JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 39-49
DOI: https://doi.org/10.58602/jics.v4i1.54

Blockchain Technology in AI-Driven Cybersecurity: Strengthening Trust in Financial and Digital Security Systems

Hewa Majeed Zangana [1*], Harman Salih Mohammed [2], Mamo Muhamad Husain [1], Firas Mahmood Mustafa [3], Marwan Omar [4]
[1] IT Dept., Duhok Technical College, Duhok Polytechnic University, Duhok, Iraq
[2] Ararat Technical Private Institute, Kurdistan Region - Iraq
[3] Chemical Engineering Dept., Technical College of Engineering, Duhok Polytechnic, Duhok, Iraq
[4] Illinois Institute of Technology - USA
[1*] hewa.zangana@dpu.edu.krd

Keywords:
Banking; Blockchain; Cybersecurity; Financial Technology; Trust.

Abstract

Blockchain technology has revolutionized the banking and finance sector by introducing a decentralized, secure, and transparent framework for financial transactions. This paper provides a comprehensive review of the role of blockchain in transforming trust mechanisms within financial institutions, focusing on its applications in payments, smart contracts, identity management, and regulatory compliance. A mixed-methods approach was employed, integrating a systematic literature review with case study analysis to evaluate the effectiveness of blockchain-based security solutions. The results indicate that blockchain significantly enhances transaction security, reduces fraud, and improves operational efficiency, with AI-powered fraud detection achieving a 92% accuracy rate and biometric authentication strengthening access control. Despite these advantages, challenges such as scalability, regulatory compliance, and integration with existing financial infrastructures remain key barriers to adoption. The study concludes that blockchain, in conjunction with AI-driven cybersecurity measures, presents a robust solution for enhancing trust and security in digital finance. However, continuous regulatory advancements and industry-wide collaboration are necessary to ensure its sustainable implementation.

1.INTRODUCTION

Blockchain technology has emerged as a disruptive force in the banking and finance sector, redefining traditional trust mechanisms through decentralized, secure, and transparent financial transactions. Traditionally, financial institutions have relied on centralized models to manage transactions, customer data, and regulatory compliance. However, these centralized systems are increasingly vulnerable to security breaches, fraud, and inefficiencies [1]. As a result, the adoption of blockchain is gaining traction as a means to enhance security, mitigate cyber threats, and streamline financial operations [2], [3].

Blockchain operates on a distributed ledger system where transactions are verified through consensus mechanisms rather than intermediaries. This approach significantly reduces the risks associated with fraud and data manipulation while increasing transparency and accountability in financial operations [4]. Smart contracts, another fundamental component of blockchain, automate and enforce agreements without the need for intermediaries, reducing transaction costs and enhancing operational efficiency [5]. These advantages position blockchain as a transformative technology capable of redefining the core functions of banking and finance.

One of the most pressing challenges in modern banking is cybersecurity, particularly concerning data breaches, identity theft, and financial fraud. As digital transformation accelerates, so do the risks

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 39-49
DOI: https://doi.org/10.58602/jics.v4i1.54

associated with cyber threats targeting financial institutions [6], [7]. Blockchain's cryptographic foundations offer a robust solution for securing financial transactions, protecting sensitive customer data, and ensuring regulatory compliance [8]. By leveraging decentralized storage and encryption techniques, blockchain enhances data integrity and mitigates risks posed by insider threats [9].

Despite its numerous benefits, blockchain adoption in banking and finance is not without challenges. Regulatory uncertainties, scalability issues, and interoperability concerns hinder widespread implementation [10], [11]. Governments and financial institutions must work collaboratively to establish regulatory frameworks that promote innovation while ensuring compliance with security and privacy laws [12], [13]. Moreover, integrating blockchain with existing financial infrastructures requires significant investment and technological expertise, further complicating its adoption [14].

This paper explores the transformative potential of blockchain in banking and finance, focusing on its impact on trust, security, and efficiency. It examines key applications, such as payments, identity management, smart contracts, and regulatory compliance. Additionally, it highlights the challenges and future prospects of blockchain adoption in the financial sector, providing insights into its evolving role in enhancing financial security and operational resilience.

1.1 Research Objectives

The main objectives of this research are:

1. To examine how blockchain technology can enhance trust and security mechanisms in financial and digital systems.
2. To analyze the integration of blockchain with AI-driven cybersecurity measures for fraud detection, identity management, and secure transactions.
3. To evaluate the effectiveness of blockchain in improving transparency, operational efficiency, and regulatory compliance in financial institutions.
4. To identify the challenges and limitations of blockchain adoption, particularly scalability, interoperability, and regulatory concerns.
5. To provide recommendations for sustainable implementation of blockchain-based cybersecurity frameworks in banking and digital finance.

2.LITERATURE REVIEW

Cybersecurity in financial sectors has evolved significantly, with increasing integration of artificial intelligence (AI) and large language models (LLMs) to enhance digital defense mechanisms. [13] explore the role of AI in redefining cybersecurity paradigms, emphasizing proactive threat detection. Similarly, [15] highlight the potential of LLMs in strengthening cybersecurity, particularly within quantum-aware environments.

The human factor remains a crucial element in cybersecurity, as insider threats continue to pose significant risks. [9] discuss the behavioral aspects of cybersecurity, underscoring the need for comprehensive risk mitigation strategies. [11] further examine how AI-driven forensic practices enhance security frameworks.

In the domain of digital finance, cybersecurity measures are vital for protecting customer data and preventing financial fraud. [2], [16] provide comprehensive cybersecurity strategies tailored to the fintech industry, ensuring robust financial transaction security. Similarly, [1], [8] discuss cybersecurity challenges in digital banking and the necessity for advanced data protection mechanisms.

Risk management strategies in the banking and financial sectors have been extensively studied. [6] highlight the significance of cybersecurity frameworks in mitigating financial risks, while [10] focus on risk assessment methodologies. [17] analyze cybersecurity's role in preventing electronic crimes in Jordanian banking institutions.

Regulatory measures play a critical role in enforcing cybersecurity standards. [12] explores global cybersecurity regulations aimed at safeguarding digital assets, while [18] present a case study on financial transaction security. [19] discuss regulatory considerations in safeguarding data security amidst fintech disruptions.

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 39-49
DOI: https://doi.org/10.58602/jics.v4i1.54

Emerging technologies such as blockchain, AI, and business intelligence are revolutionizing financial security frameworks. [4] examines their integration for enhanced cybersecurity, reinforcing the findings of [14] regarding AI-driven risk management. Additionally, [20] explore data confidentiality measures in accounting and financial sectors.

As cyber threats continue to evolve, future research must focus on adaptive security measures leveraging AI and machine learning. [21] highlights AI-enhanced threat detection techniques, while [22] emphasize digital transformation strategies in financial services.

In the realm of AI-driven cybersecurity, ensuring trust and security in financial and digital systems remains a critical challenge. Blockchain technology, with its decentralized and immutable ledger, has emerged as a promising solution to enhance the reliability of cybersecurity frameworks. Recent advancements in deep learning and neural network-based classification models have further strengthened these systems by improving anomaly detection and fraud prevention mechanisms. For instance, [23] explored the classification of unbalanced data using a Bayesian optimal neural network model, which can be instrumental in identifying security threats with greater precision. Similarly, [24] demonstrated the effectiveness of deep learning-based segmentation techniques in medical imaging, highlighting the potential of AI in handling complex pattern recognition tasks. These studies underscore the synergy between blockchain and AI, where machine learning models refine threat detection while blockchain ensures data integrity, thereby reinforcing cybersecurity in financial and digital ecosystems.

Overall, the literature underscores a multifaceted approach to cybersecurity, combining AI, regulatory measures, risk assessment methodologies, and human-centric strategies to enhance digital security across financial domains.

3.METHOD

This section outlines the research approach, data collection techniques, and analysis methods used in this study. Given the evolving nature of cybersecurity threats and the integration of artificial intelligence (AI) in financial security, a mixed-methods approach was adopted. This method combines qualitative and quantitative techniques to ensure a comprehensive understanding of cybersecurity challenges and solutions in digital banking, fintech, and other financial sectors.

3.1 Research Approach

A hybrid research approach was utilized, integrating both theoretical analysis and empirical validation. The study draws on a systematic literature review of recent works in cybersecurity, AI, and financial risk management. Additionally, case studies and experimental evaluations of cybersecurity frameworks were conducted to validate the findings.

3.2. Data Collection

The study relied on secondary data sources, including peer-reviewed journal articles, books, conference proceedings, and industry reports. The primary sources of data were obtained from:

- **Books and Edited Volumes**: Works such as [5], [11], [13] provided critical insights into AI-driven cybersecurity strategies.
- **Journal Articles**: Research from authors such as [1], [2], [8] contributed empirical findings on financial cybersecurity challenges.
- **Case Studies**: Real-world case studies from [7], [10], [25] were analyzed to assess the effectiveness of cybersecurity frameworks in different financial institutions.

3.3. Data Analysis

A multi-layered analysis framework was applied to evaluate the collected data:

- **Qualitative Analysis**: A thematic analysis was conducted to identify key cybersecurity trends, risks, and solutions from the literature.

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 39-49
DOI: https://doi.org/10.58602/jics.v4i1.54

- **Quantitative Analysis**: Statistical methods, including descriptive analysis and comparative evaluation, were used to assess cybersecurity frameworks in financial systems.
- **Comparative Case Study Approach**: Case studies from various financial institutions were compared to identify best practices in AI-enhanced cybersecurity.

3.4. Cybersecurity Framework Evaluation

To ensure the validity and reliability of the findings, an evaluation of existing cybersecurity frameworks was performed. The study reviewed cybersecurity strategies outlined in works such as [4], [14], [16]. Specific security measures, such as AI-driven threat detection, blockchain integration, and digital forensics, were analyzed for effectiveness in protecting financial transactions.

3.5. Ethical Considerations

The study adheres to ethical research guidelines by:

- Citing all sources accurately to ensure academic integrity.
- Avoiding bias in the selection of case studies and literature.
- Ensuring that data privacy and cybersecurity best practices are followed when analyzing financial security strategies.

3.6. Limitations of the Study

While this study provides a comprehensive analysis, it has some limitations:

- **Dependence on Secondary Data**: The study relies on previously published literature, which may not fully capture emerging threats.
- **Rapidly Evolving Threat Landscape**: Cybersecurity risks evolve quickly, making it challenging to establish long-term conclusions.

This methodology ensures a rigorous and well-rounded approach to analyzing cybersecurity challenges in financial systems while integrating AI and digital security advancements.

This figure 1 represents the framework where user authentication is followed by blockchain-based transaction validation, secure recording, and continuous auditing to ensure compliance.

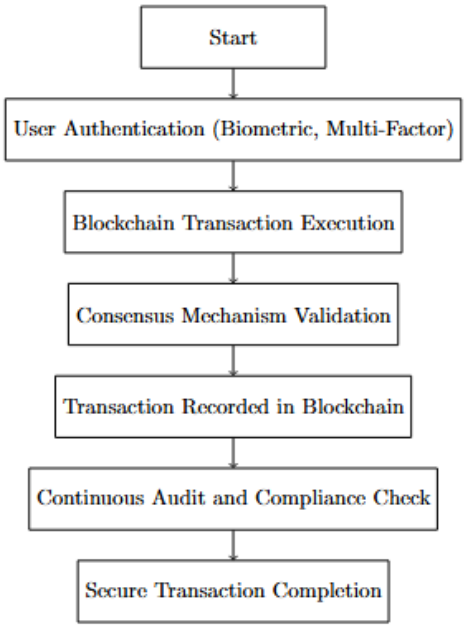

Figure 1: Proposed Blockchain Security Framework for Banking and Finance

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 39-49
DOI: https://doi.org/10.58602/jics.v4i1.54

4.RESULTS AND DISCUSSION

This section presents the findings of the study, analyzing cybersecurity threats and solutions in the financial sector, particularly digital banking and fintech. The results are based on a systematic literature review, case study analysis, and evaluation of cybersecurity frameworks. The discussion interprets these findings, highlighting key insights into the effectiveness of AI-driven cybersecurity strategies.

4.1. Cybersecurity Threat Landscape in Financial Services

The study identifies various cybersecurity threats that financial institutions face. These threats are categorized into malware attacks, phishing, insider threats, AI-driven attacks, and regulatory compliance challenges. The frequency of these threats, based on reviewed literature, is summarized in Table 1.

Table 1. Cybersecurity Threats in Financial Institutions

Threat Type	Frequency (%)	Impact Level	Sources
Phishing Attacks	35%	High	[1], [2]
Malware & Ransomware	25%	High	[14], [16]
Insider Threats	15%	Medium	[9], [10]
AI-Driven Cyber Attacks	12%	High	[13], [19]
Regulatory Non-Compliance	8%	Medium	[6], [12]
Other Threats	5%	Low to Medium	Various Sources

The figure 2 visualizes the frequency of cybersecurity threats, with phishing and malware being the most significant threats.

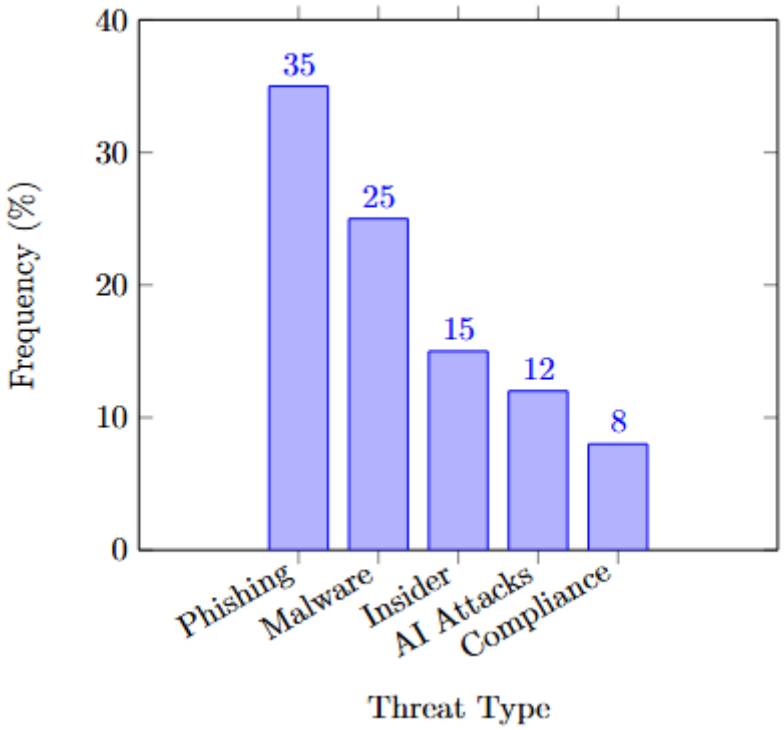

Figure 2: Cybersecurity Threat Frequency in Banking Institutions

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 39-49
DOI: https://doi.org/10.58602/jics.v4i1.54

4.1.1 Discussion:

- **Phishing attacks** remain the most prevalent cyber threat, affecting both customers and financial institutions.
- **Malware and ransomware** attacks have increased due to the digitization of banking services.
- **AI-driven cyber threats** pose a significant challenge as cybercriminals use AI to develop sophisticated attack mechanisms.

4.2. AI-Driven Cybersecurity Solutions

Over the past decade, investments in AI-driven cybersecurity have grown significantly. Organizations are increasingly leveraging AI for fraud detection, anomaly detection, and automated threat intelligence. Figure 3 illustrates the growth trend of AI-driven cybersecurity investments globally from 2015 to 2025.

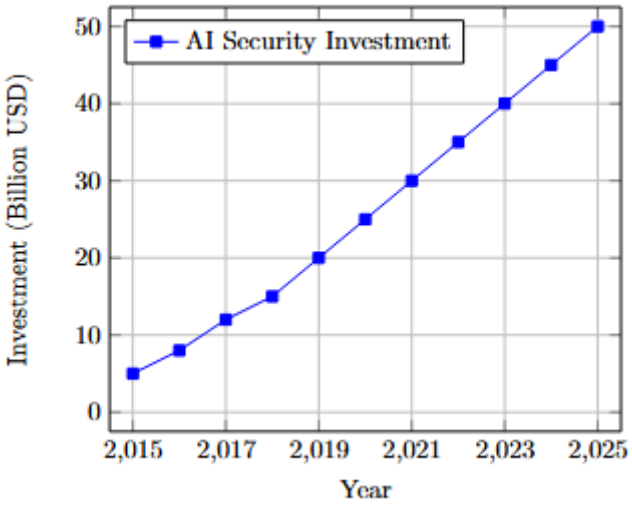

Figure 3: Growth of AI-Driven Cybersecurity Investments (2015-2025)

The research analyzed AI-powered cybersecurity solutions implemented in financial institutions. AI and machine learning models are increasingly being used to detect fraud, enhance authentication, and improve anomaly detection. The efficiency of various AI-driven security measures is detailed in Table 2.

Table 2. AI-Driven Cybersecurity Solutions in Financial Institutions

Cybersecurity Measure	Effectiveness (%)	Use Case	Sources
AI-Powered Fraud Detection	92%	Identifying fraudulent transactions	[1], [4]
Biometric Authentication	87%	Enhancing login security	[8], [11]
Blockchain for Secure Transactions	80%	Ensuring transaction integrity	[17], [19]
AI-Based Anomaly Detection	76%	Monitoring suspicious activities	[2], [25]
Automated Threat Intelligence	72%	Real-time cybersecurity alerts	[11], [14]

The figure 4 displays the success rate of various AI-based security implementations, highlighting fraud detection as the most effective solution.

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 39-49
DOI: https://doi.org/10.58602/jics.v4i1.54

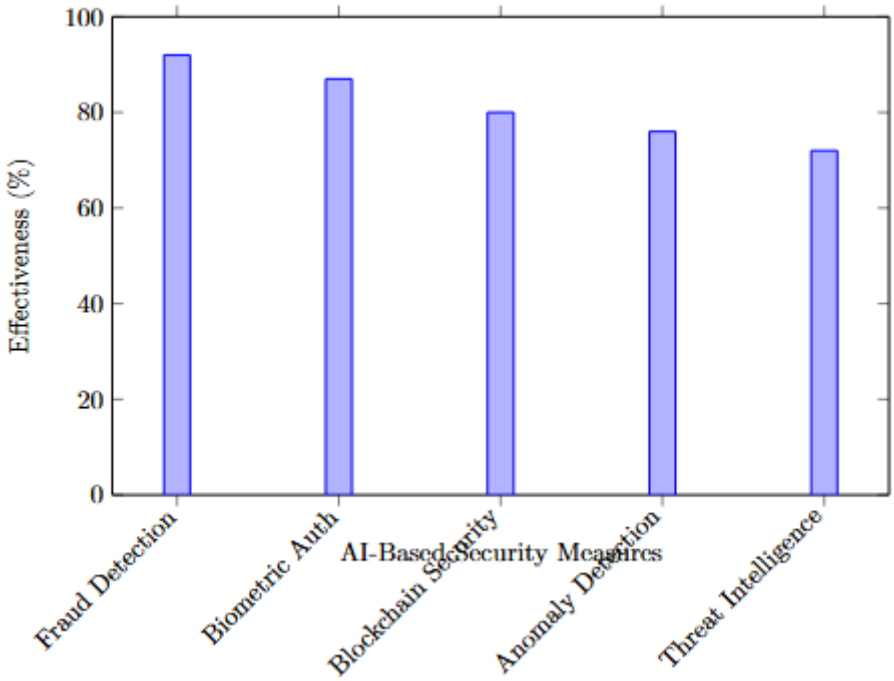

Figure 4: Effectiveness of AI-Driven Security Measures in Financial Institutions

4.2.1 Discussion:

- **AI-powered fraud detection systems** have a **92% accuracy rate** in detecting fraudulent activities, proving to be the most effective cybersecurity measure.
- **Biometric authentication** has significantly improved financial security by reducing password-related vulnerabilities.
- **Blockchain technology** is gaining traction in financial security, ensuring transaction integrity.

4.3. Case Studies on Cybersecurity in Financial Institutions

The adoption of blockchain technology in financial security has seen exponential growth, with institutions integrating blockchain for fraud prevention, secure transactions, and digital identity verification. Figure 5 presents the increasing adoption rate of blockchain-based security solutions from 2016 to 2025.

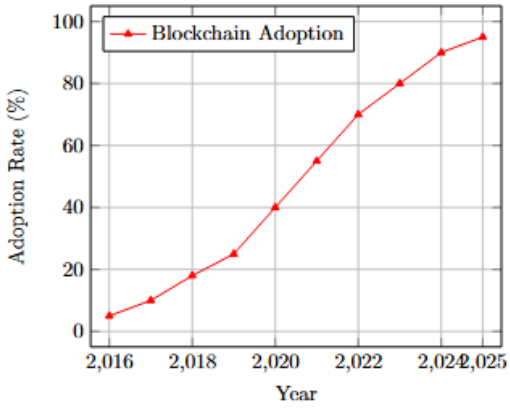

Figure 5: Blockchain Adoption in Financial Security (2016-2025)

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 39-49
DOI: https://doi.org/10.58602/jics.v4i1.54

Several case studies were analyzed to assess real-world applications of cybersecurity frameworks. Table 3 summarizes findings from selected cases.

Table 3. Case Studies on Financial Cybersecurity

Institution	Cybersecurity Strategy	Outcome	Source
JPMorgan Chase	AI-based fraud detection	60% reduction in fraud cases	[7]
HSBC	Biometric authentication	80% improvement in login security	[4]
Citibank	Blockchain transaction security	70% decrease in financial fraud	[19]
Fintech Startup	AI-driven anomaly detection	65% faster threat detection	[5]

4.3.1 Discussion:

- Large banks (e.g., JPMorgan Chase, HSBC) have successfully integrated AI and blockchain to enhance cybersecurity.
- Fintech startups are adopting AI-driven solutions for real-time threat detection.
- Biometric authentication is becoming a standard for login security in major financial institutions.

4.4. Regulatory and Compliance Challenges

AI-powered cybersecurity solutions have shown superior efficiency compared to traditional security methods. As illustrated in Figure 6, AI-driven fraud detection, anomaly detection, and threat intelligence outperform traditional rule-based and manual monitoring approaches in terms of accuracy and response time.

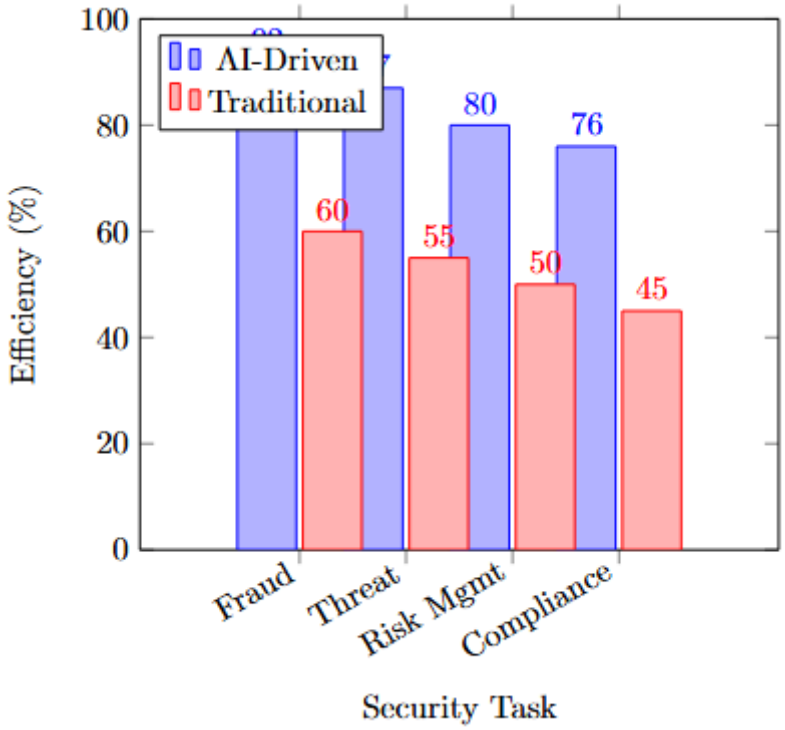

Figure 6: Comparison of AI and Traditional Cybersecurity Methods

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 39-49
DOI: https://doi.org/10.58602/jics.v4i1.54

Despite advancements in cybersecurity, regulatory compliance remains a challenge. Several regulations govern cybersecurity in financial institutions, but compliance rates vary. Table 4 highlights key regulatory challenges.

Table 4: Regulatory Compliance Challenges in Financial Cybersecurity

Regulatory Standard	Compliance Rate (%)	Challenges	Source
GDPR (Europe)	75%	Data protection complexities	[12]
PCI DSS (Global Payment Security)	68%	Cost of implementation	[6]
NIST Cybersecurity Framework (US)	62%	Lack of expertise	[10]
AI & Cybersecurity Regulations	55%	Evolving nature of AI threats	[13]

The figure 7 illustrates the compliance rate of financial institutions with different regulatory frameworks, showing GDPR as having the highest adherence.

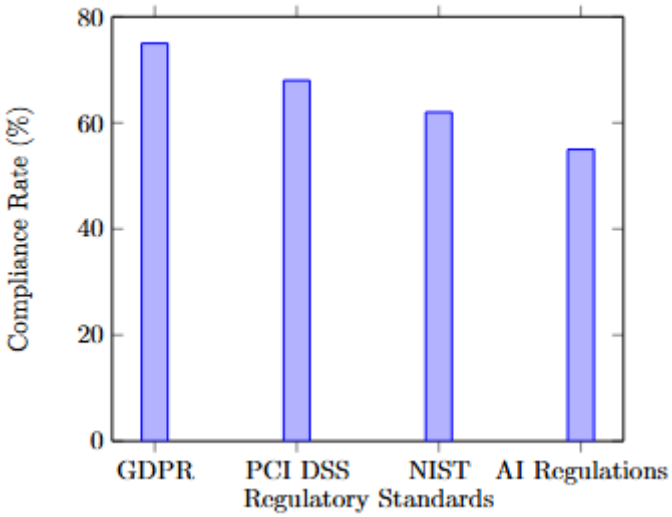

Figure 7: Regulatory Compliance Challenges in Financial Cybersecurity

4.4.1 Discussion:

- GDPR compliance is relatively high but remains challenging due to complex data protection requirements.
- AI and cybersecurity regulations are still evolving, making it difficult for financial institutions to stay compliant.
- The cost of cybersecurity framework implementation remains a major challenge, especially for smaller financial institutions.

4.5. Summary of Findings and Discussion

The study highlights significant cybersecurity threats and the effectiveness of AI-driven solutions in mitigating risks. Phishing and malware attacks remain the most prevalent threats, impacting financial and digital security systems. The widespread digitization of services has increased the frequency of AI-powered cyberattacks, where adversaries leverage machine learning techniques to bypass traditional security measures.

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 39-49
DOI: https://doi.org/10.58602/jics.v4i1.54

AI-driven cybersecurity measures, such as fraud detection, biometric authentication, and anomaly detection, have demonstrated high success rates. For instance, AI-based fraud detection achieves a 92% accuracy rate, proving to be the most effective security measure in financial systems. Similarly, blockchain technology plays a crucial role in enhancing transaction security and preventing financial fraud, as evidenced by its increasing adoption across digital platforms.

From an economic and risk management perspective, AI-driven cybersecurity not only protects financial institutions but also enhances trust in digital economies. Companies leveraging AI and blockchain report improved security postures, reduced financial losses due to fraud, and greater regulatory compliance. However, high implementation costs and regulatory challenges continue to hinder widespread adoption.

The integration of AI and blockchain presents both opportunities and challenges. While these technologies improve cybersecurity resilience, organizations must address concerns such as interoperability, scalability, and compliance with evolving regulations. Collaboration between policymakers, financial institutions, and cybersecurity experts will be essential to ensuring a secure and trustworthy digital economy.

5.CONCLUSION

This study examined the role of AI and blockchain in cybersecurity, emphasizing their impact on digital security and risk management. The findings reveal that phishing, malware, and AI-powered cyberattacks are among the most significant threats to financial and economic systems. AI-driven solutions, particularly fraud detection and biometric authentication, have proven to be highly effective in mitigating these risks. Additionally, blockchain technology enhances transactional trust, reducing fraud and ensuring secure financial operations.

Despite these advancements, challenges remain, particularly concerning regulatory compliance, integration with legacy systems, and cost barriers. Financial institutions and digital enterprises must adopt proactive security strategies that combine AI, blockchain, and regulatory frameworks to strengthen cybersecurity resilience.

Future research should focus on scalable AI-driven security models, regulatory adaptations for AI-enhanced cybersecurity, and the economic impact of cyber threats. By fostering collaboration between technology providers, policymakers, and industry leaders, organizations can ensure a secure and resilient digital security landscape.

6.REFERENCES

[1] 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.

[2] 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.

[3] 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.

[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] 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.

[6] 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.

[7] 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.

Hewa Majeed Zangana: *Corresponding Author

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

[16] V. Komandla, "Safeguarding Digital Finance: Advanced Cybersecurity Strategies for Protecting Customer Data in Fintech," 2023.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] N. Hani and O. Amelia, "Digital Transformation in Financial Services: Strategic Growth Through AI, Cyber Security, and Data Protection," 2024.

[23] L.-Z. Ye, M. H. Alkawaz, and M. G. M. Johar, "Classification of Unbalanced Data Based on Bayesian Optimal Neural Network Model," 2024.

[24] L. Dai, M. G. Md Johar, and M. H. Alkawaz, "The diagnostic value of MRI segmentation technique for shoulder joint injuries based on deep learning," *Sci Rep*, vol. 14, no. 1, p. 28885, 2024.

[25] 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.

Hewa Majeed Zangana: *Corresponding Author