Journal of Information Technology and Digital World (ISSN: 2582-418X)
www.irojournals.com/itdw/

Blockchain-Powered Secure Communication Protocol for the Internet of Medical Things (IoMT)

Dinesh Kumar M[1], N. Santhiyakumari[2]

[1]Assistant Professor, Electronics and Communication Engineering, Knowledge Institute of Technology, Salem, Tamil Nadu, India

[2]Professor, Electronics and Communication Engineering. Knowledge Institute of Technology, Salem, Tamil Nadu, India

E-mail: [1]mdece@kiot.ac.in, [2]dirrd@kiot.ac.in

Abstract

The Internet of Medical Things (IoMT) through network technology provides smart medical devices, equipment, and software to connect different patients and users with medical information. Integrating Blockchain technology into IoMT-based healthcare IoT solutions increases security and privacy. Blockchain's decentralized architecture ensures data integrity, confidentiality, and traceability of patient information throughout its entire lifecycle. It solves deficiencies in data storage, transmission, and computation in the IoT ecosystem by using encryption technology and smart contracts. This integration provides real-world benefits such as creating tamper-proof documents and building trust between patients and doctors. The research helps improve the security of healthcare systems and highlights the important role of Blockchain in protecting sensitive medical data in the IoT environment.

Keywords: Blockchain technology, Internet of Medical Things (IoMT), Health monitoring systems, Data security, Privacy protection, Cryptographic techniques, Smart contracts, Healthcare data management

DOI: https://doi.org/10.36548/jitdw.2024.2.005
Received: 13.04.2024. received in revised form: 02.05.2024, accepted: 15.05.2024, published: 29.05.2024

1. Introduction

The research presented here describes a new technology that enhances the security and privacy of IoT-based healthcare by collaborating with Blockchain technology. The system collects patient health data over time using a variety of IoMT devices, including heart rate sensors, temperature sensors, air quality sensors, and humidity sensors [3]. Using these IoMT devices, the system can monitor various vital signs and health variables, laying the foundation for effective treatment. An important part of the planning process is the use of Blockchain technology to securely store and process received medical information. The technology ensures the integrity, confidentiality and traceability of patient information by creating an integrated Blockchain network. This new concept not only improves information security, but also increases trust and openness in the processing of sensitive medical information[5-10]. The operation of the system is based on the creation of a secure and reliable communication protocol that ensures interaction between IoT devices and Blockchain networks. The system provides instant analysis of health metrics, allowing doctors to quickly identify and respond to gaps in patient data. In addition, the agreement emphasizes patient privacy and ensures that health information is protected throughout the data transfer process. Additionally, Blockchain technology improves the scalability and interoperability of IoT-based healthcare services, enabling better collaboration and information sharing among healthcare stakeholders. This collaboration not only improves health, but also stimulates new treatments and research. In summary, this article presents a general framework that combines IoT and Blockchain technology to create a secure, reliable, and privacy-preserving environment for healthcare. By leveraging the power of both technologies, the proposed system will take a significant step in solving the changing problems of managing medical information and patient privacy in the era of medical IoT [11-16].

2. Literature Survey

This work introduces the development of the rich thin client architecture ERTCA to solve the limitations of IoT devices. ERTCA optimizes resources by distributing tasks efficiently to avoid collisions due to overload. It improves IoT-Blockchain connectivity by connecting high-performance initial nodes to the Blockchain, allowing other nodes to benefit from overload. Node classifications include power and storage. The performance of ERTCA is

evaluated and compared with hierarchical models. Ethereum-based private Blockchain is also being evaluated. The design model includes collaborative health management, improved efficiency, resource utilization, data privacy, and system security. Additionally, the study demonstrates the advantages of a private Blockchain system for public collaboration, including factors such as cost and efficiency. [1]

The BFT-PNT protocol assumes that a trusted client can resolve handshake conflict and prioritize the update process. The market is regulated by the customer and each exchange has a government agreement. The data is stored separately to ensure their confidentiality and immutability. Optimization is applied to the existing BFT system, especially in the context of electronic medical records EHR and medical records. The concept provides semantics to distinguish between two types of operations. These considerations are based on the characteristics of medical records: temporary-easy insertion and use that does not disrupt data. The integrity of the resource is attributed to the supplier. Additionally, the applicability of the process is verified in conflicting cases using the Ed25519 signature and SHA-256 fingerprint standard used in Xtend/Java. This approach expands EHR's capabilities, improving consistency, availability and data protection. [2]

In this work multiple healthcare providers are collaborating on a unified system of electronic health records (EHR) and Blockchain technology. The process begins with the identification of the patient's EHR by the HC clinic after a physical examination. The doctor then creates the electronic medical record EMR following the diagnosis. Patients are equipped with body sensor networks and IoT systems to collect physical data, create personal health records (PHRs) and send them via mobile devices. This personal information is compiled in the APHR Personal Health Information Form. The aggregation process involves transferring EHRs, EMRs, and PHRs to the Blockchain network. Additionally, participants are involved in shared authentication, generating shared keys, and decrypting the patient's APHR. Although there are security issues, this proposed process also aims to contribute to addressing threats and operational needs.

In this study, the Ethereum Blockchain platform was used to develop electronic health services. Similar to Bitcoin, Ethereum operates as a decentralized Blockchain network, but its adaptability and flexibility make it ideal for many applications, including e-health. The main

components of the Ethereum network include the Blockchain, which contains transaction information and smart contracts. These blocks are verified and expanded by miners using proof of work, thus ensuring the security and transparency of network nodes. Each block references the hash of the previous block and ensures that no changes are made. This study identifies key problems in current EHR integration and provides effective solutions using a model. While security monitoring evaluates the physical potential for threats, a smart contract manages users to ensure the security of the shared EHR. The Ethereum Blockchain is deployed on the Amazon cloud and integrated with peer-to-peer IPFS storage to enable data storage and sharing. The results show that this framework has the ability to trust and share medical information in the cloud environment faster than traditional methods. [4]

3. Existing System

Many hospitals and other healthcare organizations are transitioning from paper technology to electronic health records (EHR). This change is possible thanks to the advancement of technology. Parties should share information stored by each other, and users should be allowed to control who has access to stored information. EVERY electronic health record suffers from management issues, trust issues, and data protection issues. Information stored on the Blockchain is immutable, private and accessible only to intended users. The use of Blockchain technology has also led to managing systems that can provide information storage in a distributed manner. However, concerns about data security, privacy and trust have become major obstacles to the use of this technology. The system offers a new solution for safe and transparent healthcare services using Blockchain technology. Blockchain is a record of private information and evidence used to solve privacy and security issues related to health information. Using this Blockchain-based healthcare system has the potential to revolutionize healthcare by providing a secure, transparent and patient-focused way to manage medical information. This system will raise privacy concerns because people will have no control over their information once it is entered into the Blockchain. It is resource heavy and may not scale well to manage the large amounts of medical information generated by people and equipment. Storing information on Blockchain can be expensive, especially when there is a large amount of health information.

4. Methodology

The combination of Blockchain technology and IoT is paving the way for advancements in healthcare. The system offers a new aspect of real-time health monitoring, involving various IoT devices, including heart rate sensors, body temperature sensors, ambient temperature and humidity sensors, air quality sensors, LCD display, and buzzer. The system plans to use Blockchain technology to ensure the security, integrity and availability of information. This Blockchain-based healthcare system can now take care of important health issues, making it useful for doctors, caregivers, and people as well. Heart rate and body temperature sensors capture data in real time and send it to a secure Blockchain network. Environmental sensors monitor the environment for health and comfort. If a measurement exceeds a preset threshold, the system triggers an alarm through a combination of LCD display and buzzer.

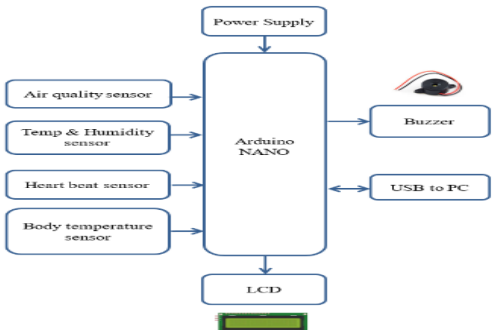

Figure 4.1. IoMT Module

Blockchain technology ensures the security and confidentiality of patient information. Each document is cryptographically locked into a block and linked to the previous block in the chain, creating an immutable and transparent health information system. Access to this information is limited and only authorized users, such as doctors and patients, are allowed access. Point-of-care monitoring allows doctors to monitor patient health indicators and respond quickly to any abnormalities, improving the quality of care and ensuring timely impact. Additionally, the system facilitates the exchange of health information between different healthcare providers, increasing continuity of care and reducing the complexity of testing. The system offers a new aspect of real-time health monitoring, involving various IoT devices, including heart rate sensors, body temperature sensors, ambient temperature and humidity sensors, air quality sensors, LCD display and buzzer. The system plans to use Blockchain

technology to ensure the security, integrity, and availability of information. This Blockchain-based healthcare system can now take care of important health issues, making it useful for doctors, caregivers, and people as well. Heart rate and body temperature sensors capture data in real time and send it to a secure Blockchain network. Blockchain technology ensures the security and confidentiality of patient information. Point-of-care monitoring allows doctors to monitor patient health indicators and respond quickly to any abnormalities, improving the quality of care and ensuring timely impact.

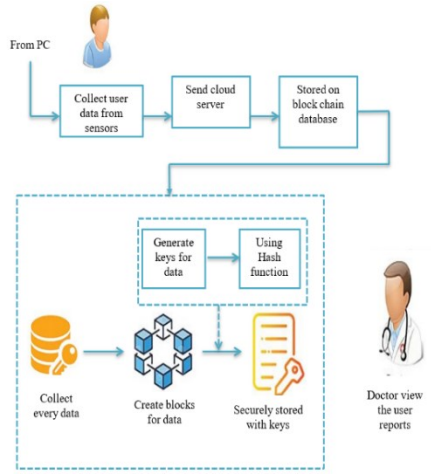

Figure 4.2. Block of Diagram of Software

4.1. User Interface

When designing and building user interfaces (UIs), many tools and libraries are available to improve the design process and increase the efficiency and functionality of the final web application. Below is a description of some of the tools and libraries used. It provides the basic structure of the website, enhanced and modified by other technologies such as CSS and JavaScript. It controls the appearance of HTML content using various properties such as color, font, spacing, and position. It includes predefined objects and utility classes that make it easy to create the best user interfaces. It allows developers to create dynamic content, control multimedia, animated images and more.

4.1.1. Admin Module

This module allows administrators to manage user accounts, including registration, authentication, and access control. Admins can register and manage IoT devices used for health monitoring. This includes associating devices with users and ensuring their proper functioning.

The admin module oversees the configuration and maintenance of the blockchain network, setting up smart contracts, and ensuring network integrity and security. Admins set access permissions and roles for users and doctors, determining what data they can view and manage.

4.1.2 User Module

Users can create accounts and provide their personal information. This data is securely stored on the Blockchain. Users can connect their IoT health monitoring devices to their accounts through a secure pairing process. Users can access real-time health data, such as heart rate, body temperature and other vital signs through IoT sensors. Users may grant permission to doctors or family members to access their health data, providing transparency and control over data sharing.

4.1.3 Doctor Module

Doctors can access patient records, including real-time health data and medical history stored on the Blockchain. This enables accurate diagnosis and treatment decisions. This module ensures secure and private communication between doctors and patients for consultations and follow-up. Doctors can utilize analytics tools to interpret data trends and provide more informed medical advice.

4.2 List of Component

Table 1. List of Components

S.No	Name of the component	Usage
1.	Heart beat sensor	To monitor the heart beat
2.	Body temperature	To measure the heat/cold
3.	Humidity sensor	Monitor the temperature and humidity of the environment
4.	Air Quality sensor	Measure a variety of environmental factors
5.	LCD	To display the information
6.	Buzzers	Used to provide alerts

4.3 Technical Stack

This research uses a robust framework and design to increase security and privacy by integrating Blockchain technology with Internet of Medical Things (IoMT) systems. This cloud database uses MongoDB and PostgreSQL to manage data and processes, is hosted on platforms like AWS and Google Cloud Platform (GCP), and uses encryptions like AES-256 (for legacy data) and TLS 1.2/1.3 (for static). Data) technology. File transfer). The Blockchain component includes Ethereum's permission platforms like Solidity and Hyperledger Fabric, as well as Hyperledger Fabric's Go/JavaScript and practical Byzantine Fault Tolerance (pBFT), Proof of Authorization (POA), etc. It is based on the private Ethereum network, using which smart contracts are created and a consensus mechanism is implemented. Integrate with IoMT secure communication tools like MQTT and CoAP, and integrate with external data through RESTful APIs and middleware like Oracle. Implementation strategies include creating a cloud environment and appropriate security measures, using Blockchain networks and smart contracts, integrating IoMT tools to complete data distribution and storage, and using tools such as Jenkins to create integration and continuous delivery (CI/CD).) pipelines and GitLab CI/CD. Performance monitoring for Prometheus and Grafana provides monitoring and control, as well as solutions and security to improve the integrity, confidentiality, and tracking of clean health data in the IoMT ecosystem.

5. Advantages

Patients and healthcare providers can trust the integrity of the information, reducing errors and misunderstandings. Patients have greater control over their data, granting permission for specific individuals or organizations to access their health information, enhancing privacy. This system ensures that data from different IoT devices and sources can be seamlessly integrated and accessed in real-time. IoT devices continuously collect and transmit data, enabling real-time health monitoring. This allows for early detection of health issues and faster responses to critical situations, potentially saving lives.

6. Result

The smart health system used in this research consists of an electronic sensor that can understand the user's condition, a control unit that can control it, and a monitoring system that can be controlled from the web application. The user's health status is stored in a secure Blockchain. The hardware configuration is shown in the image above. This setup includes important components and sensors such as Arduino NANO, heart rate sensor, body temperature sensor, ambient humidity and temperature sensor, air quality sensor, LCD and buzzer. These sensors and components are controlled by Arduino NANO.

Heartbeat Sensor: The heartbeat sensor emits infrared light into the skin. When blood pulses through the finger or another part of the body, it changes the amount of light absorbed by the photo detector in the sensor. It usually works by emitting light into the skin and measuring the light that reflects back due to blood flow. Changes in blood volume during each heartbeat create variations in the reflected light, allowing the sensor to calculate the heartbeat rate.

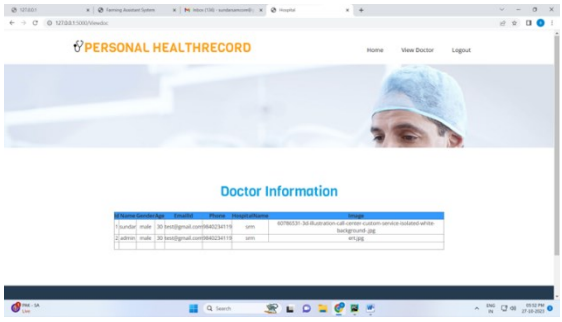

Figure 6.1. Doctor Information

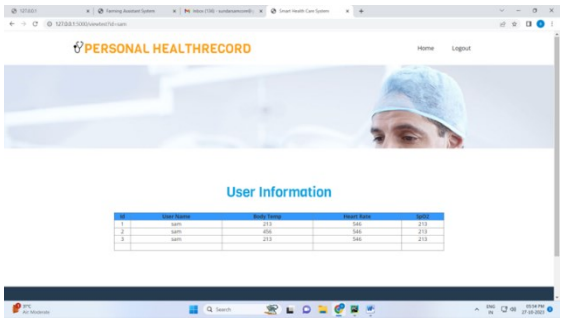

Figure 6.2. Data Collected from User

Body Temperature Sensor: Temperature sensors measure temperature based on the change in electrical resistance with temperature. Thermistors' resistance changes significantly with temperature, while digital sensors provide a digital signal corresponding to the temperature.

Environment Humidity and Temperature Sensor: These sensors use capacitive sensing to measure humidity. The sensor has a capacitor that changes its capacitance based on the humidity of the surrounding air. Temperature is measured using a thermistor inside the sensor, similar to the body temperature sensor.

Air Quality Sensor: Air quality sensor detects PM2.5 and PM10, carbon dioxide CO2, volatile organic compounds VOC etc. It can detect various pollutants in the air, such as It provides an air quality indicator that indicates whether the air is safe to breathe. Sensors react to gases or specific substances and provide measurement of the air quality index AQI.

LCD Screen: LCD screen is used to display real-time information such as heart rate, body temperature, humidity, temperature and air quality. Provide a user-friendly interface to view information.

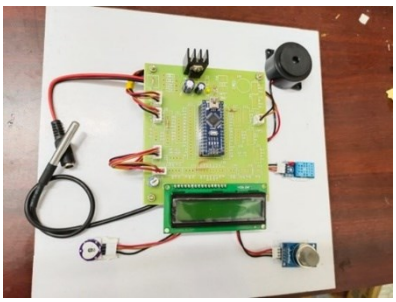

Figure 6.3. Hardware Setup

Buzzer: A buzzer can be used as an alert system. This can sound an alarm if abnormal readings are detected, ensuring timely attention to the user's health status.

7. Conclusion

Integrating Blockchain technology into on-site healthcare using IoT has the potential to revolutionize healthcare in many aspects. This new combination provides a secure, transparent and effective way to manage health information, improve patient care and advance medical

research. First of all, the use of Blockchain ensures the security and confidentiality of information. Provides tamper-proof certificates so patients can control their health information and allow access only to authorized individuals; This is important for protecting medical records. This empowers patients and encourages them to participate in medical decisions.

Additionally, real-time health monitoring of IoT devices enables continuous data collection and instant transmission to healthcare providers. This means emergency situations can be addressed in a timely manner or chronic conditions can be better managed. Doctors and caregivers can monitor patients' conditions remotely, reducing the need for frequent hospital visits and potentially reducing healthcare costs. Blockchain also facilitates collaboration between various medical systems and devices, allowing for better collaboration between different healthcare providers and improving overall care. It can also facilitate medical research and encourage innovation in the field by providing a safe and transparent sharing platform.

Reference

[1] Bataineh, Marah R., Wail Mardini, Yaser M. Khamayseh, and Muneer Masadeh Bani Yassein. "Novel and secure blockchain framework for health applications in IoT." IEEE Access 10 (2022): 14914-14926.

[2] Pedrosa, Micael, Rui Lebre, and Carlos Costa. "A performant protocol for distributed health records databases." IEEE Access 9 (2021): 125930-125940.

[3] Li, Chun-Ta, Dong-Her Shih, Chun-Cheng Wang, Chin-Ling Chen, and Cheng-Chi Lee. "A blockchain based data aggregation and group authentication scheme for electronic medical system." IEEE Access 8 (2020): 173904-173917.

[4] Nguyen, Dinh C., Pubudu N. Pathirana, Ming Ding, and Aruna Seneviratne. "Blockchain for secure ehrs sharing of mobile cloud based e-health systems." IEEE access 7 (2019): 66792-66806.

[5] Ying, Zuobin, Lu Wei, Qi Li, Ximeng Liu, and Jie Cui. "A lightweight policy preserving EHR sharing scheme in the cloud." IEEE Access 6 (2018): 53698-53708.

[6] L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, ‘‘Blockchain for managing heterogeneous Internet of Things: A perspective architecture,’’ IEEE Netw., vol. 34, no. 1, pp. 16–23, Jan. 2020.

[7] C.-T. Li, T.-Y. Wu, and C.-M. Chen, ‘‘A provably secure group key agreement scheme with privacy preservation for online social networks using extended chaotic maps,’’ IEEE Access, vol. 6, pp. 66742–66753, 2018.

[8] M. Samaniego and R. Deters, ‘‘Internet of smart Things–IoST: Using Blockchain and CLIPS to make things autonomous,’’ in Proc. IEEE Int. Conf. Cognit. Comput. ICCC, Jun. 2017, pp. 9–16.

[9] L. A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, ‘‘Mobile cloud computing model and big data analysis for healthcare applications,’’ IEEE Access, vol. 4, pp. 6171–6180, 2016.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Achieving secure, scalable, and fine-grained data access control in cloud computing,’’ in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.

[11] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, ‘‘The Internet of Things for health care: A comprehensive survey,’’ IEEE Access, vol. 3, pp. 678–708, Jun. 2015.

[12] Bahga and V. K. Madisetti, ‘‘A cloud-based approach for interoperable electronic health records EHRs,’’ IEEE J. Biomed. Health Inform., Vol. 17, no. 5, pp. 894–906, Sep. 2013.

[13] M. Meingast, T. Roosta, and S. Sastry, ‘‘Security and privacy issues with health care information technology,’’ in Proc. Int. Conf. IEEE Eng. Med. Biol. Soc., Aug./Sep. 2006, pp. 5453–5458.

[14] Ibrahim, B. Mahmood, and M. Singhal, ‘‘A secure framework for sharing electronic health records over clouds,’’ in Proc. IEEE Serious Games Appl. Health, May 2016, pp. 1–8.

[15] N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, ‘‘Towards using Blockchain technology for eHealth data access management,’’ in Proc. IEEE 4th Int. Conf. Adv. Biomed. Eng., Oct. 2017, pp. 1–4.

[16] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, ‘‘Smart contractbased access control for the Internet of Things,’’ IEEE Internet Things J.,vol. 6, no. 2, pp. 1594–1605, Apr. 2019.