# Cybersecurity and Artificial Intelligence: An Examination of Integration and Challenges of AI in Selected Financial Institutions in Port Harcourt LGA

**Emmanuel Oluwaseun, Amuda**
Email: emmanuel.amuda@rsu.edu.ng
Phone: 08164055371

**Prof. Emmanuel. B, Okemini**
emmanuel.okemini@ust.edu.ng
Phone: 08037088813
Department of Sociology
Rivers state university, Nkpolu-Oroworukwo,
Port Harcourt, Rivers State, Nigeria

https://doi.org/10.56201/ijssmr.vol.12no9.2026.pg217.222

***Abstract***
*The study examined the relationship between Artificial Intelligence (AI) and cybersecurity in selected financial institutions in Port Harcourt Local Government Area, Rivers State, Nigeria. Specifically, it examined the integration of AI into cybersecurity practices, the cybersecurity challenges associated with AI adoption, the effectiveness of AI-driven cybersecurity solutions compared with traditional security measures, and strategies for mitigating the risks arising from the dual-use nature of AI. The study adopted a descriptive survey design. A total of 50 respondents were purposively and proportionately selected from five selected financial institutions, with 10 respondents drawn from each institution. Data were collected through a structured five-point Likert-scale questionnaire administered electronically using Google Forms and analyzed using SPSS version 25 through frequencies, percentages, means, and standard deviations. Findings revealed that AI is widely integrated into cybersecurity practices, particularly for real-time monitoring, threat detection, suspicious-activity identification, and rapid response. However, AI adoption was also associated with increased cybersecurity complexity, data protection concerns, inadequate technical expertise, and emerging vulnerabilities. Respondents perceived AI-driven cybersecurity solutions as faster and more effective than traditional security measures, although they acknowledged that AI introduces new security risks. The study concludes that AI provides significant opportunities for strengthening cybersecurity but requires appropriate governance and oversight. It recommends continuous staff training, regular risk assessments, stronger data protection, hybrid cybersecurity frameworks, enhanced third-party risk management, and closer collaboration between financial institutions and regulatory bodies.*

***Keywords:*** *Artificial Intelligence, Cybersecurity, Financial Institutions, AI-Driven Threat Detection, Emerging Cyber Threats.*

## Introduction

The growing complexity of Artificial Intelligence has provided opportunities to various institutions including, Education, Finance, and Healthcare. On the other hand, the challenges that accompany this development cannot be overlooked as this pose serious threats to these institutions that have integrated it into their systems of operations due to its dual-usage nature.

Notably, TechRadar (2025), explains that, the incorporation of large language models (LLMs) into offensive operations has enabled cyber attackers to independently plan and execute assaults with minimum human participation, posing a substantial threat to traditional security mechanisms. This explains that while AI may enhance cybersecurity by enabling real-time threat detection, it also introduces a paradox: it can be weaponized by cybercriminals to execute more sophisticated attacks, like automated phishing or deepfake scams, which can bypass traditional security measures. The convergence of AI and cybersecurity is particularly important because cybercriminals are increasingly using advanced technologies to improve phishing, social engineering, deepfake impersonation, and other forms of cyber-enabled fraud. At the same time, financial institutions can use AI to analyze large volumes of transaction and security data, identify unusual patterns, detect potential threats, and support faster responses to cyber incidents. This creates a dual relationship in which AI can simultaneously strengthen institutional defenses and introduce new vulnerabilities. The challenge for financial institutions is therefore not simply to adopt AI, but to ensure that its application is supported by appropriate cybersecurity controls, risk management, data protection, human oversight, and regulatory compliance (Aldasoro et al., 2024; International Monetary Fund [IMF], 2026). In Nigeria, these concerns are particularly relevant as financial institutions continue to expand digital financial services and face an evolving cybersecurity environment. Against this background, examining cybersecurity and artificial intelligence in selected financial institutions in Port Harcourt is important for understanding how these institutions are responding to emerging cyber risks while taking advantage of AI-driven technologies. Financial institutions in the city operate within an increasingly digital environment where the protection of customer information, financial transactions, and institutional systems is essential for maintaining trust and operational continuity. The study therefore focuses on the interaction between AI and cybersecurity, particularly the ways AI can improve threat detection and response as well as the vulnerabilities that may arise from its misuse. Understanding this relationship can provide useful evidence for developing more effective cybersecurity strategies and ensuring that financial institutions can benefit from AI without unnecessarily increasing their exposure to emerging cyber threats.

## Statement of the Problem

The increasing digitalization of financial institutions in Port Harcourt, Rivers State, has improved service delivery, operational efficiency, and access to financial services, but it has also increased exposure to cybersecurity threats such as phishing, ransomware, fraud, and data breaches. Although Artificial Intelligence (AI) offers financial institutions opportunities to strengthen cybersecurity through fraud detection, predictive analytics, anomaly detection, and faster threat response, its dual-use nature also enables cybercriminals to develop more sophisticated attacks. Existing studies have established the effects of cybersecurity threats on the financial performance of Nigerian banks and highlighted the benefits and challenges associated with AI adoption (Aderinto & Faforiji, 2025; Aliyu & Iheonkan, 2025; Ayobami, 2025).

Similarly, research has shown that integrating AI-based and conventional cybersecurity measures can improve cyber-threat detection, while AI itself can introduce new security vulnerabilities

(Kovacevic et al., 2024; Parambil, 2024). However, much of the existing literature focuses on the Nigerian financial sector generally, with limited empirical attention to how selected financial institutions in Port Harcourt are using AI to address cybersecurity threats and the challenges associated with such integration. Consequently, there is insufficient context-specific evidence on the effectiveness of AI-driven cybersecurity measures, the risks arising from the malicious use of AI, and the strategies required to manage these challenges within Port Harcourt's financial environment. This knowledge gap provides the basis for the present study, which examines cybersecurity and artificial intelligence in selected financial institutions in Port Harcourt Local Government Area, Rivers State, Nigeria.

## Theoretical Framework

### Technological Determinism Theory

Technological Determinism Theory explains how technological development can drive changes in social structures, institutional practices, organizational behaviour, and human activities. Associated with scholars such as McLuhan (1964) and Smith and Marx (1994), the theory suggests that technological innovations do not merely support existing institutional processes but can fundamentally transform how organizations operate and respond to emerging challenges.

In the context of artificial intelligence (AI) and cybersecurity in financial institutions, the theory is particularly relevant because the increasing adoption of AI is transforming both financial operations and cybersecurity practices. AI technologies such as machine learning, predictive analytics, and automated threat detection enable financial institutions to identify suspicious transactions, detect cyber threats, and respond to security incidents more rapidly. However, the same technological advancement also creates new vulnerabilities, including algorithm manipulation, data poisoning, adversarial attacks, AI-enabled phishing, and automated cyberattacks (Brundage et al., 2018).The key argument of the theory for this study is therefore that technological advancement creates both opportunities and new risks, compelling financial institutions to continuously adapt their cybersecurity systems, organizational structures, employee competencies, and security policies. As AI-driven cyber threats become more sophisticated, traditional reactive cybersecurity approaches may become inadequate, requiring institutions to adopt intelligent, predictive, and automated security mechanisms. Thus, technological determinism provides a useful theoretical foundation for examining how the adoption of AI is reshaping cybersecurity practices and creating new forms of cyber risk within financial institutions in Port Harcourt.

## Methodology

The study adopted a descriptive survey design to examine the influence of Artificial Intelligence (AI) on cybersecurity in selected financial institutions in Port Harcourt City Local Government Area, Rivers State, Nigeria. The study population comprised employees of selected financial institutions, with respondents drawn from relevant IT, cybersecurity, operations, and digital banking functions. A purposive and quota sampling technique was employed to select participants with relevant knowledge and experience of AI and cybersecurity. A total of 50 respondents were selected from five financial institutions, with an equal quota of 10 respondents allocated to each institution. Primary data were collected using a structured questionnaire comprising demographic questions and five-point Likert-scale items aligned with the study objectives. The questionnaire was administered electronically through Google Forms and retrieved from the respondents. The

instrument was validated by the researcher's supervisor and a departmental expert, while a pilot study was conducted to assess its reliability.

Data were coded and analyzed using SPSS version 25. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were used to summarize respondents' characteristics and examine patterns in their responses. Results were presented using tables and charts to facilitate interpretation.

**Findings**

The findings indicate that Artificial Intelligence (AI) is significantly integrated into cybersecurity practices within the selected financial institutions in Port Harcourt. All respondents (100%) reported that their institutions use AI-based systems for cyber-threat detection and prevention, real-time security monitoring, suspicious-activity identification, and improved threat-detection speed and accuracy. Respondents also unanimously agreed that AI adoption has improved overall cybersecurity effectiveness. However, AI adoption has introduced notable challenges. Ninety percent of respondents reported increased cybersecurity complexity, while 90% acknowledged challenges in protecting sensitive customer data associated with the volume of data required for AI systems. Furthermore, 95% identified inadequate technical expertise as a major challenge. Although 66% disagreed that their AI systems were vulnerable to model manipulation, data poisoning, or adversarial attacks, 86% considered existing cybersecurity policies and regulatory frameworks inadequate for addressing AI-related risks. The findings further show that AI-driven cybersecurity solutions were perceived as more effective than traditional approaches: 92% agreed that AI improves threat detection, while 100% reported faster detection and response. Nevertheless, 94% recognized that AI introduces new vulnerabilities. Respondents strongly supported governance, regular risk assessments, continuous staff training, integration of AI with traditional security measures, and stronger regulatory collaboration as key mitigation strategies.

Overall, the findings demonstrate that AI offers substantial cybersecurity benefits while simultaneously creating emerging risks that require stronger technical capacity, governance, and regulatory oversight.

**Discussion of Findings**

The findings demonstrate that AI has become an important component of cybersecurity in selected financial institutions in Port Harcourt. Regarding the first objective, all respondents indicated that AI is integrated into cybersecurity frameworks for real-time monitoring, threat detection, and identification of suspicious activities. This finding is consistent with Accenture (2025), which reported that financial institutions are increasingly adopting AI-driven solutions to modernize infrastructure and strengthen operational capabilities.

The second objective revealed that AI adoption also increases cybersecurity complexity, particularly in protecting sensitive customer data and managing AI-enabled systems. This finding is supported by TechRadar (2025), which noted that the use of large language models in offensive cyber operations enables attackers to plan and execute sophisticated attacks with reduced human intervention, challenging conventional defence mechanisms.

For the third objective, respondents perceived AI-driven cybersecurity solutions as more effective and faster than traditional security measures in detecting and responding to cyber threats. However, the findings also indicate that AI introduces new vulnerabilities, suggesting that technological advancement does not eliminate cybersecurity risks. This aligns with Parambil (2024), who found

that combining AI-based and conventional cybersecurity approaches provides more comprehensive protection against evolving threats.
Regarding the fourth objective, respondents emphasized strict AI governance, regular risk assessments and audits, continuous staff training, data encryption and tokenization, stronger third-party risk management, and expanded cybersecurity teams. Collectively, these findings suggest that effective AI cybersecurity requires a balanced approach combining technological innovation, human expertise, institutional governance, and regulatory oversight.

**Conclusion**

The study concludes that Artificial Intelligence (AI) has become an important component of cybersecurity in selected financial institutions in Port Harcourt, particularly through real-time monitoring, threat detection, and rapid response to cyber incidents. However, AI adoption also introduces challenges, including increased system complexity, data protection concerns, and emerging security vulnerabilities. The findings further indicate that AI-driven cybersecurity solutions are generally more effective and faster than traditional measures, but their effectiveness is enhanced when combined with conventional cybersecurity approaches. To address the dual-use risks of AI, financial institutions should strengthen AI governance and oversight, conduct regular risk assessments and security audits, provide continuous staff training, enhance data protection, strengthen third-party risk management, and expand in-house cybersecurity capacity. Overall, the study concludes that financial institutions should adopt a balanced, strategic, and well-regulated approach to AI implementation to maximize its cybersecurity benefits while minimizing associated risks.

**Recommendations**

**1** Financial institution should enhance the integration of AI-based cybersecurity systems by consistently upgrading their technologies to facilitate real-time monitoring and a swift response to emergent cyber threats.
**2** In order to establish a more comprehensive and multilayered defense against cyber-attacks, banks should implement a hybrid cybersecurity framework that integrates AI-driven security systems with conventional cybersecurity tools.
**3** Banks should invest in continuous staff training and capacity building to improve employees' knowledge and competence in managing AI-powered cybersecurity systems and responding effectively to cyber threats.
**4** Financial institutions should strengthen data protection mechanisms by implementing advanced encryption, tokenization, and secure data management practices to safeguard sensitive customer information used in AI systems.
**5** Financial institutions should enhance third-party and vendor risk management practices to ensure that external technology providers and service partners comply with established cybersecurity and AI governance standards.
**6** Regulatory bodies and financial institutions should collaborate more closely to develop standardized policies and frameworks that guide the safe adoption of AI technologies in the financial sector while minimizing cybersecurity risks.

**References**

Accenture. (2025, January 7). *Top 10 banking trends in 2025 and beyond*. Accenture.

Aderinto, A. A., & Faforiji, A. C. (2025). Cybersecurity threats and financial performance of listed commercial banks in Nigeria. *Asian Journal of Advanced Research and Reports, 19*(4), 381–394.

Aliyu, I., & Iheonkan, I. S. (2025). Impact of artificial intelligence on financial services in Nigeria. *Journal of Accounting and Financial Management, 11*(3), 158–171.

Ayobami, T. (2025). *Cybersecurity challenges in Nigeria's financial sector*. ResearchGate.

Brundage, M., Avin, S., Clark, J., et al. (2018). The malicious use of artificial intelligence. *AI Journal, 5*(2), 1–25.

Kovacevic, A., Radenkovic, S. D., & Nikolic, D. (2024). *AI and cybersecurity in banking*. arXiv.

McLuhan, M. (1964). *Understanding media*. McGraw-Hill.

Parambil, M. M. (2024). *Integrating AI-based cybersecurity methods*.

Smith, M. R., & Marx, L. (1994). *Does technology drive history?* MIT Press.

TechRadar. (2025). *AI LLMs and cyberattacks*.