International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 01 | Jan-2021 ISSN: 2582-3930

Medical Record Management with Decentralized Framework

Harshal Jorwekar[1], Atharva Chaudhari[2], Mayuresh Wadgaonkar[3], Shraddha Khonde[4], Deepali Ahir[5]

[1] Student, BE Computer Engineering, MES College of Engineering, Pune
[2] Student, BE Computer Engineering, MES College of Engineering, Pune
[3] Student, BE Computer Engineering, MES College of Engineering, Pune
[4]Assistant Professor, BE Computer Engineering, MES College of Engineering, Pune
[5]Assistant Professor, BE Computer Engineering, MES College of Engineering, Pune

---

Abstract -The mystery between the emotional improvement of medical information protection interest and long periods of administrative guideline has eased back advancement for electronic medical records (EMRs). In this paper, we propose a efficient, secure and decentralized Blockchain system for data privacy preserving and sharing. This manages confidentiality, authentication, data preserving and data sharing when handling sensitive information. We exploit consortium Blockchain and smart contracts to accomplish secure information storage and sharing, which forestalls information sharing without consent. The patient's historical data, medical record, patient's private information is very critical and needs to be stored and maintained securely. The proposed framework builds information security and eliminates the cost, time, and assets needed to deal with the medical care information records.

Key Words:Blockchain, EMR, Security and Privacy, Smart Contracts

1.INTRODUCTION

Health data is highly sensitive and valuable for institutes. It is troublesome for users when they have treatment in different hospitals as before because institutes and hospitals do not share data. The U.S. is poised to spend 20% of its GDP on healthcare in the near future.[2] Focusing on quality health care services means ensuring patient health management at a superior level at all times. However, in the health care sector, critical patient data and information remains scattered across different departments and systems. We cannot deny the possibility of private server data leak for commercial profits.[1],[3] Furthermore, the lack of (correct) information has been considered the primary cause of problems in health care, leading to medical errors and adverse events.[4] The issue of a single point of failure along with data security and patient's privacy risk prevailing still exist in cloud-based systems. According to the statistics provided by the Health Insurance Portability and Accountability Act (HIPAA), 13,236,569 medical records were breached in 2018 which were as twice as compared to 5,138,179 records breached in 2017.[5]

2. BLOCKCHAIN TECHNOLOGY

Blockchain is a Decentralized, Distributed network. It is a data structure where each block is time-stamped chronological order and linked to another block. It is a distributed digital ledger that records transactions in a growing chain of immutable blocks linked by cryptographic hashes. Each participant verifies the transaction by a majority consensus of the system participants. This ensures the tamperproof property of transactions once they are packed into the Blockchain. In regards to immutability of Blockchain, a same copy of the ledger is replicated, hosted and maintained by all participants. All data on the ledger is verifiable and auditable but cannot be edited. There are different types of Blockchain:

- Public Blockchains: Every member can access the Blockchain content and could take part in the consensus process.
- Private Blockchains: Dedicated to a specific group of organizations where only selective members have access to the chain.
- Consortium Blockchains: A consortium blockchain is a permissioned network and public only to a privileged group.
- Hybrid Blockchains: Combination of Public and Private Blockchain.

2.1 Features of Blockchain

1) Consensus Mechanism: Blockchain is a peer-to-peer distributed network. Transaction is generated and stored in a block. Each digitally signed block is sent to the mining pool where it is taken over by network nodes called miners and verified using the consensus algorithm. The consensus algorithm allows the community to make sure that every added block is legitimate.
2) Decentralization: In Decentralized Systems resources are owned shared by network

members and it is difficult to maintain since no one owns it. In Decentralized system each member has exact same copy of distributed ledger. Decentralized system has extremely high fault tolerance. In Decentralized system no one controls or no one owns data. Security increases as the number of network members increase in Decentralized network.

3) Immutability: Blockchain is immutable and tamper proof thus ultimately provides security to the system. According to the transactions in block it proceeds using a hash value or cryptographic hash key. Cryptographic hash is generated on the transactions in the block. Hash value has an alphanumeric string generated by each block distinctly. Hash function makes the system as a tamper resistant ledger.
4) Smart Contracts: A smart contract is a computerized computational logic or term of the contract. Transactions are automatically triggered between parties after fulfilling encoded logic. Main aim of smart contract is to automatically execute the term of argument once the specified conditions are met.

2.2 Component of Blockchain

1) Transaction: A process that is used to change the state of the Blockchain ledger. The transaction can be the execution of a smart contract or Depending on the application, the transfer of any valuable asset.
2) Block: It consists of a number of transactions which are supposed to be added to the Blockchain network. Its architecture includes a block header and a block data.
3) Merkle Tree Root Hash: A hashing algorithm is used to hash all the transactions in the block. The hash values are then combined and are hashed again to obtain a single hash value known as Merkle tree root hash value.
4) Nodes: Nodes can be defined as the participants in the network. A typical Blockchain network has three different type of nodes namely, simple node, full node and mining node.
5) Mining: It is the process of adding the valid transactions in a block and broadcasting that block to the network.
6) Genesis Block: This is the first block in the Blockchain network to which all the following blocks in the chain are linked. It does not have any parent block.
7) Public and Private keys: A user requires a pair of public and private keys to propose a transaction, get it validated and added in the block. The public key is known to everyone in the network whereas the private key is only known to the user

3.BLOCKCHAIN IN HEALTHCARE

The inclusion of Blockchain in the healthcare industry is divided into a number of stages. The first stage includes tracking and storage of the clinical data into existing health IT systems. The healthcare providers, using Patient IDs transmit the patient's data to the Blockchain network as they have direct connection to the Blockchain network. A smart contract is then used to execute the inward transactions. All the transactions in the Blockchain network are committed using patient public IDs. These transactions do not contain the patient's personal information. The blocks are then created and added to the immutable ledger which makes all the transactions unique. Only non-identifiable patient data such as gender, age, and illnesses is stored in the database of blocks. Clinical data is analyzed to uncover new insights. The patient can share his/her identity with the healthcare provider using the private key. This is how the healthcare provider is able to access the patient's data for identifying the symptoms and provide solutions or care. Thus, the data remains confidential to those who do not have the private key of the patient.

4. PREVIOUS WORK

Various attempts have been made to apply the Blockchain technology in E-health systems in recent years having different architecture. Each of them uses a different Blockchain, algorithms and Encryption techniques which results into varying evaluation metrics like performance, latency, throughput, etc. Network security being one of the major concerns is also determined by the above-mentioned factors. It becomes difficult to compare these systems because of their varying approaches. The relative comparison of the state of-the-art Blockchain-based approaches to secure EHR systems is given in Table 1. Advantages of Blockchain in Healthcare: Distributed ledger: Transactions are appended in a distributed system on the network, which creates system recovery by eliminating a single point of failure or centralized entity. Provenance: The complete data or asset's history is available on the Blockchain network. Immutability: All information is secure and trusted as the Records on the network cannot be modified or tampered with. Finality:

A transaction cannot be modified or reversed once it is committed on a Blockchain.

5. PROPOSED SYSTEM

We base our system on the IPFS service which is a decentralized platform. IPFS integrates Merkle Linked structure with the data addressability of P2P file sharing systems. We plan to store the actual medical records on a decentralized cloud storage Each medical record will

Table -1: PREVIOUS WORK

Author	Blockchain	Encryption	Architecture	Consensus
Jiang S.et al. [8]	EMRChain and PHDChain	MD5	Dual Chain	Proof-ofWork (PoW)
Tanwar S. et al. [7]	Hyperledger Fabric	Symmetric Key Cryptography	Patientcentered	Solo and Kafka
Hylock RH, Zeng X. [9]	HealthChain	Proxy ReEncryption	Distributed PatientCentered	Proof-ofConcept(PoC)
Shahnaz A. et al. [6]	Etherum and IPFS	-	Dual Chain	Proof-ofWork(PoW)

have aunique hash which will be combined with the decryption key. We also plan to include Versioning control mechanism. The approach we will be using for this project could be as follows:

1) 1)The user will add their personal information, health records and medical history.
2) 2)Hospital authority will submit the patient will be appended with the patient existing history.
3) 3)A transaction will be generated which will be added to a block. That block will then be added appended to the existing chain.
4) 4)The user can then access the data according to his will

6. CONCLUSIONS

This paper presents a survey of approaches to overcome limitations like scalability, security and privacy in healthcare management system using Blockchain technology which can revolutionize the whole ecosystem. We also have demonstrated an innovative approach for integrating with existing systems and prioritizing network structure transparency.

REFERENCES

[1] Keke Gai, Yulu Wu, Liehuang Zhu, Lei Xu, Yan Zhang, Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks, IEEE Internet Things J. 6 (5) (2019) 7992–8004.
[2]https://www2.deloitte.com/content/dam/Deloitte/global /Documents/Life-Sciencs-HealthCare/gx-lshc-hc-outlook2019.pdf
[3] Liu Ziqi, Chen Chaochao, Yang Xinxing, Zhou Jun, Li Xiaolong, Song Le, Heterogeneous graph neural networks for malicious account detection, in: Proceedings of the 27th ACM International Conference on Information and Knowledge Management, in: CIKM '18, ACM, New York, NY, USA, 2018, pp. 2077–2085.
[4] CRICO. 2015. Malpractice Risks in Communication FailuresURL: https://www.rmf.harvard.edu/Malpractice-Data/AnnualBenchmark-Reports/Risks-in-Communication-Failures
[5] Healthcare Data Breach Statistics. Accessed: Jun. 11, 2019. [Online]. Available: https://www.hipaajournal.com/healthcare-databreachstatistics/
[6] Shahnaz, A., Qamar, D. U., Khalid, D. A. (2019). Using Blockchain for Electronic Health Records. IEEE Access, 1–1.
[7] Tanwar, S., Parekh, K., Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407.
[8] Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., He, J. (2018). BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange. 2018 IEEE International Conference on Smart Computing (SMARTCOMP).
[9] Hylock RH, Zeng X A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study J Med Internet Res 2019;21(8):e13592.