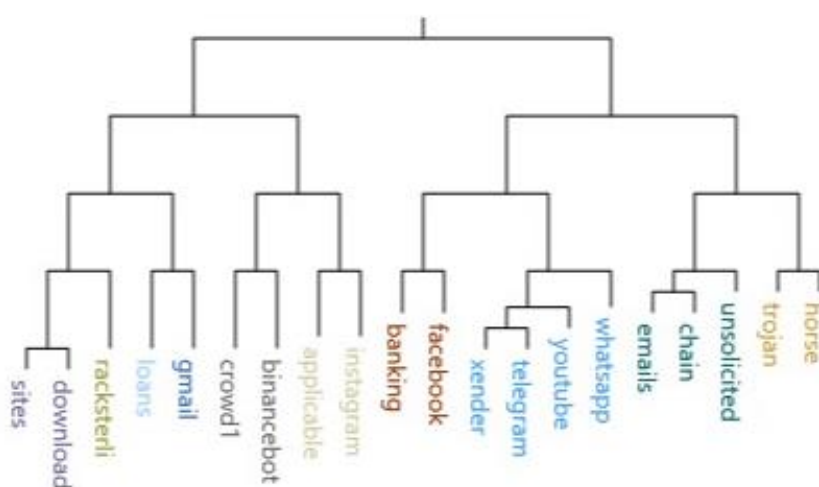


Figure 16: A cluster or hierarchical analysis of cyber threat most experienced website

Therefore, the website with most experienced cyber threat in Nigeria is Facebook and Instagram as indicated in the thematic analysis.

Technological Advancements Driving Adoption

AI technologies have revolutionized cybersecurity by enabling real-time threat detection and adaptive responses to emerging risks. In the Nigerian banking sector: (1) These algorithms analyse vast datasets to identify patterns indicative of malicious activity. For example, anomaly detection systems powered by ML can flag unusual transactions or unauthorized access attempts. (2) AI automates routine tasks such as log analysis and incident reporting, reducing human error and improving efficiency. (3) By analyzing historical data, predictive models forecast potential vulnerabilities or attack vectors before they occur. (4) Many Nigerian banks are migrating their operations to cloud platforms that incorporate built-in AI-driven security features. These technological advancements not only enhance security but also reduce operational costs associated with manual monitoring and response efforts.

Organisational Needs Driving Implementation of AI

The internal dynamics within Nigerian banks also contribute significantly to the adoption of AI-driven cybersecurity: (1) Banks face increasing incidents of fraud, phishing attacks, and malware infiltration targeting both customers and internal systems. (2) Maintaining customer trust is paramount in an industry where breaches can lead to reputational damage and loss of clientele. (3) While initial investments in AI technology may be high, long-term cost savings from reduced breaches and automated processes make it an attractive option. (4) Many traditional IT teams lack expertise in handling modern cyber threats; thus, integrating AI helps bridge this gap by providing automated intelligence. Banks recognize that failing to adapt could result in significant financial losses due to both direct attacks and penalties for non-compliance with regulations.

External Pressures Influencing Adoption of AI

Beyond internal factors, external pressures also drive the adaptation of AI-based cybersecurity: (1) With fintech companies rapidly adopting advanced technologies, traditional banks must follow suit or risk losing market share. (2) As Nigerian banks expand operations internationally or partner with foreign entities, they must meet stringent global cybersecurity requirements. (3) Hackers are increasingly leveraging their own forms of artificial intelligence for attacks (e.g., deepfake scams). This forces organisations to adopt equally sophisticated defenses. These external pressures create an environment where embracing innovation becomes essential for survival.

What are the Challenges Hindering Adoption?

While there are numerous drivers pushing for the adaptation of AI-driven cybersecurity solutions in Nigeria's banking sector, several challenges persist: (1) Advanced tools require significant upfront investment in hardware/software infrastructure. (2) There is a shortage of professionals trained in both artificial intelligence and its application within cybersecurity contexts. (3) Increased use of surveillance tools raises concerns about privacy violations among customers. (4) Cybercriminals may exploit vulnerabilities within poorly designed or untested AI models. Addressing these challenges will require coordinated efforts between stakeholders including government agencies, private organisations, academia, and international partners.

The results indicate that AI-driven cybersecurity adoption is emerging within Nigerian banks, with a notable proportion of respondents confirming AI deployment for cybersecurity functions. This supports the growing recognition that traditional security approaches alone are insufficient for detecting advanced and rapidly evolving threats in financial systems. Respondents also largely perceived AI as capable of improving banking cybersecurity outcomes, particularly through faster detection and improved service availability. These findings align with broader evidence that AI strengthens cyber defence by enabling anomaly detection, automated threat triage, and predictive risk identification (Uzoka et al., 2024). However, readiness constraints were strongly reflected in responses

relating to experience, skills, and access to tools. A substantial share of respondents was undecided or disagreed regarding the availability of the required tools and competencies for AI implementation, suggesting workforce and infrastructure gaps. This pattern is consistent with the TOE framework, which predicts that adoption is influenced not only by perceived usefulness but also by organisational readiness and technological infrastructure (Qin et al., 2020). Similarly, TAM suggests that adoption may be slowed when perceived ease of use is undermined by limited expertise and system complexity (Bryan & Zuva, 2021). The thematic analysis further revealed that Facebook and Instagram were frequently associated with cyber threat experiences. This is significant because social engineering, impersonation, and phishing schemes often exploit social media platforms to target banking customers and staff. The clustering of "Facebook" and "banking" highlights the convergence between consumer digital behaviour and financial fraud risk, indicating that cybersecurity must extend beyond internal controls to include customer-focused security awareness and digital identity protection measures.

In addition, respondents identified inadequate funding and weak technological infrastructure as major barriers. This reinforces evidence that cybersecurity challenges in Nigerian banks are often linked to institutional capacity limitations and governance gaps (Ama et al., 2024; Ojeka et al., 2017). From a managerial perspective, these findings suggest that AI cybersecurity investments must be supported by sustained funding, strategic workforce development, and infrastructure upgrades to achieve effective adoption and operational impact.

Conclusion and Recommendations

Conclusion

This study examined the determinants influencing the adoption of AI-driven cybersecurity in Nigeria's banking sector using survey evidence and thematic analysis. Findings suggest that AI deployment for cybersecurity is increasingly recognised as valuable for improving threat detection and supporting service availability. However, implementation is constrained by skills shortages, limited access to appropriate tools, funding limitations, and inadequate technological infrastructure. The study contributes empirically by providing context-specific evidence on adoption readiness and barriers within Nigerian deposit money banks, while also reinforcing the explanatory relevance of TAM and TOE frameworks for understanding AI adoption decisions in cybersecurity contexts.

Recommendations

Nigerian banks should invest in structured workforce training programmes covering AI security analytics, incident response automation, and cyber threat intelligence. Management should prioritise modern security infrastructure such as cloud security tooling, endpoint analytics to support AI deployment at scale. In addition, regulators and

bank leadership should strengthen AI governance frameworks addressing model transparency, auditability, and data privacy risks.

Banks should intensify anti-phishing and fraud awareness campaigns, especially targeting social media-driven cyber fraud vectors. Furthermore, partnerships between banks, universities, cybersecurity vendors, and government agencies should be encouraged to close skills and technology gaps.

Statements/Declarations

Conflict of Interest Statement:

The author certifies that there is no affiliation with or involvement in any organisation or entity with any financial or non-financial interest in the subject or materials discussed in this manuscript.

Ethics Statement:

I testify that: this material has not been published in whole or in part elsewhere; the manuscript is not currently being considered for publication in another journal; I have been personally and actively involved in substantive work leading to the manuscript, and will hold myself responsible for its content.

Funding Statement:

This is to declare that there is no funding or research grants received in the course of the study or assembly of the manuscript.

Data Access Statement:

Author confirms that the data supporting the findings of this study are available within the article.

Artificial Intelligence (AI) Declaration:

AI and AI-assisted technologies were not used in the development of this manuscript.

References

- Abiodun, A. (2023). Nigeria's financial sector under siege: The alarming rise of cyber fraud and inadequate defenses. *Business Day* <https://businessday.ng/opinion/article/nigerias-financial-sector-under-siege-the-alarming-rise-of-cyber-fraud-and-inadequate-defenses/>
- Ama, G. A. N., Onwubiko, C. O., & Nwankwo, H. A. (2024). Cybersecurity Challenge in Nigeria Deposit Money Banks. *Journal of Information Security* 15(4), 494-523. <https://doi.org/10.4236/jis.2024.154028>
- Arewa, A. (2018). Borderless crimes and digital forensic: Nigerian perspectives. *Journal of Financial Crime* 25(2), 619-631.
- Arora, D., Garg, M., & Mongia, S. (2022). Global case studies, domains and used methodologies concerning cyber security in online banking: a review. 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),
- Braun, V., & Clarke, V. (2012). *Thematic analysis*. American Psychological Association.

- Bryan, J. D., & Zuva, T. (2021). A review on TAM and TOE framework progression and how these models integrate. *Advances in Science, Technology Engineering Systems Journal* 6(3), 137-145. <https://doi.org/10.25046/aj060316>
- Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-methods research: A discussion on its types, challenges, and criticisms. *Journal of Practical Studies in Education* 2(2), 25-36. <https://doi.org/10.46809/jpse.v2i2.20>
- Ebenezer, A. J., Paula, A. M., & Allo, T. (2016). Risk and investment decision making in the technological age: A dialysis of cyber fraud complication in Nigeria. *International Journal of Cyber Criminology* 10(1), 62.
- Gholami, Z., Abdekhoda, M., & Gavvani, V. Z. (2018). Determinant Factors in Adopting Mobile Technology-based Services by Academic Librarians. *DESIDOC Journal of Library Information Technology* 38(4). <https://doi.org/10.14429/djlit.38.4.12676>
- Gulyas, O., & Kiss, G. (2022). Cybersecurity threats in the banking sector. 2022 8th International Conference on Control, Decision and Information Technologies (CoDIT),
- Hinchliffe, A. (2017). Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime. *Computer Fraud Security* 2017(5), 5-9.
- Kedarya, T., & Elalouf, A. (2023). Risk management strategies for the banking sector to cope with the emerging challenges. *Foresight STI Governance*, 17(3), 68-76. <https://dx.doi.org/10.17323/2500-2597.2023.3.68.76>
- Lottu, O. A., Abdul, A. A., Daraojimba, D. O., Alabi, A. M., John-Ladega, A. A., & Daraojimba, C. (2023). Digital transformation in banking: a review of Nigeria's journey to economic prosperity. *International Journal of Advanced Economics*, 5(8), 215-238. <https://doi.org/10.51594/ijae.v5i8.572>
- Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, 6(2), 1001.
- Ojeka, S. A., Ben-Caleb, E., Ekpe, E.-O. I. J. I. R. o. M., & Marketing. (2017). Cyber security in the nigerian banking sector: an appraisal of audit committee effectiveness. *International Review of Management Marketing* 7(2), 340-346.
- Osho, O., & Onoja, A. D. (2015). National cyber security policy and strategy of Nigeria: a qualitative analysis. *International Journal of Cyber Criminology* 9(1), 120. <https://doi.org/10.5281/zenodo.22390>
- Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research Reviews*, 21(3), 625-643. <https://doi.org/10.30574/wjarr.2024.21.3.0707>
- Qin, X., Shi, Y., Lyu, K., & Mo, Y. (2020). Using a TAM-TOE model to explore factors of Building Information Modelling (BIM) adoption in the construction industry. *Journal of Civil Engineering Management* 26(3), 259-277. <https://doi.org/10.3846/jcem.2020.12176>
- 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. <https://doi.org/10.51594/csitrj.v5i2.761>
- Tambawal, S. M. (2024). *Cybercrimes (Prohibition, Prevention, etc), ACT* NFIU. [https://cert.gov.ng/ngcert/resources/CyberCrime Prohibition Prevention etc Act 2024.pdf](https://cert.gov.ng/ngcert/resources/CyberCrime%20Prohibition%20Prevention%20etc%20Act%202024.pdf)
- Uzoka, A., Cadet, E., & Ojukwu, P. (2024). Applying artificial intelligence in Cybersecurity to enhance threat detection, response, and risk management. *Computer Science IT Research Journal*, 2709-0043. <https://doi.org/10.51594/csitrj.v5i10.1677>
- Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, 27(1), 13-15. <https://doi.org/10.4314/mmj.v27i1.4>