Journal of
Sensor and Actuator Networks

MDPI

Article

A Secure Blockchain-Enabled Remote Healthcare Monitoring System for Home Isolation

Jongsuk Kongsen [1], Doungsuda Chantaradsuwan [1], Peeravit Koad [1], May Thu [2] and Chanankorn Jandaeng [3,*]

[1] Department of Information Technology, School of Informatics, Walailak University, Thasala, Nakhon Si Thammarat 80160, Thailand; ojongsuk@mail.wu.ac.th (J.K.); doungsuda.ch@mail.wu.ac.th (D.C.); harrykoad@gmail.com (P.K.)
[2] Faculty of Engineering, Cambodia University of Technology and Science, CamTech Street, Sangkat Prek Tasek, Khan Chroy Chongvar Phnom Penh, Phnom Penh 121003, Cambodia; may.thu@camtech.edu.kh
[3] Informatics Innovative Center of Excellence (IICE), School of Informatics, Walailak University, Thasala, Nakhon Si Thammarat 80160, Thailand
* Correspondence: cjundang@gmail.com

Abstract: This article presents a secure framework for remote healthcare monitoring in the context of home isolation, thereby addressing the concerns related to untrustworthy client connections to a hospital information system (HIS) within a secure network. Our proposed solution leverages a public blockchain network as a secure distributed database to buffer and transmit patient vital signs. The framework integrates an algorithm for the secure gathering and transmission of vital signs to the Ethereum network. Additionally, we introduce a publish/subscribe paradigm, thus enhancing security using the TLS channel to connect to the blockchain network. An analysis of the maintenance cost of the distributed database underscores the cost-effectiveness of our approach. In conclusion, our framework provides a highly secure and economical solution for remote healthcare monitoring in home isolation scenarios.

Keywords: blockchain technology; Internet of Medical Things; smart contract

Citation: Kongsen, J.; Chantaradsuwan, D.; Koad, P.; Thu, M.; Jandaeng, C. A Secure Blockchain-Enabled Remote Healthcare Monitoring System for Home Isolation. *J. Sens. Actuator Netw.* **2024**, *13*, 13. https://doi.org/10.3390/jsan13010013

Academic Editor: Lei Shu

Received: 26 December 2023
Revised: 26 January 2024
Accepted: 30 January 2024
Published: 5 February 2024

1. Introduction

Home isolation, which is a strategy to contain COVID-19, involves individuals who have been diagnosed as being positive staying at home to reduce infection risk [1]. It is driven by technology and has revolutionized patient care by enabling the real-time tracking of health parameters through sensors and microcontrollers. This continuous data collection aids in the early detection of health conditions with accessibility to healthcare professionals and patients through networks or cloud storage [2–5]. Home isolation, which relies on Internet of Medical Things (IoMT) technology [6], utilizes IoT devices and wearables to collect real-time physiological data. These types of applications are called remote healthcare monitoring systems (RHMSs). RHMSs enable the continuous monitoring of vital signs, activity levels, and other health metrics, as well as facilitate timely intervention by healthcare professionals [7–10].

For the healthcare monitoring system in home isolation scenarios, securing sensitive medical data exchange is critical, yet traditional security measures may impact data transmission speed [2]. The implementation of e-health systems introduces challenges in security and privacy [11], and these are addressed through innovative solutions like advanced encryption [12], streamlined access control, and the blockchain. While these measures enhance overall security and efficiency, smart healthcare monitoring systems still face challenges, such as unauthorized access and data breaches (particularly in IoT technology and due to poor connectivity in rural areas [13–15]). IoMT significantly improves home isolation by ensuring secure communication, remote healthcare, and enhanced healthcare services [6]. Essential practices such as regular security audits and vulnerability

assessments are crucial to address system weaknesses [15,16]. Additionally, preserving patient privacy within IoMT systems is achieved through vital privacy protection measures like anonymization and de-identification techniques [17,18].

Integrating home isolation with the healthcare information system (HIS) is crucial for continuous healthcare delivery, but a direct connection may pose security vulnerabilities, thereby necessitating approaches that achieve objectives while ensuring information security. To address the main issues outlined in the context of our proposed blockchain-based framework for remote healthcare monitoring systems (RHMSs), two primary concerns are given prominence.

Firstly, the proposed framework addresses the critical issue of unqualified device interfaces accessing the hospital information system (HIS) by implementing robust access controls and role-based access. Blockchain technology ensures transparency, thereby enhancing overall confidentiality and integrity in remote healthcare monitoring systems (RHMSs).

Secondly, in addressing the vital concern of system availability, the proposed framework utilizes a distributed database architecture. Leveraging the blockchain's decentralized storage enhances data availability and reliability by dispersing information across a network, thus making remote healthcare monitoring systems (RHMSs) resilient to failures and ensuring continuous availability, even during localized disruptions.

This research aims to address security concerns in remote healthcare monitoring in home isolation conditions, particularly those that involve unauthorized access to a hospital information system from external locations. The proposed solution involves creating a secure remote healthcare monitoring system by implementing an external database detached from the hospital system's network. Distributed databases enhance availability, and blockchain technology has been suggested as an optimal solution as it meets the criteria for distributed databases and cybersecurity.

2. Literature Reviews and Related Works

2.1. Remote Healthcare Monitoring Systems (RHMSs)

Hospitals rely on hospital information systems (HISs) for efficient patient data management. A proposed layered system architecture was designed aiming at reducing complexity and enhancing stability [19], while external device integration through a secured network has also been suggested [20]. A HIS is implemented in a secure network with physical server protection and logical segmentation, such as in medical device networks, outpatient departments (OPDs), and in-patient departments (IPDs) (including VLANs). Strict authentication measures safeguard remote HIS access, and network segregation reinforces security. This architecture ensures efficient management, confidentiality, and integrity, as depicted visually in Figure 1.

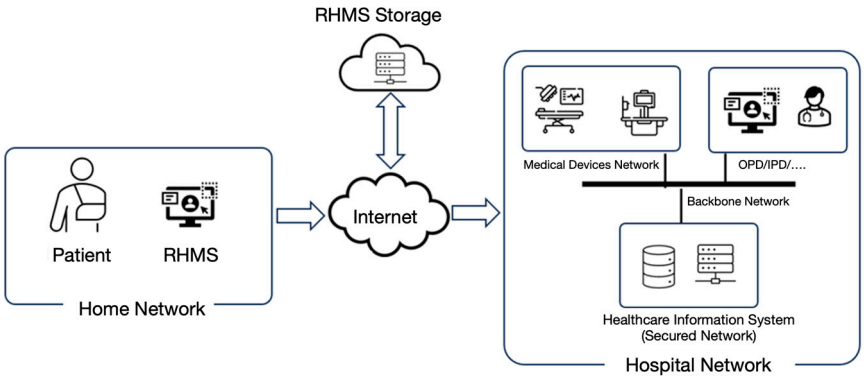

Figure 1. The traditional healthcare information system architecture.

Remote healthcare monitoring systems (RHMSs) assume a critical role in the collection and pre-processing of patient vital sign data, which are subsequently transmitted to a hospital information system (HIS). RHMSs demonstrate versatility by functioning both

within and outside hospital environments, and its categorization as a medical device is rooted in security considerations. It is noteworthy that all sensory data undergo rigorous verification and are securely stored within the confines of a medical network. HISs operate by retrieving these data as necessary, such as in the acquisition of other critical medical test results, thereby ensuring a streamlined approach to data management. Furthermore, implementing vital sensors facilitates remote patient monitoring, with the resulting data being securely housed within RHMS devices, which serve as compact medical gateways. Stringent security protocols, including data encryption and the utilization of secure transmission channels, guarantee the secure transfer of data to either cloud-based storage or direct integration with HISs, thus maintaining security standards that are commensurate with those applied to conventional medical devices.

2.2. Security Issues of RHMSs

Security in healthcare involves preserving confidentiality, integrity, and availability (CIA), as well as managing authentication, authorization, and accounting (3As). Security aspects are divided into central and supplementary systems. The central system encompasses the registry's central database, decentralized identity (DID) system, and collaboratively developed systems. Supplementary system security includes medical tools, data importation, and telemedicine platforms. Designing a robust healthcare security system necessitates comprehensive management of both central and supplementary components, whereby the diverse perspectives involved in safeguarding assets and ensuring the integrity and confidentiality of healthcare records are recognized.

Remote healthcare monitoring systems (RHMSs) encounter significant privacy vulnerabilities that stem from a lack of transparency in access control mechanisms, thereby necessitating the implementation of robust measures such as role-based access. To enhance the security in third-party Internet of Medical Things (IoMT) applications, suggested measures have included lightweight, password-based authentication [21]; anonymous, two-way authentication [22]; blockchain-based, cross-domain authentication [22]; or enhanced blockchain-based authentication protocols [23].

The traceability challenges in controlling access to patient data highlight the deficiencies in traditional approaches, thus emphasizing the importance of comprehensive auditing and logging mechanisms, as well as robust traceability measures for monitoring data transfers. The security approaches that are guilty of traceability issues are black box traceable and robust data security mechanisms [24], fine-grained access control on encrypted EHRs [25], or the clinical concept standard openEHR [26].

2.3. Blockchain Technology

Blockchain technology [27] involves an autonomous and distributed digital ledger that enables secure, intermediary-free transactions within a network. Blockchain technology is applied in various fields, including engineering [28], logistics [29], supply chains [30], land rights management [31], the prevention of government corruption [32], insurance [33], digital patents [34], and healthcare [35]. It holds great potential for revolutionizing engineering systems, particularly in healthcare, by offering features like immutability, traceability, transparency, and decentralization [36]. In healthcare, the blockchain ensures data security, availability, and reliability through a decentralized architecture, whereby tamper-proof records of healthcare assets are maintained and authorized access to medical information is securely granted [37]. Its applications in healthcare encompass electronic health records, medical imaging, clinical trials, telemedicine, and drug supply chain management [38]. By leveraging the blockchain, healthcare systems can ensure the integrity, security, accuracy, and accessibility of patient medical data while facilitating data management and integration, thus marking a significant advancement in the field [35].

Blockchain technology has emerged as a comprehensive solution for enhancing remote healthcare monitoring systems (RHMSs), whereby it can aid in effectively addressing privacy, security, authentication, traceability, and data transfer monitoring concerns. It

provides transparency in access control mechanisms, enforces role-based access, and creates a secure environment for patient data. The blockchain's encryption and decentralized storage significantly enhances data security, while smart contracts efficiently manage encryption keys, thus reducing vulnerabilities [39,40]. Notably, robust user authentication and transparent vendor security contracts ensure reliable access to patient data, particularly those concerning third-party devices [41]. The blockchain's immutable ledger, as well as its automating, auditing, and logging procedures, tracks data transfers and aids in the detection of unauthorized access and breaches, thereby greatly enhancing the overall integrity and efficiency of the system.

Ethereum [42], as a decentralized computing platform, is distinguished by its unique and self-governing network. It has gained widespread recognition, primarily due to its revolutionary concept of smart contracts. These smart contracts act as digital agreements, which are encoded with specific rules, obligations, addresses, states, and functions. The innovation of smart contracts allows for traditional business agreements to be translated into code on the Ethereum platform, thereby enabling automatic executions and enforcements based on predefined conditions. This eliminates the need for intermediaries in transactions, thus offering transparency and security by recording the entire process on the Ethereum blockchain.

The most compelling concept within blockchain technology is the smart contract. Leveraging the self-enforcing and event-driven attributes of Ethereum enables certain online transactions to occur without reliance on a trusted third party [43]. This technology boasts a robust community and a dedicated platform for information exchange. In essence, a smart contract encapsulates rules and obligations through encryption, comprising essential components such as an address, states, and functions. Notably, a smart contract address serves as the unique identifier for a contract that is implemented on the Ethereum blockchain network. Ethereum executes smart contracts and facilitates the deployment of distributed applications. The front end can take the form of a web application, which is then complemented with a Solidity smart contract that serves as the back end.

2.4. Security Enhancement with Blockchain Technology

The blockchain enhances cybersecurity by enforcing strong rules, thereby ensuring confidentiality, privacy, and intellectual property protection among organizations [25]. It enhances cybersecurity by capturing and assuring data integrity, thus preserving internal structures, relationships, and constraints [44]. It also supports authentication, which enables users to verify the record authenticity in cybersecurity with the decentralized security in the blockchain [45]. Moreover, the blockchain authorizes using attribute-based access control rules in smart contracts, whereby it stores attributes as metadata, thus enhancing cybersecurity [46]. In addition, the blockchain enables non-repudiation through a privacy-preserving authentication scheme, thereby verifying vehicles while maintaining privacy in cybersecurity [47]. Traceability is enabled by appending transactions to the blockchain, thus ensuring transparency during vehicle authentication.

Hence, the integration of blockchain technology into the design and implementation of secure applications results in the deployment of a distributed database, and this inherently ensures the safeguarding of data in the realm of the 3As. The unique identification of applications and users is encapsulated in the wallet address, thereby authenticating all transactions. Meanwhile, the access control for the distributed database is governed by smart contracts and the utilization of calling APIs for authorization. The blockchain platform, serving as a foundation, facilitates the meticulous tracing of all transactions, and it addresses accounting concerns comprehensively.

2.5. Related Works

Blockchain technology has been applied in a great deal of research to secure healthcare monitoring systems, and instances of these are summarized in Tables 1 and 2. The research related to the use of blockchain in HISs can be categorized into two main formats: enhancing

security for medical record systems and implementing the blockchain to enhance security for medical devices. The fundamental requirements for a medical record system include data integrity and network security. In this context, blockchain technology is applied to improve security in both data and communication aspects, and it is aimed at reducing errors in system operations.

Table 1. The previous works of secured medical record systems with blockchain technology.

Ref.	Contributions	C	I	A
[6]	_ Use of the blockchain for the secure monitoring of elderly individuals at home. _ Emphasis on reducing medical errors and enhancing transparency. _ Goals include transparent consultations and secure data access.	-	-	-
[48]	_ Use of the blockchain and smart contracts for transparency and security. _ Focus on enhancing security in healthcare data storage.	-	-	-
[49]	_ Use of an E-PoW blockchain and deep learning for patient record management. _ Addressed challenges in health record management. _ Implementation of a decentralized network using the blockchain for healthcare. _ Aims to reduce medical errors and increase transparency.	-	-	-
[50]	_ Introduction of a blockchain-based model for healthcare data security. _ Utilized the SHA256 hash algorithm for data integrity.	-	✓	-
[51]	_ Used a blockchain solution for security in healthcare data sharing. _ Use of a context-aware model for data encryption in a 5G network.	-	✓	-
[52]	_ Proposal of a decentralized electronic health record (EHR) architecture. _ Use of the Hybrid Computing Paradigm System (H-CPS) for low storage and response time.	✓	-	-
[53]	_ Advocacy for the blockchain to safeguard and distribute electronic health records. _ Focus on the secure distribution of electronic health records.	✓	✓	-
[54]	_ The use of the healthchain as a privacy-preserving scheme for large-scale health data. _ Focus on fine-grained access control and health data encryption.	✓	✓	-
[55]	_ Introduction of a blockchain-assisted secure data management framework (BSDMF). _ High accuracy, precision, trust value, low response time, and latency ratios.	-	-	✓

C = confidentiality; I = integrity; A = availability.

Table 1 elucidates the integration of blockchain technology to fortify information security within medical information systems. Prior research endeavors, as indicated by various proposals and studies, have spanned diverse applications encompassing the secure monitoring of elderly individuals [6] and the management of patient health records [49]. Additionally, a concerted effort has been directed toward augmenting data security in healthcare through the implementation of security measures [48,50,51,54]. The proposals further extend to secure management and distribution of health records [52,53,55]. These scholarly discussions underscore the utilization of the blockchain to amplify trustworthiness in medical information systems, thereby addressing nuances like data accuracy, confidentiality of treatment information, encryption, and the perpetuation of seamless service provisions. A pivotal concern also arises in assessing the dependability of externally linked devices, and this is exemplified by remote patient monitoring systems.

Integrating the blockchain into Internet of Medical Things (IoMT) systems strengthens system security through embedded security measures, authentication, and automated upgrades, while decentralization serves to reduce the risk of failures. The related works are summarized in Table 2.

Table 2. The previous works involving secured IoMT applications with blockchain technology.

Ref.	Contributions	C	I	A
[7]	_ Contribution of a private blockchain for secure medical data sharing in IoMT. _ Emphasis on scalability and robust healthcare services.	✓	✓	-
[56]	_ Proposal for a decentralized blockchain-based IoT for IoMT applications. _ Emphasis on privacy and security in IoMT applications.	✓	✓	-
[57]	_ The use of an encryption scheme and the blockchain for larger capacity and efficiency in smart healthcare. _ Addressing security and trustworthiness in smart healthcare.	✓	-	-
[58]	_ Introduction of a private blockchain framework for IoMT devices. _ Emphasis on high-security standards and compatibility.	✓	-	-
[59]	_ Blockchain-based architecture for the real-time monitoring of COVID-19 patients. _ Four-layer structure using IoT and blockchain techniques.	-	-	✓
[60]	_ Application of the blockchain in IoT applications for reliability and security. _ Development of a blockchain-based IoT platform.	-	-	✓
[61]	_ The use of a multi-modal secure data dissemination framework (MMSDDF) for secure patient data access. _ High accuracy and prediction ratios with low delay and latency.	-	-	✓

C = confidentiality; I = integrity; A = availability.

The blockchain has been pivotal for enhancing IoT and data security in the medical industry as it prioritizes confidentiality, privacy, and integrity. A private blockchain architecture that is tailored for the Internet of Medical Things (IoMT) ensures scalable and secure medical data sharing [7]. Decentralized blockchain-based IoT solutions are implemented to reinforce security and preserve privacy in medical data transactions [56].

While the data in transit over blockchain networks are encrypted, a potential risk of unauthorized disclosure exists due to plain-text storage on the blockchain. To address this, encrypting data before publishing them in blockchain transactions emphasizes increased confidentiality [57]. Additionally, a private blockchain framework for IoMT devices emphasizes high-security standards and compatibility [58].

Distributed databases, which are a strategy to avert failures, involve using the blockchain to store patient data from IoMT devices, thus enhancing overall system security [59]. A blockchain-based IoT platform was designed for improved reliability and security [60]. In contrast, a multi-modal secure data dissemination framework (MMSDDF) was designed to facilitate secure patient data access, which focuses on accuracy and prediction ratios while minimizing delay and latency [61].

2.6. Summary

This research aimed to enhance the stability of a home isolation system by transmitting patient data through the Internet of Medical Things (IoMT), as well as working to secure it in a distributed database outside the medical center's network. The system connects to a secure medical network and registry, and it ensures that access is only granted to authorized personnel. Considering secured data transmission, this research explored using the blockchain to buffer patient records, and it was aimed at reducing database maintenance costs and bolstering security. The investigation focused on factors like scalability, integration, encryption protocols, and access control within the IoMT framework to optimize efficiency. Ultimately, the goal was to create a robust and secure data transmission and storage system for home isolation.

3. Proposed Models

In this study, our primary emphasis was on designing and implementing remote healthcare monitoring systems. The research commenced with an analysis of the traditional healthcare information system architecture, and we then delved into the security issues associated with remote healthcare monitoring systems (RHMSs). Our contribution includes the formulation of a security model tailored for RHMSs. Additionally, we put forth a system model and executed a security mechanism that leverages blockchain technology and other integral components to fortify the support structure for RHMSs.

3.1. Security Model

Let $V = \{v_1, v_2, v_3, \ldots, v_n\}$ represent the set of vital signs that measure the patient, including pulse, heartbeat, temperature, etc. The health number (HN) is assigned by the HIS, whereas t is the timestamp. Hence, the transaction of the sensing data is represented by Equation (1).

$$msg = \langle HN, t, V \rangle. \tag{1}$$

The primary objective was to ensure security by preventing unauthorized access and authentication, which is a key requirement in the context of RHMSs. Additionally, traceability is an essential aspect of the RHMS system. Therefore, this paper introduced a security model, represented by Equation (2), to address these critical concerns.

$$TX(msg) = \langle E_k\,(msg), S_k\,(msg) \rangle, \tag{2}$$

where the plain text, msg, refers to the plain data that comprises the HN, a timestamp, and a set of vital signs. The encryption algorithm, denoted as $E_k()$, was applied to secure this information, and a digital signature, $S_k()$, was added to authenticate the method.

Equation (2) represents the traditional model used to secure plain messages, which necessitates the use of cryptographic keys and their distribution. The proposed RHMS introduced a decentralized paradigm, thereby effectively eliminating the external connections to the HIS network. Consequently, the implementation of a distributed database using blockchain technology served as the solution for this work, with the security model being managed by smart contracts. Additionally, this approach resulted in the automatic implementation of traceability.

3.2. Proposed System Architecture

The system architecture, as depicted in Figure 2, signifies the transformation of healthcare through the integration of healthcare monitoring devices, blockchain technology, and decentralized data management. It capitalizes on IoT devices with vital sign sensors and secure blockchain data storage for improved data accuracy and security. This architecture leverages data brokers and health information systems to enhance data collection and management, ultimately optimizing the healthcare ecosystem.

Healthcare monitoring devices, which are a subset of the Internet of Medical Things, feature vital sign sensors that can connect via various interfaces and derive power from the MCU board; moreover, they are responsible for power management and data transmission. These MCUs are commonly linked to power sources like adapters and rely on reliable networks such as WiFi or 3G/4G. To ensure seamless operation, these devices support real-time or embedded operating systems like RaspbianOS, especially in Raspberry Pi applications. There are two functions in the healthcare monitoring devices: *sense_data()* and *send_data()*.

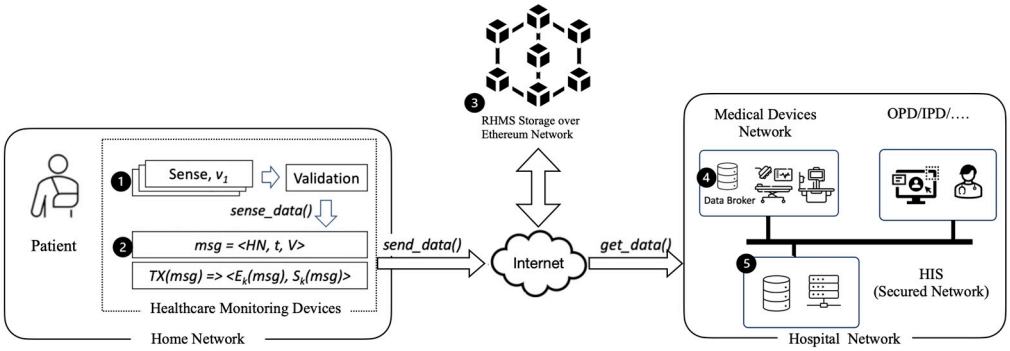

Figure 2. The proposed system architecture.

The sense_data() function

The *sense_data()* function is tasked with capturing vital signs data from the patient. Following this data acquisition, it assesses data reliability by evaluating the precision of each sensor value. This evaluation involves establishing a linear equation, computing the standard error of the data, and determining the vital sign value based on the data's average.

To precise the value of the vital sign, let $\overline{v_i} \in V$ be such that V is the set of vital signs. In addition, $\overline{v_i}$ is calculated from the set of sensing data under the following conditions: (1) the sensing data are in the linear equation, $v_i = \alpha_i x + \varepsilon_i$, with the coefficient α_i; and (2) the precise vital sign is $\frac{dv_i}{dx} = \alpha_i \approx 0$. The *sense_data()* function is shown in Algorithm 1.

Algorithm 1 *sense_data():* sense precise vital signs

round ← *trial*
while $\alpha_i \approx 0$ and *round* $\neq 0$ **do**
$t_0 \leftarrow 0$
$S \leftarrow \phi$
while $t - t_0 \leq \Delta t$ **do**
$i \leftarrow$ *sense()*
$S \leftarrow S \cup i$
$t \leftarrow$ *timestamp()*
end while
$\alpha_i \leftarrow$ *LinearRegression()*
round ← *round* − 1
end while
if *round* = 0 **then**
return *S. average()*
else
return error

Algorithm 1 illustrates the sensing and refining actions that are performed on the sensor data. The medical device collects data from the vital sensor for a duration of Δt. The sampling rate is determined by the sensor specifications provided in its datasheet. Subsequently, the algorithm computes a linear regression model and provides the coefficient α_i. The algorithm returns the average of the sensing data when α_i is close to zero or within an acceptable range. The complexity of the algorithm is proven in Theorem 1.

Theorem 1. *The sense_data() is the O(r·k) complexity.*

Proof of Theorem 1. The outer loop runs until either α_i is not approximately equal to 0 or the number of rounds (*round*) is not equal to 0. In each iteration of the outer loop, there is an inner loop that continues until the time difference $(t - t_0)$ exceeds a threshold Δt. In each inner loop iteration, the algorithm performs a constant number of operations as follows: sensing (i), updating a set (S), and obtaining a timestamp (t).

Let us denote the number of rounds as r and the maximum number of inner loop iterations as k. The time complexity of the inner loop is $O(k)$ since it depends on the threshold Δt. The outer loop runs until α_i is not approximately equal to 0, and the worst-case scenario is that it runs r times.

$$O(r \cdot k)$$

□

The send_data() function

The *send_data()* function is responsible for transmitting encrypted data to the blockchain platform. The input data for this function are based on Equation (1), and these include the health number (HN) and unique wallet address that is assigned by the HIS for simple authentication, along with a set of vital sign data, which is denoted as V, as well as the automatically collected timestamp t from healthcare monitoring devices. The process of the healthcare monitoring device is shown in Figure 3.

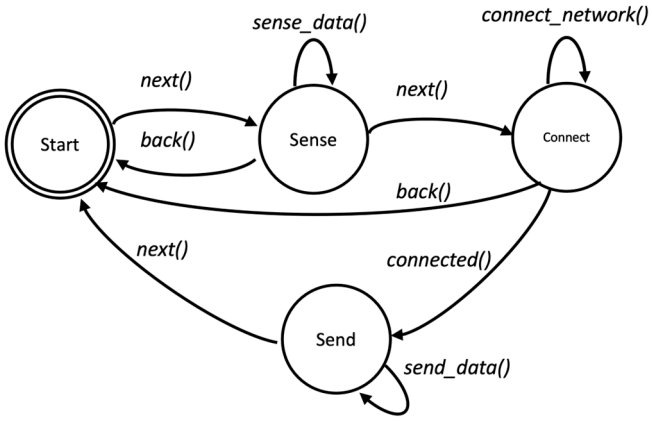

Figure 3. The process state machine of healthcare monitoring devices.

The process state machine illustrates the healthcare monitoring device's operation in Figure 3. This device is controlled using two buttons: "*next*" and "*back*". The "*next*" button confirms actions and progresses to the next state, while the "*back*" button is used to cancel. Additionally, the device requires an LCD or OLED screen to display its state and sensing values.

In the initial state, the user inputs their health number (HN) and blockchain wallet information, and then "*next*" is selected to transition to the sense state. In the sense state, the device invokes the "*sense_data()*" function to gather vital signs. This state repeats until all vital signs have been sensed. Afterward, it displays the sensing data and awaits a transition to the next state, which is triggered by the selection of "*next*".

The medical device attempts to establish a network connection in the connected state. This process halts when the device cannot connect to the network. When the network connection is successful, the medical device generates a transmission message based on Equation (2). This message is encrypted and signed with a signature using the blockchain library and its associated smart contract. Finally, the message is secured by the blockchain library and sent to the distributed database on the blockchain platform.

3.2.1. Blockchain Architecture Design

In the decentralized paradigm, the data reside in a distributed database and are encrypted, signed, and securely transferred through channels. Smart contracts within the blockchain platform oversee business processes and security policy management, and the platform provides secure APIs for data access, thus ensuring authorized data retrieval.

Smart contracts play a crucial role in safeguarding vital sign data. These contracts are built upon a data structure, which is outlined in Equation (1) and comprises essential

elements such as the healthcare number, timestamp, and a set of vital signs. For a detailed view of the data structure and the function prototype of the smart contract, refer to Figure 4.

```
pragma solidity ^0.8.18;
contract S3RHPatients{
    address public owner = msg.sender;

    struct Patients {
        address ID;
        uint HN;
    };
    mapping (address => Patients) patientList;

    struct VitalSign{
        address ID;
        string vital_sign;
        uint timestamp;
    }
    mapping (address =>VitalSign[]) vitalSign;

    function addPatients(address id, uint HN);
    function getPaitents(address id);
    function addVitalSign (address id, string vital_sign);
    function getVitalSign(address id);
}
```

Figure 4. The smart contract of S3RH.

Figure 4 encompasses two distinct data structures along with their associated functions. The "Patient" structure serves as a container for storing the healthcare number and wallet address, which serve as a unique identifier for the user. In contrast, the "Vitalsign" structure is specifically created to store both timestamp and vital sign information in a textual format. The vital sign data are stored in textual structures like CSV, JSON, XML, etc. To illustrate, consider the following three sensor data points (all of which include a corresponding timestamp): temperature, heart rate, and SPO3. The "Patients" and "VitalSign" structures are equipped with a set of get functions. These data structures are organized within a sequential list. Adding the data involves pushing new information into the list, while the "get" method allows for constant and efficient access to the stored data.

3.2.2. Web APIs with an MQTT Data Broker

Figure 5 illustrates the comprehensive network flow within the proposed system. The remote healthcare monitoring system (RHMS) initiates the transmission of vital signs to the blockchain network utilizing the *send_data()* function. The transmission of sensitive data occurs through a secure channel, which ensures its confidentiality during transit over the Internet.

Upon the retrieval of data from the blockchain network, the hospital's web API service issues a request API, which incorporates an authentication message (comprising the hospital number, HN, and wallet ID) as a concealed secret key. This transaction transpires over a secure network. Subsequently, the API service disseminates the response message to the "S3RH" topic on the MQTT broker. Notably, the message queuing telemetry transport (MQTT) protocol is employed as a lightweight protocol for the publish/subscribe mechanism. Moreover, the MQTT protocol incorporates support for a transport layer security (TLS) secure channel, which is used to augment the overall security of the system.

In the context of our proposed system, the MQTT broker assumes a pivotal role by facilitating secure and efficient machine-to-machine communication. It empowers web agents to retrieve patient records seamlessly from hospital information systems, thereby ensuring the timely and secure handling of data. The integration of patient medical data into a blockchain-based storage system further enhances security and decentralizes access,

thereby safeguarding patient information. Consequently, the MQTT broker emerged as a critical component within the healthcare architecture.

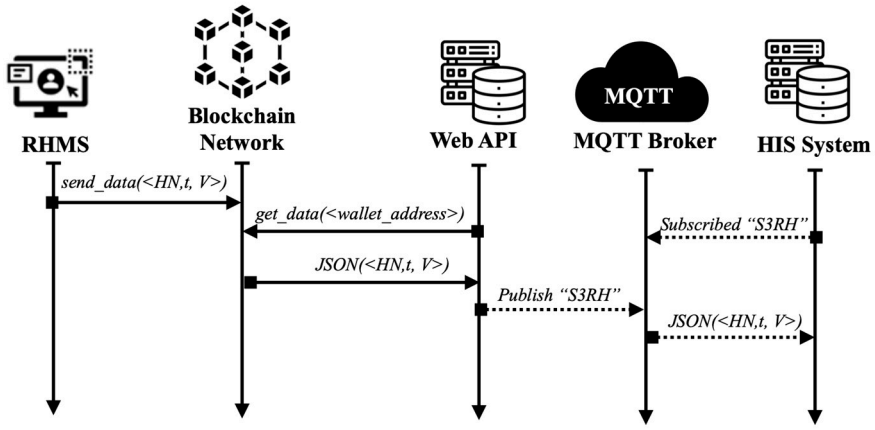

Figure 5. Network flows of the proposed architecture.

The operational flow of the MQTT protocol in our framework is depicted in Figure 5. Subsequently, the web API orchestrated the publication of acquired sensor data to the MQTT broker. Conversely, the hospital information system (HIS) functions as a client and assumes the role of a subscriber within the MQTT paradigm. It systematically collects data from the MQTT broker via its authorization parameters, thereby further enhancing the interoperability and efficiency of our proposed healthcare system.

3.2.3. HIS Software Agent

The healthcare number (HN) serves as the primary key for accessing patient records across the various hospitals that patients have visited. Our system is strictly read-only, and it does not make any updates to the hospital information system (HIS). Each HIS is equipped with a dedicated query module, which is developed to retrieve and format the patient information requested through the web agents or web API. This process is read-only and does not involve any alterations to the patient's data in the HIS. Web agents receive the HN through the MQTT protocol and use it to request patient information. The query module mentioned earlier retrieves and returns the data to the web agent. These web agents are software processes developed in any programming language. They can either be embedded within the hospital's system or can be run on a Raspberry Pi computer-on-a-board system, whereby it serves as a front end connected to the hospital's server machine via their local area network (LAN). The installation and maintenance of this hardware and software are managed by our development team. One of the tasks performed by each agent is to format and restructure the patient information extracted from the HIS into an electronic health record (EHR). Subsequently, the data are encrypted before being transmitted to the central server, which is then ready to be analyzed by the doctor in the next step.

4. Proposed S3RH Using Raspberry Pi

4.1. Hardware and Software Implementation

We illustrated our proposed system by applying it to the home isolation of COVID-19 patients. Our prototype system includes a microcontroller with a built-in ADC, a heart rate sensor, a contactless temperature sensor, and an oximeter. When COVID-19 initially enters the body through the nostrils and mouth, it progresses toward the respiratory system. Monitoring the temperature and oxygen levels of COVID-19 patients is crucial for identifying potential cases. COVID-19-infected individuals often experience a significant decrease in oxygen levels, thus necessitating the use of an oximeter to measure oxygen saturation. All these sensors are designed to be seamlessly interfaced with the system. The prototype is shown in Figure 6.

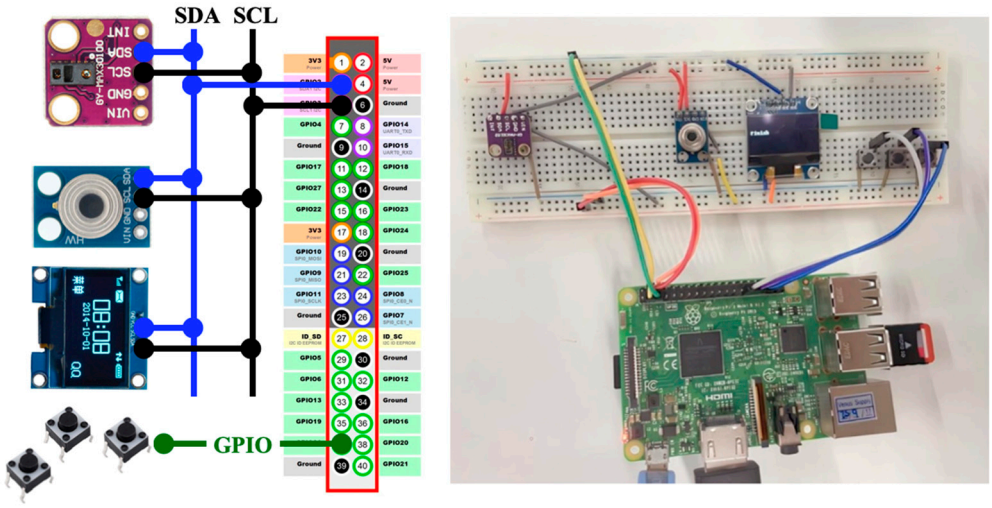

Figure 6. The prototype of the smart remote healthcare monitoring devices.

The prototype was designed to record data and communicate with a blockchain network for future processing. The Raspberry Pi platform has been described as a compact single-board computer that runs a customized Linux/Android distribution optimized for its ARM processor. It is versatile and interfaces with sensors and external devices, and it can be programmed using Python. Two sensor modules are mentioned in the text. The first is the GY-MAX30102, which combines a photoplethysmogram (PPG) sensor and an infrared LED to measure heart rate and blood oxygen levels (SpO2). This sensor is commonly used in healthcare and fitness devices like pulse oximeters and fitness trackers. It communicates with a microcontroller through I2C interfaces. The second sensor module is the GY-906 (or MAX90614), which incorporates the MAXIM MAX90614 infrared temperature sensor. It allows for non-contact temperature measurement through IR radiation and is suitable for applications like industrial temperature monitoring, non-contact thermometers, and HVAC systems. Like the GY-MAX30102, it also communicates with microcontrollers through I2C. The patient controls the devices via a button and follows the steps with the button.

4.2. Sensor Calibration

To investigate the differences between the sensors and the EarlyVue VS30 vital signs monitor (the vendor is Philips Medizin Systeme Böblingen GmbH, Germany), 30 sets of data were simulated, including temperature, blood oxygen levels, and heart rate. The data were then analyzed using an R script, which involved generating frequency distributions; calculating percentages, means, and standard deviations; and conducting tests to assess the differences between the sensor and the Philips-EarlyVue VS30 monitor. The relationships were evaluated using *t*-tests, which were conducted employing a two-tailed test approach since a non-directional alternative hypothesis was utilized. The results are shown in Table 3.

Table 3. Comparison of the sensing data from the sensor and commercial product.

Testcase	N	Mean	*t*	$p\ (T \leq t)$	Error
Temperature (MAX90614)	30	36.81	1.676	0.105	1.26%
EarlyVue VS30	30	36.35			
SPO2 (MAX30102)	30	95.40	−3.064	0.005	−2.88%
EarlyVue VS30	30	98.23			
Heart rate (MAX30102)	30	92.93	−2.244	0.033	−3.89%
EarlyVue VS30	30	96.70			

As shown in Table 3, we conducted a two-tailed *t*-test to compare the variables of MAX90614 and EarlyVue VS30, which resulted in a *p*-value of 0.105. This *p*-value indicated

the likelihood of observing the differences between MAX90614 and EarlyVue VS30 under the assumption that there is no significant distinction between them. With the commonly accepted significance level set at 0.05, a *p*-value of 0.105 suggested that there was not enough statistical evidence to support a significant difference between these variables.

On the other hand, when we used *t*-tests with a two-tailed approach to compare the MAX30102 and EarlyVue VS30, we obtained a *p*-value of 0.033. This *p*-value represents the probability of witnessing the observed differences between the MAX30102 and EarlyVue VS30, and this was achieved by assuming there was no significant distinction between them. However, with a *p*-value of 0.033, we still did not have strong statistical evidence to confirm a significant difference (as this value exceeded the commonly accepted significance level of 0.05).

It is important to note that the values obtained from the MAX30102 sensor for the SPO2 and heart rate variables were slightly less than the actual values of 2.88% and 3.89%, respectively. These variations were addressed by adjusting the values in the sensor node before they were sent to the smart contract. Certainly, it is important to emphasize that these sensors are exclusively intended for prototype testing and should not be relied upon for medical diagnostic purposes.

The experiment focused on validating a prototype's functionality for data accuracy before integrating it with a blockchain network. It emphasized its flexibility in modifying hardware components in a real system environment, as well as clarified that the equipment used was for assessing system stability, not production. The outcomes highlighted the prototype's reliability and underscored that the observed variations did not jeopardize the proposed framework's stability mechanism.

5. Experiment Setup

5.1. Testbed

The blockchain network manages the smart contracts and data through a transaction process, where the transaction fee depends on the size and complexity of the smart contract data. Additionally, the sender of the transaction is required to specify a charge, which the node confirms upon obtaining the fee. It is crucial to set reasonable fees to ensure the prompt handling of transactions.

In Ethereum, the primary way for users to interact with the platform is through financial transactions or smart contracts. The user specifies a value, a gas, and a gas price, which Ethereum executes via a virtual machine (EVM) until the task is completed or runs out of gas. Upon completion, the transaction enters the transaction pool, which historically experiences backlogs until a miner decides to mine it. Once mined, the transaction is added to the blockchain.

Ethereum's unique feature is an internal metering variable known as "gas," which measures the complexity of each blockchain transaction. The transaction's execution cost is calculated by an algorithm in gas units, where the more complex the transaction, the more gas the user needs to have and pay for the transaction to be processed and recorded.

5.2. Transaction Fee or Gas

In Ethereum, gas is the metric used to quantify the computational expenses of executing a smart contract, and it is the responsibility of the user to cover the associated costs. The gas mechanism rewards the miner in Ether for facilitating the transaction.

The calculation of the transaction fees in blockchain networks, particularly in Ethereum, involves the concept of gas and *gasPrice*. The total transaction fee is the product of the *gasUsed* and the *gasPrice*, where *gasUsed* represents the maximum number of gas units that a user is willing to spend on a transaction. It is a cap on the computational work the transaction can perform, and the *gasPrice* is the cost per unit of gas in terms of the cryptocurrency used on the blockchain (e.g., Ether). It represents the fee the user is willing to pay for each unit of computational work. Users typically set the gas price when initiating

a transaction, and the complexity of the transaction determines the gas used. One can convert the transaction fee from GWei to Ether by dividing by 10^9.

5.3. Scenarios

The primary goal of this experiment was to assess the performance of a smart contract within a controlled environment. The experiment examined the relationship between the length of order descriptions and transaction fees as the key performance metrics. This evaluation was conducted using black box testing methodology.

The experiment assumed that our hardware senses vital signs from patients and is validated with Algorithm 1. The hardware is already connected to the local network via WiFi. The Ethereum network ran on our laptop, as shown in Figure 7.

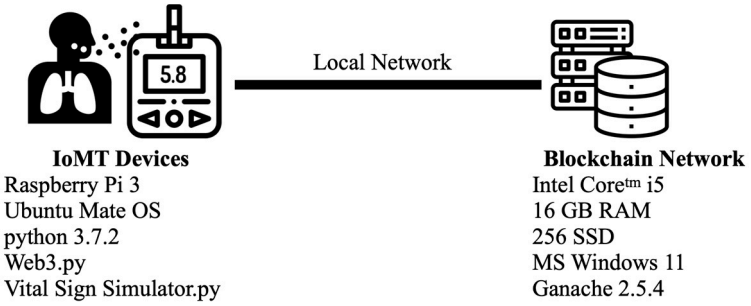

Figure 7. The systematic environment for the experiment.

The systematic environment consisted of two modules: IoMT devices and the blockchain network. Both modules used point-to-point communication. The smart contract was coded in Solidity and compiled using the Remix IDE. Additionally, we crafted the application in Python, and we established communication with the blockchain network through Web3.py. The experiment consisted of dispatching 100 transactions to the blockchain network, each containing random data lengths from the vital sign emulator [62], which was facilitated by a script. The wallet ID, HN, and vital sign data, which were generated in textual form with variations between 45 and 512 bytes, were formatted in JSON. These steps were performed to examine the correlation between the data length and *gasUsed*.

For testing purposes, we employed a laptop running MS Windows 11 with the following specifications: 11th Gen Intel® Core™ i5 processor operating at 2.70 GHz, 16 GB of RAM, and a 256 GB SSD. We selected the Ethereum network with a proof of work (POW) methodology as the consensus algorithm and used Ganache version 2.5.4. To eliminate the potential impact of network delays, this experiment did not connect to an external computer.

6. Experimental Results

The primary goal of this paper was to create a distributed application framework with a focus on ensuring confidentiality, integrity, and traceability. Additionally, this study assessed the performance of a blockchain-based application, specifically in terms of emphasizing transaction fees.

In this study, the dependent variable under scrutiny was the data length, while the independent variables were the transaction fee in terms of *gasUsed*. To maintain control over the experiment conditions, we conducted the tests within a closed system, thereby mitigating the influence of network-related delays. The experimental results are shown in Figure 8.

Figure 8 shows the direct impact of data length on the hashing and block processing functions within the blockchain. The experiment found that the initial gas consumption was 21,208. As the data length increased by 1 byte, the gas consumption experienced significant changes. In particular, the gas consumption increased by 12 units for each additional byte

of data and by 140 units for every 32 bytes of data. The function's gas consumption utilized *addVitalSign()* increases in steps.

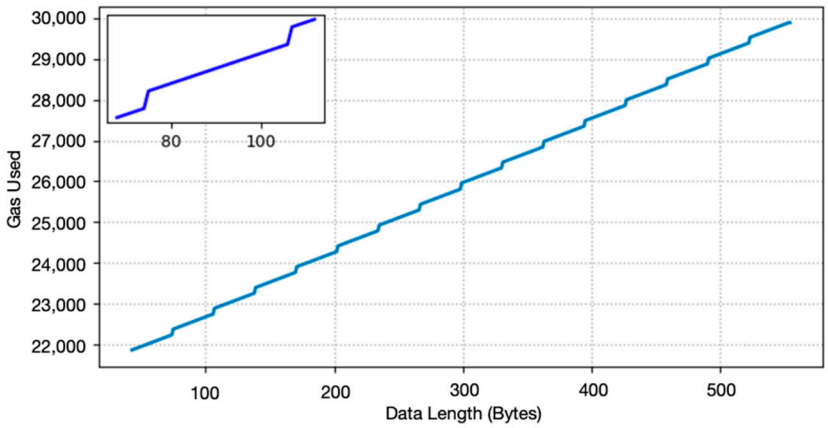

Figure 8. The gas used of the experiment increase as stepwise function.

7. Discussion

7.1. Transaction Fee

When we obtained the precise results, which are shown in the sub-figure in Figure 7, we found that the stepwise line chart of the data length between 43 and 120 represented two levels of the step. We have represented this pattern through a fitted stepwise line chart, which is also described by Equation (3):

$$G(X) = 128 \left\lfloor \frac{x - c}{BlockSize} \right\rfloor + mx + 21,208 + \varepsilon \quad (3)$$

Let x represent the data length of the textual data. The constant c is an adjustment value in the equation. For this experiment, it was set at 10.5. The *BlockSize* function was fixed at 32 bytes per block. Additionally, the slope of the linear function, denoted by m, was 12 units. Lastly, the initial gas usage was 21,208, which was close to the declared value of 21,000 on the yellow page.

Equation (3) demonstrates that a patient who sends vital signs is represented in a JSON format with a length of 64 bytes. The associated *gasUsed* function was 22,104, and this led to a transaction fee of 22,104 $\times$ 1 GWei, which is equivalent to 22,104 GWei (where 1 GWei = 10^{-9} Ether). With the current Ether value of USD 2511.69 (updated on 16 January 2024), the overall transaction cost in fiat was calculated as 22,104 $\times$ 10^{-9} $\times$ 2511.69, thus resulting in USD 0.05 for 64 bytes of data length.

The empirical findings indicated that the transaction costs associated with data transmission through the Internet of Medical Things (IoMT) were not exorbitant. Moreover, the viability of employing this tool for patient monitoring was substantiated in many scenarios. Traditionally, healthcare practitioners conduct patient data tracking bi-daily, i.e., during morning and evening intervals. The frequency of data tracking is contingent upon the individual patient's medical status. However, the absence of real-time tracking is notable, as data are necessitated for transmission to the blockchain network, and a lack of it potentially incurs latency. Consequently, the methodology employed was of a non-real-time type, and the investigation deliberately omitted an analysis of the reporting time dimension.

Furthermore, the system itself can contemplate strategies for mitigating transaction costs. One such strategy involves a reduction in gas prices, albeit in a non-real-time context. This measure enhances the cost-effectiveness of the data transmission. Alternatively, a data processing approach that utilizes a batch service model presents another avenue for cost reduction. This model enables the consolidation of transactions into a daily aggregate. Patients adhere to a predetermined schedule for vital sign measurements, after which the data are synchronized with the blockchain network at specified intervals, such as daily

intervals. This procedural adjustment serves to further optimize overall transaction costs with efficiency.

7.2. Security Issues

Security challenges in remote healthcare monitoring, including unauthorized access and data breaches, are compounded by vulnerabilities in sensor integration and IoT technology, which are further exacerbated by limited connectivity in rural areas. To effectively address these concerns, the implementation of robust measures like authentication, encryption, regular updates, and security audits is essential. Our proposed framework, which is named S3RH, introduces blockchain technology to prevent security issues in remote healthcare monitoring. It serves as a preventive measure against unauthorized access and data breaches, and it ensures the integrity and confidentiality of patient health information.

Our S3RH framework is based on blockchain technology that enhances the security in remote healthcare monitoring by addressing various aspects of security, including confidentiality, integrity, availability, authentication, authorization, and non-repudiation. This is achieved through the following qualities:

- Confidentiality—Encrypted Data Storage: The utilized blockchain employs advanced cryptographic techniques to secure patient health information, and this is achieved by storing it in encrypted blocks that are accessible only to authorized individuals with the corresponding private keys.
- Integrity—Immutable Record: The blockchain ensures data integrity by incorporating a chain of blocks, each containing a hash of the previous block, thus making any attempt to alter the data infeasible due to the decentralized and distributed nature of the utilized blockchain.
- Availability—Decentralized Architecture: The decentralized network architecture of blockchain ensures continuous data availability in the process of healthcare monitoring as the system remains resilient to node failures or compromises, thereby maintaining functionality in the presence of network disruptions or attacks.
- Authentication—Smart Contracts: Smart contracts provide an additional layer of authentication in the IoMT network by automatically executing predefined rules, thereby establishing and enforcing permissions, thus ensuring that only authenticated devices and users can access and update data within the system.
- Authorization—Role-Based Access Control (RBAC): The utilized blockchain, which is implemented through smart contracts, enforces role-based access control (RBAC). This aids with defining roles and permissions to restrict access within the healthcare monitoring system, thereby ensuring that only authorized personnel can access specific patient information, thus preventing unauthorized access.
- Non-Repudiation—Immutable Transaction History: The blockchain's immutable and timestamped record of every transaction ensures non-repudiation by preventing alterations or deletions, thus offering a transparent and auditable trail of all activities within the system, which is also delivered by the system, permanently recording any changes made by users or devices.

In summary, by leveraging blockchain technology in remote healthcare monitoring, the proposed system gains the advantages of a decentralized and secure framework. This not only protects sensitive patient data but also establishes trust in the system's reliability and security. The use of cryptographic techniques, decentralized architecture, and smart contracts contributes to a comprehensive approach to the securing of IoT applications in healthcare.

7.3. Limitations

We have introduced, implemented, and assessed a conceptual framework centered around blockchain technology. The framework was deployed on a local blockchain network, and a Web API was developed, with a subsequent evaluation conducted on an emulator. Notably, our evaluation did not encompass the impact of network speed and hardware

resources, thus rendering the experimental results inapplicable as a reference for real-life applications. An inherent limitation of our experiment lay in all the test cases being executed on the blockchain simulation platform "Ganache". Utilizing a genuine blockchain network would enable an authentic evaluation of the system's gas consumption; however, estimating the response time would become challenging due to the pronounced influence of network bandwidth on the experiment compared to the response time of operations within the blockchain network.

This paper refrained from discussing the overall response time of the proposed system as the application under consideration was characterized as a non-real-time application. The omission of the discussion on the response time was intentional, given the inherent nature of the application. However, it is acknowledged that, in the context of an implementation involving real-time awareness, future work could delve into a comprehensive analysis of the response time and the implications of an augmented *gasPrice*. Such an investigation would provide valuable insights into the system's performance under different conditions and further contribute to the understanding of its suitability for real-time applications.

8. Conclusions

This article introduced the S3RH framework: a secured, distributed database designed for home isolation scenarios. The framework focuses on ensuring the confidentiality, integrity, and availability of patient data in a remote health monitoring system. The prototype includes a smart contract that was demonstrated on a local Ethereum network and was implemented on a Raspberry Pi. Notably, our approach employs blockchain technology to enhance the security of patient information, with a key emphasis on reducing the connections from external health information system (HIS) networks. By initiating the data gathering from the HIS broker, our system minimizes the risk of malicious attacks on the HIS system, which is further fortified by firewalls and robust security controls. Our cost-effective solution boasts low transaction fees, averaging approximately ETH 0.000022104 per transaction (around USD 0.05–0.10, depending on the exchange rate). Though response time was not discussed in this paper due to conducting a closed environment demonstration, we assert that, as a non-real-time application, our framework prioritizes confidentiality, integrity, and service availability. The transactions in the system are processed based on queue waiting times that exceed a predefined threshold to prevent starvation situations. Our smart remote healthcare monitoring device is a prototype and is not compact. To ensure the device is more compact in future works, the single board will need to be changed to a type of tiny IoT device. In addition, the vital sensor will need to be changed to one that can work at the medical level. Finally, the Web3 library also needs to be changed and tested depending on the new platform.

Author Contributions: Conceptualization, J.K., C.J. and D.C.; methodology, C.J.; software, D.C.; validation, J.K., P.K., M.T. and C.J.; formal analysis, P.K., M.T. and C.J.; investigation, J.K. and D.C.; resources, C.J.; data curation, D.C.; writing—original draft preparation, C.J.; writing—review and editing, J.K., D.C., P.K., M.T. and C.J.; visualization, D.C. and C.J.; supervision, C.J.; project administration, C.J.; funding acquisition, C.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Publicly available datasets were analyzed in this study. This data can be found here: [https://www.kaggle.com/datasets/chanankornjandaeng/gas-used-of-blockchain-for-iomt, accessed on 21 November 2023].

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Hernández-Moreno, Y.; Sánchez-Vélez, J.A.; Cruz-Caizaluisa, M.D.L.Á.; Marcillo-Vera, F. Analysis of level compliance with the home isolation protocol in patients diagnosed with COVID-19. *Cienc. Huasteca Boletín Científico Esc. Super. Huejutla* **2023**, *11*, 1–6. [CrossRef]

2. Jabeen, T.; Jabeen, I.; Ashraf, H.; Ullah, A.; Jhanjhi, N.Z.; Ghoniem, R.M.; Ray, S.K. Smart Wireless Sensor Technology for Healthcare Monitoring System Using Cognitive Radio Networks. *Sensors* **2023**, *23*, 6104. [CrossRef]
3. Sowmya, V.; Dharani, K.; Sujitha, R.P. Smart Healthcare Monitoring System. *J. ISMAC J. IoT Soc. Mob. Anal. Cloud* **2023**, *5*, 65–73. [CrossRef]
4. Kishore, A.S.; Chinni, G.R.; JayaLakshmi, G.; Reddy, K.S.K. Smart Healthcare Monitoring System Using IoT Technology. In Proceedings of the 2023 11th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON), Jaipur, India, 10–11 February 2023; pp. 1–5. [CrossRef]
5. Malathi, M.; Muniappan, A.; Misra, P.K.; Rajagopal, B.R.; Borah, P. A Smart Healthcare Monitoring System for Patients Using IoT and Cloud Computing. *AIP Conf. Proc.* **2023**, *2603*, 030012. [CrossRef]
6. Ravi, P.S.; Mohd, J.; Abid, H.; Raju, V.; Shokat, A. Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications. *J. Clin. Orthop. Trauma* **2020**, *11*, 713–717. [CrossRef]
7. Badri, S.; Jan, S.U.; Alghazzawi, D.M.; Aldhaheri, S.; Pitropakis, N. BIoMT: A Blockchain-Enabled Healthcare Architecture for Information Security in the Internet of Medical Things. *Comput. Syst. Sci. Eng.* **2023**, *46*, 3667–3684. [CrossRef]
8. Vieira, M.; Velasco, G.; Carvalho, S. A Decentralized Health Data Repository for Remote Patient Monitoring Using Blockchain and FHIR. In *Anais do VI Workshop em Blockchain: Teoria, Tecnologias e Aplicações*; SBC: Porto Alegre, Brazil, 2023; pp. 85–98. [CrossRef]
9. Mehta, K.; Gaur, S.; Maheshwari, S.; Chugh, H.; Kumar, M.A. Big Data Analytics Cloud-based Smart IoT Healthcare Network. In Proceedings of the 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–13 April 2023; pp. 437–443. [CrossRef]
10. Kciuk, M.; Kowalik, Z.; Sciuto, G.L.; Sławski, S.; Mastrostefano, S. Intelligent medical velostat pressure Sensor Mat based on Artificial Neural Network and Arduino Embedded System. *Appl. Syst. Innov.* **2023**, *6*, 84. [CrossRef]
11. Tahir, R. Framework for Health Data Security within Smart Healthcare. *Res. Sq.* **2023**. [CrossRef]
12. Hamza, R.; Maizate, A.; Ettaoufik, A. Data Security Mechanisms, Approaches, and Challenges for e-Health Smart Systems. *Int. J. Online Eng. IJOE* **2023**, *19*, 42–66. [CrossRef]
13. Shakah, G. Modeling of Healthcare Monitoring System of Smart Cities. *TEM J.* **2022**, *11*, 926–931. [CrossRef]
14. Yeruva, A.R.; Durga, C.V.; Gokulavasan, B.; Pant, K.; Chaturvedi, P.; Srivastava, A.P. A Smart Healthcare Monitoring System Based on Fog Computing Architecture. In Proceedings of the 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 10–12 October 2022; pp. 904–909. [CrossRef]
15. Bera, B.; Mitra, A.; Das, A.K.; Puthal, D.; Park, Y.-H. Private Blockchain-Based AI-Envisioned Home Monitoring Framework in IoMT-Enabled COVID-19 Environment. *IEEE Consum. Electron. Mag.* **2023**, *12*, 62–71. [CrossRef]
16. Prasad, P.K.; Mishra, V.S.; Gajbhar, V.; Pardeshi, T. Home Appliances Controlling using IOT Technique. *J. Name* **2020**, *7*, 288–291.
17. Almaiman, L.; Alqahtani, N. Security and Privacy on IoMT. In Proceedings of the 12th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2020), Online, 15–18 December 2020; pp. 956–963. [CrossRef]
18. Seeman, N. Innovations to Address Social Isolation for Elderly Canadians Aging at Home. *Healthc. Q.* **2023**, *26*, 14–17. [CrossRef]
19. Babu, S.V.; Ramya, P.; Sundar, C.; Pradeep, D. The architecture of smartness in healthcare. In *Edge-of-Things in Personalized Healthcare Support Systems*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 25–44. [CrossRef]
20. Chauhan, N.; Dwivedi, R.K. A Secure Design of the Healthcare IoT System using Blockchain Technology. In Proceedings of the 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 23–25 March 2022; pp. 704–709. [CrossRef]
21. Narwal, B.; Gandhi, K.; Anand, R.; Ghalyan, R. PUASIoT: Password-Based User Authentication Scheme for IoT Services. In Proceedings of the 6th International Conference on Advance Computing and Intelligent Engineering, Odisha, India, 23–24 December 2021; Pati, B., Panigrahi, C.R., Mohapatra, P., Li, K.-C., Eds.; Springer Nature: Singapore, 2023; pp. 141–149.
22. Ghodsi, M.R. Consortium Blockchain Based Anonymous and Trusted Authentication Mechanism for IoT. In Proceedings of the International Conference On Signal and Information Processing, Networking and Computers, Online, 27–29 December 2021; pp. 292–302. [CrossRef]
23. Li, W.; Zhang, S.; Chen, Z.; Sen, L. Cross-Domain Authentication Scheme for IoT Devices Based on BlockChain. In Proceedings of the 2022 IEEE 13th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 21–23 October 2022; pp. 67–73. [CrossRef]
24. Stranieri, A.; Balasubramanian, V. Remote Patient Monitoring for Healthcare: A Big Challenge for Big Data. In *Research Anthology on Big Data Analytics, Architectures, and Applications*; IGI Global, Ed.; IGI Global: Hershey, PA, USA, 2022; pp. 1054–1070. [CrossRef]
25. Yue, K.B.; Sha, K.; Thamarai Selvan, J.S.; Guerra, M.; Wei, W.; Chakka, S.; Vuchuru, P.; Koduru, M.; Liu, X.; Tang, V.; et al. Confidentiality and Data Integrity in Consortium Blockchain Applications for Model Based Systems Engineering. In Proceedings of the AIAA SCITECH 2023, National Harbor, MD, USA, 23–27 January 2023. [CrossRef]
26. Shanthi, S.; Mithun, S.; Prakash, P.K.; Maharajan, K.; Kishore, C.N. A Sensor-Based Data Analytics for Patient Monitoring in Connected Healthcare Applications. In Proceedings of the 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 25–26 March 2022; pp. 2104–2107. [CrossRef]
27. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 26 December 2023).
28. Wang, X.; Liu, L.; Liu, J.; Huang, X. Understanding the Determinants of Blockchain Technology Adoption in the Construction Industry. *Buildings* **2022**, *12*, 1709. [CrossRef]

29. Chukleang, T.; Jandaeng, C. Security Enhancement in Smart Logistics with Blockchain Technology: A Home Delivery Use Case. *Informatics* **2022**, *9*, 70. [CrossRef]
30. Liu, J.; Yan, L.; Wang, D. A Hybrid Blockchain Model for Trusted Data of Supply Chain Finance. *Wirel. Pers. Commun.* **2022**, *127*, 919–943. [CrossRef]
31. Daniel, D.; Speranza, C.I. The Role of Blockchain in Documenting Land Users' Rights: The Canonical Case of Farmers in the Vernacular Land Market. *Front. Blockchain* **2020**, *3*, 19. [CrossRef]
32. Garcia, H.C.E. Blockchain Innovation Technology for Corruption Decrease in Mexico. *Asian J. Innov. Policy* **2021**, *10*, 177–194. [CrossRef]
33. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? *Future Internet* **2018**, *10*, 20. [CrossRef]
34. Dehghani, M.; Mashatan, A.; Kennedy, R.W. Innovation within networks—Patent strategies for blockchain technology. *J. Bus. Ind. Mark.* **2021**, *36*, 2113–2125. [CrossRef]
35. Govardhan, R.; Jagadeesh, V.R.; Lakshminath, S.M.; Sangamad, L. A Literature Review of Blockchain Applications in Healthcare. *Int. J. Sci. Technol. Eng.* **2023**, *11*, 1338–1346.
36. Husain, M.R. Blockchain Applications for Engineering Systems. *Eng. Rep.* **2023**, *5*, 1–3. [CrossRef]
37. Ramzan, S.; Aqdus, A.; Ravi, V.; Koundal, D.; Amin, R.; Ghamdi, M.A.A. Healthcare Ap, plications Using Blockchain Technology: Motivations and Challenges. *IEEE Trans. Eng. Manag.* **2023**, *70*, 2874–2890. [CrossRef]
38. Zia, A.S.; Sayed, M. Blockchain in Healthcare: Unlocking the Potential of Blockchain for Secure and Efficient Applications for Medical Data Management—A Presentation of Basic Concepts. *Liaquat Med. Res. J.* **2023**, 5. [CrossRef]
39. Upadrista, V.; Nazir, S.; Tianfield, H. Secure data sharing with blockchain for remote health monitoring applications: A review. *J. Reliab. Intell. Environ.* **2023**, *9*, 349–368. [CrossRef] [PubMed]
40. Alruwaill, M.N.; Mohanty, S.P.; Kougianos, E. hChain: Blockchain Based Healthcare Data Sharing with Enhanced Security and Privacy Location-Based-Authentication. In Proceedings of the Great Lakes Symposium on VLSI 2023, GLSVLSI '23, Knoxville, TN, USA, 5–7 June 2023; pp. 97–102. [CrossRef]
41. Samuel, O.; Omojo, A.B.; Mohsin, S.M.; Tiwari, P.; Gupta, D.; Band, S.S. An Anonymous IoT-Based E-Health Monitoring System Using Blockchain Technology. *IEEE Syst. J.* **2023**, *17*, 2422–2433. [CrossRef]
42. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. [CrossRef]
43. Hu, B.; Zhang, Z.; Liu, J.; Liu, Y.; Yin, J.; Lu, R.; Lin, X. A comprehensive survey on smart contract construction and execution: Paradigms, tools, and systems. *Patterns* **2021**, *2*, 100179. [CrossRef]
44. Namamula, L.; Chaytor, D. Enhancing the Confidentiality and Integrity of Uncertain Dynamic Data Workflows of B2C (Business-2-Consumers) Using Blockchain Technology. *J. Uncertain Syst.* **2022**, *16*, 2242009:1–2242009:17. [CrossRef]
45. Parmar, K.; Patil, S.; Patel, D.K.; Patel, V.J. Privacy-preserving Authentication Scheme for VANETs using Blockchain Technology. *Procedia Comput. Sci.* **2023**, *220*, 40–47. [CrossRef]
46. Vangala, A.; Das, A.K. Privacy-Preserving Blockchain-Based Authentication in Smart Energy Systems. In Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems, Boston, MA, USA, 6 November 2022. [CrossRef]
47. Hoang, S.T.; Do, Q.T.; Luc, N.-Q. Build a Blockchain-based Confidentiality and Privacy Solution Using Cryptographic Techniques. *Tạp Chí Khoa Học Và Công Nghệ Việt Nam* **2023**, *65*, 1–6. [CrossRef]
48. Malsa, N.; Vyas, V.; Singh, P. Blockchain-Enabled Smart Contract Optimization for Healthcare Monitoring Systems. In *Cloud Computing Enabled Big-Data Analytics in Wireless Ad-Hoc Networks*; CRC Press: Boca Raton, FL, USA, 2022; pp. 229–250.
49. Tamazirt, L.; Alilat, F.; Agoulmine, N. Blockchain Technology: A new secured Electronic Health Record System. In Proceedings of the 6th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2018), Santiago, Chile, 11–12 January 2018; pp. 134–141. Available online: https://hal.science/hal-01777462 (accessed on 26 December 2023).
50. Rajawat, A.S.; Rawat, R.; Barhanpurkar, K.; Shaw, R.N.; Ghosh, A. Blockchain-Based Model for Expanding IoT Device Data Security. In *Advances in Applications of Data-Driven Computing*; Bansal, J.C., Fung, L.C.C., Simic, M., Ghosh, A., Eds.; Advances in Intelligent Systems and Computing, 1319; Springer: Singapore, 2021. [CrossRef]
51. Srinivasu, P.N.; Bhoi, A.K.; Nayak, S.R.; Bhutta, M.R.; Woźniak, M. Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network. *Electronics* **2021**, *10*, 1437. [CrossRef]
52. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. *IEEE Internet Things J.* **2021**, *8*, 11717–11731. [CrossRef]
53. Saxena, A. Blockchain grounded electronic record for healthcare monitoring system. *Int. J. Health Sci. IJHS* **2022**, *6*, 3414–3423. [CrossRef]
54. Xu, J.; Xue, K.; Li, S.; Tian, H.; Hong, J.; Hong, P.; Yu, N. Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. *IEEE Internet Things J.* **2019**, *6*, 8770–8781. [CrossRef]
55. Pawar, P.; Parolia, N.; Shinde, S.; Edoh, T.O.; Singh, M. eHealthChain—A Blockchain-based Personal Health Information Management System. *Ann. Telecommun.* **2022**, *77*, 33–45. [CrossRef] [PubMed]
56. Ramzan, T.; Zafar, S. Blockchain-based Security for Internet of Medical Things Application. In Proceedings of the 2022 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 7–8 December 2022. [CrossRef]

57. Wang, J.; Fan, S.; Alexandridis, A.; Han, K.; Jeon, G.; Zilic, Z.; Pang, Y. A Multistage Blockchain-Based Secure and Trustworthy Smart Healthcare System Using ECG Characteristic. *IEEE Internet Things Mag.* **2021**, *4*, 48–58. [CrossRef]
58. Mohan, D.; Alwin, L.; Neeraja, P.; Lawrence, K.D.; Pathari, V. A Private Ethereum Blockchain Implementation for Secure Data Handling in Internet of Medical Things. *J. Reliab. Intell. Environ.* **2022**, *8*, 379–396. [CrossRef]
59. Alam, T. Blockchain-Enabled Mobile Healthcare System Architecture for the Real-Time Monitoring of COVID-19 Patients. 2021. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3772643 (accessed on 26 December 2023).
60. Sangaiah, A.K.; Jeong, S.; Shen, J.-H.; Ahn, B. A Study on Smart Healthcare Monitoring Using IoT Based on Blockchain. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 9932091. [CrossRef]
61. Arul, R.; Al-Otaibi, Y.D.; Alnumay, W.S.; Tariq, U.; Shoaib, U.; Piran, M.D.J. Multi-modal secure healthcare data dissemination framework using blockchain in IoMT. *Ubiquit Comput.* **2021**. [CrossRef]
62. Machado-Gamboa, K.; Gonzalez-Vargas, A. Development ofa Low-Cost Pulse Oximeter Simulator for Educational Purposes. In Proceedings of the 2018 IEEE ANDESCON, Santiago de Cali, Colombia, 22–24 August 2018; pp. 1–6. [CrossRef]