Acta Informatica Pragensia
2025, Volume 14, Issue 1, 128–154
https://doi.org/10.18267/j.aip.256

PRAGUE UNIVERSITY OF ECONOMICS AND BUSINESS

Article Open Access

Blockchain Approach for Healthcare Using Fog Topology and Lightweight Consensus

Aya Laouamri, Sarra Cherbal, Yacine Mosbah, Chahrazed Benrebbouh, Kamir Kharoubi

Laboratory of Networks and Distributed Systems, Department of Computer Science, Faculty of Sciences, Ferhat Abbas Sétif University 1, Setif, Algeria

Corresponding author: Sarra Cherbal (sarra_cherbal@univ-setif.dz)

Editorial Record

First submission received:
September 1, 2024

Revisions received:
October 29, 2024
November 29, 2024

Accepted for publication:
December 7, 2024

Academic Editor:
Zdenek Smutny
Prague University of Economics and Business, Czech Republic

This article was accepted for publication by the Academic Editor upon evaluation of the reviewers' comments.

How to cite this article:
Laouamri, A., Cherbal, S., Mosbah, Y., Benrebbouh, C., & Kharoubi, K. (2025). Blockchain Approach for Healthcare Using Fog Topology and Lightweight Consensus. *Acta Informatica Pragensia*, 14(1), 128–154. ttps://doi.org/10.18267/j.aip.256

Abstract

Background: The internet of things (IoT) has transformed healthcare by integrating various devices and systems, fostering innovation in data management and operational efficiency. However, ensuring data integrity, security and trust within IoT networks remains a pressing challenge, particularly in critical sectors such as healthcare.

Objective: This study aims to explore the integration of blockchain technology with IoT systems, focusing on addressing scalability and real-time applicability issues in healthcare data management. By proposing novel solutions, the research seeks to enhance the security and reliability of IoT systems in healthcare environments.

Methods: The proposed framework incorporates a lightweight raft-based consensus protocol and enhanced cryptographic measures, such as Schnorr signatures and hashes, to address existing limitations in scalability and latency. The architecture and algorithms for signature generation, encryption, emergency state actions and consensus are developed and evaluated through extensive simulations using the NS3 toolkit.

Results: The simulation results validate the effectiveness of the proposed approach in improving healthcare IoT systems. The findings demonstrate enhancements in energy efficiency, throughput and network usage, establishing the potential of the framework for revolutionizing healthcare data management by providing secure, scalable and efficient solutions.

Conclusion: The study contributes to advancing secure and reliable decentralized data management systems for IoT in healthcare by making use of blockchain technology. The proposed architecture addresses critical challenges and offers practical benefits such as resource efficiency and system stability. While promising, the framework requires real-world testing and further optimization to overcome potential scalability bottlenecks in large-scale healthcare deployments.

Index Terms

IoT; Blockchain; Healthcare; Data integrity; Security; Privacy; Decentralized systems.

1 INTRODUCTION

The adoption of IoT technologies has enabled connectivity across various fields, transitioning healthcare from paper-based methods to electronic patient records for greater efficiency. IoT connectivity has transformed healthcare data exchange, enabling real-time monitoring, collection and analysis through smart devices and sensors (Sadhu et al., 2022; Tomar et al., 2023). However, the integration of IoT into healthcare also introduces significant security and privacy concerns that need careful consideration due to the sensitive nature of the data collected, transmitted and processed by IoT devices (Chinbat et al., 2024).

The interconnected nature of IoT devices increases the potential attack surface and vulnerability to malicious activities, including unauthorized access, data breaches and tampering (Cherbal & Benchetioui, 2023). The sensitivity and personal nature of healthcare data make them an attractive target for cybercriminals, necessitating robust security measures to protect the privacy and integrity of patient information (Raghuvanshi et al., 2022; Karunarathne et al., 2021). Additionally, Integrating IoT devices from different manufacturers raises compatibility, standardization and interoperability concerns that must be addressed for efficient operation.

Blockchain technology, known for its success in cryptocurrency, has the potential to significantly affect healthcare. It offers a secure and decentralized platform for managing patient data, enabling individuals to control their medical records and share information transparently with healthcare providers and researchers. Blockchain also improves interoperability by enabling seamless data exchange between different organizations while enhancing security and privacy through tamper-proof and immutable ledgers. The integration of blockchain in healthcare holds promise for improved patient outcomes, cost reduction and increased industry efficiency (Andrew et al., 2023).

The primary objective of this work is to develop a secure, efficient and scalable framework for managing healthcare IoT systems by integrating blockchain technology. Specifically, this study aims to address key challenges in healthcare IoT, such as ensuring data privacy, maintaining patient data integrity and preventing unauthorized access. By eliminating energy-intensive consensus mechanisms such as proof of work (PoW) and implementing the RaftNode algorithm, we enhance fault tolerance, consistency and efficiency. Our approach also strengthens privacy protection and optimizes the leader election process, making it suitable for real-time healthcare applications. Through these objectives, we seek to deliver a robust solution that protects patient data, supports secure healthcare services and fosters trust in IoT applications within the healthcare sector.

Existing healthcare IoT security approaches face limitations due to scalability and efficiency concerns, particularly in handling large volumes of data from wearable devices and ensuring rapid response times during emergencies (Qu et al., 2021; Chaudhary and Chatterjee, 2020; Gupta et al., 2023, Nanda et al., 2023). To address these challenges, we propose a blockchain-based architecture that utilizes a fog and cloud topology to enhance security across the entire data lifecycle, from the receipt of medical data from patient wearables to decision making based on emergency status. This topology provides distributed processing closer to the data source via fog nodes, enabling real-time data analysis and reducing latency, which is critical for emergency response.

The decentralized and tamper-resistant blockchain framework holds significant promise for addressing healthcare IoT security requirements, but traditional consensus protocols such as proof of work (PoW) used in some approaches (e.g., Qu et al., 2021) are unsuitable for healthcare IoT. PoW-based systems are often energy-intensive, introduce latency and face scalability issues, making them impractical for managing real-time data needs of healthcare IoT and stringent resource constraints (Allam et al., 2024). Consequently, this work utilizes the raft consensus protocol, which is more efficient and better suited to healthcare applications. The raft design prioritizes quick leader election and log replication across distributed nodes, ensuring consensus while maintaining high throughput and low latency, which are vital features for systems handling life-critical healthcare data.

Some approaches omit mentioning specific algorithms for authentication, session keys and access control (e.g., Liu et al., 2020), which questions the system security. Thus, our approach also integrates advanced cryptographic methods, including Schnorr signatures and hashing, to further enhance data integrity and ensure secure, tamper-resistant records without relying on a single point of failure. The fog and cloud topology, coupled with the raft consensus, allows our proposed system to handle high volumes of device data efficiently, prioritize emergency situations in real time and maintain decentralized trust, all while meeting the strict security standards of healthcare.

By addressing the limitations of current security frameworks in healthcare IoT, this work advances the field with an architecture that is both scalable and efficient. Our solution aims to optimize energy consumption, enhance data throughput and maintain network efficiency, demonstrating significant potential to secure healthcare IoT systems and protect patient information.

The key limitations identified in previous studies that we address in our work can be summarized as follows:

1. **Enhanced fault tolerance and consistency:** Unlike traditional consensus algorithms that may struggle with network partitions and node failures, our implementation based on the RaftNode algorithm ensures strong consistency and fault tolerance among distributed servers. This is crucial in healthcare environments where

the integrity of patient data is paramount. Existing work, such as the architecture by Qu et al. (2021), demonstrates the challenges of energy inefficiency and scalability in consensus mechanisms, which our solution directly addresses by optimizing leader election and validation processes.

2. **Improved privacy mechanisms:** Previous works, such as the solution proposed by Liu et al. (2020), introduced privacy enhancements in biomedical systems. However, they often lacked specific protocols for authentication and encryption of sensitive patient information. In our approach, we address this by encrypting identifiable patient data, ensuring that only authorized personnel can access them, thereby strengthening privacy while supporting healthcare providers' needs.
3. **Fog and cloud topology:** We implement distributed processing closer to the data source via fog nodes, enabling real-time data analysis and reducing latency, which is critical for emergency responses. This builds upon approaches such as the Federation Security System Manager (FSSM) by Alshudukhi et al. (2023), which introduced microservices for cloud interoperability but faced challenges related to latency and complex transactions in healthcare environments.
4. **Efficient leader election process:** Our implementation features an optimized leader election process that minimizes downtime and ensures prompt consensus on treatment protocols, addressing challenges observed in other consensus approaches.
5. **Streamlined validation procedures:** By incorporating feedback from multiple servers, we enhance validation procedures, allowing collaborative improvements to treatment protocols. This contrasts with systems such as those by Gupta et al. (2023), where single server dependency and computational overheads limited scalability and fault resilience in medical access control.
6. **Periodic block creation:** Instituting a regular block creation schedule (approximately every 7 minutes) enhances blockchain resilience against tampering, increasing the security of patient records. This method contrasts with reactive block creation in systems such as the blockchain-based architecture by Rizzardi et al. (2024).
7. **Optimized energy consumption:** Unlike energy-intensive methods such as PoW in the MinT architecture by Qu et al. (2021), our work aims to optimize energy consumption, enhance data throughput and maintain network efficiency.

Through these contributions, our work not only enhances the functionality and security of blockchain-based healthcare systems but also directly addresses the limitations found in previous research, providing a more robust solution for managing patient treatment protocols.

The rest of the paper is organized as follows: Section 2 provides a general overview of blockchain and smart healthcare concepts. In Section 3, we present an extensive review of the current literature and research focusing on blockchain in IoT and healthcare. Our proposed scheme is detailed in Section 4. Section 5 explains the security factors achieved by our approach. Section 6 describes the experimental methodology and presents the results obtained from simulation experiments using the NS3 toolkit. Section 7 presents a comparison with other works and Section 8 summarizes the limitations of our work. Finally, Section 9 concludes the paper by summarizing the key findings.

2 BACKGROUND

2.1 Blockchain

Blockchain is a distributed ledger replicated across a network of peers (Adjeroud et al., 2024), secured with cryptography and composed of blocks that are linked together through a virtual chain, meaning that they are connected cryptographically (Mohammadi, 2023). Each block consists of a header, body and footer (Saleem et al., 2022). The header references the previous footer, which is the hash result of the header and the body containing transactions made by the nodes, as shown in Figure 1. The exception is the first block, called the genesis block, whose header does not refer to any other blocks. Once a block is successfully verified and validated by the majority of nodes (at least 51% of nodes), it is added to the blockchain, linked to the rest of the chain and becomes permanent and distributed to all participants in the blockchain. Blocks are generated with either time or transaction limits, making the blockchain continuously grow and challenging to hack (Ratta et al., 2021).

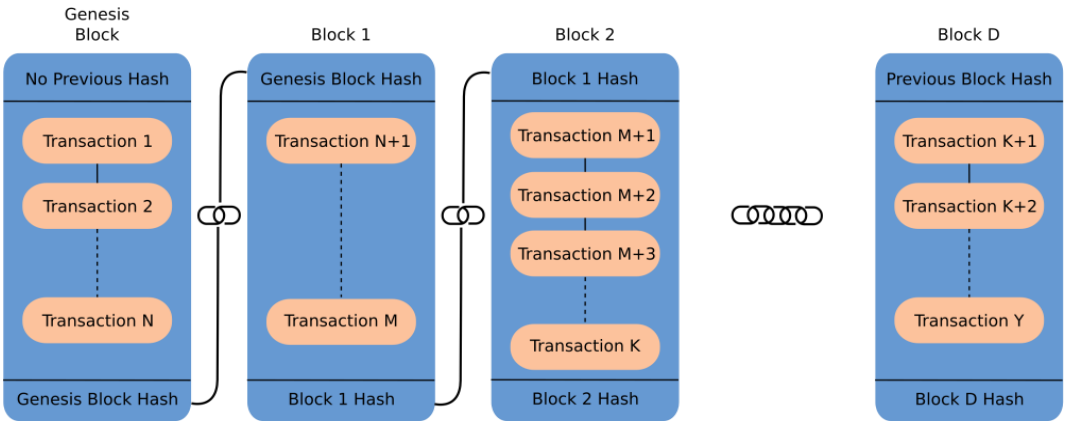


Figure 1. *Blockchain structure.*

2.2 Smart healthcare

Smart healthcare has emerged as a new revolution in the healthcare sector, where integrated devices, such as sensors placed in patients' bodies, have proven to be crucial elements in saving patients' lives (Shari & Malip, 2024). These devices facilitate the collection and recording of patient data for medical analysis and treatment (Tiwari et al., 2021). By integrating these sensors with the IoT, healthcare providers can transmit patient data to doctors for monitoring and analysis (Adeniyi et al., 2021) (see Figure 2). Moreover, utilizing blockchain technology for data exchange, this approach can enable consensus among patients and agreed-upon terms for exchanging data from diverse sensors. This approach has the potential to free patients from the constraints of centralized hospital structures and allow continuous remote monitoring by medical professionals, improving the quality of care and patient outcomes (Abdelmaboud et al., 2022).

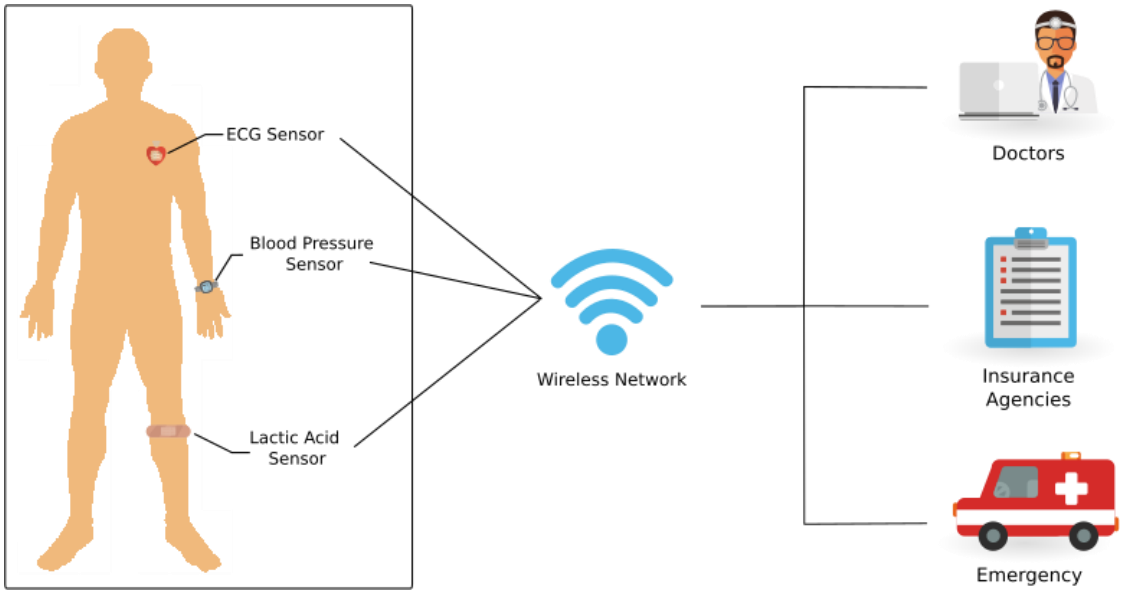


Figure 2. *Smart healthcare system.*

3 RELATED WORKS

In this section, we present a brief overview of selected articles that contribute to the field of blockchain technology in IoT. These articles, published between 2020 and 2024, explored various applications and advancements in utilizing blockchain technology within the IoT domain. Table 1 provides a summary of related works.

3.1 Authentication and access control

Authentication and access control in IoT involve verifying the identities of devices and users, as well as regulating their permissions and privileges to ensure secure interactions within IoT systems and protect data integrity. Numerous exceptional access control models have been proposed by researchers.

Zhang et al. (2023) presented a cutting-edge access control scheme that combines edge computing and license chain technology within the IoT environment. This scheme offers several advantages, including low latency, fine-grained access control and dynamic performance. In the protocol presented by Gupta et al. (2023), users, including medical professionals and relatives, have the ability to access the medical data of patients who utilize wearable medical devices. The protocol operates through a medical server (MS) that stores the patient's medical information, accessible to authorized users via a smart card authentication mechanism.

Stock et al. (2022) proposed a prototype system that combines blockchain, IoT and smart contract technology to create a physical access control system for visitors. This blockchain-based solution offers various benefits compared to centralized systems, including the elimination of single points of failure, prevention of unauthorized data modifications (including those performed by insiders), auditability and resistance to tampering. Zerraza et al. (2024) proposed a solution for authentication and access control in the IoT. The proposed solution integrates the Chacha20 algorithm with higher-order attribute-based access control (HoBAC) and blockchain technology. The security of the proposed solution was evaluated using the Scyther tool. The performance evaluation demonstrates the lightweight nature of the solution as it uses an asymmetric encryption algorithm.

3.2 Healthcare security systems in IoT

Healthcare security systems in IoT focus on safeguarding patient data, securing medical devices and ensuring the privacy and integrity of healthcare information. These systems employ encryption, authentication protocols and intrusion detection measures to mitigate security risks and protect against unauthorized access or data breaches.

In the context of healthcare IoT systems, the storage and computation requirements of blockchain pose challenges due to the large volume of sensitive data involved. To address this, Zaman et al. (2022) proposed a holochain-based framework that offers scalability and resource efficiency, making it suitable for resource-constrained IoT environments. Their thorough analysis and performance results demonstrate that the holochain-based solution outperforms blockchain in terms of resource requirements while maintaining the desired level of privacy and security.

Table 1. *Summary of related works.*

Reference	Application area	Used technology	Proposed solution	Advantages	Limitations
Zhang et al. (2023)	Authentication and access control	License chain technology	Combines edge computing and license chain technology in IoT.	Low latency, fine-grained access control, dynamic performance.	Limited by processing power and storage capacity of edge devices.
Gupta et al. (2023)	Authentication and access control	Smart card	Access control for medical data using a smart card authentication mechanism.	Authorized access to patient information, i.e., only for medical professionals and relatives.	High computational costs, unsuitable for IoMT resource constraints, Significant storage and communication overheads, vulnerable to quantum attacks.
Stock et al. (2022)	Authentication and access control	Blockchain, smart contracts	Physical access control system for visitors using blockchain.	Elimination of single points of failure, prevention of unauthorized data modifications, auditability, resistance to tampering.	Single authority blockchain limits decentralization, wearable design needs enhancements for accessibility and durability, prototype lacks full-scale, long-term usability assessment.

Reference	Application area	Used technology	Proposed solution	Advantages	Limitations
Zerraza, Et al., (2024)	Authentication and access control	Blockchain	Authentication scheme for IoT devices using symmetric algorithm to create a session key and blockchain technology.	Lower computation and communication costs.	Traditional access control methods are unsuitable for IoT systems due to centralized control and complex management. The current protocol design is tested within an edge computing framework, limiting its evaluation scope to edge architecture.
Zaman et al. (2022)	Healthcare security	Holochain	Holochain-based framework for IoT healthcare systems.	Scalability, resource efficiency, maintains privacy and security.	Scalability of holochain in IoT environments, real-time cryptocurrency processing and monitoring, demanding high computation and memory, challenging for IoT nodes.
Chaudhary and Chatterjee (2020)	Healthcare security	Lightweight block ciphers	Discusses lightweight block ciphers (Simon, Speck, HIGHT, LEA) and proposes a modified block cipher technique.	Suitable for constrained devices, improved encryption.	Implements blockchain for decentralized trust, scalable architecture and data immutability, enhancing security.
Rizzardi et al. (2024)	Healthcare security	Blockchain, smart contract	Blockchain-based architecture for protecting medical records, integrating access control mechanisms.	Enhances data security, reduces fraud, improves trust among participants, ensures integrity and traceability of medical records.	High energy consumption and storage demands, scalability remains a concern as the performance tends to degrade slightly when the number of assets increases.
Alshudukhi et al. (2023)	Blockchain security in IoT	Microservice technology	Federation Security System Manager (FSSM) for federated cloud systems.	Interoperability, enhances security and privacy in distributed IoT environments.	Centralized dependency of conventional security methods, creating a single point of failure that compromised system resilience, scalability and complex transaction communications within federated cloud systems, high latency.
Qu et al. (2021)	Blockchain security in IoT	Digital twins (DT)	MinT (miner twin) architecture for fair PoW consensus mechanism.	Fair mining violation detection, effective for IoT environments.	Energy inefficiency, low scalability, high latency, reduced throughput and security issues with PoW.
Ali et al. (2023)	Blockchain security in healthcare	XAI, blockchain	XAI and blockchain-based architecture in the metaverse for healthcare services.	Enhances data safety, privacy, transparency and trust.	High computational resources, scalability and interoperability, resource-intensive requirements for users.
Liu et al. (2020)	Blockchain security in healthcare	Blockchain	BDL-IBS: Blockchain and distributed ledger-based improved biomedical security system.	Enhances privacy and data security, facilitates fast, easy and secure interactions.	Lacks specific protocols for authentication, session keys and data storage or access control.
Taloba et al. (2023)	Healthcare blockchain for IoT	Blockchain	Security architecture utilizing blockchain for maintaining real-time control	High degree of data integrity and traceability, detection of information transitions,	Vulnerability to IoT-specific attacks: IoT devices in healthcare are susceptible to a range of attacks, including wormhole and falsification

Reference	Application area	Used technology	Proposed solution	Advantages	Limitations
			system security and confidentiality.	modifications and medication breaches.	threats, high verification latency.
Nanda et al. (2023)	Healthcare blockchain for IoT	Blockchain, smart contracts	NAIBHSC: Integrated IoT with blockchain for health supply chain management.	Security, privacy, trust, visibility, decentralized tracking and tracing of medical products, prevents counterfeit drugs, mitigates damage to medical components.	Scalability issues: While the approach improves response time and reduces latency for a specific user group (500 users), scalability to larger networks.
Ashraf et al. (2022)	Healthcare blockchain for IoT	AI, blockchain	Combines lightweight ANN and FL in a blockchain-based framework for healthcare data privacy.	Prevents poisoning attacks, ensures transparency and immutability, minimal overhead.	Limited storage and computational resources.

Chaudhary and Chatterjee (2020) explored different lightweight block ciphers for security in healthcare IoT systems. Specifically, they discussed the Simon, Speck, HIGHT and LEA ciphers, highlighting their features, block sizes, key lengths and suitability for constrained devices. Additionally, the authors proposed a modified block cipher technique based on matrix rotation, XOR and expansion functions. Rizzardi et al. (2024) proposed a blockchain-based architecture for the healthcare supply chain to protect medical records from tampering and breaches. The architecture uses Hyperledger Fabric and smart contracts for secure, traceable medical records, with access control for authorized personnel.

While these contributions offer insights into lightweight block ciphers for healthcare IoT security, it is important to acknowledge certain weaknesses associated with these approaches. Firstly, limited scalability can be a concern as the numbers of devices and data in healthcare IoT systems increase. The performance of lightweight block ciphers may degrade under such circumstances. Secondly, traditional lightweight block ciphers often rely on a centralized trust model, introducing a single point of failure. If the central authority or key management system is compromised, the security of the entire system is at risk. Lastly, lightweight block ciphers primarily focus on encryption and decryption but lack built-in mechanisms for data integrity and immutability. This poses challenges in ensuring the integrity of healthcare data throughout their life cycle.

3.3 Blockchain security in IoT

Blockchain (BC) security in IoT involves making use of the decentralized and tamper-resistant nature of blockchain technology to enhance the security and privacy of IoT devices and data. It offers benefits such as immutability, data integrity, transparency and distributed consensus mechanisms to mitigate risks and vulnerabilities in IoT systems.

Alshudukhi et al. (2023) introduced BC security managers based on microservice technology (MS) for federated cloud systems in the IoT context. Specifically, they presented the Federation Security System Manager (FSSM), which is designed with interoperability features to facilitate transaction exchange between permissioned BC managers operating across different cloud providers. Their proposed framework effectively enables interoperability, enhances security and ensures privacy in distributed IoT environments that rely on the federated cloud system.

Qu et al. (2021) proposed a MinT (miner twin) architecture, which utilized an edge-fog-cloud paradigm to enable a fair PoW consensus mechanism. They presented a PoC (proof of concept) prototype and an experimental study using Raspberry Pis, a fog server and containerized PoW modules. SSA (singular spectrum analysis) detected change points and PoB (proof of behaviour) ensured fair mining detection. While the authors' work showcased several positive aspects in their proposed MinT architecture, there are certain weaknesses that need to be addressed. The use of PoW as the consensus mechanism introduces concerns related to energy efficiency, scalability, latency, throughput and security. The energy consumption associated with PoW can be substantial and unsustainable in the long run. Additionally, as the network grows, PoW faces scalability challenges, leading to slower transaction processing and potential bottlenecks. The confirmation times in PoW can result in higher latency, which may not be

suitable for real-time healthcare applications. Furthermore, the throughput of PoW-based systems is limited, which can restrict the number of transactions the system can handle effectively.

3.4 Blockchain security in healthcare

Blockchain security in healthcare utilizes the decentralized and immutable features of blockchain technology to strengthen data integrity, privacy and access control in healthcare systems. It provides a secure framework for sharing and managing sensitive patient information while mitigating the risks of unauthorized access or tampering.

Ali et al. (2023) introduced an architecture that combines explainable artificial intelligence (XAI) and blockchain in the metaverse to enhance healthcare services in a secure and realistic digital space. The paper explores the building block technologies of the metaverse and discusses the advantages and challenges of using it in healthcare. Liu et al. (2020) introduced a blockchain and distributed ledger-based improved biomedical security system (BDL-IBS) to enhance privacy and data security in healthcare applications. The system allows patients to control their data and ensures secure consent for sharing across organizations, using blockchain to manage and secure medical information. The results demonstrate that blockchain-based digital platforms facilitate fast, easy and secure interactions between data suppliers, thereby enhancing privacy and data security, including for patients.

However, the proposed biomedical security system with blockchain exhibits several potential weaknesses that should be considered when assessing its effectiveness. Firstly, the unclear trust and privacy factors, along with the limited adversary model, raise concerns about the ability of the system to address a wide range of threats. Moreover, the absence of specific protocols and algorithms for authentication and session keys, as well as the lack of information on data storage and access control, raise doubts about the overall system security. Finally, the absence of real-world implementation and evaluation further limits the understanding of the system robustness and resilience to actual threats and attacks.

3.5 Healthcare blockchain for IoT

Healthcare blockchain for IoT combines blockchain technology with the IoT in healthcare systems to improve data security, privacy and interoperability, enabling secure and efficient management and sharing of healthcare data and services.

Taloba et al. (2023) utilized IoT in healthcare to enhance patient care and resource distribution while reducing costs. To mitigate risks associated with IoT devices, blockchain technology was proposed. The architecture enhances data integrity and traceability by detecting breaches. Nanda et al. (2023) introduced a novel approach for integrated IoT with blockchain in the health supply chain (NAIBHSC). This approach helps prevent counterfeit drugs, mitigate damage to medical components, facilitate authentication and provide real-time status updates during the shipment process from manufacturers to end users. However, the integration of blockchain and IoT in health supply chain management, as proposed in this approach, shows potential but raises concerns regarding data encryption and security. Weaknesses include Solidity contract vulnerabilities, and off-chain data and IoT device security must also be assessed.

Ashraf et al. (2022) introduced the FIDChain IDS, which combines lightweight artificial neural networks (ANN) and federated learning (FL) in a blockchain-based framework to preserve healthcare data privacy. The FIDChain IDS prevents poisoning attacks, ensures transparency and immutability and has minimal overhead by aggregating local weights and broadcasting updated global weights. However, the proposed system has weaknesses in data encryption and security. The centralized architecture risks a single point of failure and while an edge-based blockchain adds security, encryption for edge-to-cloud data transmission is insufficient. Cloud-based blockchain security, including access controls and attack protection, must also be addressed.

4 PROPOSED APPROACH

In this section, we introduce a blockchain-based security solution designed for specific IoT systems, specifically a healthcare monitoring system. Our focus is on a typical remote patient monitoring system in which patients utilize wearable healthcare IoT devices to collect health-related data such as heart rate, walking distance and sleeping conditions. Patients retain control over their data and can grant or revoke access to healthcare providers as needed. In cases where treatment is required, patients can selectively share their data with relevant healthcare providers and

once treatment is complete, they can revoke access to the network. Our proposed architecture, illustrated in Figure 3, features three tiers: the patient (equipped with wearable devices), the fog computing system (transmitting patient data to servers and executing the smart contract) and the smart servers of the hospitals that validate and store the blockchain.

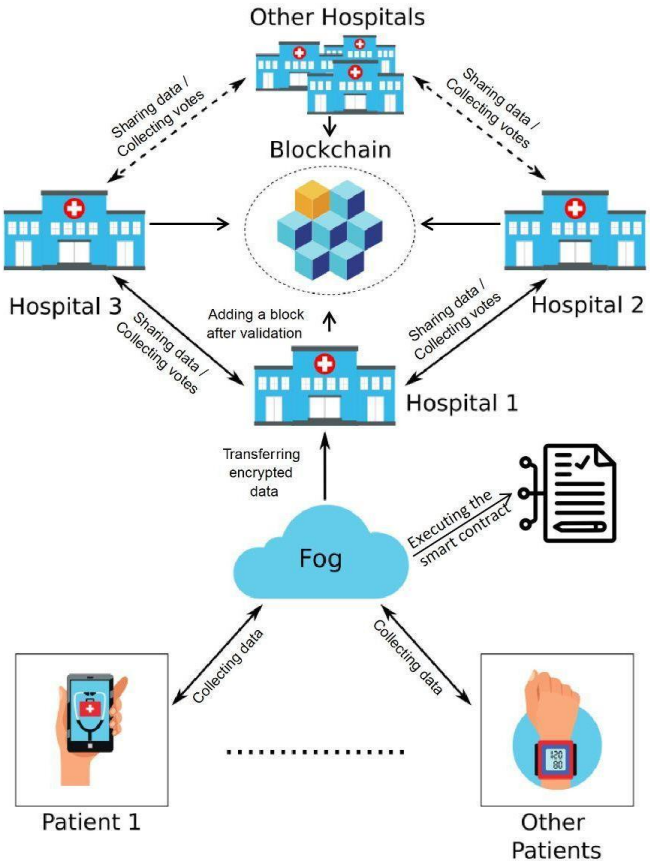


Figure 3. *Blockchain security in healthcare IoT.*

4.1 Patient health monitoring and alert system

In the proposed scheme, the patient health monitoring and alert system plays a crucial role in ensuring the timely detection of abnormal health conditions and notifying the patient accordingly. To initiate the process, each patient undergoes a key generation phase where a unique set of public and private keys is generated for them. These keys serve to authenticate, encrypt and secure the patient's data throughout the system.

The patient wears a healthcare smartwatch equipped with sensors to continuously monitor their vital signs and health parameters. The smartwatch collects data such as heart rate, blood pressure, temperature and other relevant physiological measurements. To ensure data privacy and security, the patient's private key remains securely stored on the smartwatch, while the public key is shared with the hospital's smart server.

4.1.1 Key generation

During the key generation phase, the patient is assigned a pair of cryptographic keys: a public key and a private key. The private key is generated within the patient's healthcare smartwatch using a strong cryptographic algorithm. The private key remains securely stored on the smartwatch and is used for decrypting sensitive information received from the hospital and signing data to ensure data integrity. On the other hand, the public key is generated using the same algorithm and shared with the hospital's smart server.

Regarding the cryptographic scheme, we use elliptic curve cryptography (ECC), as it is more suitable for IoT devices with constrained resources. ECC provides security with smaller key sizes compared to other schemes such as RSA. The key size that we use for ECC encryption/decryption and Schnorr signatures is 256 bits, and the cryptographic hash function used is SHA-256. This size offers a balanced trade-off between efficiency, memory usage and adequate

security (128-bit level in ECC), making it suitable for most practical applications such as healthcare. Besides, SHA-256 offers strong security against collision and pre-image attacks, with greater resistance than older functions such as MD5 and SHA-1. Its fixed 256-bit output enhances data integrity and provides a balance of security and efficiency, making it ideal for applications such as digital signatures and blockchain. Additionally, SHA-256 is widely adopted in security protocols such as SSL/TLS and cryptocurrency systems, ensuring compatibility and trust.

In our paper, we employ ECC for encryption and Schnorr signatures for authentication, providing strong security and efficiency in resource-constrained environments. Compared to Zhang et al. (2023), who also used ECC, our method enhances authentication with the compact Schnorr signature scheme, reducing computational overhead. Lattice-based cryptography (Gupta et al., 2023) is resilient to quantum attacks but requires larger key sizes. The hash chain method (Stock et al., 2022) focuses on transaction integrity but lacks the public-key advantages of ECC. ChaCha20 (Zerraza et al., 2024) allows fast symmetric encryption but offers less authentication than our approach. Zaman et al. (2022) faced key management complexities that our ECC solution simplifies, while SHA-256 (Alshudukhi et al., 2023) lacks public-key benefits. Lastly, X.509 digital certificates (Rizzardi et al., 2024) may introduce management overhead, whereas our approach is more streamlined. Overall, our methods effectively balance security and resource efficiency, making them advantageous for IoT applications.

4.1.2 Transmission and processing of patient data

When the smartwatch detects any unusual readings or symptoms exceeding predefined thresholds, such as abnormal heart rate or elevated temperature, it promptly triggers an alert to notify the patient. The alert can be in the form of a visual or auditory notification, ensuring that the patient is promptly informed about the potential health concern.

Upon receiving the notification, or after the timeout ending (in case the patient is unconscious), the patient can respond by acknowledging the alert through the smartwatch interface. By acknowledging the alert, the patient indicates their consent to share their health data with the healthcare system for further analysis and assistance. In response to the patient's acknowledgment, the smartwatch initiates the transmission of the patient data to the fog network.

4.2 Fog network communication and hospital selection

During this phase, the fog network plays a crucial role in collecting patient data and securely transmitting them to the hospital server. This transmission is carried out using a secure algorithm, which will be elaborated upon in the subsequent sections. Additionally, we introduce a complementary sequence diagram (Figure 4) detailing the initial steps of our approach; this offers a more nuanced understanding of our proposed solution.

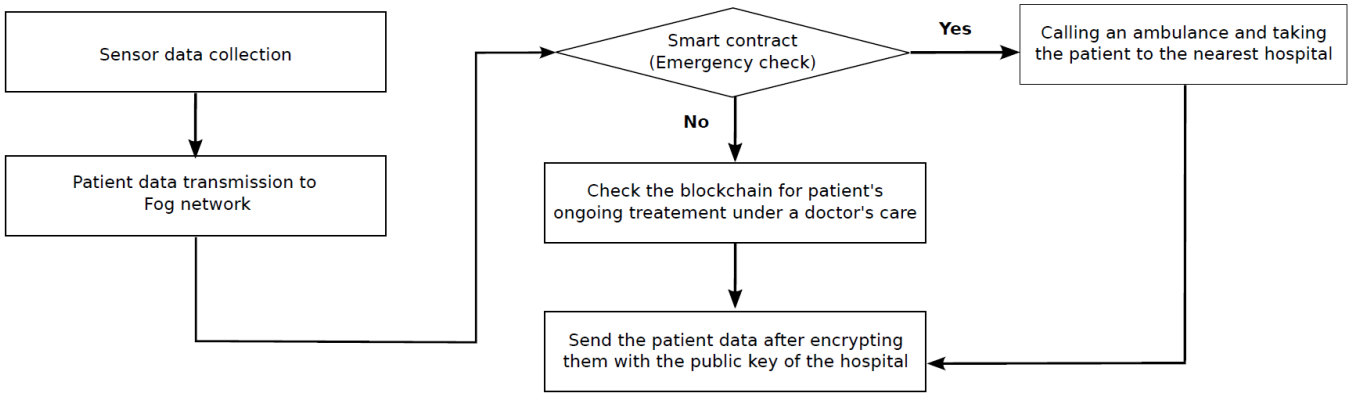


Figure 4. *Collecting and transmitting data.*

4.2.1 Data collection and communication with fog

After the wearable device collects the necessary data, including the patient's health readings and location information, the collected data are transmitted to the nearby fog network. The fog network, which can be a smartphone or computer, serves as an intermediary between the wearable device and the healthcare system. It acts as a bridge for transmitting the relevant data to the appropriate entities. The fog network establishes communication

with the smart contract, providing the necessary data to identify the most suitable hospital to receive the alert. This data may include the patient's health parameters, location coordinates and other pertinent information. The smart contract, which operates on the blockchain, responds by providing details about the designated hospital, such as its IP address and public key.

4.2.2 Data encryption and emergency response

In emergency situations, the smart contract analyses the received data to determine if they qualify as an emergency. If an emergency is identified, the smart contract initiates immediate actions. First, it triggers a call for an ambulance and dispatches it to the patient's location for prompt transportation to the nearest hospital.

Simultaneously, the smart contract acquires the public key of the designated hospital and transmits it to the fog network. This enables the fog network to encrypt the patient's data using the hospital's public key, ensuring that only the hospital, possessing the corresponding private key, can decrypt and access the encrypted data. This encryption process guarantees the confidentiality and integrity of the transmitted information, safeguarding the patient's privacy.

After the encryption algorithm regenerates the ciphertext, we add an additional layer of security to our protocol by implementing a digital signature. This cryptographic mechanism authenticates the integrity, origin and authenticity of a digital document or message. It provides a way to verify that the content has not been altered or tampered with since it was signed and that it was indeed signed by the claimed sender. We specifically chose the Schnorr signature due to its efficiency and smaller signature size, which is crucial for performance in IoT healthcare systems. Unlike other schemes, the Schnorr signature is resistant to forgery attacks, providing robust security against potential breaches. The unique signature it creates for each message uses a private key held by the signer, ensuring both confidentiality and traceability. This signature is then attached to the message and can later be verified using the corresponding public key. As presented in Algorithm 1, the Schnorr signature involves three main steps: key generation, signing and verification after receiving the message (Zhang et al., 2023).

Algorithm 1. *Schnorr signature algorithm.*

Input: Message M

Output: Signature (r, s)

Key generation:

Choose prime numbers p and q and a generator g of order q

Select private key x (a random integer in the range [1, q − 1])

Compute public key $y \equiv g^x \ (mod\ p)$

Signing:

Choose a random number $\boldsymbol{k}$ in the range $[\boldsymbol{1}, \boldsymbol{q-1}]$

Compute $\boldsymbol{r \equiv g^k mod\ p}$

Compute $\boldsymbol{e \equiv H(M) \oplus H(r)}$

Compute $\boldsymbol{s \equiv (k + ex) mod\ q}$

Return signature $(\boldsymbol{r}, \boldsymbol{s})$

Verification:

After receiving the message M , the signature (r, s) and the public key y:

Compute $e \equiv H(M) \oplus H(r)$

Compute $w \equiv s^{-1} mod\ q$

Compute $u1 \equiv ew\ mod\ q$

Compute $u2 \equiv rw\ mod\ q$

Compute $v \equiv (g^{u1}.y^{u2}\ mod\ p) mod\ q$

```
if v=r then
            The signature is valid.
      end
else
            The signature is invalid.
      end
```

The encryption algorithm used to secure the patient's data before transmission can be described as presented in Algorithm 2. This algorithm outlines the step-by-step process involved in encrypting the patient's data. To begin, the patient's data are encrypted using the hospital's public key. This encryption process ensures that only the hospital, possessing the corresponding private key, can decrypt and access the encrypted data. By encrypting the patient's data directly with the hospital's public key, the algorithm guarantees the confidentiality and integrity of the transmitted information.

Algorithm 2. *Encryption algorithm.*

```
Input:      PatientData: Patient's data to be encrypted
            HospitalPublicKey: Public key of the hospital
Output:     EncryptedData: Encrypted patient's data
//Steps:
EncryptedData       ←       Encrypt(PatientData, HospitalPublicKey)
return      EncryptedData + Schnorr signature
```

4.2.3 Non-emergency situation and hospital selection

In non-emergency situations, the smart contract performs an additional verification step. It scans the blockchain to determine whether the patient is already undergoing treatment for their specific condition under a doctor's care. If the patient is receiving treatment, the smart contract retrieves the details of the hospital where the treating doctor practices. The pertinent patient information is securely transferred to this hospital to ensure continuity of care and informed decision making. If the patient is not receiving treatment at any hospital, the smart contract applies the rule of selecting the nearest hospital. It identifies the nearest healthcare facility based on the patient's location and transfers the necessary patient data to initiate the appointment scheduling process. This ensures that the patient receives appropriate medical attention and facilitates efficient coordination between the patient and the healthcare provider.

Algorithm 3 below describes the conditions and actions performed by the smart contract based on the emergency or non-emergency state. It highlights the critical role of the fog network communication and hospital selection phase in efficiently routing patient data, ensuring secure transmission and facilitating timely healthcare interventions. By utilizing the capabilities of the fog network and the smart contract, the system optimizes resource allocation, enhances response times and improves overall patient care.

Algorithm 3. *Smart contract algorithm.*

```
Input: State (emergency or non-emergency)
//Steps:
if state == "emergency" then
      //Trigger a call for an ambulance and dispatch it to the patient's
      location.
      call ambulance
end
if state == "non-emergency" then
      //Perform an additional verification step
```

```
        //Scan the blockchain to check whether the patient is already undergoing
        treatment.
        if patient is receiving treatment then
              // Retrieve details of the hospital where the treating doctor
              practices.
              // Transmit the public key of the designated hospital to the fog
              network.
              Encrypt(PatientData, publicKey)
        end
        if patient is not receiving treatment then
              // Apply the rule of the nearest hospital based on the patient's
              location.
              // Transfer the patient's data to the nearest hospital for
              appointment scheduling.
              if hospital == nearest then
                    transfer(PatientData)
              end
        end
  end
```

4.3 Hospital smart server and treatment protocol management

This session involves the smart server at the hospital receiving the ciphertext transmitted from the fog network. The server utilizes its private key to decrypt the ciphertext, thereby gaining access to the content of the message. With this information, the server can make informed decisions and communicate the necessary instructions to the relevant hospital staff, who will then proceed to implement the prescribed protocol.

This phase of the system focuses on the hospital smart server, where decisions regarding patient care are made based on the nature of the situation, i.e., whether it is an emergency or a non-emergency scenario. The role of the smart server is crucial in coordinating medical staff, ensuring prompt actions, securely transmitting data and maintaining a comprehensive record of the treatment process.

Upon receiving the data, the server analyses them and determines whether they correspond to an emergency or a normal situation, each of which will be further explained below.

4.3.1 Emergency care management

The utilization of a smart contract can significantly save time by promptly initiating an ambulance call for the patient. This enables the server to make critical decisions regarding patient care. After reviewing the received data, the server contacts the required doctors and nurses. If a surgical room is required, the server issues instructions for its preparation. In instances where no rooms are available at the current hospital, the server automatically searches for nearby hospitals that can accommodate the patient. The server dispatches the ambulance to the new location and securely transmits the patient's data to the other hospital's server using its public key, ensuring the confidential transmission of sensitive information. Through these automated processes, patients can receive timely and appropriate care during critical moments. Once the necessary care has been given to the patient, the server records the executed protocol, along with the patient's medical data and treatment outcome. This record undergoes validation by other servers and is added to a block within the blockchain.

The emergency care management phase, as governed by Algorithm 4, utilizes a smart contract to make critical care decisions and ensure timely interventions. The algorithm outlines the steps involved in reviewing patient data, contacting medical staff, coordinating surgical room preparations and securely transmitting information to other hospitals for efficient and confidential care delivery.

Algorithm 4. *Emergency care management algorithm.*

```
Input: Patient data, Emergency condition flag
Output: Executed protocol record
//Steps:
Verify (Schnorr signature)
if Emergency == true then
      Review received data; contact required doctors and nurses.
      if surgical room is required then
            Issue instructions for surgical room preparation.
            if no rooms available at current hospital then
                  Search for nearby hospitals to accommodate the patient;
                  dispatch ambulance to the new location.
                  Transmit patient's data to other hospital's server using public
                  key encryption.
            end
      end
      Give the patient necessary care.
      Record executed protocol, patient's medical data and treatment outcome
      Validate the record by doctors of other servers.
      Add the validated record to a block within the blockchain.
end
```

4.3.2 Non-emergency care management and consensus gathering

In non-emergency cases, the hospital smart server coordinates doctors' decision making and consensus on treatment protocols. It facilitates meetings to discuss the patient's condition and determine the best treatment. Once decided, the server shares the protocol and hashed medical data with all connected servers in the blockchain network to ensure privacy. Moreover, sharing treatment protocols and medical data between hospitals ensures consistent, high-quality care by providing healthcare providers with a unified, secure view of a patient's medical history. This enables timely, coordinated responses and informed decision making across facilities.

Algorithm 5. *Non-emergency care management and consensus gathering algorithm.*

```
Input: Emergency condition flag
Output: Suitable protocol
//Steps:
if Emergency == false then
      Make a meeting with relevant doctors.
      Return the suitable protocol.
      Distribute the protocol to other connected servers .
      Apply consensus.
      Retrieve responses.
      Add data to the blockchain.
End
```

Doctors review the protocol and provide feedback, either approving or suggesting improvements. The RaftNode consensus algorithm collects responses from all servers to determine the majority opinion. Once consensus is reached, the validated protocol is added as a new blockchain block, ensuring consistency and reliability in future

treatments. The RaftNode consensus algorithm enables collaboration, makes use of medical expertise and ensures the quality of treatment protocols in the blockchain. Algorithm 5 outlines the non-emergency care management, decision making and consensus gathering phase, which will be detailed further in the next section.

4.3.3 Consensus

In the consensus phase, the RaftNode consensus algorithm is utilized to establish consensus among the distributed servers. In our approach, we ensure that most participating servers agree on the treatment protocols to be added to the blockchain, as shown in Figure 5. Before diving into the specific implementation details of the RaftNode consensus algorithm used in this paper, let us first provide a general overview of RaftNode consensus.

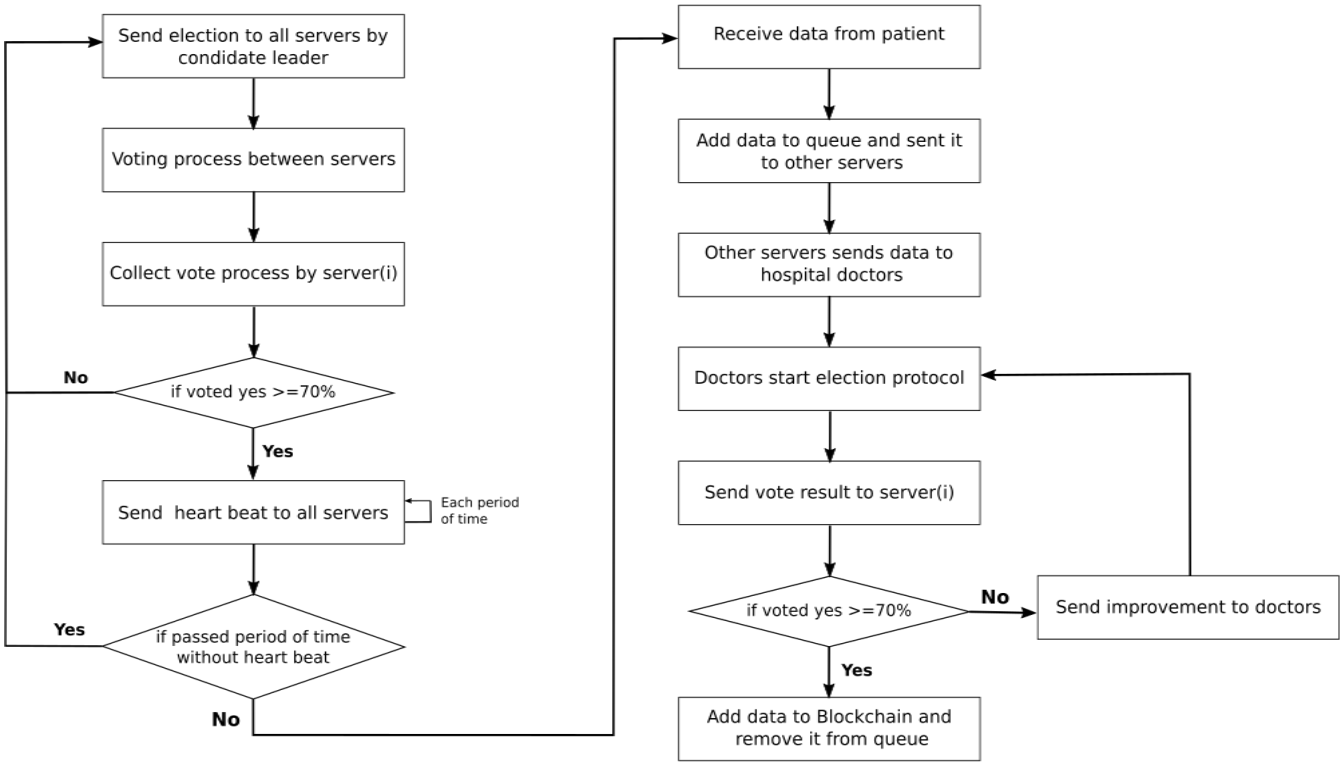


Figure 5. *Consensus and blockchain validation flowchart.*

The RaftNode consensus algorithm is a widely adopted consensus algorithm for managing a replicated log. It is designed to provide fault tolerance and strong consistency in distributed systems. In our implementation, the RaftNode algorithm is employed to achieve consensus among the hospital smart servers regarding the treatment protocols. Given the critical nature of healthcare data, the raft consensus protocol provides fault tolerance, prevents unauthorized access and maintains data consistency, all of which are paramount for handling sensitive patient information securely. Therefore, consensus is indispensable in our approach, as it establishes a reliable, trustworthy environment for managing treatment protocols and patient data.

In comparison with other blockchain consensus mechanisms, raft consensus stands out for its high throughput and low latency, making it ideal for real-time applications such as healthcare IoT where fast, reliable data processing is essential. Unlike proof of work (PoW), raft is energy-efficient, avoiding the need for intensive computation, which is especially beneficial for resource-limited environments. Its leader-based design enables rapid decision making and straightforward log replication across nodes, distinguishing it from proof of stake (PoS) and practical byzantine fault tolerance (PBFT), which can be slower or more complex. While raft does not handle byzantine faults as PBFT does, it ensures strong consistency and quick recovery through efficient leader election, making it a streamlined yet robust choice for distributed networks.

The consensus process in our approach begins with the election of a leader node. When the nodes are initially created, one of the nodes sends a message to all other nodes expressing its intention to become the leader. The voting

process commences, where nodes cast their votes by either accepting or rejecting the candidate node as the leader. If there is no current leader, the nodes vote with a ”yes” to support the candidate node. The votes are sent to the candidate node and when 70% of the votes received are ”yes”, the candidate node becomes the leader. Throughout the simulation, the leader node regularly sends heartbeats to all other nodes, indicating its leadership and continued liveliness. In case the leader fails to send the heartbeat within a specific period, the other nodes detect the failure and initiate a new leader election process.

Once a leader is elected among the nodes, it takes responsibility for adding its own block to the blockchain. The leader then delegates the task of adding subsequent blocks to another server that wants to add a transaction in a round-robin fashion, ensuring that all participating servers actively contribute to the growth and maintenance of the blockchain.

Algorithm 6 below describes the leader election phase within the consensus phase of the RaftNode consensus algorithm. This phase ensures the selection of a leader node among the hospital smart servers, facilitating the consensus and coordination of treatment protocols within the blockchain network.

Algorithm 6. *Consensus phase – RaftNode consensus (leader election).*

```
Input: Nodes (set of hospital smart servers)
Output: Leader election
// Steps:
Create (nodes)
// Create a set of hospital smart servers connected within the blockchain network
Start leader election function; distribute (NodeiId) to nodes
Vote = yes / no (depends on the queue).
Collect vote responses.
if voted yes by >= 70% then
            Nodei = leader
      end
else
      Restart leader election
end
Send heartbeat function.
Every (specificPeriod)  Send heartbeat to other nodes.
if time > specificPeriod without receiving heartbeat then
      Restart leader election
end
```

4.3.4 Validation and addition to blockchain

Moving on to the phase of validation and adding to the blockchain, when data arrive at the hospital smart server and reach the step of being sent to other servers, the information is temporarily stored in a queue, awaiting validation. This queue acts as a transaction buffer, holding the data until they undergo the validation process before being added to the blockchain. The data stored in the queue include crucial information such as the patient’s ID, name, health information, public key, emergency state and the treatment protocol suggested by the hospital doctors, in addition to the server ID. These details collectively form a transaction that represents the patient’s treatment plan. By storing the data in the queue, the hospital smart server ensures that all necessary information is available for validation and inclusion in the blockchain. The queue acts as an intermediate step, allowing the coordination of validation among distributed servers before committing the transaction to the blockchain. Therefore, the validation of the blocks is a collaborative process handled by the distributed servers within the blockchain network. Each

participating server evaluates the incoming transactions stored in the queue, verifying their authenticity and ensuring they meet the predefined criteria for inclusion in the blockchain. Our blockchain implementation is based on a private blockchain network shared among all participating hospitals, rather than individual networks for each hospital. This shared private blockchain enables secure, coordinated collaboration and data exchange across hospitals while ensuring decentralized control over access and network operations.

Once the validation process takes place and consensus is reached among the participating servers, the transaction is considered validated and it is then added to the blockchain. This ensures that only verified and approved treatment protocols are permanently recorded in the blockchain, promoting the consistency, integrity and reliability of the patient's medical records within the decentralized network. Our blockchain implementation is based on a single private blockchain network exclusively shared among the participating hospitals. This private blockchain ensures that the network is secure and accessible only to authorized participants, guaranteeing the confidentiality and privacy of patient data. It enables secure collaboration and data exchange between hospitals while maintaining control over the blockchain network operations. The validation process is initiated through an election among the distributed servers. Each doctor on every server casts their vote by either approving the protocol or suggesting improvements to enhance patient care. The responses from all participating servers are collected by the hospital smart server. If 70% of the responses indicate approval ("yes" votes), the data are considered validated and are added as a new block to the blockchain. However, if the approval threshold is not met, the hospital smart server sends a request to its doctors, incorporating the suggested improvements from other servers. The doctors collaborate to create a revised treatment protocol that addresses the concerns raised by the servers. While this process increases the daily workload of doctors, the collective votes of a majority of medical professionals are valuable in ensuring consistent and high-quality patient care. By involving multiple doctors in the validation process, the system ensures that treatment decisions and medical records are thoroughly checked, reducing the risk of errors that might arise from individual treatment. However, this idea of including doctors is supplementary; we can be satisfied by implementing voting in the consensus algorithm, which is handled by servers to validate block information.

To further enhance the security of our blockchain, each block within the chain contains only one transaction. This design choice ensures that any attempt to tamper with or modify the blockchain would require altering every single block, making it practically impossible and highly resistant to unauthorized modifications. Moreover, as a time-based measure, a new block is created approximately every 7 minutes, regardless of whether a new transaction has been added. This periodic block creation further strengthens the security of the blockchain, as it increases the complexity and effort required to manipulate the system. By combining the implementation of single transaction blocks and the regular creation of new blocks, our blockchain achieves an exceptionally robust and secure environment for storing and managing patient treatment protocols. Algorithm 7 outlines the steps for validating and adding blocks to the blockchain, as part of the consensus phase using the RaftNode consensus algorithm.

Algorithm 7. *Consensus phase – RaftNode consensus (block validation).*

```
Input: Patient data (set of data to be validated)
Output: Blockchain creation
//Steps:
After receiving patient data
Add data to the queue
Send data + Schnorr signature to other servers
//Other servers side:
Upon receiving data from server (i)
Verify Schnorr signatures
Send data to hospital doctors
Start protocol election
Vote = yes / to improve
if vote == yes then
```

```
                Send vote to server (i)
        end
    else
        Suggest improvement
        Send improvement to server (i)
    end
    //Server (i) side:
    Upon receiving votes from other servers
    if voted by yes >= 70% then
        Add data to the blockchain
        Remove data from the queue
        end else
        Send improvement suggestions to doctors
        Receive newProtocol from doctors data.protocol = newProtocol
        Restart protocol election between doctors
    end
    if (transactionsNumber == 1) OR (time >= 7 min) then
        Add new Block // an empty one
    end
```

It is important to note that the patient's ID and name are the only pieces of information that are encrypted. This ensures that doctors accessing the information cannot identify the patient. Only the hospital and the doctor have access to the patient's identity. Furthermore, even in the event of a security attack, the patient's ID remains unidentifiable. The patient has the ability to access their own information stored in the block using their private key, which grants them access to their data while preserving the privacy of others in the block.

In summary, the consensus phase utilizes the RaftNode consensus algorithm to achieve agreement among the distributed servers regarding treatment protocols. The validation and adding to the blockchain phase involve collecting responses from servers, validating the data based on a specified threshold and incorporating suggested improvements. The patient's privacy is safeguarded through encryption and the use of private keys for accessing their own information within the block.

5 INFORMAL SECURITY ANALYSIS

In the following, we demonstrate the resilience of the proposed scheme against some known attacks and highlight several advantages:

- **Impersonation and man-in-the-middle attacks:** Starting with an impersonation attack, where someone falsely assumes the identity of another person, such as a man-in-the-middle attack (MITM), our system effectively mitigates these threats by employing the Schnorr signature for authentication. This signature ensures secure and reliable identification.
- **Privacy and anonymity:** By securely encrypting patients' personal information, our system provides a significant advantage in terms of anonymity. This safeguards user privacy, ensuring that all users can keep their personal lives private and stay safe.
- **Immutability:** The use of blockchain technology guarantees data immutability, making it impossible to alter or modify data once they have been added to the blocks. This enhances the integrity and reliability of our system.
- **Distributed denial of service attack:** Implementing a distributed network of blockchain helps mitigate traffic-related issues and serves as a major defence against distributed denial of service (DDoS) attacks. As

detailed in the upcoming section, our system is designed to handle massive amounts of data efficiently and that also helps mitigate traffic.

- **Decentralization and stability:** With the utilization of the RaftNode consensus protocol, our system ensures that there is always a designated leader responsible for writing its blocks to the blockchain. This approach minimizes problems in critical sections and strengthens decentralization by avoiding selecting the same leader each time. Additionally, the RaftNode protocol utilizes heartbeats to promptly detect any server failures, enabling swift action and maintaining system stability.
- **Data integrity:** After the server receives all votes and if the majority votes are in favour of "yes", the server begins the necessary steps to add the new block. Subsequently, each server receives a copy of that block along with the corresponding signature. If all the information is correct and the signature is valid, all the servers should add the block to their chain. However, if any discrepancies are found, the block is rejected and the process moves on to the next one.

6 SIMULATION AND RESULTS

6.1 Architecture model using NS3

In our scheme implementation, we adopted an architecture model using NS3 to simulate and evaluate the effectiveness of our proposed solution. The architecture model encompasses a carefully designed network topology that replicates real-world scenarios in healthcare IoT systems.

6.1.1 Topology and network design implementation

Our topology centres on a patient node that connects via a peer-to-peer (p2p) link to the fog network, a WiFi-based system of interconnected nodes. The fog network connects to a node representing the hospital's smart server, which manages data processing within the hospital's infrastructure. The server is linked to a local area network (LAN) that connects doctors' workstations for efficient communication. Besides, to ensure interoperability, the smart server connects to a wide area network (WAN), enabling secure data exchange between distributed hospital servers. Using technologies such as VPN or encrypted connections, hospitals can establish a protected communication channel. The networks in the system are interconnected via p2p links, allowing simultaneous data transmission and efficient real-time communication across patients, fog nodes and hospital servers.

Figure 6 represents our topology, illustrating the interconnected networks and nodes within the architecture model. The figure visually depicts the patient node, the fog network, the smart server and the connections between them.

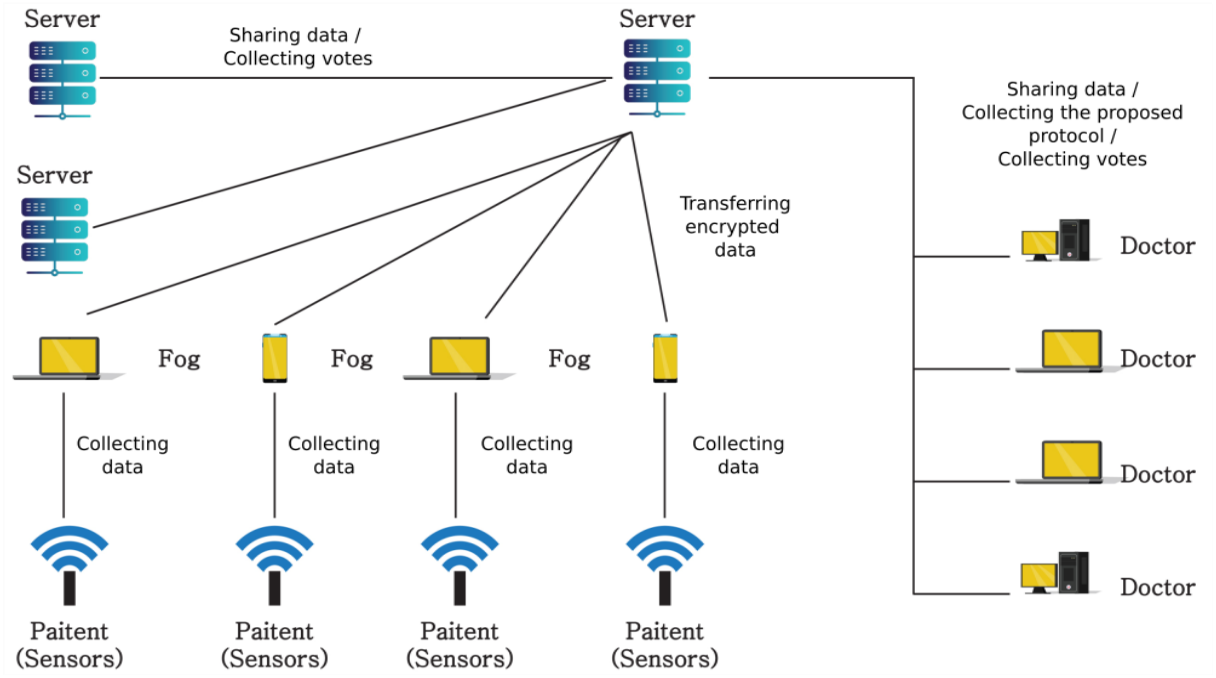


Figure 6. *Topology illustration.*

6.1.2 Simulation process

The simulation process begins with the patient's data being transmitted from their smart device to the fog network via wireless connections. The smart contract then checks whether the data indicate an emergency. If so, the fog network generates a packet containing the data and forwards it to the smart server, which acts as the central hub. The server then distributes the data to doctors and other hospital servers, enabling timely access and decision making.

The smart server receives a protocol along with the patient data and uses the RaftNode consensus algorithm to involve other servers in the network for validation. Servers vote on the protocol and once consensus is reached, they send their voting results back to the smart server. The smart server evaluates the results, determines whether the protocol is approved or requires adjustments and communicates the outcome to the doctors. It then adds the relevant data to the blockchain for secure storage and immutability, completing the simulation for evaluating protocol effectiveness and consensus efficiency in healthcare.

6.2 Simulation parameters

This section outlines the various configuration parameters utilized in our simulation. Table 2 presents different parameters of each node in the system, while Table 3 displays the data types and length.

Table 2. *Configuration of nodes.*

Node type	RAM (MB)	Upload bandwidth (MB)	Download bandwidth (MB)	Busy power (Joules)	Idle power (Joules)	Level
Server	102400	100	100	1500	130	0
Doctor	4096	10	100	51.34	2	1
Fog	2048	5	100	15.25	1	1
Sensor	No RAM	0.3	0	1.26	0.1	2

- The cost of sending a message for the sensor and fog is 1.5 joules.
- The costs of sending a message to servers and doctors depend on the data length.
- The latency between server and fog is 120 seconds.
- The latency between server and doctor is 60 seconds.
- The latency between server and server is 150 seconds.

Table 3. *Configuration of data.*

Data type	Data length
Collected data	8 Mb
Hashed data	30 Mb
Vote	5 Mb
Suggested protocol	15 Mb
Suggested improvement	15 Mb
Heartbeat	5 Mb
Transaction	150 Mb

- Latency between sensor and fog: 10 seconds
- Number of servers: 6
- Number of doctors: 125
- Number of fogs: 30
- Number of sensors: 30

6.2.1 Complexity of proposed work

The algorithm complexity is $O(mn)$, where m represents the number of messages in the system and n is the number of participants in the network. Additionally, we calculated other critical criteria, such as energy consumption, time efficiency and throughput, to assess the speed and effectiveness of our work. We conducted simulations using the network simulator NS3, which aided us in testing the complexity of the algorithm, particularly regarding the number of participants and messages.

6.3 Comparison graphs

6.3.1 Discussion of throughput graph

Figure 7 illustrates the relationship between the number of blocks and the throughput. The x-axis represents the throughput in Mbps (megabits per second), while the y-axis represents the number of blocks. The comparison results demonstrate that our contribution can handle a greater volume of bits and transactions compared to the PoW under various difficulties (the hash value of the block starts with 2 zeros, 3 zeros or 4 zeros). This is due to the higher throughput values, which indicate faster data transfer and processing rates. Consequently, more blocks can be created within a given time frame, enhancing the security of our blockchain.

This experiment highlights the capability of our approach to manage higher data flow and transaction volume, making it suitable for real-time applications where quick data processing is crucial.

6.3.2 Discussion of energy graph

Figure 8 visually presents the energy expended during the block creation process, comparing our contribution to the PoW approach. The x-axis displays the energy consumed in joules, while the y-axis represents the number of blocks. Upon careful examination, a stark contrast becomes evident in the energy consumption between our contribution and PoW for each difficulty level. This discrepancy arises from the significant amount of joules required by PoW for calculating the hash value, coupled with the relatively low probability of successfully identifying the correct nonce. In contrast, our approach demonstrates remarkable energy efficiency, as it does not demand such a substantial energy expenditure. In fact, our contribution proves to be highly economical in terms of energy utilization during block creation.

This result demonstrates the energy efficiency of our approach, an important factor for sustainable blockchain solutions, especially in resource-constrained environments.

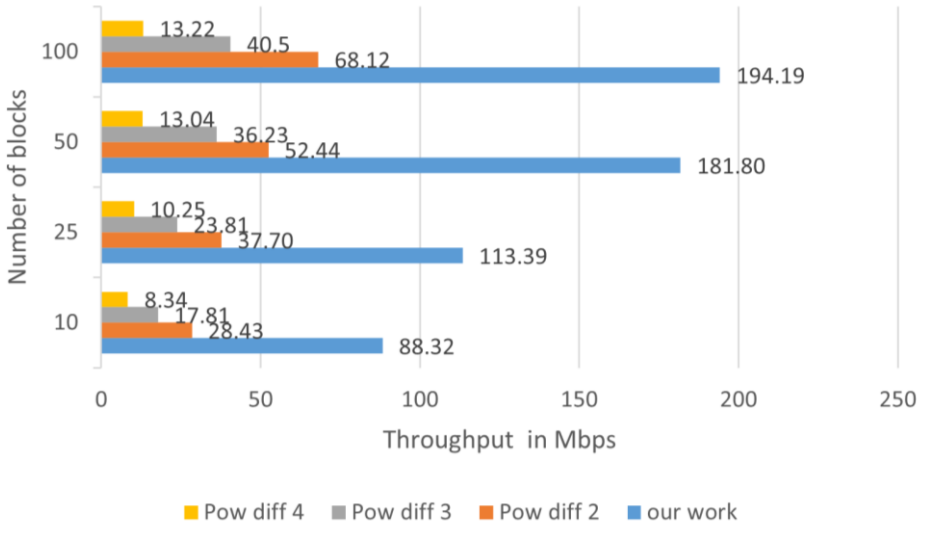


Figure 7. *Throughput in relation to number of blocks.*

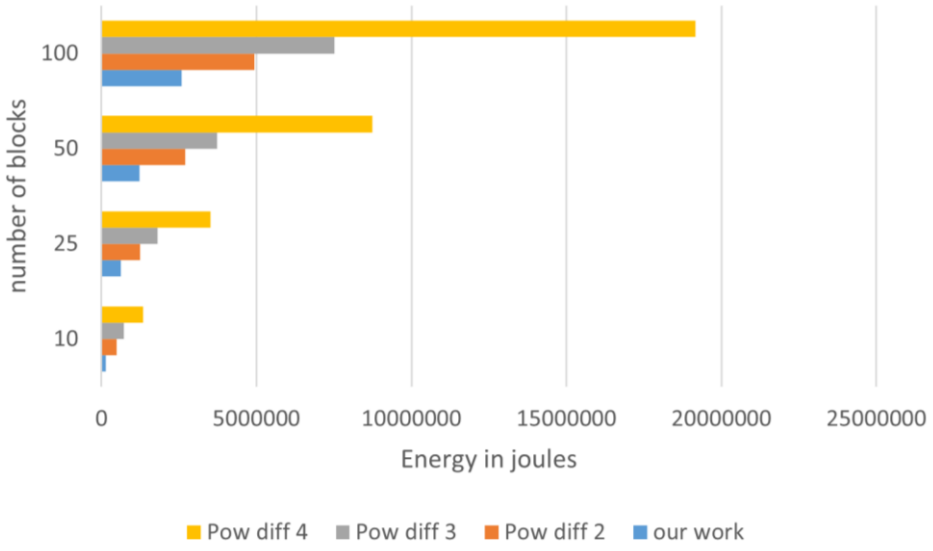


Figure 8. *Energy in relation to number of blocks.*

6.3.3 Discussion of time graph

Figure 9 illustrates the time required for block creation, comparing our contribution to the PoW approach. The x-axis represents time in seconds, while the y-axis represents the number of blocks. Upon analysing the results, it becomes apparent that our contribution exhibits superior speed in block creation compared to PoW. This characteristic holds significant importance when considering the security aspect of blockchain systems. The faster our contribution can generate blocks, the less vulnerable the system becomes to potential security breaches. Conversely, PoW necessitates substantially more time for block creation, providing hackers with an extended window of opportunity for malicious activities. The increased duration required by PoW not only hampers overall system efficiency but also diminishes the security of the blockchain. The more time it takes to create blocks, the higher the likelihood of unauthorized access and potential hacking attempts. In light of these findings, the accelerated block creation process offered by our contribution enhances the security of the blockchain system. By minimizing the time needed for block creation, we decrease the chances of potential security breaches, boosting the overall integrity and robustness of the blockchain network.

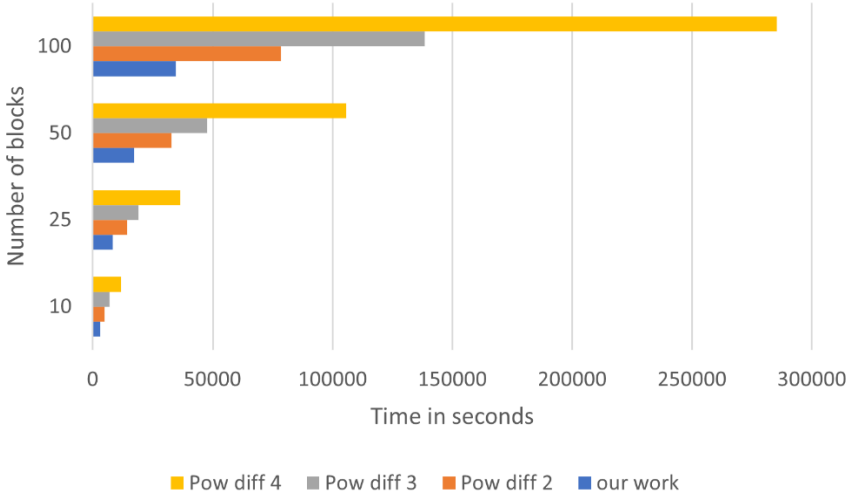


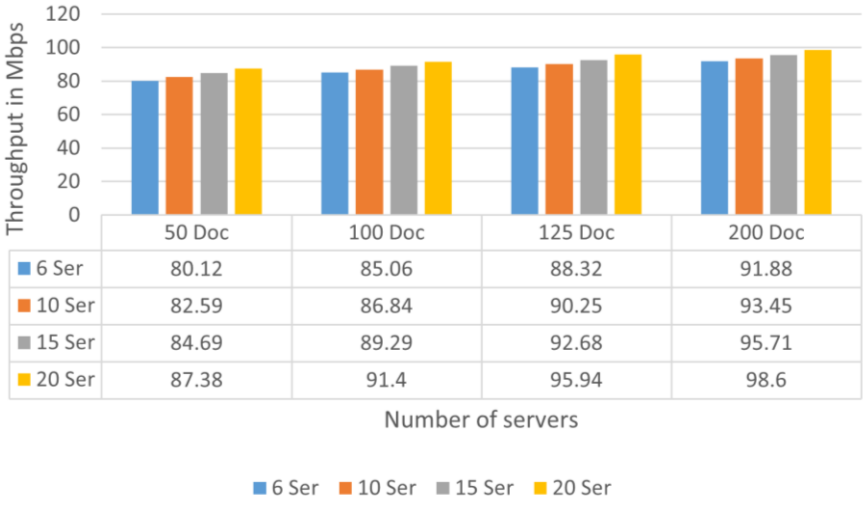
Figure 9. *Time needed for creation of blocks.*

The faster block creation in our approach reduces the vulnerability window for attacks, enhancing both the security and responsiveness of the system for real-time decision making.

6.3.4 Discussion of network usage graphs

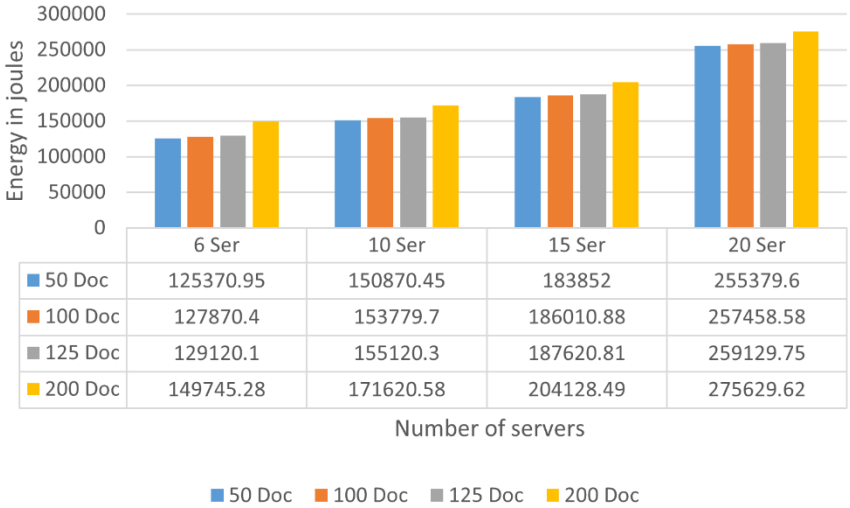
In this section, we discuss the internal comparison within our system. We aim to explore the impact of varying the number of servers and doctors, and we analyse the results based on three criteria: throughput (Figure 10), energy consumption (Figure 11) and processing time (Figure 12). Figure 10 depicts the relationship between throughput (measured in Mbps: megabits per second) and the number of servers and doctors. The results indicate that increasing the number of servers or doctors leads to a gradual improvement in throughput. This suggests that our system can handle a significant volume of data transmission without encountering any major issues.

In Figure 11, the x-axis represents energy consumption (measured in joules), while the y-axis represents the number of servers and doctors. The findings reveal that increasing the number of doctors has a negligible impact on energy consumption. However, augmenting the number of servers results in higher energy costs since the main operations of our contribution take place in that component.



	50 Doc	100 Doc	125 Doc	200 Doc
6 Ser	80.12	85.06	88.32	91.88
10 Ser	82.59	86.84	90.25	93.45
15 Ser	84.69	89.29	92.68	95.71
20 Ser	87.38	91.4	95.94	98.6

Figure 10. *Throughput in relation to number of servers and doctors.*



	6 Ser	10 Ser	15 Ser	20 Ser
50 Doc	125370.95	150870.45	183852	255379.6
100 Doc	127870.4	153779.7	186010.88	257458.58
125 Doc	129120.1	155120.3	187620.81	259129.75
200 Doc	149745.28	171620.58	204128.49	275629.62

Figure 11. *Energy in relation to number of servers and doctors.*

Figure 12 showcases the relationship between processing time (measured in seconds) and the number of servers and doctors. The results demonstrate that as we increase the number of doctors or servers, the processing time also increases. This phenomenon is primarily due to the growing number of messages for voting. Nevertheless, these time differences are insignificant in light of the increase in the number of servers and doctors.

This analysis shows that our approach maintains effective performance and scalability, adapting well to increased server and doctor counts with manageable impact on throughput, energy and processing time.

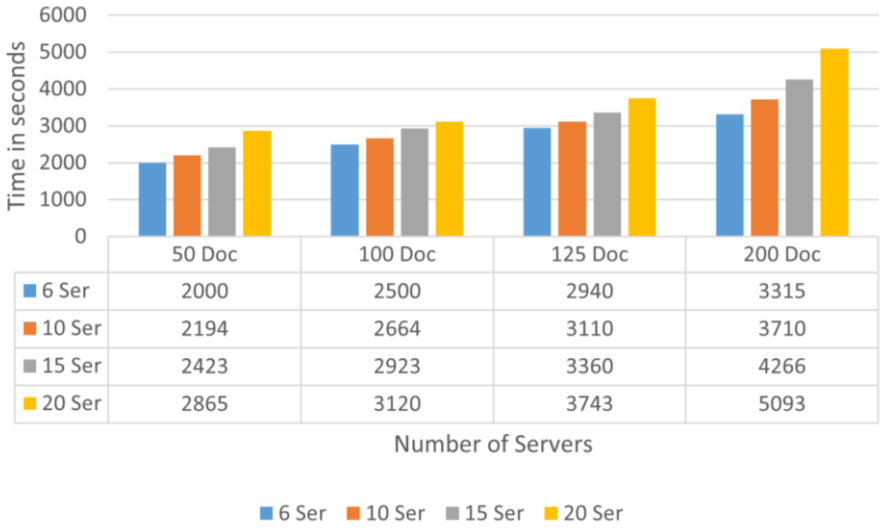


Figure 12. *Time needed for creation of blocks in relation to number of servers and doctors.*

7 OUR APPROACH COMPARED TO EXISTING WORKS

In the realm of IoT security, especially within healthcare applications, various approaches have been proposed to address challenges such as data integrity, scalability and trust. Comparing these methods provides valuable insights into their strengths and limitations, helping identify the most effective solutions for secure and efficient IoT environments. This section presents a comparative analysis of the leading solutions, focusing on aspects such as consensus mechanisms, encryption methods and system performance. A detailed comparison of these approaches is provided in Table 4. This table highlights the key features, advantages and limitations of each solution, facilitating a clearer understanding of how each approach addresses critical requirements in healthcare IoT security.

Table 4. *Our approach versus existing works.*

Work	Strengths	Weaknesses	Existing work versus our approach (our work)
Qu et al. (2021)	Addresses healthcare IoT security; explores blockchain integration.	Energy inefficiency, low scalability, high latency, reduced throughput and security issues with PoW; fault tolerance and consistency issues in traditional consensus mechanisms; latency concerns during emergency response.	Introduces raft consensus to improve scalability, latency and security; fog topology for real-time data analysis; optimized energy consumption.
Chaudhary and Chatterjee (2020)	Utilizes lightweight block ciphers for healthcare IoT.	Limited scalability as device numbers grow; centralized trust creates a single point of failure; insufficient privacy mechanisms for sensitive patient data; lack of collaborative validation of treatment protocols.	Implements decentralized trust with blockchain; enhanced data integrity using Schnorr signatures; scalable fog-cloud architecture for IoT healthcare systems.
Liu et al. (2020)	Investigates protocols and algorithms for healthcare IoT.	Lacks specific protocols for authentication, session keys and data storage or access control; security vulnerabilities in irregular block creation; inefficient leader election processes.	Proposes a comprehensive blockchain-based solution with robust protocols for data access control, secure session management, periodic block creation and efficient leader election.
Gupta et al. (2023)	Authorized access to patient information, i.e., only for medical professionals and relatives.	Single server dependency and computational overheads limit scalability and fault resilience in medical access control.	Enhances validation procedures by incorporating feedback from multiple servers, allowing collaborative improvements to treatment protocols.
Ali et al. (2023)	Enhances data safety, privacy, transparency and trust.	High computational resources, scalability and interoperability, resource-intensive requirements for users.	Addresses high computational demands by optimizing energy consumption and enhancing scalability through the efficient use of the raft consensus algorithm.

Work	Strengths	Weaknesses	Existing work versus our approach (our work)
Nanda et al. (2023)	Ensures security, privacy, trust visibility, decentralized tracking and mitigates medical component damage.	While the approach improves response time and reduces latency for a specific user group, it faces scalability challenges.	Makes use of the raft consensus algorithm to enhance scalability, ensuring efficient performance even in extensive and distributed systems.
Rizzardi et al. (2024)	Enhances data security, reduces fraud, improves trust among participants, ensures integrity and traceability of medical records.	Faces scalability challenges as system performance degrades with increasing numbers of assets and relies on reactive block creation.	A regular 7-minute block creation schedule strengthens blockchain resilience and secures patient records, while raft consensus enhances scalability.
Alshudukhi et al. (2023)	Microservices enhance interoperability and security in distributed IoT environments within federated cloud systems.	Introducing microservices for cloud interoperability faces challenges with latency and complex transactions in healthcare environments.	Uses fog nodes for distributed processing closer to the data source, enabling real-time analysis and reducing latency, crucial for emergency responses.
Proposed approach	Introduces raft consensus, Schnorr signatures and blockchain-based mechanisms to provide high scalability, decentralized trust, data integrity and tamper resistance for secure and efficient healthcare IoT systems.	N/A	N/A

8 LIMITATIONS OF OUR SOLUTION

While our proposed approach demonstrates significant advancements in integrating blockchain technology with IoT systems in healthcare, it also presents certain limitations. One notable limitation is the requirement for extensive resources and time for large-scale simulations to fully validate the effectiveness of the system, which may hinder practical implementation. Additionally, while our use of the Schnorr signature and RaftNode consensus protocol enhances security and reduces resource demands, these techniques may not fully address all potential vulnerabilities or performance issues as the number of devices and data scale increases. Furthermore, the adaptation of our work to other domains within the IoT ecosystem requires careful consideration of the specific challenges and requirements of those contexts, which may not have been thoroughly explored in this study. Overall, future research should focus on addressing these limitations to enhance the robustness and applicability of our approach across various IoT environments.

9 CONCLUSION

This paper explored the integration of blockchain technology with IoT systems, specifically in the context of healthcare data management. By examining fundamental concepts, opportunities and challenges, we identified the potential benefits of blockchain in IoT, such as enhanced data integrity, security and trust. Our proposed architecture and algorithms yielded promising results in addressing existing limitations and providing tailored solutions for IoT environments. Through extensive simulations and evaluations using NS3, we validated the effectiveness of our approach, as demonstrated by performance metric comparisons. This research contributes significantly to advancing secure and reliable decentralized data management systems for IoT and healthcare.

At a practical level, our approach can improve healthcare data management by securing patient data against tampering and unauthorized access. By employing efficient techniques such as the Schnorr signature and RaftNode consensus, we designed a system that conserves resources and enhances system stability, making it feasible for real-world healthcare IoT applications. This work provides a foundation that can be adapted for broader IoT applications, offering healthcare providers a more secure and resilient system for managing sensitive patient information and supporting essential healthcare operations.

While promising, our approach has limitations. The proposed system, while optimized for security and low resource consumption, has yet to be tested in real-world healthcare environments, and extensive simulation only provides a

partial understanding of how the system might perform at scale. Additionally, the inherent scalability challenges of blockchain may still affect performance in large-scale deployments, and further work is needed to address potential bottlenecks in real-time data processing.

Future work could focus on conducting large-scale simulations and real-world testing to evaluate the system performance in diverse healthcare settings, with varying device numbers and data types. Expanding the framework to accommodate additional consensus mechanisms or hybrid blockchain approaches may also enhance scalability and performance. Moreover, we envisage using formal security tools such as AVISPA and blockchain platforms such as Ethereum.

ADDITIONAL INFORMATION AND DECLARATIONS

Conflict of Interests: The authors declare no conflict of interest.

Author Contributions: A. L.: Conceptualization, Software, Writing – Original draft preparation. S. C.: Conceptualization, Project administration, Writing – Reviewing and Editing, Validation. Y. M.: Conceptualization, Software, Writing – Original draft preparation. C. B.: Software, Writing – Reviewing and Editing. K. H.: Writing – Reviewing and Editing.

Statement on the Use of Artificial Intelligence Tools: The authors declare that they didn't use artificial intelligence tools for text or other media generation in this article.

Data Availability: The data that support the findings of this study are available from the corresponding author.

REFERENCES

Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S. A., & Karim, F. K. (2022). Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions. *Electronics*, 11(4), 630. https://doi.org/10.3390/electronics11040630

Adeniyi, E. A., Ogundokun, R. O., & Awotunde, J. B. (2021). IoMT-based wearable body sensors network healthcare monitoring system. In *IoT in Healthcare and Ambient Assisted Living*, (pp. 103–121). Springer. https://doi.org/10.1007/978-981-15-9897-5_6

Adjeroud, I., Cherbal, S., Benrebbouh, C., & Baaraoui, H. (2024). Authentication scheme based on blockchain and Proof-of-Work for IoT. In *2024 6th International Conference on Pattern Analysis and Intelligent Systems*, (pp. 1-8). IEEE. https://doi.org/10.1109/PAIS62114.2024.10541147

Ali, S., Abdullah, N., Armand, T. P. T., Athar, A., Hussain, A., Ali, M., Yaseen, M., Joo, M., & Kim, H. (2023). Metaverse in Healthcare Integrated with Explainable AI and Blockchain: Enabling Immersiveness, Ensuring Trust, and Providing Patient Data Security. *Sensors*, 23(2), 565. https://doi.org/10.3390/s23020565

Allam, A. H., Gomaa, I., Zayed, H. H., & Taha, M. (2024). IoT-based eHealth using blockchain technology: a survey. *Cluster Computing*, 27(6), 7083–7110. https://doi.org/10.1007/s10586-024-04357-y

Alshudukhi, K. S., Khemakhem, M. A., Eassa, F. E., & Jambi, K. M. (2023). An interoperable blockchain security frameworks based on microservices and smart contract in IoT environment. *Electronics*, 12(3), 776. https://doi.org/10.3390/electronics12030776

Andrew, J., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications*, 215, 103633. https://doi.org/10.1016/j.jnca.2023.103633

Ashraf, E., Areed, N. F. F., Salem, H., Abdelhay, E. H., & Farouk, A. (2022). FIDCHAIN: Federated Intrusion Detection System for Blockchain-Enabled IoT Healthcare Applications. *Healthcare*, 10(6), 1110. https://doi.org/10.3390/healthcare10061110

Chaudhary, R. R. K., & Chatterjee, K. (2020). An efficient lightweight cryptographic technique for IoT based E-healthcare system. In *2020 7th International conference on signal processing and integrated networks*, (pp. 991–995). IEEE. https://doi.org/10.1109/SPIN48934.2020.9071421

Cherbal, S., & Benchetioui, R. (2023). Scpuak: Smart card-based secure protocol for remote user authentication and key agreement. *Computers and Electrical Engineering*, 109, 108759. https://doi.org/10.1016/j.compeleceng.2023.108759

Chinbat, T., Madanian, S., Airehrour, D., & Hassandoust, F. (2024). Machine learning cryptography methods for IoT in healthcare. *BMC Medical Informatics and Decision Making*, 24(1), 153. https://doi.org/10.1186/s12911-024-02548-6

Gupta, D. S., Mazumdar, N., Nag, A., & Singh, J. P. (2023). Secure data authentication and access control protocol for industrial healthcare system. *Journal of Ambient Intelligence and Humanized Computing*, 14(5), 4853–4864. https://doi.org/10.1007/s12652-022-04370-2

Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and privacy in IoT smart healthcare. *IEEE Internet Computing*, 25(4), 37–48. https://doi.org/10.1109/MIC.2021.3051675

Liu, H., Crespo, R. G., & Martínez, O. S. (2020). Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts. *Healthcare*, 8(3), 243. https://doi.org/10.3390/healthcare8030243

Mohammadi, R. (2023). A comprehensive Blockchain-oriented secure framework for SDN/Fog-based IoUT. *International Journal of Information Security*, 22(5), 1163–1175. https://doi.org/10.1007/s10207-023-00683-1

Nanda, S. K., Panda, S. K., & Dash, M. (2023). Medical supply chain integrated with blockchain and IoT to track the logistics of medical products. *Multimedia Tools and Applications*, 82(21), 32917–32939. https://doi.org/10.1007/s11042-023-14846-8

Qu, Q., Xu, R., Chen, Y., Blasch, E., & Aved, A. (2021). Enable fair Proof-of-Work (POW) consensus for blockchains in IoT by Miner Twins (MINT). *Future Internet*, 13(11), 291. https://doi.org/10.3390/fi13110291

Raghuvanshi, A., Singh, U. K., & Joshi, C. (2022). A review of various security and privacy innovations for IoT applications in healthcare. In *Advanced Healthcare Systems: Empowering Physicians with IoT-Enabled Technologies*, (pp. 43–58). Wiley. https://doi.org/10.1002/9781119769293.ch4

Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of blockchain and Internet of Things in healthcare and medical sector: applications, challenges, and future perspectives. *Journal of Food Quality*, 2021, 7608296. https://doi.org/10.1155/2021/7608296

Rizzardi, A., Sicari, S., M, J. F. C., & Coen-Porisini, A. (2024). IoT-driven blockchain to manage the healthcare supply chain and protect medical records. *Future Generation Computer Systems*, 161, 415–431. https://doi.org/10.1016/j.future.2024.07.039

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. *Sensors*, 22(19), 7433. https://doi.org/10.3390/s22197433

Saleem, T., Janjua, M. U., Hassan, M., Ahmad, T., Tariq, F., Hafeez, K., Salal, M. A., & Bilal, M. D. (2022). ProofChain: An X.509-compatible blockchain-based PKI framework with decentralized trust. *Computer Networks*, 213, 109069. https://doi.org/10.1016/j.comnet.2022.109069

Shari, N. F. M., & Malip, A. (2024). Enhancing privacy and security in smart healthcare: A blockchain-powered decentralized data dissemination scheme. *Internet of Things*, 27, 101256. https://doi.org/10.1016/j.iot.2024.101256

Stock, F., Kurt Peker, Y., Perez, A. J., & Hearst, J. (2022). Physical visitor access control and authentication using blockchain, smart contracts and internet of things. *Cryptography*, 6(4), 65. https://doi.org/10.3390/cryptography6040065

Taloba, A. I., Elhadad, A., Rayan, A., El-Aziz, R. M. A., Salem, M., Alzahrani, A. A., Alharithi, F. S., & Park, C. (2023). A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. *Alexandria Engineering Journal*, 65, 263–274. https://doi.org/10.1016/j.aej.2022.09.031

Tiwari, A., Dhiman, V., Iesa, M. a. M., Alsarhan, H., Mehbodniya, A., & Shabaz, M. (2021). Patient Behavioral Analysis with Smart Healthcare and IoT. *Behavioural Neurology*, 2021, 4028761. https://doi.org/10.1155/2021/4028761

Tomar, A., Gupta, N., Rani, D., & Tripathi, S. (2023). Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system. *Internet of Things*, 23, 100849. https://doi.org/10.1016/j.iot.2023.100849

Zaman, S., Khandaker, M. R. A., Khan, R. T., Tariq, F., & Wong, K. (2022). Thinking out of the blocks: Holochain for distributed security in IoT healthcare. *IEEE Access*, 10, 37064–37081. https://doi.org/10.1109/access.2022.3163580

Zerraza, I., Seghir, Z. A., & Hemam, M. (2024). An Efficient Lightweight Authentication and Access Control for IoT Edge Devices. *International Journal of Safety and Security Engineering*, 14(3), 807–813. https://doi.org/10.18280/ijsse.140313

Zhang, L., Li, B., Fang, H., Zhang, G., & Liu, C. (2023). An internet of things access control scheme based on permissioned blockchain and edge computing. *Applied Sciences*, 13(7), 4167. https://doi.org/10.3390/app13074167

Acta Informatica Pragensia is published by the Prague University of Economics and Business, Czech Republic | eISSN: 1805-4951