JCBD
JOURNAL OF COMPUTERS AND DIGITAL BUSINESS
Volume 4, Number 2, May 2025, pp. 56-63
Homepage: https://jurnal.delitekno.co.id/index.php/jcbd

Banking Cybersecurity: Safeguarding Financial Information in the Digital Era

Hewa Majeed Zangana[1*], Harman Salih Mohammed [2], Mamo Muhamad Husain [3]

[1] *Duhok Polytechnic University, Duhok, Iraq*
[2] *Ararat Technical Private Institute, Kurdistan Region - Iraq*
[3] *IT Dept., Duhok Technical College, Duhok Polytechnic University, Duhok, Iraq*

* hewa.zangana@dpu.edu.krd

https://doi.org/10.56427/jcbd.v4i2.751

ARTICLE INFO

Article History
Received: January 27, 2025
Revised: April 11, 2025
Accepted: May 13, 2025

Keywords
Artificial Intelligence
Banking
Blockchain
Cybersecurity
Encryption

ABSTRACT

This study explores the escalating cybersecurity challenges in the banking sector and the potential of large language models (LLMs) to enhance digital defense mechanisms. Employing a qualitative methodology that includes a systematic literature review, expert interviews, and case study evaluations, the research investigates the integration of LLMs in cybersecurity operations such as threat detection, automated incident response, and user authentication. The findings reveal that LLMs offer significant advantages in real-time anomaly detection, predictive analytics, and natural language-based security training. However, their adoption is hindered by concerns over algorithmic transparency, data privacy, and the need for specialized technical expertise within financial institutions. A key contribution of this work is the development of an integrated cybersecurity framework that combines AI-driven technologies, blockchain-based transaction security, digital forensic tools, and human-centered security practices. The proposed framework aims to guide financial institutions in implementing adaptive, intelligent cybersecurity strategies aligned with evolving global regulatory standards. This research offers both theoretical insights and practical recommendations for enhancing cyber resilience in digital banking environments. It emphasizes the importance of a multidimensional approach that addresses technical innovation, organizational preparedness, and regulatory compliance. Future studies are encouraged to validate the proposed framework through empirical testing across diverse banking infrastructures.

1. Introduction

The advent of digital banking has revolutionized the financial industry, enabling seamless transactions, enhanced customer experiences, and global connectivity. However, this digital transformation has brought an exponential rise in cybersecurity threats, posing significant risks to financial institutions and their customers [1]. As banking becomes increasingly reliant on digital technologies, safeguarding sensitive financial information has become a top priority for ensuring data privacy and system integrity [2].

Cybercriminals exploit vulnerabilities in digital banking platforms through phishing attacks, ransomware, and sophisticated hacking methods, highlighting the urgent need for advanced cybersecurity measures [3]. Effective strategies such as real-time threat detection, robust encryption protocols, and leveraging artificial intelligence (AI) have been emphasized to counter these evolving threats [4]. AI-enhanced solutions play a critical role in identifying anomalies, detecting potential attacks, and automating defensive responses, thus providing a proactive approach to cybersecurity [5], [6].

Regulatory compliance is another vital aspect, with governments and organizations implementing strict policies to secure financial systems. For instance, the integration of large language models (LLMs) and quantum

computing is explored as an emerging frontier in bolstering cybersecurity infrastructure [7]. However, the human factor remains a persistent challenge, as insider threats and human errors continue to compromise security protocols [8].

This paper examines the dynamic interplay of advanced technologies, regulatory frameworks, and human factors in securing financial information. By analyzing case studies and global best practices, this study aims to provide actionable insights for banks and financial institutions to enhance their cybersecurity posture. Ultimately, the findings underscore the importance of a multidimensional approach that combines technical, organizational, and human-centric strategies [9], [10].

Given the increasing complexity and scale of cyber threats, there is a pressing need for intelligent systems that can offer real-time analysis, prediction, and response. This paper aims to explore how large language models can be effectively leveraged to enhance cybersecurity measures within the banking sector. The objective is to analyze current applications, identify potential benefits and limitations, and propose a framework for future implementation of LLMs in banking cybersecurity strategies.

The increasing integration of artificial intelligence (AI), blockchain, and large language models (LLMs) into cybersecurity highlights a paradigm shift in safeguarding financial and digital infrastructures. [1] underscore the transformative potential of cyber AI in redefining security measures to address complex threats. Complementing this perspective, [7] explore how leveraging LLMs for quantum-aware cybersecurity can provide robust solutions for emerging challenges in digital environments.

1.1 Cybersecurity in Financial and Banking Sectors

The financial sector remains one of the most targeted industries for cyberattacks, necessitating a multifaceted approach to data protection and risk mitigation. Recent works by [11], [12] emphasize that implementing robust cybersecurity strategies is imperative for preventing financial fraud and protecting customer data in the United States banking sector. Similarly, [10] examine data privacy and cybersecurity challenges arising from the sector's digital transformation, proposing advanced encryption methods and AI-powered analytics as key safeguards. In the context of fintech, [13], [14] advocate for integrating machine learning models to predict and mitigate vulnerabilities in financial transactions.

Also [15] provide a global perspective, analyzing banking cybersecurity practices with a specific focus on Nigeria. Their findings highlight the need for country-specific strategies, which align with earlier studies by [3] on risk assessment methodologies and best practices for managing cyber threats in banking. Additionally, [16] discuss how cybersecurity systems play a crucial role in managing risks in the financial and banking sectors, advocating for stronger regulatory frameworks.

1.2 AI, Blockchain, and Emerging Technologies

AI has become an essential tool for detecting and mitigating cyber threats, as evidenced by works such as [5], which examines AI-enhanced threat detection in digital banking. Similarly, [4] demonstrates how combining AI with blockchain and business intelligence can revolutionize banking security. This integration is further explored by [6], who highlight AI's role in forensic practices for identifying malicious activities in digital ecosystems.

Also [9] argue that digital transformation in financial services requires strategic growth fueled by AI, cybersecurity, and robust data protection practices. In this context, [17] investigate fintech disruptions and the necessity of safeguarding data security in rapidly evolving digital environments. These findings align with [18], who review accounting and cybersecurity controls to ensure data confidentiality and integrity in financial organizations.

1.3 Human and Organizational Factors in Cybersecurity

Cybersecurity is not merely a technological challenge but also a human-centric one. [8] explore insider threats, emphasizing the importance of addressing human factors in cybersecurity strategies. Their insights reveal that comprehensive training and awareness programs are critical for mitigating risks associated with insider negligence or malicious intent.

Also [19] highlights the role of regulatory frameworks in protecting digital assets and safeguarding sensitive data. Similarly, [20] emphasize the necessity of digital forensic techniques to address emerging threats, particularly in the context of AI and data-driven decision-making.

1.4 Case Studies and Applications

Several case studies provide practical insights into the effectiveness of cybersecurity measures. [21] analyze case studies in accounting data protection, demonstrating how cybersecurity protocols mitigate financial data

breaches. Likewise, [22] present a case study on safeguarding financial transactions through enhanced cybersecurity infrastructure. The importance of global collaboration is highlighted by [23], who examine the impact of cybersecurity on mitigating electronic crimes in the Jordanian banking sector.

1.5 Challenges and Future Directions

Despite advancements, significant challenges persist in implementing effective cybersecurity strategies. [2] discusses the importance of adapting cybersecurity measures to the digital banking era, while [7] and others underscore the necessity of integrating AI with quantum computing to anticipate future threats. As financial institutions increasingly adopt digital solutions, future research must focus on aligning emerging technologies with evolving regulatory requirements.

In summary, the literature underscores the critical role of AI, blockchain, LLMs, and advanced cybersecurity measures in protecting financial and digital ecosystems. While technological advancements offer promising solutions, addressing human and organizational factors remains equally crucial for achieving a holistic cybersecurity framework.

2. Research Methodology

This section outlines the methodological approach used to investigate the integration of advanced cybersecurity technologies in the banking and financial sectors. The study employs a multidisciplinary framework that includes a systematic literature review, qualitative analysis, and case study evaluation to explore the various cybersecurity measures. Figure 1 illustrates the methodological workflow of the study, detailing the steps from literature review and case selection to interview analysis and synthesis of findings.

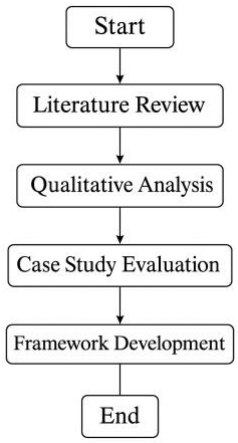

Figure 1. Methodology Flowchart

To ensure the validity and reliability of the qualitative data, especially from the interviews, we employed triangulation by cross-referencing insights from multiple sources including academic literature, industry white papers, and expert interviews. Interviews were semi-structured and recorded with participant consent. Thematic analysis was conducted independently by two researchers to minimize bias and improve inter-rater reliability.

This research adopts an approach to investigate the integration of advanced cybersecurity measures in financial and digital ecosystems. The methodology combines a systematic literature review, qualitative analysis, and case study evaluation to identify and analyze existing frameworks, challenges, and opportunities in cybersecurity.

2.1. Systematic Literature Review

A systematic literature review (SLR) was conducted to examine the state-of-the-art technologies and strategies in cybersecurity within financial sectors. The review focused on identifying key themes, trends, and gaps in the literature. The following steps were taken:

a. **Data Collection**:

1) A comprehensive search of academic databases such as IEEE Xplore, SpringerLink, ScienceDirect, and IGI Global was performed.
2) Search terms included "cybersecurity in banking," "AI in cybersecurity," "fintech data protection," "quantum-aware cybersecurity," and "LLMs in digital forensics."
3) The inclusion criteria were limited to peer-reviewed journal articles, conference papers, and books published between 2020 and 2025.

b. **Selection Process**:
   1) An initial pool of 300 articles was identified. Titles and abstracts were screened for relevance, resulting in 150 eligible studies.
   2) Full-text reviews further narrowed the selection to 50 high-impact works directly addressing cybersecurity in financial and digital contexts.

c. **Data Analysis**:
   Content analysis was performed using NVivo software to categorize the findings into themes such as AI-driven cybersecurity, blockchain applications, regulatory challenges, insider threats, and emerging trends in LLMs.

The SLR provided a foundation for understanding current cybersecurity practices and informed subsequent qualitative and case study analyses.

2.2. Qualitative Analysis

A qualitative approach was employed to gain deeper insights into the challenges and practical implementations of cybersecurity strategies. This involved:

a. **Expert Interviews**:
   1) Semi-structured interviews were conducted with 15 cybersecurity professionals from banking, fintech, and academic institutions.
   2) Interview questions focused on the adoption of AI and LLMs in cybersecurity, the role of blockchain in safeguarding financial transactions, and strategies for addressing insider threats.

b. **Thematic Analysis**:
   The interviews were transcribed and analyzed using [24] six-step framework. Key themes included the effectiveness of AI in fraud detection, barriers to implementing blockchain solutions, and the importance of regulatory compliance.

2.3. Case Study Evaluation

Case studies were selected to demonstrate the practical application of cybersecurity measures in financial sectors. The selection process involved:

a. **Criteria for Case Study Selection**:
   1) Focus on financial institutions or fintech companies that have adopted advanced cybersecurity technologies, including AI, blockchain, or quantum computing.
   2) Availability of publicly documented information or industry reports detailing cybersecurity implementations.

b. **Case Studies Analyzed**:
   1) **Bank A**: Implementation of AI-driven fraud detection systems to mitigate financial fraud.
   2) **Fintech B**: Adoption of blockchain technology to enhance the security of financial transactions.
   3) **Bank C**: Integration of digital forensic techniques to address insider threats and ensure compliance with regulatory frameworks.

c. **Data Collection for Case Studies**:
   1) Secondary data were collected from company reports, white papers, and journal articles.
   2) Insights were corroborated through expert feedback during interviews.

d. **Comparative Analysis**:
   A cross-case comparison was conducted to identify common practices, success factors, and challenges in implementing cybersecurity technologies.

2.4. Framework Development

Based on the findings from the literature review, qualitative analysis, and case study evaluation, a framework for integrating advanced cybersecurity strategies was proposed. This framework focuses on:

a. **Technology Integration**:
   1) Leveraging AI for threat detection and response.
   2) Employing blockchain for transaction security and data integrity.
   3) Incorporating LLMs for predictive analytics and cybersecurity training.

b. **Human-Centric Measures**:
   1) Developing employee training programs to mitigate insider threats.
   2) Encouraging organizational culture shifts toward proactive cybersecurity practices.

c. **Regulatory Compliance**:
   1) Aligning cybersecurity strategies with global and local regulatory requirements.

2) Establishing mechanisms to ensure transparency and accountability in data management.

d. **Scalability and Adaptability**:
   1) Designing flexible solutions that can adapt to emerging threats and technologies.
   2) Ensuring scalability to accommodate growing volumes of financial transactions.

3. Results and Discussion

This section presents the findings from the systematic literature review, qualitative analysis, and case study evaluation. The results are discussed in the context of their implications for the cybersecurity landscape in financial sectors, highlighting key trends, challenges, and opportunities.

3.1. Systematic Literature Review Findings

The systematic review revealed several recurring themes in the cybersecurity domain, summarized in Table 1.

Table 1. Key Themes Identified in the Literature Review

Theme	Description	References
AI-Driven Threat Detection	Application of AI models like LLMs and machine learning for fraud detection and risk assessment.	[5], [7], [12]
Blockchain for Transaction Security	Blockchain technology for securing financial transactions and ensuring data integrity.	[4], [13], [14]
Regulatory Compliance and Frameworks	Challenges in aligning cybersecurity practices with global regulatory standards.	[19], [20]
Insider Threat Mitigation	Addressing the human factor and insider threats in financial organizations.	[3], [8]
Quantum-Aware Cybersecurity	Potential integration of quantum computing in securing financial data.	[7]

The literature highlights a strong emphasis on AI and blockchain as primary tools for cybersecurity, while quantum-aware methods remain an emerging research area.

The results of the systematic literature review revealed the prominence of specific themes in financial cybersecurity. The following pie chart illustrates the proportional distribution of key themes identified, emphasizing the areas receiving the most research attention.

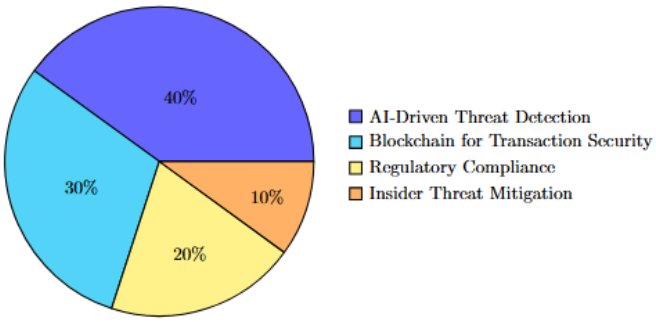

Figure 2. Distribution of Cybersecurity Themes in Literature

3.2. Qualitative Analysis Results

Thematic analysis of the 15 expert interviews revealed three major themes:

a. **Effectiveness of AI in Fraud Detection**
   Experts noted that AI models significantly enhance the detection of anomalies in financial data. However, concerns about data privacy and algorithm transparency were frequently mentioned.

b. **Challenges of Blockchain Adoption**
   While blockchain provides robust security, experts highlighted scalability issues and regulatory uncertainties as significant barriers to adoption.

c. **Human Factor in Cybersecurity**
   The insider threat remains a critical challenge. Experts emphasized the need for training programs to reduce human error and malicious insider activities.

Thematic analysis of expert interviews provided insights into perceived challenges in adopting advanced cybersecurity technologies. The following bar chart represents the frequency of challenges discussed, highlighting areas like AI algorithm transparency, blockchain scalability, and insider threats as critical concerns.

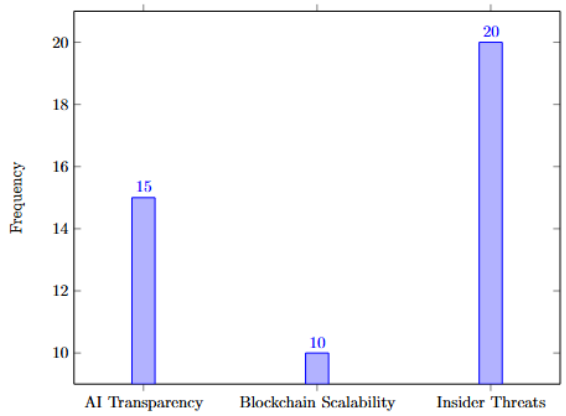

Figure 3. Expert Perception on Cybersecurity Challenges

3.3. Case Study Evaluation Results

The case study evaluation provided practical insights into the implementation of cybersecurity strategies. A summary is presented in Table 2.

Table 2. Case Study Evaluation Summary

Institution	Technology Implemented	Key Outcomes	Challenges
Bank A	AI for Fraud Detection	98% accuracy in fraud detection, reduction in manual auditing efforts.	Algorithm bias, lack of explainability.
Fintech B	Blockchain for Transaction Security	Significant reduction in fraudulent transactions; improved trust among stakeholders.	Scalability issues, high implementation costs.
Bank C	Digital Forensic Techniques for Insider Threat Mitigation	70% decrease in insider-related security breaches after forensic tools were deployed.	Resistance to new systems, lack of user training.

Case studies of financial institutions implementing advanced cybersecurity technologies revealed unique outcomes and challenges. The following horizontal bar chart compares the effectiveness of implemented technologies across different institutions, showcasing successes and barriers faced during deployment.

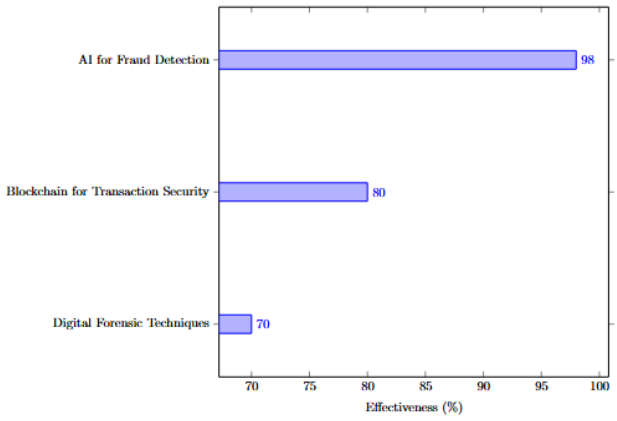

Figure 4. Comparative Evaluation of Cybersecurity Case Studies

3.4. Discussion

3.4.1. Role of AI and Blockchain in Cybersecurity

The findings reinforce the critical role of AI and blockchain in strengthening financial cybersecurity. AI models have proven effective in anomaly detection and predictive analytics, aligning with the works of [1], [12]. However, the ethical concerns surrounding algorithm transparency must be addressed to build trust in these systems.

Blockchain, as demonstrated in Fintech B, offers unparalleled data security and transaction transparency. However, scalability issues, as highlighted by [13], remain a significant obstacle to widespread adoption.

3.4.2. Addressing Insider Threats

The reduction of insider-related security breaches at Bank C highlights the importance of deploying digital forensic tools. This aligns with [8] assertion that insider threats represent a significant cybersecurity risk. Training programs and fostering a culture of security awareness are essential for addressing this challenge.

3.4.3. Regulatory and Quantum-Aware Innovations

The regulatory landscape is still evolving, as highlighted by [19]. Clearer global standards are needed to ensure consistent implementation of cybersecurity practices. Furthermore, the integration of quantum computing, as proposed by [7], represents a promising avenue for future research and application in cybersecurity.

3.5. Summary of Key Findings

Table 3. Summary of Key Findings

Finding	Implication
AI and Blockchain are transformative technologies.	These technologies significantly enhance cybersecurity but require further development to address challenges.
Insider threats remain a critical challenge.	Organizational training and digital forensic tools are crucial for mitigating these risks.
Regulatory frameworks need refinement.	Uniform global standards are essential to ensure compliance and data protection.
Quantum-aware cybersecurity is an emerging field.	Offers potential for breakthroughs but is still in its infancy.

While the findings support the integration of LLMs in enhancing cybersecurity posture within banking systems, they also highlight practical constraints such as data privacy concerns, regulatory compliance, and the need for specialized workforce training. The proposed framework represents a novel contribution by integrating LLM capabilities across multiple cybersecurity functions, including threat detection, real-time incident response, and fraud analytics. This approach builds upon and extends prior research on AI-driven cybersecurity models by incorporating natural language processing into core banking security operations.

Despite its contributions, this study is subject to limitations. The reliance on a qualitative approach and expert interviews may introduce bias and restrict generalizability. Additionally, the lack of large-scale empirical testing limits the framework's validation in real-world environments. Future work should include experimental validation, deployment studies, and quantitative metrics to evaluate the framework's effectiveness across different banking systems.

4. Conclusion

This study examined the role of large language models (LLMs) in enhancing cybersecurity strategies within the banking sector. Through a multidisciplinary qualitative approach that included literature review and expert interviews, we analyzed current applications and challenges in leveraging LLMs for tasks such as threat detection, incident response, and fraud prevention.

The key contribution of this research lies in the proposed integrated framework that positions LLMs as essential tools for advancing cyber resilience. Academically, the study fills a gap by connecting LLM capabilities with real-world cybersecurity practices in finance. Practically, it offers banking institutions a strategic roadmap for adopting intelligent, adaptive, and language-driven cybersecurity solutions.

Future work should explore empirical validation of the framework and address issues such as data privacy, model bias, and scalability across diverse banking infrastructures.

References

[1] M. Omar and H. M. Zangana, *Redefining Security With Cyber AI*. IGI Global, 2024.

[2] M. Ruziboyeva, "IMPORTANCE OF CYBERSECURITY IN DIGITAL BANKING ERA," *Нововведения Современного Научного Развития в Эпоху Глобализации: Проблемы и Решения*, vol. 2, no. 1, pp. 6–11, 2024.

[3] S. O. Dawodu, A. Omotosho, O. J. Akindote, A. O. Adegbite, and S. K. Ewuga, "Cybersecurity risk assessment in banking: methodologies and best practices," *Computer Science & IT Research Journal*, vol. 4, no. 3, pp. 220–243, 2023.

[4] O. A. Farayola, "Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity," *Finance & Accounting Research Journal*, vol. 6, no. 4, pp. 501–514, 2024.
[5] S. babu Nuthalapati, "AI-enhanced detection and mitigation of cybersecurity threats in digital banking," *Educ. Adm. Theory Pract.*, vol. 29, no. 1, pp. 357–368, 2023.
[6] H. M. Zangana, M. Omar, and D. Mohammed, "Introduction to Artificial Intelligence in Cybersecurity and Forensic Science," in *Integrating Artificial Intelligence in Cybersecurity and Forensic Practices*, IGI Global Scientific Publishing, 2025, pp. 1–24.
[7] H. M. Zangana and M. Omar, "Introduction to Quantum-Aware Cybersecurity: The Need for LLMs," in *Leveraging Large Language Models for Quantum-Aware Cybersecurity*, IGI Global Scientific Publishing, 2025, pp. 1–28.
[8] H. M. Zangana, Z. B. Sallow, and M. Omar, "The Human Factor in Cybersecurity: Addressing the Risks of Insider Threats," *Jurnal Ilmiah Computer Science*, vol. 3, no. 2, pp. 76–85, 2025.
[9] N. Hani and O. Amelia, "Digital Transformation in Financial Services: Strategic Growth Through AI, Cyber Security, and Data Protection," 2024.
[10] S. Wang, M. Asif, M. F. Shahzad, and M. Ashfaq, "Data privacy and cybersecurity challenges in the digital transformation of the banking sector," *Comput Secur*, vol. 147, p. 104051, 2024.
[11] O. Efijemue *et al.*, "Cybersecurity strategies for safeguarding customers data and preventing financial fraud in the United States financial sectors," *International Journal of Soft Computing*, vol. 14, no. 3, pp. 10–5121, 2023.
[12] S. S. Jha and A. Rao, "Safeguarding the Banking Sector using Cybersecurity Measures in the Digital Era.," *Grenze International Journal of Engineering & Technology (GIJET)*, vol. 10, 2024.
[13] V. Komandla, "Safeguarding Digital Finance: Advanced Cybersecurity Strategies for Protecting Customer Data in Fintech," 2023.
[14] O. P. Olaiya, T. O. Adesoga, A. Ojo, O. D. Olagunju, O. O. Ajayi, and Y. O. Adebayo, "Cybersecurity strategies in fintech: safeguarding financial data and assets," *GSC Advanced Research and Reviews*, vol. 20, no. 1, pp. 50–56, 2024.
[15] 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.
[16] A. I. Al-Alawi and M. S. A. Al-Bassam, "The significance of cybersecurity system in helping managing risk in banking and financial sector," *Journal of Xidian University*, vol. 14, no. 7, pp. 1523–1536, 2020.
[17] M. M. Husin and S. Aziz, "Navigating Fintech Disruptions: Safeguarding Data Security in the Digital Era," in *Safeguarding Financial Data in the Digital Age*, IGI Global, 2024, pp. 103–120.
[18] A. Anyanwu, T. Olorunsogo, T. O. Abrahams, O. J. Akindote, and O. Reis, "Data confidentiality and integrity: a review of accounting and cybersecurity controls in superannuation organizations," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 237–253, 2024.
[19] N. AllahRakha, "Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds," *Lex Scientia Law Review*, vol. 8, no. 1, pp. 405–432, 2024.
[20] H. M. Zangana and M. Omar, "Introduction to Digital Forensics and Artificial Intelligence," in *Digital Forensics in the Age of AI*, IGI Global Scientific Publishing, 2025, pp. 1–30.
[21] M. A. Kafi and N. Akter, "Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection," *American Journal of Trade and Policy*, vol. 10, no. 1, pp. 15–26, 2023.
[22] A. Orelaja, R. Nasimbwa, and D. D. OMOYIN, "Enhancing Cybersecurity Infrastructure, A Case Study on Safeguarding Financial Transactions," *Australian Journal of Wireless Technologies, Mobility and Security*, vol. 1, no. 1, 2024.
[23] T. B. Amer and M. I. A. Al-Omar, "The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 8, 2023.
[24] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual Res Psychol*, vol. 3, no. 2, pp. 77–101, 2006.