EHR using Blockchain

Soham Sagade, Atharva Lonkar, Param Sonawane, Abhishek Deshmukh, Prof. Jyoti Kulkarni

Dept. of Computer Engineering, Sinhgad college of Engineering, Maharashtra, India.

Abstract – *Traditionally and as of today, patient's health information is stored on organization owned centralized database. The current system seems fine at first but has some serious underlying issues. Some of the issues are that the system is not patient centric, seamless data sharing is not possible, inconvenient for patient, etc. To summarize, the one who stores the data owns the data. So, it is evident that there is a need for a system which is more patient oriented. Such system can be developed by using blockchain. Since the nature of blockchain is decentralized, EHRs when stored on a blockchain will take the ownership of data away from the hospitals and will put patients in control of the data. Ethereum based decentralized application can be developed to store patient's confidential medical information in a distributed way. The application will store patient's data in an encrypted format to provide additional layer of security and will also overcome the drawbacks of public blockchain.*

Keywords — IPFS, Data-Masking, EHR

1.INTRODUCTION

Blockchain in a nutshell is a distributed ledger, that records transactional data, of the parties that were involved in the transaction. Blockchain is a chain of blocks and each block in the blockchain is linked to the previous block via cryptographic hash. Each transaction is recorded on the block and a block can hold fixed number of transactions and next block is added when the previous block is full.

The inherent feature of blockchain is immutability. Immutability in the context of blockchain means, once the transaction is recorded on the blockchain it cannot be reversed or undone. This makes blockchain secure and immune to modification. Because of the property of immutability, one of the important applications of blockchain is recording financial transactions.

Blockchain design is decentralized and it is not controlled or driven by central authority but managed by peer-to-peer nodes or users. Since, there is no central authority to authenticate and validate transactions, blockchain uses consensus algorithm to authenticate and validate transactions. Consensus basically means before the block is added on to the blockchain, the registered nodes in the network must form an agreement regarding the state of the blockchain. There are various consensus algorithms such as Proof of Work (PoW), Practical Byzantine Fault Tolerance (PBFT), Proof of Stake (PoS), Proof of Burn (PoB) etc.

Data privacy in blockchain is achieved using cryptography. Every individual block in blockchain is connected to the block before and after it. This makes it hard for a hacker to alter with any record as the hacker would also need to change the records or blocks linked to the record that he desires to manipulate or access, which is practically impossible to do in a huge network where there are a large number of blocks in a blockchain. (Preserving the Privacy of Electronic Health Records using Blockchain).

In current healthcare system when patient visits hospital, hospital stores patient's data in the database. That means hospital owns or controls the patient's data, even though the data belongs to the patient. Also because of this centralized storage architecture security of patient's data is compromised against data leaks or data breaches. Electronic health record exchange becomes a challenge between different organizations. This impediment can be tackled by introducing a separate third-party entity which enables easy data sharing. But drawback of this method is exposure of patient's confidential data to an independent entity.

Blockchain can be a potential solution to the problem of storage of electronic health records. Blockchain can provide solution that is patient centric, reliable and secure. With blockchain there is no need of centralized authority and every transaction follows the protocol given by the smart contract. Smart contracts are tools of blockchains that allows execution of true and credible transactions.

2. Literature Survey

Authors of the paper [1]make a case about data security issue in cloud based EHR systems. Data security issue is responsible for problems like data leaks, data tampering, etc. According to the authors, main reason behind the issue of data security is centralized nature of cloud based ehrs. Blockchain is one the possible solution to the above-mentioned problem. However, implementing new blockchain solution is expensive and time consuming. Paper suggests, instead of developing a new solution from scratch, integration of existing cloud based ehr with blockchain is more feasible. Solution proposed in the paper makes use of public blockchain. The architecture proposed in the paper has four main components. Firstly, User application with which different users of the system interact with the system. This component is also responsible for interacting with blockchain handshaker. Secondly, Blockchain Handshaker, it is the core component of the proposed architecture. It acts as an intermediary amongst blockchain, cloud and user application. It receives transaction from user, converts it into appropriate format, forwards transaction to blockchain for verification. The validated transaction is forwarded to cloud for storage. If response is invalid, transaction is stored for auditing tasks. Thirdly, Blockchain, public blockchain used in the system, main responsibility is validation of transactions. Lastly, cloud, used for storage of health records.

Yogesh Sharma and Prof. Balamurugan, the authors of the paper[2] use Hyperledger fabric and Hyperledger composer to implement the blockchain based ehr system. Hyperledger fabric is open source blockchain framework founded by Linux foundation. Business logic of the system is contained inside smart contracts. Besides the business logic, smart contracts also contain permissions to read, write or update. System proposed in the paper has three main external actors namely, patients, doctors and laboratories. Admin actor is responsible for management of smart contract. The paper gives basic implementation of the blockchain based ehr system with transactions such as creation of medical record, grant access to a doctor, add a participant, update information of a participant, etc.

Guang Yang and Chunlei Li, the authors of the paper[3] propose blockchain architecture built on top of existing health providers databases. Blockchain will keep track of all database queries, hence any ill tampering of health records can be traced back to its source. Authors of the paper propose the use of private blockchain instead of public blockchain. In private blockchain only authorized nodes can participate, validate or perform transactions. Additionally, paper introduces an incentive mechanism to select the provider for generating or creating new block. This selection is done on the basis of significance value. Each provider in the system is associated with a significance value. Significance value depends on the number of records that provider has in the database and value of each record. Whenever a selected provider generates a new block, that provider is rewarded with incentive. Architecture proposed in the paper is not for specific blockchain platform but a general one. Paper proposes a system built on existing infrastructure which makes it feasible for health providers to adopt the proposed system.

Authors of the paper[4] propose the use of Hyperledger fabric as open source blockchain platform. Architecture proposed in the system has four main components client, storage, certificate authority, blockchain Hyperledger. Client component represents all the real-world entities which will use the system. Storage is responsible for storing health records. Certificate authority generates public and private key and delivers them to the users. The paper proposes the use of multiple blockchains, one global blockchain and one local blockchain for each health institution. Global blockchain stores unique patient hospital visits and local blockchain records EHR associated with patients. Paper analyzes the proposed multi blockchain approach by comparing it with single blockchain approach. Comparison is based on storage size scalability. Results of comparison show that multi blockchain model is more scalable that single blockchain model in terms of storage size.

In this paper[5] the authors have proposed a electronic medical record security sharing model based on blockchain (EMSRB), that makes use of the different characteristics of blockchain to facilitate the secure and tamperproof way of storing the medical records. The paper proposes use of different technologies to support this cause, along with blockchain. They are as follows: 1. Data masking: Data masking is the technology that is used to prevent the selected or sensitive information from being displayed to the user. here it has been proposed that data masking can be achieved by various ways like generalization, substitution and other specific algorithms. 2. IPFS (Inter Planetary File System): Here is proposed that the system can take advantage of IPFS, which is a peer-to-peer file system, which is a single BitTorrent cluster using git repo for distributed storage. IPFS can store files in different formats, but it also can return a hash pointing to that file that will be used to retrieve the file. The paper also describes the working of the system with various block diagrams, to make it more readable. Authors have also provided a way to improve the currently used consensus algorithm, that is, Proof of Work (PoW), to make the working of the system better and more reliable.

In this paper[6] the authors have presented a broad view on how using Decentralized health management system can drastically improve the decision time for treatment. Here, they describe the working of a hypothetical Electronic Health Record Management System, that is based on blockchain technology. This system makes use of the decentralized nature of the blockchain for patient's benefit. The authors further propose the methodology for preserving different types of medical records under different types. The system aims to provide a robust alternative to the current centralized system, by storing the data on decentralized nodes and letting the patient be in charge of his own data. In the methodology, along with general working of the system, authors have also proposed generation of e-stamps for the patients, to prove the authenticity of the individuals, so that they are given the correct medical treatment without any errors or exploitations.

Jayneel Vora, Anand Nayyar[7] the authors of the paper propose a Blockchain-based approach for efficient storage and transfer of EHRs.The system proposed in the paper preserves privacy. The system makes it extremely difficult if not impossible for anyone to uniquely identify a patient through its existing account number and Ethereum address. The system comprises of four major portions based on utility and function such as the Blockchain, patient nodes, provider networks and proxy nodes. The blockchain used in this system uses the following contracts -service contracts, owner contracts, classification contracts and permission contracts. The records are normally created at the end user nodes in this case the patient node. This framework can be used in various ideas to support scalability. The storage of hashes and small EHRs ensures scalability Hence this system ensures Unauthorized access by various actors is further minimized and a sense of decentralization while consisting certain nodes with an improvised authority is achieved.

This paper[8] proposes a different approach for the Management of Health Records by utilizing the mobile infrastructure that we have in our possession. The aper put emphasis on two main key points related to the health records. First one being, health data can be highly sensitive, hence it must be stored securely and privately. Secondly, current systems use centralized architecture, which requires central trust, the paper aims to eliminate both these hurdles by implementing the management system with the help of decentralized blockchain system and using mobile infrastructure as an aid to achieve this goal. In the system overview, the paper considers many use case scenarios such as user, healthcare provider, health insurance company, wearable devices; to collect user medical data from etc. This can be considered as one of the pros of this paper. The paper suggests that the system will make use various wearable devices to monitor health of the users and store this data on decentralized storage solution, that is, blockchain. This data can be then made accessible to the specified medical practitioner for review and treatment purposes. The paper also provides a flow diagram to depict the sequence of activities within the system. The authors further conclude that, the system can handle a large dataset at low latency, which indicates efficiency and scalability of the data process.

Authors of the paper [9]address the problems regarding user privacy when using third party applications. Authors focus on the mobile applications that collect user data and over which users have no control. These mobile applications require users to grant permissions during application installation. In current scenario only way user can resist application policy is by not using the application, there is no way for user to change or revoke permissions and still use application to its full potential. Authors suggest framework where control of the user data is in the hands of the user. Proposed solution consists of three entities users, services and nodes responsible for the blockchain. The proposed framework stores access control policies on blockchain. The overall framework is user oriented, hence user is able to change accesses of entities at any given point. User data is stored on off chain storage, but pointer to that is stored on blockchain. Before services can access user data, blockchain verifies the access control policy and responds accordingly.

Author of the paper[10] suggests the solution that tackles the privacy issue in electronic medical record (EMR) and big data nature of the medical records. Author makes use of blockchain platform BigChainDB for the implementation of the platform. BigChainDB has fast transaction speed and it allows storage of data in BSON format (format similar to JSON). Main difference between Ethereum and BigChain is that in BigChainDB there is no concept of transaction fees.

3.Proposed Methodology

Proposed system allows secure storage of patient's medical records on blockchain. Records of the patient are stored on the IPFS system in an encrypted manner and hash returned is stored on blockchain. There are various actors or entities in the proposed system, namely, doctor, patient, pharmacy and data analyst. We are proposing use of two encryption algorithms, AES and RSA to ensure data confidentiality.

In the system, doctor will generate data, the doctor will share data with patient. Patient will have option of sharing prescription with pharmacy, granting access to doctor and revoking access from doctor. Pharmacy will share the generated bill with patient.

3.1 Major Classes

Patient Class:

This class is responsible for storing patient's medical records, providing the functionality for retrieving medical records, sharing prescription with pharmacy, granting revoking access from doctor.

Doctor Class:

This class provides the functionality for reading and writing patient's medical record.

Pharmacy Class:

This class is responsible for storage of shared prescription and generated bill. Class also provides functionality for sharing the generated bill with patient.

Data Analyst Class:

This class is responsible for storage and retrieval of data shared by patient's consent.

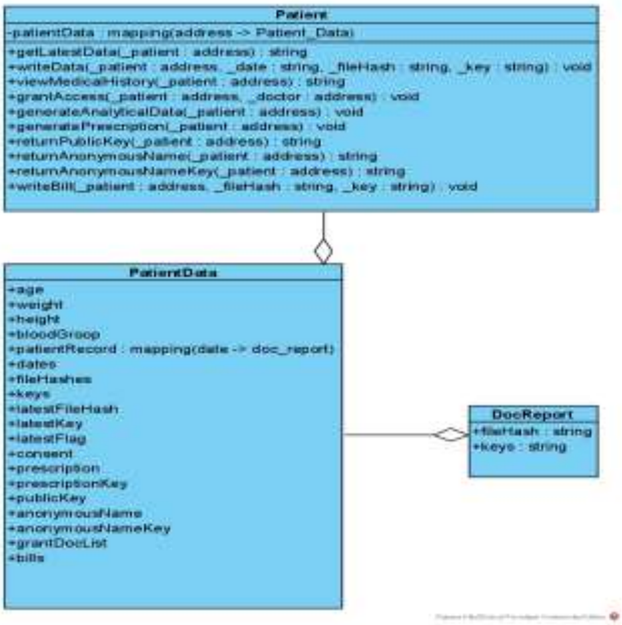
Patient
-patientData : mapping(address -> Patient_Data)
+getLatestData(_patient : address) : string
+writeData(_patient : address, _date : string, _fileHash : string, _key : string) : void
+viewMedicalHistory(_patient : address) : string
+grantAccess(_patient : address, _doctor : address) : void
+generateAnalyticalData(_patient : address) : void
+generatePrescription(_patient : address) : void
+returnPublicKey(_patient : address) : string
+returnAnonymousName(_patient : address) : string
+returnAnonymousNameKey(_patient : address) : string
+writeBill(_patient : address, _fileHash : string, _key : string) : void
PatientData
+age
+weight
+height
+bloodGroop
+patientRecord : mapping(date -> doc_report)
+dates
+fileHashes
+keys
+latestFileHash
+latestKey
+latestFlag
+consent
+prescription
+prescriptionKey
+publicKey
+anonymousName
+anonymousNameKey
+grantDocList
+bills
DocReport
+fileHash : string
+keys : string

Fig 1. Patient Class

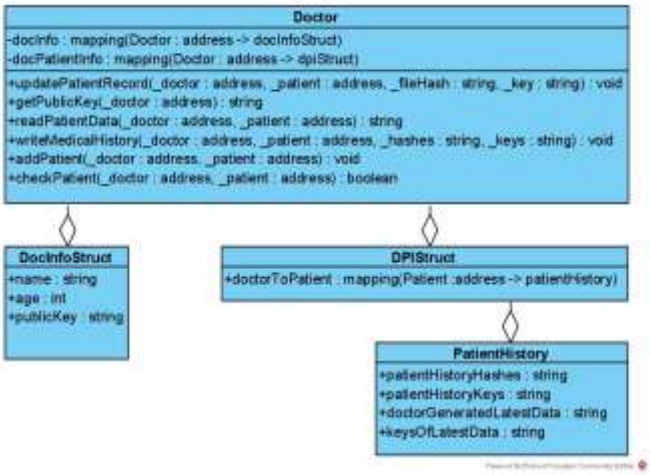
Doctor
-docInfo : mapping(Doctor : address -> docInfoStruct)
-docPatientInfo : mapping(Doctor : address -> dpiStruct)
+updatePatientRecord(_doctor : address, _patient : address, _fileHash : string, _key : string) : void
+getPublicKey(_doctor : address) : string
+readPatientData(_doctor : address, _patient : address) : string
+writeMedicalHistory(_doctor : address, _patient : address, _hashes : string, _keys : string) : void
+addPatient(_doctor : address, _patient : address) : void
+checkPatient(_doctor : address, _patient : address) : boolean
DocInfoStruct
+name : string
+age : int
+publicKey : string
DPIStruct
+doctorToPatient : mapping(Patient :address -> patientHistory)
PatientHistory
+patientHistoryHashes : string
+patientHistoryKeys : string
+doctorGeneratedLatestData : string
+keysOfLatestData : string

Fig 2. Doctor Class

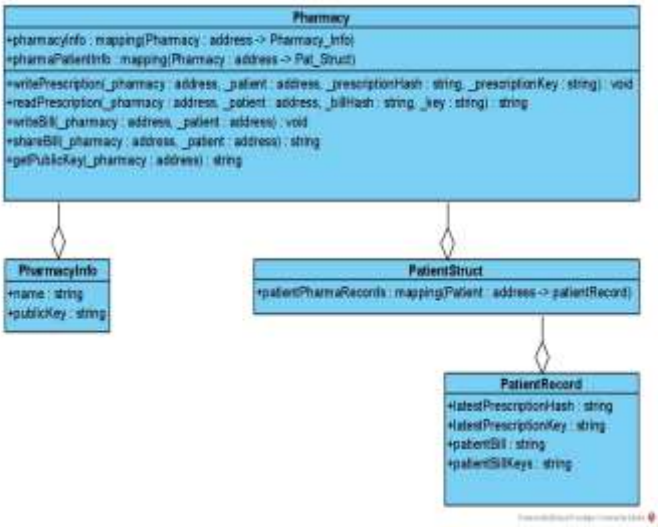
Pharmacy
+pharmacyInfo : mapping(Phamacy : address -> Pharmacy_Info)
+pharmaPatientInfo : mapping(Phamacy : address -> Pat_Struct)
+writePrescription(_pharmacy : address, _patient : address, _prescriptionHash : string, _prescriptionKey : string) : void
+readPrescription(_pharmacy : address, _patient : address, _billHash : string, _key : string) : string
+writeBill(_pharmacy : address, _patient : address) : void
+shareBill(_pharmacy : address, _patient : address) : string
+getPublicKey(_pharmacy : address) : string
PharmacyInfo
+name : string
+publicKey : string
PatientStruct
+patientPharmaRecords : mapping(Patient : address -> patientRecord)
PatientRecord
+latestPrescriptionHash : string
+latestPrescriptionKey : string
+patientBill : string
+patientBillKeys : string

Fig 3. Pharmacy Class

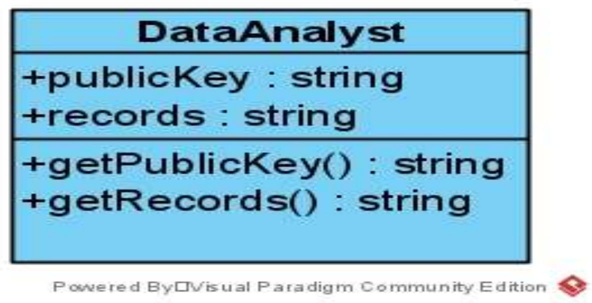

Fig 4. Data Analyst Class

4. Conclusion

From the literature survey, it has been observed that some papers propose a total blockchain based solution, while others suggest a blockchain based solution built on top of the existing system. One of the major issues with implementing blockchain as a potential solution is scalability, in terms of both, storage as well as performance. However, paper [4] attempts to solve storage size scalability problem, the issue regarding performance scalability remains unsolved.

Proposed system considers external entities and their interaction scenarios and also puts patient in charge of his/her data.

REFERENCES

[1]. Rahman, M.S., Khalil, I., Mahawaga Arachchige, P.C., Bouras, A. and Yi, X., 2019, July. A novel architecture for tamper proof electronic health record management system using blockchain wrapper. In *Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure* (pp. 97-105).

[2]. Sharma, Y. and Balamurugan, B., 2020. Preserving the privacy of electronic health records using blockchain. *Procedia Computer Science*, *173*, pp.171-180.

[3]. Yang, G. and Li, C., 2018, December. A design of blockchain-based architecture for the security of electronic health record (EHR) systems. In *2018 IEEE International conference on cloud computing technology and science (CloudCom)* (pp. 261-265). IEEE.

[4]. Fernandes, A., Rocha, V., da Conceição, A.F. and Horita, F., 2020, March. Scalable Architecture for sharing EHR using the Hyperledger Blockchain. In *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)* (pp. 130-138). IEEE.

[5]. Wu, S. and Du, J., 2019, January. Electronic medical record security sharing model based on blockchain. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy* (pp. 13-17).

[6]. Khushalani, J., Chandwani, S., Shaikh, A.S., Talreja, B. and Hande, R., 2020, July. Blockchain: The Novel Way to Secure Confidence! In *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 754-759). IEEE.

[7]. Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M.S. and Rodrigues, J.J., 2018, December. BHEEM: A blockchain-based framework for securing electronic health records. In 2018 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

[8]. Liang, X., Zhao, J., Shetty, S., Liu, J. and Li, D., 2017, October. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC) (pp. 1-5). IEEE.

[9]. Zyskind, G. and Nathan, O., 2015, May. Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.

[10]. Gupta, P., 2019. Usage of Permissioned Blockchain Architecture for Big Data in Electronic Medical Records. arXiv preprint arXiv:1909.01091.