Journal of Advanced Health Informatics Research (JAHIR)
Vol. 2, No. 2, (2024), pp. 75-84
ISSN: 2985-6124, DOI: 10.59247/jahir.v2i2.290

Exploring Blockchain as a Security Framework for IoT in Healthcare: A Systematic Literature Review

Lutviana [1], Iis Setiawan Mangkunegara [2], Hamzah M. Marhoon [3]
[1,2] *Informatics, Universitas Harapan Bangsa, Indonesia*
[3] *College of Information Engineering, Al-Nahrain University, Iraq*

ARTICLE INFO

Article history:

Received February 09, 2024
Revised July 16, 2024
Published September 18, 2024

Keywords:

Blockchain;
Security;
IoT;
Healthcare;
Review

ABSTRACT

This systematic literature review explores the use of blockchain technology to improve the security of communication between IoT devices in the healthcare sector. The integration of IoT in healthcare has revolutionized patient data management but introduced security challenges. Blockchain, as a decentralized and immutable ledger, offers a potential solution by providing a secure method of data storage and transmission. This review analyzed 62 relevant studies published in the last five years using the PRISMA methodology. The main contributions of blockchain include improved data security, privacy, and data integrity, with decentralization and cryptographic techniques ensuring patient data remains secure and accessible only to authorized entities. Challenges of blockchain implementation include interoperability, data storage efficiency, and the need for strong cryptographic algorithms. Proposed solutions include the development of a specialized blockchain framework for healthcare, the integration of advanced encryption methods, and the use of distributed ledger technology to manage electronic medical records. Further research is needed to develop more efficient and secure blockchain solutions in healthcare applications, including improved interoperability, encryption algorithms, and real-world case studies. Although challenges remain, blockchain has great potential to improve the communication security of IoT devices in the healthcare sector.

Corresponding Author:

Lutviana, Department of Informatics, Universitas Harapan Bangsa, Purwokerto, Indonesia
Email: luthvianna41@gmail.com

1. INTRODUCTION

1.1 Background

Real-time connectivity and communication between medical devices have been made possible by the Internet of Things (IoT), which has completely changed the healthcare industry [1]. IoT devices, such as heart monitors and glucose sensors, enable continuous patient data collection and remote surveillance, improving diagnosis and treatment [2]. Significant security challenges are presented by the adoption of IoT technology due to the limited computing capacity and power of IoT devices, making traditional security protocols difficult to implement [3]. IoT devices are vulnerable to cyberattacks, which threaten the integrity and privacy of patient data [4].

A potential solution to these security challenges is offered by blockchain. As a distributed ledger technology, blockchain provides a secure, transparent, and immutable mechanism for recording transactions. With this, the security of communication between IoT devices can be enhanced [5]The decentralized nature of blockchain protects data from threats such as eavesdropping and data manipulation [6]. Automatic permission and access control of devices can be granted by smart contracts that run automatically when certain conditions are met. Only authorized entities can access or change data, ensuring that data access and changes are controlled [7] [8]. Smart contracts can also verify the identity of IoT devices and prevent unauthorized access [7].

Blockchain implementation provides a transparent and verifiable audit trail and is essential for compliance with healthcare regulations such as the Health Insurance Portability and Accountability Act (HIPAA) [9]. This audit trail enables real-time tracking and verification of every transaction or data change [10]. Blockchain uses robust cryptographic mechanisms to protect data during transmission and storage, reducing the risk of data theft or manipulation [11] [12]. The use of cryptographic keys and hashing algorithms ensures data cannot be altered without detection, providing an additional layer of security [13].

Blockchain can improve trust and traceability in health data management [14] [15]. This traceability enables tracking and verification of every step in the data process, assisting in auditing and regulatory compliance [16]. Blockchain is emerging as an attractive solution to address IoT security challenges in the healthcare ecosystem, offering significant improvements in technical security, regulatory compliance, trust, and traceability, and supporting the evolution of IoT-based health system.

1.2 Research Question (RQ)

This research explores the application of Blockchain technology as a security framework for IoT in the healthcare sector. Several key research questions have been designed to focus on identifying the benefits, challenges, and limitations in Blockchain implementation in this systematic review. Through an in-depth literature search and rigorous analysis, comprehensive insights into the role of Blockchain in enhancing the security of IoT devices in healthcare are expected to be gained. These research questions help direct the research, analyze the findings, and identify areas that require further research in the future.

RQ1: How Blockchain is being used to improve the security of communication between IoT devices in the healthcare ecosystem?

RQ2: What are the key benefits of using Blockchain in securing communication between IoT devices in the healthcare sector?

RQ3: What are the challenges and limitations faced in Blockchain implementation for IoT security in healthcare?

RQ4: What solutions are proposed or developed to overcome these challenges and limitations?

RQ5: How does the effectiveness of Blockchain-based solutions compare to traditional security methods in the context of IoT communications in healthcare?

RQ6: What are the latest research trends and future directions in the use of Blockchain for IoT security in the healthcare sector?

This study answers these questions with the hope of significantly contributing to the understanding of the application of Blockchain technology as a security solution for IoT in the healthcare sector. This study is also expected to pave the way for further research and implementation.

2. METHODS

2.1. Review Protocol

The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-analyses) approach was used in this study to ensure a systematic and transparent literature review process. PRISMA is an international guideline that provides a framework for conducting systematic reviews [17]. This research followed the PRISMA flow chart which involved four main phases of identification namely, screening, eligibility, and inclusion [18].

2.2. Inclusion and Exclusion Criteria

One way to ensure this systematic review includes the most relevant and high-quality studies is to carefully establish inclusion and exclusion criteria. These criteria were established to screen literature that fit

the research focus and study objectives, while excluding studies that were irrelevant or did not meet the required methodological standards. Table 1 lists the inclusion and exclusion criteria used.

Table 1. Inclusion and Exclusion Criteria

Inclusion	Exclusion
Studies that address the application of Blockchain technology in enhancing IoT security in the healthcare sector.	Studies that do not focus on the application of blockchain in the healthcare or IoT sectors
Articles published in peer-reviewed journals or scientific conferences in the last 5 years	Articles that do not provide verifiable data or findings.
Studies written in English.	Non-peer-reviewed studies, including opinion articles, editorials, surveys, reviews, books and unverified industry reports.
Research that includes empirical analysis, theoretical studies, or case studies relevant to the research topic.	Incomplete publications such as not having clear results or research findings or inactive DOIs.

2.3. Data Sources and Search Strategy

This literature review utilizes credible data sources such as PubMed, ACM Digital Library, IEEE Xplore, Scopus, and Google Scholar to ensure completeness and relevance. These databases were chosen due to their extensive coverage in publications related to Blockchain, IoT, and the healthcare sector. The search strategy used the keywords "Blockchain", "Internet of Things", "IoT", "Healthcare", and "Security" combined with Boolean operators (AND, OR) to cover relevant variations. The search was conducted in several stages: an initial search based on titles and abstracts, further screening by reading the full text, and reviewing the reference lists of selected articles to find additional studies. This approach aims to collect the most relevant and high-quality literature, providing an in-depth understanding of the application of Blockchain as a security framework for IoT in the healthcare sector.

2.4. Study Selection Process

The study selection process in this systematic review followed PRISMA guidelines to ensure transparency and reproducibility. Four main stages were followed: identification, screening, eligibility assessment, and inclusion. Relevant studies were retrieved from databases, screened to eliminate duplication, and titles and abstracts were checked for criteria appropriateness. Studies that passed the screening were evaluated in detail and independently by several researchers. Studies that met all criteria were included in the final analysis, with inclusion or exclusion decisions documented in detail. The PRISMA flowchart in Figure 1 shows this study selection process.

2.5. Data Extraction

This systematic literature review's data extraction phase adheres to PRISMA principles and is an essential phase. Key information from the selected studies was collected in a systematic and structured manner, including bibliography, research objectives, study design, data collection and analysis methods, and key findings. Data extraction was conducted using standardized forms to minimize bias and ensure consistency. The extracted data was organized in tables to identify relevant patterns, themes, and conclusions, ensuring all critical information was integrated for valid conclusions on the applicability of Blockchain as a security framework for IoT in the healthcare sector.

2.6. Analysis Methodology

The analysis process began with data extraction from the selected studies, including authors, year of publication, research objectives, methods and key findings. A structured data extraction form ensured consistency and completeness. After extraction, study quality was assessed using a critical appraisal tool that assessed internal and external validity based on research design, methodology, data analysis, and relevance of findings.

The extracted and assessed data were then analyzed qualitatively and quantitatively. Qualitative analysis identified key themes and patterns in the data, using thematic analysis techniques to organize the data into meaningful categories. Quantitative analysis involved coding the data and using descriptive statistical methods to summarize study characteristics. Where possible, a meta-analysis was conducted to combine results from multiple studies.

The results of the analysis were synthesized to provide a comprehensive picture of the application of Blockchain in IoT security in the healthcare sector, integrating qualitative and quantitative findings to thoroughly

answer the research questions. This methodological approach aims to make a significant contribution to the literature and practice in the field.

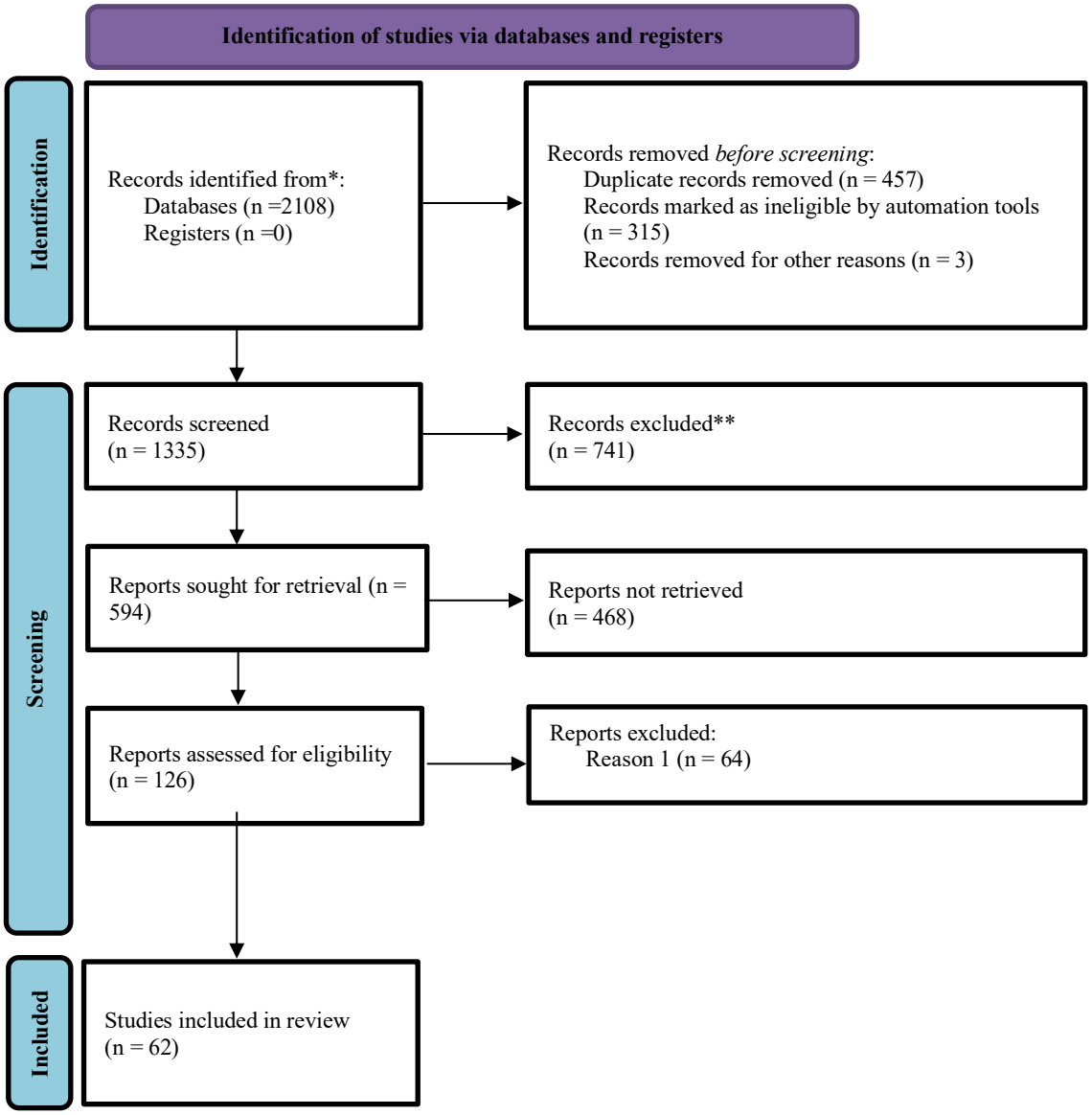

Fig. 1. PRISMA Flowchart

3. RESULTS

3.1. PRISMA Diagram

Based on Figure 1, 2,108 articles were identified through database and registry searches. Of these, 457 duplicate articles were removed, leaving 1,651 articles for further assessment. Furthermore, 315 articles of the "Survey" or "Review" type were also removed. At this identification stage, 3 articles of the "Book" type were also removed, leaving 1,335 articles for the screening process.

During the screening stage, 741 articles were excluded for not meeting the inclusion criteria, leaving 594 articles eligible for full-text assessment. Of these, 468 articles did not have an active DOI, which left 126 articles that were considered eligible. Upon further review, it was found that 74 articles were not related to the health sector theme, and there were still 62 "Survey" or "Review" articles. Finally, 62 articles were included in the

systematic review. These studies were deemed relevant and met all inclusion criteria set out in the review protocol.

3.2. Characteristics of Included Studies

3.2.1 Most Cited Publications

The table shows each of the most cited documents. Global citations refer to the annual citation rate at the time the data set used in this study was extracted. Based on Figure 2, the article titled "Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals" [19] is the article with the highest number of citations. This article proposes a platform to monitor patient vital signs using smart contracts on a private blockchain network developed with hyperledger infrastructure.

The article with the title "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems" [20] became the second most cited article with 274 citations. This research develops Decentralized Interoperable Trust (DIT) and Indirect Trust Inference System (ITIS). The contribution offered from the research is a semantic data model for managing IoT objects and metadata. The proposed framework aims to maintain data security in healthcare IoT systems.

The article with the title "Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain" [21] became the article with the third highest number of citations with 223 citations. The research that has been done contributes to the creation of decentralized authentication using blockchain in distributed hospital networks. The results of the research that has been carried out show an increase in throughput, reduction in overhead, faster response time and lower energy consumption.

The article entitled "Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems" [22] became the fourth most cited article with 212 citations. The resulting contribution is the integration of permissioned blockchain and smart contracts on health data. In addition, this study integrates self-attention-based bidirectional long short term memory (SA-BILSTM) with stacked sparse variational autoencoder (SSVAE). Under this method, SA-BiLSTM detects and enhances the attack detection process, while SSVAE encodes or transforms healthcare data into a new format. The benefits of the PBDL framework over current state-of-the-art methods are confirmed by security analysis and experimental results utilizing IoT-Botnet and ToN-IoT datasets.

The article with the title "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control" [23] became the fifth most cited article with 211 citations. This article proposes a blockchain-based architecture for decentralized IoMT healthcare systems. It also introduces a hybrid computing paradigm and a distributed data storage system.

Table 2. Most Cited Publication

Title	Citation
Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals	290
DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems	274
Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain	223
Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems	212
Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control	211

3.2.2 Most Productive Country

Table 3. Most Productive Country by Frequency

Country	Frequency
Amerika Serikat	16
India	14
Pakistan	6
Arab Saudi	5
China	5
Inggris	4
Indonesia	2
Malaysia	2
Maroko	1
Yordania	1

Table 4. Most Productive Country by Citation

Country	Citation
India	1020
Amerika Serikat	416
Inggris	333
South Korea	290
Egypt	274
Canada	223
Saudi Arabia	213
Pakistan	207
China	204
Australia	130

3.2.3 Most Productive Institution

Institutions with relevant publication productivity are presented in Table 5. Based on the table, Stanford University has the most publications with 6 articles. The second place is Massachusetts Institute of Technology (MIT) with 6 articles. The third place is the National Institute of Technology with 4 articles. Based on Table 6, Jeju National University is the institution with the highest number of citations with 290 citations. The second place is Menoufia University with 274 citations, and the third place is the National Institute of Technology with 239 citations.

Table 5. Most Productive Institution by Frequency

Institution	Frequency
Stanford University	6
Massachusetts Institute of Technology (MIT)	6
National Institute of Technology	4
Taif University	2
University of Cambridge	2
Massachusetts Institute of Technology	2
Universitas indonesia	1
Politehnica University	1
National Institute of Technology	1
Dawood University	1

Table 6. Most Productive Country by Citation

Institution	Citation
Jeju National University	290
Menoufia University	274
National Institute of Technology	239
University Guelph	223
SRM University	211
Graphic Era University	194
Massachusetts Institute of Technology (MIT)	177
Newcastle University	158
Deakin University	130
Edinburgh Napier University	117

3.2.4 Most Frequent Keywords

The occurrence and relevance of widely used keywords in the selected publications can be analyzed based on the inclusion criteria of this study. Table 7 lists the most searched keywords by researchers interested in the topic “Exploring Blockchain as a Security Framework for IoT in Healthcare”. Based on Table 7, “blockchain” is the most frequently occurring keyword in the included articles with a total of 49. Furthermore, “iot” with a total of 21, “security” with a total of 19, “healthcare” with a total of 12, “medical services” with a total of 8, “authentication” with a total of 8, “internet of medical things” with a total of 7, “privacy” with a total of 5, and the remaining keywords appear 4 times from all included articles.

Table 7. Top 10 Most Searced Keyword

Keyword	Count
blockchain	49
Iot	21
security	19
healthcare	12
medical services	8
authentication	8
internet of medical things	7
privacy	5
data security	4
internet of things	4
data privacy	4
healthcare system	4

3.3. Answers to Research Questions

The formulated research questions were answered based on the results of the analysis process of relevant articles according to the inclusion criteria. Each research question is answered by referring to the findings of the analyzed studies and synthesizing relevant data. This aims to provide a deep and comprehensive insight into the topic under study. The answers to these questions are expected to add to the scientific understanding of the field and can be further enhanced through contributions from the analysis of existing research findings.

Table 8. Answers to Research Questions

Research Question	Answer
RQ1: How can Blockchain be used to improve the security of communication between IoT devices in the healthcare ecosystem?	Blockchain is used to improve the security of communication between IoT devices in the healthcare ecosystem by managing and securing data in a decentralized manner. For example, the Blockchain-based IoMT Authenticated Key Exchange (BIoMTAKE) protocol [24] uses Hyperledger Fabric to ensure secure access to IoMT data through authenticated key exchange.
RQ2: What are the key benefits of using Blockchain in securing communication between IoT devices in the healthcare sector?	Manfaat utama dari penggunaan Blockchain dalam the key benefits of using Blockchain in securing communication between IoT devices in the healthcare sector include improved data privacy and security, reduced risk of cyberattacks, improved data integrity, and increased transparency and efficiency in health data management. For example, Optimized Data Management and Secured Federated Learning (ODMSM-FL) [25] improves data management, privacy, and integrity of patient data in the IoMT ecosystem.
RQ3: What are the challenges and limitations faced in Blockchain implementation for IoT security in healthcare?	Challenges and limitations in Blockchain implementation for IoT security in healthcare include system complexity, high computing resource requirements, scalability challenges, and reliance on blockchain technology and smart contracts that may have vulnerabilities. For example, the challenge of ensuring all IoT devices can support and effectively implement the BIoMTAKE protocol in scenarios with large volumes of data and different types of devices.
RQ4: What solutions are proposed or developed to overcome these challenges and limitations?	The proposed solutions to overcome the challenges and limitations in Blockchain implementation for IoT security in healthcare include the development of more efficient consensus mechanisms such as Verifiable Random Ranking based Secure Blockchain Consensus (VRR-SBC) [26], as well as the use of federated learning[25] to maintain data privacy during the machine learning process. Also, the implementation of Ciphertext-Policy Attribute-Based Encryption

	(CP-ABE) encryption and attribute-based key management mechanisms to address the security issues of encryption keys
RQ5: How does the effectiveness of Blockchain-based solutions compare to traditional security methods in the context of IoT communications in healthcare?	The effectiveness of Blockchain-based solutions compared to traditional security methods in the context of IoT communications in healthcare shows significant improvements in terms of consensus speed, data security, and reduced verification costs. For example, the VRR-SBC algorithm shows improvements in consensus speed and security compared to conventional consensus algorithms
RQ6: What are the latest research trends and future directions in the use of Blockchain for IoT security in the healthcare sector?	The integration of blockchain technology with federated learning, the use of post-quantum encryption [28] to strengthen security against quantum computing threats, and the creation of a metaverse framework for remote health monitoring and virtual consultations are some recent research trends and future directions in the use of Blockchain for IoT security in the healthcare sector.

4. DISCUSSION

4.1. Synthesis of Key Findings

The Internet of Medical Things (IoMT) ecosystem offers important ways to enhance data security and privacy in the healthcare industry. One such way is through the application of blockchain technology. Blockchain enables more secure and decentralized data management, reducing the risk of cyberattacks and data leakage through advanced authentication and consensus mechanisms. The main benefits of this technology are improved data integrity, transparency, and efficiency in health data management.

Blockchain implementation faces challenges such as system complexity, high computing resource requirements, and scalability and interoperability issues. Proposed solutions include more efficient consensus mechanisms and the use of encryption to improve key security. The effectiveness of blockchain over traditional security methods has been proven through studies, which show increased consensus speed, data security, and reduced verification costs.

Recent research trends show promising directions with the integration of blockchain and federated learning, as well as the use of post-quantum technology for future security. The potential for blockchain to revolutionize security and privacy in the IoT ecosystem is immense and promises more extensive research and implementation in the future.

4.2. Practical Implications

The security and privacy of patient data in the healthcare industry can be greatly enhanced by the use of blockchain technology in the IoMT ecosystem. Blockchain enables hospitals and healthcare providers to manage sensitive medical data more securely and transparently, reducing the risk of cyberattacks and data leakage. Efficient consensus mechanisms such as VRR-SBC and advanced encryption such as CP-ABE optimize data authentication and verification processes, enabling fast and secure communication between IoT devices. Federated learning enables distributed learning without sharing raw data, maintaining patient data privacy and improving healthcare quality through data analysis. The integration of blockchain technology in IoT not only enhances security and privacy, but also drives operational efficiency and innovation in the healthcare system, providing direct benefits to patients and healthcare providers.

4.3. Review Limitations

This review process has several limitations that need to be considered. First, limited access to the full literature may affect the scope of the studies reviewed, as some articles may not be available in full. Second, the search and study selection methods may not include all relevant research, and language bias may occur as only English-language articles were included. Third, varying study quality, such as inconsistent methodology and small sample sizes, may affect the validity of the findings. Finally, limitations in data analysis and synthesis of findings, including time and resource constraints, limit the ability to conduct a more in-depth meta-analysis. Although this review provides valuable insights into the use of blockchain in IoT communication security in the healthcare sector, the results should be considered with these limitations in mind. Further research with more robust study designs, broader literature access, and more comprehensive analysis methods is needed to strengthen these findings.

4.4. Future Research Directions

Future research into the use of blockchain for IoT security in the healthcare sector should focus on a few key areas. First, increased scalability and efficiency with better consensus algorithms, such as sharding and off-chain processing. Second, integration of post-quantum encryption to protect against quantum computing threats. Third, the development of interoperability standards to enable efficient communication and data exchange between blockchain platforms and IoT devices. Fourth, improved sustainability and energy efficiency with eco-friendly solutions such as proof-of-stake algorithms. Fifth, improved privacy and regulatory compliance through advanced data anonymization and access control technologies. Sixth, development of practical clinical applications such as remote patient monitoring and electronic health record (EHR) management through case studies and field trials. Finally, focus on security and resilience to cyberattacks with AI-based anomaly detection. Developing these areas will maximize the potential of blockchain technology in improving the security, efficiency, and quality of healthcare services in the IoMT ecosystem.

5. CONCLUSION

Enhancing data security, privacy, and operational efficiency in the healthcare sector is expected to be made possible by the incorporation of blockchain technology into the Internet of Medical Things (IoMT) ecosystem. The decentralized and irreversible ledger of blockchain technology enhances data integrity and transparency, effectively tackling important issues like data leakage and cyberattacks. Advanced encryption and consensus methods offered by blockchain facilitate secure communication and authentication between IoT devices. In the face of obstacles pertaining to system complexity, scalability, and interoperability throughout its deployment in the healthcare industry, attempts are still being made to improve scalability by using post-quantum encryption to counteract new threats and to improve scalability through creative consensus methods. Moreover, efforts are underway to develop interoperability standards in order to enable smooth data transfer between various blockchain systems and Internet of Things devices. Research priorities for the future will include investigating useful applications like electronic health record management and remote patient monitoring, as well as enhancements in sustainability, energy efficiency, and regulatory compliance. Improvements in AI-based anomaly detection are also focused on strengthening resistance against cyber threats, guaranteeing strong security protocols in the IoMT ecosystem.

REFERENCES

[1] N. Tariq, A. Qamar, M. Asim, and F. A. Khan, “Blockchain and Smart Healthcare Security: A Survey.” May 2020. doi: 10.1016/j.procs.2020.07.089.
[2] X. Yang, S. Nazir, H. U. Khan, M. Shafiq, and N. Mukhtar, “Parallel Computing for Efficient and Intelligent Industrial Internet of Health Things: An Overview.” May 2021. doi: 10.1155/2021/6636898.
[3] H. W. S. Z. C. G. W. S. W. C. Z. L. Y. F. S. W. Guoyan, “Security and Privacy in the Medical Internet of Things: A Review.” May 2018. [Online]. Available: https://www.hindawi.com/journals/scn/2018/5978636/
[4] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, “An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security.” May 2020. doi: 10.1109/jiot.2020.2997651.
[5] O. Delgado-Mohatar, R. Tolosana, J. Fiérrez, and A. Morales, “Blockchain in the Internet of Things: Architectures and Implementation.” May 2020. doi: 10.1109/compsac48688.2020.0-131.
[6] X. Peng, X. Zhang, X. Wang, H. Li, J. Xu, and Z. Zhao, “Multi-Chain Collaboration-Based Information Management and Control for the Rice Supply Chain.” May 2022. doi: 10.3390/agriculture12050689.
[7] Z. Ma, L. Wang, W. Xiaochang, Z. Wang, and W. Zhao, “Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data.” May 2020. doi: 10.1109/jiot.2019.2960526.
[8] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, “Smart contract-based access control for the internet of things,” *IEEE Internet Things J*, vol. 6, no. 2, pp. 1594–1605, Apr. 2019, doi: 10.1109/JIOT.2018.2847705.
[9] U. Jafar, M. J. A. Aziz, and Z. Shukur, “Blockchain for Electronic Voting System—Review and Open Research Challenges.” May 2021. doi: 10.3390/s21175874.
[10] B. M. R. Philippe, “Blockchain technology for improving clinical research quality - Trials.” May 2017. [Online]. Available: https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z
[11] J. Gong, Y. Mei, X. Feng, H. Hong, Y. Sun, and Z. Sun, “A data privacy protection scheme for Internet of things based on blockchain.” May 2020. doi: 10.1002/ett.4010.
[12] T. Xu, Z. Fu, M. Yu, J. Wang, H. Liu, and T. Qiu, “Blockchain Based Data Protection Framework for IoT in Untrusted Storage.” May 2021. doi: 10.1109/cscwd49262.2021.9437831.
[13] X. Peng, X. Zhang, X. Wang, H. Li, J. Xu, and Z. Zhao, “Construction of rice supply chain supervision model driven by blockchain smart contract.” May 2022. doi: 10.1038/s41598-022-25559-7.
[14] H. Echchaoui, B. Roumaissa, and R. Boudour, “A Proposal of Blockchain and NFC-Based Electronic Voting System.” May 2023. doi: 10.1007/978-3-031-21216-1_7.

[15] F. K. Nishi *et al.*, "Electronic Healthcare Data Record Security Using Blockchain and Smart Contract." May 2022. doi: 10.1155/2022/7299185.
[16] C. W. M. N. L. L. M. Sean, "Blockchain Compliance by Design: Regulatory Considerations for Blockchain in Clinical Research." May 2019. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fbloc.2019.00018/full
[17] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.
[18] K. Hutchings, R. Bainbridge, K. Bodle, and A. Miller, "Determinants of Attraction, Retention and Completion for Aboriginal and Torres Strait Islander Higher Degree Research Students: A Systematic Review to Inform Future Research Directions," *Res High Educ*, vol. 60, no. 2, pp. 245–272, Mar. 2019, doi: 10.1007/s11162-018-9511-5.
[19] F. Jamil, S. Ahmad, N. Iqbal, and D.-H. Kim, "Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals," *Sensors*, vol. 20, no. 8, p. 2195, 2020, doi: 10.3390/S20082195.
[20] E. M. Abou-Nassar, A. M. Iliyasu, P. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. A. El-Latif, "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020, doi: 10.1109/ACCESS.2020.2999468.
[21] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain," *IEEE J Biomed Health Inform*, vol. 24, no. 8, pp. 2146–2156, 2020, doi: 10.1109/JBHI.2020.2969648.
[22] "Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems," *IEEE Trans Industr Inform*, vol. 18, no. 11, pp. 8065–8073, 2022, doi: 10.1109/tii.2022.3161631.
[23] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control," *IEEE Internet Things J*, vol. 8, no. 14, pp. 11717–11731, 2021, doi: 10.1109/JIOT.2021.3058946.
[24] A. Tomar, N. Gupta, D. Rani, and S. Tripathi, "Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system," *Internet of Things*, vol. 23, p. 100849, Oct. 2023, doi: 10.1016/j.iot.2023.100849.
[25] R. Ramani, A. Rosline Mary, S. Edwin Raja, and D. Arun Shunmugam, "Optimized data management and secured federated learning in the Internet of Medical Things (IoMT) with blockchain technology," *Biomed Signal Process Control*, vol. 93, p. 106213, Jul. 2024, doi: 10.1016/j.bspc.2024.106213.
[26] M. Pundlik, D. Sukheja, S. Nagini, and K. Choudary, "Innovating Healthcare IoT with a Secure Blockchain Consensus Algorithm based on Verifiable Random Ranking," *Procedia Comput Sci*, vol. 230, pp. 264–274, 2023, doi: 10.1016/j.procs.2023.12.082.
[27] A. Xiang, H. Gao, Y. Tian, L. Wang, and J. Xiong, "Attribute-based key management for patient-centric and trusted data access in blockchain-enabled IoMT," *Computer Networks*, vol. 246, p. 110425, Jun. 2024, doi: 10.1016/j.comnet.2024.110425.
[28] K. Mansoor, M. Afzal, W. Iqbal, Y. Abbas, S. Mussiraliyeva, and A. Chehri, "PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems," *Internet of Things*, p. 101228, May 2024, doi: 10.1016/j.iot.2024.101228.