IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13301

AI-Driven Data Security for Remote Work in Financial Institutions: A Phenomenological Study

Temitope Awodiji Owoyemi

School of Computer and Information Sciences, University of the Cumberlands, Williamsburg, KY, USA

Abstract: The proliferation of remote work across U.S. financial institutions has created an expanded cybersecurity threat surface, exposing sensitive financial data to sophisticated attack vectors. This study examines how AI-driven technologies enhance data security protocols within remote financial work environments, drawing on the lived experiences of cybersecurity specialists and IT managers. Using a qualitative phenomenological design, semi-structured interviews were conducted with 12 senior cybersecurity and IT professionals across U.S. financial institutions. Data were analyzed using Braun and Clarke's six-phase thematic analysis framework in NVivo. Five interconnected themes emerged: AI as a catalyst for data security; cybersecurity leaders' perceptions of AI; drivers and barriers to AI adoption; AI-enabled Zero Trust identity and access controls; and compliance and ethics in AI security. Findings demonstrate that AI-powered tools-including machine learning-based anomaly detection, behavioral analytics, and automated incident response-substantially strengthen threat detection and compliance monitoring in remote environments. Participants consistently characterized AI as an augmenter of human expertise rather than a replacement, expressing concern over algorithmic opacity, integration costs, and regulatory complexity. The study provides empirical evidence on the theory-practice intersection of AI adoption in financial cybersecurity, offering practical recommendations for governance, explainability, and workforce capability development.

Keywords: Artificial Intelligence; Cybersecurity; Remote Work; Financial Institutions; Zero Trust Architecture; Phenomenological Research; Machine Learning

I. INTRODUCTION

The U.S. financial industry has undergone a radical transformation driven by widespread technology adoption and the rise of remote work. The COVID-19 pandemic accelerated this shift, compelling financial institutions to rapidly expand their digital infrastructure to support decentralized workforces. According to the U.S. Bureau of Labor Statistics [1], more than 25% of financial and insurance employees worked remotely in 2021 and subsequent years, a sharp increase from the pre-pandemic era. Although this transformation has created new productivity and workforce flexibility, it has also heightened cybersecurity risks and exposed sensitive financial data to novel threat vectors.

Banks and financial institutions remain primary targets for cyberattacks due to the value of the data they hold. Remote access networks, personal endpoints, and cloud resources have exposed vulnerabilities that traditional security models have proven inadequate to address. Temitope and Owoyemi [31] identify virtual desktop infrastructure and secure remote access technologies as foundational to establishing a defensible security perimeter for distributed financial workforces. Bello et al. [2] and Bello et al. [3] observe that integrating machine learning and AI into fraud detection and cybersecurity architecture has become imperative for institutions seeking to maintain resilience in distributed environments.

Artificial intelligence has emerged as a transformative enabler in this context. AI-powered solutions-including machine learning-based anomaly detection, behavioral analytics, and automated incident response-offer capabilities that far exceed the scale of manual monitoring. Cao [4] argues that AI's role in financial security continues to evolve, offering predictive analytics for anomaly detection, streamlining security monitoring, and reducing operational costs. Awodiji et al. [27] further demonstrate that harnessing predictive analytics proactively can intercept cyber threats before they materialize, offering a strategic advantage over reactive incident response. Despite the promise of AI, significant challenges remain, such as algorithmic opacity, integration complexity, regulatory uncertainty, and ethical concerns over data privacy and employee surveillance, which have tempered widespread adoption [5][6].

This paper presents findings from a qualitative phenomenological study examining how cybersecurity specialists and IT managers in U.S. financial institutions experience and perceive AI-driven data security in remote work environments. Guided by five research questions (RQs), the study sought to uncover how AI-powered security solutions are

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13301

transforming the security landscape of remote financial services, what factors influence their adoption, how they interact with Zero Trust architectures, and what compliance and ethical considerations shape their deployment.

The remainder of this paper is organized as follows: Section II reviews the relevant literature; Section III describes the research methodology; Section IV presents the findings and discussion; Section V concludes with implications and recommendations.

II. LITERATURE REVIEW

A. AI-Driven Cybersecurity in Financial Institutions

The financial sector's adoption of AI in cybersecurity represents one of the most significant technological developments of the past decade. Mishra et al. [7] provide a comprehensive review of AI applications in cybersecurity, noting that machine learning algorithms have substantially improved threat detection accuracy while reducing false positive rates. Bello et al. [2] demonstrate that integrating machine learning and AI into financial cybersecurity frameworks enables more robust fraud detection and threat response, particularly in distributed operational contexts. Similarly, Rizvi [8] highlights how AI-enhanced threat intelligence improves incident response times and overall security posture.

The transition to remote work has intensified the need for adaptive security solutions. Hassan et al. [9] identify remote access vulnerabilities, personal device risks, and cloud configuration weaknesses as leading attack vectors in distributed financial environments. Ajayi et al. [10] specifically examine AI-driven anomaly detection for insider threat identification in banking, demonstrating that behavioral analytics can surface risks that conventional rule-based systems miss entirely [28]. These findings underscore the operational value of AI in managing the expanded threat surface created by remote work. Emerging attack vectors, including deep-fake-based social engineering and identity spoofing, further compound the threat landscape, making AI-powered detection capabilities increasingly indispensable [29]. The security of financial databases and backend systems has received growing scholarly attention as dynamic IT environments continuously expand the vulnerability surface [26].

B. Zero Trust Architecture and AI Integration

Zero Trust Security, encapsulated by the principle of 'never trust, always verify,' has emerged as a foundational paradigm for securing distributed environments. Paul et al. [11] describe the synergy between AI and Zero Trust as a convergence that enables dynamic, context-aware risk assessments rather than static perimeter-based controls. Buckley et al. [12] emphasize that AI-enhanced Zero Trust models can significantly reduce the risks of credential compromise and lateral movement by continuously evaluating user and device behavior against risk profiles.

Srivastava et al. [13] conducted a survey of AI (XAI) applications in cybersecurity, noting that transparency in AI decision-making is a prerequisite for effective Zero Trust implementation, as security teams need to interpret AI-generated risk scores to make informed access decisions. This intersection of explainability and access control represents a critical research gap that practitioners are actively navigating.

C. Regulatory and Ethical Dimensions

Financial institutions operate within a complex regulatory environment that shapes AI adoption. Cortez and Dekker [6] analyze cybersecurity risk disclosure requirements and note that regulatory frameworks, such as the FFIEC guidelines and NYDFS cybersecurity regulations, increasingly require AI-enabled controls. Buckley et al. [12] observe that regulatory uncertainty, particularly around algorithmic accountability and cross-border data transfers, has constrained more aggressive AI deployment.

Cheng et al. [14] examine the ethical dimensions of AI, identifying concerns around algorithmic bias, surveillance overreach, and data minimization as central to responsible deployment. Bahangulu and Owusu-Berko [5] specifically address governance frameworks for AI in analytics, arguing that bias audits, fairness assessments, and ethics impact evaluations should be institutionalized alongside technical deployments.

D. Theoretical Framework

The study draws on two complementary theoretical frameworks. Socio-Technical Systems (STS) Theory, originating with the Tavistock Institute in the 1950s, posits that maximum organizational performance occurs when social (human, cultural, procedural) and technical subsystems are jointly optimized [15]. Applied to AI-driven cybersecurity, STS theory frames the integration of AI tools as inherently dependent on the people who use, interpret, and govern them, not as a standalone technical solution. General Systems Theory (GST) complements STS by providing a holistic lens for

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13301

understanding how AI-based cybersecurity mechanisms interact within broader organizational ecosystems, particularly when employees operate remotely [16].

Together, these frameworks support examining AI adoption not as a purely technical problem but as a socio-organizational challenge that requires alignment among human expertise, institutional culture, and technological capability.

III. METHODOLOGY

A. Research Design

The study employed a qualitative phenomenological design to capture the lived experiences and professional perspectives of cybersecurity and IT practitioners in the financial sector. Phenomenological inquiry is appropriate when the research aim is to understand how individuals experience a specific phenomenon [17], in this case, the deployment and governance of AI-driven security in remote work environments. This design enabled the researcher to move beyond surface-level descriptions to uncover the meanings, perceptions, and contextual factors shaping practitioner experience.

Five research questions guided the study: RQ1 examined how AI-driven technologies enhance data security in remote work; RQ2 explored practitioner perspectives on AI's effectiveness and limitations; RQ3 investigated factors influencing AI adoption; RQ4 probed the integration of AI with Zero Trust frameworks; and RQ5 examined compliance and ethical challenges in AI deployment.

B. Participants and Sampling

Twelve senior cybersecurity and IT professionals from U.S. financial institutions were recruited using purposeful and snowball sampling strategies. Palinkas et al. [18] note that purposeful sampling is particularly suited to phenomenological inquiry as it enables the selection of participants with direct, relevant experience. Participants included three Cybersecurity Analysts, two Information Security Managers, two AI Implementation Specialists, two Compliance and Risk Officers, two Technology Consultants, and one Chief Information Security Officer (CISO). Institutions represented included regional banks, global financial services firms, insurance companies, and investment management organizations.

Data saturation was achieved at the twelfth interview, as subsequent interviews produced no substantively new codes or themes. This is consistent with Guest et al.'s [19] empirical finding that saturation typically occurs between 9 and 12 interviews in homogeneous purposeful samples.

C. Data Collection

Semi-structured interviews, averaging 55 minutes, were conducted virtually via Zoom. An interview protocol of open-ended questions was developed based on the theoretical framework and research questions, then validated through expert review by three faculty members with expertise in cybersecurity and qualitative methods. A field test with two proxy participants confirmed clarity and appropriate duration. Interviews were audio-recorded with participant consent and transcribed verbatim for analysis.

D. Data Analysis

Data were analyzed using Braun and Clarke's [20] six-phase thematic analysis framework: (1) data familiarization, (2) initial code generation, (3) theme searching, (4) theme review, (5) theme definition and naming, and (6) report production. Analysis was conducted using NVivo qualitative software, which facilitated systematic coding and pattern identification across the interview corpus. Both inductive and deductive approaches were employed: inductive codes emerged from the data, while deductive codes were aligned with the five research questions.

E. Trustworthiness

Trustworthiness was ensured through four criteria outlined by Lincoln and Guba [21]. Credibility was established via prolonged engagement, triangulation across participant accounts and existing literature, and member checking with three participants. Dependability was supported by a comprehensive audit trail documenting methodological decisions. Transferability was addressed through rich, thick descriptions of participants, settings, and contexts. Confirmability was maintained through reflexivity practices, including bracketing of researcher assumptions before and throughout data collection.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13301

IV. FINDINGS AND DISCUSSION

Thematic analysis of 12 participant interviews yielded five overarching themes, each comprising interrelated sub-themes. Together, these themes illuminate the multi-dimensional nature of AI-driven security in remote financial work environments.

A. Theme 1: AI as a Catalyst for Data Security

The most pervasive theme across all 12 interviews was AI's transformative role in strengthening data security in distributed environments. Participants described three principal mechanisms through which AI delivered security value.

Sub-theme 1.1 - Augmenting Threat Detection and Response: AI-powered tools enabled real-time monitoring of vast datasets and identified subtle anomalies that traditional rule-based systems could not detect. One participant described:

> *"CrowdStrike's AI is constantly learning from global data streams. It can recognize when something is off, such as a strange login time or a type of malware not seen before. That is something we could not do manually."*

Another added:

> *"AI lets us move from reactive to proactive. Before, we only knew there was a problem after someone reported it. Now, AI is often the first to alert us."*

These perspectives align with Broadbent [22], who characterizes AI as a force multiplier in cybersecurity, and Dietz et al. [23], who caution that without adequate human oversight, AI systems can amplify false positives and undermine confidence in automated alerts.

Sub-theme 1.2 - Behavioral Analytics for Insider Threats: Remote work has blurred traditional boundaries of accountability, making insider threats more difficult to detect manually. Participants described AI-based behavioral analytics as indispensable for identifying anomalous behavior patterns indicative of data exfiltration or policy violation.

Sub-theme 1.3 - Automating Compliance Checks: In distributed environments, AI automates enforcement of data handling policies, monitors for violations in real time, and reduces reliance on human vigilance. As one participant noted:

> *"Our email gateways use AI to scan for sensitive information. If someone accidentally sends out client data, the system flags or blocks it before it leaves the network."*

TABLE I. SUMMARY OF THEME 1 INSIGHTS

Theme Aspect	Participant Perspective	Literature Support
Threat Detection	AI enables proactive real-time detection of novel threats	Broadbent [22]; Dietz et al. [23]
Insider Threats	Behavioral analytics uncovers hidden risk patterns	Ajayi et al. [10]
Compliance	AI enforces policy dynamically, reduces violations	Cortez & Dekker [6]

B. Theme 2: Practitioner Perceptions - Augmentation, not Replacement

A consistent and strongly held view across all participants was that AI functions as an augmentation technology-amplifying human capacity-rather than as a replacement for professional judgment. As one participant remarked:

> *"AI helps us analyze behaviors at scale. It can identify subtle deviations from normal patterns much faster than any team could, but the final call on what constitutes a real threat still needs a human."*

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13301

Participants simultaneously expressed significant concern about the 'black box' nature of many AI models. The inability to explain or audit AI-generated security decisions creates barriers to regulatory compliance and undermines organizational trust in AI outputs. This finding is consistent with Srivastava et al.'s [13] call for explainable AI (XAI) as an essential dimension of responsible cybersecurity deployment.

A third sub-theme revealed that practitioners approach AI adoption with cautious optimism: they value its capabilities but remain skeptical of vendor claims and are acutely aware of organizational barriers to effective implementation, including skills gaps, change resistance, and governance immaturity.

C. Theme 3: Drivers and Barriers to AI Adoption

Participants identified a dynamic interplay between adoption drivers and constraints. Primary drivers included scalability, efficiency, and pattern recognition capabilities beyond human capacity. One participant captured the efficiency imperative:

> *"AI enabled us to analyze millions of events in real time, something impossible to achieve manually. In a remote environment where endpoints are distributed globally, this scalability is crucial."*

The primary barriers to AI adoption were: (1) explainability deficits that complicate regulatory justification; (2) high implementation and integration costs, particularly for legacy system modernization; (3) regulatory uncertainty around AI-driven decision-making in high-stakes financial contexts; and (4) internal resistance driven by fear of job displacement and insufficient technical training.

A notable organizational preference also emerged: participants from institutions handling highly sensitive or proprietary data strongly preferred internally developed AI solutions over third-party platforms, reflecting concerns about data sovereignty and vendor risk.

D. Theme 4: AI-Enabled Zero Trust Architecture

All participants positioned Zero Trust as foundational to their organization's remote security strategy. The principle of 'never trust, always verify' was described as particularly essential in environments where physical oversight of employees is absent. One participant summarized:

> *"Zero Trust is central to how we think about security. Every access request is treated as potentially hostile- we verify identity, device health, and context before granting any access."*

AI substantially enhances Zero Trust implementation by enabling dynamic, context-aware risk assessment that moves beyond binary access decisions. Rather than granting or denying access based on static rules, AI-powered Zero Trust systems continuously evaluate behavioral signals, device posture, and contextual risk factors to adjust access privileges in real time.

Participants noted that AI-Zero Trust integration remained in early or intermediate stages at most institutions, constrained by integration complexity and the need for substantial security infrastructure investment. This finding aligns with Paul et al. [11], who describe AI-augmented Zero Trust as a next-generation framework requiring a phased implementation, supported by rigorous piloting and an organizational readiness assessment.

E. Theme 5: Compliance, Ethics, and Data Sovereignty

The fifth theme revealed the compliance and ethical terrain practitioners must navigate when deploying AI security solutions. Participants from multinational institutions highlighted the challenge of regulatory fragmentation across jurisdictions:

> *"We operate in over 90 countries, and the privacy laws in Germany are much stricter than in Brazil. Any AI model or security measure has to account for those differences before we can roll it out globally."*

Governance and oversight emerged as equally critical. Participants described the need for AI Oversight Councils, Model Risk Management (MRM) processes, and ethics impact assessments to ensure that AI systems operate within sanctioned boundaries. Bahangulu and Owusu-Berko [5] and Cheng et al. [14] provide theoretical grounding for these practices, emphasizing that algorithmic fairness, bias audits, and human oversight mechanisms must be institutionalized alongside technical deployments.

DOI: 10.17148/IARJSET.2026.13301

Data sovereignty and privacy emerged as distinct tensions: AI-based insider threat monitoring requires access to employee behavioral data, raising concerns about surveillance overreach and compliance with data minimization principles under frameworks such as the GDPR and the CCPA. Participants consistently described this as a live governance challenge that requires ongoing dialogue among security, legal, and HR leadership.

V. CONCLUSION

This study contributes empirical evidence to the growing body of knowledge on AI-driven cybersecurity in financial institutions, specifically in the context of remote work environments. Through the lived experiences of 12 senior cybersecurity and IT professionals, five interconnected themes illuminate both the transformative potential and the practical limitations of AI as a security enabler.

The findings confirm that AI substantially enhances threat detection, insider risk management, and compliance enforcement in distributed financial environments-capabilities that are operationally indispensable given the scale and complexity of remote work. At the same time, the study highlights important constraints: algorithmic opacity undermines trust and regulatory compliance; integration costs and legacy system complexity impede adoption; and data privacy tensions require careful governance.

The consistently expressed view of AI as an augmenter rather than a replacement for human expertise has significant implications for workforce strategy. Organizations must invest not only in AI tools but in the human capability to interpret, challenge, and govern AI outputs. Explainable AI (XAI) frameworks, AI literacy training, and structured governance mechanisms-including AI Oversight Councils and Model Risk Management processes-are essential complements to technical investment.

Three strategic recommendations emerge from the findings. First, organizations should prioritize XAI-capable solutions that produce interpretable outputs for security analysts, auditors, and regulators. Second, governance frameworks for AI in cybersecurity should be formalized and institutionalized, with diverse representation across technical, legal, ethical, and operational functions. Third, AI-enabled Zero Trust architectures should be implemented through phased approaches, with realistic expectations grounded in organizational readiness assessments and pilot program evidence.

Future research should examine AI adoption experiences across smaller and community-level financial institutions, which face different resource constraints and regulatory environments than the large institutions represented in this study. Longitudinal research tracking outcomes as AI security capabilities mature would also advance understanding of the evolving practice landscape. Additionally, adversarial attacks targeting generative AI systems represent an emerging frontier that warrants dedicated investigation, as these threats may undermine the integrity of AI-driven security tools themselves [30].

ACKNOWLEDGMENT

The author wishes to thank the 12 cybersecurity and IT professionals who generously contributed their time and expertise to this study. Gratitude is also extended to the dissertation committee - Dr. Alexandre Lazo (Chair), Dr. William Souza, and Dr. Segun Odion - for their exceptional guidance throughout the doctoral journey at the University of the Cumberlands.

REFERENCES

[1]. U.S. Bureau of Labor Statistics, "American Time Use Survey - 2021 Results," U.S. Department of Labor, 2022. [Online]. Available: https://www.bls.gov/news.release/atus.nr0.htm

[2]. O. A. Bello, A. Folorunso, J. Onwuchekwa, and O. E. Ejiofor, "A comprehensive framework for strengthening USA financial cybersecurity: Integrating machine learning and AI in fraud detection systems," European Journal of Computer Science and Information Technology, vol. 11, no. 6, pp. 62–83, 2023.

[3]. O. A. Bello, A. Ogundipe, D. Mohammed, F. Adebola, and O. A. Alonge, "AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities," European Journal of Computer Science and Information Technology, vol. 11, no. 6, pp. 84–102, 2023.

[4]. L. Cao, "AI in finance: Challenges, techniques, and opportunities," ACM Computing Surveys, vol. 55, no. 3, pp. 1–38, 2022.

DOI: 10.17148/IARJSET.2026.13301

[5]. J. K. Bahangulu and L. Owusu-Berko, "Algorithmic bias, data ethics, and governance: Ensuring fairness, transparency, and compliance in AI-powered business analytics," World Journal of Advanced Research and Review, vol. 25, no. 2, pp. 1746–1763, 2025.
[6]. E. K. Cortez and M. Dekker, "A corporate governance approach to cybersecurity risk disclosure," European Journal of Risk Regulation, vol. 13, no. 3, pp. 443–463, 2022.
[7]. S. Mishra, S. Singh, and A. Sharma, "Artificial intelligence in cyber security: A comprehensive review," Journal of Information Security, vol. 13, no. 1, pp. 25–50, 2022.
[8]. M. Rizvi, "Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention," International Journal of Advanced Engineering Research and Science, vol. 10, no. 05, 2023.
[9]. A. O. Hassan, S. K. Ewuga, A. A. Abdul, T. O. Abrahams, M. Oladeinde, and S. O. Dawodu, "Cybersecurity in banking: A global perspective with a focus on Nigerian practices," Computer Science & IT Research Journal, vol. 5, no. 1, pp. 41–59, 2024.
[10]. A. M. Ajayi, A. O. Omokanye, O. Olowu, A. O. Adeleye, O. M. Omole, and I. U. Wada, "Detecting insider threats in banking using AI-driven anomaly detection," International Journal of Cybersecurity Research, vol. 2, no. 3, pp. 190–223, 2024.
[11]. E. M. Paul, U. Mmaduekwe, J. D. Kessie, and M. Dolapo, "Zero trust architecture and AI: A synergistic approach to next-generation cybersecurity frameworks," International Journal of Science and Research Archive, vol. 13, no. 2, pp. 4159–4169, 2024.
[12]. R. P. Buckley, D. A. Zetzsche, D. W. Arner, and B. W. Tang, "Regulating artificial intelligence in finance: Putting the human in the loop," The Sydney Law Review, vol. 43, no. 1, pp. 43–81, 2021.
[13]. G. Srivastava et al., "XAI for cybersecurity: State-of-the-art, challenges, open issues, and future directions," arXiv Preprint arXiv:2206.03585, 2022.
[14]. L. Cheng, K. R. Varshney, and H. Liu, "Socially responsible AI algorithms: Issues, purposes, and challenges," Journal of Artificial Intelligence Research, vol. 71, pp. 1137–1181, 2021.
[15]. M. Sony and S. Naik, "Industry 4.0 integration with socio-technical systems theory: A systematic review and proposed theoretical model," Technology in Society, vol. 61, 101248, 2020.
[16]. D. L. Morgan and A. Nica, "Iterative thematic inquiry: A new method for analyzing qualitative data," International Journal of Qualitative Methods, vol. 19, 2020.
[17]. J. W. Creswell and C. N. Poth, Qualitative Inquiry and Research Design: Choosing Among Five Approaches, 4th ed. SAGE Publications, 2018.
[18]. L. A. Palinkas et al., "Purposeful sampling for qualitative data collection and analysis in mixed method implementation research," Administration and Policy in Mental Health, vol. 42, no. 5, pp. 533–544, 2015.
[19]. G. Guest, A. Bunce, and L. Johnson, "How many interviews are enough? An experiment with data saturation and variability," Field Methods, vol. 18, no. 1, pp. 59–82, 2006.
[20]. V. Braun and V. Clarke, "Using thematic analysis in psychology," Qualitative Research in Psychology, vol. 3, no. 2, pp. 77–101, 2006.
[21]. Y. S. Lincoln and E. G. Guba, Naturalistic Inquiry. SAGE Publications, 1985.
[22]. M. Broadbent, "What is Ahead for a Cooperative Regulatory Agenda on Artificial Intelligence?" Center for Strategic and International Studies, 2021.
[23]. K. Dietz et al., "The missing link in network intrusion detection: Taking AI/ML research efforts to users," IEEE Access, 2024.
[24]. J. A. Smith, P. Flowers, and M. Larkin, Interpretative Phenomenological Analysis: Theory, Method and Research. SAGE Publications, 2009.
[25]. T. O. Awodiji and K. Y. Williamsburg, "Malicious malware detection using machine learning perspectives," Journal of Information Engineering and Applications, vol. 12, no. 2, pp. 10–17, 2022.
[26]. T. O. Awodiji, "Database security in a dynamic IT world," AIRCC Conference Proceedings, vol. 11, no. 16, pp. 151-161, 2021.
[27]. T. O. Awodiji, F. Ayoola, J. Owoyemi, and A. Tosin-Amos, "Stop cyber-attacks before they happen: Harnessing the power of predictive analytics in cybersecurity," 2023.
[28]. T. O. Awodiji, J. Owoyemi, and O. Edeamah, "Exploring techniques and applications for anomaly detection in time series data," International Advanced Research Journal in Science, Engineering and Technology, 2023.
[29]. T. O. Awodiji and J. Owoyemi, "Advanced detection and mitigation techniques for deepfake video: Leveraging AI to safeguard visual media integrity in cybersecurity," 2024.
[30]. T. O. Awodiji and J. Owen, "Developing a deep learning framework for detecting and mitigating adversarial attacks on generative AI systems in cybersecurity applications," 2025.
[31]. T. O. Awodiji and J. Owoyemi, "Revolutionizing remote work: The importance of virtual desktops and secure remote access," University of the Cumberlands, 2025.

