Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Blockchain based Implementation of Healthchain

Nishma K
Department of Computer Science and Engineering
AWH Engineering College
Kozhikode, India

Divya M
Department of Computer Science and Engineering
AWH Engineering College
Kozhikode, India

***Abstract*— Medical care has been an indispensable part of our lives and so the medical data such as prescriptions, previous medical records has also become a vital part for patient's diagnosis and for further proceeding. Traditionally, medical data were recorded on paper, which were prone to get damaged and modified. Therefore, it was necessary to preserve the data electronically. So we introduce Healthchain, A blockchain-based privacy preserving scheme for health data. health analyzers can diagnose anytime and anywhere based on the Health data and publishes the diagnosis as a transaction. We also introduce Inter Planetary File System(IPFS) which is a content addressable, distributed file system to store data with high integrity and resiliency.**

Keywords:-Blockchain, Health Analyzer, Content Addressable, Distributed File System, Interplanetary File System

1. INTRODUCTION

Technology always plays a very significant role if it is about enhancing the quality or about resolving issues such as resource allocation along with information blocking, here in medical-care data sharing technology needed to be evolved with time.Generally,patients may havea lot of service providers in terms of medical healthcare that include general physicians or specialists or even therapists. Since a disease could be because of the previous disease, so they all need to share health record securely without any manipulation. Patient need not be always a professional or to have a good memory to remember all the data properly if all the data are stored and shared securely.patients need to keep updating their own medical data history.So we use blockchain based technology to protect the health data

The blockchain technology provides a public, digitized and distributed ledger, which is firstly proposed by Nakamoto [8]. It has been widely used in cryptocurrency transactions such as Bitcoin [8] and Ether [9]. Meanwhile, it has also become the key technology for various IoT scenario for more innovations. All nodes in the blockchain construct a Peer-to-Peer (P2P) network to interconnect with each other. All participating nodes are equal and collaboratively provide services without a single central point, which can avoid the risk of singlepoint bottleneck. The blockchain consists of a series of blocks and grows over time, in which each block mainly contains a hash of its previous block, a timestamp, a nonce, and some transactions. A transaction records the data that a user wants to add to the blockchain, and new transactions are broadcast to other nodes. Some nodes collect new transactions into a block. The method to add a block to a blockchain is determined by a specific consensus mechanism. Nodes accept the block only if all transactions in it are valid. Once a block is added to the blockchain, it cannot be tampered with under certain security assumptions. The blockchain cannot be forked and all nodes keep working on its extension

In this paper, we propose Healthchain, a blockchain-based privacy preserving scheme for health data. In Healthchain, users can periodically upload the health data publish them as a transaction. Doctors or artificial intelligence (AI) health analyzers can diagnose anytime and anywhere based on the IoT data and publishes the diagnosis as a transaction. In fact, with the explosive growth of the Internet of Things devices, there will be large-scale health data and these health data will continue to increase. It is not appropriate to record users' complete data on the blockchain, as resource requirements for each node on the blockchain will be extremely high. Otherwise, the blockchain will be too complex to maintain, search and verify. Considering the limited storage capacity of each blockchain node, we introduce InterPlanetary File System (IPFS), which is a content-addressable, distributed file system to store data with high integrity and resiliency. There is no central server in IPFS, and data are distributed and stored in different IPFS nodes all over Internet. Thus, IPFS has no single point of failure. IPFS can efficiently distribute large amounts of data without duplication [7]. Each file uploaded to the IPFS system has a unique hash string through which the file can be retrieved. In our proposed Healthchain, users' complete health data is stored in IPFS storage system. Only hash string of health data, stored in blockchain, is used to verify data's integrity and map to the complete data in IPFS storage. In this way, Healthchain supports large-scale health data and has good scalability.If a user is not satisfied with the current doctor decision so user can revoke to another hospital specialists so the health analyzer will share the information to other hospital

2. RELATED WORK

people are increasingly hoping to get more accurate, comprehensive and efficient health information about themselves, and meanwhile their personal privacy can be well preserved. With the development of information and communication technology (ICT), and cloud computing, many research efforts have been devoted to improving the efficiency and security of smart healthcare systems.

Jie Xu et al[1] proposed Blockchain-based Privacy Preserving Scheme for Large-scale Health Data where health data are encrypted to conduct finegrained access control. Specifically, users can effectively revoke or add authorized doctors by leveraging user transactions for key management. Furthermore diagnosis cannot be deleted or tampered with so as to avoid medical disputes. Security analysis and experimental results

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

show that the proposed system is applicable for smart healthcare system

Zhang et al [2] Proposed a novel patient-centric framework ie, PASH, a privacy-aware s-health access control system, in which the key ingredient is a large universe CP-ABE with access policies partially hidden. CP-ABE schemes can be directly adopted to design fine-grained access control systems, it is still necessary to simultaneously address the issues of policy hiding, decryption test, large universe, full security and policy expressiveness in CP-ABE to ensure its secure and efficient applications in s-health but internal malicious attacks and cloud server crashes.

Al et al. [3] presented a user centric healthcare data privacy preserving scheme called MediBchain. In MediBchain, users encrypt sensitive health data and store them on permissioned blockchain. Only users with the correct password can get data from MediBchain. However, users must share passwords when sharing their health data, which can conduct a coarsegrained access control, but it may lead to key leaks easily. MediBchain lacks password update and key update schemes. Moreover, MediBchain is vulnerable to replay attacks and offline dictionary attacks.

Azaria et al[4] propose MedRec:A novel, decentralized record management system to handle EMRs, using blockchain technology. Our system gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Leveraging unique blockchain properties,MedRec manages authentication, confidentiality, accountability and data sharing– crucial considerations when handling sensitive information. A modular design integrates with providers' existing, local data storage solutions, facilitating interoperability and making our system convenient and adaptable. We incentivize medical stakeholders to participate in the network as blockchain "miners". This provides them with access to aggregate, anonymized data as mining rewards, in return for sustaining and securing the network via Proof of Work.Blockchain implementations still grapple with how best to scale the technology for high transaction volume. This may affect our system, determining the natural size of each MedRec.

Kassab et.al[6] developed a research on blockchain technology and how blockchain is being utilized in the sphere of healthcare, healthcare is a data-intensive domain, once a considerable volume of data is daily to monitoring patients, managing clinical research, producing medical records, and processing medical insurance claims.While the focus of applications of blockchain in practice has been to build distributed ledgers involving virtual tokens,the impetus of this emerging technology has now extended to the medical domain. With the increased popularity, it is crucial to study how this technology accompanied with a system for smart contracts can support and challenge the healthcare domain for all interrelated actors (patients, physicians, insurance companies,regulators)and involved assets (e.g.patients' data, physician's data, equipment's and drug's supplychain).

3. PROBLEM DEFINITION

The biggest challenge that is being faced by health care systems throughout the world is how to share medical data with known and unknown stakeholders for various purposes while ensuring data integrity and protection patient privacy. Although data standards are better thanever, each electronic health record(EHR) stores data using different workflows ,so it is not obvious who recorded what, and when and hence Creating a trusted environment for decision making is a challenge for medical fraternity.The growing focus oncare coordination and EHR access across the care continue has raised questions about how to ensure that multiple providers can view, edit, and share patient data while still maintaining an authoritative and up-to-date record of diagnoses, medications, and services rendered.

4. PROPOSED SYSYTEM

Our proposed system, which can be divided into five layers. As shown in Fig.1, from bottom to top, these five layers are given as: Data layer, Network layer, Consensus layer, Incentive layer, and Application layer.

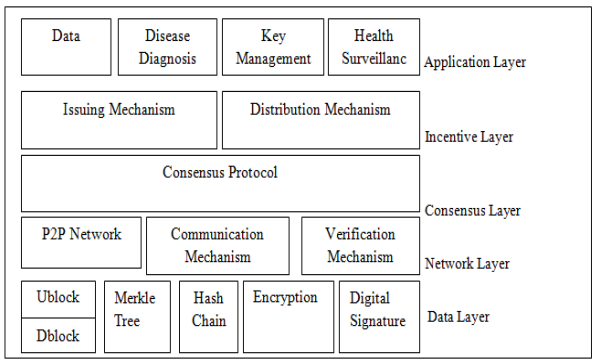

Figure 1:The Architecture of Healthchai

Data layer

There are two main data structures in data layer: Ublock and Dblock, and a few cryptographic algorithms(AES,SHA 256). Userchain consists of Ublocks, where each Ublock contains information about users.Each Ublock can be divided into two main parts: block header and block body. The block header contains an index Index, a timestamp Gtime, a hash of the previous block prehash, a nonce nonce, and a root of the merkle tree userroot. The merkle tree, as the block body in a Ublock, contains hash values of user transactions. Docchain is composed of Dblocks. Similarly to Ublock.

Network Layer

Provide verification and communication mechanisms to the blocks done by Accounting node. It's a special node in the system, which is deployed by the consortium. It can verify that whether the transactions from doctor nodes are correct and valid. At each time period, all accounting nodes select a leader. The leader aggregates valid transactions from doctor nodes in the consortium, and generates new Dblock and adds new Dblock to Docchain.

Consensus Layer

The consensus mechanism determines when and which node adds a new block to the blockchain for the transaction it receives. Because Userchain is a public blockchain, and Docchain is a consortium blockchain, the two blockchains have their own consensus in Healthchain. Userchain is a public blockchain, anyone can send and aggregate

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

transactions. A malicious user node may masquerade as several user nodes at a low cost, known as Sybil attack. However, other users cannot distinguish whether it is a Sybil node or a real user. This makes it difficult to fairly select a core user node to add a new block to Userchain. We choose the consensus mechanism of Proof of Work (PoW) to select a core user node to aggregate users' transactions, generate a new Ublocks and add it to Userchain. Docchain is a consortium blockchain, only accounting nodes authorized by the consortium can aggregate transactions generated by permissioned doctors and add Dblock to Docchain. Instead of relying on the computationally intensive consensus mechanism PoW we choose Practical Byzantine Fault Tolerance (PBFT) [7] as the consensus of Docchain

Incentive layer

In order to promote more users to continue to participate in Healthchain, economic factors are considered in the incentive layer. We introduce Healthcoin to Userchain as an incentive token Healthcoin is consumed when the doctor's diagnosis transaction is successfully added to Docchain. Doctor node gets rewards from the consortium based on transactions he/she adds to Docchain.

Application layer

The topmost application layer provides different services for users and doctors. Specifically, data security, key management, and disease diagnosis can be provided in our scheme

we briefly show data flows of our system shown in fig 2 User health data to the user node periodically or on event triggers. The user node encrypts the health data and sends them to an IPFS storage node. User node adds the hash of the encrypted data as a transaction to Userchain. The doctor node decrypts the users' data and gives real-time online diagnoses. Then the doctor sends the encrypted diagnosis to the storage node and generates a transaction for diagnosis which includes the address of the encrypted diagnosis. Users read the information on Docchain to understand their own health status.

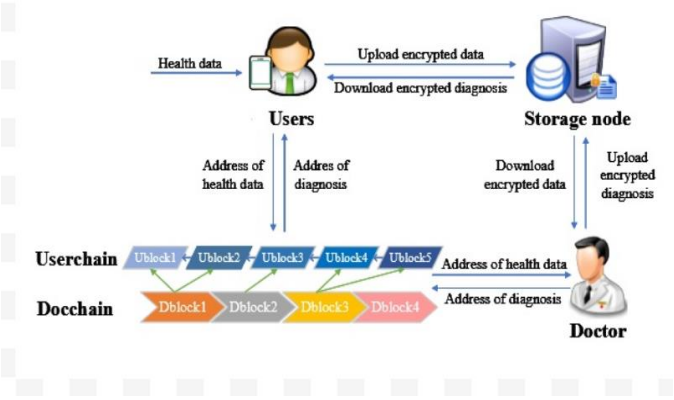

Figure 2: System Model Of Healthchain

5. EXPERIMENT SETUP AND RESULT

In proposed method we have 3 users are available ie, Patients, doctors and Lab. Patients will register with the application and then create profile and give access to doctors. Doctors will register with the application and then login and access all those patients' records who gave permission to this doctor. Doctor will add prescription to patient profile. Lab person will login to application using username and password and after login he will upload reports of patients. Patients can login and download or view reports based on filtration .To store patient medical records using blockchain technology as its provide inbuilt support to secured at a store in it. To store details we are using blockchain Ethereum tool [9].

Ethereum[9] is a decentralized software platform that has functionality like smart contract and distributed applications to be built without any downtime, error, fraud or third party interference. it possess smart contract functionality, it is a computer code where we can write what kind of operations we want to perform and also errors can be easily identified it can be installed from the official ethereum platform with an windows/mac version and geth is installed which is a multipurpose command line tool which serves as a ethereum full node in blockchain. Ethereum is better than other bock chain platforms because here user can create whatever operations he wants to perform with this ethereum functionality and errors are also easily identified.

Ganache-cli which is the most widely used local test node by Ethereum developers. Ganache is a personal blockchain for Ethereum development you can use to deploy contracts, develop your applications, and run tests.

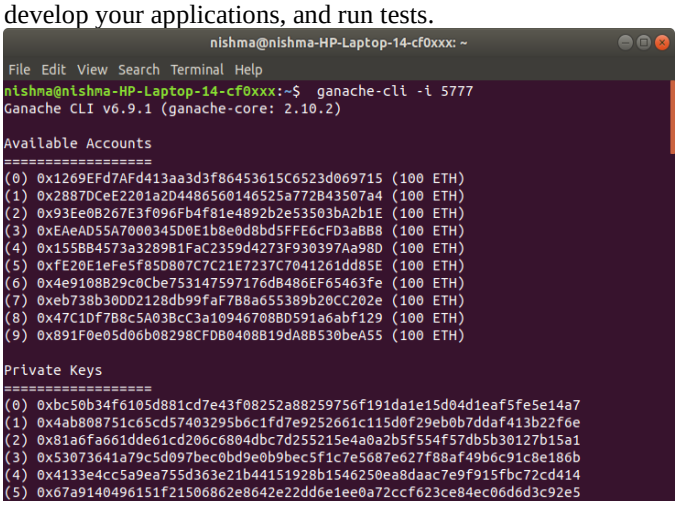

Figure 3:Screenshot 1

Copy and paste the any one of the above available account address into app.js then save the file and compile the truffle function in a terminal. Open the browser and enter URL as http://localhost:3000 to get below screen

Figure 4 :Screenshot 2

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

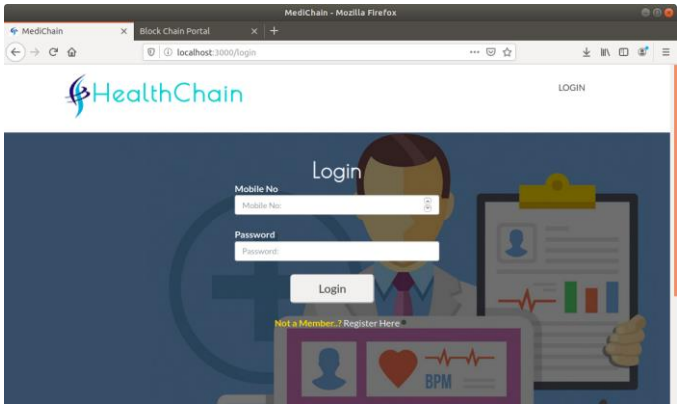

Figure 5:Screenshot 3

Registered patient can login the page otherwise register has a new user.

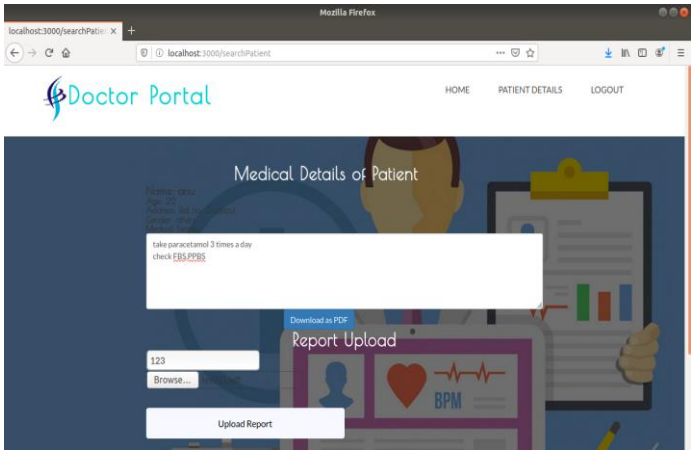

Figure 6:Screenshot 4

The patient information is uploaded into IPFS and hash keys is stored in blockchain .When user want to get the reports enter the mobile number then enter view report a hash key will be displayed.

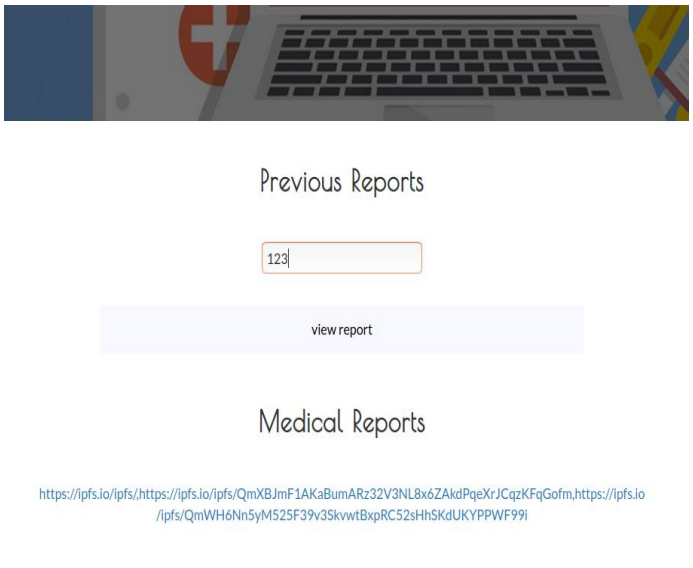

Figure 7:Screenshot 5

While clicking the link we get the complete health data of a patient. Patient can also share their health data to other doctor from the different hospitals.

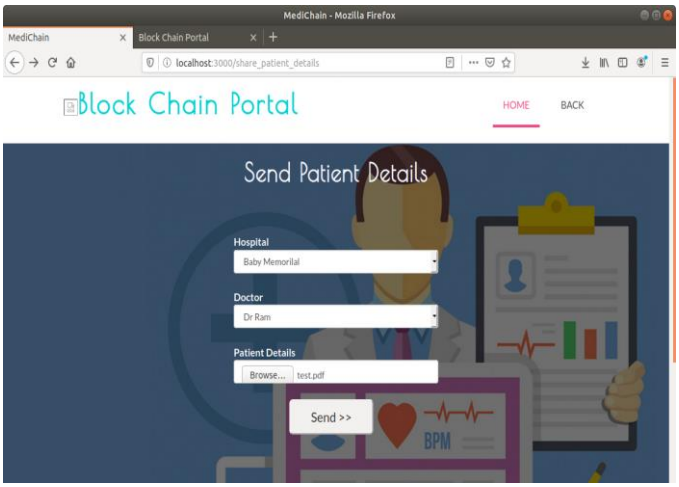

Figure 8:Screenshot 6

6.CONCLUSION

Healthchain is a data-intensive discipline in which large scale data is generated, disseminated, stored, and accessed daily. we proposed a privacy-preserving scheme for fine-grained access control of large scale health data based on blockchain.We introduced two blockchains to ensure that both users 'health data and doctors 'diagnoses cannot be tampered to avoid medical disputes..In Healthchain, users' complete health data is stored in IPFS storage system. Only hash string of health data, stored in blockchain, is used to verify data's integrity and map to the complete data in IPFS storage. In this way, Healthchain supports large-scale health data and has good scalability. Each file uploaded to the IPFS system has a unique hash string through which the file can be retrieved. which can also efficiently reduce communication overhead and computation overhead while ensuring privacy preserving, Healthchain can allow users to dynamically revoke doctors and update keys at anytime .Healthchain is efficient and feasible in practice.

This work can be extended further Along protecting the medical data blockchain also used a way to reward patients.If patients stay healthy keep their appointments and follow their care plans, they may be rewarded through the blockchain. If a patient is not satisfied with an hospital we can generate a consortium between hospital so we can provide a good services to patients. Using Deep Learning can help in the following clinical predictions by doctor: Medical codes, clinical notes, Time series data, Medical scans, etc.

REFERENCES

[1] Jie Xu, Kaiping Xue, Shaohua Li, Hangyu Tian, Jianan Hong, "A Blockchain-based Privacy Preserving Scheme for Large-scale Health Data" pp. 2327-4662 ,2019 ,IEEE

[2] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attributebased access control," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2130–2145, 2018.

[3] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," IEEE Communications Magazine, vol. 56, no. 7, pp. 82–88, 2018.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

[4] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in Proceedings of 2017 International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, 2017, pp. 534–543.

[5] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in Proceedings of 2016 International Conference on Open and Big Data (OBD). IEEE, 2016, pp. 25–30.

[6] Kassab, M. H., DeFranco, J., Malas, T., Laplante, P., Neto, V. V. G., et al. (2019).Exploring research in blockchain for healthcare and a roadmap for the future. IEEE Transactions on Emerging Topics in Computing.

[7] N. Nizamuddin, H. R. Hasan, and K. Salah, "IPFS blockchain-based authenticity of online publications," in International Conference on Blockchain. Springer,2018, pp. 199–212.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[9] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.