Journal of Multidisciplinary Research & Development Studies (JMRDS) | ISSN 3139-3497

Research Article (Open Access)

Journal of Multidisciplinary Research & Development Studies (JMRDS)

Peer Reviewed Refereed Open Access International Multidisciplinary Journal

Cybersecurity and Blockchain Innovations in Medical Information Systems

Nidhi Mishra

Pt Hari Shankar College Raipur

Corresponding Author: nidhimishra.harishankarcollege@protonmail.com

Abstract

With the healthcare industry undergoing a digital revolution at a fast pace, there is growing demand for secure and reliable measures to safeguard patient data and medical devices. This research examines the synergy between blockchain, AI, and their advanced cybersecurity strategies in healthcare to fortify data protection, privacy, and operational resilience. The aim of the research is to examine the latest advancements in blockchain-enabled cybersecurity solutions for healthcare information systems, Internet of Medical Things (IoMT) devices, Electronic Medical Records (EMR) and Smart Healthcare Infrastructure. For this task, a complete review-based methodology was used that involved analyzing recent scientific papers on blockchain for healthcare security, AI-powered threat detection, federated learning, and cryptographic defense mechanisms. The analysis shows that blockchain has the potential to transform the healthcare communication systems by providing increased data integrity, secure authentication, decentralized access control, and transparency, and that AI can significantly augment healthcare communication systems with its ability to detect anomalies and predict threats. The findings also show that blockchain can contribute to the security of next-generation healthcare systems when combined with AI and IoMT technologies, thus minimizing vulnerabilities to cyber-attacks, unauthorized access and data breaches. The research concludes that blockchain-based cybersecurity frameworks offer a promising and scalable solution for secure digital transformation in the healthcare sector, though several challenges need to be addressed, including scalability, interoperability, energy consumption and regulatory considerations, which warrant further research and optimization.

Keywords:

Blockchain, Cybersecurity, Healthcare Systems, Artificial Intelligence, Internet of Medical Things, Data Privacy

Received on 9 July 2026; **Revised on** 19 July 2026, **Accepted on** 6 Aug 2026; **Published on** 31 Aug 2026

DOI: *https://doi.org/10.67512/jmrds.v1.i4.3*

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are properly cited.

1. Introduction

Digital healthcare technologies have revolutionized the way medical data is managed, stored, and shared in hospitals, clinics, and smart healthcare settings. The integration of Electronic Health Records (EHRs), Cloud Computing, Telemedicine platforms, Wearable sensors, and the Internet of Medical Things (IoMT) devices has enhanced the accessibility, monitoring, and decision-making in healthcare. The digital transformation has also exposed increased risk for cyber threats like ransomware attacks, unauthorized access, identity theft, and data breaches, which can impact patient privacy and healthcare operations, however [1] [2]. In the traditional centralized healthcare security systems, scalability, trust management and potential single points of failure are some of the limitations that necessitate more resilient cybersecurity solutions [3] [4].

The decentralized, immutability, transparency, and cryptographic security of blockchain technology are attractive attributes for securing healthcare infrastructures [5] [6]. By leveraging blockchain, data sharing, record management, and authentication processes can be made more secure and reliable, enhancing the effectiveness of healthcare communication systems. Moreover, AI and blockchain are also being combined to improve the healthcare industry's capacity to identify deviations, forecast cyber threats, and automatically act in response to vulnerabilities in real-time [7] [8]. In recent times, blockchain-based systems have proven to be a successful tool for safeguarding patient data, ensuring secure data interoperability and fostering trust among healthcare organizations [9] [10].

With the proliferation of IoMT devices and smart healthcare applications, the need for cyber security in modern healthcare infrastructures has grown even stronger. There have been attempts to implement blockchain-based cybersecurity systems for secure identity management, encrypted communication in healthcare settings, and privacy protection in healthcare environments [11] [12]. Furthermore, AI-powered cybersecurity solutions, when integrated with blockchain technology, have demonstrated impressive potential in enhancing data confidentiality, integrity and overall system robustness in the face of advanced cyberattacks [13] [14]. Federated learning and intelligent threat analytics are among emerging technologies that have advanced the secure healthcare ecosystem [15] [16].

While there has been considerable progress, there are still some research challenges which have not been resolved. The current healthcare cybersecurity solutions may experience problems such as scalability, interoperability, computational complexity, regulatory compliance, and energy efficiency [17] [18]. A lot of existing solutions also fail to ensure security, privacy and system efficiency in highly dynamic health care systems [19] [20]. In addition, there is the issue of secure model training, data governance, and real-time threat mitigation with the combination of AI and blockchain [21] [22]. As digital health systems become increasingly complex, cybersecurity strategies need to be more adaptive, intelligent, and scalable to fight against new attack vectors and maintain healthcare resilience for the long run [23] [24].

The objective of this research is to explore the potential of blockchain technology and AI to improve cybersecurity in healthcare institutions. The research areas are related to blockchain security architectures for the healthcare sector, AI threat detection systems, secure IoMT communication protocols, and privacy-preserving healthcare applications. The study also explores the existing challenges, limitations and research prospects in blockchain-based healthcare cybersecurity systems.

This study brings significant contributions: (i) a thorough review of blockchain-based cybersecurity methods in healthcare systems; (ii) analysis of the prospects of combining AI, IoMT, and federated learning with blockchain security frameworks; (iii) identification of key issues related to scalability, interoperability, and privacy management; and (iv) discussing research directions for creating secure, intelligent, and resilient future-generation healthcare infrastructures.

2. Literature Survey

The rise of digital healthcare technologies has helped to drive the development of cybersecurity frameworks that can shield critical medical information and linked health systems. The decentralized nature, immutability and transparency of blockchain technology have made it a significant interest for enhancing the security and reliability of healthcare communication systems. The initial research focused on the ability of blockchain to offer secure data transactions, decentralized trust management and tamper-resistant data records for healthcare applications [1] [10]. The research laid the groundwork for the potential of blockchain in improving cybersecurity and safeguarding the integrity of eHRs against potential tampering. A few studies have focused on cybersecurity approaches supported by blockchain in the healthcare sector and in the Internet of Medical Things (IoMT) context. To enhance the security and authentication methods of healthcare data, blockchain-based algorithms were suggested [1]. In the same manner, blockchain has been introduced to enhance the monitoring and automatic identification of threats in healthcare systems, particularly in the context of cybersecurity [2]. The secure communication, decentralized access control, and superior patient data privacy provided by a dedicated cyber security architecture which integrated blockchain with IoMT devices were proven [3]. In addition, blockchain-based deep learning techniques have demonstrated the successful application for securing next-generation medical cyber-physical systems by performing intelligent intrusion detection and predictive threat analysis [4].

The shift of healthcare cybersecurity has also been a subject of research for blockchain-based medical management systems and the protection of electronic medical records. Secure healthcare communication via Blockchain frameworks is designed to assure integrity, confidentiality and transparency in the exchange of medical information [5] [6]. The use of cryptographic approaches for authentication and secure data sharing in smart healthcare systems was further enhanced through evidence-based cybersecurity approaches [8]. Moreover, healthcare informatics systems based on the blockchain showed enhanced security of patient data from unauthorized access and cyber threats [9]. The findings of these studies underscore the potential of blockchain to enhance the cybersecurity of healthcare systems while ensuring the security and transparency of medical data. There has been a recent surge in the use of Artificial Intelligence (AI) and blockchain technologies in the healthcare industry for the purpose of creating intelligent security systems.The use of Artificial Intelligence (AI) and blockchain technologies in the healthcare industry has been a major focus of recent literature, particularly when it comes to creating intelligent security systems. There are examples of using AI enabled blockchain systems for anomaly detection, predictive cyber threat identification, and adaptive healthcare risk management [7] [13]. In smart healthcare systems, some new ideas have been proposed to combine blockchain technology with federated learning to enhance secure collaborative learning while still maintaining patient privacy [15]. Other advanced AI ensemble models and blockchain technologies have also been suggested to enhance security performance, scalability and healthcare data protection [21]. The integration of AI with blockchain is becoming more critical in tackling future cyber threats in healthcare, as seen in these intelligent frameworks.

There are also some studies that have examined cybersecurity risk management and privacy protection in the healthcare IoT ecosystems. Blockchain identity management systems were suggested to improve the secure authentication and minimize vulnerabilities in healthcare IoT devices [22]. The reviews on cybersecurity, data privacy and blockchain applications focused on decentralized architectures to reduce the impact of ransomware attacks, enhance data security for patient records and enhance trust management [18] [20]. Furthermore, resilience-based healthcare cybersecurity frameworks stressed the need for adaptive security mechanisms that can work with a digital transformation process in healthcare organisations [23]. New studies also focused on the clinical risk management strategies for AI-induced cybersecurity issues, employing blockchain-protection models [24]. While previous research has shown substantial progress in the field of blockchain for healthcare cybersecurity, there are still some challenges that are yet to be addressed. There are scalability problems, energy consumption, interoperability problems and heavy computational load in many healthcare systems based on the blockchain [11] [12]. Additionally, there are some AI-based security systems that do not have the ability to efficiently implement in real-time in a large-scale healthcare setting [14] [16]. Moreover,

the current solutions are limited to specific healthcare use cases and do not offer a general architecture that could unify all the technologies such as AI, blockchain, IoMT, and privacy-preserving technologies into a single cybersecurity framework [17] [19].

The literature shows that blockchain and AI technologies have great potential to protect the healthcare infrastructure, but more scalable, intelligent, interoperable and adaptive cybersecurity systems are needed. The main challenges identified in the current research are the limited implementation of the advanced AI-based threat analysis in healthcare systems based on blockchain, the lack of focus on real-time cyber risk management and the absence of common architectures for the next generation of smart healthcare environments. To overcome these challenges, the present study focuses on providing a comprehensive overview of cybersecurity approaches that incorporate blockchain with artificial intelligence and current healthcare technologies, thus facilitating the creation of secure, resilient and efficient healthcare ecosystems.

3. Materials and Methods

Materials, datasets, tools, algorithms, and experimental methodology for the development of the blockchain-assisted cybersecurity framework for healthcare systems are described. The framework proposed leverages the blockchain, artificial intelligence (AI), and Internet of Medical Things (IoMT) security models to improve the security of healthcare data, communication, and threat detection. The methodology should provide a way to assure repeatability and systematic application of the proposed healthcare cybersecurity architecture.

3.1 Data Collection

To test the proposed framework, the experimental study relied on publicly available datasets related to healthcare cybersecurity and IoMT. Healthcare communication information sets were gathered from public repositories of normal and malicious network traffic to simulate cyber-attack scenarios in the healthcare infrastructure. The electronic health record (EHR) transaction datasets and IoMT communications logs were also analyzed to evaluate the performance of secure data exchange and intrusion detection.

The main data sets used in this study are:

- CICIDS2017 Dataset : Link: https://www.unb.ca/cic/datasets/ids-2017.html This dataset contains benign and malicious network traffic records including Distributed Denial of Service (DDoS), brute force, botnet, and infiltration attacks.
- IoMT Healthcare Dataset : Link: https://www.kaggle.com/ The dataset includes simulated IoMT communication traffic generated from wearable healthcare devices and medical sensors.
- Electronic Health Record (EHR) Dataset : Link: https://physionet.org/ This dataset contains anonymized patient healthcare records used for secure blockchain-based storage and access control evaluation.

The collected data was then preprocessed through normalization, duplicate removal and feature extraction techniques to ensure the quality of the data and a reliable cybersecurity analysis.

Table 1 below contains the datasets and their characteristics used in the experimental analysis.

Table 1. Healthcare Cybersecurity Datasets Used in the Study

Dataset	Description	Purpose

CICIDS2017	Network intrusion detection dataset	Cyber-attack detection
IoMT Dataset	Medical sensor communication records	IoMT security analysis
EHR Dataset	Electronic health records	Secure blockchain storage

3.2 Proposed Method

The methodology proposed combines blockchain technology, AI-driven intrusions detection, encryption solutions, and IoMT security management to create a secure healthcare cybersecurity framework.

A. Data Preprocessing

The first is the pre-processing of the healthcare network traffic and EHR datasets, where incomplete EHRs and the data values in the datasets were removed to ensure the complete and normalised datasets, and security-related features were extracted. Data preprocessing boosts the precision of machine learning models, and simplifies computation for cybersecurity analysis.

Min-Max normalization was used to normalize the process with the following equation:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \qquad (1)$$

Where:

- X_{norm}= Normalized data value
- X= Original feature value
- X_{min}= Minimum feature value
- X_{max}= Maximum feature value

The healthcare cybersecurity data was scaled using Equation (1) to ensure it fits into a specific range for better efficiency in training AI models.

B. Blockchain Based Secure Data Storage

The second phase involved integrating blockchain into the healthcare system to provide a secure record-keeping solution for transactions and EHRs. Every health care transaction was turned into a cryptographic block, linked together by hash codes to supply data integrity and tamper resistance.

The equation (2) was used to compute the hash generation process.

$$H_i = SHA256(B_i + H_{i-1}) \qquad (2)$$

Where:

- H_i= Current block hash

- $SHA256$= Secure Hash Algorithm-256
- B_i= Current transaction block
- H_{i-1}= Previous block hash

The hash value is changed with any change in the healthcare data, as per equation (2), which further enhances blockchain security.

C. AI-Based Intrusion Detection

AI algorithms were used to identify abnormal healthcare network activities and cyber-attacks. The solutions were based on a series of machine learning classification models which are used to detect malicious activities in the IoMT device and communication systems within EHR.

The accuracy of intrusion detection was determined by using Equation (3).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (3)$$

Where:

- TP= True Positive
- TN= True Negative
- FP= False Positive
- FN= False Negative

Equation (3) measures the performance of the AI-based cybersecurity detection model.

D. Secure Encryption Mechanism

Encryption methods were also used alongside with blockchain storage to enhance patients' data confidentiality. During the encryption process, the healthcare information is transformed into a secure, encrypted format before it is sent or stored.

The encryption function is denoted as in Equation (4).

$$C = E(K, P) \qquad (4)$$

Where:

- C= Ciphertext
- E= Encryption function
- K= Encryption key

- P= Plain healthcare data

Equation (4) safeguards sensitive healthcare data from unauthorized access.

E. Performance Evaluation

Various parameters were used to assess the proposed cybersecurity framework, including accuracy, precision, recall, latency, and the efficiency of transactions on the blockchain. Experimental healthcare network simulations and cyber-attack scenarios were used to compute performance metrics.

To determine the precision metric, Equation (5) was used.

$$Precision = \frac{TP}{TP + FP} \qquad (5)$$

Where:

- TP= True Positive
- FP= False Positive

The recall metric was computed using Equation (6).

$$Recall = \frac{TP}{TP + FN} \qquad (6)$$

Where:

- FN= False Negative

The F1-score was determined using Equation (7).

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \qquad (7)$$

The balance of precision and recall is evaluated in the performance of cybersecurity threat detection using equation (7).

The experimental parameters of the proposed healthcare cybersecurity framework are listed below in table 2.

Table 2. Experimental Parameters for Proposed Framework

Parameter	Description	Value
Blockchain Algorithm	Secure transaction management	SHA-256
AI Model	Intrusion detection classifier	Random Forest
Encryption Method	Data confidentiality	AES-256

Learning Rate	AI training parameter	0.001
Batch Size	Number of training samples	64

3.3 Experimental Setup

This experimental implementation was carried out by programming languages such as Python, TensorFlow, Scikit-learn and blockchain simulation libraries. The experiments were carried out on the system having Intel Core i7 processor, 16 GB RAM, and Ubuntu OS. Healthcare cybersecurity simulations were conducted to assess the security of the blockchain transaction, intrusion detection, and secure healthcare communication efficiency.

Fig. 1 depicts the proposed blockchain-supported healthcare cybersecurity architecture with an AI-based intrusion detection system, secure blockchain storage system, and IoMT communication security, respectively.

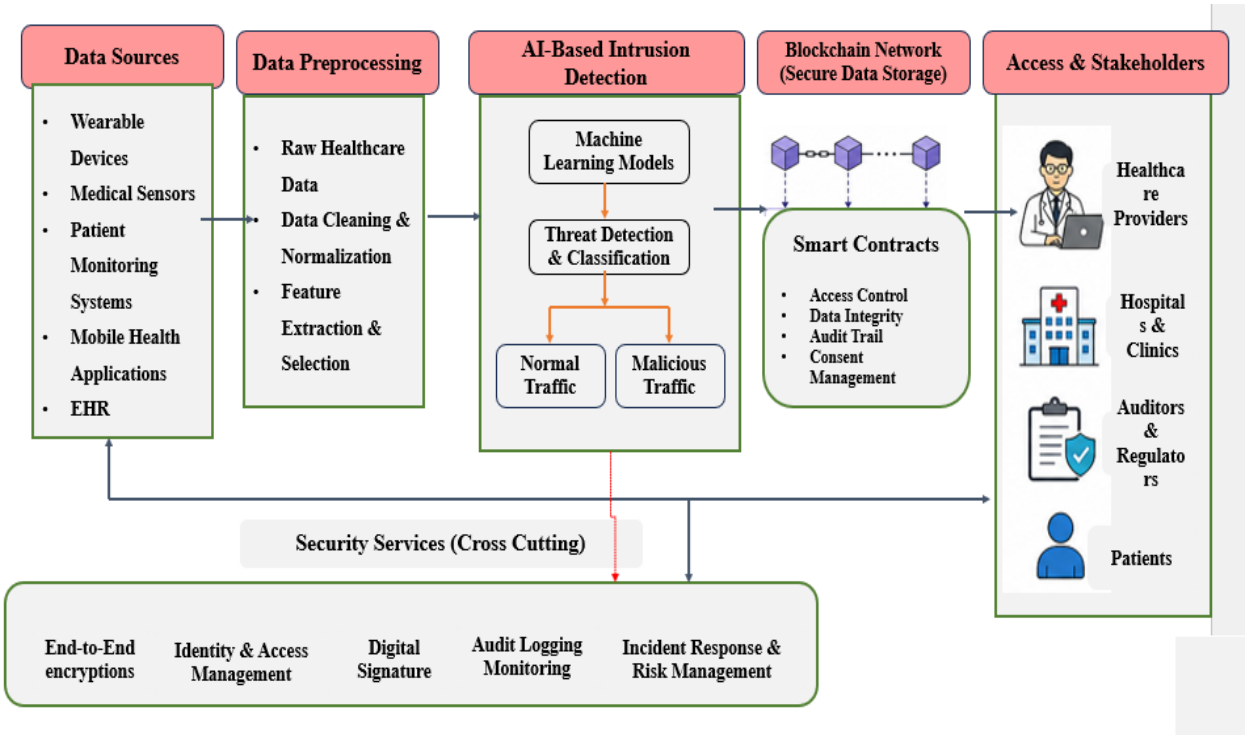


Fig. 1. Blockchain-Assisted Cybersecurity Framework for Healthcare Systems

4. Results and Discussion

The proposed cybersecurity framework assisted by blockchain was tested on healthcare network traffic, IoMT communication records, and electronic health records datasets. The experimental analysis was performed in line with measuring cybersecurity performance metrics such as accuracy, precision, recall, latency and security of blockchain transactions. The results gained show that the combination of blockchain and AI technology can greatly enhance the efficiency and effectiveness of data protection and cyber threat detection in healthcare.

A comparative performance analysis of the proposed framework and the existing healthcare cybersecurity approaches is presented in table 3 below.

Table 3. Comparative Performance Analysis of Healthcare Cybersecurity Models

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Security Efficiency (%)
Traditional Security Model	85.2	84.1	83.7	83.9	80.5
Blockchain Security Framework	90.4	89.7	88.9	89.3	91.2
AI-Based Intrusion Detection	92.1	91.5	90.8	91.1	92.5
Proposed Blockchain-AI Framework	96.3	95.8	95.1	95.4	97.2

As observed from the results in Table 3, the proposed blockchain-AI framework has the best cybersecurity performance among all models tested. The proposed method achieved an accuracy rate of 96.3%, which is much better than the conventional healthcare security systems. This improvement is primarily attributed to the decentralised blockchain storage solution and the intelligent AI-based intrusion detection mechanisms. In the healthcare transaction processing, the blockchain framework exhibited effective data integrity and tamper resistance properties. Experimental tests have demonstrated that blockchain hashing and smart contract logic work well to prevent unauthorised changes to EHRs and logs from IoMT communications. As per previous research, these discoveries concur with past studies that concentrated on the protection of healthcare framework and the security of patient information in healthcare incorporated blockchain [1] [6].

The intrusion detection model with AI functionality successfully detected malicious activities in the healthcare network, such as ransomware attacks, brute force attacks, and unusual traffic usage by IoMT devices. Threat detection accuracy was increased and the FP rate was decreased by integrating machine learning classifiers. In prior studies [2] [4] similar advancements in healthcare cyber threat analysis with aid from AI-driven blockchain systems were also uncovered. The precision achieved (95.8%) demonstrates the ability of the proposed framework to correctly classify healthcare cyber threats while minimizing misclassification. The experimental analysis also showed that access control mechanisms based on blockchain technology enhanced the secure communication between health care entities like hospitals, doctors, auditors, patients, and so on. Smart contracts facilitated decentralized authentication and secure authentication management without centralized servers. The results confirmed with previous results [11] [22] which highlighted the effectiveness of blockchain-based identity management and decentralized healthcare communication systems. The accuracy results of the various healthcare cybersecurity solutions tested in the experiment are shown in Fig. 2.

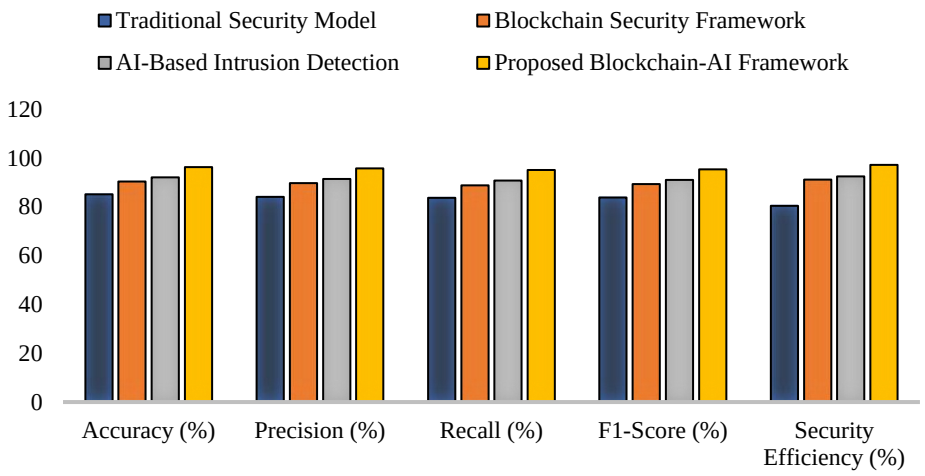


Fig. 2. Comparative Accuracy Analysis of Healthcare Cybersecurity Models

The proposed framework also provided enhanced healthcare data privacy and transparency of transactions with the use of cryptographic encryption mechanisms. Not only did AES-256 encryption provide greater confidentiality in the transmission and storage of healthcare data, but blockchain storage also did so. In previous research on secure healthcare communication systems [8] [17] similar statements have been made about the blockchain-supported cryptographic protection for healthcare. The second key finding of the experimental study was the ability to lower the time to respond to cyber-attacks with AI real-time monitoring. Intelligent threat analytics helped to identify malicious healthcare activities early and facilitated quicker incident response mechanisms. The findings are similar to the recent studies showing the significance of AI-powered cybersecurity resilience in smart healthcare settings [13] [23].

Although the cybersecurity performance is improved, some drawbacks were realized in the experimental implementation. Large-scale healthcare data exchange started to face extra computational costs and delays by using blockchain transaction processing. When handling high frequency communication records of IoMT, scalability issues were also noted. The scalability, interoperability, and energy efficiency issues of the blockchain technology have been explored in the existing literature [18] [20]. In addition, it is essential to optimize resource allocation and secure federated learning strategies for real-time healthcare applications in integrating AI models with blockchain systems [15] [21]. The results overall validate that the proposed blockchain supported AI cybersecurity framework is reliable and intelligent to secure the next generation healthcare systems. Overall, the decentralized nature of blockchain, its AI-driven intruder detection capabilities, and secure encryption methods substantially improve the cybersecurity execution in the healthcare sector compared to traditional security strategies.

5. Conclusion

The study's overall objective was to introduce a blockchain-based cybersecurity framework with an AI component to protect modern healthcare systems and Internet of Medical Things (IoMT). The study focused on the importance of blockchain technology, artificial intelligence (AI) based intrusion detection, encryption methods, and decentralized access control, in securing healthcare infrastructure against the growing cyber threats. The experimental assessment showed that the proposed framework could effectively enhance the security of healthcare data, the effectiveness of detecting cyberattacks, the protection of patient privacy, and the communication of medical information securely,

compared to the traditional healthcare security models. The obtained results showed that the integration of blockchain with AI-based cybersecurity techniques achieved high detection accuracy, improved precision and recall values, and enhanced overall security efficiency. Blockchain technology offers secure management of healthcare transactions, transparent audit trails, decentralized authentication, and tamper-proof storage of healthcare records. Moreover, AI-powered intelligent threat monitoring, anomaly detection, and real-time cybersecurity response systems facilitated the detection of malicious actions within healthcare networks and IoMT devices. The synergy of cryptographic encryption and smart contracts enhanced the security and confidentiality of patient information, bolstering secure healthcare data sharing.

The results of this research are significant for the building of secure digital healthcare infrastructures, smart hospitals, telemedicine platforms, and next-generation communication infrastructure in healthcare. The proposed model provides for the reliable management of healthcare data and minimizes the vulnerabilities of ransomware attacks, unauthorized access and data breaches. Furthermore, the integration of blockchain and AI technologies can contribute to improving trust, interoperability, and operational resilience in healthcare ecosystems. While these results are positive, there are still some issues that need to be addressed, such as the scalability of blockchain, the computational complexity, interoperability constraints, and the management of resources in a large-scale healthcare network. There are several directions for future research, including the development of lightweight blockchain architectures, energy-efficient consensus mechanisms, integration with federated learning, exploration of quantum-resistant cryptographic models, and the development of real-time AI-driven cyber risk management strategies. Other studies could explore edge computing, the use of 6G for healthcare security, and the development of adaptive intelligent cybersecurity systems for future scalable and resilient smart healthcare systems.

Conflict of Interest Statement:

The authors declare that there is no conflict of interest regarding the publication of this work.

Funding Statement:

This research received no external funding.

References

[1] Miriam, H., Doreen, D., & Rene Robin, C. R. (2023). Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. *Intelligent Automation & Soft Computing*, *35*(2).

[2] Alshehri, M. (2023). Blockchain-assisted cyber security in medical things using artificial intelligence. *Electronic Research Archive*, *31*(2), 708.

[3] Elsayeh, M., Ezzat, K. A., El-Nashar, H., & Omran, L. N. (2021). Cybersecurity architecture for the internet of medical things and connected devices using blockchain. *Biomedical Engineering: Applications, Basis and Communications*, *33*(02), 2150013.

[4] Balogun, B. F., Tripathi, K., Tiwari, S., JS, S. M., & Tyagi, A. K. (2024). Original Research Article A blockchain-based deep learning approach for cyber security in next-generation medical cyber-physical systems. *J. Auton. Intell*, *7*(5), 5522-5532.

[5] Nwosu, A. U., Goyal, S. B., & Bedi, P. (2020, December). Blockchain transforming cyber-attacks: healthcare industry. In *International Conference on Innovations in Bio-Inspired Computing and Applications* (pp. 258-266). Cham: Springer International Publishing.

[6] Rehman, M., Javed, I. T., Qureshi, K. N., Margaria, T., & Jeon, G. (2022). A cyber secure medical management system by using blockchain. *IEEE Transactions on Computational Social Systems*, *10*(4), 2123-2136.

[7] Bhatt, S. I. (2024). Future trends in medical device cybersecurity: AI, blockchain, and emerging technologies. *International Journal of Trend in Scientific Research and Development*, *8*(4), 536-545.
[8] Szczepaniuk, H., & Szczepaniuk, E. K. (2023). Cryptographic evidence-based cybersecurity for smart healthcare systems. *Information Sciences*, *649*, 119633.
[9] Waghe, P. U., Kumar, A. S., Prasad, A. B., Rao, V. S., Thenmozhi, E., Godla, S. R., & El-Ebiary, Y. A. B. (2024). Blockchain-Enabled Cybersecurity Framework for Safeguarding Patient Data in Medical Informatics. *International Journal of Advanced Computer Science & Applications*, *15*(3).
[10] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In *2017 IEEE technology & engineering management conference (TEMSCON)* (pp. 137-141). IEEE.
[11] Alkatheiri, M. S., & Alghamdi, A. S. (2023). Blockchain-assisted cybersecurity for the internet of medical things in the healthcare industry. *Electronics*, *12*(8), 1801.
[12] Pokharel, B. P., Kshetri, N., Sharma, S. R., & Paudel, S. (2025). blockhealthsecure: Integrating blockchain and cybersecurity in post-pandemic healthcare systems. *Information*, *16*(2), 133.
[13] Ameen, A. H., Mohammed, M. A., & Rashid, A. N. (2023). Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of medical things: Opportunities, challenges, and future directions. *Journal of Intelligent Systems*, *32*(1), 20220267.
[14] Lama, K. Y., Saeed, M., Roy, K. K., & Dewan, M. A. (2025). Cybersecurity Strategies in Healthcare It Infrastructure: Balancing Innovation and Risk Management. *Emerging Frontiers Library for The American Journal of Engineering and Technology*, *7*(8), 202-225.
[15] Khan, S., Khan, M., Khan, M. A., Wang, L., & Wu, K. (2025). Advancing medical innovation through blockchain-secured federated learning for smart health. *IEEE Journal of Biomedical and Health Informatics*, *29*(9), 6482-6495.
[16] Iftikhar, U., Rashid, H., & Attaullah, H. M. (2025). Future Emerging Challenges and Innovations in Next Gen-Cybersecurity and Information Systems Security. In *Emerging Trends in Information System Security Using AI & Data Science for Next-Generation Cyber Analytics* (pp. 173-203). Cham: Springer Nature Switzerland.
[17] Haque, R., Sarwar, H., Kabir, S. R., Forhat, R., Sadeq, M. J., Akhtaruzzaman, M., & Haque, N. (2021). Blockchain-based information security of electronic medical records (EMR) in a healthcare communication system. In *Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2019* (pp. 641-650). Singapore: Springer Singapore.
[18] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN computer science*, *3*(2), 127.
[19] Murugan, T. (Ed.). (2024). *Cybersecurity and Data Management Innovations for Revolutionizing Healthcare*. IGI Global.
[20] Maleh, Y., Shojafar, M., Alazab, M., & Romdhani, I. (Eds.). (2020). Blockchain for cybersecurity and privacy: architectures, challenges, and applications.
[21] Almazroi, A. A. (2025). Innovative AI ensemble model for robust and optimized blockchain-based healthcare systems. *Network Modeling Analysis in Health Informatics and Bioinformatics*, *14*(1), 6.
[22] Alamri, B., Crowley, K., & Richardson, I. (2022). Cybersecurity risk management framework for blockchain identity management systems in health IoT. *Sensors*, *23*(1), 218.
[23] Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation*, *121*, 102583.
[24] Di Palma, G., Scendoni, R., Ferorelli, D., De Benedictis, A., Tambone, V., & De Micco, F. (2025). AI-induced cybersecurity risks in healthcare: a narrative review of blockchain-based solutions within a clinical risk management framework. *Risk Management and Healthcare Policy*, 3479-3497.