Hyperledger blockchain based secure storage of electronic health record system in edge nodes

Hyperledger blockchain based secure storage of electronic health record system in edge nodes

P Arul[1] and S Renuka[1,*]

[1] Department of Computer Science, Government Arts College (Affiliated To Bharathidasan University, Trichy-24), Tiruchirappalli-620 022, India.

[*]spkumarrenu@gmail.com

Abstract. An Electronic Health Record (EHR) is a database for storing patients medical information collected from different sources such as smart wearable devices, smart sensors and diagnostic imaging equipment. An EHR contains sensitive private information for the patients and the treatment of their diseases. Furthermore, it's often shared among different members consists of healthcare providers, insurance companies, medical researchers, and others. The main difficulty for EHR information management is the result of gathering, storing, and sharing patient healthcare without affecting privacy and security. Blockchain has recently proposed an efficient way to manage EHR data. This paper provides hybrid architecture for EHR data management by using both Hyperledger blockchain network in on-chain and edge node in off-chain. In this architecture is used to authenticate user without affecting sensitive patient's information and also used to authenticate the encrypted EHR information in edge node. In the on-chain approach EHR activities and Patient authentication activities are recorded in the blockchain for the purpose of accountability and traceability. Edge nodes stored the encrypted EHR data in the off-chain method. So the combination of on-chain and off-chain approaches only allows the authorized data user who has to meet the EHR access activities and to decrypt the EHR data. If the EHR information is alter by an unauthorized user, the hash code is newly generated which is different from old hash code stored in the blockchain. As the result the user can easily detect that their EHR information has been hacked.

1. Introduction

According to Health Insurance Portability and Accountability Act (HIPAA) in Europe, Healthcare hacking incidents increased by 42% in 2020, continuing a 5-year that has seen hacking incident rise each year [1]. At the same time EHR information will have grown at 48 percentage per year, reaching 2,314 ZB (ZettaBytes). Specifically in EHR management, each patient has a profile containing personal information and medical history. Therefore gathering, storing, and sharing patient's information without interrupt privacy or compromising security is a major difficulty for EHR management. Although healthcare practitioners like physician, nurses, medical laboratory scientists, pathologists, and others must verify patients in EHR system [2]. Furthermore, patients' healthcare data must be protected, and patients must set an access policy that specifies who has the authorization to access what data. The blockchain is the best approach to share and store the information of a healthcare institution securely with time-stamped [3]. Blockchain distributed ledger has reduced the

costs for verifying transactions by removing the need for reliable third parties such as central authority. The decentralized nature of a blockchain, all the events and activities would be transparent to all the participants. However, the following challenges must be addressed to utilize the blockchain-based EHR management. First, because of the distributed and transparent character of blockchain, patient identification and sensitive details could not be able to store directly in blockchain. The size of blocks is a second factor to consider. The blocks of blockchain is typically too small in size to handle EHR data containing X-rays, CT scans, MRI scans, and ultrasound videos. This paper proposes hybrid blockchain edge architecture to protect data owners' privacy information and secure EHR data. In on-chain Hyperledger Fabric blockchain [11] executes smart contracts to provide patient authentication while maintaining EHR access records. Furthermore in edge node, the encrypted EHR information is stored by off-chain method, which can only be decrypted by healthcare practitioners who has meet the access policy [4]. Thus in on-chain method, the verification of patients and EHR entry activities are stored and maintained by the blockchain. In EHR management a blockchain's tamper-proof register maintain authenticate of the patients and the event of user's EHR data. If the patient's account has been hacked, this system will be traceable the attacker's activities and find the altered data. To make EHR maintenance easier this system proposes a hybrid method of hyperledger fabric blockchain(HFB) with edge nodes.

2. Related work

Damiano et al [5] proposed blockchain technology that assures the verification of access control policies evaluation, these policies and their attribute are assigned by smart contract organized by the blockchain technology. Rui Guo, Huixian Shi et al [6] proposed the 'Multi Authority Attribute Based Signature' (MAABS) for distributed EHR scheme. In this scheme, a user is validated according to their attribute while disclosing no other interrelated data other than the proof of the patient has need to verify by it. QI Xia, Sifah et al [7] proposed the 'Medshare: Trust-less medical data sharing among cloud service providers via blockchain' is a blockchain based technology for distributing medical related information in cloud sources between different big data. In this system, Smart contracts were used to implement access control strategies on medical data. Wang, Zhang et al. [8] proposed blockchain based architecture for data sharing in a distributed storage platform, which utilized both Ethereum smart contract and ABE and the keyword search purpose on the ciphertext of the distributed storage system is also implemented in their scheme. Guo, Meamari et a l[9] proposed a 'Multi authority attribute based access control mechanism' by using Ethereum's smart contract. Zghaibeh et al. [10] proposed the user friendly graphical interface Smart-Health, which is a private multilayered blockchain system combined with a multi addressing system that defines the rights and permissions of entities in the system. This Smart Health proposed the smart contracts with complete independence to patients such as medical activities or the history.

3. Electronic Health Record with Blockchain

Blockchain is a distributed and decentralized ledger that can maintain a permanent and verifiable record of transactions between users. Each block in a blockchain is made up of a sequence of time-stamped transactions and a hash reference that connects it to the previous block and each block contains batches of valid transactions. Each transaction is stored in a Merkle hash tree within a block because every block includes a digest of its previous block's value, this feature allows verification that the contents of the preceding block have not been changed. All-access events and documents are validated by consensus mechanism before added to the blockchain. A blockchain-based architecture can provide a tamper-proof digital ledger of all EHR transactions. HFB is a modular and adaptable blockchain implementation framework that allows for plug-and-play components like consensus algorithms. HFB uses Access Control Lists (ACLs)[19] in smart contracts to implement identity-based access control of EHR information. The Hyperledger network which is private and permission, allows only limited entities to participate. Hyperledger also features an integrated architecture that gives you

a lot of freedom in terms of how you use it. In August 2015, NIST released SHA-3 (Secure Hash Algorithm) [12] the most recent algorithm of the SHA standard. The hash code result is included in the smart contract, and the transaction is stored on the blockchain network indefinitely. A piece of data in the URL is the key to decrypting the address. This generated URL does not saved by the server. Hence only a valid and one-time self-destructive URL link can be used to display the address information. Once the address information has been checked then the encrypted data will be erased from the system and the URL link will disappear never to be found again. This system will preserve records of EHR addresses and access logs in blockchain transactions which are available by all participants. In addition, each patient's personal information, such as their GID, names are retained in a secure location. In order for data users (healthcare practitioners) to view the patient profile the patient will choose an access policy which will be enforced via access control lists, [19]. The HFB module keeps track of patients' name and gender. The address of EHR information is encoded by one time self-destructive URL link [13] and stored on the edge node. After reading that address the URL link becomes invalid and cannot be used to view the same EHR information again.

4. The proposed secure storage of EHR system

A secure storage of EHR system based on hyperledger fabric blockchain with edge node. There are four entities namely the data owner, the data user, the hyperledger fabric blockchain and the edge node as shown in figure 1.

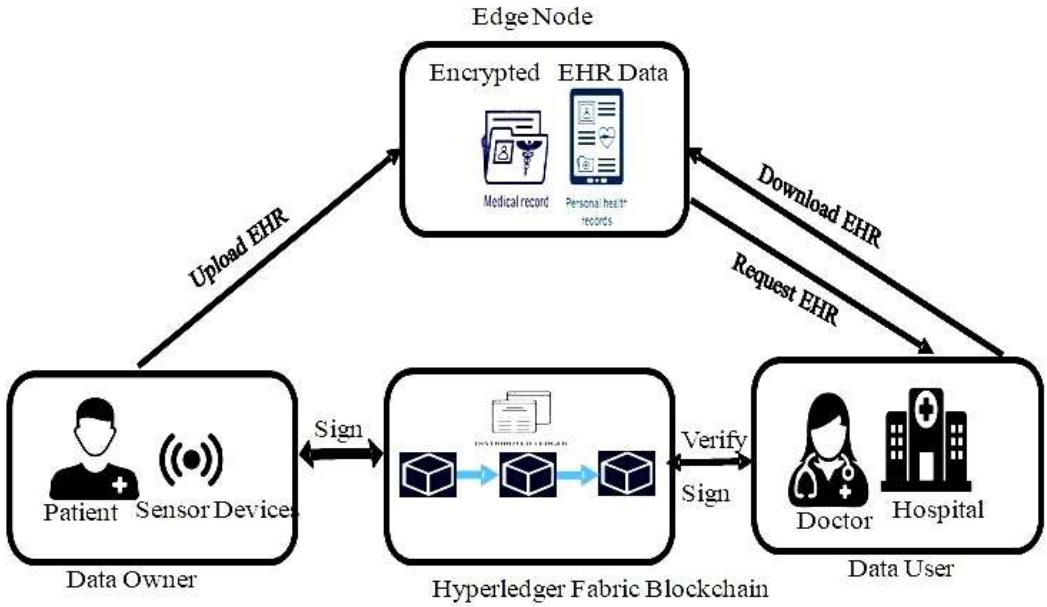

Figure 1.Hyperledger Blockchain-Based Edge Storage of EHR System

4.1 Procedure HFB encoding
Encoding the address of the edge node where the data is archived performs the following procedure

Input: Patient details

Output: Encode the details

Begin:

1. Initialize the system

2. Fetch the patient credentials →Pcred
3. Use the security procedure to encrypt the addresss→Pcred-Add
4. Store the Pcred-Add on the Edge Node
5. Destroy the security procedure

End

4.2 Procedure HFB- Decoding
Decoding the address of the edge node and accessing the private data performs the following procedure.

Input: Security code

Output: Decode the patient details

Begin:

1. Initialize the system
2. ∀ Encoded address E in Edge Node
3. Identify the correct Pcred-Add using the credentials
4. Use the security procedure to decode the address
5. If(hash code not tampered in blocks)
Do begin
6. If (User has the policy permission to access)
Allow the user to access the private medical data
Else
Deny access
End IF
ELSE
Hacking attempt is identified
End IF

End procedure

5. Results and discussion

The test run executed on various amount of healthcare data, the external data archived is initially fetched from the database or a repository using oracle-based service and this data is fed into the blockchain (Oracles acts as a bridge to connect the data from the external world to the block chain). This data pushed into the Blocks are first identified using a unique address which is then encoded using security mechanism (actually this encoding takes few micro seconds). The encoded address that contains the data in the blockchain is added on the edge node. During retrieval, the nodes are scrutinized first, the credentials of the user requesting the data is initially checked and verified and only the authorized users are allowed to decode the address data present in the edge node which enable the system to retrieve the precious health care data without any tampering or loss in the privacy. The detection percentage of the genuine user requesting for the data is found to be in the range of 98 to n100 percent depending on the number of false identities inducted purposefully to gauge the performance of the proposed approach. The execution speed of the encoding and decoding is fair and more number of test cases are to be carried out to check the overall performance of the proposed approach and from the result it is quite clear that the proposed approach worked 99% efficiently and blocked the unauthorized access to the patient data. The execution speed of the process is also noted as the speed of verifying the blocks is a major concern in many of the blockchain smart contract processes. A total of 100 test runs are carried out with 20 false identities and 90 proper identities. The

experimental result is shown in the following table 1. Overall, the proposed approach aimed to provide the utmost privacy and security to the data present in the blocks of blockchain.

Table 1: Test results with respect to execution speed and accuracy in detecting the right user

Number of Test runs	Number of false identity	Execution speed in sec	Detection percentage
20	2	0.25	100
50	8	1.2	99
75	12	1.6	98.8
100	20	1.9	98.5

6. Conclusion

This system proposed the hybrid architecture of EHR data management by utilizing both Hyperledger blockchain network in on-chain mode and edge node in off-chain mode. And HFB programmed with smart contracts to apply access control policies and record valid access events on the blockchain. Furthermore, this approach ensuring the reliability and security of EHR information by preventing unauthorized users from access authorization. For future work, we plan to design a consensus protocol for the proposed system to attain improved performance.

References

[1] IDC. Digital universe healthcare vertical report. https://www.emc.com/ analyst-report/digital-universe-healthcare-vertical-report-ar.pdf.
[2] Dubovitskaya A, Xu Z, Ryu S, Schumacher M. and Wang *Secure and trustable electronic medical records sharing using blockchain. AMIA annual symposium proceedings*. Vol. 2017. American Medical Informatics Association, 2017.
[3] Conti M, Kumar ES, Lal C, Ruj Set *A survey on security and privacy issues of bitcoin IEEE Communications Surveys & Tutorials* 20.4 (2018): 3416-52
[4] Guo H, Li W, Nejad M, Shen CC. *Access control for electronic health records with hybrid blockchain-edge architecture 2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019.
[5] Maesa, Damiano Di Francesco, Paolo Mori, and Laura Ricci. *A blockchain based approach for the definition of auditable access control system* Computers & Security 84 (2019): 93-119
[6] Rui Guo, Huixian Shi, Qinglan Zhao, and Dong Zheng. *Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems*. IEEE Access, 6:11676–11686, 2018
[7] QI Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani *Medshare: Trust-less medical data sharing among cloud service providers via blockchain.* IEEE Access, 5:14757–67, 2017
[8] Shangping Wang, Yinglong Zhang, and Yaling Zhang *A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems* IEEE Access, 6:38437–50, 2018
[9] Hao Guo, Ehsan Meamari, and Chien-Chung Shen *Multi-authority attribute-based access control with smart contract* In Proceedings of 2019 International Conference on Blockchain Technology (ICBCT 2019). ACM, 6 pages. https://doi.org/10.1145/3320154. 3320164
[10] Manaf Zghaibeh, Umer Farooq, Najam Ul Hasan, and Imran Baig *Shealth: A blockchain- based health system with smart contracts capabilities*. IEEE Access, 8:70030–70043, 2020.
[11] Hyperledger Fabric. https://www.hyperledger.org/projects/fabric.

[12] NIST. SHA-3. https://www.nist.gov/news-events/news/2015/08/ nist-releases-sha-3-cryptographic-hash-standard.
[13] 1ty.me. https://1ty.me/
[14] Rui Guo, Huixian Shi, Qinglan Zhao, and Dong Zheng *Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems.* IEEE Access, 6:11676–11686, 2018.
[15] Yinghui Zhang, Dong Zheng, Xiaofeng Chen, Jin Li, and Hui Li *Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts*. In International Conference on Provable Security, pages 259–273. Springer, 2014.
[16] Su, Qianqian, Rui Zhang, Rui Xue, and Pengchao Li *Revocable attribute-based signature for blockchain-based healthcare system.* IEEE Access 8 (2020): 127884-127896
[17] Ullah, Syed Sajid, Insaf Ullah, Hizbullah Khattak, Muhammad Asghar Khan, Muhammad Adnan, Saddam Hussain, Noor Ul Amin, and Muazzam A. Khan Khattak. *A lightweight identity-based signature scheme for mitigation of content poisoning attack in named data networking with internet of things.* IEEE Access 8 (2020): 98910-98928.
[18] Shahandashti, Siamak F., and Reihaneh Safavi-Naini. *Threshold attribute-based signatures and their application to anonymous credential systems.* In International conference on cryptology in Africa, pp. 198-216. Springer, Berlin, Heidelberg, 2009
[19] Namasudra, Suyel. *Data access control in the cloud computing environment for bioinformatics* International Journal of Applied Research in Bioinformatics (IJARB) 11, no. 1 (2021): 40-50