Blockchain-Enabled Internet of Medical Things (IoMT): A Systematic Review of Security Frameworks for Remote Patient Monitoring

[1]Megha Panwar, [2]Dr. Vishal Shrivastava, [3]Dr. Akhil Pandey, [4]Ram Babu Buri, [5]Amit Tewari

[1]B.TECH. SCHOLAR, [2,3]PROFESSOR, [4]ASST. PROFESSOR, [5]ASSOC. PROFESSOR
ARYA COLLEGE OF ENGINEERING AND IT, JAIPUR, INDIA

Abstract

The rapid proliferation of the Internet of Medical Things (IoMT) has revolutionized healthcare through Remote Patient Monitoring (RPM), allowing for real-time data collection and continuous physiological tracking. However, the centralization of conventional healthcare data management systems introduces significant vulnerabilities, including single points of failure, data breaches, and unauthorized access to sensitive patient information. Blockchain technology emerged as a transformative solution, offering a decentralized, immutable, and transparent ledger for securing IoMT ecosystems. This paper provides a systematic review of the current security frameworks that integrate blockchain with IoMT. We analyze various architectural designs, consensus mechanisms, and the role of smart contracts in ensuring data integrity, privacy, and availability. Furthermore, a comparative analysis of existing frameworks is presented, highlighting their strengths and limitations regarding scalability, latency, and storage overhead. The findings suggest that while blockchain significantly enhances security, challenges such as high computational costs and regulatory compliance remain. This review concludes by outlining future research directions, specifically focusing on the integration of Artificial Intelligence (AI) and the transition toward quantum-resistant cryptographic protocols.

Keywords: Blockchain, IoMT, Remote Patient Monitoring, Healthcare Security, Smart Contracts, Data Privacy.

I. Introduction

The healthcare industry is undergoing a digital transformation, shifting from traditional clinic-based visits to decentralized, patient-centric care. At the heart of this evolution is the Internet of Medical Things (IoMT), a sub-ecosystem of the Internet of Things (IoT) that connects medical devices, sensors, and software to healthcare IT systems [1]. Remote Patient Monitoring (RPM) utilizes IoMT devices to track vital signs such as heart rate, glucose levels, and oxygen saturation, transmitting this data to clinicians in real-time. This is particularly crucial for managing chronic diseases and elderly care, reducing hospital readmission rates, and improving patient outcomes.

Despite these advantages, IoMT faces daunting security challenges. Most IoMT devices are resource-constrained, possessing limited processing power and battery life, which makes the implementation of robust encryption protocols difficult [2]. Furthermore, the traditional cloud-based storage models for IoMT data are centralized, making them attractive targets for cyberattacks such as Ransomware-as-a-Service (RaaS), Distributed Denial of Service (DDoS), and Man-in-the-Middle (MITM) attacks. A breach in this context does not just

involve data theft; it poses a direct threat to human life if medical records are altered or life-critical devices are tampered with.

Blockchain technology has been identified as a robust framework to address these vulnerabilities. By utilizing a Distributed Ledger Technology (DLT), blockchain eliminates the need for a central authority, ensuring that medical data is synchronized across a P2P network [3]. Every transaction—whether it is a data upload from a wearable device or a doctor's access request—is recorded in an immutable block linked through cryptographic hashes.

A. Motivation and Scope Existing literature has explored blockchain for general IoT, but the specific requirements of IoMT—such as high sensitivity of data and the need for low-latency responses in emergencies—require a specialized review. This paper systematically evaluates security frameworks specifically designed for blockchain-enabled RPM systems.

B. Structure The remainder of the paper is organized as follows: Section II provides a background on IoMT and Blockchain. Section III details the research methodology. Section IV presents the literature review and comparative analysis. Section V discusses open challenges and future directions, and Section VI concludes the paper.

II. Background and Fundamentals

A. The IoMT Architecture for RPM

A standard IoMT-based RPM system comprises three main layers:

1. **Perception Layer:** Consists of medical sensors (e.g., ECG sensors, pulse oximeters) and actuators. These collect raw physiological data.
2. **Network Layer:** Responsible for transmitting data via protocols like Bluetooth Low Energy (BLE), Zigbee, or 5G to a gateway or cloud environment.
3. **Application Layer:** Where healthcare providers, emergency services, and patients interact with the processed data.

B. Blockchain Fundamentals in Healthcare

Blockchain is characterized by four key pillars relevant to medical security:

- **Decentralization:** Data is not stored in a single location, reducing the risk of data loss.
- **Immutability:** Once a medical record is validated and added to the chain, it cannot be altered without the consensus of the network [4].
- **Transparency and Traceability:** Every access to the patient's data is logged, providing a clear audit trail.
- **Smart Contracts:** Self-executing digital contracts with the terms of the agreement written directly into code. In RPM, these can automatically trigger alerts to physicians if a patient's vitals exceed a predefined threshold [5].

C. Types of Blockchains in IoMT

- **Public (Permissionless):** Anyone can join (e.g., Ethereum). High security but low throughput and high latency—often unsuitable for real-time RPM.
- **Private/Consortium (Permissioned):** Participation is restricted (e.g., Hyperledger Fabric). These offer higher speeds and better privacy, making them the preferred choice for hospital networks [6].

III. Research Methodology

To ensure a comprehensive and unbiased review, a systematic search was conducted following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines.

A. Data Sources Primary databases searched include:

- IEEE Xplore
- ACM Digital Library
- ScienceDirect (Elsevier)
- SpringerLink
- PubMed

B. Inclusion and Exclusion Criteria

- **Inclusion:** Peer-reviewed journals and conference papers published between 2018 and 2024; focus on blockchain, IoMT, and security security/privacy; frameworks specifically mentioning Remote Patient Monitoring.
- **Exclusion:** Papers focusing on general blockchain (e.g., cryptocurrency), non-English publications, and short white papers without technical validation.

C. Search Keywords "Blockchain" AND "IoMT" OR "Internet of Medical Things" AND "Security" AND "Remote Patient Monitoring" AND "Privacy."

IV. Literature Review and Comparative Analysis

Recent research has proposed various frameworks to bridge the gap between IoMT efficiency and blockchain security. These can be categorized based on their primary focus: Data Privacy, Authentication, or Storage Optimization.

A. Privacy-Preserving Frameworks

Privacy is the foremost concern in RPM. Patient data contains Protected Health Information (PHI). Work by [7] proposed a framework using **Zero-Knowledge Proofs (ZKP)**. ZKP allows the system to verify that a patient's vital signs are within a healthy range without actually revealing the exact numerical values to the blockchain, thus maintaining maximum privacy. Another approach by [8] utilizes **Differential Privacy** integrated with blockchain to add "noise" to datasets, ensuring that individual patients cannot be identified even if the database is subjected to statistical analysis.

B. Authentication and Access Control

Unauthorized access to IoMT devices can lead to lethal consequences. Researchers in [9] developed a **Multi-Factor Authentication (MFA)** scheme based on Smart Contracts. In this model, the device must authenticate through the blockchain gateway using a combination of biometric data and a device-specific cryptographic key. The work in [10] introduced **Attribute-Based Access Control (ABAC)**, where access permissions are dynamically granted based on the doctor's role, location, and the urgency of the patient's condition.

C. Storage and Scalability Solutions

Storing large volumes of high-frequency IoMT data directly on a blockchain (on-chain) is prohibitively expensive and slows down the network. A widely adopted solution is the **Off-chain Storage Model** using **InterPlanetary File System (IPFS)** [11]. In this framework, the actual medical images or telemetry data are stored in a decentralized IPFS, while only the cryptographic hash of the data is stored on the blockchain. This ensures data integrity while maintaining high system performance.

D. Comparative Analysis of Existing Frameworks

The following table summarizes and compares key frameworks identified in the literature based on several performance and security metrics.

Reference	Core Technology	Primary Focus	Consensus Mechanism	Scalability	Security Strength
[7]	ZKP + Ethereum	Privacy	PoW (Proof of Work)	Low	Very High
[9]	Smart Contracts	Auth/Access	PBFT	Medium	High
[11]	IPFS + Hyperledger	Storage	Kafka/Raft	High	Moderate
[12]	Edge Computing + BC	Latency	DPoS	High	High
[13]	PUF + Blockchain	Device Security	PoS	Medium	Very High

Note: PBFT (Practical Byzantine Fault Tolerance), DPoS (Delegated Proof of Stake), PUF (Physically Unclonable Functions).

E. Synthesis of Findings

The comparative analysis reveals a clear trade-off between security and performance (The Blockchain Trilemma). Frameworks based on Public Blockchains (Ethereum) offer the highest decentralization but suffer from high latency and "gas" costs. Conversely, frameworks utilizing Edge Computing and Permissioned Blockchains (Hyperledger) offer the throughput required for real-time RPM but require a higher degree of trust among the participating nodes [12].

V. Discussion: Challenges and Open Issues

Despite the promising potential of blockchain-enabled IoMT, several hurdles prevent widespread clinical adoption.

1. **Storage Overhead:** IoMT devices generate gigabytes of data daily. Even with off-chain storage, the metadata on the blockchain grows linearly, leading to the "bloat" of the ledger.
2. **Energy Consumption:** Many consensus algorithms require significant computational power. For battery-operated wearables, this is a critical bottleneck.
3. **Interoperability:** Different hospitals use different blockchain protocols. A patient moving from Hospital A (Hyperledger) to Hospital B (Ethereum) may find their data is not easily transferable [14].
4. **Legal and Regulatory Compliance:** The General Data Protection Regulation (GDPR) includes the "Right to be Forgotten." However, the fundamental nature of blockchain is immutability (data cannot be deleted), creating a legal paradox [15].
5. **The Threat of Quantum Computing:** Current cryptographic standards (RSA, ECC) used in blockchain are vulnerable to future quantum attacks. The transition to post-quantum cryptography is an urgent area of research.

VI. Conclusion and Future Work

A. Conclusion

This systematic review has explored the intersection of Blockchain and the Internet of Medical Things in the context of Remote Patient Monitoring. We have demonstrated that blockchain effectively addresses the core security requirements of confidentiality, integrity, and availability (the CIA triad). By integrating smart contracts for automated access control and IPFS for scalable storage, researchers have created frameworks that are significantly more resilient than centralized cloud-resident databases. However, the comparative analysis highlights that no single framework currently optimizes all parameters; choices must be made based on the specific needs of the medical application (e.g., emergency response vs. long-term wellness tracking).

B. Future Work

Future research should focus on the following domains:

- **AI-Blockchain Integration:** Implementing Machine Learning models at the Edge to filter "normal" data and only record "anomalous" health events on the blockchain to save storage space.
- **Energy-Efficient Consensus:** Developing "Proof of Physiological Sense" or other lightweight consensus mechanisms tailored for low-power medical wearables.
- **Cross-Chain Communication:** Engineering interoperability layers that allow different healthcare blockchains to share PHI securely.
- **Regulatory-Friendly Blockchain:** Designing "Redactable Blockchains" that allow authorized deletion of data to comply with GDPR without compromising the integrity of the remaining ledger.

References

[1] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[2] M. Papaioannou et al., "A Survey on Security Threats and Intrusion Detection Systems in IoMT Libraries," *IEEE Access*, vol. 10, pp. 57123–57155, 2022.

[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Manubot*, 2008.

[4] M. A. Rahman, M. S. Hossain, G. Loukas, J. Hassan, and S. S. Ghinea, "Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications," *IEEE Access*, vol. 6, pp. 72469–72478, 2018.

[5] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "How Blockchain-Control Can Be Used to Support Patient-Centric Health Data Sharing," *JMIR Medical Informatics*, vol. 5, no. 1, p. e14, 2017.

[6] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.

[7] L. S. S. S. Singh and S. S. S. Rathkanthiwar, "Privacy-Preserving IoMT Data Security Using Zero Knowledge Proofs," *Int. Conf. on Emerging Smart Computing*, 2021.

[8] Y. Liu et al., "Privacy-Preserving Blockchain-Based Federated Learning for IoMT," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, 2022.

[9] P. Gope and B. Sikdar, "Lightweight and Privacy-Preserving Mutual Authentication Scheme for Registering Smart Healthcare Devices in IoMT," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 583–593, 2019.

[10] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based Electronic Healthcare Record System for IoMT," *Journal of Information Security and Applications*, vol. 50, 2020.

[11] J. J. S. Huang et al., "A Decentralized Framework for Health Data Management using Blockchain and IPFS," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 2, 2020.

[12] R. Kumar and R. Tripathi, "Scalable and Secure Edge-Blockchain Framework for IoMT Ecosystem," *IEEE Communications Letters*, vol. 24, no. 8, pp. 1650-1654, 2020.

[13] M. Wazid et al., "PUF-Based Secure Authentication Protocol for IoT-enabled Health Care Applications," *IEEE Transactions on Convergence Information Technology*, 2021.

[14] G. S. S. Chalapathi et al., "Interoperability in Blockchain: A Survey of Healthcare Standards," *IEEE Review of Biomedical Engineering*, 2023.

[15] C. J. Barber and J. B. Smith, "GDPR Compliance and the Immutability of Blockchain in Healthcare," *Nature Digital Medicine*, vol. 4, no. 12, 2021.

[16] T. K. Dasaklis et al., "Blockchain Applications in Health Care," *Context, Methodology, and Current Challenges*, 2019.

[17] H. F. Atlam and G. B. Wills, "IoT Security and Privacy: The Role of Blockchain," *Studies in Computational Intelligence*, 2020.

[18] X. Liang et al., "Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications," *IEEE 28th Annual Int. Symp. on PIMRC*, 2017.

[19] K. N. Griggs et al., "Healthcare Blockchain System Using Smart Contracts for Secure Real-Time Patient Monitoring," *Journal of Medical Systems*, vol. 42, no. 7, 2018.

[20] D. V. Dimov and S. Ivanov, "Analysis of Consensus Protocols for Blockchain in Medical IoT," *Proc. of the IEEE Conference on Innovations in Intelligent Systems*, 2022.