https://doi.org/10.31436/ijpcc.v11i1.513

The Use of Blockchain in Internet of Medical Things (IoMT)

Haifa Alotaibi, Rana Alaklab, M M Hafizur Rahman
Department of Computer Networks and Communications, King Faisal University, Al-Hofuf, Al-Ahsa 31982, Saudi Arabia

*Corresponding author mhrahman@kfu.edu.sa

(Received: 6th December, 2024; Accepted: 26th December, 2024; Published on-line: 30th January, 2025)

Abstract— The goal of this current study is to address important concerns about data security, privacy, and integrity by amalgamating blockchain technology with the Internet of Medical Things. The IoMT ecosystem consists of wearables, implanted sensors, and remote monitoring tools that generate sensitive medical data continuously, revealing several security vulnerabilities. Blockchain, with its principles of decentralization, transparency, immutability, and cryptographic security, opens up new avenues for securing health data without the use of third-party authorities. This paper outlines the methodology used in this review, including a systematic analysis of relevant literature, utilizing the PRISMA framework to evaluate sources. The analysis identifies key protocols and components of blockchain relevant to IoMT, highlights challenges, and provides solutions. Key findings emphasize blockchain's ability to reduce attacks using distributed ledgers, permissioned access, and encrypted transactions. Furthermore, blockchain may improve patient care by providing real-time data exchange and enabling interoperability across health systems.

Keywords— Blockchain, IoMT, healthcare security, privacy, encryption, interoperability, data management

I. Introduction

Standardized data exchange reinforces clinical decision-making because health professionals will always ensure access to updated and correct patient information [1]. The purpose of the study is to discuss how blockchain technology can be one of the major components in IoMT systems, secure and efficient ones, by stressing how it might solve some of the security and privacy issues when it comes to managing medical data, or how this technology could protect patients' privacy [2]. It further investigates the practical challenges to integrating blockchain into large-scale healthcare systems, including technological complication, cost, and compliance with regulations. Blockchain can improve the overall security of IoMT systems, thereby opening up creative solutions for both medical research and healthcare data management using encryption techniques and decentralized networks [3].

A successful integration of blockchain and IoMT may bring a sea change in healthcare delivery by offering transparent and impregnable data management. It can also be opening up new avenues of collaboration between researchers, insurance companies, and healthcare institutions by guaranteeing secure flow and protection of patient privacy [4]. This is necessary for meeting the legal and ethical criteria when it concerns blockchain-based solutions. In other words, IoMT and blockchain together can pave the path to a more secure, faster, and faultless environment in healthcare for better possibilities in patient care, research based on more reliable data, and therapy personalized. There is greater effort on enhancing health care systems to reach the demand of the patients due to the rapidly developing wearable technologies, wireless connectivity, and implanted sensors. These developments have targeted the continuous and remote patient monitoring while making it decentralized and digitized. Wearables include smartwatches, continuous glucose monitors, ECG sensors, and remote patient monitoring systems that generate enormous data streams at real-time levels [5-6]. These are biometric signals, input from environmental sensors, medical imagery, and patient health records-good examples that can provide time-critical interventions in case scenarios dealing with the health status of a patient. Data such as these can clear the way for healthcare professionals to manage chronic ailments better, early disease diagnosis, and personalized treatment schemes. In addition, remote monitoring technologies continually push the boundaries on standards of treatment by lessening unnecessary hospitalizations and improving patient outcomes [7].

However, the volume and sensitivity of medical data raise several concerns about privacy, security, data management, and interoperability. Sharing healthcare data among multiple stakeholders, such as patients, insurance companies, healthcare providers, and linked devices, raises a variety of trust and illegal access issues [8]. Therefore, the increasing IoMT adoption brings about many threats; in turn, strong security measures are required for the protection of patient privacy and integrity. Medical data breaches or poor handling can lead to severe consequences, such as a loss of trust among patients, litigation issues, and even adverse health consequences. It is thus very important to create secure, transparent, and trustworthy healthcare data ecosystems. Because of its nature, blockchain technology has become a feasible manner in which to overcome these challenges [9]. At first, blockchain technology was used to secure bitcoin transactions; however, today it has evolved as an effective tool in the management and handling of complicated data scenarios. The decentralized nature of blockchain makes alteration or tampering with the data impossible because no one single party would have the complete set of data. Transparency and traceability are added, as every transaction is encrypted and timestamped, with each being verified by the entire network involved. Once data has been entered into the blockchain, the system is virtually unalterable, therefore being a secure means of storing medical information. Since healthcare data management requires strict integrity and confidentiality standards, blockchain pertains especially to this type of data management.

II. Research Methodology

The PRISMA flow diagram describes the study selection process for this review. Initial database searching identified 1,006 records. After excluding 220 records—150 duplicates, 50 automation tool-eligible records, and 20 excluded for other reasons—786 records remained to be screened. After the relevance screening, in the screening phase, a total of 756 records were excluded, and 30 reports were left to retrieve. Of these, 5 reports could not be retrieved due to accessibility issues, thus leaving 25 reports to assess for eligibility.

The eligibility assessment excluded 23 reports on the following grounds: 10 reports on the ground of not meeting the inclusion criteria

- Reason 1 8 due to incomplete data
- Reason 2 and 5 on account of methodological limitations
- Reason 3 Finally, 30 studies met the eligibility criteria and were therefore included in this review.

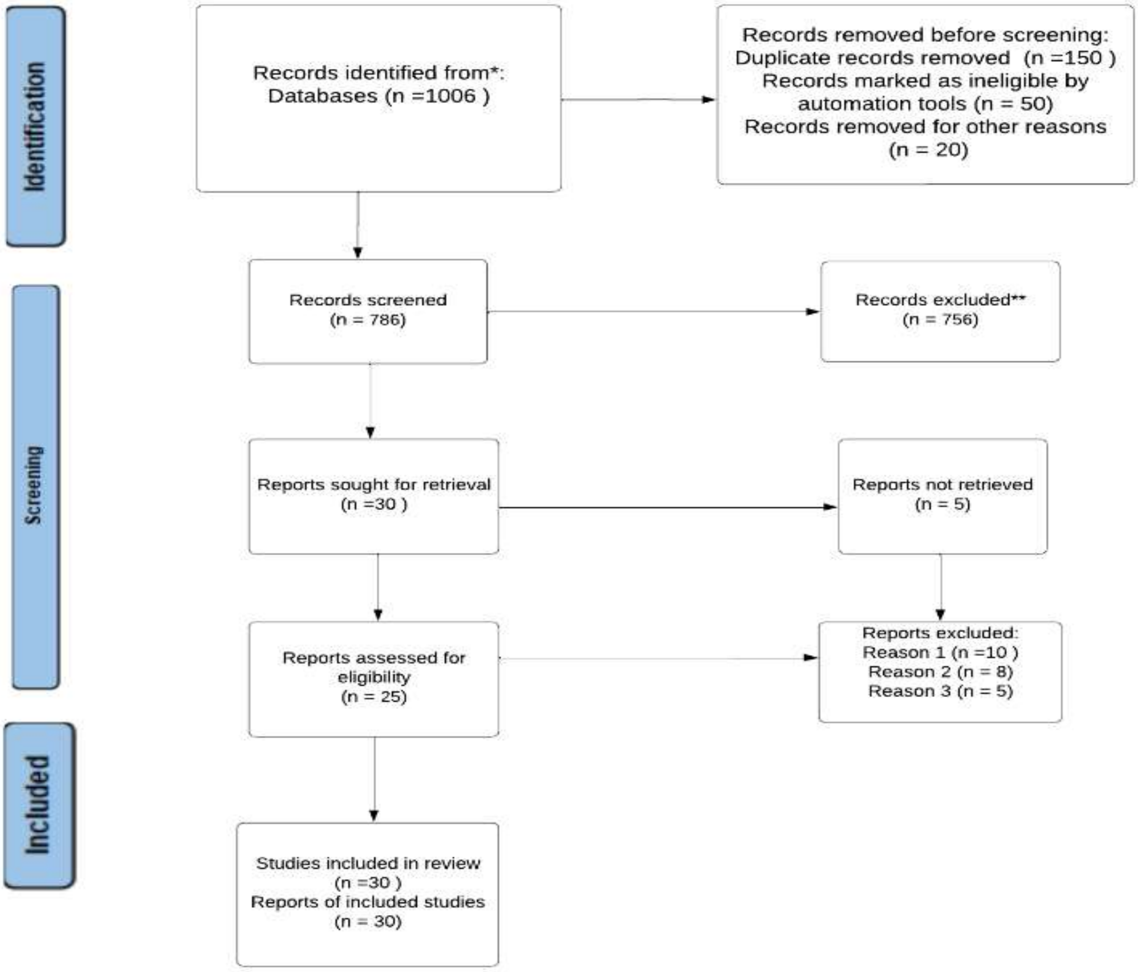
Identification
Screening
Included
Records identified from*:
Databases (n =1006)
Records removed before screening:
Duplicate records removed (n =150)
Records marked as ineligible by automation tools (n = 50)
Records removed for other reasons (n = 20)
Records screened (n = 786)
Records excluded** (n = 756)
Reports sought for retrieval (n =30)
Reports not retrieved (n = 5)
Reports assessed for eligibility (n = 25)
Reports excluded:
Reason 1 (n =10)
Reason 2 (n = 8)
Reason 3 (n = 5)
Studies included in review (n =30)
Reports of included studies (n = 30)

Fig 1: PRISMA Flow Diagram of Study Selection

III. *Related works*

Blockchain is "adecentralized and immutable ledger that securely and transparently records transactions, eliminating the need for a central authority." Blockchain applications in the healthcare industry range from simple data storage to the assurance of patient privacy, data integrity, and trust mechanisms that meet the specific security and accountability requirements of the industry. Therefore, blockchain provides a secure, decentralized foundation for the management of private health information created by IoMT devices, from sophisticated imaging systems to wearable health monitors.

The integration of blockchain into IoMT networks hence improves device security by addressing the inefficiencies of classical systems. For example, a blockchain-based architecture to guarantee secure health data management. As they claimed, such a decentralized blockchain reduces the occurrence of single points of failure while its cryptographic algorithms practically eliminate unwanted accesses, which guarantees the security and integrity of sensitive data. [7]

In this context, security not only includes data protection but also management of digital identities within healthcare networks. IoMT devices are often left vulnerable due to either inappropriate or default authentication mechanisms. The automation of identity verification procedures using smart contracts in blockchain technology is a major constituent of the prevention of identity theft and unauthorized access, ensuring that access to data is allowed only to subjects with permission [11-14]

Given this, researchers in recent times have explored blockchain as a potential solution for IoMT systems' scalability challenges. It also identified how blockchain can further enhance real-time monitoring at minimal costs in healthcare, even though they emphasize that scalability remains one of the most critical issues [12]. They state that though blockchain provides decentralization and integrity, it cannot support the high frequency of flows generated by the devices around IoMT, especially when there are multiple stakeholders present in a system. The balancing of decentralization, security, and scalability without compromising any in effectiveness is really essential via some creative off-chain and on-chain strategies.

While academics are trying to overcome the challenges of protecting sensitive IoT data, much emphasis has been paid to the inclusion of Blockchain technology into IoT security frameworks. According to Banerjee et al. [11] who review IoT security solutions, research and development are hampered by a crucial gap in the availability of publicly available IoT statistics. They argue that blockchain may fill this gap by assuring data integrity and traceability, thus enabling the secure sharing of sensitive datasets. The authors also propose two theoretical Blockchain-based strategies for enhancing the security of IoT systems and call for deeper research into nine specific research problems with a view to guiding future investigations. This position illustrates blockchain as the game-changing technology that would promise safe IoT ecosystems, such as the Internet of Medical Things. [6]

Integrating Blockchain into IoMT to improve data security in the healthcare industry is very important. The underlying data is guaranteed to be accessible while maintaining its integrity without third-party intermediaries due to methods of encryption and Blockchain's inherent decentralized architecture [15]. The approach allows secure communication of IoMT devices with the practitioners of healthcare, privacy laws are ensured, and the weaknesses of a centralized system are reduced. The findings showed that improved clinical practices and real-time, patient-centered care rely on secure data handling. [10]

In addition, the role of blockchain in enabling secure data exchange in healthcare has been investigate [12-18]. It has been noted that smart contracts make possible the secure sharing of data between IoMT devices and healthcare providers, therefore improving data interoperability and adherence to privacy regulations. Secure data exchange is critical within medical contexts, where timely, accurate data sharing is crucial in ensuring proper patient care and related outcomes. [19]

Strong security frameworks need to be designed considering the intrinsic vulnerabilities arising in real-time patient monitoring due to increased IoMT integration in healthcare.IoMT-based security architecture powered with Blockchain, integrated with recent federated learning and state-of-the-art encryption techniques. Availability, confidentiality, and integrity of the data are ensured by this approach through mitigation against different risks related to replay attack, eavesdropping, and manipulation of data. Comparing their results against some benchmark solutions, such as MRMS and BACKM-EHA, they demonstrate very promising enhancements regarding the detection of anomalies and resistance to various types of cyber-attacks. Besides that, an adaptive learning mechanism gives this framework a future-proofed solution for IoMT security because it is also adaptive in changing according to new threats. [20]

Whereas it had been widely regarded that blockchain would help solve some IoMT security challenges that have haunted the world for quite some time, gaps still exist in terms of scalability, interoperability, and regulatory compliance. The advantages of blockchain transparency and traceability but emphasize limitations in handling big volumes of data generated from IoMT systems. This calls for further innovation of blockchain solutions to meet such high demands of frequency without compromising [13].

Consequently, blockchain and IoMT security have turned into an interdisciplinary study that conceptually extracts ideas from information technology, cryptography, and healthcare informatics. These disciplines remain instrumental for the researchers to understand, predict, and improve the applications of blockchain in IoMT, with the ultimate aim of creating a more secure and reliable healthcare system.

Integrating blockchain technology into the Internet of Medical Things (IoMT) has transformative potential for healthcare, notably by enhancing interoperability, data security, and privacy. However, while the promise of blockchain is clear, I believe that several critical challenges must be addressed before widespread, practical implementation in real-world healthcare settings becomes feasible. [18]

TABLE I
KEY STRENGTH OF BLOCKCHAIN TECHNOLOGY IN IOMT

Strength	**Description**
Decentralization	Reduces single-point failures through distributed networks.
Data Security	Protects sensitive medical data through encryption and ensure unauthorized access is minimized.
Identity Management	Verifies identities using smart contracts, ensuring only authorized users can access data.
Data Integrity	Tracks and audits data all changes to ensure accountability and transparency.
Real-Time Monitoring	Enables continuous monitoring of IoMT devices, providing instant alerts for anomalies.

IV. Strengths of Blockchain in IoMT:

Decentralization: Because blockchain technology does not require a central authority, the probability of single-point failures is greatly decreased.

Data Security: By guaranteeing encryption and anonymity and making illegal access very difficult, blockchain's cryptographic processes protect health data. [1][3][7]

Identity Management: Blockchain improves safe identity verification through the use of smart contracts and decentralized identifiers, which is essential for preventing data fraud and identity theft. [1][3][7]

Data Integrity and Traceability: The immutable nature of blockchain technology facilitates accurate data monitoring and auditing, which promotes accountability and openness in the administration of healthcare data. [1][3][7]

Real-Time Monitoring: Blockchain technology enables ongoing IoMT device monitoring and provides real-time warnings when security abnormalities are detected, facilitating prompt action. [1][3][7]

Weaknesses and Research Gaps in Blockchain for IoMT:

Scalability Issues: IoMT devices generate enormous volumes of data that are too big for existing blockchain platforms to manage. Latency and performance problems result from this incapacity to handle such large numbers, especially in real-time applications.

Performance Issues: IoMT systems' efficiency, which is crucial for applications involving real-time patient monitoring, may be adversely affected by the computational and storage needs necessary for blockchain activities.

Interoperability Limitations: Inadequate interoperability between different blockchain frameworks and IoMT devices makes it difficult to integrate and exchange data seamlessly, which lowers healthcare networks' overall efficiency.

Regulatory and Compliance Issues: The regulatory environment in the healthcare industry poses issues for blockchain compliance, especially in relation to the right to data rectification and data immutability.

Blockchain strengthens IoMT by enhancing data security, decentralizing data management, and improving secure identity verification. Its cryptographic approach reduces vulnerabilities and supports real-time monitoring, giving patients more control over their data. However, challenges like scalability, interoperability, regulatory compliance, and limited user-friendly design remain barriers to widespread adoption in healthcare.

- The Need for New Strategies

The healthcare sector has to embrace novel strategies that go beyond accepted practices in order to reduce the security threats connected to IoMT devices. These tactics have to concentrate on strengthening device authentication, guaranteeing safe data transfer, and preserving the accuracy of medical records.

1. Decentralized Identity Management: Blockchain technology can provide safe identity management systems that guarantee sensitive data is only accessible by authorized people and devices. Blockchain technology can assist with identity verification without the need for a

central authority by utilizing cryptographic keys and decentralized identifiers. [1][3][7]

2. Safe Data Exchange: IoMT devices may exchange data with only those who are allowed thanks to blockchain technology. By automating the authorization procedures, smart contracts can guarantee adherence to privacy laws and foster device interoperability.

3. Real-Time Monitoring and Alerts: Blockchain's real-time features allow for ongoing IoMT device monitoring, identifying irregularities that could point to security lapses. Automatically triggering alerts enables prompt action and correction. [1][3][7]

4. Data Integrity Verification: The immutability of blockchain technology makes it possible to trace and validate any modifications made to patient data, creating an audit trail that improves accountability and transparency in the administration of healthcare data. [1][3][7]

- Identification of Gaps

There are still a number of important gaps in the research, despite the fact that several studies have highlighted the advantages of using blockchain technology into the Internet of Medical Things (IoMT) to improve security. These limitations point to areas that need more research to guarantee the successful and expandable use of blockchain technologies in the medical field.

1. Scalability Challenges The scalability of blockchain solutions in IoMT contexts is one of the main research needs. The majority of studies, such as those by Zhang et al. (2018) and Kuo et al. (2017), concentrate mostly on security and privacy issues without sufficiently discussing how these solutions can scale to handle the enormous amount of data produced by IoMT devices. The underlying blockchain network may find it difficult to handle large transaction volumes in real-time as the number of linked medical devices grows dramatically, which might result in latency problems and poor performance. This is especially important in medical contexts where prompt access to patient data is necessary for efficient care. As transaction volumes increase, the consensus techniques used by many blockchain networks—such as proof-of-work or even proof-of-stake—may create bottlenecks. Alternative consensus algorithms created especially for IoMT contexts should be investigated in future studies in order to improve scalability without sacrificing security.

2. Performance Issues Performance concerns are linked to scalability and have not received enough attention in the literature to yet. Although the studies frequently emphasize the security advantages of blockchain, they frequently fail to consider how the intrinsic features of blockchain affect the overall functionality of IoMT systems. For example, delay may be introduced by the computational and storage cost needed to operate a blockchain, especially in applications that demand real-time patient vital sign monitoring.

3. Interoperability Issues Interoperability between various blockchain systems and IoMT devices is not given enough attention in the current corpus of research, which is another important gap. As there are several blockchain implementations and standards available, it is still difficult to guarantee smooth communication and integration between various IoMT devices and blockchain networks. Without taking into account how they could interact with other healthcare technologies or current systems, the evaluated research frequently isolate their blockchain applications. The broad adoption and integration of blockchain solutions in IoMT may be hampered by the absence of established standards for interoperability. In order to guarantee that data may move freely and securely between platforms, future research should focus on creating frameworks that promote interoperability among different blockchain systems and IoMT devices.

4. Regulatory and Compliance Challenges Although the regulatory environment around data security and privacy is mentioned in a number of publications, thorough examinations of how blockchain applications in IoMT can comply with these frameworks are conspicuously lacking. More study is required to determine how blockchain might facilitate adherence to current standards while encouraging innovation, given the intricate and sometimes disjointed structure of healthcare legislation throughout the world. The regulatory issues of identity verification have been mentioned in studies such as those by Chakchai So-In, but there hasn't been a full analysis of the legal ramifications of blockchain's immutability, particularly with regard to data rectification rights and audit trails. To give practitioners and legislators useful information, researchers should look at how blockchain technology, healthcare laws, and ethical issues interact.

5. User-Centric Design Finally, a gap exists in blockchain applications for IoMT with regard to user-centric design. The majority of current research ignores the end-user experience in favor of technological frameworks and algorithms. The usability of blockchain solutions for patients, healthcare professionals, and other stakeholders is essential to their efficacy in the industry. Studies frequently neglect to discuss how people can be successfully informed about the intricacies of blockchain technology or how user interface design may promote usability while upholding strong security protocols. User experience studies should be given top priority in future research in order to comprehend the requirements, inclinations, and actions of stakeholders dealing with blockchain-enabled IoMT systems.

- Personal Opinion

Blockchain technology's incorporation into the Internet of Medical Things (IoMT) is revolutionizing the healthcare industry, especially in terms of improving interoperability, data security, and privacy. However, even though I see that blockchain solutions have a lot of promise, I also think that there are a lot of issues that need to be resolved before they can be successfully applied in actual healthcare settings.

Stressing the Value of Scalability The scalability of blockchain technology in IoMT apps is one of my main worries. Any blockchain system used in healthcare must be able to manage this expansion without sacrificing speed, given the quickly growing number of linked medical devices and the amount of data they produce. Despite their security, current consensus methods might not be appropriate for IoMT systems' high throughput needs. I think that the creation of scalable, lightweight blockchain systems that can meet the unique requirements of healthcare applications should be the main focus of future research.

Performance as a Crucial Elements Another important topic that, in my opinion, needs further research is performance. It is impossible to ignore the latency problems brought forth by blockchain's intrinsic features in an area where instantaneous data access might mean the difference between life and death. Researchers must concentrate on speeding up blockchain technology without compromising the security aspects that first drew people in since applications like emergency services and remote patient monitoring require quick reaction times.

Performance as a Vital Component Performance is another crucial subject that, in my opinion, requires more investigation. In a field where immediate data access might be life-or-death, it is hard to overlook the latency issues posed by blockchain's inherent properties. Because applications like emergency services and remote patient monitoring demand rapid reaction times, researchers must focus on accelerating blockchain technology without sacrificing the security features that first attracted users.

Handling Regulatory Environments Blockchain technology's regulatory issues are also important to consider. Researchers need to look at how blockchain can fit into these frameworks as healthcare rules continue to change. Blockchain solutions must meet legal requirements for data access, modification, and storage in addition to improving security and privacy. Gaining the trust of patients and healthcare professionals alike will depend on resolving these problems, which is critical for the broad use of blockchain in IoMT.

Using User-Centric Design to Close the Gap Lastly, it is impossible to exaggerate the significance of user-centric design. Any blockchain application in healthcare must prioritize the user experience, even while technological developments are crucial. The advantages of improved security and privacy will be compromised if patients and healthcare providers find blockchain technologies difficult to use or unwieldy. In order to guarantee that the final systems are safe and easy to use, I support a comprehensive strategy that integrates user input into the design process.

In conclusion, even if blockchain technology has unquestionably enormous promise for the Internet of Medical Things, academics and practitioners must fill in the gaps in the literature. Blockchain applications in healthcare may be made safe and successful by emphasizing scalability, performance, interoperability, regulatory compliance, and user-centric design. I'm still hopeful about IoMT's future and how blockchain technology might help build a more patient-centered, safe, and effective healthcare system as we continue to investigate these possibilities.

V. Future Research Directions

Blockchain technology has the potential to significantly improve the security and privacy of Internet of Medical Things (IoMT) systems, particularly when it comes to safeguarding sensitive medical data and maintaining electronic health records. However, because of its high computing needs, blockchain implementation is difficult on IoMT devices, which frequently have limited computational capabilities.

1. **Improving Blockchain Efficiency for Resource-Constrained IoMT Devices**:

   Making blockchain protocols lighter and more effective should be the main focus of future research in order to meet the resource constraints of IoMT devices. This may entail:

   - creating consensus techniques like Delegated Proof-of-Stake (DPoS) and Proof-of-Authority (PoA) that require less computing power.
   - employing off-chain processing strategies to reduce the stress on the device.
   - investigating edge and fog computing as a way to lower latency and energy usage in conjunction with blockchain-based IoMT systems.

2. **New Applications for Data and Permission Management**: Similar to the MedRec concept, blockchain can facilitate safe, permission-based access to health data, giving consumers and healthcare practitioners the ability to manage who has access to the data. Among the possible avenues for investigation are:

   - establishing structures that enable precise management of patient data access.
   - using smart contracts to guarantee data integrity and automate access rights.

- investigating distributed identity management options to improve patient data control while adhering to privacy laws.

3. **Integrating Blockchain with Other Security Technologies**: The synergy between blockchain and technologies such as artificial intelligence (AI) can bolster IoMT systems by:
   - Enhancing threat detection through AI-based anomaly detection integrated with immutable blockchain records.
   - Facilitating predictive analytics by securely sharing anonymized health data.
   - Improving patient outcomes by enabling real-time data sharing among healthcare providers while preserving security.
4. **Developing Security Assessment Standards for Blockchain in IoMT**: To improve system It is crucial to create security assessment guidelines specifically for blockchain applications in IoMT in order to foster confidence and guarantee dependability. This includes:
   - defining measures to assess durability, scalability, and privacy.
   - creating standardized frameworks for penetration testing in IoMT settings.
   - working together with regulatory agencies to guarantee adherence to changing international healthcare standards.
5. **Exploring Hybrid Solutions**: Data security and regulatory compliance may be improved by hybrid models that blend centralized systems with decentralized blockchain components. Solutions that are hybrid could:
   - For data provenance, use decentralized blockchain systems; for storage-intensive operations, use centralized servers.
   - Permit selective decentralization, in which access logs and metadata are maintained on the blockchain while important data is kept in centralized storage.
   - Enable adherence to laws such as GDPR while preserving the advantages of blockchain immutability.
6. **Enhancing Storage Solutions Focused on Users**
   Creating user-owned and controlled decentralized storage systems is a new field of study. Among the possible directions are:

- developing mobile gadgets or systems that run on smartphones for safe local data storage.
- use smart contracts to enforce user-defined access rules in order to ensure accessibility.
- investigating how to integrate distributed storage systems to offer safe and scalable data-sharing options.

7. **Reward-Based Data Contribution Models**
   Current systems often do not recognize or reward patients for contributing valuable health data. Future blockchain-based IoMT ecosystems could:

- Implement **token-based rewards** for individuals who contribute data, incentivizing data sharing while respecting privacy.
- Foster **data crowdsourcing** to advance scientific research and improve public health.
- Shift the paradigm from **system-centric to user-centric**, empowering individuals to become active participants rather than passive consumers.

By boosting data security, giving patients more control over their data, and providing transparent, decentralized solutions, integrating blockchain technology into IoMT systems has the potential to completely transform the healthcare industry. But accomplishing these objectives would need overcoming formidable obstacles pertaining to data management, resource limitations, security standards, and regulatory compliance. To fully realize the benefits of blockchain in IoMT and build safe, patient-centered healthcare ecosystems, future research will need to concentrate on creating more effective blockchain protocols, sophisticated data access control, AI-integrated security, standardized security assessment frameworks, and hybrid blockchain models.

VI. Conclusions

The research emphasizes how blockchain technology can alter healthcare systems when combined with the IoMT. Blockchain offers a strong framework for improving patient-centric healthcare by tackling issues like data privacy, decentralized administration, and identity verification. Real-time monitoring and safe exchange among stakeholders are made possible by its cryptographic capabilities, which guarantee the confidentiality and privacy of sensitive medical data and give patients control over their health information. Blockchain supports safe data interchange across institutions, promoting collaborative care and stimulating innovation in healthcare research. It also makes decentralized data administration possible, reducing the hazards associated with centralized repositories, such as breaches and illegal access. However, a number of barriers prevent blockchain from being widely used in IoMT systems for healthcare. The processing needs of blockchain continue to cause scalability problems, which might place a strain on IoMT devices with limited resources. Blockchain solutions must comply with strict healthcare regulations and complicated implementations can lead to unintuitive designs that prevent patient and provider acceptance. Regulatory compliance is still a major barrier. Future research must concentrate on creating standardized security assessment frameworks to guarantee strong privacy and security, investigating hybrid blockchain models to address issues of scalability and compliance, incorporating artificial intelligence to improve security and facilitate predictive analytics, and developing off-chain solutions and lightweight blockchain protocols to support devices with limited resources. Additionally, patients can be empowered to actively manage their health data by giving priority to user-centric platforms with intuitive designs. Large-scale health data collecting is made possible by modern IoMT devices, which presents chances for better patient care and tailored treatment. Blockchain can further this development by developing safe platforms that put privacy, scalability, and interoperability first. These platforms can facilitate cooperative ecosystems in which patient data directly advances science and improves healthcare results. Blockchain-enabled IoMT systems have the potential to build safe, open, and patient-centered healthcare ecosystems, promoting a better-informed and healthier society, even though there are still obstacles to overcome.

Acknowledgment

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

References

[1]. J. Indumathi, A. Shankar, M. R. Ghalib, J. Gitanjali, Q. Hua, and Z. Wen, “Block chain based internet of medical things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (BC IoMT U6 HCS),” *IEEE Access*, vol. 8, no. 12, pp. 123-135, Nov. 2020, doi:10.1109/ACCESS.2020.3040240.

[2]. Y. Sun, F. P.-W. Lo, and B. Lo, “Security and privacy for the internet of medical things enabled healthcare systems: A survey,” *IEEE Access*, vol. 8, no. 1, pp. 123-135, Dec. 2019, doi: 10.1109/ACCESS.2019.2960617.

[3]. M. El Khatib, H. M. Alzoubi, S. Hamidi, M. Alshurideh, A. Baydoun, and A. Al-Nakeeb, “Impact of using the internet of medical things on ehealthcare performance: Blockchain assist in improving smart contract,” *ClinicoEconomics and Outcomes Research*, vol. 15, pp. 397-411, Jun. 2023, doi: 10.2147/CEOR.S407778.

[4]. S. Razdan and S. Sharma, “Internet of medical things (IoMT): Overview, emerging technologies, and case studies,” *IETE Technical Review*, vol. 39, no. 4, pp. 775-788, May 2022, doi: 10.1080/02564602.2021.1927863.

[5]. M. Jmaiel, M. Mokhtari, B. Abdulrazak, H. Aloulou, and S. Kallel, Eds., *The impact of digital technologies on public health in developed and developing countries*, LNCS 12157, Proceedings of the 18th International Conference, ICOST 2020, Hammamet, Tunisia, Jun. 24–26, 2020, doi: 10.1007/978-3-030-51517-1.

[6]. H. Taherdoost, “Blockchain-based internet of medical things,” *Applied Sciences*, vol. 13, no. 1287, 2023, doi: 10.3390/app13031287.

[7]. G. Bigini, V. Freschi, and E. Lattanzi, “A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision,” *Future Internet*, vol. 12, no. 208, Nov. 2020, doi: 10.3390/fi12120208.

[8]. Z. Sun, D. Han, D. Li, X. Wang, C.-C. Chang, and Z. Wu, “A blockchain-based secure storage scheme for medical information,” *Journal of Wireless Communications and Networking*, vol. 2022, no. 40, 2022, doi: 10.1186/s13638-022-02122-6.

[9]. W. A. N. A. Al-Nbhany, A. T. Zahary, and A. A. Al-Shargabi, “Blockchain-IoT healthcare applications and trends: A review,” *IEEE Access*, vol. 12, pp. 1-10, Jan. 2024, doi:10.1109/ACCESS.2023.3349187.

[10]. S. Yongjoh, C. So-in, P. Kompunt, P. Muneesawang, and R. I. Morien, “Development of an internet-of-healthcare system using blockchain,” *IEEE Access*, vol. 9, pp. 136158-136169, Aug. 2021, doi: 10.1109/ACCESS.2021.3103443..

[11]. M. Banerjee, J. Lee, and K.-K. R. Choo, “A blockchain future for internet of things security: A position paper,” Digital Communications and Networks, vol. 3, no. 2, pp. 149–157, 2018, doi: 10.1016/j.dcan.2017.10.006.

[12]. Y. Yasin Ghadi, T. Mazhar, T. Shahzad, M. A. Khan, A. Abd-Alrazaq, A. Ahmed, and H. Hamam, “The role of blockchain to secure internet of medical things,” Scientific Reports, vol. 14, no. 1, pp. 1011-1020, 2024, doi: 10.1038/s41598-024-68529-x.

[13]. M. Pilkington, "Can Blockchain improve healthcare management? Consumer medical electronics and the IoMT," SSRN Electronic Journal, 2016, doi: 10.2139/ssrn.3025393..

[14]. A. Sharma, S. Singh, R. Tomar, N. Chilamkurti, and B.-G. Kim, "Blockchain based smart contracts for Internet of Medical Things in e-healthcare," Electronics, vol. 9, no. 10, pp. 1609, 2020, doi: 10.3390/electronics9101609.

[15]. H. Taherdoost, “Blockchain-based internet of medical things,” *Applied Sciences*, vol. 13, no. 1287, 2023, doi: 10.3390/app13031287. [7] G. Bigini, V. Freschi, and E. Lattanzi, “A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision,” *Future Internet*, vol. 12, no. 208, Nov. 2020, doi: 10.3390/fi12120208.

[16]. C. C. Y. Hang, M. Batumalay, T. D. Subash, R. Thinakaran, and B. Chitra, "Blockchain-based and IoT-based health monitoring app: Lowering risks and improving security and privacy," Journal of Health Informatics, vol. 7, no. 1, pp. 42-48, 2020.

[17]. Y. Wang and L. Sun, "Privacy protection of secure sharing electronic health records based on blockchain," Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 7, pp. 922-928, 2024. doi:10.1109/ACCESS.2023.3349187.

[18]. A. Sharma, S. Singh, R. Tomar, N. Chilamkurti, and B.-G. Kim, "Blockchain based smart contracts for Internet of Medical Things in e-healthcare," Electronics, vol. 9, no. 10, p. 1609, Oct. 2020.DOI: https://doi.org/10.3390/electronics9101609

[19]. F. Ellouze, G. Fersi, and M. Jmaiel, "Blockchain for Internet of Medical Things: A Technical Review," in Proc. ICOST 2020, Sfax, Tunisia, 2020, vol. 12157, pp. 259–267. [Online]. Available: https://doi.org/10.1007/978-3-030-51517-1_22

[20]. H. Mansouri, R. Hireche, C. Benrebbouh, and A.-S. K. Pathan, "A Review of Blockchain in Internet of Medical Things," in Cryptology and Network Security with Machine Learning, A. Chaturvedi et al., Eds., Lecture Notes in Networks and Systems, vol. 918, Singapore: Springer Nature, 2024, pp. 1–10. [Online]. Available: https://doi.org/10.1007/978-981-97-0641-9_28