ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 2(05), May 2023, pp. 17-25

Article Title: **A Blockchain Framework of Improved Security for Internet of Things Health Applications**

A Blockchain Framework of Improved Security for Internet of Things Health Applications

Roshni V Jose[1], Siva Prasad Mannivannan I.[2]

[1]PG Student, Department of Computer Science and Engineering, Rohini College of Engineering and Technology, Kanyakumari, India, v.roshnijose@gmail.com

[2]Assistant Professor, Department of Computer Science and Engineering, Rohini College of Engineering and Technology, Kanyakumari, India, sivaprasad.84@hotmail.com

ABSTRACT

The design and development of the Internet of Things (IoT) have a remarkable advancements in recent years. An "Internet of Things" (IoT) is a term used to describe an interconnection of physical objects with a network that incorporates software, sensors, and other devices to exchange information. Because patient health records (PHR) are valuable and significant, security is the most crucial component of encryption over the Internet. Sensitive data is typically secured by a third party during transmission in an IoT setting, which leads to complex and sometimes deadly problems. To address security issues and do away with third parties' involvement in an IoT environment, blockchain technology is the modern solution. The idea of a secure blockchain for Internet of Things (IoT) health applications is presented in this paper. Electronic health records (EHRs), which are used to deliver healthcare directly to patients while reducing physical contact between patients and healthcare providers, are the health information that is collected and saved electronically for educational purposes in today's healthcare. Decision makers can enhance the healthcare industry and gain from the current e-government cloud computing infrastructure by using the provided framework. As a result, the proposed Blockchain work enhances the dependability of IoT systems. It also has the potential to reduce costs and boost efficiency.

Keywords: Patient health records, electronic health records, Internet of things, e-government cloud computing.

1 Introduction

Virtually every part of life in the twenty-first century have been impacted by the rapid progress in numerous technical disciplines. Numerous examples exist of how technologies collects data and embeds it in different formats for use in different uses [1]. Smart devices, such smartphones and tablets, can be used to track many health metrics, including blood pressure, heart rate, steps implemented, and calories burned. This illustration, along with a number of other sensor- and communication-related use cases, gave rise to a concept of the IoT. There have been enormous improvements in the medical field, just two examples of which include the ability to predict diseases and follow patients for particular diseases based on symptoms collected from a range of IoT devices [2-5]. The medical industry is getting used to cloud

technologies and has been using it to make health care more accessible and cost-effective because to the rising benefits of digital transmission through IoT. Packages with patient health information can now be sent to a doctor or hospital personnel from all over the world to modern wireless technologies [6]. Sensitive data, such as patient history data, are encrypted using the most fundamental and important cryptographic method. It is believed that the platform for sending and receiving patient health records is the digital healthcare system. However, due to a lack of encryption and access control technologies, the bulk of current healthcare systems are not sufficiently secure. The sharing of medical data with authorised users is an essential part of providing good healthcare [7-9]. Recently, business assistants from a number of industries, including healthcare, real estate, administration, and financial services, have become curious about blockchain technology. The advancement of blockchain technology and its numerous applications in the healthcare industry [10]. Furthermore, data on improved operations, access to patient records, and health records will be gathered as a result of the use of blockchain in healthcare. Additionally, both the transmitter and recipient may regularly update the distribution of drugs using IoT frameworks linked to locations where their excess stock moves from one place to another [11-12]. The main aim is to find multimedia data processing in an IoT healthcare ecosystem to safeguard health care management programmes by gathering each person's daily occupation. [13-14].Healthcare organisations' adoption of blockchain technology has also helped society in a number of ways, including by protecting the privacy and accountability of patient data and allowing patients the right to decide who has significant access to it [15].

For IoT applications in the healthcare industry, a new, safe Blockchain Foundation is presented in this study. More and more people are paying attention to the blockchain method, which has had great success with crypto currencies. The proposed system provides a high level of EHR integration, compatibility, and sharing between patients and medical professionals of healthcare providers. So, the proposed Blockchain work improves the efficiency and stability of IoT systems.

2 Proposed Methodology

The limitations of IoT devices are addressed by the suggested system's Enhanced Rich-Thin-Client Architecture (ERTCA). For customers with money, it provides an IoT solution based on Blockchain. The research objectives for the constrained IoT and the centralised architecture challenge are met by the ERTCA design. The Enhanced Rich Thin Clients Architecture (ERTCA) is designed in opposition to the hierarchical architecture. The thin clients associated with one particular rich client create a star topology. A collaborative monitoring of health system is developed by successfully managing health activities through combination of Blockchain and IoT, which provides data immutability and ensures that business logic is maintained.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 2(05), May 2023, pp. 17-25

Prior to outsourcing, it is a good idea to encrypt PHRs to guarantee that patients maintain control over who has access to their records. In this paper, a novel patient centred paradigm and a number of techniques for restricting access to PHRs kept on servers with a certain level of trust are proposed. Each patient's PHR file is encrypted with attribute based encryption (ABE) methods in order to achieve granular and scalable data access control. It is crucial to implement fine grained data access control strategies that interact with semi trusted servers to provide patient centric privacy management of their own PHRs.

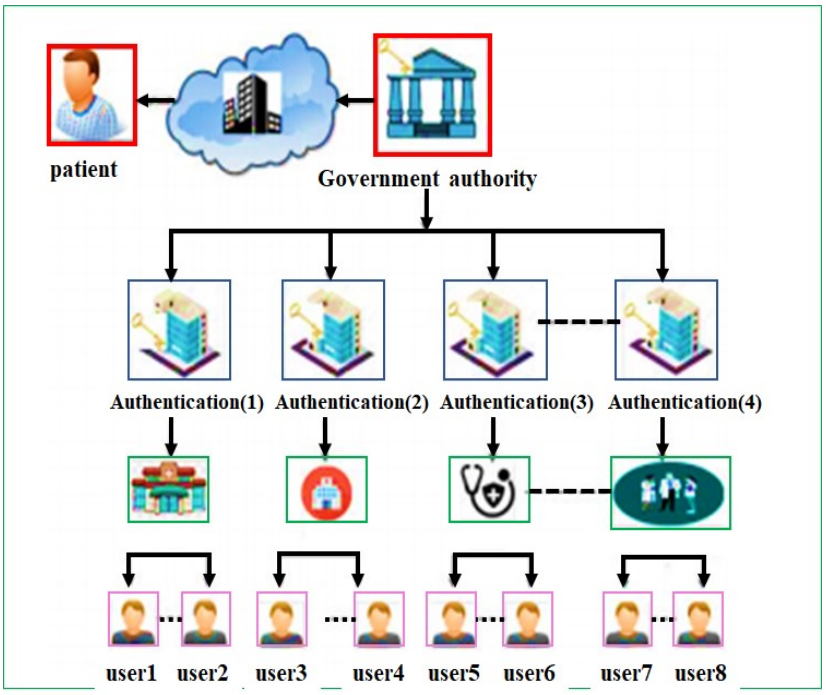

Figure 1: *Block diagram for the proposed work*

The private health information saved on a server that is only partially recognised is protected using this method using attribute-based encryption (ABE) as the primary encryption primitive. Access controls are expressed using ABE based on the characteristics of users or data, so by encryption file with a specific set of attributes, a patient can share her PHR with a certain group of users without having to be connected to the entire list of users.

2.1 Modules

2.1.1 Health Care Providers

Healthcare providers are those that arrange all types of healthcare services for every community member. Doctors, nurses, chemists, surgeons, medical technicians, lab personnel, and other staff members make up the group of people who work in healthcare.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 2(05), May 2023, pp. 17-25

2.1.2 Trusted Authority

The following actions are covered under the trusted authority's (TU) control, which must be the Ministry of Health or another government agency: Identify each user who interacts with the system by checking their information. Create keys for medical professionals and make political variables accessible to cryptography activity.

2.1.3 Patient and Service Providers Identity Proofing

Users must register with the recognized medical organization as patients and service providers prior to utilising the portal for the first time. Aspirants use a restricted web portal with access dependent on the end user's privileges to send, update, and receive medical information from the e-government cloud's central databases.

2.1.4 Proposed Access Control

The patient uploads their EHR to the cloud in accordance with the access specifications outlined by each service provider in accordance with their domains and classifications. Hierarchical organization then begins. THA encrypts the patient's electronic health record (EHR), includes it in designated policies, and gives out various decryption keys to the appropriate service providers. The features associated with the decryption key and the access pattern of the encrypted file must match for the file to be unlocked when a healthcare service provider acquires an encrypted EHR.

2.1.5 Data Distribution

It is unacceptable for the trusted central authority to separately encrypt the EHR for each user given the complexity of the EHR database and the quantity of users with different levels of access privileges. The EHR should still be encrypted just once before being distributed to different attribute authorities (AAs), according to each AA's roles.

2.1.6 Access Structure of EHRS

The suggested access structure has a lightweight key management system that eases the strain on the GA as one of its main benefits. When it comes to encrypting the EHR, creating decryption keys, and distributing them to authorized users are significant functions.

2.2 Block Chain

Blockchain are distributed public ledgers that are digitalized, decentralized, and serve as a single, synchronized database for tracking Cryptocurrency transactions. The fact that block chains are fundamentally decentralized databases means that there is no single owner of the data. To ensure that identical copies of the data are received and continuously updated, users interact to decide which data are added to the blockchain. In any setting, e-hospital generates a variety of complex and rich data, from private patient information to operational analytics.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 2(05), May 2023, pp. 17-25

Article Title: A Blockchain Framework of Improved Security for Internet of Things Health Applications

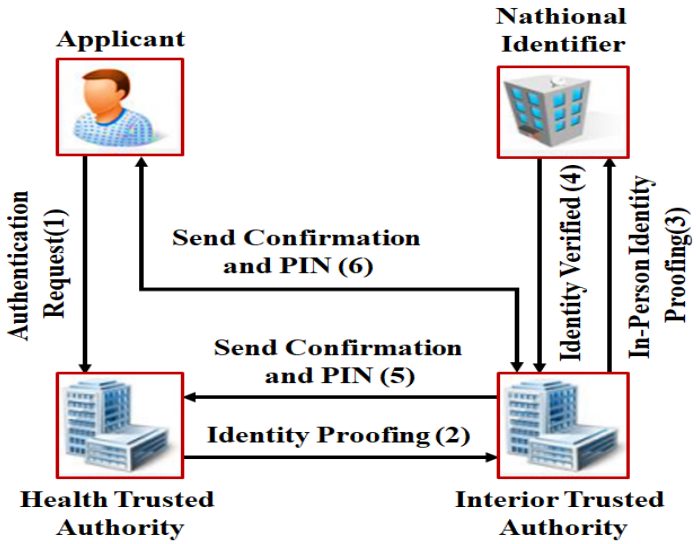

Figure 2: *Flow diagram*

3 Results and Discussion

The figures below reflect the methods used to demonstrate user login, patient registration, doctor login, nurse login, and patient details. The proposed Blockchain approach hence increases both the effectiveness and stability of IoT devices.

Figure 3: *User login*

As shown in Figure 3, a logon needs the user to have both a user ID and a password.

Figure 4 illustrates patient registration. Medical professionals gather patient information prior to their hospital stay using a hospital patient registration form. This includes a summary of medical history, information about insurance policies, a list of prescription drugs, and a list of food allergies.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 2(05), May 2023, pp. 17-25

Article Title: A Blockchain Framework of Improved Security for Internet of Things Health Applications

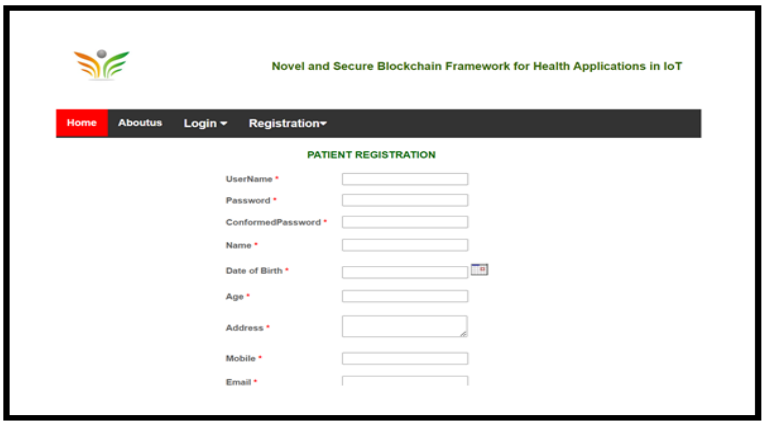

Figure 4: *Patient registration*

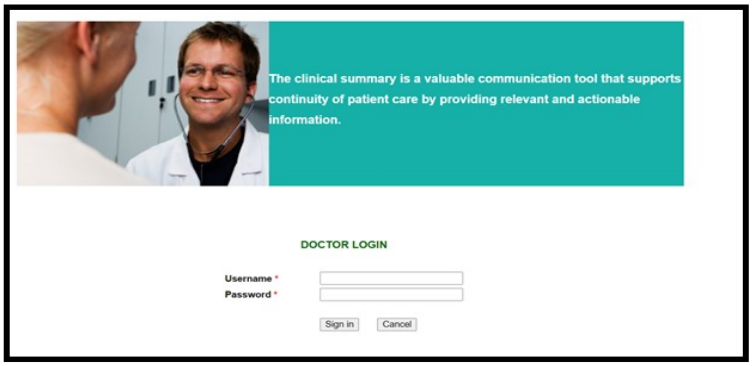

Figure 5: *Doctor Login*

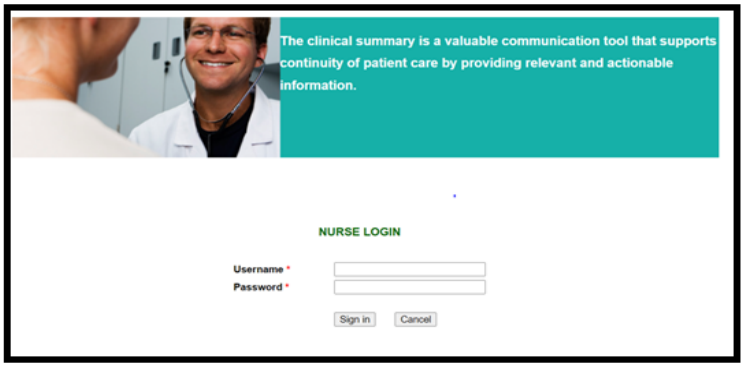

Figure 6: *Nurse Login*

The login screens for nurses and doctors are shown in Figures 5 and 6. The login systems have evaluated when the username and password are signed, as seen in the figure.

According to figure 7, the patient's information includes their user ID, user name, date of birth, age, mobile number, and email address.

Figure 7: *Patients details*

4 Conclusion

In this paper, a new, safe Blockchain Foundation is developed, which will be used by Internet of Things applications in the healthcare industry. As a result of its tremendous success with crypto currencies, blockchain technology is gaining more and more attention. The suggested solution offers a high level of EHR integration, interoperability, and sharing between practitioners and clients of healthcare providers. Any government that offers treatment services to the majority of its constituents' patients and has a cloud computing infrastructure adopts the suggested plan. Future development will involve putting the Blockchain framework's encryption and decryption procedures to the test. The government authority also doesn't perform any computational work, and multifactor applicant authentication has been established and proven. A readable message is rendered unreadable in this paper so that it cannot be read by unauthorized parties. Once a communication has been encrypted, a decryption process is developed to return it to its original (readable) format. The suggested Blockchain work improves the reliability of IoT systems as a result, and it also has the potential to save costs and increase efficiency.

References

1. Khan Minhaj Ahmad; Khaled Salah, Year: 2018, “IoT security: Review, blockchain solutions, and open challenges,” Future Gener. Comput. Syst., Vol: 82, pp. 395–411.

2. Hakak Saqib; Wazir Zada Khan; Gulshan Amin Gilkar; Muhammad Imran; Nadra Guizani, Year: 2020, “Securing smart cities through blockchain technology: Architecture, requirements, and challenges,” IEEE Netw., Vol: 34, no: 1, pp. 8–14.

3. Arul Rajakumar; Yasser D. Al-Otaibi; Waleed S. Alnumay; Usman Tariq; Umar Shoaib; MD Jalil Piran, "Multi-modal secure healthcare data dissemination framework using blockchain in IoMT", Pers Ubiquitous Comput., pp. 1–13.

4. Rajput Ahmed Raza; Qianmu Li; Milad Taleby Ahvanooey, Year: 2021, "A blockchain-based 1614 secret-data sharing framework for personal health records in emer- 1615 gency condition", Healthcare, Vol: 9, no: 2, pp. 206.

5. Kishori Kasat; D. Leela Rani; Bhola Khan; Ashok. J. d; M.K. Kirubakaran; P. Malathi, Year: 2022, "A novel security framework for healthcare data through IOT sensors", Measurement: Sensors, Vol: 24, pp. 01-05.

6. Park Eunil; Yongwoo Cho; Jinyoung Han; Sang Jib Kwon, Year: 2017, "Comprehensive approaches to user acceptance of Internet of Things in a smart home environment," IEEE Internet of Things Journal, Vol: 4, no: 6, pp. 2342–2350.

7. Ali Aitizaz; Mohammed Amin Almaiah; Fahima Hajjej; Muhammad Fermi Pasha; Ong Huey Fang; Rahim Khan; Jason Teo and Muhammad Zakarya, Year: 2022, "An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network", Sensors, Vol: 22, no: 2, pp. 572.

8. Huh Seyoung; Sangrae Cho; Soohyung Kim, Year: 2017, "Managing IoT devices using blockchain platform", In 2017 IEEE 19th international conference on advanced communication technology (ICACT), pp. 464-467.

9. Liang Xueping; Sachin Shetty; Deepak Tosh; Daniel Bowden; Laurent Njilla and Charles Kamhoua, Year: 2018, "Towards blockchain empowered trusted and accountable data sharing and collaboration in mobile healthcare applications", EAI Endor Trans Pervas Health Technol, Vol: 4, no: 15.

10. Taloba Ahmed I.; Ahmed Elhadad; Alanazi Rayan; Rasha M. Abd El-Aziz; Mostafa Salem; Ahmad A. Alzahrani; Fahd S. Alharithi; Choonkil Park, Year: 2023, "A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare", Alexandria Engineering Journal, Vol: 65, pp. 263-274.

11. Guan Zhitao; Zefang Lv; Xiaojiang Du; Longfei Wu; Mohsen Guizani, Year: 2021, "Achieving data utility-privacy tradeoff in Internet of medical things: A machine learning approach", Future Gener. Comput. Syst., Vol: 98, pp. 60–68.

12. Disha Kalbhor; Vaibhav Deshpande; Saishree Gole; Shubham Deshmukh; Umesh Nanavare, Year: 2021, "Secure E-Healthcare System Using Block chain Technology", International Journal of Scientific Development and Research, Vol: 06, no: 06, pp. 164-167.

13. Priyanka B. Dongre; Pushpneel Verma, Year: 2021, "Towards Implementation of IOTDMS Blockchain Framework for Secure Data Sharing Among IoT Devices", International Journal of Innovative Research In Technology, Vol: 07, no: 11, pp. 645-657.

14. Novo Oscar, Year: 2018, "Blockchain meets iot: An architecture for scalable access management in iot", IEEE Internet of Things Journal, Vol: 5, no: 2, pp. 1184–1195.

15. J. Indumathi; N. Asha; and J. Gitanjali, Year: 2020, ''Smart security system using IoT and mobile assistance", In Emerging Research in Data Engineering Systems and Computer Communications, pp. 441–453.