JCRES
Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6- Issue 1, Paper 14,January 2023

A Ethereum Based Block Chain Electronic Health Records System Using Secure Hashing Algorithm

Dr. P. BOOBALAN , ANUKEERTHANA S , ASHUVIN N, HEMAPRABHU V

Department of Information Technology
Puducherry Technological University
Puducherry, India
boobalanp@ptuniv.edu.in

Abstract— **Electronic Health Record (EHR) contains a patient's medical history, diagnoses, medications. The challenge in implementing EHR is how to be able to collect, store, and analyze patient data in a comprehensive and integrated manner without having to violate patient privacy. However, the information is stored in a centralized form where the control is provided only to the medical institution. In this project, a framework that could be used for the implementation of block chain technology in healthcare sector for EHR is presented. The aim of the proposed framework is firstly to implement block chain technology for EHR based on Ethereum and secondly to provide secure storage of electronic records by defining access rules for the users of the proposed framework. This system uses a secure hashing algorithm (SHA) that performs a hashing function on user records for better security. This framework aims in providing the EHR system with the benefits of having a scalable, secure and integral block chain-based solution.**

Keywords— ***Electronic Health Records, Blockchain, Secure Hashing Algorithm, Smart Contract.***

I. INTRODUCTION

An electronic record of health-related information on and individual that can be created, gathered, managed and consulted by authorized clinicians and staff within one healthcare organization. It is basically a health record stored in a computerized form. These EHR records are connected in such a way that there is an interconnection between the databases containing of all or some patient's records. These EHR being shared is made sure that it reaches to the authorized person. EHR basically provides the ability to exchange health information electronically in order to provide high quality and safer care for patients while creating tangible environments for the medical organizations. EHR helps in providing complete information of the patients up to date and with high accuracy. There will be secure sharing of the patient's history between the patient and any third-party organizations. Better clinical decision making is done based on the collection of data of the patients from different sources primarily hospitals. Diagnosing the patients, reduction of medical errors and maintaining of patient's history is achieved in a most efficient and effective way.

II. LITERATURE SURVEY

Ayesha Shahnaz et al [2] Blockchain have been an interesting research area for a long time and the benefits it provides have been used by a number of various industries. Similarly, the healthcare sector stands to benefit immensely from the blockchain technology due to security, privacy, confidentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management. In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these issues. We present a framework that could be used for the implementation of blockchain technology in healthcare sector for EHR. The aim of our proposed framework is firstly to implement blockchain technology for EHR and secondly to provide secure storage of electronic records by defining granular access rules for the users of the proposed framework. Moreover, this framework also discusses the scalability problem faced by the blockchain technology in general via use of off-chain storage of the records. This framework provides the EHR system with the benefits of having a scalable, secure and integral blockchain-based solution.

Fengqi Li et al [4] There is an urgent need to solve the problems of secure storage, reliable sharing, access control and privacy protection in medical industry. In this paper, we propose EHRChain, a blockchain-based EHR system using attribute-based and homomorphic cryptosystem to solve the above problems. First, we design a medical record storage scheme to realize secure high capacity medical data storage and reliable sharing based on blockchain technology and IPFS. Second, we propose an improved cryptographic primitive called SHDPCPC-CP-ABE. Our SHDPCPC-CP-ABE realizes the functions of semi-policy hiding and dynamic permission changing based on partial ciphertext simultaneously. Furthermore, our program achieves the neutrality of the subject of judicial identification in medical disputes and fine-grained access control of medical data. Third, our system applies an additive homomorphic cryptosystem, Paillier cryptosystem with optimized parameters on patients privacy protection during the process of the medical insurance claim. After analysis and experiment, we have proved that the SHDPCPC-CP-ABE is indistinguishable under chosen plaintext attack and takes one third of the time of CP-ABE when changing access policy. Our system has higher performance than other EHR systems based on blockchain.

Pronaya Bhattacharya et al [5] Electronic Health Records (EHRs) allows patients to control, share, and manage their health records among family members, friends, and healthcare service providers using an open channel, i.e., Internet. Thus, privacy, confidentiality, and data consistency are major challenges in such an environment. Although, cloud-based EHRs addresses the aforementioned discussions, but these are prone to various malicious attacks, trust management, and non-repudiation among servers. Hence, blockchain-based EHR systems are most popular to create the trust, security, and privacy among healthcare users. Motivated from the aforementioned discussions, we proposes a framework called as Blockchain-Based Deep Learning as-a-Service (BinDaaS). It integrates blockchain and deep-learning techniques for sharing the EHR records among multiple healthcare users and operates in two phases. In the first phase, an authentication and signature scheme is proposed based on lattices-based cryptography to resist collusion attacks among N-1 healthcare authorities from N. In the second phase, Deep Learning as-a-Service (DaaS) is used on stored EHR datasets to predict future diseases based on current indicators and features of patient. The obtained results are compared using various parameters such as accuracy, end-to-end latency, mining time, and computation and communication costs in comparison to the existing state-of-the-art proposals. From the results obtained, it is inferred that BinDaaS outperforms the other existing proposals with respect to the aforementioned parameters.

III. PROPOSED SYSTEM

In the proposed system, block chain technology based EHR provides decentralized system. This proposed system provides trustworthy access control mechanism by using the smart contracts in order to achieve secured EHR sharing between the patients and the health care providers including hospital and pharmacist. In the proposed system, a patient can register and the doctors feeds his patient details regarding health which then will be converted into hash value using SHA(Secure Hashing Algorithm) 256 algorithm and then it will be embed to a EHR Data in the IPFS(Inter planetary file system) hash. Using this hash-value the doctor and the hospital can view the details permitted by the patients. These hash values are store in an encrypted form in order to ensure security of the medical records.

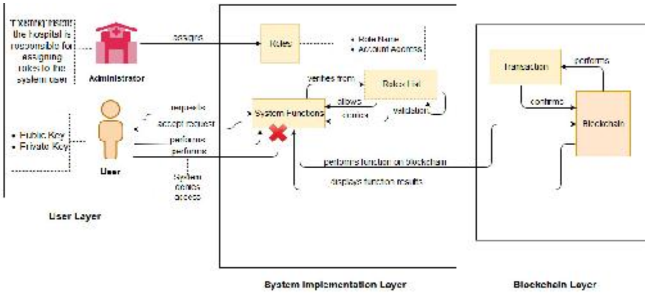

Fig 1. Architecture diagram of the proposed system

A. User Layer

The user of a system is defined as an individual who makes effective use of the system and its resources. A user has various roles and features on the system, making him identifiable on the system.
The users of this system could be patients, doctors and administrative staff etc. The main task of these users would be to interact with the system and perform basic tasks such as create, read, update and delete the medical records.
The users using this system would be accessing the system's functionality by a browser, as it is containing the GUI (Graphical User Interface) of the proposed system framework.
The GUI contains all the functions that could be accessed by a particular user. The user according to the assigned role could use this GUI for interacting with the other layer of the system, i.e., blockchain layer.

B. Blockchain Layer

This layer contains the code or mechanism for interaction of user with the application which is functioning on the blockchain. This layer contains three elements inside it. They are:

a. Blockchain Assets

In Ethereum blockchain, transaction is the process by which external user can update the state of the record or information stored on the Ethereum blockchain network. These transactions are treated as assets by the Ethereum blockchain as they are piece of information that user can send to another user or to simply store it for using it later.

b. Governance Rules

Ethereum blockchain uses Proof of Work (PoW) consensus algorithm, the reason behind using it is also for ensuring that governance of blockchain is maintained in a trusted manner which is through consent from all the trusted nodes attached to the blockchain network

c. Network

Ethereum blockchain uses the peer-to-peer network. In this network all the nodes are connected as peers. With no node acting as the central node controlling all the functions of the network. The reason behind using this network was because the idea was to create a distributed platform not a centralized.

d. Transactions

The system includes following transactions

- Add records

This would create patient's medical records in the Application. It contains the fields of ID, name, co-morbid, blood group, and IPFS hash. The patient's basic medical records is stored along with the IPFS hash that contains the file uploaded containing the lab results or other medical records of patient.

- Update records

This would update the medical records of patient. This can only change the basic information of the patient not the IPFS hash. IPFS hash is non-updateable to ensure security of records.

- View records

The view records function is used both by doctors and patients. The patient can view his records by the system authenticating that patient views only his own medical records. For this purpose, system uses the public account address of the patient to ensure that only the relevant medical records is shown to the patient.

- Delete records

This would make the user be able to delete record of any patient. The user here would be the doctors they are given this right to delete any patient's record stored on the blockchain.

- Grant Access

For each of the above mentioned transactions, certain user would need to have access to them, i.e., only the doctor or nursing staff can make changes in the records of the patient or add them. So, add and update records would only be accessible to these entities. Moreover, patient can view his medical records but won't be given the access to add or update them.

e. Ganache

Ganache is a personal blockchain for rapid Ethereum and Corda distributed application development. You can use Ganache across the entire Development cycle, enambling you to develop, deploy and test your application in safe and deterministic environment.

f. Metamask

MetaMask is a popular and established browser extension which functions as a cryptocurrency wallet that connects to the Ethereum blockchain. MetaMask allows users to interact with the Ethereum ecosystem, which hosts a vast universe of decentralized applications (Dapps), without having to download the entire blockchain on their device.

C. System Implementation Layer

The system was implemented by using the Ethereum and its dependencies.

a) Smart contracts are an important part of the application as they are used for performing basic operations.
b) Following are the contracts that are included in this framework:
   - Patient Records
   - Roles
c) The *Patient Records* smart contract is made purely for implementing the functionality of the proposed framework.
d) These contracts are used for giving access to the users on the application and performing CRUD operations on the records of the patient.
e) *Roles* is a predefined smart contract by the Open Zeppelin smart contract library. This library contains several smart contracts performing various functionalities that could be used for creating our own functions.

f) This role-based access would ensure that no third party is accessing these functions and only the authenticated users of the system would have access to these functions.

IV. RESULT ANALYSIS AND DISCUSSION

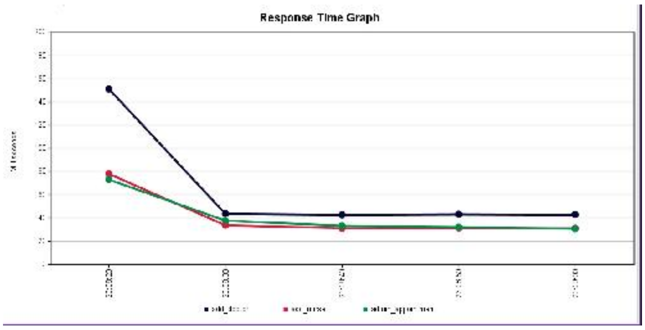

Fig.2 Response Time Graph for Admin's side

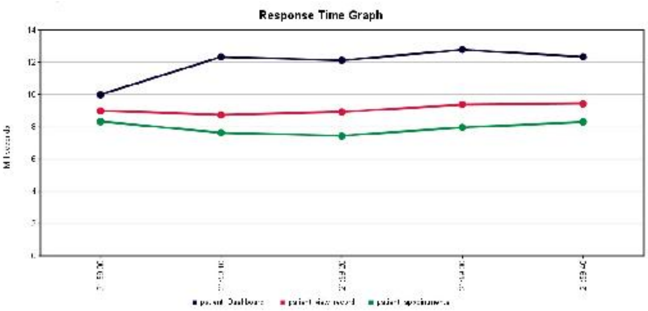

Fig.3 Response Time Graph for Patient's side

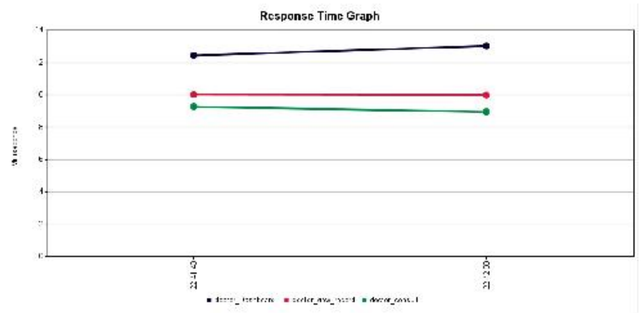

Fig.4 Response Time Graph for Doctor's side

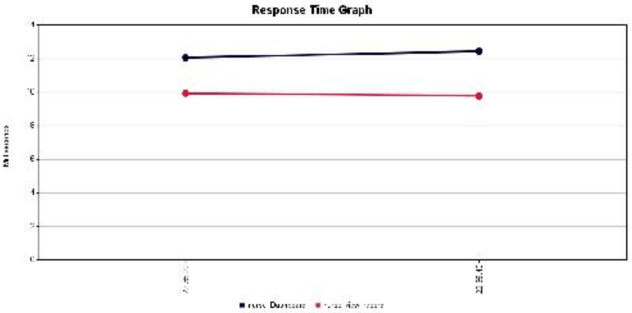

Fig.5 Response Time Graph for Nurse's side

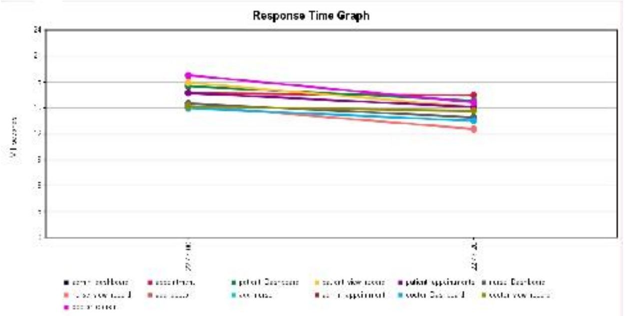

Fig.6 Overall Response Time Graph for each user

The above figures(2)(3)(4)(5)(6) shows the response time taken by each user dashboard to perform their respective tasks.

V. CONCLUSION

In the EHR system the patient can access their report and can use the report for their lifetime with security. The Hash Code is used for the patient which can be used for the further use of the reports. This project proposes a block chain security framework to store EHRs effectively and securely. This framework offers patients access to extensive, consistent records and free access to EHRs, and it also protects the privacy of patients and maintains the consistency of EHRs.

ACKNOWLEDGMENT

We are deeply indebted to Dr. P. Boobalan, Associate Professor, Department of Information Technology, Puducherry Technological University, Puducherry, for his valuable guidance throughout the project work.

REFERENCES

[1] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "Privacyprotector: Privacy-protected patient data collection in iot-based healthcare systems," IEEE Communications Magazine, vol. 56, no. 2, pp. 163–168, Feb 2018.

[2] Ayesha Shahnaz, Usman Qamar, Ayesha Khalid, "Using Block chain for Electronic Health Records", IEEE Access Journals and Magazines,2019,pp.147782-147795.

[3] Jack Huang; Yuan Wei Qi; Muhammad Rizwan Asghar; Andrew Meads; Yu-Cheng Tu "MedBloc: A Blockchain-Based Secure EHR System for Sharing and Accessing Medical Data", IEEE International Conference On Big Data Science And Engineering, 2019.

[4] Dagher, G, Mohler, J, Milojkovic, M and Marella, P. B, "Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," Sustainable Cities and Society, vol. 39, 2019, pp. 293-297.

[5] Fengqi Li, Member, IEEE, Kemeng Liu, Lupeng Zhang, Sikai Huang, and Qiufan Wu,"EHRChain: A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem", IEEE Access Journals and Magazines ,May 2021.

[6] Pronaya Bhattacharya; Sudeep Tanwar; Umesh Bodkhe; Sudhanshu Tyagi; Neeraj Kumar,BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications, June 2021, pp.1242 – 1255.

[7] Usharani Chelladurai, Seethalakshmi Pandian "A novel blockchain based electronic health record automation system for healthcare" , Journal of Ambient Intelligence and Humanized Computing, pp.693-703,January 2022.

[8] https://ieeexplore.ieee.org/documen t/