INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION (IRJMT)

http://www.mapletreejournals.com/index.php/IRJMT
Received 20 March 2019 ISSN 2582-1040
Accepted 23 March 2019 2019; 1(2); 57-61
Published online 25 March 2019

Electronic Health Record System using Blockchain

R.Sangeetha[1*], B.Harshini[1], A.Shanmugapriya[1], T.K.P. Rajagopal[2]

[1]*UG Scholar, Department of Computer science & Engg, Kathir College of Engg, Coimbatore, TN, India.*
[2]*Associate Professor, Department of Computer Science & Engg, Kathir College of Engg, Coimbatore, TN, India.*

**Corresponding author E-Mail ID: sangitaramar5698@gmail.com , Mobile: +91 7871459504*
DOI: https://doi.org/10.34256/irjmt1927

ABSTRACT

This paper deals with the Electronic Health Records for storing information of the patient which consist of the medical reports. Electronic Health Records (EHRs) are entirely controlled by Hospitals instead of patients, which complicates seeking medical advices from different hospitals. In the existing system of storing details of the patients are very dependent on the servers of the organization. In the proposed all the information of the patient are stored in the blockchain by using the Metamask and these details are stored in the block chain as a blocks of data. Each block consists of the data which is encrypted data. Electronic Health Record (EHR) systems record health-related information on an individual so that it can be consulted by clinicians or staff for patient care. The data is encrypted by the algorithm known as SHA-256 which is used to encrypt all the data of the patients into a single line 256 bit encrypted text which will be stored in the block at etherscan. These records for not only useful for the consultation but also for creation of historic family health information tree that keeps track of genetic health issues and diseases it can also be used for any health service with the authorization from both the patient and medical organization.

Keywords: Blockchain, SHA 256 algorithm, Encryption of data, Metamask.

1. INTRODUCTION

The objective of this project is to provide the application which is user friendly and cost effective. The major advantage of this project is security. A securable system is more important to be reliable. Electronic Health Records (EHRs) provide a convenient health record storage service, which promotes traditional patient medical records on paper to be electronically accessible on the web. This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. However, in the current situation, patients scatter their EHRs across the different areas. During life events, causing the EHRs to move from one service provider database to another. Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers.

Blockchain is a decentralized database whose data block is connected chronologically. In the healthcare industry, there are many different parties who need to collaboratively manage personal EHRs blockchain (in a model of consortium blockchain), such as medical specialists, hospitals,

insurance departments, etc. Electronic Record Systems are proprietary that is centralized by design. This means that, there's a single supplier that controls the code base, database and the system outputs and supplies the monitoring tools at the same time. It is difficult for centralized systems to gain trust from patients, doctors and hospital management. Open source, independently verifiable systems solves this issue. This paper deals with the Electronic Records for storing information of the patient which consist of the medical reports. Electronic Records (EHRs) are entirely controlled by Hospitals instead of patients, which complicates seeking medical advices from different hospitals.These details are stored using the blockchain technology .In the existing system of storing details of the patients are very dependent on the servers of the organization. In the proposed all the information of the patient are stored in the blockchain by using the Metamask and these details are stored in the block chain as a blocks of data. Each block consist of the data which is encrypted data. Electronic Record(EHR) systems record health-related information on an individual so that it can be consulted by clinicians or staff for patient care. The data is encrypted by the algorithm known as SHA-256 which is used to encrypt all the data of the patients into a single line 256 bit encrypted text which will be stored in the block at Etherscan.

2. RELATED WORKS

Blockchain is considered as a new technological revolution that was introduced as the backbone of the Bitcoin cryptocurrency. It is a peer-to-peer distributed ledger technology to record transactions, agreements, and sales. The benefits of the blockchain technology are decentralized maintenance, data saving in the block-then-chain structure, secure transporting and accessing of data as well as anti-tamper and undeniable data security. Taking advantage of these distinguishing features above in an EHRs system, blockchain enables the management of authentication, confidentiality, accountability and data sharing while handing information related to privacy, medical resource saving and facilitating for the patient, and making population healthcare smarter. Assuming that there is an EHRs system in a cloud storage platform, which consists of some departments, such as hos- pitals, pharmaceutical departments, insurance departments, disease research departments and so on, EHRs systems can be jointly managed. All departments can offer services for patients together and restrict the rights of each department to prevent EHRs abuse. Thus, an EHRs system with a blockchain structure is designed. Suppose that every patient owns one blockchain of healthcare alone. After being treated in a hospital, all the information including EHRs, consumption records, insurance records, etc. is encapsulated in one block. Patient treatments at different times will be generated in different blocks.

3. SYSTEM HIERARCHY

3.1 Existing System

In the existing system the records are stored and maintained under the organization. So that, the patient can’t able to access these records for further references. When the particular server(database) gets crashed then all the records will be spoiled. To overcome these drawbacks the proposed system is developed. Electronic Records (EHRs) provide a convenient record storage service, which promotes traditional patient medical records on paper to be electronically accessible on the web. In the current situation, patients scatter their EHRs across the different areas during life events, causing the EHRs to move from one service provider database to another. Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers. Interoperability challenges between different providers, hospitals. The patient should have right to access his EHRs for managing and sharing them independently Institutions, etc.

This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. Without coordinated data management and exchange, the records are fragmented instead of cohesive. If the patient has the capability of managing and sharing his EHRs securely and completely.

3.2 Proposed System

In the proposed future system, the patient should have right to access his EHRs for managing and sharing them independently. The patient can be access his medical report directly and can use the digitalized report with anyone. By storing the data in the blockchain the user's data is encrypted and stored as blocks in the etherscan. The user stores data by two way authentication process such as getting secret key generated by the Metamask. Electronic Health Record Systems are proprietary that is centralized by design. This means that, there's a single supplier that controls the code base, database and the system outputs and supplies the monitoring tools at the same time. It is difficult for centralized systems to gain trust from patients and doctors and hospital management. Open source, independently verifiable systems solves this issue. This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved.

A blockchain is managed by a network of computers where there is no single computer is responsible for maintaining or storing the data, and any computers can enter or leave this network at any time Using Blockchain for records can make the whole process End to End verifiable and transparent. The stored data will be transactions, from which we can create a blockchain that will keep track of the database of the patient records. Using this approach, all the patients can make use of the records by themselves, and because of the blockchain they can use these records without any permission request from the organization directly by using the secret key given to them.

3.3 Module Description

Modules present in the proposed system are

- Ethereum
- Smart Contract
- Frontend Contract
- Truffle Framework
- Mist Browser

3.3.1 Ethereum

Ethereum is smart contract platform that is inspired by block chain technology. Its elemental unit is called ether. Ether, similarly to bitcoin is divisible up to 10-18, its smallest subunit is called wei. Due to the fee-by-computation18 policy, Ether (abbr. ETH) is sometimes referred as the fuel of Ethereum. The intention of Ethereum is to merge together enhanced scripting possibilities, meta protocol and time stamped database to allow development of an arbitrary application. The key difference from other block chain protocols is built-in programming language, various types of accounts and unlimited variation of application that can be built on top of it.

3.3.2 Client

Geth is the client software used to download the blockchain and run the Ethereum node on a local machine. It is a Go language implementation, hence meaning Go-Ethereum for Geth. It enables us to sync with the **Testnet** or the **Mainnet** in order to interact with it. Once Geth is initiated, it will connect to the respective blockchain and start downloading the blocks from the peers. While the sync is happening, the block numbers will be displayed in the output which can be used to verify the blocks.

3.3.3 Accounts

In Ethereum, the state is defined by the objects named "accounts", those are 20bytes addresses and the state transitions are the transfers between such accounts.
Example of Ethereum address: 0xc2b1918bc7a2c398ec6f20b754992d7c10d3e2cb
Account contains four elemental fields:

- The nonce – counter ensuring each transaction is processed only once
- Ethereum balance
- Contract code – optional depending if account is used as contract or as a standard transaction. Contracts specify hash of the bytecode, for standard transaction is used empty string.
- Storage – space for contract bytecode

3.3.4 Merkle Patricia Trees

Unlikely from Bitcoin, Ethereum uses more complex hashing structure called "Merkle Patricia trees". Merkle Patricia are a combination of Merkle's scheme of hashing and Patricia (Radix) tree structure, providing a tree that that has cryptographically authenticated data structure that can store key-value bind data. (Xie, 2015) It is very efficient for insert, deletes and especially lookups which are very important for integrity checks made by nodes.

3.3.5 Application Of Blockchain

The transaction histories aremore transparent because of the use of blockchain technology. Information is stored across a network of computers instead of on a single server, makes it very difficult for hackers to compromise the transaction data. Process with blockchain, transaction can be completed faster and more efficiently.

4. RESULTS AND DISCUSSION

EHR is building the future of healthcare on blockchain. There are similar projects but EHR's unique vision stands out. It comes with the specialization of using the blockchain. The blockchain technology makes it easy to monitor population health, identify risk and trends in spread of any issues as it has updated medical report of the patient. This helps to promote effective treatment for the patients throughout the globe. As it is decentralized it in not owned by a single entity, the data is cryptographically stored and they are highly secured. The results of the system were as expected.

5. CONCLUSION

In the EHR system the patient can access their report and can use the report for their lifetime with security. The private key is used for the patient which can be used for the further use of the reports. The one who don't have the private key cannot involve in the process of retrieving data. Hence the Health Records of the patients are more secured with the BlockChain and can used with their own private key as well as they can make use of that for further reference. Currently, there is a huge obstacle for using ethereum platform, which lays in difficulty of obtaining ETH units. The units can be obtained either by mining or purchased for fiat or cryptocurrency like Bitcoin. Once ETH units are available, the publishing and execution of smart contract is really smooth. At this stage, the solidity code has been deployed and verified. The deployed contract is accessed with the

help of metamask injected on web3. Following the port from plain JS to Truffle Framework, we have developed a web application user interface for the health record system. For increased security, we can add account authentication features using some unique identity features.

5.1 Future Work

The proposed voting system can be improved by implementing the following

Allowing only Authorized patients - The authorization of the patients can be verified by using the secret key to prevent malpractices.

Record Limit - Limiting the number of people that can participate and limiting the number of the records that can be casted.

Time Limit - A time limit for the blockchain to accept records.

Providing Ether - Providing limited amount of ether sufficient for the casting of records.

REFERENCES

[1] K. D. Mandl, P. Szolovits, and I. S.Kohane, Public standards and patients' control: How to keep electronic medical records accessible but private, *BMJ*, 2001, vol. 322, no. 7281, pp. 283_287.

[2] G. Irving and J. Holden, How blockchain-timestamped protocols could improve the trustworthiness of medical science ,F1000Research, 2016, vol. 5, p. 222.

[3] M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, 2015, pp. 53_68.

[4] M. Weinger, Dangers of postoperative opioids, APSF Newslett., 2007, vol. 21,no. 4, pp. 61–68.

[5] Sung-Huai Hsieh, Sheau-Ling Hsieh, Po-Hsun Cheng, and Feipei Lai E-Health and Healthcare Enterprise Information System Leveraging Service-Oriented Architectur, Telemedicine and e-Health, 2012, Volume 18, No. 3.

[6] S.D. Cannoy and A.F. Salam, A Framework for Health Care Information Assurance Policy and Compliance, communications of the ACM, 2010 ,vol. 53, no. 3.

[7] Y.S.Rao and R. Dutta, Efficient attribute-based signature and signcryption realizing expressive access structures" IntJ. Seu, 2016 , vol. 15. no. 1, pp. 81-109.

[8] K. Gu, W. Jia, G. Wang, and S. Wen, Efficient and secure attribute-based signature for monotone predicates, Acta Inf., 2017, vol. 54. no. 5, pp, 521-541,.

[9] J Liu la Protecting mobile health records in cloud computing secure, efficient, and anonymous design | ACM Trans. Embed. Comput Syst., Apr. 2017, vol. 16. 10. 2.

Conflict of Interest

None of the authors have any conflicts of interest to declare.