International Journal of Research in Engineering, Science and Management
Volume 5, Issue 6, June 2022
https://www.ijresm.com | ISSN (Online): 2581-5792

Data Security in Healthcare System using Blockchain

Shivani Niddo[1*], K. B. Sudeep[2]
[1]*M.Tech. Student, Department of Computer Science, NMAM Institute of Technology, Karkalla, India*
[2]*Associate Professor, Department of Computer Science, NMAM Institute of Technology, Karkalla, India*

***Abstract*: Blockchain is a decentralized ledger that may be used to store a wide range of personal information. Once safe storage is established, data privacy should be protected. Some systems rely on blockchain and good contracts to maintain auditability. Blockchain technology will not check/address a method of securing information. Blockchain technologies, which have just lately gained popularity in the field of eHealth, can aid in the creation of a reliable, localized, and patient-driven record management system. We look at the growing literature and implementations for blockchain-based consent management in the tending system in this study. It claims that they may be used to share medical data in a secure and auditable manner. Furthermore, smart contracts based on the blockchain can make some types of permission and data processing, as well as data access management and analysis, easier. The goal of this paper was to perform a thorough investigation on the potential of blockchain as a method of securely storing health-care data.**

***Keywords*: Blockchain, Etherium, Smart contract.**

1. Introduction

Healthcare is a top priority for any nation or individual seeking to strengthen their economy and develop globally. Today, blockchain has become extremely popular, and technological change is the only constant in the fight to protect data in the insecure digital era. A blockchain, as its name suggests, is a collection of data-filled blocks. The original goal of blockchain's design and development was to provide a timestamp for digital documents.

Smart contracts are computer programmers that provide instructions for controlling smart characteristics and their processing mechanisms. Maintaining access control with numerous consents, as well as storing and transmitting data across numerous organizations, adds to the complexity. In most hospitals, transmitting patient information through email is not contemplated since it may represent a safety concern while the patient's health data are in transit. The system is one and the same thanks to the central body that keeps and manages patient information as well as access control regulations. Patients must be able to provide authorized people access to their personal information whether selected, limited or complete. This is referred to as consent control, and it is a serious health issue. Blockchain technology may hold the key to finding a solution.

Blockchain is a distributed public ledger that records transactions in an ever-growing chain of immutable blocks connected by cryptographic hashes.

2. Background of Blockchain

Satoshi Nakamoto created the Bitcoin cryptocurrency in a pseudonymous paper in 2008, with blockchain technology as the main core technology underlying it. Bitcoin was the first to introduce the blockchain, and meant to keep track of financial transactions; nevertheless, extending its use cases to non-financial ones, such as for researchers, controlling EMRs is a mission. The blockchain is a decentralised database that holds an ever-growing collection of data records that participants validate and confirm. To achieve the status of a consistent consensus system without the need for a trusted third party, blockchain technology employs a variety of contemporary distributed computing approaches, cryptography, and game theory. A block is a data structure that has two parts: a block header that holds the hash value of the previous block, a timestamp, and a Merkle root, and a data component that contains transaction data. The hash value's order connects all of the blocks. The chain of blocks is transferred over the distributed blockchain network and preserved by the blockchain's minor nodes.

3. Literature Survey

The ability to successfully restrict data access rights in the medical profession and safely communicate data between institutions is a key difficulty in the standardisation of medical information, as discussed in this [1] research. This study presents a data access and safe sharing paradigm based on block chain's decentralisation, tamper resistance, and traceability. The system employs attribute-based encryption technology to maintain the integrity of data and to address issues such as information asymmetry in the traditional medical sector, difficulties in data enquiry, difficulty in locating responsible parties, and inability to track data.

They suggest a method to keep access to and process patient health records safely and securely in this paper [2]. The system's technique, which incorporates a data protection and accessibility mechanism based on smart contracts. The system is built on block chain technology to ensure the integrity and

*Corresponding author: shivaniniddoshivapura@gmail.com

security of health data. There are four network nodes in the healthcare management system: administration (admin), organization, doctor, and patient each have their own. The administrative level is at the top of the organizational structure. You can add/remove hospitals and assign/de-assign personnel in the system. 2) A doctor may be added or removed by an organization (hospital), and a doctor may add/remove patients and access their medical data. 3) A patient may add/remove and access their own medical information, and a doctor can add/remove and examine their medical records.

The difficulty in this [3] study is that to implement the health information sharing approach, a third-party fair association was required, and many associations want to be third-party fair. As a result, many hospitals are experiencing financial difficulties and medical institutes are unsure of who to collaborate with or trade information with. As a result, the project will use block chain technology and encryption to address the issue of third-party fairness. The Health Coin was presented as a valued token, not currency, that would only be utilized in the medical sector. Health Coin can be used to incentivize medical organizations to exchange healthcare data resources. The research is based on block chain and cryptography, and there are three rules: hospitals, physicians, and patients are nodes on our proposed block chain system.

A literature review on the usage of block chain technology in healthcare is presented in this [4] publication. It explores and categorizes the major issues surrounding the administration of medical data, with a focus on developing nations. It explains the security and privacy standards that must be met in order to maintain medical confidentiality in this situation. Most notably, it examines how block chain may be used to solve a variety of medical data management problems while also maintaining their security. The study also discusses the difficulties in selecting and implementing a block chain solution in underdeveloped nations.

The problem in this [5] is data privacy and regular engagement between patients and health professionals. MedChain is a mechanism for maintaining medical records that was employed in this case. This paper presents a novel incentive mechanism that takes use of health professionals' efforts to keep medical data up to date and create new blocks. Med Chain is intended to enhance existing systems by allowing patients, health care providers, and other third-party access to medical information that is interoperable, secure, and effective while respecting patient privacy. Med Chain use time-based smart contracts to manage transactions and regulate access to electronic medical information. It employs cutting-edge encryption technology.

4. Healthcare Security Requirements

IoT-enabled smart healthcare systems handle the majority of patients' personal information and findings. This knowledge is quite beneficial. It is vulnerable to hostile attacks if it is not secured with contemporary and effective security procedures. Unfortunately, several of the smart gadgets and sensors used in smart healthcare are resource constrained. For example, a patient's health development record. The issue is secret, and therefore necessitates a safeguarding technique to prevent information from being disseminated in an unapproved manner group. No one can see or alter the data in this way, and no one can transmit a defective patient health record. It also protects a doctor from making mistakes when dealing with patients. If no precautionary measures are taken. So, the requirements are,

1. *Confidentiality:* It guarantees that personal health information is secure and that unauthorized individuals do not have access to it. In the IoT area, the healthcare domain includes a number of linked devices, apps, and parties, leading data to be hampered by inaccurate diagnoses.
2. *Integrity:* refers to the correctness of health data that has not been tampered with or altered and has been gathered or transferred to authorized entities.
3. *Availability:* Healthcare data must be provided as and when needed without delay for prompt diagnosis and treatment.
4. *Ownership:* it guarantees that all rights to the health information and data gathered belong to a single entity (the originator). This trait limits your options illegal access and misappropriation
5. *Privacy:* Only authorised individuals have access to health data and information, according to privacy. Patients' data and information, for example, are not supplied. without their permission, to any other party In addition, privacy guarantees that data is secure whether in transit or storage.
6. *Authenticity:* It relates to the honesty of the inquiring entity, implying that only the genuine party has access to or may change the data.
7. *Non-repudiation*: It guarantees that neither the user nor the patient will be able to dispute the information provided. It might be dealt with using digital signatures and encryption.
8. *Auditing:* It ensures a healthcare application's overall trustworthiness. It refers to keeping a record of all transactions (captured or modified).
9. *Anonymity:* It refers to the protection of a patient's identity from prying eyes and unauthorized parties. It guarantees that the data is kept in such a way that patient identity remains anonymous.
10. *Data Transfer:* That Is Safe It assures that data in transit is safe and secure, and that it is not tampered with or monitored in any way. It assures that the enemy will not be able to access the information. I can't access the data while it's in transit.

5. Implementation

The help management system is divided into four sections: administration, organisation, doctor, and patient. Each and every health record detail is saved in the block, and the components will interact with one another. The login is used to verify each component. When authentication is blooming, each component will do more labor. Admin is the highest position in the hierarchy. Admin can update or remove hospital information, as well as assign or de-assign allowed users. The

organization will add or remove doctor information. The doctor will update or remove patient information and review the patient's medical records. The patient will be able to add, remove, and retrieve their own medical records as you needed.

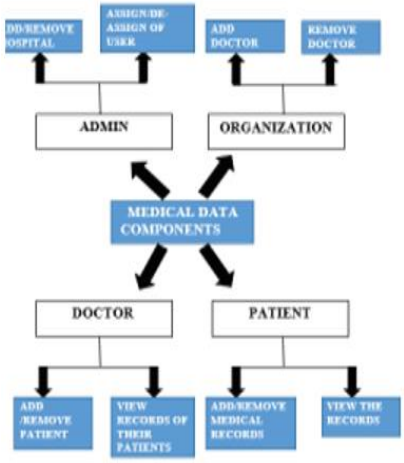

Fig. 1. Healthcare design model

Implementation of web-based software for handling electronic health records using Flask, html, CSS, bootstrap and mongodb to show high level implementation of blockchain. Html+CSS+Bootstrap+JS has been utilized to create an intuitive website that allow users to login as admin, doctor or patient and perform their specific niche operations. The information collected to create a new medical record is based on the key points provided by the Ministry of Health and family welfare.

Blockchain implementation (Backend). Flask, the micro framework in python is utilized for the implementation. Information collected is stored in the cloud server (MongoDB) and a block is created with hash based on attributes of the medical record and it also holds the previous hash and timestamp of creation.

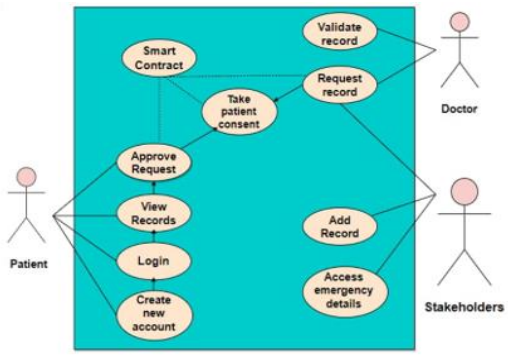

Fig. 2. Blockchain in healthcare

The doctor is an organisation user with the proper role who may post docs for their patients as well as download/view documents for which they have been authorised access. The blockchain contains the patient's medical history, which includes the doctor's information, the patient's medical condition, and any prescribed prescriptions. Any effort by a user to examine the patient's information must be made by sending a request to the patient. If the patient refuses the request, the user will not be able to see the data; however, data that has been accepted will be displayed. When a patient sees a doctor, the doctor might ask to see and add information to the patient's medical record. On the other hand, the patient will get this request on his account, and if approved, the patient's medical history will be available to the doctor.

6. Result

Interoperability, security, integrity, traceability, and universal access are just a few of the difficulties that the healthcare business faces today, and blockchain offers us a fantastic chance to address them. A Blockchain database is a distributed database that collects and saves transaction data in the form of time stamped "Blocks" that are connected to each other in such a manner that no one can change the data. Nodes are Blockchain network participants who validate transactions. Using an overview of blockchain technology, a private and public key pair is cryptographically connected, allowing identification in just one direction. A message encrypted with a private key can be read only by nodes that have a public key associated to the private key. Because every activity on blockchain is a function of the network, a hacker would have to change the same data on all nodes in the network to change any transaction data.

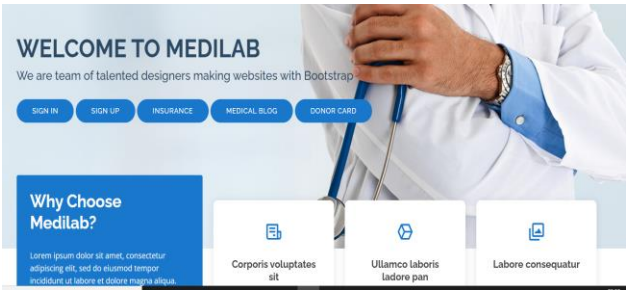

Fig. 3. Front page

The above figure 3 shows the front page of project that means how it look like.

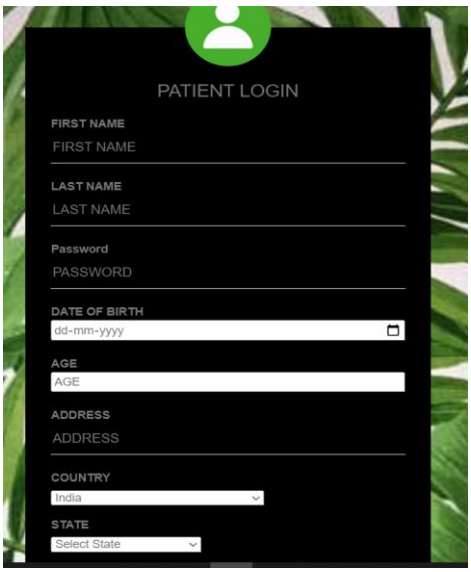

Fig. 4. Patient Signup

The figure 4 shows the patient signup page. Here we can enter patient details.

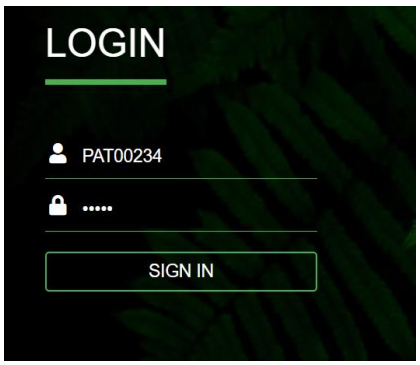

Fig. 5. Patient Login

The figure 5 shows the patient login page.

Fig. 6. Patient Dashboard

The figure 6 shows the patient dashboard page. Here we can view, access, book appointment of patient.

Fig. 7. Doctor Dashboard

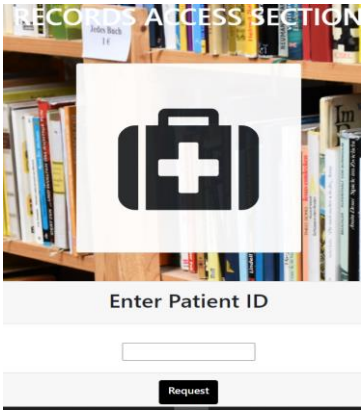

Fig. 8. Request Record

The figure 7 shows the doctor dashboard page. Here we can create patient detail, request patient record and see the available records.

The figure 8 shows the request patient record page. Here we can enter patient id to get that patient details.

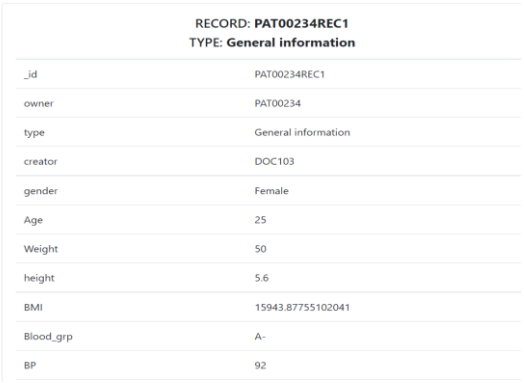

Fig. 9. Patient Record

The figure 9 shows the patient record that is requested.

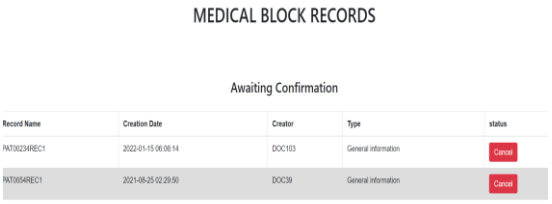

Fig. 10. Available Record

The figure 5.9 shows the available record of patient.

7. Conclusion

The major goal of this project was to give consumers with long-term computer proof of evidence in the medical profession. eHealth stores sensitive personal medical information that must be kept secure. Blockchain is a game-changing technology. It will make life safer by altering the way personal data is maintained and transactions for excellent services are conducted. It not only makes data storage more secure, but it also makes data sharing more efficient. Medical errors are common nowadays, and the qualities of block chains that cannot be tampered with also indicate the person who is guilty. It has aided in some way. We looked at the security needs of IoT-enabled smart healthcare systems as well as the use of blockchain-based security solutions in this research.

References

[1] Zi-chen, W., Xiao-yu, W., Wan-jun, Y., Jia-lan, L., Huai-lin, Z., & Nai-meng, C. (2019). *Medical Information Storage Model Based on Block Chain. 2019 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS).*

[2] Parameswari, C. D., & Mandadi, V. (2020). *Healthcare Data Protection Based on Blockchain using Solidity. 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4).*

[3] Wu, W.-C., & Wei, Y.-C. (2019). *A Health Information Exchange Based on Block Chain and Cryptography. Frontier Computing, 1985–1990.*

[4] Rghioui, A. (2020). Managing Patient Medical Record using Blockchain in Developing Countries: Challenges and Security Issues. *2020 IEEE International Conference of Moroccan Geomatics (Morgeo).*

[5] Daraghmi, E.-Y., Daraghmi, Y.-A., & Yuan, S. M. (2019). MedChain: A Design of Blockchain-based System for Medical Records Access and Permissions Management. *IEEE Access*, *1–1*.

[6] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *2017 IEEE Technology & Engineering Management Conference (TEMSCON).* IEEE, 2017, pp. 137–141.

[7] Gupta, R., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Sadoun, B. (2019). HaBiTs: Blockchain-based Telesurgery Framework for Healthcare 4.0. *2019 International Conference on Computer, Information and Telecommunication Systems*.

[8] V. Chamola, V. Hassija, V. Gupta and M. Guizani, "A comprehensive review of the COVID-19 pandemic and the role of IoT drones AI blockchain and 5G in managing its impact", *IEEE Access,* vol. 8, pp. 90225-90265, 2020.

[9] Zhang, X., Poslad, S., & Ma, Z. (2018). Block-Based Access Control for Blockchain-Based Electronic Medical Records (EMRs) Query in eHealth. *2018 IEEE Global Communications Conference (GLOBECOM).*

[10] Rupa, C., & Midhunchakkaravarthy, D. (2020). Preserve Security to Medical Evidences using Blockchain Technology. *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS).*

[11] A. K. Jha, D. Doolan, D. Grandt, T. Scott, and D. W. Bates, "The use of health information technology in seven nations," *Int. J Med. Inform.*, vol. 77, no. 12, pp. 848–854, 2008

[12] Aiqing Zhang and Xiaodong Lin (2018) Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *J Med Syst,* 42(8): 140.

[13] Chakraborty, S., Aich, S., & Kim, H. C. (2019). A Secure Healthcare System Design Framework using Blockchain Technology. *2019 21st International Conference on Advanced Communication Technology (ICACT).*