E-Healthcare System Using Blockchain for Secure EHRs Sharing of Mobile Cloud Based with Machine Learning

[1]N.Saravana Kumar, [2]R.Sreenidhi, [3]A.Samydurai

[1]PG Scholar, [2]UG Scholar, [3]Assistant Professor
Department of Computer Science
[1,3]SRM Valliammai Engineering College, Kattankulathur, India
[2]Sri Krishna College of Engineering and Technology, Coimbatore, India

***Abstract*: For the past few years, we have come across various innovative technologies in EHR where the mobile devices and cloud computing are integrated in order to facilitate the medical data exchanges between patients and the healthcare centers. This advanced technology allowed the health care centers to operate with low cost and high flexibility and security. In the old system, the patient's records are stored in a file database which may lead to high risk such as file theft or change of information of the patients in the file by the muggers. In order to overcome this problem, we have provided a decentralized system by implementing blockchain technology based EHR. Here we have built a access control system using smart contracts which is trustworthy in order to achieve secure EHR sharing between patients and healthcare providers. Our proposed systems integrate crypto currency (ethereum preserving sensitive information about health) against potential threats. Also this proposed system invokes doctor, patients and pharmacist authentications. When patients register themselves, a unique block along with hash value will be created. Once the patients conveys about the disease they have, the doctor will be able to analyze it and prescribe the medicines. The prescribed medicines will be updated to the pharmacist and later the invoice will be generated.**

***Index Terms*: Blockchain, ethereum, patients, cloud computing, flexibility, currency, technology.**

I. INTRODUCTION

This smart electronic health care allows monitoring patients remotely and also offers ambulatory care at home which not only helps to provide care at home but also gives economic benefits to the patients. Further the complete availability of EHR on cloud helps the health care providers to track the patients health and provide proper medical service during diagnosis and treatment process. Apart from these advantages, the concept of storage on cloud also has security challenges which interrupt the electronic health services to be deployed on cloud. The EHR's sharing of information between patients and health care also falls under one among such issues.

Unauthorized entities which gain access without the consent of the patients can have impact on data integrity, privacy and security. Also patients can find it difficult to track and maintain their health record. Therefore it becomes essential to give efficient access control for mobile cloud system. The traditional access control approaches for EHR are completely trusted by the data owners which enable the server to perform access control and enable services. However the traditional assumption is not helpful in case of mobile cloud since the server is honest but it is also curious.

II. INTRODUCTION TO BLOCKCHAIN

The cloud servers will securely perform the data request but mean time it also collect the personal information without the consent of the patients which leads to information leakage issue and breach of network security. Blockchain concept is one of the important feature of digital crypto currency bitcoin. The blockchain follows distributed database of records which are obtained by digital transaction performed by different parties participating in the network. Each transaction done in the network is authenticated by most of the participants in the network system. This concept stores each of the transaction's record. On of the uncorrupted application of block chain is Bitcoin. The reason behind this is that it records all the transactions via digital ledger which is distributed over the network. When one block stored a new data it is added to the series of block chain. As per the name, Blockchain is a series of blocks attached together[8]. To add a single block to the block chain the following four things need to be done. The first is that a transaction must occur. Let us take an example of a sudden Amazon purchase. After crazily clicking through many of the items we come across the final one and purchase it.

The second is that the transaction has to be verified. Once we purchase the item, the transaction made by us has to be verified. Considering the other public records such as Wikipedia, there will be a quality control in charge for the new data entries. But in case of blockchain to it is the network of computers which has thousands of computers spread across the globe. When the purchase is made this network of computers urges to check whether the transaction has happened or not i.e. they check the details of the purchase such as the time of the transaction, the amount and so on. The third is that the transaction verified will be stored in a block. After the verification of the transaction, it will get a green light. All the details of the transaction like amount, signature of the customer and signature of Amazon will be stored in the block. This block will join thousands of other blocks like it.

Finally the block added must be assigned with a hash value. Once the transaction is verified, the block is assigned with unique and identifying hash value. Once the block is assigned with the hash value then the block will be added to the blockchain. Once the

block is added, then it becomes available for everyone including the user. The user is able to view when, where and by whom the block is added to the blockchain.

III. TYPES OF BLOCKCHAIN

There are three types of block chain. They are as follows[3].

Public: The public block chain is also known as permission less block chain. Everyone can be the participant of this blockchain by making transaction in bit coin, by mining a block or by running and connecting as a node.

Private: The private block chain can also be referred as permission block chain. The public participants are restricted and only the members of organization or selected individuals are allowed to participate.

Consortium: It can be called as partially centralized and decentralized. This kind of block chain is controlled by a group of organizations whereas others will be controlled by single organization.

IV. BENEFITS OF BLOCKCHAIN

***Time Saving*:** Since verification of mp central authority is needed for settlements, this process is faster and cheaper.

Cost Saving: It eliminates the third party verification and direct sharing of assets. It reduces the intermediaries and minimizes the efforts of transaction by sharing a copy of the ledger done by participant. This is how the blockchain reduces the cost.

Tighter Security: The client system acts as a barrier and guards against the cyber crime and fraud. Since the data in the block chain is shared with millions of participants, it is difficult to tamper it.

V. LITERATURE REVIEW

Bihuan Chen, Zhixiong Tan, Wei Fang "Blockchain-Based Implementation for Financial Product Management" IEEE 2018.

In the above project, they have proposed the platform for financial product management which is based on blockchain. It forms a constructed architecture of network for management of financial product information which own information transparency and secured environment for information sharing. The management platform in this project uses Hyper Ledger Fabric as underlying architecture concluded the fundamental financial product operations such as routine maintenance of product, multiple function of data inquiry and financial product tractability. At last, considering the financial product management characteristics, a follow-up for improving the weakness of Hyper Ledger has been put forward.

V. Arun, Aditya Dutta, Sourav Rajeev, Rohan Varghese Mathew "E-Voting using a Decentralized Ethereum Application" IJEAT, 2019.

As the technology progress day by day its impact is only positive. One of such evolution is blockchain. It can revolutionize the voting process since it has decentralized nature and immutability. Voting in most of the place is a cloudy process and it is common to corruption. By introducing the concept of blockchain in voting process, a potential protocol can be created which makes the voting process open, fair and verifiable by anyone. Moreover this paper illuminates the potential of the ledger using a case study. It also aims to highlight the advantage and disadvantage of using the architecture of blockchain as a application in the voting process.

Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee"Blockchain Technologies for the Internet of Things: Research Issues and Challenges" IEEE 2019.

This paper presents a complete survey on existing technology of blockchain protocol for IOT networks. This paper starts with introduction of blockchain and explains the existing survey that is associated with the blockchain concept. Then an overview of application domain of blockchain in IOT is provided. Moreover the five main classification of blockchain in IOT is also provided briefly.

Xing Liu "A Small Java Application for Learning Blockchain" IEEE 2018.

This paper preface Chain Tutor, a Java application for learning the concepts of blockchain technology .Even though the concept of blockchain is widely known and its application are found in various areas such as health care, etc some of its concepts are not known for beginners. Text based tutorials can be difficult to follow. Even the pictures of block chain can also be lost in such documented tutorials. With the help of the Java application introduced in this paper, user can implement the concept of blockchain technology via GUI. They can also view how the mining works and how each blocks are added to the blockchain.

Andrei Cirstea, Nicu Bizon, Cosmin Stirbu "Blockchain Technology Applied in Health" ECAI, 2018.

This paper provides a small introduction of blockchain concepts and then brief on its medical applications. The purpose of this application is to make the medical field more efficient. This technology has the ability to transform medical and any other field for decentralization. This can bring a change to the world via secure and efficient way. The main idea of this paper is to show the exceptional potential of this technology and how it change all ways of receiving, securing and transmitting the information.

***M. Drozdova, S. Rusnak, P. Segec, J. Uramova, M. Moravcik, "Contribution to cloud computing security architecture",* ICETA 2017**

Cloud computing has changed complex system's software support from server oriented to service oriented. By this change a wide range of demands in design and delivery of services has been emerged. All the users are relocating their application software to remote servers due to cloud flexibility. This should be able to provide relevant information service and storage for client data by

ensuring availability of data, integrity and privacy. This may also cause data stealing and data breach of the data stored in cloud. This paper identifies the threats and provides solutions to the challenges using the existing solutions.

VI. EXSISTING SYSTEM

Medical data intervention is always possible because the existing system is a centralized distributed system. In the existing system there are drawbacks such as no data privacy, less reliability and lack of network security in sharing the health record among the cloud servers. Also failure in single point can happen in existing system which results in unavailability of data. It also lacks in data retrieval process since the existing system faces storage issues[3].

VII. PROPOSED SYSTEM

In the proposed blockchain 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 feed his details regarding health which then will be converted into hash value using SHA 256 algorithm and then it will be embed to a QR code. Using this hash value the doctor and the hospital can view the details permitted by the patients. The doctors can now provide the medicines by viewing the patients record and this will be converted into a block. This block can be viewed by pharmacist and automatically invoice will also be created. This proposed system also integrates crypto currency that is ethereum which preserves sensitive health information against threats. The crypto currency can also be used to book a doctor's appointment and also pay for it.

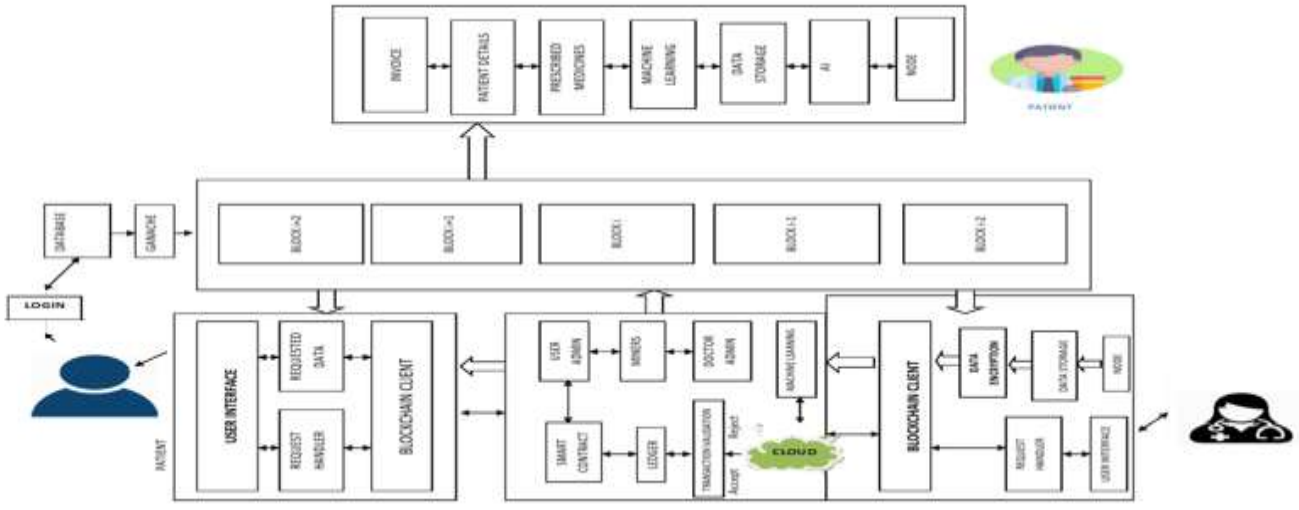

Fig 1. Architecture Diagram

VIII. IMPLEMENTATION OF PROPOSED SYSTEM

REGISTRATION

Registration module helps the doctors and patients to register their details. This module collects the details of the users. In case of doctors, they have to fed their name, date of birth, address, mail id, phone number and registration number. Each doctors in the system belongs to anyone of the healthcare providers. In case of patients, they have to submit their name, date of birth, address, mobile number and details about their health insurance. Apart from these, both the doctors and patients has to provide a valid password. The patients also note the details of the disease which the patient suffers from. All these details are converted into a block and hash value is generated. SHA 256 algorithm is used to encrypt the values. These details cannot be viewed by anyone. Even the doctors cannot view the details of the patients until the patients gives permission to the doctors.

SMART CONTRACT CREATION

A smart contract is a self operating program which executes automatically when the specific condition is satisfied. Incase of ethereum blockchain, smart contract is a collection of data and code with various programmable functions. Users are able to use the Ethereum account to interact with the smart contract through application binary interface. Functions that are defined in the smart contracts can be triggered when a new transaction is made from Ethereum account[7]. This property enable entities to perform their job functionalities such as access management, request handling and data transmission. With the help of Ethereum, the user can communicate with the contractor and the doctor can send the prescribed medicines to the patients. Doctors can also make one by one session of the reports. The same report will be reflected to the patients which makes their communication easier.

Fig 2.Patient Form

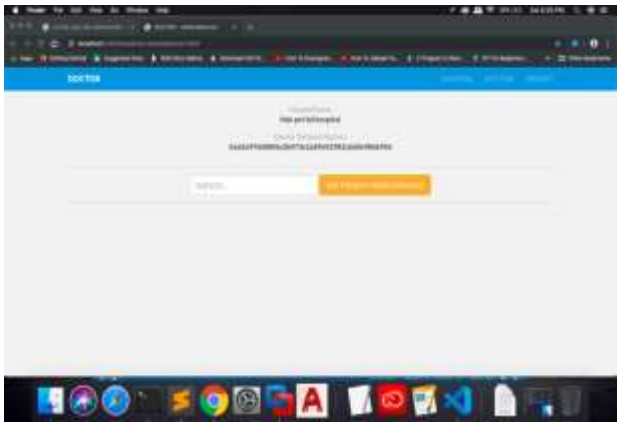

Fig 3.Contract Creation

HASH VALUE CREATION

The cryptographic hash is defined as an algorithm which takes an input and converts it into an output of fixed value. The output is a mix of letters and numbers. There are different types of cryptographic hashes. One of the example is Bitcoin, which uses SHA 256 algorithm. Hashing algorithm is a computational function that converts the input into a fixed value output called as hash value. Hash values are used to compare, identify and run calculation against files containing data.

Fig 4. Hash Value Generation

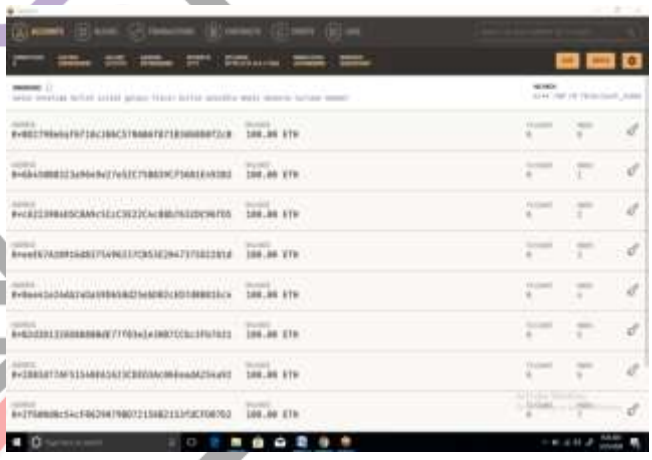

Fig 5.Middleware Currency

BLOCK CREATION

Patients receive EHR notification which has to be approved by them. This way of approval avoids double spending kind of attacks. After verification of EHR, the Block Generator module generates a block which contains the EHR details. Every block in blockchain has a separate hash of block data[9].

PRIVACY PRESERVING

Blockchain technology acts as a complete solution for data privacy and security. The block is connected to each other in form of chain[4]. Every block in blockchain consists of Block header, transaction and transaction counter. The very first block in the chain is called as Genisis.

CRYPTOCURRENCY

Cryptocurrency is a digital asset which can act as a medium for exchange. This blockchain technology provides crypto currencies with adequate level of security in order to withstand the attacks on the system and also to prevent double spending. When a user sends cryptocurrency, manual change of coins does not takes place instead there will be signing off of ownership in sender's and receiver's address. When the sender sends the public key, the receiver should have a private key in order to access the coin sent[6]. If the private key of the receiver matches the public key of the sender then the transaction is recorded in the blockchain and the balance is alerted in both the sender and receiver address. With cryptocurrency, the patient can pay bills, doctor fees, appointment fees, etc.

IX. CONCLUSION AND FUTURE SCOPE

In the above project, the existing challenges of the EHR system are identified and solution is provided to address these issues via a real prototype implementation. This project mainly focuses on to design a trustworthy access control mechanism based on smart contract to ensure users for efficient and secure EHR sharing[2]. This access control can identify and prevent unauthorized access of electronic health system to achieve aimed level of data privacy and network security. Also by the use of machine learning technology, it is able to provide medicine to the patients based on their disease instantly.

The use of Blockchain technology in healthcare system primarily provides reliability of the data stored. Reliability is measured when each record is confirmed for several sources. Secondarily the data will be remained over the time. And no one will be able to modify or delete the data without agreeing with the other sources. Finally it ensures proper data security as no one will be able to view the data without the approval of data source. These kind of qualities makes the blockchain technology an effective one to use in medicine field.

REFERENCES

[1] Kuo TT, Kim HE, and Ohno-Machado L, "Blockchain distributed ledger technologies for biomedical and health care applications," Ame. Medi. Infor. Assoc. J., vol. 6, pp. 1211-1220, 2017.

[2] Matthias Mettler, "Blockchain technology in healthcare: The revolution starts here," in Proc. 18th IEEE Int. Conf e-Health Net., Appli. and Ser, Sept 2016.

[3] Gordon W and Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," Comput Struct Biotechnol J., pp. 224-230, 2018.

[4] Alevtina Dubovitskaya, Zhigang Xu, Samuel Ryu, Michael Schumacher, and Fusheng Wang "Secure and Trustable Electronic Medical Records Sharing using Blockchain,"inProc.AMIAAnnuSymp,pp.650-659,2017.

[5] Marko Holbl et al., "A Systematic Review of the Use of Blockchain in Healthcare," Symmetry, 2018.

[6] Shan Jiang, Jiannong Cao, Hanqing Wu, Yanni Yang, Mingyu Ma,Jianfei He, "BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange," in Proc. IEEE on Smart Compu. (SMARTCOMP), 2018.

[7] Lo.ai A. Tawalbeh, Rashid Mehmood, Elhadj Benkhlifa, and Houbing Song,"Mobile Cloud Computing Model and BigData Analysis for Healthcare Applications," IEEE Access, vol. 4, pp. 6171-6180, 2016.

[8] S. M. Riazul Islam, Daehan Kwak, MD. Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678-708, 2015.

[9] Bahga A, and Madisetti VK "A Cloud-based Approach for Interoperable Electronic Health Records (EHRs)," IEEE J Biomed Health Inform., pp. 894-906, 2013.