



Security Impact Assessment Of Artificial Intelligence In The Banking Sector

Bamisaye David Tunde; Dr S.E. Chaku; Dr. M. Idris & Paul Owoicho Gideon

Centre for Cyberspace Studies,
Nasarawa State University Keffi, Nigeria
tunedamilola1@gmail.com; onvelebocho100@gmail.com

ABSTRACT

This study investigated the impact of artificial intelligence (AI) technologies on cybersecurity in the financial sector. A cross-sectional survey research design was adopted, with a structured questionnaire developed to collect data from a sample of 392 respondents. The data collected were analysed using SPSS 27, and t-tests were employed to test the hypotheses. The study sought to examine the relationship between AI implementation and cybersecurity practices, the preparedness of financial institutions to mitigate AI-related security threats, and the strategies adopted to enhance the security of AI systems. The findings revealed that AI technologies significantly contributed to strengthening the cybersecurity framework of financial institutions. Respondents generally agreed that AI played a crucial role in improving threat detection and response capabilities. However, some concerns were raised regarding the vulnerability of financial institutions to sophisticated cyber threats due to AI integration. The study also found that while financial institutions made efforts to prepare for AI-related security challenges, there was a gap in the training programs and resources available to address these threats adequately. The use of multi-layered security protocols, continuous monitoring, and AI-specific security protocols were identified as effective strategies to mitigate the security risks associated with AI. In conclusion, the study highlighted the critical role of AI in enhancing cybersecurity in the financial sector, though it also emphasized the need for further investment in training, resources, and advanced security strategies to fully harness the potential of AI while managing its associated risks. Based on these findings, the study recommended that financial institutions strengthen their preparedness for AI-related cybersecurity challenges through proactive measures and collaboration with cybersecurity experts.

Keywords: artificial intelligence, cybersecurity, financial sector,

INTRODUCTION

The financial sector has continually led in adopting new technologies to improve efficiency and competitiveness. In the digital era, Artificial Intelligence (AI) has become a key driver transforming financial operations, risk management, and customer engagement (Adebayo et al., 2023). Technologies such as Machine Learning (ML), Natural Language Processing (NLP), and Robotic Process Automation (RPA) now enhance decision-making, fraud detection, and customer experience (Russell & Norvig, 2023). Nigerian banks increasingly employ AI chatbots, predictive analytics, and automation to reduce costs and improve service quality (Akinbami & Johnson, 2024).

However, the integration of AI introduces new security challenges. Financial institutions face risks of data breaches, algorithmic bias, and system manipulation due to the heavy dependence of AI on data integrity (Eze & Chinedu, 2024). The “black box” nature of many AI models also limits transparency and accountability (Chakraborty & Joseph, 2025). Moreover, the financial sector’s high value attracts cybercriminals, and AI deployment expands potential attack surfaces—especially in developing countries like Nigeria, where cybersecurity infrastructure remains weak (CBN, 2023a).

To address these challenges, **Security Impact Assessment (SIA)** provides a structured means of identifying and mitigating risks related to AI systems. It examines model transparency, data governance, and cybersecurity robustness (Oduwole & Emecheta, 2024). While AI itself enhances security through threat detection and behavioral analytics (Adeyemi & Ogundipe, 2024), its dual-use potential demands effective regulation and ethical oversight (KPMG Nigeria, 2025).

Nigeria’s regulatory frameworks on AI remain nascent and lack provisions on algorithmic accountability and ethical application (CBN, 2023b; NITDA, 2023). Strengthening these is vital to maintain public trust, which is central to financial inclusion and stability (Adebisi & Iwundu, 2023). Globally, the fusion of AI with blockchain offers additional transparency and resilience for financial systems (Olatunji & Ajayi, 2025).

Therefore, a comprehensive **Security Impact Assessment of AI systems in Nigeria’s financial sector** is essential. Beyond technical evaluation, it should include organizational policies, staff training, and regulatory compliance. Collaboration among banks, fintechs, regulators, and researchers is also critical to ensure AI adoption promotes both innovation and security (Deloitte, 2024; Digital Rights Foundation, 2025).

Research Questions

The study is guided by the following research questions:

- i. What are the major security risks associated with the use of Artificial Intelligence in the financial sector?
- ii. To what extent do AI technologies impact the overall cybersecurity framework of financial institutions?
- iii. How prepared are financial institutions in mitigating AI-related security threats?
- iv. What strategies can be employed to strengthen the security of AI systems in financial operations?

1.4 Objectives of the Study

The main objective of this study is to assess the security impact of Artificial Intelligence in the financial sector. The specific objectives are:

- i. To identify the key security risks associated with the implementation of AI in financial institutions.
- ii. To examine the effect of AI technologies on existing cybersecurity infrastructures within the financial sector.
- iii. To assess the level of preparedness of financial institutions in addressing AI-related security vulnerabilities.
- iv. To recommend strategic measures for enhancing the security of AI systems in financial operations.

1.5 Statement of the Hypotheses

To guide the study, the following hypotheses are proposed:

H₀: There is no significant relationship between AI use and security risks in the financial sector.

H₁: There is a significant relationship between AI use and security risks in the financial sector.

H₀: AI implementation has no significant impact on existing cybersecurity infrastructures.

H₁: AI implementation has a significant impact on existing cybersecurity infrastructures.

H₀: Financial institutions are not adequately prepared for AI-related security challenges.

H₁: Financial institutions are adequately prepared for AI-related security challenges.

H₀: Security strategies have no significant effect on mitigating AI-related threats.

H₁: Security strategies have a significant effect on mitigating AI-related threats.

LITERATURE REVIEW

Conceptual Framework

Artificial Intelligence (AI)

Artificial Intelligence (AI) is a branch of computer science that develops systems capable of performing tasks requiring human-like intelligence, including learning, reasoning, and decision-making (Russell & Norvig, 2023). In finance, AI enhances operations through automation, predictive analytics, and real-time decision-making. Nigerian banks use AI for fraud detection, customer support, and credit scoring, enabling faster, data-driven services (Eze & Chinedu, 2024). AI-driven digital banking platforms also promote financial inclusion by providing credit access to those without traditional banking records (Adebayo et al., 2023).

Cybersecurity

Cybersecurity encompasses the technologies and processes designed to protect systems, networks, and data from cyber threats. In finance, it ensures the confidentiality, integrity, and availability of information, which is vital for maintaining customer trust and operational stability (Eze & Nwankwo, 2024). With increased digitization, Nigerian banks face threats such as phishing, ransomware, and data breaches, making strong cybersecurity policies essential (Adebayo, Olatunji, & Yusuf, 2023).

Financial Sector and Digital Transformation

The Nigerian financial sector has undergone major transformation through the adoption of digital technologies, fundamentally reshaping operations, service delivery, and customer engagement. Digital transformation refers to the integration of digital systems into all aspects of banking operations, leading to enhanced efficiency, accessibility, and innovation (Oduwole & Emecheta, 2024). Technologies such as mobile banking, blockchain, artificial intelligence (AI), and cloud computing have redefined how banks manage risks, deliver services, and interact with customers.

Security Impact Assessment (SIA)

A **Security Impact Assessment (SIA)** is a structured process for identifying and mitigating potential security risks associated with new technologies or systems. It helps organizations safeguard the confidentiality, integrity, and availability of information assets during digital transformation (Russell & Norvig, 2023). As banks adopt AI, blockchain, and mobile systems, SIA becomes essential to prevent vulnerabilities that could undermine trust and stability in financial operations.

SIA begins with identifying critical assets—both physical, such as servers, and intangible, such as customer data. These assets are then evaluated for potential threats and vulnerabilities, including cyberattacks, unauthorized access, and algorithmic weaknesses (Eze & Nwankwo, 2024). In Nigerian financial institutions, such risks are particularly relevant given the rise in sophisticated cybercrime and AI-driven fraud (Adebayo, Olatunji, & Yusuf, 2023).

Machine Learning in Finance

Machine Learning (ML) has become a major driver of innovation in the financial sector, enhancing decision-making, risk management, and customer experience. It enables systems to learn from data and make predictions without explicit programming (Russell & Norvig, 2023). In finance, ML supports fraud detection, credit scoring, trading, and customer service, offering faster and more accurate outcomes.

Fraud detection is a leading ML application, as financial institutions face increasing cyber-fraud risks. By analyzing transaction data, ML models identify anomalies that indicate fraudulent behavior, providing real-time alerts (Brynjolfsson & McAfee, 2023). Nigerian banks increasingly rely on these models to minimize financial losses (Eze & Chinedu, 2024).

Data Privacy and Protection in Financial Systems

Data privacy and protection are now central to financial security, given institutions' reliance on digital technologies to store and process sensitive information. Data privacy concerns individuals' rights to control their personal data, while data protection involves safeguarding it from unauthorized access (Russell & Norvig, 2023).

With growing digital banking adoption, data breaches and cyberattacks have become more sophisticated, often leading to identity theft and financial losses. Common threats include phishing, malware, and

ransomware, necessitating strong cybersecurity measures such as encryption, multi-factor authentication, and continuous monitoring (Adebayo, Olatunji & Yusuf, 2023; Adebisi & Iwundu, 2023).

Risk Management in AI Applications

Risk management in Artificial Intelligence (AI) applications is essential, particularly in high-stakes sectors such as finance, healthcare, and cybersecurity. As AI systems become integral to decision-making, they introduce operational, ethical, and security risks that can have severe consequences if unaddressed (Russell & Norvig, 2023). Effective AI risk management therefore entails identifying, assessing, and mitigating these potential threats throughout an AI system's lifecycle.

Algorithmic Bias and Manipulation

Algorithmic bias and manipulation present serious threats to the integrity of AI-driven systems. Bias occurs when AI algorithms produce unfair or discriminatory results due to flawed data or programming assumptions, while manipulation involves intentional exploitation of algorithms to achieve unethical or deceptive outcomes (Russell & Norvig, 2023). Both issues undermine trust and fairness in automated decision-making.

AI bias often originates from unbalanced or historically skewed datasets. In finance, biased training data can result in discriminatory credit scoring or loan approvals, disadvantaging certain demographic groups (Adebayo, Olatunji, & Yusuf, 2023). Such outcomes perpetuate existing inequalities rather than correcting them. Similarly, in employment or insurance sectors, biased AI models may favor or penalize individuals based on gender, ethnicity, or geography (Akinola & Ojo, 2023).

Regulatory Compliance and Financial Technology

Regulatory compliance in the financial technology (fintech) sector ensures adherence to legal and ethical standards that safeguard consumers, promote stability, and prevent fraud (Olayemi, 2024). The rise of fintech innovations—such as AI, blockchain, and mobile payments has transformed banking operations, but also created new regulatory challenges requiring adaptive oversight (Akinbami & John on, 2024).

A major issue is the **regulatory gap** between rapid technological advancement and slower policy development. Fintech firms often operate in areas not fully covered by traditional banking laws, creating risks of non-compliance and exploitation (Akinola & Ojo, 2023). For example, blockchain's decentralized nature complicates anti-money laundering (AML) monitoring and transaction verification (Oduwole & Emecheta, 2024). Regulators must balance innovation with protection, fostering a secure and transparent digital financial environment.

Predictive Analytics and Decision-Making in Finance

Predictive analytics involves using statistical methods, machine learning algorithms, and historical data to forecast future outcomes. In the financial sector, it has become an essential tool for enhancing decision-making, enabling institutions to anticipate market changes, manage risks, and improve operational efficiency (Akinbami & Johnson, 2024). The growing use of predictive analytics is transforming how financial organizations assess credit risk, detect fraud, and make investment decisions.

The adoption of predictive analytics has been accelerated by the availability of massive datasets generated from customer transactions, market activities, and digital interactions. Financial institutions now analyze these data streams to forecast stock prices, interest rates, and credit risk with higher precision (Olatunji & Ajayi, 2025). Predictive models allow decision-makers to interpret complex financial patterns and respond proactively to emerging risks and opportunities.

Empirical Review

Adebayo et al. (2023) conducted a quantitative study using a descriptive design to examine the impact of Artificial Intelligence (AI) on financial inclusion in Nigeria. Using descriptive statistics and chi-square analysis, they found that AI technologies such as mobile banking and automated services significantly improve access to finance for underserved populations. These tools reduce barriers related to geography and literacy, promoting financial empowerment. The study emphasized AI's potential to extend affordable financial services to the unbanked and called for policies that encourage technology-driven inclusion.

Adebisi and Iwundu (2023) investigated trust and security perceptions in Point of Sales (POS) systems using regression and chi-square analysis. They found that while POS adoption is increasing, persistent concerns over fraud and data breaches hinder user confidence. The study recommended stronger security frameworks and clearer communication by vendors to improve trust and adoption.

Adeyemi and Ogundipe (2024) employed a mixed descriptive-correlational design to assess how AI and blockchain technologies enhance IT security in Nigerian banks. Regression results showed that integrating these tools strengthens transparency, reduces fraud, and enhances customer trust. They concluded that AI and blockchain provide complementary mechanisms for securing digital banking and urged wider institutional adoption to mitigate cyber threats.

Akinbami and Johnson (2024) used a cross-sectional survey to evaluate AI chatbots' role in improving customer satisfaction in Nigerian banks. Findings revealed that chatbots increase responsiveness, reduce waiting time, and enhance user experience, leading to higher satisfaction and loyalty. The study recommended that banks expand chatbot deployment to strengthen service efficiency and customer engagement.

Akinola and Ojo (2023) applied a qualitative case study approach, interviewing IT managers and security officers to explore AI and blockchain adoption in banks. The study found that while adoption is rising, high costs and regulatory uncertainty remain barriers. They suggested cost-effective strategies and clearer policies to accelerate adoption and bolster IT security.

Brynjolfsson and McAfee (2023), in their literature-based analysis, examined the digital transformation of financial services. They concluded that AI enhances operational efficiency, automation, and personalization, positioning it as a strategic necessity for competitive advantage. The study stressed that banks must integrate AI to remain efficient, customer-focused, and relevant in the digital era.

Chakraborty and Joseph (2025) adopted a mixed-methods approach to explore AI's effect on customer experience in banking. Statistical analysis revealed that predictive analytics, recommendation systems, and automated service tools improve satisfaction and loyalty by providing timely, personalized solutions. The study recommended prioritizing AI adoption to sustain competitiveness and enhance user-centered banking.

Eze and Chinedu (2024) used regression analysis to evaluate AI's role in fraud detection within Nigerian banks. Results showed that AI systems effectively identify transaction anomalies and detect fraud in real time, outperforming traditional methods. The integration of AI reduced financial losses and improved operational trust. The study advocated for continuous AI investment to strengthen fraud prevention.

Eze and Nwankwo (2024) employed a mixed-methods design to assess AI's role in IT security. They found that AI tools—such as biometric authentication and behavioral analytics—enhance detection and prevention of unauthorized access. Continuous system updates were deemed vital to counter evolving cyber threats. The study concluded that AI significantly improves institutional resilience and customer trust.

Theoretical Framework

Socio-Technical Systems (STS) Theory

Socio-Technical Systems (STS) Theory, developed by Eric Trist and Fred Emery in 1960, emphasizes the interdependence between social systems (people, culture, and relationships) and technical systems (tools, technologies, and processes). It posits that organizations perform optimally when both systems are jointly optimized rather than separately developed. This framework provides insight into how technology and human factors can be aligned to enhance productivity, adaptability, and satisfaction in workplaces, especially as digital and AI technologies become central to organizational operations.

The theory's relevance is evident in Nigerian banks adopting Artificial Intelligence (AI) and blockchain technologies to strengthen IT security and service delivery. Adeyemi and Ogundipe (2024) showed that these technologies improve data integrity and transparency but require skilled personnel and customer trust to succeed. Similarly, Akinbami and Johnson (2024) found that AI-powered chatbots enhance customer satisfaction, though their success depends on users' comfort and interaction quality. These

findings validate STS Theory's assertion that technical innovations must align with social systems for sustainable outcomes.

However, STS has been criticized for being overly idealistic, assuming an achievable balance between technical and social subsystems. In profit-driven industries like banking, efficiency often overrides human considerations. For instance, Adebisi and Iwundu (2023) observed that while Point-of-Sale (POS) systems improve convenience, users' security concerns undermine adoption—highlighting the human element often overlooked in technical implementations. STS also underrepresents external factors such as regulation and economic conditions that influence technology adoption in developing economies.

Despite its limitations, STS remains relevant to this study, offering a dual lens for understanding technical efficiency and social adaptation in AI integration. Eze and Chinedu (2024) noted that AI-driven fraud detection requires continuous human oversight, while Oduwole and Emecheta (2024) found that blockchain and AI's combined effectiveness relies on employee comprehension and user trust. These examples affirm STS's premise that successful technology adoption depends on harmonizing human and technical components.

Technology Threat Avoidance Theory (TTAT)

Technology Threat Avoidance Theory (TTAT), proposed by Liang and Xue (2009), explains how individuals and organizations perceive and respond to information technology threats. It suggests that when users perceive risks such as cyberattacks or data breaches, they assess threat severity, susceptibility, and the effectiveness of safeguards before adopting protective behaviors. TTAT is particularly relevant to cybersecurity, as users' perceptions and coping strategies influence system adoption and resilience.

In Nigerian banking, TTAT helps explain responses to AI and blockchain-based security systems. Eze and Nwankwo (2024) found that AI-driven biometric systems and machine learning tools enhance protection but depend on users' confidence in their reliability. Adeyemi and Ogundipe (2024) similarly noted that blockchain's transparency reassures users and mitigates fraud fears. Thus, TTAT provides a framework for analyzing behavioral and perceptual responses to emerging digital security tools.

RESEARCH METHODOLOGY

Research Design

Research design is a critical aspect of any study as it dictates the overall structure and strategy for data collection and analysis (Saunders, Lewis, & Thornhill, 2019). This study adopted a cross-sectional and **quantitative survey research design**, which was deemed appropriate due to the objective of assessing the security impact of Artificial Intelligence (AI) in the financial sector. The survey design allows for the systematic collection of numerical data, which can be used to identify patterns, relationships, and correlations among the variables under investigation (Bell, Bryman, & Harley, 2019).

Quantitative research is effective when the study seeks to quantify variables, test hypotheses, and generalize findings to a larger population (Creswell & Creswell, 2018). In this case, the study aimed to evaluate the extent of AI deployment in the financial sector and its associated security risks, as well as the preparedness of financial institutions to address these challenges. A survey-based approach is ideal because it allows for the collection of data from a wide range of financial institutions, thereby providing a comprehensive understanding of the issue across different contexts and regions.

3.2 Population, Sample, and Sampling Techniques

The population for this study consisted of employees working in the IT and cybersecurity departments of various financial institutions, including commercial banks, insurance companies, and fintech firms, located in major cities such as Lagos, Abuja, Port Harcourt, and Kano. These individuals were selected because they are directly involved in the implementation and management of AI technologies and the cybersecurity measures in their respective organizations. According to the Central Bank of Nigeria (CBN) and the National Insurance Commission (NAICOM), these institutions represent the most technologically advanced financial organizations in Nigeria, thus providing the appropriate context for examining the integration of AI and its security implications.

To ensure the sample size was statistically significant, a **simple random sampling technique** was employed. This approach ensures that every member of the population has an equal chance of being selected, which minimizes bias and enhances the representativeness of the sample (Tavakol & Dennick, 2021). Given that the total number of employees in these departments is estimated to be around 2000 individuals across the selected regions, the sample size was determined using the Taro Yamane formula. This formula helps determine an optimal sample size based on the population size, margin of error, and confidence level (Charan & Biswas, 2019).

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

where n represents the sample size, N is the population size, and e is the margin of error.

Applying the values to the formula, with a population size (N) of 2000 and an error margin (e) of 0.05:

$$n = 2000 / (1 + 2000 \times 0.05^2)$$

$$n = 171 / (1 + 2000 \times 0.0025)$$

$$n = 2000 / 1 + 5 = 2000 / 6$$

$$n \approx 333$$

Rounded to the nearest whole number, the calculated sample size using the Taro Yamane formula is approximately 333. Therefore, a sample size of 333 respondents was adopted for this study.

3.3 Methods of Data Collection

Data for this study were collected using a structured questionnaire, which was designed to capture relevant information regarding the use of AI in the financial sector, associated security risks, and the preparedness of institutions to address these challenges. The questionnaire consisted of both closed-ended questions, which were suitable for quantitative analysis, and a few open-ended questions that allowed respondents to provide additional insights.

The choice of a questionnaire as the primary data collection method was driven by the need to gather a large amount of data from a geographically dispersed sample. Questionnaires are efficient for this purpose because they can be distributed widely and completed in a relatively short time frame. Additionally, they are cost-effective and allow for standardization of responses, which is crucial when analyzing data quantitatively (Bernard & Ryan, 2019). The survey was distributed through both electronic and paper-based formats, depending on the respondent's preference and accessibility.

The questionnaire included sections on demographics, AI technologies currently in use by the respondents' organizations, their perceptions of security risks associated with AI, the preparedness of their institutions in mitigating these risks, and the security strategies employed. The items were developed based on a review of existing literature on AI and cybersecurity in the financial sector, ensuring that the questions were both relevant and comprehensive.

3.4 Technique for Data Analysis

The data collected from the questionnaires were analyzed using SPSS27 (Statistical Package for the Social Sciences), which is a widely recognized statistical tool for analyzing quantitative data. SPSS allows for the application of various statistical techniques, including descriptive statistics, correlation analysis, and regression analysis, which were suitable for answering the research questions posed in the study (Frankfort-Nachmias, Nachmias, & DeWaard, 2021).

Descriptive statistics were used to summarize the demographic characteristics of the respondents and to present an overview of the AI technologies being used by the financial institutions. Measures such as frequency, percentage, and mean were used to summarize the responses to the closed-ended questions. Correlation analysis was used to examine the relationships between variables, such as the use of AI technologies and the perceived increase in security risks. Additionally, regression analysis was applied to test the hypotheses and assess the impact of AI deployment on the cybersecurity framework of financial institutions.

SPSS27 was selected for its ability to handle large datasets and perform complex statistical analyses, which is crucial for a study of this scope and nature. It also provides a user-friendly interface that allows for the efficient processing and interpretation of data, ensuring the accuracy and reliability of the results (Morse et al., 2022).

DATA PRESENTATION AND ANALYSIS

Data Presentation

Demographic Distribution of Respondents

Table 4.1: Demographic Distribution of Respondents (Total Response = 333)

Demographic Category	Response Options	Frequency (f)	Percentage (%)
Gender	Male	180	54.05%
	Female	153	45.95%
	Total	333	100%
Age Group	Below 20 years	30	9.00%
	21 - 30 years	85	25.53%
	31 - 40 years	105	31.53%
	41 - 50 years	70	21.01%
	51 - 60 years	33	9.91%
	Above 60 years	10	3.00%
	Total	333	100%
Highest Level of Education	High School/Secondary School	20	6.00%
	Bachelor's Degree	170	51.06%
	Master's Degree	100	30.03%
	Doctorate (PhD)	25	7.51%
	Professional Certification (e.g., ACCA, CISSP)	15	4.51%
	Other	3	0.90%
	Total	333	100%
Occupation/Job Title	IT Specialist	90	27.03%
	Cybersecurity Analyst	60	18.02%
	Financial Analyst	70	21.01%
	Bank Manager	45	13.51%
	Risk Management Officer	40	12.01%
	Software Developer	15	4.51%
	Other	13	3.90%
	Total	333	100%
Years of Experience in the Financial Sector	Less than 1 year	15	4.51%
	1 - 5 years	60	18.02%
	6 - 10 years	110	33.03%
	11 - 15 years	75	22.51%
	16 - 20 years	50	15.03%
	More than 20 years	23	6.90%
	Total	333	100%
Type of Financial Institution	Commercial Bank	120	36.03%
	Microfinance Bank	30	9.00%
	Insurance Company	40	12.01%
	Investment Bank	50	15.03%
	Fintech Organization	70	21.01%
	Central Bank	10	3.00%
	Other	13	3.90%
	Total	333	100%

Region of Operation (for financial institution)	North	60	18.02%
	South	100	30.03%
	East	70	21.01%
	West	50	15.03%
	National/All regions	53	15.91%
	Total	333	100%
Familiarity with AI in Financial Operations	Very Familiar	150	45.05%
	Somewhat Familiar	120	36.03%
	Not Familiar at All	63	18.91%
	Total	333	100%
Has your institution adopted AI technologies?	Yes	200	60.06%
	No	100	30.03%
	I don't know	33	9.91%
	Total	333	100%
Position within the Organization	Executive/Management	85	25.53%
	Technical Staff	140	42.03%
	Support Staff	50	15.03%
	Consultant/External Partner	35	10.51%
	Other	23	6.90%
	Total	333	100%

Source: Researcher's Analysis, 2025

Table 4.1 presents the demographic characteristics of 333 respondents who participated in the study on Artificial Intelligence (AI) and cybersecurity in the financial sector. The sample comprised 54.05% males and 45.95% females, indicating near gender balance. Most respondents were between 31–40 years, suggesting mid-career professionals with practical experience. Educationally, 51.06% held bachelor's degrees, and 30.03% had master's degrees, showing a highly educated workforce. Major occupational groups included IT specialists (27.03%), cybersecurity analysts (18.02%), and financial analysts (21.01%), with most respondents having 6–15 years of experience. Participants represented various financial institutions, mainly commercial banks (36.03%) and fintech firms (21.01%), covering all regions of Nigeria. Notably, 60.06% confirmed their institutions had adopted AI technologies, and 45.05% reported being highly familiar with AI operations, demonstrating substantial engagement and valuable insights into the associated cybersecurity implications within the Nigerian financial landscape.

DATA ANALYSIS AND RESULTS

Research Question 1: *What are the major security risks associated with the use of Artificial Intelligence in the financial sector?*

Table 4.2: Major Security Risks Associated with the Use of Artificial Intelligence in the Financial Sector

Security Risk Statement	Response Options	Frequency (f)	Percentage (%)
The use of AI in the financial sector increases the risk of cyber-attacks.	Strongly Agree	180	54.05%
	Agree	90	27.03%
	Uncertain	30	9.00%
	Disagree	20	6.00%
	Strongly Disagree	13	3.90%

	Disagree		
	Total	333	100%
AI systems in financial institutions are vulnerable to data breaches.	Strongly Agree	140	42.03%
	Agree	120	36.03%
	Uncertain	45	13.51%
	Disagree	18	5.41%
	Strongly Disagree	10	3.00%
	Total	333	100%
AI-enabled systems can be exploited for fraudulent activities in the financial sector.	Strongly Agree	170	51.06%
	Agree	90	27.03%
	Uncertain	40	12.01%
	Disagree	20	6.00%
	Strongly Disagree	13	3.90%
	Total	333	100%
The implementation of AI increases the risk of privacy violations in financial transactions.	Strongly Agree	160	48.03%
	Agree	100	30.03%
	Uncertain	50	15.03%
	Disagree	13	3.90%
	Strongly Disagree	10	3.00%
	Total	333	100%
AI systems pose a significant threat to the integrity of financial data due to their complexity.	Strongly Agree	180	54.05%
	Agree	80	24.02%
	Uncertain	50	15.03%
	Disagree	13	3.90%
	Strongly Disagree	10	3.00%
	Total	333	100%

Source: Researcher's Analysis, 2025

Table 4.2 summarizes respondents' perceptions of major security risks linked to Artificial Intelligence (AI) in the financial sector. Out of 333 participants, 81% agreed that AI increases cyber-attack risks, emphasizing the need for stronger cybersecurity protocols. Similarly, 78% believed AI systems are highly vulnerable to data breaches due to their handling of sensitive financial information. About 78% also viewed AI as susceptible to fraudulent manipulation, such as identity theft and algorithmic abuse. Privacy concerns were equally significant, with 78% agreeing that AI heightens risks of personal data misuse. Furthermore, 78% of respondents feared that AI complexity could threaten data integrity through bias, model errors, or lack of transparency. Overall, the findings indicate a broad consensus among financial professionals that AI introduces serious cybersecurity and ethical challenges. These insights highlight the urgent need for stricter regulations, ethical frameworks, and robust data protection strategies in AI-driven financial operations.

Research Question 2: *To what extent do AI technologies impact the overall cybersecurity framework of financial institutions?*

Table 4.3: Impact of AI Technologies on the Overall Cybersecurity Framework of Financial Institutions

AI Technology Impact Statement	Response Options	Frequency (f)	Percentage (%)
The introduction of AI technologies significantly strengthens the cybersecurity framework of financial institutions.	Strongly Agree	150	45.05%
	Agree	110	33.03%
	Uncertain	40	12.01%
	Disagree	20	6.00%
	Strongly Disagree	13	3.90%
	Total	333	100%
AI technologies have made financial institutions more vulnerable to sophisticated cyber threats.	Strongly Agree	140	42.03%
	Agree	120	36.03%
	Uncertain	40	12.01%
	Disagree	20	6.00%
	Strongly Disagree	13	3.90%
	Total	333	100%
AI integration into cybersecurity infrastructures enhances the ability of financial institutions to detect and respond to security threats.	Strongly Agree	180	54.05%
	Agree	100	30.03%
	Uncertain	40	12.01%
	Disagree	10	3.00%
	Strongly Disagree	3	0.90%
	Total	333	100%
The impact of AI technologies on financial cybersecurity is minimal.	Strongly Agree	20	6.00%
	Agree	30	9.00%
	Uncertain	80	24.02%
	Disagree	100	30.03%
	Strongly Disagree	103	30.93%
	Total	333	100%
AI-driven tools are critical in identifying potential security breaches within financial institutions' systems.	Strongly Agree	170	51.06%
	Agree	120	36.03%
	Uncertain	30	9.00%
	Disagree	10	3.00%
	Strongly Disagree	3	0.90%
	Total	333	100%

Source: Researcher's Analysis, 2025

Table 4.3 presents respondents' views on how Artificial Intelligence (AI) influences cybersecurity in financial institutions. A majority (78.08%) agreed that AI strengthens cybersecurity frameworks through automation, predictive analytics, and real-time threat detection. However, a similar proportion (78.06%) acknowledged that AI also exposes institutions to more sophisticated threats, revealing its dual impact on security systems. Furthermore, 84.08% affirmed that AI enhances the ability to detect and respond to threats, underscoring its value in improving operational resilience. Conversely, 60.96% disagreed that AI's impact is minimal, confirming its significant role in cybersecurity advancement. Finally, 87.09% strongly supported that AI-driven tools effectively identify potential breaches, emphasizing their growing importance in financial security management despite the evolving complexity of AI-related risks.

Research Question 3: How prepared are financial institutions in mitigating AI-related security threats?

Table 4.4: Preparedness of Financial Institutions in Mitigating AI-Related Security Threats (Total Response = 333)

Preparedness Statement	Response Options	Frequency (f)	Percentage (%)
Financial institutions are well-prepared to mitigate security risks associated with AI technologies.	Strongly Agree	90	27.03%
	Agree	130	39.03%
	Uncertain	50	15.03%
	Disagree	40	12.01%
	Strongly Disagree	23	6.90%
	Total	333	100%
Financial institutions have adequate training programs in place to address AI-related security threats.	Strongly Agree	80	24.02%
	Agree	120	36.03%
	Uncertain	60	18.02%
	Disagree	50	15.03%
	Strongly Disagree	23	6.90%
	Total	333	100%
The current cybersecurity strategies in financial institutions are not sufficient to handle AI-related threats.	Strongly Agree	110	33.03%
	Agree	80	24.02%
	Uncertain	60	18.02%
	Disagree	50	15.03%
	Strongly Disagree	33	9.91%
	Total	333	100%
Financial institutions are continuously updating their systems to stay ahead of AI-related security vulnerabilities.	Strongly Agree	130	39.03%
	Agree	90	27.03%
	Uncertain	50	15.03%
	Disagree	40	12.01%
	Strongly Disagree	23	6.90%
	Total	333	100%
Financial institutions lack the resources to adequately prepare for AI-related security challenges.	Strongly Agree	100	30.03%
	Agree	80	24.02%
	Uncertain	50	15.03%
	Disagree	60	18.02%
	Strongly Disagree	43	12.91%
	Total	333	100%

Source: Researcher's Analysis, 2025

Table 4.4 shows respondents' views on financial institutions' preparedness for AI-related security threats. About 66.06% believe institutions are well-prepared, though 18.91% disagree and 15.03% are uncertain, revealing uneven readiness. Only 60.05% agree that adequate staff training exists, while 21.93% disagree, suggesting limited or outdated programs. Notably, 57.05% believe current cybersecurity strategies are insufficient to address AI threats, emphasizing the need for improved AI-focused measures. Overall, while institutions demonstrate progress in aligning with emerging risks, significant gaps remain in strategy, training, and resource allocation, indicating partial but not comprehensive readiness for AI-driven cybersecurity challenges.

Research Question 4: *What strategies can be employed to strengthen the security of AI systems in financial operations?*

Table 4.5: Strategies to Strengthen the Security of AI Systems in Financial Operations

Strategy Statement	Response Options	Frequency (f)	Percentage (%)
Implementing multi-layered security protocols can significantly enhance the security of AI systems in financial operations.	Strongly Agree	140	42.04%
	Agree	110	33.03%
	Uncertain	40	12.01%
	Disagree	25	7.51%
	Strongly Disagree	18	5.41%
	Total	333	100%
Continuous monitoring of AI systems is essential to identify and prevent potential security threats.	Strongly Agree	130	39.03%
	Agree	120	36.03%
	Uncertain	40	12.01%
	Disagree	25	7.51%
	Strongly Disagree	18	5.41%
	Total	333	100%
Financial institutions should adopt a collaborative approach with external cybersecurity experts to strengthen AI system security.	Strongly Agree	125	37.54%
	Agree	115	34.53%
	Uncertain	50	15.03%
	Disagree	28	8.41%
	Strongly Disagree	15	4.50%
	Total	333	100%
Regular AI system audits and security testing are vital in strengthening security measures in financial operations.	Strongly Agree	135	40.54%
	Agree	115	34.53%
	Uncertain	45	13.51%
	Disagree	23	6.90%
	Strongly Disagree	15	4.50%
	Total	333	100%
The development of AI-specific security protocols can reduce the likelihood of security breaches in financial operations.	Strongly Agree	128	38.44%
	Agree	120	36.03%
	Uncertain	45	13.51%
	Disagree	25	7.51%
	Strongly Disagree	15	4.50%
	Total	333	100%

Source: Researcher's Analysis, 2025

Table 4.5 highlights respondents' views on strategies to strengthen AI system security in the financial sector. A strong 75.07% endorsed multi-layered security protocols such as encryption and AI-based threat detection, reflecting broad support for layered defenses. Continuous monitoring also received 75.06% approval, emphasizing the need for real-time vigilance against emerging threats. Likewise, 72.07% supported collaboration with external cybersecurity experts to enhance expertise and access to threat intelligence. Regular AI audits and testing gained 75.07% backing, reinforcing the value of proactive assessments. Finally, 74.47% agreed on the need for AI-specific security protocols tailored to unique algorithmic risks. Overall, respondents emphasized comprehensive, collaborative, and proactive security strategies as key to protecting AI-driven financial operations.

Table 4.6: One-Sample t-Test Results on AI and Cybersecurity in the Financial Sector

Statement	Mean	Std. Dev.	t-value	df	p-value	Decision
There is no significant relationship between the use of AI and the increase in security risks in the financial sector.	3.89	0.82	18.457	332	0.000	Reject Null Hypothesis
AI implementation has no significant impact on the effectiveness of existing cybersecurity infrastructures in financial institutions.	3.76	0.91	15.932	332	0.000	Reject Null Hypothesis
Financial institutions are not adequately prepared to handle AI-related security challenges.	3.61	0.88	13.208	332	0.000	Reject Null Hypothesis
There is no significant effect of security strategies on the mitigation of AI-related threats in the financial sector.	3.94	0.79	19.003	332	0.000	Reject Null Hypothesis

Source: Researcher's Analysis, 2025

Table 4.6 presents the results of one-sample t-tests conducted to determine the statistical significance of key assertions related to AI and cybersecurity within the financial sector. All four hypotheses tested returned p-values of 0.000, which are well below the conventional significance threshold of 0.05. Consequently, the null hypotheses were rejected in each case, indicating that the respondents' perceptions strongly support the existence of significant relationships in the areas assessed.

For the first statement, the high mean score of 3.89 and t-value of 18.457 suggest a statistically significant relationship between AI use and increased security risks in financial institutions. This supports the perception that AI can both enhance and complicate security measures. Similarly, a mean of 3.76 and t-value of 15.932 for the second statement indicate that AI implementation meaningfully impacts the effectiveness of existing cybersecurity infrastructure—either by improving detection or by introducing new vulnerabilities.

The third hypothesis, with a mean of 3.61, supports the view that financial institutions are inadequately prepared for AI-related security challenges. Lastly, the fourth hypothesis, with the highest mean of 3.94, confirms that strategic interventions significantly influence how well AI-related threats are mitigated. These findings collectively underscore the need for comprehensive AI-aware cybersecurity planning in the sector.

Test of Hypotheses

Based on the results from Table 4.6, the hypotheses were tested and the following conclusions can be drawn:

For the first hypothesis, which tested whether there is no significant relationship between the use of AI and increased security risks in the financial sector, the result shows a t-value of 18.457 and a p-value of 0.000. Since the p-value is less than 0.05, the null hypothesis is rejected, indicating that there is a significant relationship between AI usage and the increase in security risks.

The second hypothesis examined whether AI implementation has no significant impact on the effectiveness of existing cybersecurity infrastructures. The result shows a t-value of 15.932 and a p-value

of 0.000, leading to the rejection of the null hypothesis. This suggests that AI does have a significant impact on the effectiveness of cybersecurity infrastructures in financial institutions.

For the third hypothesis, which tested if financial institutions are adequately prepared to handle AI-related security challenges, the result shows a t-value of 13.208 and a p-value of 0.000. This indicates that financial institutions are not adequately prepared to handle AI-related threats.

Lastly, the fourth hypothesis tested whether security strategies have no significant effect on mitigating AI-related threats. With a t-value of 19.003 and a p-value of 0.000, the null hypothesis is rejected, implying that security strategies play a significant role in mitigating AI-related risks.

Overall, these results indicate that AI significantly influences security risks, cybersecurity effectiveness, preparedness, and the need for robust security strategies in financial institutions.

DISCUSSION OF FINDINGS

The findings from this study highlight the significant role of Artificial Intelligence (AI) in enhancing the cybersecurity framework of financial institutions, particularly in the Nigerian banking sector. The introduction of AI technologies has both improved the security of financial institutions and, at the same time, exposed them to more sophisticated cyber threats. This dual impact is consistent with the observations of Adebayo et al. (2023), who found that AI adoption in Nigerian financial institutions has increased both opportunities for improved security and risks due to the sophistication of cyber threats. This shows that while AI systems can enhance the cybersecurity infrastructures of banks by providing real-time threat detection and predictive analysis, they also create new vulnerabilities that cybercriminals may exploit.

In relation to the findings on the preparedness of financial institutions to mitigate AI-related security threats, the study revealed that while many financial institutions are implementing strategies to address AI security concerns, there is still a gap in training and preparedness. This aligns with the findings of Akinbami and Johnson (2024), who argue that customer satisfaction in Nigerian banks is significantly influenced by AI-powered systems, but that many institutions fail to provide adequate training for their staff in the effective management of AI-related security risks. This highlights the need for continuous investment in training programs to mitigate the security threats associated with AI technologies.

Moreover, the strategies proposed to strengthen the security of AI systems, such as multi-layered security protocols, regular audits, and collaboration with external cybersecurity experts, are in line with the conclusions of Akinola and Ojo (2023). These authors emphasize the importance of robust security protocols and regular system audits to ensure that financial institutions can maintain the security of their AI systems. Additionally, the need for collaborative efforts with external cybersecurity experts is reinforced by the observations of Deloitte (2024), which underscores the growing importance of expert partnerships in mitigating AI-related cybersecurity risks.

The results from the one-sample t-test also support these findings, showing that AI has a significant impact on both the security risks and the effectiveness of cybersecurity strategies in the financial sector. Specifically, the rejection of the null hypotheses related to AI and cybersecurity effectiveness aligns with the work of Eze et al. (2024), who found that AI significantly contributes to improving fraud detection and enhancing cybersecurity infrastructures in Nigerian banks. These results suggest that AI is an essential tool in the fight against cyber threats, but its potential is not fully realized without adequate preparation, training, and strategy implementation.

The conclusions drawn from this study also resonate with the findings of Brynjolfsson and McAfee (2023), who argue that while AI is a transformative technology, it requires careful management and robust security frameworks to avoid exacerbating cybersecurity risks. Furthermore, the Central Bank of Nigeria's (CBN) 2023 report on AI adoption in Nigerian financial institutions points to the challenges and opportunities presented by AI. The report highlights that while AI has the potential to improve cybersecurity, it also requires significant investments in training, infrastructure, and strategic planning.

SUMMARY, CONCLUSION AND RECOMMENDATIONS

Summary

The research focused on exploring the relationship between artificial intelligence (AI) and cybersecurity in the financial sector, particularly within Nigerian financial institutions. Given the rapid adoption of AI technologies in the financial sector, it has become crucial to assess how these advancements influence the overall security environment. This study aimed to assess the preparedness of financial institutions in mitigating AI-related security threats, evaluate the strategies they employ to strengthen AI system security, and test the effectiveness of AI integration in enhancing the security of financial operations.

Conclusion

The results of the hypotheses tested in this study indicate a significant relationship between the use of artificial intelligence (AI) and the effectiveness of cybersecurity measures in Nigerian financial institutions. The rejection of the null hypothesis, particularly regarding AI's impact on the increase in security risks, suggests that AI implementation is strongly linked to both the enhancement and the complexity of security challenges in the financial sector. The findings emphasize that while AI technologies have the potential to improve cybersecurity, they also introduce new risks that financial institutions must address proactively.

Additionally, the significant relationship between AI adoption and the effectiveness of existing cybersecurity infrastructures underscores the importance of integrating AI with robust security protocols. Financial institutions must adopt multi-layered security strategies, conduct regular audits, and collaborate with cybersecurity experts to ensure that AI systems do not create vulnerabilities. The preparedness of these institutions to handle AI-related threats is also critical, as the study revealed gaps in resource allocation and workforce readiness.

RECOMMENDATIONS

Based on the findings of this study, the following recommendations are made for improving the cybersecurity framework of financial institutions in Nigeria, particularly in relation to the adoption of artificial intelligence (AI) technologies:

1. **Strengthen Cybersecurity Infrastructure with AI Integration:** Financial institutions should prioritize the integration of AI technologies into their existing cybersecurity frameworks. However, this integration must be accompanied by the adoption of multi-layered security protocols to safeguard against the increased risks associated with AI. A robust combination of traditional cybersecurity measures and AI-driven tools will help detect and mitigate threats more effectively.
2. **Invest in Continuous Training for Staff:** Institutions should invest in continuous training programs for their employees to enhance their ability to manage AI-related security challenges. This training should focus on emerging AI-driven threats, data privacy concerns, and the proper use of AI tools to ensure that staff can effectively utilize AI technologies to prevent security breaches.
3. **Collaborate with External Cybersecurity Experts:** Financial institutions should collaborate with external cybersecurity experts and consultants to assess their AI security measures. External professionals can provide valuable insights into potential vulnerabilities, help implement best practices, and assist in conducting regular security audits of AI systems to prevent security lapses.
4. **Establish Regular Security Audits and Risk Assessments:** Regular audits and risk assessments should be a core part of any financial institution's cybersecurity strategy. This includes evaluating the performance of AI systems, identifying potential security gaps, and addressing vulnerabilities that could be exploited by cybercriminals. Financial institutions must not rely solely on AI but must also ensure human oversight and regular checks on AI system performance.
5. **Develop AI-Specific Security Protocols:** Institutions should prioritize the development of AI-specific security protocols tailored to the unique challenges posed by AI technologies. These protocols should focus on protecting data integrity, ensuring system resilience, and reducing the

likelihood of AI-related security breaches. This would help financial institutions better align their security strategies with the evolving threat landscape introduced by AI adoption.

REFERENCES

- Adebayo, S., Olatunji, T., & Yusuf, A. (2023). The impact of artificial intelligence on financial inclusion in Nigeria. *Journal of Financial Innovation*, 9(2), 45–63.
- Adebisi, A., & Iwundu, M. P. (2023). Point of Sales (POS) Security Information Management (POS-SIM): An assessment of trust and security perception. *Future X Journal*, 2(2), 19–37.
- Adeyemi, O., & Ogundipe, M. (2024). Artificial intelligence and blockchain in enhancing IT security in Nigerian banks. *African Journal of Banking and Finance*, 18(1), 45–63.
- Akinbami, O., & Johnson, K. (2024). Customer satisfaction in Nigerian banks: The role of AI-powered chatbots. *African Journal of Banking and Finance*, 15(3), 89–101.
- Akinola, S., & Ojo, T. (2023). Case studies on AI and blockchain adoption for IT security in Nigerian banks. *Journal of Financial Security and Technology*, 14(3), 34–51.
- Bell, E., Bryman, A., & Harley, B. (2019). *Business research methods* (5th ed.). Oxford University Press.
- Bernard, H. R., & Ryan, G. W. (2019). *Analyzing qualitative data: Systematic approaches* (2nd ed.). Sage Publications.
- Brynjolfsson, E., & McAfee, A. (2023). *Machine, platform, crowd: Harnessing our digital future*. W. W. Norton & Company.
- Central Bank of Nigeria (CBN). (2023). *AI adoption in the Nigerian financial sector: Challenges and opportunities*. CBN Annual Report.
- Central Bank of Nigeria (CBN). (2023). *Regulatory insights on AI and blockchain adoption in Nigerian banking*.
- Chakraborty, K., & Joseph, S. (2025). Enhancing customer experience with artificial intelligence in banking. *International Journal of Banking Innovation*, 12(4), 112–124.
- Charan, R., & Biswas, S. (2019). Sample size determination in research studies. *International Journal of Research in Applied Science and Engineering Technology*, 7(6), 34-41.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage Publications.
- Deloitte. (2024). *AI and blockchain: Emerging technologies for cybersecurity in Nigerian commercial banks*.
- Digital Rights Foundation. (2025). *Cybersecurity evolution: AI and blockchain in Nigerian banking systems*.
- Eze, P., & Chinedu, U. (2024). Artificial intelligence in fraud detection: Evidence from Nigerian banks. *Journal of Emerging Economies and Policy*, 10(1), 45–61.
- Eze, S., & Nwankwo, U. (2024). Artificial intelligence in IT security: A focus on Nigerian banks. *International Journal of Financial Innovation*, 17(2), 45–61.
- Frankfort-Nachmias, C., Nachmias, D., & DeWaard, J. (2021). *Research methods in the social sciences* (9th ed.). Worth Publishers.
- KPMG Nigeria. (2025). *AI and blockchain integration: Implications for IT security in Nigeria's financial sector*.
- Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2022). *Verifying qualitative research findings: Approaches and techniques*. Sage Publications.
- NITDA (National Information Technology Development Agency). (2023). *Blockchain and AI guidelines for enhancing cybersecurity in Nigerian financial institutions*.
- Oduwole, K., & Emecheta, J. (2024). The combined impact of AI and blockchain on IT security in Nigerian banks. *African Journal of IT and Finance*, 20(1), 23–41.
- Olatunji, B., & Ajayi, O. (2025). The role of AI and blockchain in transforming IT security in Nigerian banks. *Journal of Financial Technology and Security*, 15(3), 34–52.
- Olayemi, S. (2024). Barriers to artificial intelligence adoption in Nigerian financial services. *Nigerian Journal of Technology and Policy*, 14(3), 211–227.
- Russell, S., & Norvig, P. (2023). *Artificial intelligence: A modern approach* (4th ed.). Pearson Education.
- Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education.
- Tavakol, M., & Dennick, R. (2021). Making sense of Cronbach's alpha. *International Journal of Medical Education*, 2, 53-55.
- World Bank. (2022). *The digital revolution in Africa: Artificial intelligence and financial inclusion*.