BLOCHIE: BLOCKCHAIN BASED ELECTRONIC HEALTH RECORD

[1]Midhun P, [2]Rohith R Nair, [3]Tom John, [4]Aby Abahai T

Mar Athanasius College of Engineering Department of Computer Science and Engineering, Kothamangalam, India

***Abstract*: The Electronic Health Record system is not capable of withstanding the privacy breaches and it cannot be shared with different hospitals. As we all know if a patient can give all the diagnosis histories of him to the new hospital it's very easy to diagnosis and prescribes the medicine. The objective of the project is to develop a blockchain based EHR, which is secure, immutable and decentralized EHR database with patient owing her/his own health data. The application considers three types of users: Doctors, Patients, and Researchers. Anyone of these users interacts with our main application user interface. Next, the user will invoke some queries. SDK will verify the global state of the blockchain and query will be submitted to the blockchain through restful service-based API. Blockchain will send the request to other peers for consensus. After the successful consensus, the transactions will be submitted to the blockchain and the subsequent keyvalue pair will be created or modied according to the request.**

***Index Terms*: EHR, EMR, CSP, HIE, API, SDK**

I. INTRODUCTION

Healthcare has always been important to society. Illness, accidents, and emergencies do arise every day, and the incurred ailments and diseases are supposed to be diagnosed, treated, and managed. In recent years, healthcare information exchange (HIE) among medical institutions has been proved to benefit the medical industry a lot. In earlier days the health recording was done completely using paper. The introduction of computers led hospitals to store their data digitally. But this data is not shareable among different hospitals. This is because each hospital has its own separate network to store its data. So even though the data is digital they are yet not smart. The sharing of health records among different hospitals have a lot of advantages. Mainly the diagnosis will become very easy and a lot more accurate since we will get the full history of the patient and etc. But sharing data can also lead to the privacy breach. So what we exactly need is that an Electronic Health Record system which is shareable, valid and secure. Early success in HIE arose from the field of cloud computing. The idea to store the huge amount of data remotely rather than locally is simple but effective. The cloud service providers (CSPs) propose various schemes for reliable data storage and efficient data processing. Then the stakeholders choose a specific CSP by balancing various factors such as cost and reliability. It has been a trend to resort to CSPs when there is some data to be stored. The beneficiaries range from patients, medical institutions, and research institutions to big corporations. Therefore, the CSPs have been taking great responsibilities to provide a controlled, cross-domain and flexible HIE platform. However, the CSPs have been struggling a lot to provide data sharing services. On the one hand, the cloud storage market has been dominated by the largest CSPs such as Google, Dropbox, etc. They are unwilling to share their data with the small/medium ones and between themselves due to market competition. On the other hand, it is risky if the healthcare data, which is highly private information, is exposed to malicious users unexpectedly. Fortunately, Blockchain technology, which starts at 2008 and booms in 2014, provides great potential for HIE through its attractive features such as security, privacy, decentralization, and immutability. Blockchain is actually a chain of blocks that are interconnected via hash values. This can be considered as a linked list where we can't delete when a block is added to it. So the data that to be added into the block must be verified correctly. We have 3 types of blockchain technologies are there. Public blockchain, Private blockchain, and Consortium blockchain. In Public blockchain, everyone can add data to the blockchain network. But in the case of Private blockchain, only a specific group of peoples have access to add data into the blockchain network. The third type is actually can be said to be the combination of the above mentioned two. Because in Consortium blockchain only those people who are the members of the network can add data into the blockchain and the data is added only if the data is verified by users. The data is added only when the majority (2/3) of people agreed to add the data to the network. Here we use a private permission-based blockchain for the EHR. This is a secure and valid method. Validation is done by the set of rules written by the network creator. Users are granted permission to access certain types of data and complete specific functions. No one can't delete the transactions made in blockchain and by being a ledger of information that is distributed across various a P2P network, blockchain ensures the security of data by not having a single point of failure. So it's also super secure. The objective of the Blochie can be achieved by the blockchain technology. Blockchain ensures secure, immutable and decentralized EHR database with patient owing her/his own health data. For validation, the proposed system enables us to verify a single version of the truth by the consensus of the participating hospitals. Sharing of selected or all EHRs as consented by the patient. All the medical history of a patient can be at one point which mainly helps for the diagnosis of the patient. Also, we can easily verify the medical prescription.The transparency can be improved and also we can easily avoid fraud insurance cases. All of the objectives stated above can be fulfilled with blochie.

II. LITERATURE SURVEY

Demonstrating the effectiveness of health information exchange (HIE) in reducing costs, improving outcomes, and creating more efficient care delivery systems requires evaluation. To evaluate is to measure the significance or value that HIE brings to

patient and population health. This chapter describes strategies and methods for evaluating HIE, principally from the perspective of a health system or other entity engaged in the implementation and use of HIE. The chapter begins with a review of the various types of evaluation, including research. Then the chapter outlines a strategy and the methods for the evaluation of HIE. Finally, the chapter provides guidance for how to disseminate outcomes from HIE development, implementation, adoption, and use. Only by evaluating HIE and sharing lessons can we expand the evidence base for HIE in support of adoption and sustainability. Related work Health-care data is considered as highly sensitive and requires secure and safer means to protect it.Thus, the storage, sharing and managing medical data should be done in secure ways. There are various mechanisms already proposed to address such issues, for example, numerous authentication schemes are presented in order to fulfill the need of secure and efficient medical data accessibility,manageability and other key security requirements.These solutions were helpful at some extent in offering various security requirements under desired health-care scenarios. However, with the current advancement in health-care technology, these approaches are not just sufficient because the patient has been exploited by various stakeholders through different means and with-out their consent. In this context, researchers are keen to nd various secure solutions based on blockchain based healthcare approaches. There have been various research studies related to potential utilization of blockchain in health-care, presented by various researchers in the literature. Electronic medical treatment processes for manual and remote access of the patients data and protecting the privacy of the health-care data are the most priorities of application where Blockchain technology can create value. The work in has proposed MedRec in which a decentralized way of using blockchain technology is adopted to manage the EHR/EMR. The authors also provided a potential case study of blockchain usage in healthcare, which provides a prototype for EHR/EMR. Moreover, the work in presents MedShare that provides the trust-less way of sharing the health-care data among various service providers using blockchain. Henceforth,research community are dening different mechanisms for the secure data accessibility of blockchain based health-care system. This work provides a contribution towards an efficient and improved data accessibility mechanism by using private/ permissioned blockchain for the secure and faster health-care data access. Thus,this paper proposes a methodology that is completely based on the patient's access control for processing and accessing the data by other stakeholders. The medical data is stored in the database located at peer to peer networks whose address is stored in the blockchain.The degree of access is for function of the data which patient are permitted to access whereas doctor needs access control from the patient.Ethereum is a public blockchain platform, with possibility to create smart contracts and focuses on the Blockchain technology development. A Smart Contract is a computer based protocol, consisting of rules, agreed by the stakeholders according to their requirements and also it has a Turing complete architecture for securing the patient's data and the rules that can also be modified by the legal person whose signature is in the agreement. A Smart Contract is also used to interact with the blockchain and health-care providers according to their need and also manages the patient's healthcare information by managing the access control given by the stakeholder and secured administration of the healthcare record.The health-care systems presented in the above literature are capable to ensure the secure data.

III. EXISTING SYSTEM

Paper-Based Records.

The most traditional way of the health recording system is a paper-based health record system. All the details and information were written into papers and were filed and stored. This was very convenient for the older day. We don't have to bother about the availability of electricity in this method.

Electronic Health Recording system

All the cons of the paper-based medical record system actually pointed to the digital storage systems. When compared with the paper-based medical record system digital health record system has many advantages. Mainly the storing and retrieval of medical records become too easy. The searching for a particular record became too easy. Digital record systems were actually all about speed and convenience.

Cloud-based Electronic Health Recording system

By sharing a health record between different hospitals, the diagnosis of a patient can be very easy. Because we can fetch the previous records of the patient from his old hospital. This idea was the real inspiration behind the Cloud-based EHR system. The idea was very simple. Putting all the electronic health records into cloud storage which can be accessed by other hospitals. But the main challenge to this system is the hacking threats which can lead to a huge privacy breach.

IV. PROPOSED SYSTEM

The proposed system is a blockchain based medical recording system. This can be used by any hospital. In this, each block in the blockchain network is a transaction. The backend is made of Hyperledger and the frontend is an HTML page. The patients and doctors can give inputs via the WebUI. This system will allow sharing our medical records between different authorized doctors. The application considers three types of users: Doctors, Patients, and Researchers. Anyone of these users interacts with our main application user interface. Next, the user will invoke some queries. SDK will verify the global state of the blockchain and query will be submitted to the blockchain through restful service-based API. Blockchain will send the request to other peers for consensus. After the successful consensus, the transaction will be submitted to the blockchain and the subsequent key-value pair will be created or modified according to the request.

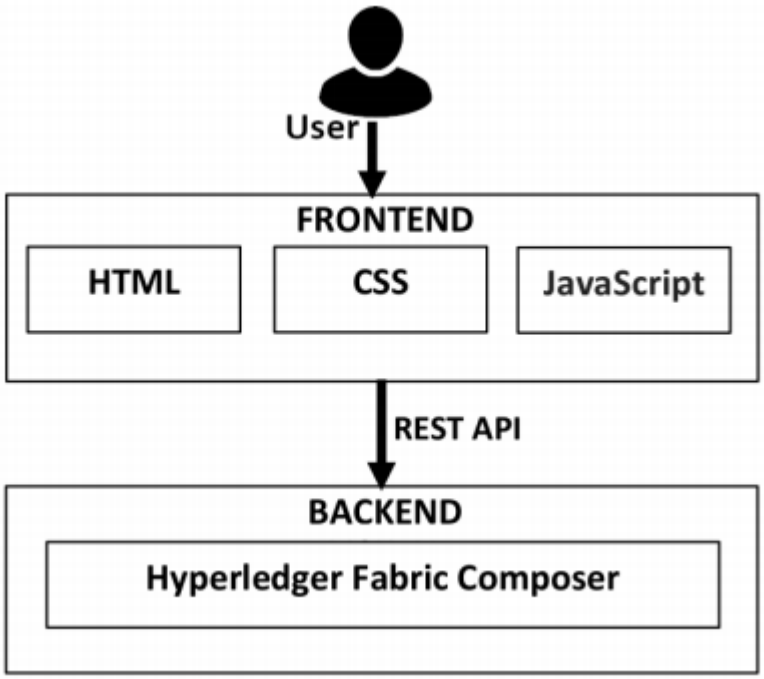

Fig 1: Basic overall diagram

V. IMPLEMENTATION

The implementation comprises of the detailed modular design of the system, how various functions work, their core algorithm. The detailed design of a project deals with the entire functionality it handles. A well-defined detailed description includes major functional components in that application along with sub-modules included and table handled. It shows the actual data flow within the system and how each function handles the data. In computer science, an implementation is a realization of a technical specification or algorithm as a program, software component, or other computer systems through computer programming and deployment. Many implementations may exist for a given specification or standard. In an information technology context, software or hardware implementation encompasses all the post-sale processes involved in something operating properly in its environment, including analyzing requirements, installation, configuration, customization, running, testing, systems integrations, user training, delivery and making necessary changes. The word ”deployment” is sometimes used to mean the same thing. For an implementation process to be successful, many tasks between different departments need to be accomplished in sequence. Companies strive to use proven methodologies and enlist professional help to guide them through the implementation of a system but the failure of many implementation processes often stems from the lack of accurate planning in the beginning stages of the project due to inadequate resources or unforeseen problems that arise. Software/hardware implementations should always be designed with the end user in mind and the implementation process usually benefits from user involvement and support from managers and other top executives in the company. If users participate in the design and implementation of the system, ideally it will serve their business objectives more accurately and reflect their priorities and the ways in which they prefer to work. Software/hardware implementations should always be designed with the end user in mind and the implementation process usually benefits from user involvement. Their involvement in the process also makes them more receptive to changes that need to be implemented because they have the first-hand experience of what the system comprises.

VI. CONCLUSION

The proposed system is an electronic health record system based on a blockchain network. This will resolve the safety and validation of the existing EHR systems. Since most of the existing system uses a centralized server, privacy attacks were common in EHR which cause loss of privacy. Also by hacking into the server network we can easily put false data for a patient. But the proposed system is based on a blockchain network. So privacy and validation are ensured. Even though it’s difficult to create the proposed system there is no additional cost to spend and also it will ensure complete safety and validation. Also, we can easily share our EHR with any hospitals in our proposed system. The user just needs to log in to their profile for the full history. Which make diagnosis very easy. Since it’s based on the blockchain it cannot be attacked.

REFERENCES

[1] BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange, 2018 IEEE International Conference on Smart Computing (SMARTCOMP)

[2] S. Jiang, J. Cao, Y. Liu, J. Chen, and X. Liu, “Programming large-scale multi robot system with timing constraints,” in Computer Communication and Networks (ICCCN), 2016 25th International Conference on. IEEE, 2016, pp. 1–9.

[3] Zhou, Z. Cao, X. Dong, and X. Lin, "Tr-mabe: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems," in INFOCOM. IEEE, 2015, pp. 2398–2406.

[4] N. Grozev and R. Buyya, "Inter-cloud architectures and application brokering: taxonomy and survey," Software: Practice and Experience, vol. 44, no. 3, pp. 369–390, 2014.

[5] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1832–1843, 2017.

[6] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.