RESEARCH ARTICLE OPEN ACCESS

Health Block: A Privacy Preserving Framework for Medical Records

Laya Chacko[1], Bibin Varghese[2], Smita C Thomas[3]
[1](PG Scholar, Computer Science and Engineering, Mount Zion College of Engineering, Kadammanitta)
[2](Assistant Professor, Computer Science and Engineering,Mount Zion College of Engineering,India)
[3](ResearchScholar, VelsUniversity, India.)

--************************----------------------------------

Abstract:

The limited computing power and storage capacity of IoT devices, user's health data are generally stored in a centralized third party, such as the hospital database or cloud, and make users lose control of their health data, which can easily result in privacy leakage and single-point bottleneck. Dramatically increasing deployment of IoT monitors health data to achieve smart healthcare which received more attention now a days. Blockchain based privacy preserving of large scale health data called HealthBlock with finegrained access control. Users can easily revoke and add doctors by using user's transaction for key management. Furthermore, by introducing HealthBlock, both IoT data and doctor diagnosis cannot be deleted or tampered with so as to avoid medical disputes.

Keywords – **Privacy Preserving, BlockChain, Internet of Things,**

--************************----------------------------------

I. INTRODUCTION

The Internet of Things (IoT) is an emerging and promising technology that connects a large number of smart devices to the Internet, where devices collect and exchange data to help people. Smart healthcare based on IoT which improves the efficiency, accuracy, and achieve remote monitoring. IoT devices, such as wearable sensors, keep collecting user's physiological data, such as electrocardiogram (ECG), blood pressure, temperature. For example, a smartphone-based wireless body sensor network to collect user physiological data using body sensors embedded in a smart shirt. These physiological data are send to further data processing, aggregation, and then sent to a healthcare provider for diagnosis and feedback, so that users can further better understand their own health status. Compared with traditional health system cloud-assisted healthcare system improves efficiency and reduces cost. However, still have many drawbacks in the system. Large-scale smart health devices require high computing and storage capabilities of cloud servers. Since cloud storage and computing can also be seen as centralized to a certain extent, once cloud servers break down or are attacked, all users might be affected. Health data is highly sensitive and should be well protected. Cloud server may leak user privacy for commercial benefits. Besides, it is difficult to share data stored in cloud among different platforms with specific access control policies. In this paper propose a blockchain based privacy preserving HealthBlock. IoT devices collects users health related data periodically and publish them as transaction. Health analyzers can diagnose anytime and anywhere based on the IoT data and publishes the diagnosis as a transaction. Due to the tremendous growth of IOT devices, It is not appropriate to record user's 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.InterPlanetary File System (IPFS) solves storage problem apart from these it only interact with the private IPFS.

II. LITERATURE SURVEY

In recent years, many studies have shown that blockchain is a promising solution to achieve personal health information security and privacy protection. To demonstrating the advantages of smart healthcare systems based on blockchain and propose architectures, but lack specific implementation details. Focus on fine-grained access control of IoT data collected from users. However, they do not further consider the privacy protection of electronic medical records (EMRs)[3] generated by the doctors. In addition, some schemes are dedicated to utilizing blockchain technology to enable users to control their EMRs, which are controlled by the hospital in traditional smart healthcare systems. A user centric healthcare data privacy preserving scheme called MediBchain[4]. 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 coarse grained 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. After that, secret sharing to authenticate users and doctors for fine-grained access authorization. However, EMRs are stored in a blockchain, and the blockchain is maintained in a trusted cloud, which leads to centralization. The literatures can achieve health data mastered by users, but as the number of users and the volume of health data increase, due to the limited size of blocks, these schemes may lead to intolerable authentication delay and storage. In order to reduce the storage overhead and improve the throughput of the blockchain, medical records are stored in external databases, and the pointers to external databases for medical records and reading permissions are stored in smart contract on the Ethereumblockchain. Recently, blocks are used to store hash values of medical records while sending the actual query link information in a private transaction over HTTPS.

III. PROPOSED SYSTEM

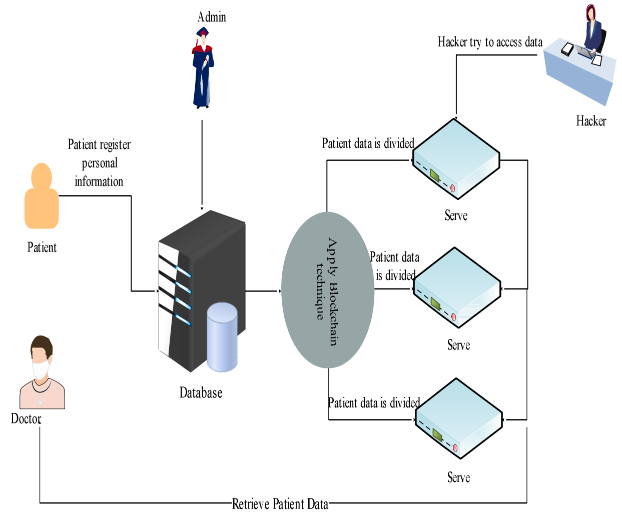
In this paper, proposed a blockchain-based smart healthcare architecture, named HealthBlock. HealthBlock can be divided into several different components: IoT devices, Doctor Node, User nodes, Accounting node, Storage nodes, Userchain, Dochain. User transaction based on the two keys: IoT transactions and key transactions. IoT transactions are used to protect the integrity of IoT data, and key transactions are used for access control. The main part of an IoT transaction is a hash of encrypted IoT data, which can be used to address encrypted IoT data at IPFS nodes. The main part of a key transaction is two symmetric keys: one called IoT key for encrypting/decrypting IoT data and the other called diagnosis key for encrypting/decrypting diagnosis. Both symmetric keys are generated by the user and encrypted with the authorized doctor’s public key. An authorized doctor obtain two symmetric keys to decrypt user’s IoT data or encrypt diagnosis by decrypting the key transaction.

Transactions on Docchain called diagnosis transaction encrypted with user’s diagnosis key. To generate a diagnosis transaction, the authorized doctor node first searches Userchain for transactions of the users they are responsible for. If it is a key transaction, the doctor node updates the stored keys for encrypting/decrypting IoT data or diagnosis. If it is related to IoT data, the doctor node goes to the IPFS system to get the complete IoT data based on the hash of user’s IoT data in the IoT transaction. Then, the doctor node generates corresponding diagnosis for the user based on the IoT transactions in a timely manner. The doctor node encrypts the diagnosis and stores it to IPFS system. The doctor node further generate a transaction including a hash of the encrypted diagnosis, and then broadcasts the diagnosis transaction to nodes involved in Docchain.

Accounting nodes collect diagnosis transactions and add them to Docchain.

After receiving the latest IoT data from IoT devices, the user node periodically encrypts the IoT data and generate IoT transactions. Doctor nodes may be compromised and leak user's key, the user needs to be able to revoke a doctor at any time and in time. In addition, depending on the need of the user, the user may need to add doctors dynamically. By publishing a new key transaction, this scheme allows users to dynamically add or revoke doctors at any time. When the user establishes contact with a new doctor, the user generates a key transaction contains the current IoT key and a diagnosis key issued to the additional doctor. When a user needs to revoke a doctor, the user first generates a new IoT key. Then, the user publishes a new key transaction, which only contains digital envelopes issued to the currently authorized doctors. Digital envelopes contain the updated IoT key. Therefore, the revoked doctor does not have the new IoT key, and can no longer read the user's data. Key transactions and IoT transactions decoupling can reduce both communication overhead and computational overhead for both users and doctors.

The doctor node continuously detects whether there is a transaction on Userchain, which is the identity of the user they are responsible for. Once detected, the doctor first goes to the consortium to check whether the user has paid enough Healthcoin. If so, the doctor performs the following steps. If the transaction is a key transaction, then the doctor updates the user key in time. If the transaction is IoT transaction, the doctor uses the hash contained in the IoT transaction to IPFS storage node to obtain complete IoT data. Then, the doctor node gives the corresponding diagnosis based on the IoT data. Next, the doctor generates a diagnosis transaction. Finally, diagnosis transaction is sent to the accounting nodes and added to Docchain.



In this approach the main focus is on private blockchain where data is decentralized but the access rights is given by a centralized authorities which give rise to the problems like data privacy, data modification, etc. because it do not use proof of work which are the very hard mathematical problems to solve to get the permission rights to modify in the data. To solve this problem the in private blockchain the rights to access given by centralized authority but read and write rights is also restricted for the users from where the can read the data and where they can write. As the data is divided into different servers the user which have right to access the data can directly get the data from this decentralized servers but he cannot modify that data. The data can be only monitor by the administrator. If in case some third party like hacker try to modify in and particular server the rest of the servers gets disable and the data which the hacker will be in double encrypted form which is very difficult to crack the data as the data is in double encrypted hash value. To generate the hash value AES algorithm is used and pailliers is applied on that AES hash value for re-encryption. The user will get the Email that someone have try to change the data with the MAC address and IP address on that device. The main focus is to secure the data of patient from any malfunctioning.

IV. CONCLUSION

This Approach have focus on the security concerns of the private blockchain by making it more secure for data privacy and by giving access control to the authenticated users only who have permission for rights, i.e. read, write and update as per their role. This approach maintains CAI assessment factors, i.e. the availability, integrity and confidentiality. The use of blockchain can come to an end because of quantum computers. In future the scope of this approach can be enhance by working on the prevention of the attacks like DOS Sybil, etc.

REFERENCES

[1] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, "HealthDep: An efficient and secure deduplication scheme for cloud-assisted ehealthsystems",IEEETransactions on Industrial Informatics, vol -14, pp: 4101–4112, 2018.

[2] J. Hua, H. Zhu, F. Wang, X. Liu, R. Lu, H. Li, and Y. Zhang, "CINEMA: Efficient and privacy-preserving online medical primary diagnosis with skyline query", IEEE Internet of Things Journal, 2018.

[3] 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, pp: 25–30, 2016.

[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, pp: 534–543, 2017.

[5] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacypreserving and efficient aggregation based on blockchain for power grid communications in smart communities", IEEE Communications Magazine, vol- 56, pp: 82–88, 2018.

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

[7] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications", Journal of the American Medical Informatics Association, vol- 24, pp: 1211–1220, 2017.

[8] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks", IEEE Internet of Things Journal, 2018.

[9] C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Du, and M. Guizani, "LPTD: Achieving lightweight and privacy preserving truth discovery in CIoT", Future Generation Computer Systems, vol- 90, pp: 175–184, 2019.

[10] G.Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacypreserving framework for access control and interoperability of EHR usingblockchain technology", Sustainable Cities and Society, vol-39, pp: 283–297, 2018.

[11] 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, pp: 2130–2145, 2018.