E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

A Secured Blockchain-based System for Maintaining and Processing Health Records

Snehal Milind Kulkarni and Dr. (Mrs.) Harmeet Kaur Khanuja

Department of Computer Engineering, Marathwada Mitra Mandal's College of Engineering, Pune, India.

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

In today's digital environment, the world is moving towards progress, to achieve the desired progress; the world should have the healthy population. Every health record is an projection of an individual's health. The current healthcare systems have several challenges such as sharing and accessing medical records across several hospitals while still maintaining security and privacy of these data. The centralized approach of maintaining the health records lead to data beaches. Since the patient have no control over the data, the chances of data being misuse is high. So we need a patient-centered approach which is completely decentralized and patient has right in access control. Blockchain technology serves the best solution to address these problems and fulfill the needs. Blockchain being the decentralized and distributed ledger, it can also impact on record sharing, medical research, identify thefts and financial data crimes in future. The objective of this paper is to highlight on patient-based healthcare model of record maintenance using Blockchain technology where smart contracts are implemented. Implementation of smart contracts in healthcare can simplify things even better where invoking, record creation and validation will be done.

Keywords: *Blockchain, healthcare, electronic health records, smart contracts, storage, security, encryption, decryption.*

Introduction

A modern healthcare system comprises several organizations from different backgrounds, including private hospitals, public hospitals, government institutions, insurance companies etc. In addition, a hospital, the main body of a healthcare system, contains several types of units, man powers, smart devices and systems, etc. In order to provide best services, patients' records and data are usually collected, processed, and communicated regularly between these entities. Maintaining and using the increasing medical data in a secure and reliable manner has become major issues in modern healthcare systems [9] . A health record is a collection of clinical data related to the patient's mental and physical health, gathered from different sources. Health record consists of a patient's medical history, examination, diagnosis, treatment, results of lab investigation, scanning reports, alerts like allergic to etc. These health records can be managed both manually and digitally [5]. Traditional method which is followed by most of the hospitals for maintaining records is manual method which includes papers and books. This method requires large amount of storage. In this method information retrieval is difficult and data manipulation is very easy. In some hospitals digital method is also used but confidentiality is a major issue. Also it requires large storage and patient do not have access to his/her information in any of these methods. In all hospitals, receptionist handles every data which includes chart preparation and daily schedule, answering to different inquiries, keeping the track on reminders and appointments, diagnostic documentation, filing updates, tracking orders, insurance claiming process, cash/cheque payments etc.

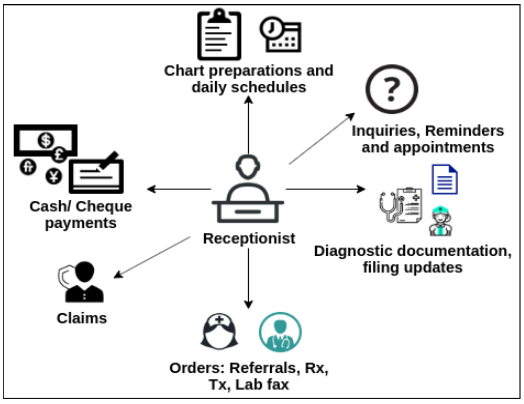
Chart preparations and daily schedules
Inquiries, Reminders and appointments
Cash/ Cheque payments
Receptionist
Diagnostic documentation, filing updates
Claims
Orders: Referrals, Rx, Tx, Lab fax

Fig 1: existing centralized healthcare model

Also, paper-based records are often incomplete, giving rise to unwanted repeat testing and medication. There is wastage of time since this system needs more manual power for transferring records by mail or faxes as these are dispersed and are not centralized. Even accessing of medical records by doctors is limited [6].

Health records can be easily and quickly shared between medical institutions by integrating digital technologies in the healthcare system. In this there are different problems about the storage of patient's data, providing authorization to access the data, security & immutability of the data. These problems can be solved by developing a decentralized digital health infrastructure that is by integrating Blockchain technology into the healthcare system Blockchain technology has the capability to rebuild the modern economy by maintaining and updating records [5] .

The rest of the paper is organized as follows: section IIA provides detailed description of blockchain technology, section IIB gives a brief review on related work that is existing Blockchain challenges and proposed solutions followed by section III where we have explained proposed methodology and section IV and V provides some concluding remarks.

Literature Survey

A. Blockchain Technology

A Blockchain is a decentralized distributed, immutable, shared and tamperproof data structure to store a continuously growing list of the transaction [9]. The Blockchain consists of linear sequence blocks, which are added to the chain with the regular intervals. The information in this block depends on the Blockchain network, but the timestamp, transaction and hash are existed in the Blockchain variants [11].

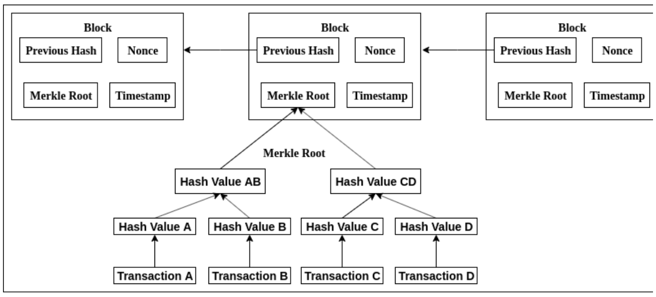

Fig 2: Structure of Blockchain

Let us consider Blockchain as a register containing transaction records into timestamp blocks. Each block has its own identity called cryptographic hash. Each block is provided with the hash of its previous block. Because of it a link is established between the blocks which create a chain of blocks. It is a peer-to-peer network where each node holds the record of each transaction that has been carried out in a network. Each node has a wallet to carry out a transaction. The interaction between the user and a network is via a pair of private and public keys.(Cryptographic keys)[12]. A private key is used to sign their own transaction and public key is to visible to all nodes in the network. Someone who wants to carry out transaction should send a message by signing the transaction with their private key, when this will combine with public key then it forms a digital signature [13]. This transaction is broadcasted onto the blockchain network where it is verified by miners. Miners are the nodes in the Blockchain with the high processing power. Miners make the unaltered and irreversible using a consensus algorithm called Proof-of-Work. There is competition among miners to generate a valid block and the one who generates a valid block is rewarded [14][5].

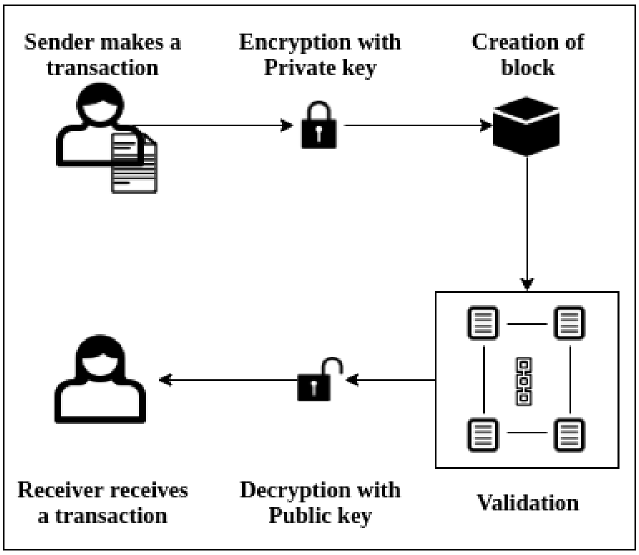
Sender makes a transaction
Encryption with Private key
Creation of block
Validation
Decryption with Public key
Receiver receives a transaction

Fig 3: Working of Blockchain technology

The block of the transaction is approved only when it is verified by all the miners in the network and if more than 51% of the miners validate the transaction then this block is considered as a valid block and is added to the longest Blockchain[13][14].

Advantages of Blockchain Technology [3]:

1. Decentralization, which minimizes the risk of failure of work in the case of failure of a separate system.
2. Increased security through the use of cryptography in the implementation of each transaction.
3. Impossibility to change the data of the approved block. This is achieved by the fact that the hash of the identifier of each block is calculated on the basis of cumulative data hash of the entire block and the hash of the identifier of the previous block.
4. Transparency, as all action is documented and available for all the participants of the system.

B. Related Work

The scheme by Jayneel Vora, Anand Nayyar, Neeraj Kumar provides provides Blochchain-based framework for efficient storage and maintainance of EHR. This also provides the secure and efficient access to medical data by patient while preserving private information of patient [1]. The work by SandroAmofa, Emmanuel BoatengSifah, Kwame O.-B ObourAgyekum, SmahiAbla, Qi Xia, James C. Gee, and JianbinGao presents

Blockchain based scheme to access the patients' data and sharing of it. This scheme is based on smart contracts [2]. The paper by Sergey P. Novikov, Oleg D. Kazakov, Natalya A. Kulagina , Natalya Yu. Azarenko presents the scheme of the distributed data register for creation of the electronic medical card of the patient. Use of smart contract is explained to provide effective Blockchain technology for storing all the data [3]. The work by Andrei Cirstea, NicuBizon, CosminStirbu introduces a minimal introduction to blockchain technology, followed by a medical application (MedBlocks). The objective of this paper is to show the extraordinary potential of this technology and how it will fundamentally change all aspects of receiving, transmitting and securing of information [4][7]. The paper by Harshini V M, Shreevani Danai, Usha H R, Manjunath R Kounte highlights on the patientdriven model of record maintenance using Blockchain technology where smart contracts can be incorporated in future days making it more potential in data exchange[5]. The paper by Kamau, Gabriel, Caroline Boore, Elizaphan Maina, and Stephen Njenga tells that the use of Blockchain in EMR safeguards continuous availability and access to real-time data. Taking the case study of EMR in Kenya, the authors have discussed the existing method of maintaining the health record and they have highlighted the importance of Blockchain technology as it increases the interoperability and security of the system. Blockchain helps the patient to have full access to the data and control on how data is shared. Further Blockchain depends on cryptographic techniques to interact in a network without preexisting trust between the parties [6]. Min Gyu Kim's scheme provides a solution for how to use medical questionnaire result data for the lifelong healthcare of patient and better quality of health care services. It also enhances the security of personal medical records [8]. Guang Yang, Chunlei Li's work proposed a Blockchain for securing EHR by adding new blocks for every data. This scheme also gives a solution for maintaining confidentiality of patient data [9]. The paper by Jamal N. Al-Karaki, Amjad Gawanmeh, Meryeme Ayache k , Ashraf Mashaleh provides management of electronic health records. Also, provides the ability to user to view their medical records regardless of their history [10]. The paper by Julija Golosova, Andrejs Romanovs, analyzes conveniences and difficulties of Blockchain integration and implementation. This also gives brief information about advantages and challenges of Blockchain [11].

Proposed Methodology

The proposed healthcare system is using digital methods for maintaining patients' health records. Presently healthcare organizations use a centralized method for saving patient's information, diagnostic reports, and doctor's prescription. Since it is centralized system there are chances of data getting leaked or exploited for various reasons as patients don't have control over their data and also exchanging of the recorded data is time-consuming and a complex process. Also, hackers are always busy improving their techniques and approaches. They are using creative ways to identify and exploit even the smallest loopholes in your systems and network. Healthcare data is greatly rewarding for hackers. They can sell stolen healthcare data on black market, use it in frauds, sell it to foreign agencies, counterfeit medicines, sell patient identity information to other criminals and use the data in illegal financial transactions. Hence we need a good security system which will monitor all healthcare information. With the aim of dealing with these problems, we are proposing an idea of switching a centralized system to a decentralized system using Blockchain technology.

A. Architecure

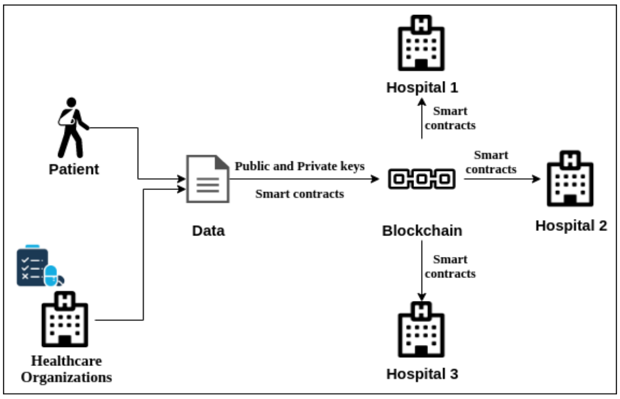

Fig 4: Proposed System Architecture

The Fig 4 shows the basic architecture of the proposed system.

i. Medical Data:

For integrating Blockchain in healthcare, firstly we need to understand the scope of data and where and how it is being generated. Healthcare organizations generate sensitive and critical medical data at every stage of medical treatment like a consultation, diagnosis and surgery. The medical data comprises of doctor's prescription, X-rays, MRI scans, ultrasound reports, endoscopy and also few sensitive health information live HIV diagnosis, cancer diagnosis or psychological conditions. This data has to be in structured manner before storing it into the Blockchain.

Also, patient will enter his/her personal data through user interface which includes personal information like name, age, gender, some previous injuries etc.

ii. Public and Private keys:

On the Blockchain network, transactions containing patient's health records are saved with their Unique IDs and patient's public key. Healthcare organizations or hospitals can access the patient's non-identifiable data through smart contracts only when the Unique IDs match. If required, patient shares the public key with the healthcare organization but without the private key data would always remain non-identifiable.

iii. Smart Contracts:

Smart contracts are self-executing contracts with the terms of the agreement between two parties being directly written in the form of code without the involvement of third party. To share/receive the data, smart contracts are necessary. It is a protocol that digitally verifies the performance of contract.

The smart contract is the script which is stored in the Blockchain. The smart contract has the unique address, set of executable functions and state variables. The user launches the smart contract by addressing the transaction to it. After that, the smart contract is automatically and independently performed in the established order on each node of the chain, depending on the data, which contained in the running transaction [11].

iv. Validation:

Validation of a block in a blockchain is done by miners by using Proof-of-work algorithms.

B. Algorithms

- Proof-of-Work:

A private key is used to sign their own transaction whereas the public key is visible to all the nodes in the network. Someone who wants to carry out transaction should send a message by signing the transaction with their private key, when this is combined with the public key it forms a digital signature. This transaction is broadcasted onto the Blockchain network where it is verified by the miners. Miners are the nodes in the Blockchain with high processing power. Miners make the transaction unaltered & irreversible using a consensus algorithm called Proof of work. There is a competition among miners to generate a valid block and the one who generates a valid block is rewarded. A block of the transaction is approved only when it is verified by all the miners in the network and if more than 51% of the miners validate the transaction then this block is considered as a valid block and is added to the longest Blockchain.

- SHA-256:

The SHA-256 algorithm generates a unique fixed size 256 bit hash. This is one way function so result cannot be decrypted back to the original value. So benefit of this algorithm is that if anyone trace the key then there is no chance to find original key or message.

C. Software Requirements:

- Ethereum – The Ethereum is the flexible Blockchain platform which is open to using by everyone. This platform has the high level of the security from different kind of the attacks. The users can create the Smart contracts and the decentralized applications. This platform is based on the Ethereum Virtual Machine (EVM) [11].

The Ethereum platform has four processes:

- Block validation
- Network discovery
- Transaction creation
- Mining

- Solidity – It is an object oriented programming language for writing smart contracts.
- Visual Studio Code – it is used for front end coding i.e. to create UI code. Also testing of smart contracts can be done in VS code.

Discussions

Proposed framework used various privacy-preserving schemes. It is very difficult to identify any specific patient through its existing account number and Ethereum address. In the proposed framework, we have used the encryption schemes on the patient private data stored on the blockchain, which reduces the chances of unauthorized access of the patient private data. In current proposed system, by using cipher manager, and incorporating the use of encryption techniques before sending and receiving the records over the network, the probability of unauthorized use of records is minimized. Also this proposed system improves ease of information collection and help to store large amount of data which is immutable. This approach also deploys smart contracts, which is a code, which executes on its own when both the parties agree on the set of protocols. Here we consider Hospital admin as one end user and the patient as another party. Doctors, researchers or anyone cannot access patients' data without digital signature that is public and private key. Each patient has unique Ethereum address and identifier which makes it easy to find unauthorized user. As the data cannot be shared outside without permission, possibility of counterfeiting medicines and misdiagnosis is decreased.

Conclusions

As an age old saying goes ”Health is Wealth” in the present scenario we can now consider in addition to health, health records are also wealth. So it is more important to keep our health records safe. The world has started moving towards patient-driven interoperability where patients provide the ondemand access to their health records A Blockchain-based architecture for Healthcare system can help us to improve efficiency in handling whole healthcare system. In this model, the patient is considered as the sole owner to his health records who would decide on sharing what data and with whom. Using this we can secure all patients' data files and provide them a better treatment or medication. As this system is decentralized, patient can access his/her data from any hospitals and any city. This system proposes smart contract based data visibility feature. Through which patient can select who can see his/her medical details.

As the patient has control over his data, the data will not get misused by other unauthorized parties and counterfeiting of any medical data is also not possible. Blockchain technology's use case is not restricted to health record management; it can also be implemented in various domains such as utility payments, banking, e-voting, transport and etc.

Acknowledgement

I would like to thank my HOD, Department of Computer Engineering and guide Prof. Harmeet Khanuja and ME coordinator for their support and guidance throughout this work. I express my gratitude towards them for giving me this opportunity. I would also acknowledge the authors of the base paper as well as references for their work and inspiration.

References

[1]. Jayneel Vora, Neeraj Kumar, M. S. Obaidat , BHEEM: A Blockchain based Framework for securing Electronic Health Records, 2018, IEEE.

[2]. Sandro Amofa, et.al, A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data, 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom).

[3]. Sergey P. Novikov, et.al, Blockchain and Smart Contracts in a Decentralized Health Infrastructure, 2018 IEEE.

[4]. Andrei Cirstea, NicuBizon, CosminStirbu , The Study of Blockchain Application in the Health System (II), ECAI 2018 - International Conference – 10th Edition, June 2018.

[5]. Harshini V M, Shreevani Danai, Usha H. R, Health Record Management through Blockchain Technology, Third International Conference on Trends in Electronics and Informatics (ICOEI 2019) IEEE.

[6]. Kamau, Gabriel, Caroline Boore, Elizaphan Maina, and Stephen Njenga. Blockchain Technology: Is this the Solution to EMR Interoperability and

[7]. Security Issues in Developing Countries?, In 2018 IST-Africa Week Conference (IST-Africa), pp. Page-1. IEEE, 2018

[8]. Andrei Cirstea, NicuBizon, CosminStirbu , The Study of Blockchain Application in the Health System (I), ECAI 2018 - International Conference – 10th Edition, June 2018.

[9]. Min Gyu Kim,et.al, Sharing Medical Questionnaires based on Blockchain, 2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)).

[10]. Guang Yang, Chunlei Li, A design of blockchain-based architecture for the security of electronic health record (EHR) systems, 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom).

[11]. Jamal N. Al-Karaki, Amjad Gawanmeh, Meryeme Ayache k , Ashraf Mashaleh, DASS-CARE:A Decentralized, Accessible, Scalable, and Secure Healthcare Framework using Blockchain, (2019 IEEE).

[12]. JulijaGolosova, Andrejs Romanovs, "The Advantages and

[13]. Disadvantages of the Blockchain Technology", (2018 IEEE).

[14]. Kaushik, Akanksha, Archana Choudhary, Chinmay Ektare, Deepti Thomas, and Syed Akram. Blockchain Literature survey, 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), pp. 2145-2148. IEEE, 2017.

[15]. Mehta, Inderpal Singh, Arnav Chakraborty, Tanupriya Choudhury, and

[16]. Mukul Sharma, Efficient approach towards bitcoin security algorithm, In Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), 2017 International Conference on, pp. 807-810. IEEE, 2017.

[17]. Mukhopadhyay, Ujan, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu, and Richard Brooks, A brief survey of cryptocurrency systems, In Privacy, Security and Trust (PST), 2016 14th Annual Conference on, pp. 745-752. IEEE, 2016.