Journal of Technology and Informatics (JoTI)
Vol. 7, No. 1, Bulan April Tahun 2025
P-ISSN 2721-4842
E-ISSN 2686-6102

A Hybrid Framework for Securing 5G-Enabled Healthcare Systems

Alton Mabina

Department of Computer Science, Universitas of Botswana, Gaborone, Botswana
e-mail: altonmabina@gmail.com

Article Information

Article History:
Received : January 20th, 2025
Revised : April 12th, 2025
Accepted : April 29th, 2025
Published : April 30th, 2025

***Correspondence:**
altonmabina@gmail.com

Keywords:
AI-driven security, Blockchain, Healthcare data privacy, Zero-trust architecture, 5G networks

10.37802/joti.v7i1.970

Journal of Technology and Informatics (JoTI)
P-ISSN 2721-4842
E-ISSN 2686-6102
https://e-journals.dinamika.ac.id/index.php/joti

Abstract:

The rapid adoption of 5G technology in healthcare introduces significant challenges regarding data privacy and security. This paper proposes a hybrid framework integrating blockchain, zero-trust architecture (ZTA), and AI-driven threat detection to address these challenges. Blockchain ensures secure, tamper-proof data storage, while ZTA strengthens access control by continuously verifying users and devices. AI contributes by providing real-time threat detection and dynamic response capabilities, making the system more resilient to evolving cyber risks. A systematic literature review was conducted to analyze existing frameworks and identify gaps in 5G healthcare security. The findings reveal that while individual technologies such as blockchain and ZTA are well-established, their integration into a cohesive framework remains underexplored. The proposed hybrid solution effectively mitigates the risks associated with 5G networks by offering a multi-layered security approach. This research contributes to the field by proposing a scalable, adaptable security model suitable for 5G-enabled healthcare systems. Future research should focus on empirical validation, scalability testing, and exploring lightweight alternatives to blockchain and AI for resource-constrained environments. Additionally, investigating the integration of emerging technologies like quantum computing and 6G networks will further enhance the framework's security capabilities. This study provides a foundation for developing secure, privacy-preserving systems for healthcare in the 5G era.

INTRODUCTION

The healthcare industry is undergoing rapid digital transformation with the adoption of 5G technology, enabling faster and more reliable connections for IoT devices, telemedicine, and remote monitoring. However, this technological advancement has introduced significant challenges in protecting sensitive patient information. The integration of numerous connected devices increases the risk of cyberattacks, data breaches, and unauthorized access. Current security frameworks often lack the robustness needed to address the scale and complexity of 5G-enabled systems. A hybrid approach integrating advanced technologies like blockchain,

zero-trust architecture (ZTA), and AI is crucial to safeguarding healthcare data effectively [1, 2, 3, 4, 5].

Research Problem

As healthcare systems adopt 5G, they face vulnerabilities stemming from inadequate data privacy and security measures. Existing frameworks often fail to address the high speed, low latency, and distributed nature of 5G networks. This creates a pressing need for an advanced security framework that can protect patient information while supporting the dynamic requirements of 5G-enabled healthcare systems [6].

Research Question and Objective

The primary research question is: How can a hybrid framework combining blockchain, zero-trust architecture, and AI enhance data privacy and security in 5G-enabled healthcare systems? The objective of this study is to propose and evaluate a robust, multi-layered security framework that effectively mitigates risks and ensures secure data transmission across connected healthcare devices.

Justification and significance of research

Protecting patient information is critical to maintaining trust in healthcare systems and ensuring compliance with global data privacy regulations. This research addresses a critical gap in existing security frameworks by proposing a comprehensive solution tailored to the unique demands of 5G technology. The findings will benefit healthcare providers by offering a scalable and reliable approach to safeguarding sensitive data, reducing the risk of breaches, and enhancing patient safety. Ultimately, the study contributes to the broader goal of securely integrating advanced technologies into healthcare delivery [7, 8].

Literature Review

Recent studies highlight the transformative role of 5G technology in healthcare, emphasizing its potential to improve service delivery through IoT devices, telemedicine, and real-time data sharing. For instance, [9] explored the vulnerabilities of big data in healthcare, identifying encryption and secure data transfer as critical needs. Similarly, [10] proposed a security framework for 5G-enabled IoT healthcare applications, focusing on mitigating risks such as data breaches and unauthorized access. More recently, advanced frameworks combining blockchain and artificial intelligence (AI) have gained attention, demonstrating promise in achieving real-time threat detection and decentralized data management [11]. These studies establish a foundation for exploring hybrid security solutions tailored to 5G networks.

Key Theories or Concepts

The literature emphasizes three key concepts: blockchain, zero-trust architecture (ZTA), and AI-driven security. Blockchain ensures tamper-proof data storage and transparent auditing, making it a cornerstone of secure frameworks. ZTA, rooted in the principle of "never trust, always verify," ensures continuous verification of devices and users, reducing attack surfaces. AI complements these technologies by enabling predictive threat analysis and real-time responses to cyberattacks. Together, these concepts form the basis for a robust multi-layered security approach in healthcare [12, 13, 14].

Despite the advances, several gaps persist. Current research often focuses on individual technologies, such as blockchain or AI, without adequately exploring how they can be integrated into a cohesive framework. Additionally, there is limited empirical validation of proposed solutions in real-world healthcare environments, raising concerns about scalability and performance under actual 5G network conditions. Controversies also arise regarding the computational overhead of blockchain and AI, with critics arguing these technologies may

compromise system efficiency. Addressing these gaps and controversies is essential for developing a practical and effective security framework for 5G-enabled healthcare systems [14, 15, 16].

METHOD

This study employs a qualitative research design based on a systematic review of existing literature and theoretical analysis. By synthesizing insights from peer-reviewed articles, conference papers, and technical reports published since 2020, the study identifies best practices, challenges, and emerging solutions in securing 5G-enabled healthcare systems. The research also integrates theoretical and practical knowledge to propose a robust hybrid framework as the primary result of the study [17, 18].

Data Collection Methods

The study utilizes secondary data sourced from academic databases such as IEEE Xplore, Google Scholar, and ScienceDirect. Articles were selected based on relevance to 5G in healthcare, blockchain, zero-trust architecture, and AI-driven security solutions. Keywords such as "5G healthcare security," "blockchain in healthcare," and "AI-driven data privacy" guided the search. Only studies published between 2020 and 2024 were considered to ensure the inclusion of the most recent advancements [19, 20].

Sample Selection

A purposive sampling strategy was used to select 50 highly cited and peer-reviewed articles that address key aspects of data privacy and security in healthcare. Priority was given to studies focusing on integrated frameworks or solutions specifically tailored to 5G networks. Exclusion criteria included papers unrelated to healthcare or not involving 5G technologies [21].

Data Analysis

Data analysis involved thematic coding to identify recurring patterns, challenges, and solutions across the selected literature. Key themes, such as the role of blockchain, ZTA, and AI in enhancing security, were analyzed to develop a coherent understanding of their integration. The findings were then mapped to the proposed hybrid framework, which was evaluated against identified gaps and controversies in the literature. The final analysis demonstrates how the framework addresses existing challenges and contributes to securing 5G-enabled healthcare systems [22].

RESULTS AND DISCUSSION

Results

1. Presentation of Findings

The study findings are presented in three main themes: (1) strengths and limitations of existing frameworks, (2) contributions of blockchain, zero-trust architecture (ZTA), and AI, and (3) the proposed hybrid framework. Table 1 summarizes the key insights from the literature, showing the strengths, limitations, and potential for integration of various technologies.

Table 1. Potential for Integration of Various Technologies

Technology	Strengths	Limitations	Potential for Integration
Blockchain	Tamper-proof data, transparent auditing	High computational overhead, scalability issues	Strong foundation for secure data transactions

Zero-Trust Architecture	Continuous verification, reduced attack surface	Complexity in implementation, resource-intensive	Essential for access control
AI	Real-time threat detection, predictive analysis	Data dependency, potential for false positives	Key for dynamic threat management

2. Proposed Framework Findings

The proposed hybrid framework integrates these technologies to address the identified gaps in existing solutions. Blockchain ensures secure data storage, ZTA enhances access control, and AI provides dynamic threat detection and mitigation. This multi-layered approach demonstrates a robust solution to securing 5G-enabled healthcare systems [23].

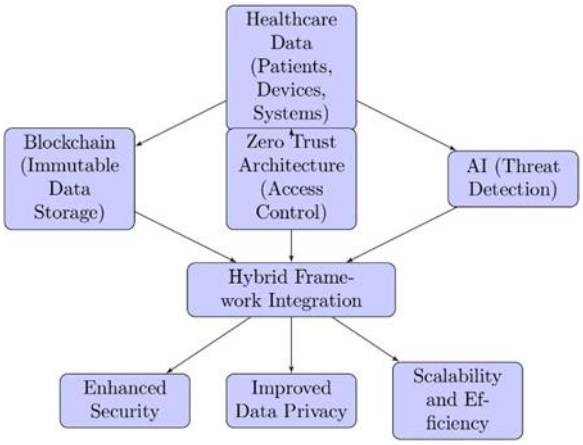

Figure 1. Architectural Diagram of the Proposed Framework

The proposed hybrid framework integrates Blockchain, Zero-Trust Architecture (ZTA), and Artificial Intelligence (AI) to enhance the security of 5G-enabled healthcare systems. Healthcare data from patients, devices, and operational systems is collected and forms the foundation of the framework. Blockchain technology ensures this data is securely stored and immutable, providing a tamper-proof system for sensitive patient records. ZTA enforces strict access controls, allowing only authenticated users and devices to interact with the system. Meanwhile, AI dynamically detects and mitigates potential threats, analysing network activities in real time to ensure continuous protection [6].

This multi-layered framework operates by seamlessly integrating its components into a unified security solution. Blockchain's cryptographic verification reduces the risk of data breaches, while ZTA ensures unauthorized access is effectively prevented through continuous verification protocols. AI adds an intelligent layer of protection, proactively identifying and responding to threats before they cause harm. The integration layer enables smooth communication between these technologies, ensuring that each component supports the other to achieve comprehensive security [23].

The framework offers significant benefits to healthcare systems. It enhances data privacy by implementing robust access control mechanisms while improving security through immutable storage and dynamic threat detection. Scalability is another key feature, allowing the framework to adapt to growing healthcare demands without compromising

efficiency. This adaptability also makes it relevant for other critical sectors, such as finance or education, where similar challenges in data protection exist [24].

For future research, the framework provides a strong foundation for exploring advanced technologies. Researchers can investigate incorporating cutting-edge AI models, such as federated learning, to enhance data security without compromising privacy. Additionally, integrating quantum-resistant Blockchain technology could future-proof the framework against emerging cyber threats. Its modular design ensures that it remains adaptable to technological advancements, making it a valuable resource for ongoing research in secure 5G-enabled environments.

By addressing core security challenges, the framework not only meets current needs but also provides a roadmap for future innovation. It is a scalable, adaptable, and robust solution that can evolve with advancements in technology. This makes it an essential contribution to securing healthcare systems in the 5G era and beyond [25].

3. Data Analysis and Interpretations

Through thematic analysis, the integration of these technologies was found to address core security gaps:

a. Data Breach Mitigation: Blockchain's immutability ensures secure patient records, reducing tampering risks.
b. Access Control: ZTA effectively restricts unauthorized access, ensuring only verified users and devices can interact with the system.
c. Threat Detection: AI enables proactive responses to threats, ensuring network security in real-time.

The hybrid framework meets the research objective by addressing the challenges posed by 5G healthcare environments. It enhances data privacy and security, ensuring scalability and efficiency without compromising performance.

4. Support for Research Question and Objective

The results directly support the research question: How can a hybrid framework combining blockchain, zero-trust architecture, and AI enhance data privacy and security in 5G-enabled healthcare systems? The findings demonstrate the viability of integrating these technologies into a single framework, providing a comprehensive and scalable solution to current challenges. This supports the study's objective of proposing a robust security framework tailored to 5G-enabled healthcare environments.

Discussion

1. Interpretation of Results

The findings reveal that a hybrid framework integrating blockchain, zero-trust architecture (ZTA), and AI effectively enhances data privacy and security in 5G-enabled healthcare systems. Blockchain's tamper-proof storage ensures data integrity, while ZTA strengthens access control by continuously verifying users and devices. AI's real-time threat detection provides a dynamic layer of defense, addressing evolving cyber risks. This multi-layered approach resolves significant gaps in current security frameworks, such as inadequate scalability and response capabilities.

2. Comparison with Existing Literature

The proposed framework aligns with existing research, such as [26] emphasis on blockchain and [27] work on ZTA. However, unlike these studies, the hybrid framework integrates AI for real-time threat management, filling a critical gap in dynamic cybersecurity responses [28], [29] highlighted the potential of blockchain and AI but did not propose a

cohesive integration. By combining these technologies, this study offers a more comprehensive solution, addressing the interconnected challenges of data privacy and security in 5G healthcare systems.

3. Implications of the Study

The study has significant implications for healthcare providers and policymakers. It provides a blueprint for developing scalable, secure systems capable of protecting patient data in 5G environments. The framework's adaptability ensures it can evolve with emerging technologies, such as 6G, and contribute to establishing global standards for healthcare cybersecurity. Additionally, this research underscores the importance of proactive strategies, encouraging investment in advanced technologies for safeguarding sensitive information [30].

4. Limitations of the Study

Despite its strengths, the study has limitations. The framework's effectiveness is based on theoretical insights from the literature, lacking empirical validation through real-world implementation. Scalability and performance under high data loads in 5G networks remain untested. Furthermore, the computational overhead associated with blockchain, and AI technologies could pose challenges for resource-constrained healthcare systems. Addressing these limitations requires future research to test and refine the proposed framework in practical healthcare settings [31, 32, 33].

The proposed hybrid framework shows promise but has several practical limitations. Its effectiveness is based on theoretical insights and lacks empirical validation in real-world healthcare environments. Testing the framework in live 5G-enabled healthcare systems is necessary to confirm its applicability and effectiveness.

Scalability poses another challenge, as the framework's ability to handle the high data volumes typical of 5G healthcare systems remains untested. Performance bottlenecks may occur, especially in resource-intensive tasks like AI-based threat detection. Additionally, the computational demands of Blockchain and AI technologies could strain resource-limited healthcare systems, particularly in developing regions [34].

Latency issues may arise from combining technologies like Blockchain and ZTA, which could delay critical operations such as transaction validation or access control. Integration complexity adds to this challenge, as modern security technologies may not easily align with existing healthcare infrastructure, requiring costly upgrades or replacements [35]. Furthermore, the framework must comply with diverse data privacy regulations like GDPR and HIPAA, which vary globally and may impose additional restrictions on data management. High implementation costs, including infrastructure upgrades and skilled personnel, could also hinder adoption, particularly for smaller healthcare providers [36].

To overcome these limitations, future research should focus on validating the framework in real-world settings, optimizing performance, and exploring cost-effective strategies for implementation. By addressing these challenges, the framework could become a transformative solution for securing 5G-enabled healthcare systems [37, 38, 39].

CONCLUSIONS AND SUGGESTIONS

Conclusions

This study investigated the challenges of data privacy and security in 5G-enabled healthcare systems and proposed a hybrid framework integrating blockchain, zero-trust architecture (ZTA), and AI to address these challenges. The findings demonstrate that

blockchain ensures data integrity through tamper-proof storage, ZTA enhances access control by continuously verifying devices and users, and AI provides real-time threat detection and dynamic risk mitigation. Together, these technologies form a robust, multi-layered defense strategy capable of meeting the demands of 5G healthcare environments. The study contributes to the field by bridging gaps in existing literature through the integration of advanced technologies into a cohesive framework. Unlike prior research, which often focused on individual technologies, this study highlights the synergistic benefits of combining blockchain, ZTA, and AI. The proposed framework provides a scalable and adaptable solution, offering a practical roadmap for enhancing data privacy and security in healthcare. This research also lays a foundation for further exploration of hybrid models in addressing cybersecurity challenges in high-speed, distributed networks like 5G [40], [41].

Future research should prioritize empirical validation of the proposed framework in real-world healthcare settings to assess its scalability, efficiency, and adaptability under diverse conditions. This involves deploying the framework in live 5G healthcare environments and monitoring its performance with varying data loads and security demands. Additionally, studies should explore solutions to mitigate the computational overhead of blockchain and AI by investigating lightweight alternatives, such as optimized algorithms or more efficient consensus mechanisms, to ensure suitability for resource-constrained environments [42]. Emerging technologies, such as quantum computing and 6G networks, offer promising avenues for further enhancing the security and performance of the framework. Future research should explore how these advancements can be integrated to address sophisticated cybersecurity threats and increase processing speed. Expanding research to include global case studies and cross-border data regulations is equally essential to evaluate the framework's universal applicability and compliance with diverse legal and ethical standards [43].

Strengthening the validation process through theoretical modeling is another critical area. Simulation environments can be used to test the framework’s components, measure potential performance metrics, and predict outcomes under various scenarios. These models can provide preliminary insights before real-world deployment, reducing risks and optimizing the framework for practical use. Together, these efforts will ensure the framework's evolution into a robust and scalable solution for healthcare cybersecurity [44], [45].

Suggestions

The proposed hybrid framework for securing 5G-enabled healthcare systems offers a robust multi-layered security approach that integrates blockchain, zero-trust architecture (ZTA), and AI-driven threat detection. Based on the identified research gaps, it is recommended that future efforts focus on developing an empirical validation of this framework in real-world healthcare environments. Additionally, scalability testing is crucial to ensure that the framework can handle the large volumes of data typical in 5G networks without compromising system performance. Researchers should also explore lightweight alternatives to blockchain and AI, specifically in resource-constrained healthcare settings, where computational resources may be limited. Lastly, fostering collaboration between academia and industry can facilitate the development of practical solutions that address the specific security challenges of 5G healthcare systems.

To further advance this research, empirical validation is a critical next step. Testing the framework in diverse healthcare contexts will help assess its effectiveness and reliability in preventing cyber threats in real-time. Additionally, scalability should be tested to ensure that the system can function efficiently as the number of devices and users increases. Research into lightweight alternatives to blockchain and AI for resource-constrained environments is also

necessary to ensure the framework is applicable in low-resource settings, such as rural healthcare facilities. Lastly, exploring the potential integration of emerging technologies like quantum computing and 6G networks will likely enhance the framework's security capabilities and ensure its longevity in the rapidly evolving technological landscape of healthcare systems.

REFERENCES

[1] D. H. Devi et al., "5G Technology in Healthcare and Wearable Devices: A Review," *Sensors*, vol. 23, no. 5, p. 2519, Feb. 2023, doi: 10.3390/s23052519.

[2] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "5G technology for healthcare: Features, serviceable pillars, and applications," *Intell. Pharm.*, vol. 1, no. 1, pp. 2–10, Jun. 2023, doi: 10.1016/j.ipha.2023.04.001.

[3] A. I. Stoumpos, F. Kitsios, and M. A. Talias, "Digital Transformation in Healthcare: Technology Acceptance and Its Applications," *Int. J. Environ. Res. Public. Health*, vol. 20, no. 4, p. 3407, Feb. 2023, doi: 10.3390/ijerph20043407.

[4] A. Kumar et al., "Evaluation of 5G techniques affecting the deployment of smart hospital infrastructure: Understanding 5G, AI and IoT role in smart hospital," Alex. Eng. J., vol. 83, pp. 335–354, Nov. 2023, doi: 10.1016/j.aej.2023.10.065.

[5] S. M. A. A. Abir, M. Abuibaid, J. S. Huang, and Y. Hong, "Harnessing 5G Networks for Health Care: Challenges and Potential Applications," in 2023 *International Conference on Smart Applications, Communications and Networking (SmartNets), Istanbul, Turkiye: IEEE*, Jul. 2023, pp. 1–6. doi: 10.1109/SmartNets58706.2023.10215757.

[6] B. Chen et al., "A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10248–10263, Jul. 2021, doi: 10.1109/JIOT.2020.3041042.

[7] Oluwabunmi Layode, Henry Nwapali Ndidi Naiho, Gbenga Sheriff Adeleke, Ezekiel Onyekachukwu Udeh, and Talabi Temitope Labake, "The role of cybersecurity in facilitating sustainable healthcare solutions: Overcoming challenges to protect sensitive data," *Int. Med. Sci. Res. J.*, vol. 4, no. 6, pp. 668–693, Jun. 2024, doi: 10.51594/imsrj.v4i6.1228.

[8] C. Petersen, "Through Patients' Eyes: Regulation, Technology, Privacy, and the Future," Yearb. *Med. Inform.*, vol. 27, no. 01, pp. 010–015, Aug. 2018, doi: 10.1055/s-0038-1641193.

[9] Janet Ngesa, "Tackling security and privacy challenges in the realm of big data analytics," *World J. Adv. Res. Rev.*, vol. 21, no. 2, pp. 552–576, Feb. 2023, doi: 10.30574/wjarr.2024.21.2.0429.

[10] S. Madanian, T. Chinbat, M. Subasinghage, D. Airehrour, F. Hassandoust, and S. Yongchareon, "Health IoT Threats: Survey of Risks and Vulnerabilities," *Future Internet*, vol. 16, no. 11, p. 389, Oct. 2024, doi: 10.3390/fi16110389.

[11] O. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni, and A. Mancini, "On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security," *IEEE Access*, vol. 12, pp. 3881–3897, 2024, doi: 10.1109/ACCESS.2023.3349019.

[12] D. H. Devi et al., "5G Technology in Healthcare and Wearable Devices: A Review," *Sensors*, vol. 23, no. 5, p. 2519, Feb. 2023, doi: 10.3390/s23052519.

[13] Islam Ahmad Ibrahim Ahmad, Femi Osasona, Samuel Onimisi Dawodu, Ogugua Chimezie Obi, Anthony Chigozie Anyanwu, and Shedrack Onwusinkwue, "Emerging 5G technology: A review of its far-reaching implications for communication and security," *World J. Adv. Res. Rev.*, vol. 21, no. 1, pp. 2474–2486, Jan. 2024, doi: 10.30574/wjarr.2024.21.1.0346.

[14] S. M. A. A. Abir, M. Abuibaid, J. S. Huang, and Y. Hong, "Harnessing 5G Networks for Health Care: Challenges and Potential Applications," in 2023 *International Conference on Smart Applications, Communications and Networking (SmartNets), Istanbul, Turkiye: IEEE*, Jul. 2023, pp. 1–6. doi: 10.1109/SmartNets58706.2023.10215757.

[15] H. Sadri et al., "Integration of Blockchain and Digital Twins in the Smart Built Environment Adopting Disruptive Technologies—A Systematic Review," *Sustainability*, vol. 15, no. 4, p. 3713, Feb. 2023, doi: 10.3390/su15043713.

[16] L. Theodorakopoulos, A. Theodoropoulou, and C. Halkiopoulos, "Enhancing Decentralized Decision-Making with Big Data and Blockchain Technology: A Comprehensive Review," *Appl. Sci.*, vol. 14, no. 16, p. 7007, Aug. 2024, doi: 10.3390/app14167007.

[17] M. L. Jones, "Application of systematic review methods to qualitative research: practical issues," *J. Adv. Nurs.*, vol. 48, no. 3, pp. 271–278, Nov. 2004, doi: 10.1111/j.1365-2648.2004.03196.x.

[18] L.-L. Ebidor and I. G. Ikhide, "Literature Review in Scientific Research: An Overview," *East Afr. J. Educ. Stud.*, vol. 7, no. 2, pp. 179–186, May 2024, doi: 10.37284/eajes.7.2.1909.

[19] J. Gamboa-Cruzado, K. Echevarria-Otazo, D. Medina-Montes, S. A. Esquivel, D. O. Gago, and I. F. Muñoz, "Understanding how healthcare innovation is shaped by 5G technology: A comprehensive systematic review," *J. Infrastruct. Policy Dev.*, vol. 8, no. 16, p. 10171, Dec. 2024, doi: 10.24294/jipd10171.

[20] A. Kumar et al., "Evaluation of 5G techniques affecting the deployment of smart hospital infrastructure: Understanding 5G, AI and IoT role in smart hospital," Alex. Eng. J., vol. 83, pp. 335–354, Nov. 2023, doi: 10.1016/j.aej.2023.10.065.

[21] L. A. Palinkas, S. M. Horwitz, C. A. Green, J. P. Wisdom, N. Duan, and K. Hoagwood, "Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research," *Adm. Policy Ment. Health Ment. Health Serv. Res.*, vol. 42, no. 5, pp. 533–544, Sep. 2015, doi: 10.1007/s10488-013-0528-y.

[22] S. R. Addula, K. Meduri, G. S. Nadella, and H. Gonaygunta, "AI and Blockchain in Finance: Opportunities and Challenges for the Banking Sector," *IJARCCE*, vol. 13, no. 2, Feb. 2024, doi: 10.17148/IJARCCE.2024.13231.

[23] Sunday Adeola Oladosu, Adebimpe Bolatito Ige, Christian Chukwuemeka Ike, Peter Adeyemo Adepoju, Olukunle Oladipupo Amoo, and Adeoye Idowu Afolabi, "Revolutionizing data center security: Conceptualizing a unified security framework for hybrid and multi-cloud data centers," Open Access *Res. J. Sci. Technol.*, vol. 5, no. 2, pp. 086–076, Aug. 2022, doi: 10.53022/oarjst.2022.5.2.0065.

[24] P. Shojaei, E. Vlahu-Gjorgievska, and Y.-W. Chow, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," *Computers*, vol. 13, no. 2, p. 41, Jan. 2024, doi: 10.3390/computers13020041.

[25] Adebimpe Bolatito Ige, Eseoghene Kupa, and Oluwatosin Ilori, "Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future," *GSC Adv. Res. Rev.*, vol. 19, no. 3, pp. 344–360, Jun. 2024, doi: 10.30574/gscarr.2024.19.3.0236.

[26] Z. Moezkarimi, F. Abdollahei, and A. Arabsorkhi, "Proposing a Framework for Evaluating the Blockchain Platform," in 2019 5th *International Conference on Web Research (ICWR), Tehran, Iran: IEEE*, Apr. 2019, pp. 152–160. doi: 10.1109/ICWR.2019.8765280.

[27] J. (Elaine) Chen, F. Bao, C. Li, and Y. Lin, "The Application and Ethics of Artificial Intelligence in Blockchain: A Bibliometric-Content Analysis," *J. Glob. Inf. Manag.*, vol. 31, no. 7, pp. 1–32, Jun. 2023, doi: 10.4018/JGIM.323656.

[28] T. R. Xuan and S. Ness, "Integration of Blockchain and AI: Exploring Application in the Digital Business," *J. Eng. Res. Rep.*, vol. 25, no. 8, pp. 20–39, Aug. 2023, doi: 10.9734/jerr/2023/v25i8955.

[29] S. Kumar, W. M. Lim, U. Sivarajah, and J. Kaur, "Artificial Intelligence and Blockchain Integration in Business: Trends from a Bibliometric-Content Analysis," *Inf. Syst. Front.*, Apr. 2022, doi: 10.1007/s10796-022-10279-0.

[30] C. Elendu, T. C. Elendu, and I. D. Elendu, "5G-enabled smart hospitals: Innovations in patient care and facility management," *Medicine (Baltimore),* vol. 103, no. 20, p. e38239, May 2024, doi: 10.1097/MD.0000000000038239.

[31] H. Elahi, G. Wang, Y. Xu, A. Castiglione, Q. Yan, and M. N. Shehzad, "On the Characterization and Risk Assessment of AI-Powered Mobile Cloud Applications," *Comput. Stand. Interfaces*, vol. 78, p. 103538, Oct. 2021, doi: 10.1016/j.csi.2021.103538.

[32] M. AlJamal et al., "A Robust Machine Learning Model for Detecting XSS Attacks on IoT over 5G Networks," *Future Internet*, vol. 16, no. 12, p. 482, Dec. 2024, doi: 10.3390/fi16120482.

[33] T. Hoeschele, C. Dietzel, D. Kopp, F. H. P. Fitzek, and M. Reisslein, "Importance of Internet Exchange Point (IXP) infrastructure for 5G: Estimating the impact of 5G use cases," *Telecommun. Policy*, vol. 45, no. 3, p. 102091, Apr. 2021, doi: 10.1016/j.telpol.2020.102091.

[34] A. Afaq, N. Haider, M. Z. Baig, K. S. Khan, M. Imran, and I. Razzak, "Machine learning for 5G security: Architecture, recent advances, and challenges," *Ad Hoc Netw.*, vol. 123, p. 102667, Dec. 2021, doi: 10.1016/j.adhoc.2021.102667.

[35] P. Thantharate and A. Thantharate, "ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain," Big Data *Cogn. Comput.*, vol. 7, no. 4, p. 165, Oct. 2023, doi: 10.3390/bdcc7040165.

[36] W. F. Shah, "Preserving Privacy and Security: A Comparative Study of Health Data Regulations - GDPR vs. HIPAA," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 8, pp. 2189–2199, Aug. 2023, doi: 10.22214/ijraset.2023.55551.

[37] B. Patel, V. K. Yarlagadda, N. Dhameliya, K. Mullangi, and S. C. R. Vennapusa, "Advancements in 5G Technology: Enhancing Connectivity and Performance in Communication Engineering," *Eng. Int.*, vol. 10, no. 2, pp. 117–130, Oct. 2022, doi: 10.18034/ei.v10i2.715.

[38] S. F. Ahmed et al., "Toward a Secure 5G-Enabled Internet of Things: A Survey on Requirements, Privacy, Security, Challenges, and Opportunities," *IEEE Access*, vol. 12, pp. 13125–13145, 2024, doi: 10.1109/ACCESS.2024.3352508.

[39] A. Ahad et al., "A Comprehensive review on 5G-based Smart Healthcare Network Security: Taxonomy, Issues, Solutions and Future research directions," *Array*, vol. 18, p. 100290, Jul. 2023, doi: 10.1016/j.array.2023.100290.

[40] Q. Tang, S. Kamarudin, S. N. A. Rahman, and X. Zhang, "Bridging Gaps in Online Learning: A Systematic Literature Review on the Digital Divide," *J. Educ. Learn.*, vol. 14, no. 1, p. 161, Sep. 2024, doi: 10.5539/jel.v14n1p161.

[41] A. I. Weinberg and K. Cohen, "Zero trust implementation in the emerging technologies era: a survey," *Complex Eng. Syst.*, vol. 4, no. 3, Sep. 2024, doi: 10.20517/ces.2024.41.

[42] A. K. Jameil and H. Al-Raweshidy, "A Digital Twin Framework for Real-Time Healthcare Monitoring: Leveraging AI and Secure Systems for Enhanced Patient Outcomes," Dec. 16, 2024, In Review. doi: 10.21203/rs.3.rs-5107583/v1.

[43] Rafiul Azim Jowarder and Sawgat Jahan, "Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection," *World J. Adv. Eng. Technol. Sci.*, vol. 13, no. 1, pp. 330–339, Sep. 2024, doi: 10.30574/wjaets.2024.13.1.0421.

[44] A. Ali et al., "Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning," *Sensors*, vol. 23, no. 18, p. 7740, Sep. 2023, doi: 10.3390/s23187740.

[45] A. Almalawi et al., "Enhancing security in smart healthcare systems: Using intelligent edge computing with a novel Salp Swarm Optimization and radial basis neural network algorithm," *Heliyon*, vol. 10, no. 13, p. e33792, Jul. 2024, doi: 10.1016/j.heliyon.2024.e33792.