computers

MDPI

Article

Integrity and Privacy Assurance Framework for Remote Healthcare Monitoring Based on IoT

Salah Hamza Alharbi *, Ali Musa Alzahrani, Toqeer Ali Syed and Saad Said Alqahtany *

Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah 42351, Saudi Arabia; a.alzahrani@iu.edu.sa (A.M.A.); toqeer@iu.edu.sa (T.A.S.)

* Correspondence: salahhalharbi.04@gmail.com (S.H.A.); s.alqahtany@iu.edu.sa (S.S.A.)

Abstract: Remote healthcare monitoring (RHM) has become a pivotal component of modern healthcare, offering a crucial lifeline to numerous patients. Ensuring the integrity and privacy of the data generated and transmitted by IoT devices is of paramount importance. The integration of blockchain technology and smart contracts has emerged as a pioneering solution to fortify the security of internet of things (IoT) data transmissions within the realm of healthcare monitoring. In today's healthcare landscape, the IoT plays a pivotal role in remotely monitoring and managing patients' well-being. Furthermore, blockchain's decentralized and immutable ledger ensures that all IoT data transactions are securely recorded, timestamped, and resistant to unauthorized modifications. This heightened level of data security is critical in healthcare, where the integrity and privacy of patient information are nonnegotiable. This research endeavors to harness the power of blockchain and smart contracts to establish a robust and tamper-proof framework for healthcare IoT data. Employing smart contracts, which are self-executing agreements programmed with predefined rules, enables us to automate and validate data transactions within the IoT ecosystem. These contracts execute automatically when specific conditions are met, eliminating the need for manual intervention and oversight. This automation not only streamlines the process of data processing but also enhances its accuracy and reliability by reducing the risk of human error. Additionally, smart contracts provide a transparent and tamper-proof mechanism for verifying the validity of transactions, thereby mitigating the risk of fraudulent activities. By leveraging smart contracts, organizations can ensure the integrity and efficiency of data transactions within the IoT ecosystem, leading to improved trust, transparency, and security. Our experiments demonstrate the application of a blockchain approach to secure transmissions in IoT for RHM, as will be illustrated in the paper. This showcases the practical applicability of blockchain technology in real-world scenarios.

Keywords: IoT healthcare security; remote healthcare monitoring; blockchain; smart contract

check for updates

Citation: Alharbi, S.H.; Alzahrani, A.M.; Syed, T.A.; Alqahtany, S.S. Integrity and Privacy Assurance Framework for Remote Healthcare Monitoring Based on IoT. *Computers* **2024**, *13*, 164. https://doi.org/10.3390/computers13070164

Academic Editor: Paolo Bellavista

Received: 2 May 2024
Revised: 13 June 2024
Accepted: 27 June 2024
Published: 3 July 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Recent developments in areas like sensor technology, robotics, artificial intelligence, communications, cloud computing, machine intelligence, etc. [1] have played a role in propelling the internet of things (IoT) to the forefront of the information technology industry. The term IoT has gained widespread acclaim in recent years among tech-savvy individuals and businesses alike. Because technology affects every part of our lives, it can be reasonably argued that it is also the most significant factor in bringing about change in the workplace. The IoT is poised to revolutionize not only domestic but also corporate healthcare remote (HR) practices. Connected or "smart" devices will help businesses save time and money, allowing them to better manage their human resources and open up new growth prospects [2].

In the realm of literature, these devices are commonly denoted as "things", IoT de-vices, smart devices, sensors, or motes. IoT devices typically exhibit resource constraints such as low processing power, small batteries, and limited memory. Nonetheless, they possess the

capability to connect to the internet, share data, and execute limited computational tasks [3]. Recognized application domains for the IoT encompass smart homes, industrial control, health monitoring, and smart grids. Nevertheless, alongside their evident advantages, the advent of IoT device has introduced novel security and privacy challenges [4].

IoT technology is rapidly developing around the world, bringing several advantages to practically every facet of human existence. Several information security flaws and attacks [1] are unfortunately opened through the IoT. The inherent computational limitations and common vulnerabilities of IoT devices, combined with their widespread deployment and the ease with which hackers can identify them, reveal the risks and potential global impact of connecting these devices to modern networks [5]. As a result of insufficient security measures, both targeted and widespread attacks on IoT devices have become feasible [6]. Therefore, there are legitimate security issues with exposing widely used real-world gadgets to the internet, and it is necessary to provide smart security solutions for the defense of IoT gadgets against assaults [3]. As stated in [7], in the context of healthcare, "Internet of Things" can apply to a wide range of devices, from implanted heart monitors to infusion pumps used to administer a steady stream of fluids to a patient at a predetermined rate. Medical equipment such as pacemakers, insulin pumps, and cochlear implants are just a few of the millions of devices that rely on the IoT. Unlike a pacemaker, which can only transmit data, some of these devices can receive data as well. Wearables, such as the Apple Watch and Fitbit, are IoT personal healthcare devices that can track vital information, such as the number of steps taken or the number of calories burned, and sync that information with the watch or another device for data analysis and to keep a history, as shown in Figure 1.

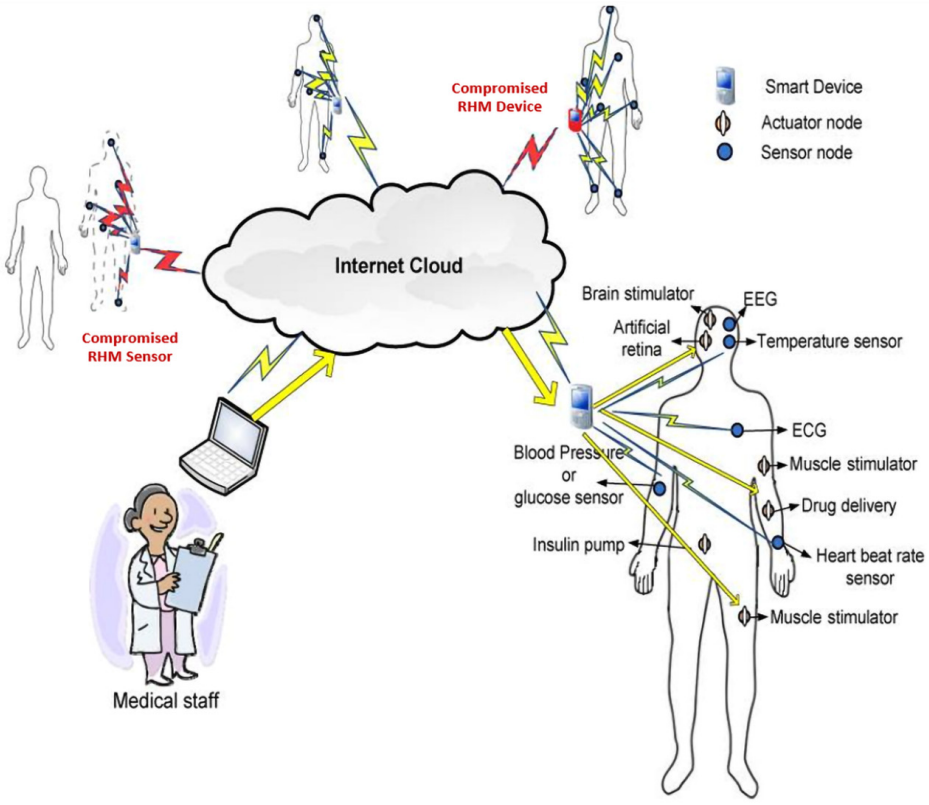


Figure 1. Illustration of a smart healthcare system.

RHM is an important healthcare solution in today's day-to-day life for many patients. For almost every medical symptom, there is a device that keeps track of it, sensing the body attributes for patient monitoring, which is critical to be secure. In this research, the scope is restricted to secure remote patient monitoring. We verified that data collection and reporting are securely documented.

For the RHM data transfer recipient, specifically the healthcare personnel in charge, the steps below in Figure 2 demonstrate our proposed framework.

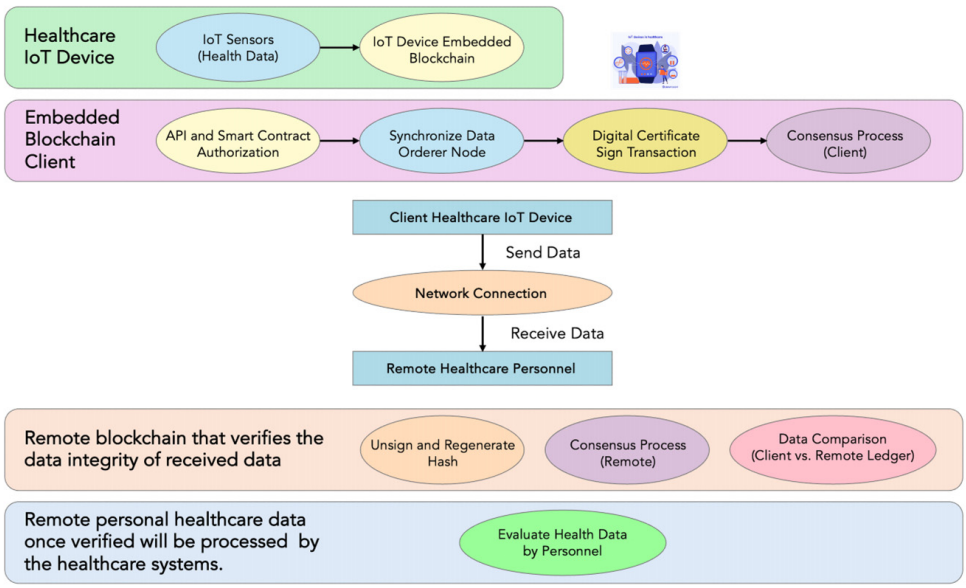


Figure 2. Proposed research methodology structure.

- **Step 1:** Subscribe to a trusted network.
- **Step 2:** Collect and report the data from the patient via IoT devices.
- **Step 3:** The platform should ensure that data is privacy preserved. Unauthorized access should be detected.
- **Step 4:** The end-to-end data from collection to receipt by the RHM should be integrity assured (a verification process will be part of the process).
- **Step 5:** All communication should be signed with a privately owned digital network and backed by a decentralized network instead centralized trusted network.

The rest of the paper is organized as follows. Section 2 presents the background for the reader's understanding of IoT RHM services, applications, blockchain, and smart contracts. A brief literature review and gap analysis are presented in Section 3. Section 4 de-scribes our proposed IoT RHM transmission via blockchain, including its technical de-tails. Section 5 outlines the practical application and deployment of the proposed IoT framework. Section 6 illustrates the experimental results. Section 7 concludes the paper. Section 8 outlines the potential avenues for future research and development based on the findings and limitations the current study identified.

2. Background

In this section, we present the necessary background and contextual information to better understand the paper topic and its significance, in addition to the latest studies related to the subject of this paper.

2.1. IoT RHM Services

2.1.1. Ambient Assisted Living

Systems have the ability to address the difficulties of individual healthcare and to get people involved in their own treatment. The systems offer a complete environment for monitoring healthcare, including hardware components such medical sensors, as well as software and networks. It follows that any service that may be delivered via IoT must itself be categorized as an IoT service [8].

2.1.2. Adverse Drug Reactions

System harm can occur after taking a single dose of a drug, during long-term use of a medicine, or as a result of taking many medications [8].

2.1.3. Community Healthcare

An example of an IoT-enabled service is a cooperative network structure that serves patients in a local community, municipal hospital, or residential area. An effective cooperative IoT infrastructure for monitoring healthcare in rural areas has been proposed [8].

2.1.4. Wearable Device Access

Nonintrusive sensors are available for a wide range of medical uses, including WSN-based healthcare services. In the future, sensors could provide the same services through the IoT. Conversely, wearable technology has the potential to ship with a suite of useful capabilities well suited to the IoT framework [8].

2.1.5. Indirect Emergency Healthcare

Inclement weather, transport (aviation, ship, train, and vehicle) accidents, and the col-lapse of earthen sites are only a few examples of the indirect emergency scenarios that can arise in systems and lead to healthcare problems. In this case, indirect emergency healthcare can provide a variety of answers, including access to relevant data [8].

2.2. IoT RHM Applications

The internet of things (IoT) has many uses in healthcare, but one of the most well known is remote healthcare monitoring (RHM), an innovative approach to enhancing patient management and care. This allows for the digital transmission of disease-related and physiological data about the patient from the patient's home to a healthcare center through telephone, internet, or videoconferencing, providing clinical feedback. Patient awareness and self-management are enhanced, and mortality and hospitalizations are decreased thanks to the early detection of illness [9]. Below are the types of RHM:

2.2.1. Glucose Monitoring

This allows the diabetic patient to make the most informed treatment decisions possible by tracking their fluctuating blood glucose levels throughout the day. The direction, amount, length, frequency, and reasons for changes in blood glucose levels are also presented. The continuous monitoring of glucose levels provides more information than the three to four blood sugar checks recommended by standard intensive glucose monitoring [10].

2.2.2. Heart Rate Monitoring

The heart rate is one of the most important indicators of a person's overall physical health, as measured by vital signs. Remote photoplethysmography offers contactless RHM by catching small light changes in the skin via a video camera, whereas traditional HR monitors often require contact with skin. The potential of this technology for digital healthcare is enormous. [11].

2.2.3. Robotic Surgery Monitoring

Improved surgical instrumentation and ergonomics in comparison to traditional laparoscopic techniques are two of the many reasons why robot-assisted minimally invasive surgery (RMIS) has become so popular in recent years. As a result, RMIS has been most widely adopted in specialized surgical fields like gynecology and urology; however, this is beginning to change as more and more institutions obtain robotic surgical systems [12].

2.2.4. Connected Inhaler Monitoring

When linked to mobile devices, inhaler systems can provide objective data on a patient's adherence and inhaler technique in real time. The e-modules house the energy source and the sensors for evaluation. Some of these are external attachments, while others are built right into the inhaler itself. Clinical studies have demonstrated that inhalers with the ability to track when a dose has been actuated or prepared have the potential to increase adherence and results [13].

IoT healthcare sensors play a crucial role in modern healthcare by enabling continuous monitoring and data collection for patients. These sensors are used to gather various health-related data, such as vital signs, medication adherence, and disease management, and transmit it to healthcare professionals for real-time monitoring and analysis [14].

2.3. Blockchain and Smart Contracts

2.3.1. Blockchain

Blockchain technology is a groundbreaking innovation that has revolutionized data security and transparency across various industries. At its core, blockchain is a distributed and immutable ledger system that utilizes cryptographic hashing to secure data. Hashing is a crucial component of blockchain, involving the transformation of data into a fixed-length string of characters. This process ensures that any change in the original data will result in a completely different hash, making it virtually impossible to tamper with the information stored in the blockchain. Each block in the chain contains a unique hash of the previous block, creating a chain of blocks where data is interconnected and secured, as shown in Figure 3. This hash-based structure enhances the trustworthiness of the blockchain by providing data integrity, authenticity, and resistance to unauthorized alterations [15].

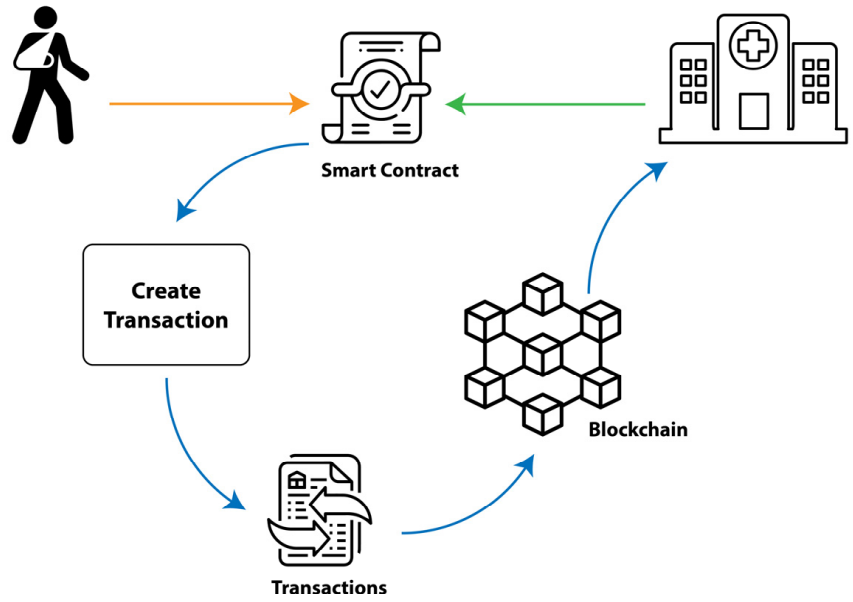


Figure 3. Blockchain-based smart contract.

2.3.2. Smart Contracts

A smart contract is a self-executing digital contract with predefined rules and conditions encoded into computer code. These contracts run on blockchain platforms and automatically execute when specific criteria are met. Smart contracts eliminate the need for intermediaries, reducing costs and increasing the efficiency of transactions, as shown in Figure 3. They find applications in various fields, including finance, supply-chain management, legal processes, and more [16,17].

2.4. IoT RHM Sensors and Microcontrollers

Securing IoT data transmission is a critical concern, and blockchain technology can provide solutions to enhance the security, privacy, and reliability of IoT data. Here are several research endeavors leveraging blockchain to enhance the security of IoT data transmission.

2.4.1. IoT RHM Sensors

IoT RHM sensors are specialized devices designed to collect and transmit various health-related data from patients or individuals. These sensors play a crucial role in modern healthcare by enabling the continuous and remote monitoring of vital signs, chronic conditions, and overall health status [18]. For instance, the heart rate and peripheral capillary oxygen saturation level (SpO2) sensor MAX30100 presents a real-time monitoring system for older adults [19].

2.4.2. MAX30100 Sensor

The MAX30100 sensor is an integrated pulse oximetry and heart rate monitor biosensor module. It operates on a single 1.8 V low-power supply and a separate 3.3 V power supply for the internal LEDs. The small physiological sensor is a complete system consisting of red light or infrared and LED. Therefore, the LED driver, photodetector or photo-diodes, ambient light rejection, digital noise cancellation, and data first-in, first-out are essential components. [20]. Figure 4 shows the MAX30100 IoT sensor used in our system.

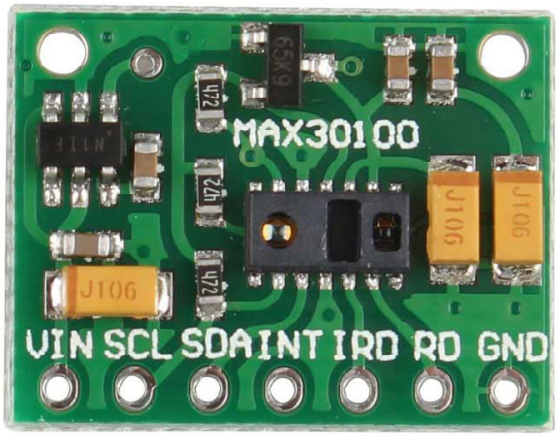


Figure 4. MAX30100 sensor (heart rate and SPO2).

2.5. Microcontrollers

A microcontroller is a compact integrated circuit that serves as the brain of many electronic devices, controlling various functions and processes. It combines a central processing unit memory, input/output peripherals, and often other specialized hardware components, all on a single chip [20]. One well-known microcontroller used in our experiment is the ESP6288, which connects to the RHM sensor to obtain data from the user or patient [19]. Also, it can transmit data to the internet through its Wi-Fi module.

ESP6288 Microcontroller

The ESP8266 is a Wi-Fi microchip with a built-in TCP/IP networking software and microcontroller capability, produced by Espressif Systems in Shanghai, China. An ESP8266 Wi-Fi module is used for the development of end-point IoT applications. It is referred to as a standalone wireless transceiver. It is used to enable internet connection for various applications of embedded systems [19]. Figure 5 shows one of the famous IoT sensors that is used in our system.

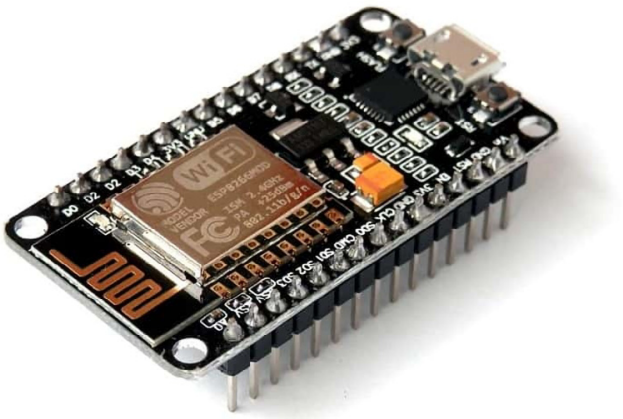
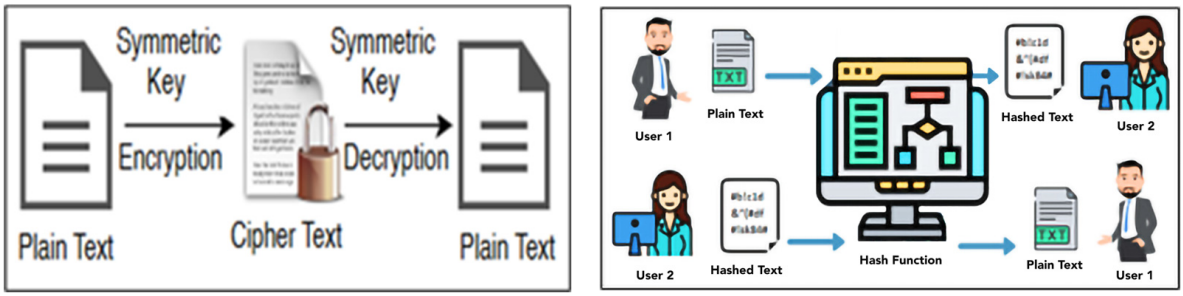


Figure 5. ESP6288 microcontroller.

2.6. Cryptography Techniques

Cryptography techniques are methods and processes used to secure information and communications by converting data into a format that is unintelligible to unauthorized users. Cryptography plays a crucial role in ensuring the confidentiality, integrity, and authenticity of data in various applications, including online transactions, secure communication, and data storage. Here are some fundamental cryptographic techniques, as shown in Figure 6 [21,22].



(**a**) (**b**)

Figure 6. Illustration of some cryptography technologies. (**a**) Symmetric key encryption (**b**) Hash function.

2.6.1. Encryption

Encryption is the process of converting plaintext (human-readable data) into ciphertext (unreadable data) using an encryption algorithm and a cryptographic key. Common encryption algorithms include the advanced encryption standard (AES), Rivest–Shamir–Adleman (RSA), and data encryption standard (DES). Symmetric encryption uses the same key for both encryption and decryption, whereas asymmetric encryption uses a pair of public and private keys [21].

2.6.2. Hash Functions

Hash functions are algorithms that take input data (often of variable length) and produce a fixed-length output called a hash value or digest. They are used to verify data integrity, as even a small change in the input data will result in a significantly different hash value [21].

These cryptographic techniques are just the foundation of modern cybersecurity. They are used in various combinations and configurations to protect data and communications in a wide range of applications and industries. The choice of technique depends on the specific security requirements and the threat model of the system or application being secured [22].

3. Literature Review and Gap Analysis

3.1. Suggested Approaches for Secure IoT Data Transmissions

In reference [23], the researcher explores the challenges and solutions for ensuring the security of edge devices used in remote health monitoring. The authors propose a framework that utilizes named data networking (NDN) architecture to ensure secure and efficient data retrieval, integrating the IoT with edge computing to provide health data security based on hashing and encryption. The paper provides an extensive literature review and background necessary for identifying gaps in current research but does not explicitly mention any existing trusted frameworks for remote health monitoring edge devices in the IoT. However, the authors discuss various protocols such as transport layer security (TLS) and secure shell (SSH) that can be used to ensure secure communication between edge devices and servers. In terms of privacy concerns, the authors emphasize the need for privacy-preserving techniques such as pseudonymization and anonymization, as remote health monitoring involves sensitive personal information. They also discuss access control mechanisms that can be used to restrict access to sensitive data. Finally, the authors propose using digital signatures to ensure data integrity during transmission between edge devices and servers. Overall, this paper provides valuable insights into securing remote health monitoring devices in the IoT through a proposed framework utilizing NDN architecture while addressing privacy concerns and ensuring data integrity through various techniques such as encryption, authentication, access control, pseudonymization, anonymization, and digital signatures.

Reference [24] discusses the challenges of securing healthcare systems based on the IoT and proposes a security framework that incorporates machine learning algorithms to enhance security. The authors identify several challenges in securing IoT-based healthcare systems, including the need to protect sensitive patient data, ensure secure communication between devices, and prevent unauthorized access to medical devices. They propose a multilayered security framework that includes authentication and access control mechanisms, encryption protocols, and intrusion detection systems. The authors also address privacy concerns by proposing measures such as using differential privacy techniques to anonymize patient data and implementing strict access controls to limit who can view sensitive information. Additionally, they suggest using blockchain technology to create an immutable record of all transactions within the system to ensure data integrity. Although there are still many open questions regarding the implementation and effectiveness of this framework in real-world settings, it represents an important step towards improving cybersecurity in healthcare. The proposed framework has the potential to improve patient outcomes by ensuring sensitive medical information is kept confidential while also allowing for secure communication between devices. By incorporating machine learning algorithms into the security framework, the framework can detect and respond to security threats in real time, which is critical for protecting against cyberattacks that could compromise patient safety.

The paper in [25] presents a literature review on the use of blockchain technology for enhancing the security of IoT-based remote patient monitoring systems. The authors discuss the benefits of using blockchain technology in remote patient monitoring systems, such as providing advanced security and privacy properties to healthcare data. They also evaluate various cryptographic technologies that can be deployed using the IoT, including the Arx encryption scheme and ring signatures. Regarding the question of whether there is any trusted framework in place, the authors do not explicitly mention any existing frameworks. However, they propose a novel blockchain-based IoT model that provides advanced security and privacy properties for remote patient monitoring systems. The authors also address privacy-related concerns by introducing the concept of ring signatures, which provide important privacy properties like signers' anonymity and signature correctness. Finally, regarding the question of whether the data transferred is integrity aware, the authors state that their model provides reliable data communication over the network and storage over the cloud with more advanced and lightweight cryptographic techniques like

the Arx encryption scheme. This suggests that their proposed model ensures data integrity during transfer.

The researchers in [14] propose a secure medical data transmission model for IoT-based healthcare systems that integrates steganography and hybrid encryption techniques to ensure the confidentiality, integrity, and authenticity of patient data. The related works section cites several studies on security issues in IoT networks and medical image security, including an efficient joint encryption and data-hiding algorithm for medical image security, a distortionless secret image sharing scheme for IoT systems, and a mobile cloud-assisted framework for the selective encryption of medical images with steganography. The paper does not explicitly mention any existing frameworks or standards that the proposed model follows or complies with. However, the authors do describe in detail the cryptographic scheme used in their model, which combines AES and RSA encryption algorithms to encrypt patient data before embedding it into a cover image using either 2DDWT-1L or 2D-DWT-2L. Patient data is encrypted using a hybrid encryption scheme that ensures confidentiality and authenticity. The embedded data is also concealed within a cover image using steganography techniques to prevent unauthorized access or detection. The authors note that their proposed model can be applied to other types of IoT-based systems beyond healthcare to protect sensitive information from cyber threats. The proposed model ensures both the integrity and authenticity of patient data by using digital signatures to verify its origin and detect any tampering attempts during transmission. The extracted data is decrypted on the destination side to retrieve the original information without any loss or distortion.

Reference [26] presents a multilayered edge-secured cloud framework for healthcare monitoring in older adult care facilities, utilizing smart systems enhanced by comprehensive user interaction. The authors discuss the challenges faced in RHM for older adults, including the fact that most chronic diseases and health disorders at early stages are either asymptomatic or have long latency periods, especially among the older age groups. The proposed framework includes smart devices facilitated with responsive user interfaces that keep patients and doctors in complete control of the smart system while maintaining efficient data communication and security. Although the paper does not mention any existing trusted frameworks used as a basis for this proposed framework, it does address privacy concerns through various security measures, such as secure communication protocols and encryption techniques. Additionally, mechanisms such as digital signatures are proposed to ensure data integrity during transmission. Overall, this paper presents a comprehensive solution to RHM for older adults using cloud-based smart systems that prioritize privacy and data integrity.

Another study [27] introduces a semiautomated framework for identifying and discovering vulnerabilities in Bluetooth low energy (BLE)-enabled wearable health monitoring devices (WHMDs). Although previous research has explored the security and privacy of such devices, there is a need for more comprehensive testing frameworks that can identify both known and unknown vulnerabilities. The authors note that WHMDs can potentially collect sensitive personal health information (PHI) and transmit it over insecure channels, which raises privacy concerns. To mitigate these risks, the authors propose several strategies, including using encryption and authentication protocols to protect data in transit, implementing access controls to limit who can access PHI, and conducting regular security audits. Although the paper does not specifically mention any existing trusted frameworks, the authors note that their framework is designed to be flexible and adaptable to different types of WHMDs. The question of whether data transferred by WHMDs is integrity aware is not directly addressed in the paper, but the authors propose several strategies for ensuring data confidentiality and integrity during transmission. Overall, this paper provides valuable insights into the potential risks and benefits of using BLE-enabled devices for health monitoring, as well as strategies for mitigating cyberattacks on these devices.

Another paper [28] explores the challenges associated with implementing effective security and privacy controls for IoT healthcare devices. The authors highlight the impor-

tance of protecting sensitive patient data and medical records from cyberattacks and discuss potential technologies and techniques that may improve the security of these devices. While several security frameworks proposed by past researchers may potentially improve IoT devices' security posture, there is a lack of combinations of frameworks, including blockchain, machine learning detection, and advanced encryption methods, that may potentially improve IoT device security. Blockchain technology presents a good option for securing data integrity during transmission and storage, and machine learning algorithms provide a way to improve threat detection to prevent potentially harmful cyberattacks against IoT devices. Overall, this literature review highlights the need for continued research into effective security frameworks for IoT healthcare devices to protect sensitive patient data from cyberattacks.

Overall, these studies propose various approaches to secure medical data transmission in IoT-based healthcare systems using different technologies such as blockchain, machine learning, fog computing, homomorphic encryption, and NDN architecture. While each approach has its own pros and cons as shown in Table 1, they all aim to address privacy concerns and ensure data integrity through various techniques such as encryption, authentication, access control, pseudonymization, anonymization, digital signatures, smart contracts, etc.

Table 1. Pros and cons for each study.

Author	Year	Objective	Pros	Cons
Gupta et al. [23]	2023	Ensure security of edge devices used in remote health monitoring using NDN architecture.	Efficient data retrieval, secure data transmission, integrates IoT with edge computing for health data security based on hashing and encryption.	No explicit mention of existing trusted frameworks.
Pirbhulal et al. [24]	2019	Secure data transmission in IoT-based healthcare systems using blockchain technology.	Transparent sharing of medical data among stakeholders while maintaining patient privacy, secure and tamper-proof system, decentralized architecture for improved security and privacy.	Limited scalability due to high computational overhead.
Srivastava et al. [25]	2019	Detect anomalies in medical sensor data collected from IoT devices in healthcare systems using machine learning techniques.	Early detection of potential health issues, unsupervised learning techniques for identifying abnormal patterns in sensor data, improves patient outcomes through early intervention and treatment planning based on detected anomalies.	Limited to detecting anomalies only; does not provide a comprehensive solution for securing medical data transmission.
Elhoseny et al. [14]	2018	Secure medical data transmission in IoT-based healthcare systems using an innovative approach addressing privacy concerns and ensuring the integrity and authenticity of patient data while being applicable to other types of IoT-based systems beyond healthcare as well.	Comprehensive approach to securing medical data transmission, addresses privacy concerns and ensures the integrity and authenticity of patient data, applicable to other types of IoT-based systems beyond healthcare as well.	No explicit mention of existing trusted frameworks.

Table 1. *Cont.*

Author	Year	Objective	Pros	Cons
Raghu et al. [26]	2022	Secure medical data transmission in IoT-based healthcare systems using a hybrid approach combining blockchain technology with homomorphic encryption techniques.	Ensures secure sharing of medical data among different stakeholders while maintaining patient privacy; ensures confidentiality of sensitive information using homomorphic encryption techniques.	Limited scalability due to high computational overhead.
Zendehdel et al. [27]	2021	Develop an intelligent system for monitoring elderly people's health status using wearable sensors and machine learning algorithms.	Predicts the risk of falls among elderly people based on sensor data, which can help prevent falls and improve their quality of life.	Limited to monitoring elderly people's health status only; does not provide a comprehensive solution for securing medical data transmission.
Ratta, et al. [28]	2021	Develop a secure and efficient data transmission protocol for IoT-based healthcare systems using blockchain technology.	Ensures secure sharing of medical data among different stakeholders while maintaining patient privacy; lightweight consensus algorithm to ensure efficient data transmission.	No explicit mention of existing trusted frameworks.

3.2. Blockchain Approaches

Securing IoT data transmission is a critical concern, and blockchain technology can provide solutions to enhance the security, privacy, and reliability of IoT data. Here are several research endeavors leveraging blockchain to enhance the security of IoT data transmission, as shown in below Table 2.

Table 2. Summary of recent studies on IoT blockchain security.

Reference	Authors	Year	Methodology	Research Field
[29]	Zheng, Zibin, et al.	(2018)	The methodology used in the paper is sound and comprehensive. The authors conducted a thorough literature review and identified a wide range of consensus protocols for IoT networks. They also developed a useful classification of consensus protocols based on their underlying mechanisms. The evaluation of the consensus protocols was also well done, and the authors provided clear and concise recommendations for future research.	Blockchain technology has the potential to revolutionize the way that IoT devices are used, and consensus protocols are essential for making blockchain-based IoT networks secure and reliable.
[30]	Majeed, Umer, et al.	(2021)	Comprehensive review of the role of blockchain in enabling IoT-based smart cities, including applications, case studies, and requirements.	IoT-based smart cities
[31]	Pustišek, Matevž, and Andrej Kos.	(2018)	Approaches to front-end IoT application development for Ethereum, with architecture comparison and practical considerations.	Conceptual paper on front-end IoT application development for Ethereum, without experiments.

Table 2. *Cont.*

Reference	Authors	Year	Methodology	Research Field
[32]	Kasey Panetta	(2018)	Blockchain-based security framework for IoT devices leveraging immutability, decentralization, and transparency.	Conceptual paper on IoT security using blockchain technology, without experiments.
[33]	M. A. Khan and K. Salah,	(2018)	Peer-reviewed collection of original research papers on the latest advances in communication and computational technologies.	Proceedings of a conference on communication and computational technologies, without experiments.
[28]	Ratta, Pranav, et al.	(2021)	"Applications, Challenges, and Future Perspectives" reviews the applications, challenges, and future perspectives of blockchain and IoT in the healthcare and medical sector.	Survey paper on applications of blockchain and IoT in healthcare, without experiments.
[34]	Zheng, Zibin, et al.	(2017)	Proposes a novel access control framework for IoT devices that leverages blockchain technology to ensure secure and dynamic access control based on device attributes and trust levels.	Blockchain-based security for IoT devices, specifically for access control.
[35]	Katende, M.	(2020)	Proposes a blockchain-based authentication mechanism for the MQTT protocol, which uses the Ethereum blockchain to implement a second-factor out-of-band channel.	Experimental paper on blockchain-based authentication mechanism for MQTT using Ethereum smart contracts.
[36]	Aborokbah, Majed M., et al.	(2019)	Discussion of the potential of blockchain technology to improve IoT security by providing secure data storage, sharing, authentication, and authorization.	Conceptual paper on the potential of blockchain technology to improve IoT security, without experiments.
[37]	Kizza, Joseph Migga, et al.	(2017)	Presents the current state of the art in blockchain-based security solutions for IoT devices and identifies key challenges and future research directions.	Survey of blockchain-based security solutions for IoT devices, without experiments.

3.3. Gap Analysis

While considerable progress has been made in the field of remote healthcare monitoring using IoT devices, a critical gap remains in ensuring the comprehensive integrity and privacy of patient data. Existing solutions often focus on data transmission and device functionality, neglecting the robust assurance of data integrity and privacy protection throughout the entire data life cycle. Furthermore, the integration of blockchain technology and smart contracts for enhanced security is a relatively unexplored area in the context of remote healthcare monitoring. This gap highlights the need for a dedicated framework that not only addresses data integrity and privacy concerns but also leverages emerging technologies to fortify the security of patient data. Additionally, a lack of standardized protocols and best practices for implementing such a framework in real-world healthcare settings underscores the necessity for comprehensive research and practical guidelines. Bridging this gap is imperative to ensure that remote healthcare monitoring systems are not only effective in data collection but also resilient against security threats and privacy breaches, ultimately fostering trust and reliability in this vital healthcare domain.

Summary

The Sections 2 and 3 provides a thorough exploration of the theoretical underpinnings, principles, and prior studies pertaining to the thesis topic. Its purpose is to create the context and knowledge base essential for readers to grasp the subsequent chapters and the research's contributions.

4. Proposed IoT RHM Blockchain Scheme

In this section, we present a detailed exposition of the proposed blockchain scheme. The primary aim of this section is to provide a comprehensive and structured elucidation of the methodology, algorithms, and techniques utilized within the scheme. The inclusion of an image provides readers with a holistic insight into the inner workings of the proposed system, its core components, and the rationale that guides its design as shown in Figure 7.

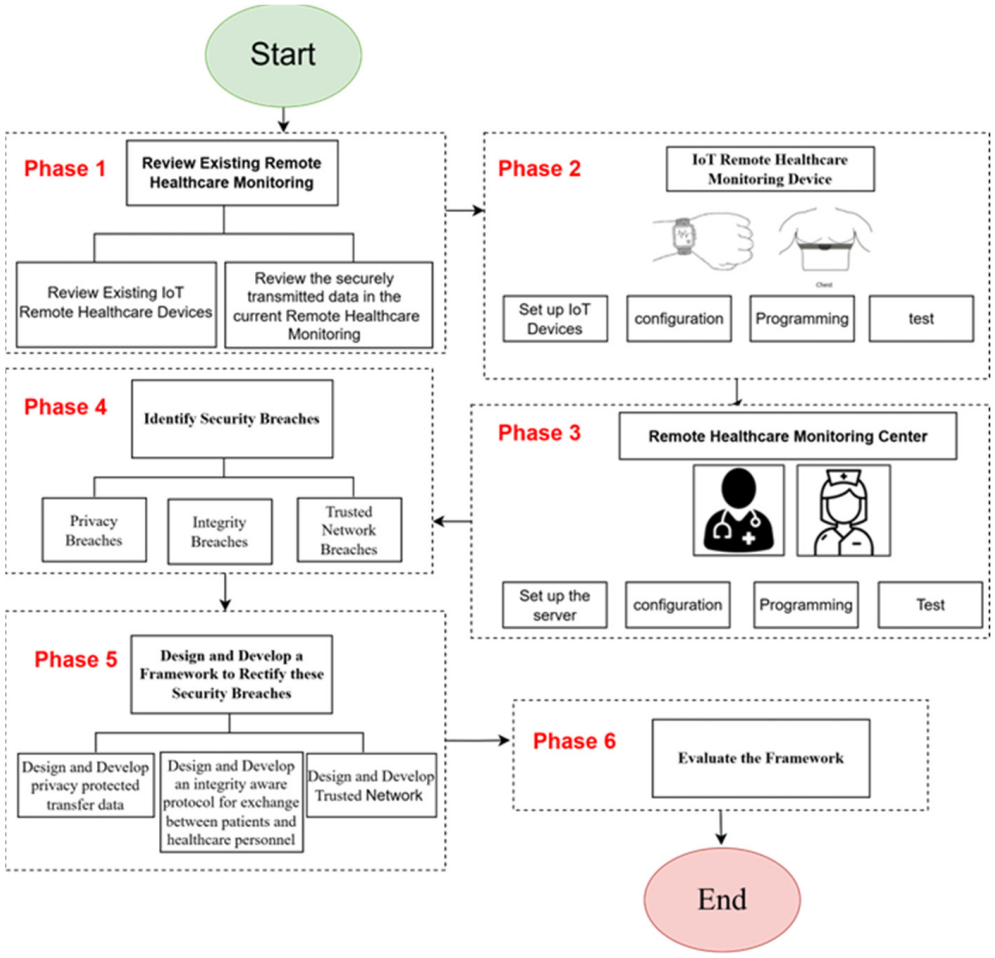


Figure 7. Illustration of the proposed IoT RHM blockchain scheme.

4.1. Core Proposed Methodology

The core proposed methodology used to design IoT RHM security through blockchain that is most appropriate in the context of our paper is derived from previous literature review and can be classified into six main phases, as shown in Figure 7. In the next subsection, you can see the details of the steps.

4.2. Methodology Phases

In this part, we aim to elaborate on the six stages that guide us in determining the most effective approach for securing IoT transaction data, drawing upon insights from the prior literature review as phases follows.

4.2.1. Review the Securely Transmitted Data in the Current RHM

Reviewing securely transmitted data in the current RHM system involves assessing the integrity, confidentiality, and accessibility of patient information as it traverses the network. This review ensures that sensitive health data is protected.

4.2.2. IoT RHM Devices

These devices allow healthcare providers to monitor patients' vital signs, such as blood pressure, heart rate, and oxygen levels, from a remote location. Some examples include wearable health monitors. Moreover, we will be establishing IoT device setup, configuring, and programming and conducting testing.

4.2.3. Remote Healthcare Monitoring Center

The RHM center functions as a centralized platform devoted to overseeing and presenting crucial health data originating from patients. In this phase, we aim to establish RHM server setup, configuring and programming and conduct testing.

4.2.4. Identify Security Breaches in the IoT Devices and Their Communication Mechanisms

In this phase, we aim to identify security vulnerabilities that arise in the context of data transmitted by IoT RHM, covering concerns related to security, privacy, data integrity, and network trust. Subsequently, we will compile common issues to construct potential attack scenarios and clarify how our framework can successfully address and mitigate these challenges, including scenarios such as detecting data-tampering attempts in the proposed system.

4.2.5. Design and Develop a Framework to Rectify These Security Breaches

In this phase, we aim to implement and develop a comprehensive security framework that can help to prevent and rectify security breaches in RHM as follows:

- **Step 1:** Design and develop privacy-protected transfer data.
- **Step 2:** Design and develop an integrity-aware protocol for exchange between patients and the healthcare center.
- **Step 3:** Design and develop a trusted network.

  So, all participants can register on a decentralized network.

4.2.6. Evaluate the Framework

IoT healthcare solutions empower healthcare providers to remotely monitor and manage patient health. This study focuses on examining the types of data received from patients' bodies and how it is processed, including the printing of patient data. Additionally, we will assess the integrity of patient data through an integrity verification process. This involves verifying whether the data remains unchanged during transmission from the patient's location to remote healthcare personnel. If such a system is not already in place, it will be integrated into our proposed health monitoring framework. Our evaluation of the IoT RHM device is guided by three core principles:

- **Privacy:** RHM devices, like any other technology that collects and stores PHI, must prioritize privacy. So, end-to-end privacy verification of patient data as soon as collected from the patient through IoT devices and until received or processed by healthcare personnel is needed. Data privacy should be protected.
- **Integrity:** Ensuring the integrity of RHM devices is important to ensure the accuracy and reliability of the data being collected. So, end-to-end integrity validation of the data is ensured for the patient. The data that is collected from the patient should be secure until receipt or processing by healthcare personnel.
- **Trusted Network:** The patient and healthcare personnel should be in a trusted network.

4.3. Proposed IoT Remote Healthcare Monitoring Transmission via Blockchain

Securing healthcare data transmission in IoT monitoring through blockchain technology represents a pivotal step towards safeguarding sensitive medical information and ensuring the well-being of patients. With the proliferation of IoT devices in healthcare, including wearable sensors and remote monitoring systems, the need for a robust security framework has never been more critical. Blockchain, known for its decentralized and immutable nature, offers a promising solution. By integrating blockchain into the IoT ecosystem, healthcare data can be securely recorded, transmitted, and accessed by authorized parties only. This not only protects patient privacy but also guards against data tampering, ensuring the accuracy and integrity of health records. In an era where the confidentiality and reliability of healthcare data are paramount, the adoption of blockchain technology in IoT healthcare monitoring transmission represents a significant stride towards a safer and more efficient healthcare landscape. In this part, we introduced and demonstrated our framework. In Figure 8, the process of measuring heart rate and SPO2 begins with the patient placing their finger on the sensor. This action triggers the microcontroller to collect the patient's data, which is then transmitted to a blockchain system. The process unfolds through a smart contract, which serves as a program stored on the blockchain and executes when predefined conditions are met. This smart contract undergoes three distinct stages.

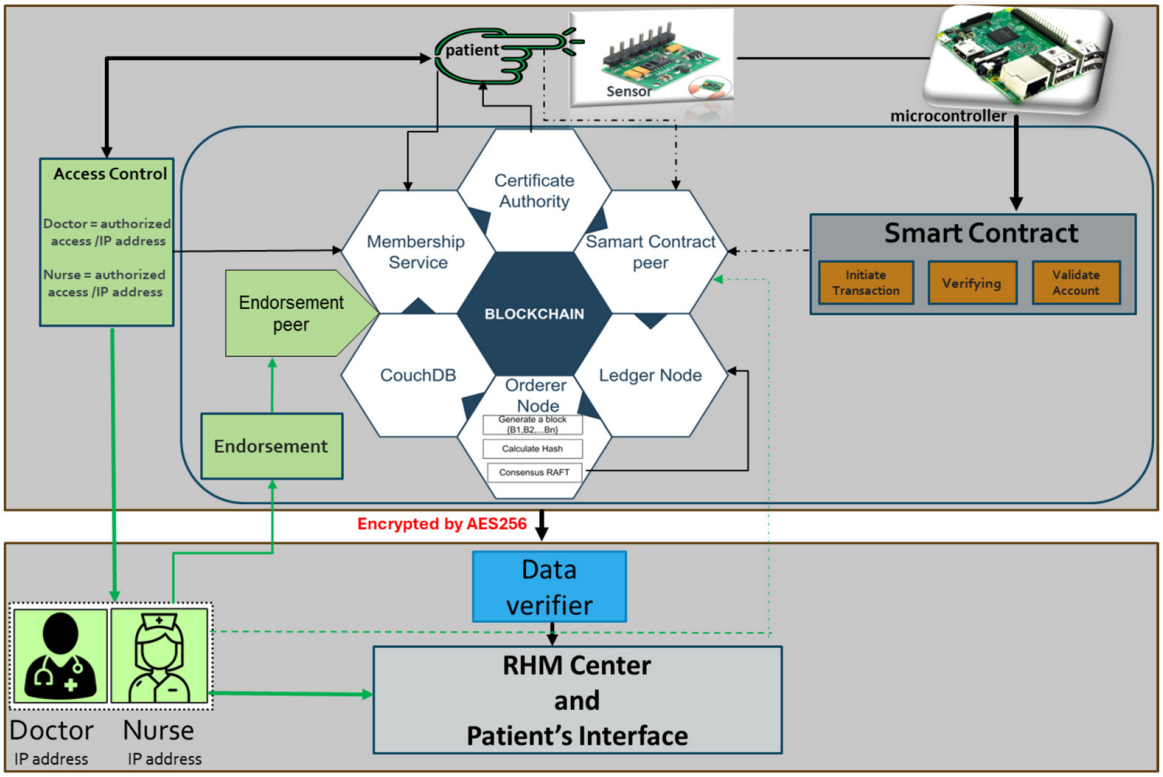


Figure 8. Illustration of the proposed framework security of RHM.

4.3.1. Initiate Transaction

The patient initiates a transaction by sending a request through a subscriber node, which acts as a smart contract peer. This subscriber node is responsible for handling access control by verifying the user's details. Upon validation, the subscriber node issues a digital certificate to the patient.

4.3.2. Verifying

The subscriber node forwards the request to the endorsement node, also through a smart contract. Here, an endorsement node executes a chain code to access the ledger and verify the transaction's validity. If the transaction meets the criteria, the endorsement

node signs the proposal and sends a response back to the patient through the smart contract application.

4.3.3. Validate Account

The transaction is broadcast to the ordering node, which generates a block and forwards it to the committing peer, also known as the consensus node. This consensus node updates the block to the ledger and utilizes the RAFT consensus algorithm, widely embraced for its reliability and efficiency.

Following this, the patient receives feedback responses at the conclusion of each transaction through the remote health monitoring (RHM) server. Each block is linked to the previous one by generating a new hash, ensuring data integrity and immutability. To enhance security during transmission, the data is encrypted using the AES256 encryption standard before being transmitted to the RHM center. Upon arrival, the server at the RHM center decrypts and validates the data using the hash and previous hash values before displaying it for further analysis and monitoring.

This comprehensive process ensures the integrity, security, and reliability of the patient's health data throughout the transmission and storage within the blockchain system, thereby enhancing trust and confidence in remote health monitoring systems.

4.4. RHM Center Data Collecting and Verifying

Healthcare data collection and verification are two essential components of managing healthcare information effectively and ensuring the quality and accuracy of medical records. These processes are crucial for providing quality patient care, medical research, and healthcare policy development. Figure 9 illustrates the protocol for collecting and verifying healthcare data and the components of the protocol, as follows:

- **Patient with wearable IoT devices:** The IoT device will collect all health data from the patient. Such data could be heartbeats and SPO2 monitoring data. Patients themselves are the owners of their personal data and are responsible for granting, denying, or revoking data access to or from any other parties, such as the RHM center. If the patient needs medical treatment, he/she will share personal health data with the desired doctor. Once the treatment is finished, the patient can deny further access to the doctor or healthcare provider.
- **Smart contract:** The smart contract enables the establishment of agreements within IoT devices, which are triggered when specific conditions are satisfied. For instance, we can configure conditions for both the highest and lowest heart rate and SpO2 levels. When the wearable device detects readings that fall outside the specified range, the smart contract will promptly dispatch an alert message to the authorized the patient or healthcare provider. Simultaneously, it will archive the anomalous data in the cloud, ensuring healthcare providers can access the patient's heart rate or SpO2 readings when necessary.
- **Blockchain:** In the blockchain system, each block in the sequence 1, 2,. . ., n contains a batch of transactions. These transactions are verified, timestamped, and added to the block by network participants, known as validators. Once a block is successfully created, it is cryptographically linked to the previous block through a unique hash, forming a secure and immutable chain of blocks. This process repeats for each block in the sequence, with the blockchain growing continuously as new blocks are added. The blockchain's decentralization and consensus mechanisms ensure the security and integrity of the data stored within it. It provides transparency and trust among participants in the network, making it a reliable technology for various applications.
- **Hash:** The hash is a crucial process of the blockchain that creates a unique hash value for each block of data, transaction, or any piece of information stored within the blockchain. This hash is generated using a cryptographic hash function. Additionally, hashing provides data privacy because the actual data is not stored on the blockchain;

instead, only its hash representation is recorded. This ensures sensitive information remains confidential while still being verifiable.

- **Data Verifier:** The data verifier plays a crucial role in ensuring data integrity and security during the transition to the remote healthcare data center. Each block contains a hash of the previous block, forming a secure chain of blocks linked and encrypted by AES256. Subsequently, the RHM center decrypts the data to map the previous hash and block hashing of each block. Any alteration in the data within a block would result in a change in its hash value, consequently impacting the subsequent blocks in the chain. This characteristic renders it exceedingly difficult for malicious actors to modify past transactions or blocks without detection.
- **RHM center:** The RHM center serves as a centralized repository for patient data, presenting vital information such as heart rate and SpO2 readings in real time or as recorded data. This center plays a pivotal role in modern healthcare by offering a key function (real-time monitoring, data display, data history, data security, improved access to healthcare, etc.).
- **Privacy:** The primary objective of privacy is to restrict, control, and safeguard access to an individual's personal information and sensitive data. This is achieved through access management processes that empower authorized individuals to determine who can access their data and under what circumstances. These processes are designed to uphold the patient's autonomy while safeguarding their confidentiality and security.
- **Doctor/nurse:** The doctor and nurse are essential nodes responsible for providing care to patients in our system. They are not allowed to disclose patients' data without proper authority or consent by the patient's access management.

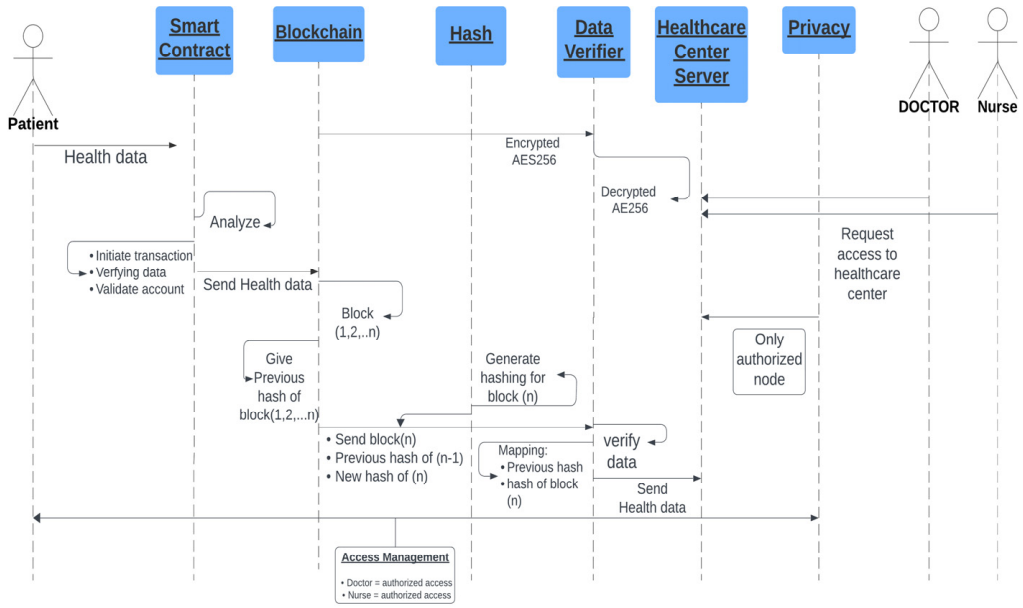


Figure 9. Illustration of the protocol for collecting and verifying RHM data.

4.4.1. Formal Description of the Protocol

Definitions:

- Let *Di* represent the health data collected at instance *i*.
- Let *H* be a cryptographic hash function, e.g., SHA-256.
- Let *Bj* represent a blockchain block containing the *j* transaction.
- Let *C* denote the concatenation operation.
- Let *V* be the verification function comparing the received data hash and the calculated hash.

4.4.2. Protocol Steps

(1) Data Collection and Hashing:

- For each data instance i, calculate the hash of the data:

$$hi = H(Di) \tag{1}$$

(2) Block Creation:

- Create a new block Bj for transaction j, which includes hi and potentially other data (e.g., timestamp, device ID).
- If multiple data instances are included in one block, concatenate their hashes:

$$hcombined = H(C(h1,\ h2\ldots,\ hn)) \tag{2}$$

(3) Blockchain Integration:

- Integrate Bj into the blockchain, ensuring that Bj contains hcombined or the individual hi for all included data instances.
- The integration also involves linking Bj with the previous block Bj by including $H(Bj-1)$ in Bj.

(4) Data Transmission and Verification:

- Transmit the collected data Di alongside its corresponding block identifier j to the healthcare monitoring platform.
- Upon receipt, the platform retrieves Bj from the blockchain and extracts hcombined or the relevant hi.
- Recalculate the hash(es) of the received data:

$$hi' = H(Di) \tag{3}$$

or

$$hcombined' = H\big(C\big(h'1,\ h'2,\ \ldots,\ h'n\big)\big) \tag{4}$$

- Verify the integrity by checking if

$$hi' = hi \tag{5}$$

for individual data instances or for combined hashes.

$$hcombined' = hcombined \tag{6}$$

4.4.3. Mathematical Representation

For all i, $hi' = H(Di)$, and hi is extracted from Bj. If $hi' = hi$ or ($hcombined' = hcombined$) for combined hashes, then data integrity is confirmed.

The proposed protocol ensures the integrity and authenticity of health data transmitted from IoT-based healthcare devices to a remote monitoring platform. By leveraging cryptographic hash functions and blockchain technology, each piece of data is hashed, and the hash is stored in a blockchain.

This process creates an immutable and verifiable record of health data as it was at the time of collection. Upon receipt of the data, the RHM center platform can verify its integrity by recalculating the hash and comparing it to the hash stored on the blockchain. If the hashes match, it confirms that the data has not been altered in transit. This verification process provides a trusted mechanism for ensuring that healthcare professionals receive accurate and untampered data, enabling them to make informed decisions and respond appropriately to patients' conditions.

5. Implementation of the proposed IoT framework

This section offers details on the actual execution of the experiment undertaken as part of the research. It outlines the methodology, tools, technologies, and procedures used to conduct the experiment and elaborate the installations of IoT device tools, configuration, and proposed protocol that are used in our experiment, as shown in Figure 10.

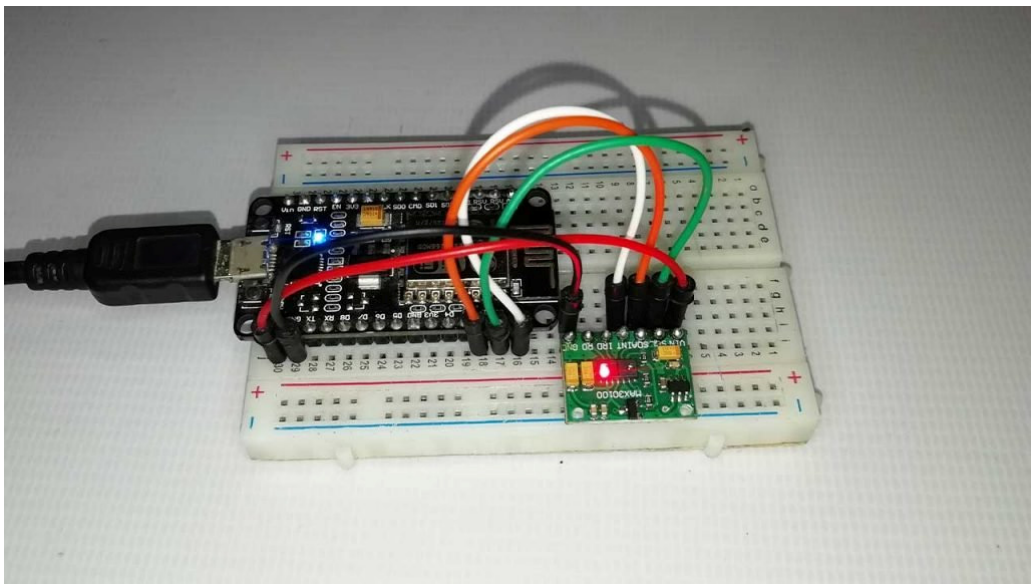


Figure 10. Illustration of IoT devices used in the lab (MAX30100 and ESP8266).

5.1. Data Collection

Collecting heart rate and SpO2 data through IoT sensors from a user's finger is a vital aspect of remote health monitoring.

To collect this data, the IoT sensor emits light through the fingertip, and a photodetector on the opposite side measures the intensity of the transmitted or reflected light. This process enables the sensor to detect the pulse blood changes in blood volume, which are directly related to the patient's heart rate.

Once the IoT sensor has collected this vital data, it is then transmitted to a central processing unit, often a microcontroller. Its role extends beyond mere data transmission, as it can also be programmed to perform real-time computations or trigger alarms based on predefined thresholds, enhancing the functionality of the IoT healthcare system. Simultaneously, the sensor can assess the absorption of specific wavelengths of light to determine the oxygen saturation level in the blood, a crucial parameter for assessing respiratory and circulatory health. Then, the collected data is transmitted wirelessly to the RHM central system or a mobile application for display and analysis.

5.2. Testbed Environment

The implementations are carried out using Arduino IDE (Integrated Development Environment) and Visual Studio Code with Windows 10, a 64-bit operating system, the IoT sensor, and the microcontroller. Table 3 shows the other specifications.

Table 3. Testbed environment.

RAM	20.0 GB
Processor	intel(R) Core (TM) i7-10750H CPU @ 2.60 GHz 2.59 GHz
Sensor	MAX 30100 pulse oximeter and heart beat sensor
Microcontroller	ESP8266 with Wi-Fi module

Table 3. *Cont.*

Software tool	Arduino IDE (2.2.1) and Visual Studio Code (1.84.2)
Development program	Node.js, SQL, Go, and PHP

Visual Studio Code

Visual Studio Code is a popular code editor developed by Microsoft that supports a wide range of programming languages and technologies, including Node.js and blockchain development. When working with blockchain technologies, you typically write and deploy smart contracts, develop decentralized applications (dApps), and interact with blockchain networks [38].

5.3. IoT Device Configuration

5.3.1. MAX30100 Sensor with ESP6388 Microcontroller

The MAX30100 is a pulse oximeter and heart rate sensor module, and the ESP8266 is a popular Wi-Fi-enabled microcontroller. To use the MAX30100 sensor with the ESP8266 microcontroller, we need to connect the sensor to the microcontroller, write code to read and process the sensor data, and install the libraries of the MAX30100 and ESP 8266 via Arduino IDE, as shown in Figure 11.

```
1   #include <ESP8266WiFi.h>
2   #include <ESP8266HTTPClient.h>
3   #include <Wire.h>
4   #include <ArduinoJson.h>
5   #include "MAX30100_PulseOximeter.h"
```

Figure 11. Install MAX30100 and ESP 8266 libraries.

The next steps are to determine and identify the parameters and Wi-Fi connection of the sensor (pulse oximeter) and RHM center. Table 4 illustrates the normal range of heart rate and SPO2.

Table 4. The range of heart rate and SPO2.

Parameter	Normal Range	Reference
Heart rate	60~130	[39]
SPO2	95~100%	[40]

5.4. Hyper-Ledger Components

In the hyper-ledger fabric, our stakeholders are situated in the initial layer. These stakeholders encompass specific individuals and entities who engage with the smart contract. They are symbolically represented as patients who possess ownership of their respective health records. Additionally, this layer includes API interfaces and any third parties, such as doctors and nurses, who require connectivity with our network.

Moving into the second layer, we encounter the heart of our system—the smart contract. This intelligent component facilitates transactions among clients or participants utilizing the network. It is imperative that these transactions adhere to three essential characteristics: reliability, traceability, and immutability, ensuring that they remain impervious to tampering or alteration. Within the hyper-ledger fabric architecture, this framework comprises various types of nodes, namely endorsers, orderers, and consensus participants, as illustrated in Figure 12.

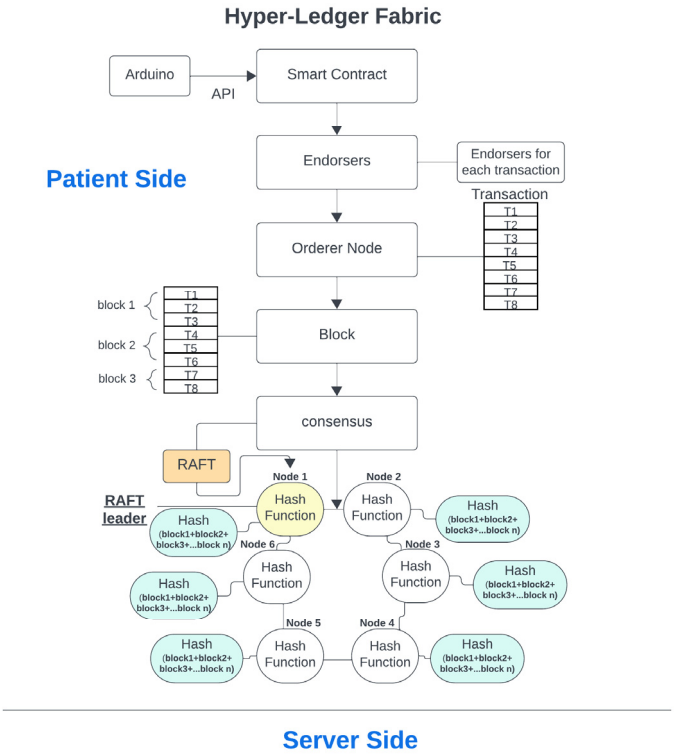
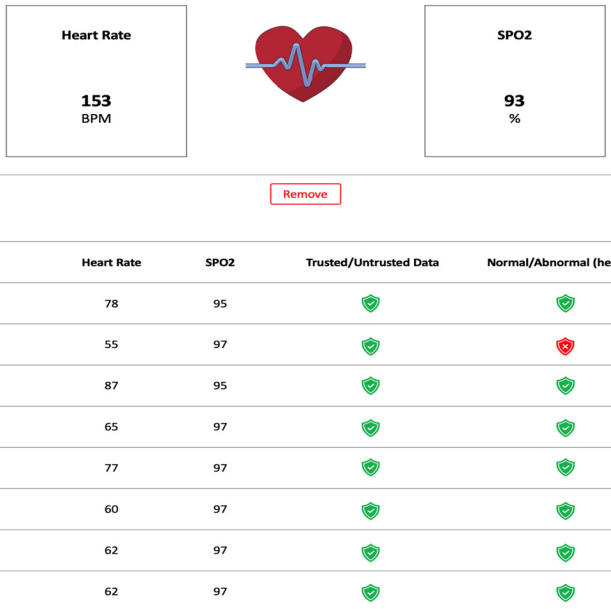


Figure 12. Illustration of the transactions over the hyper-ledger fabric.

5.5. Remote Healthcare Monitoring Center

The RHM center serves as a central platform dedicated to monitoring and displaying critical health information from patients in remote locations. This includes real-time tracking of essential metrics such as heart rate and SPO2 levels. The center ensures the integrity and security of patient data, guaranteeing its accuracy and privacy. Through a user-friendly interface, healthcare professionals can access and assess patients' vital signs, enabling timely interventions when necessary. The status of heart rate and SPO2 levels is prominently displayed, allowing healthcare providers to make informed decisions and provide remote care, as shown in Figure 13.



ID	Date	Heart Rate	SPO2	Trusted/Untrusted Data	Normal/Abnormal (heartbeat)	Normal/Abnormal (SPO2)
1	1/5/2024 22:55:26	78	95			
2	1/5/2024 22:55:40	55	97			
3	1/5/2024 22:55:44	87	95			
4	1/5/2024 22:55:40	65	97			
5	1/5/2024 22:55:53	77	97			
6	1/5/2024 22:56:02	60	97			
7	1/5/2024 22:56:07	62	97			
8	1/5/2024 22:56:07	62	97			

Figure 13. RHM interface for the patient.

6. Experimental Results

This section offers a thorough examination of the experimental outcomes, delivering an overview of the system that was used to validate the proposed secure IoT transmission data via blockchain. It will delve into the outcomes, analysis, and interpretation of the experimental data. The central goal is to clarify the experiment's objectives and the methods employed for data collection and analysis. We inspected a sample of 40 requests from the patient side to measure our system's performance.

6.1. Performance of Our System

The performance of the experimental system is a critical aspect of the study, assessing how effectively the system operates in real-world conditions. This evaluation involves measuring various performance metrics, such as data integrity, throughput, and latency. By analyzing these metrics, the system's efficiency and effectiveness can be gauged, providing valuable insights into its overall performance. Figure 14 depicts a chart illustrating the trends and data for both heart rate and SPO2 levels.

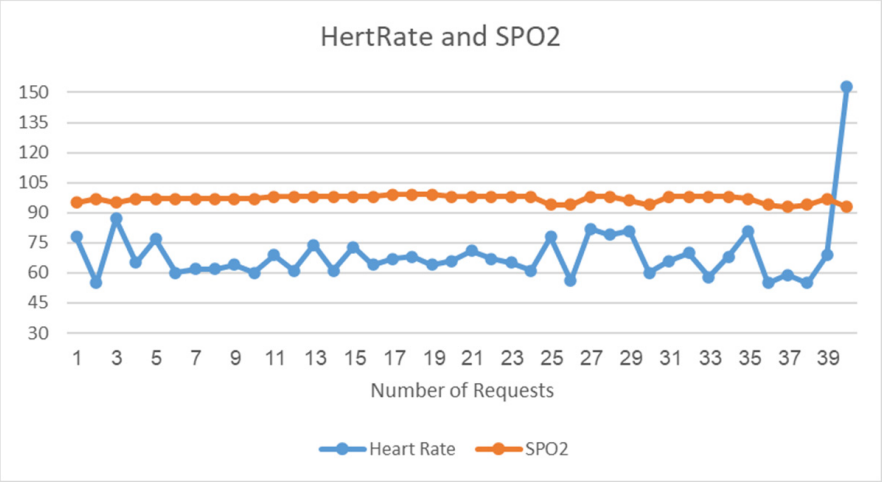


Figure 14. Benchmarking of heart rate and SPO2.

Table 5 offers an extensive insight into supplementary patient information that is presented within the RHM center, encompassing the three primary components:

- Trusted data: This component verifies the integrity of the data. In the event of any tampering attempts, the system employs a "Data Verifier" located within the RHM center to detect and ensure the security and integrity of patient data. 'Trusted' is highlighted as green and 'Untrusted' is highlighted as red.
- Heart rate status: This component indicates the status of the heart rate, which can fall into either a normal or abnormal category (60~130), based on the heart rate range described in Section 5.3.1. 'Normal' is highlighted as green and 'Abnormal' is highlighted as red.
- SPO2 status: This component indicates the status of the SPO2, which can fall into either a normal or abnormal category based on the heart rate range described in Section 5.3.1. 'Normal' is highlighted as green and 'Abnormal' is highlighted as red.

Table 5. RHM center patient's information.

ID	Date	Heart Rate	SPO2	Trusted Data	Heart Rate Status	SPO2 Status
1	1 May 2024	78	95	Trusted	Normal	Normal
2	1 May 2024	55	97	Trusted	Abnormal	Normal
3	1 May 2024	87	95	Trusted	Normal	Normal

Table 5. *Cont.*

ID	Date	Heart Rate	SPO2	Trusted Data	Heart Rate Status	SPO2 Status
4	1 May 2024	65	97	Trusted	Normal	Normal
5	1 May 2024	77	97	Trusted	Normal	Normal
6	1 May 2024	60	97	Trusted	Normal	Normal
7	1 May 2024	62	97	Trusted	Normal	Normal
8	1 May 2024	62	97	Trusted	Normal	Normal
9	1 May 2024	64	97	Trusted	Normal	Normal
10	1 May 2024	60	97	Trusted	Normal	Normal
11	1 May 2024	69	98	Trusted	Normal	Normal
12	1 May 2024	61	98	Trusted	Normal	Normal
13	1 May 2024	74	98	Trusted	Normal	Normal
14	1 May 2024	61	98	Trusted	Normal	Normal
15	1 May 2024	73	98	Trusted	Normal	Normal
16	1 May 2024	64	98	Trusted	Normal	Normal
17	1 May 2024	67	99	Trusted	Normal	Normal
18	1 May 2024	68	99	Trusted	Normal	Normal
19	1 May 2024	64	99	Trusted	Normal	Normal
20	1 May 2024	66	98	Trusted	Normal	Normal
21	1 May 2024	71	98	Trusted	Normal	Normal
22	1 May 2024	67	98	Trusted	Normal	Normal
23	1 May 2024	65	98	Trusted	Normal	Normal
24	1 May 2024	61	98	Trusted	Normal	Normal
25	1 May 2024	78	94	Trusted	Normal	Abnormal
26	1 May 2024	56	94	Trusted	Abnormal	Abnormal
27	1 May 2024	82	98	Trusted	Normal	Normal
28	1 May 2024	79	98	Trusted	Normal	Normal
29	1 May 2024	81	96	Trusted	Normal	Normal
30	1 May 2024	60	94	Trusted	Normal	Abnormal
31	1 May 2024	66	98	Trusted	Normal	Normal
32	1 May 2024	70	98	Trusted	Normal	Normal
33	1 May 2024	58	98	Trusted	Abnormal	Normal
34	1 May 2024	68	98	Trusted	Normal	Normal
35	1 May 2024	81	97	Trusted	Normal	Normal
36	1 May 2024	55	94	Trusted	Abnormal	Abnormal
37	1 May 2024	59	93	Untrusted	Abnormal	Abnormal
38	1 May 2024	55	94	Trusted	Abnormal	Abnormal
39	1 May 2024	69	97	Trusted	Normal	Normal
40	1 May 2024	153	93	Trusted	Abnormal	Abnormal

6.2. Detecting Tampering Attempts in the RHM System

The system detected alterations in request number 37, as illustrated in Figures 15 and 16. Consequently, the system preserved all blocks, including their previous hash and new block hash, in the database. Subsequently, during the transmission to the RHM center, a crucial stage known as the "Data Verifier" comes into play. In this stage, mapping is established between the hashes transmitted by the system and those stored in the database. If there is a match, the data is deemed "Trusted"; otherwise, it is labeled as "Untrusted". Following this, the system will seamlessly resume processing other requests without encountering conflicts arising from tampered requests.

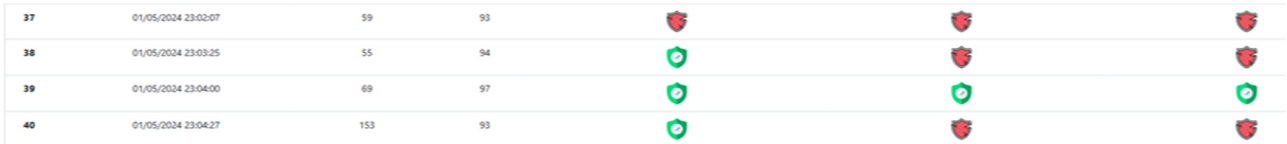


Figure 15. Illustration of detected tampering attempts by the RHM system.

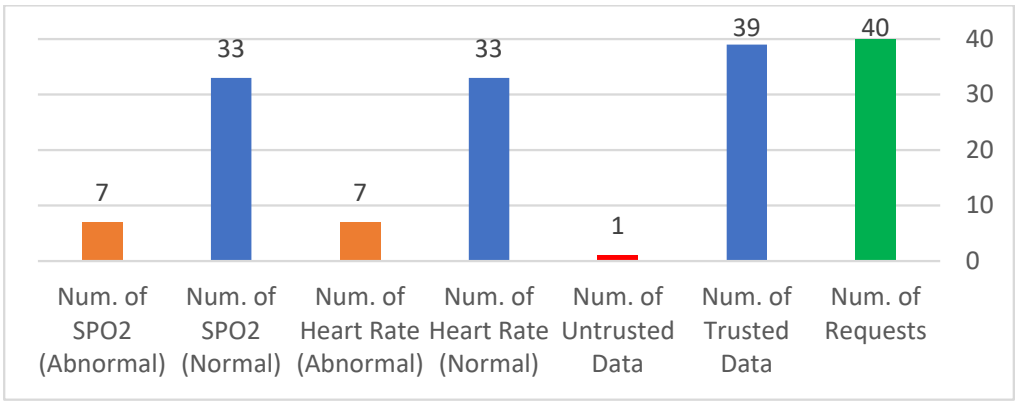


Figure 16. RHM center patient's information chart.

6.3. Data Integrity

One way to ensure data integrity is by monitoring two key metrics:

- **Step 1:** The percentage of data packets or requests received without errors.

The formula is

$$Data\ Integrity\ (\%) = (\frac{Total\ Data\ Packets - Data\ Packets\ with\ Errors}{Total\ Data\ Packets}) \times 100 \quad (7)$$

So, $Data\ Integrity(\%) = [(40-1)/40] * 100 = 97.5\%$

- **Step 2:** Number of detected data-tampering attempts.

Our system identified a single tampering attempt, which was successfully detected, as illustrated in Figure 17. These metrics provide valuable insights into the reliability and security of the data being transmitted and stored.

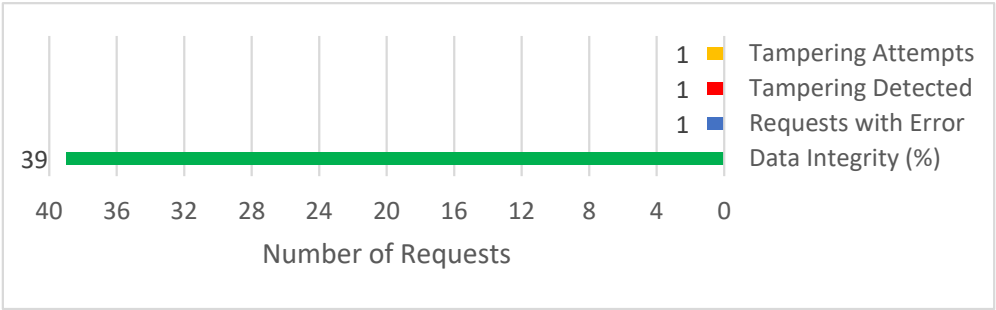


Figure 17. Data integrity analysis.

6.4. Throughput

To calculate the throughput of a system, we measured important aspects:

- Maximum data transfer rate achievable under normal conditions.

This refers to the maximum rate at which data can be transmitted or processed by the system under typical operational conditions. It can be expressed in bytes per second (Bps), or any other relevant data rate unit, as shown in Figure 18. Our system can handle more than 3000 per minute as a maximum.

Formula:

$$Throughput\ (Data\ Rate) = (\frac{Amount\ of\ data\ transferred}{Time\ duration}) \times 100 \quad (8)$$

So, *Throughput* = (40/13.553 s) = 5.95 Bps.

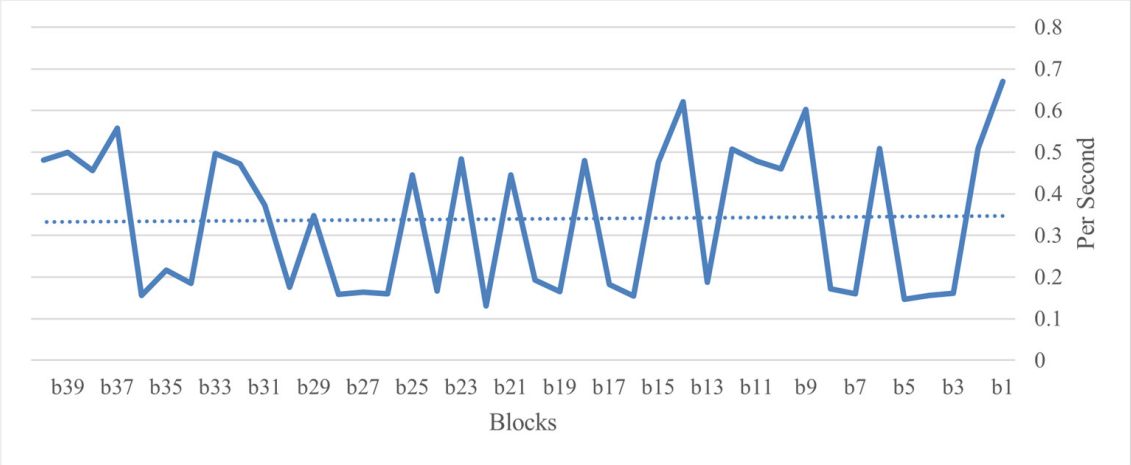


Figure 18. Transactions processed per second (s).

6.5. Latency

Latency in the context of IoT data transmission via blockchain can be calculated by considering two important factors:

- **Step 1:** Round-trip time: This is how long it takes for data packets to move from IoT devices to the blockchain network and then back to IoT devices. Alternatively, within our framework, the IoT and blockchain are considered an integrated entity, eliminating the concept of round-trip time.
- **Step 2:** Average delay due to blockchain consensus: Blockchain networks often introduce delays in transaction confirmation due to the consensus mechanisms in place.

To calculate the average delay, we measured the time it takes for transactions to be confirmed and added to the blockchain over a significant number of transactions. Then, we calculated the average delay as follows:

Formula:

$$Average\ Delay = \left(\frac{Total\ Time\ for\ Confirmation\ of\ all\ Transactions}{Number\ of\ transactions}\right) \quad (9)$$

So, *Average Delay* = (13.553 s/40) = 0.339 s.

By monitoring these latency metrics, we can assess the efficiency and responsiveness of the IoT data transmission system through the blockchain and identify any bottlenecks or delays that may need optimization.

7. Conclusions

In this paper, we aimed to ensure the integrity and privacy of RHM data transmission in the healthcare sector through the innovative application of blockchain technology and smart contracts. Through our research and implementation, we have demonstrated the potential of blockchain to fortify the integrity and privacy of RHM data. As evidenced by our findings, the metrics of data integrity at 97.5%, a throughput rate = 2.95 bytes per second, and an average delay = 0.339 s (across 40 requests) underscore the tangible improvements achieved in terms of data security and performance. Additionally, the system's capability to detect tampering within the RHM system reinforces its robustness. In closing, our research has illuminated the potential of blockchain technology to revolutionize data security within the realm of healthcare, ultimately contributing to improved patient care and a more resilient healthcare infrastructure. The journey towards secure and private RHM transmission continues, driven by innovation and a commitment to ensuring integrity and privacy in healthcare.

8. Future Work

While we have examined the limitations and challenges, it becomes essential to identify areas for improvement and expansion. The significant areas are resource optimization, privacy enhancement, and real-world implementation. Furthermore, resource optimization involves developing lightweight consensus mechanisms and efficient cryptographic algorithms to save energy consumption in the IoT.

By addressing these areas of future work, our research aims to contribute to the ongoing development of secure IoT data transmission through blockchain technology. These avenues hold promise for making IoT networks more resilient, efficient, and trustworthy, which is essential for the continued growth and adoption of the IoT in RHM.

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

Funding: This research is funded by the Deanship of Scientific Research, Islamic University of Madinah, Madinah, Saudi Arabia.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding authors.

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

References

1. Gupta, R.; Gupta, R. ABC of Internet of Things: Advancements, benefits, challenges, enablers and facilities of IoT. In Proceedings of the 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, India, 18–19 March 2016; pp. 1–5.
2. Venkatesh, D.A.N. Connecting the dots: Internet of Things and human resource management. *Am. Int. J. Res.Humanit. Arts Soc.Sci.* **2017**, *17*, 21–24.
3. Asharf, J.; Moustafa, N.; Khurshid, H.; Debie, E.; Haider, W.; Wahab, A. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. *Electronics* **2020**, *9*, 1177. [CrossRef]
4. Ioulianou, P.; Vasilakis, V.; Moscholios, I.; Logothetis, M. A Signature-Based Intrusion Detection System for the Internet of Things. Available online: https://eprints.whiterose.ac.uk/133312/ (accessed on 2 May 2024).
5. Meidan, Y.; Bohadana, M.; Shabtai, A.; Ochoa, M.; Tippenhauer, N.O.; Guarnizo, J.D.; Elovici, Y. Detection of unauthorized IoT devices using machine learning techniques. *arXiv* **2017**, arXiv:1709.04647.
6. Wang, J.; Hao, S.; Wen, R.; Zhang, B.; Zhang, L.; Hu, H.; Lu, R. IoT-praetor: Undesired behaviors detection for IoT devices. *IEEE Internet Things J.* **2020**, *8*, 927–940. [CrossRef]
7. Hussain, F.; Abbas, S.G.; Shah, G.A.; Pires, I.M.; Fayyaz, U.U.; Shahzad, F.; Garcia, N.M.; Zdravevski, E. A framework for malicious traffic detection in IoT healthcare environment. *Sensors* **2021**, *21*, 3025. [CrossRef]
8. Alshamrani, M. IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 4687–4701. [CrossRef]
9. Rashid, S.; Paul, S.P. Proposed methods of IP spoofing detection & prevention. *Int. J. Sci. Res.* **2013**, *2*, 438–444.
10. Klonoff, D.C. Continuous glucose monitoring: Roadmap for 21st century diabetes therapy. *Diabetes Care* **2005**, *28*, 1231–1239. [CrossRef]
11. Polat, H.; Polat, O.; Cetin, A. Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. *Sustainability* **2020**, *12*, 1035. [CrossRef]
12. van Amsterdam, B.; Clarkson, M.J.; Stoyanov, D. Gesture Recognition in Robotic Surgery: A Review. *IEEE Trans. Biomed. Eng.* **2021**, *68*, 2021–2035. [CrossRef]
13. Kim, M.S.; Henderson, K.A.; Van Sickle, D. Using Connected Devices to Monitor Inhaler Use in the Real World. Available online: https://propellerhealth.com/wp-content/uploads/2017/09/Kim-et-al_Using-Connected-Devices-to-Monitor-Inhaler-Use-in-the-Real-World-1.pdf (accessed on 2 May 2024).
14. Elhoseny, M.; Ramírez-González, G.; Abu-Elnasr, O.M.; Shawkat, S.A.; Arunkumar, N.; Farouk, A. Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access* **2018**, *6*, 20596–20608. [CrossRef]
15. McGhin, T.; Choo, K.-K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [CrossRef]
16. 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] [PubMed]

17. Zhang, Y.; Liu, D. Toward vulnerability detection for ethereum smart contracts using graph-matching network. *Futur. Internet* **2022**, *14*, 326. [CrossRef]
18. Yew, H.T.; Ng, M.F.; Ping, S.Z.; Chung, S.K.; Chekima, A.; Dargham, J.A. Iot based real-time remote patient monitoring system. In Proceedings of the 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), Langkawi, Malaysia, 28–29 February 2020; pp. 176–179.
19. Tham, O.Y.; Markom, M.A.; Bakar, A.H.A.; Tan, E.S.M.M.; Markom, A.M. IoT health monitoring device of oxygen saturation (SpO2) and heart rate level. In Proceedings of the 2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE), Yogyakarta, Indonesia, 13–14 October 2020; pp. 128–133.
20. Iqbal, W.; Abbas, H.; Daneshmand, M.; Rauf, B.; Bangash, Y.A. An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet Things J.* **2020**, *7*, 10250–10276. [CrossRef]
21. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef] [PubMed]
22. Srivastava, G.; Dwivedi, A.D.; Singh, R. PHANTOM protocol as the new crypto-democracy. In *Computer Information Systems and Industrial Management, Proceedings of the 17th International Conference, CISIM 2018, Olomouc, Czech Republic, 27–29 September 2018, Proceedings 17*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 499–509.
23. Gupta, D.; Rani, S.; Raza, S.; Qureshi, N.M.F.; Mansour, R.F.; Ragab, M. Security paradigm for remote health monitoring edge devices in internet of things. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 101478. [CrossRef]
24. Pirbhulal, S.; Pombo, N.; Felizardo, V.; Garcia, N.; Sodhro, A.H.; Mukhopadhyay, S.C. Towards machine learning enabled security framework for IoT-based healthcare. In Proceedings of the 2019 13th International Conference on Sensing Technology (ICST), Sydney, Australia, 2–4 December 2019; pp. 1–6.
25. Srivastava, G.; Crichigno, J.; Dhar, S. A light and secure healthcare blockchain for iot medical devices. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019; pp. 1–5.
26. Raghu, R.; Jayaraman, V.; Jayaraman, J.; Nukala, S.S.V.; Díaz, V.G. A multi-layered edge-secured cloud framework for healthcare monitoring in old-age homes using smart systems driven by comprehensive user interaction. *Int. J. Saf. Secur. Eng.* **2022**, *12*, 449–457. [CrossRef]
27. Zendehdel, G.A.; Kaur, R.; Chopra, I.; Stakhanova, N.; Scheme, E. Automated security assessment framework for wearable ble-enabled health monitoring devices. *ACM Trans. Internet Technol.* **2021**, *22*, 1–31. [CrossRef]
28. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives. *J. Food Qual.* **2021**, *2021*, 7608296. [CrossRef]
29. Wang, H.; Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352. [CrossRef]
30. Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.M.A.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *J. Netw. Comput. Appl.* **2021**, *181*, 103007. [CrossRef]
31. Pustišek, M.; Kos, A. Approaches to front-end iot application development for the ethereum blockchain. *Procedia Comput. Sci.* **2018**, *129*, 410–419. [CrossRef]
32. Panetta, K. *Gartner Top 10 Strategic Technology Trends for 2019*; Gartner: Stamford, CT, USA, 2018.
33. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
34. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Boston, MA, USA, 11–14 December 2017; pp. 557–564.
35. Katende, M. Combining mqtt and blockchain to improve data security. In Proceedings of the 3rd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Seoul, Republic of Korea, 13 July 2020.
36. Aborokbah, M.M.; Al-Mutairi, S.; Sangaiah, A.K.; Samuel, O.W. Adaptive context aware decision computing paradigm for intensive health care delivery in smart cities—A case analysis. *Sustain. Cities Soc.* **2018**, *41*, 919–924. [CrossRef]
37. Kizza, J.M.; Kizza, J.M. Internet of Things (IoT): Growth, challenges, and security. In *Guide to Computer Network Security*; Springer International Publishing: Cham, Germany, 2020; pp. 517–531.
38. Górski, T. Towards Continuous Deployment for Blockchain. *Appl. Sci.* **2021**, *11*, 11745. [CrossRef]
39. Virani, S.S.; Alonso, A.; Aparicio, H.J.; Benjamin, E.J.; Bittencourt, M.S.; Callaway, C.W.; Carson, A.P.; Chamberlain, A.M.; Cheng, S.; Delling, F.N.; et al. Heart disease and stroke statistics-2021 update: A report from the American Heart Association. *Circulation* **2021**, *143*, e254–e743.
40. Poorzargar, K.; Pham, C.; Ariaratnam, J.; Lee, K.; Parotto, M.; Englesakis, M.; Nagappa, M. Accuracy of pulse oximeters in measuring oxygen saturation in patients with poor peripheral perfusion: A systematic review. *J. Clin. Monit. Comput.* **2022**, *36*, 961–973. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.