International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Health Record using Blockchain

[1]Aarti Ghumare, [2]Suruchi Talele, [3]Omkar Padmane, [4]Pranali Patil, [5]Prof. D. J. Gosavi

[1]Computer Engineering Pune Vidyarthi Griha's College of Engineering Nashik, India
[2]Computer Engineering Pune Vidyarthi Griha's College of Engineering Nashik, India
[3]Computer Engineering Pune Vidyarthi Griha's College of Engineering Nashik, India
[4]Computer Engineering Pune Vidyarthi Griha's College of Engineering Nashik, India
[5]Project Guide, Computer Engineering Pune Vidyarthi Griha's College of Engineering Nashik, India

Abstract---

Electronic health records are health information of patients that are saved digitally in a network. The information of the patient are stored in the block chain and these details are stored in the block chain as a blocks of data. The data is encrypted by the algorithm known as AES which is used to encrypt all the data of the patients. A Block chain network is used in the healthcare system to exchange patient data improve the performance, security, and transparency of sharing medical data in the health care system. The three main feature of block chain technology – Security, Decentralization Transparency make any application secure and not accessible by unauthorized parties.

Keywords— ***Health records, Block chain, Encryption of data***

Introduction

As patient healthcare records have been developed from traditional paper management to electronic record management, they can be safely stored and accessed and authorized only by legitimate medical centers. With the electronic health record (EHR) management system, storage availability and historical errors can be minimized, improving the availability and accuracy of healthcare records.

An EHR is a structure in digital format of a patient's health data that is created and maintained throughout the patient's life and is typically stored by and spread among multiple hospitals, clinics, and health providers.

Blockchain is a decentralized and public digital ledger that records transactions on many computers so that no record involved can be altered retroactively without altering any blocks afterwards. Blockchain is verified and linked to the preceding 'block,' forming a long chain. After all, Blockchain is the name of the record. As any transaction is registered and checked publicly, Blockchain provides a good deal of accountability. When entered, no one can modify all the information written in the Blockchain. It serves to demonstrate that the data is actual and unchanged. In Blockchain, data are maintained on networks instead of a central database, improving stability and showing its proneness to be hacked.

Blockchain technology has the potential to transform health care by placing the patient at the center of the health system and increasing the security, privacy, and interoperability of health data.

We illustrate the architecture to facilitate access control of EHR data by using both blockchain and edge node. We first enumerate the following entities which take part in the architecture.

Firstly, there is a registration process for patient hospital after that they login into th system. The hospital insert the patient records in the system. Then records is being encrypted with AES algorithm for security purpose. Hash value will be generated for the particular record using blockchain record stored in cloud , in the cloud hash value and original record also stored.

If another hospital need records they send request to cloud for access of the records using special access key. Request goes to patient they gives access to their record. After that record is send to hospital at time of transaction hash value get verify for particular record, that there is any changes does not occur in record then the record successfully send to the requested hospital or any changes occur in blocks at the time of transaction then record goes in temper and alert massage will be send to the hospital through mail. We use the patient mobile number to make authentication using OTP.

LITERATURE SURVEY

In eHealth, data for the Electronic Health Records (EHRs) of patients can be gathered from multiple sources, such as wearable devices, smart sensors, and medical imaging equipment. It has been reported that the amount of EHR data will continue to grow at a rate of 48% each year to reach 2,314

zettabytes by 2020 . However, according to the U.S. Department of Health and Human Services, there were more than 2,181 cases of healthcare data violations between 2009 and 2017, resulting in the exposure of 176,709,305 medical records . As a result, safe-guarding the EHR data has become a pivotal issue in eHealth. Although encryption addresses some fundamental security and privacy issues of EHR, access control, in particular, is difficult to enforce effectively due to the highly distributed and fragmented nature of EHR data and the complex relationship between data owners and data users.

Therefore, providing a flexible and fine-grained access control solution for EHR data is of paramount interest. Recently, blockchain has been suggested to be a promising solution for EHR data management . The inherent secureby-design feature of a blockchain-based infrastructure has the potential to provide a tamper-proof log for all the access events of EHR. In particular, all the access events can be verified and recorded through a consensus mechanism before being added to the blockchain. However, from the prospective of EHR management, the traditional blockchain-based solutions suffer from two significant drawbacks.

First, although blockchain can ensure data integrity, it lacks proper access control mechanisms to contain operations performed by different participants. Second, the size of blocks in a blockchain is too limited to accommodate EHR data containing images (e.g., X-ray, CT scan, and MRI) and/or videos (e.g., ultrasound). This paper proposes a hybrid architecture of using both blockchain and edge nodes to facilitate attribute-based access control of EHR data. Specifically, the Hyperledger Composer Fabric blockchain executes smart contracts programmed with Access Control Lists (ACLs) to enforce identity-based access control of EHR data and log legitimate access events into blockchain for traceability and accountability. In collaboration, edge nodes store EHR data and further enforce attribute-based access control (ABAC)1 of EHR data with policies specified in the Abbreviated Language For Authorization (ALFA) . ALFA maps directly into eXtensible Access Control Markup Language (XACML) and provides succinct representation.

In addition, hash digest is used to protect the integrity of EHR data stored in the edge nodes, which helps detect any alteration of EHR. Furthermore, one-time self-destructing urls , containing the addresses of EHR data on the edge nodes, are referenced in smart contracts, which will be returned to the healthcare providers after the successful execution of the ACL access policy. The healthcare providers then use the urls to access EHR data from edge nodes. Therefore, only eligible users who pass the attribute-based access control imposed by edge nodes can access the requested EHR data.

This paper proposes a hybrid architecture of using both block chain and edge nodes to facilitate attribute-based access Control of EHR data. Specifically, the hyper ledger Composer

Fabric block chain executes smart contracts programmed With Access Control Lists (ACLs) to enforce identity-based access control of EHR data and log legitimate access events into block chain for traceability and accountability. In collaboration, edge nodes store EHR data and further enforce attribute-based access control (ABAC) 1 of EHR data with policies specified in the Abbreviated Language for Authorization (ALFA).

ALFA maps directly into extensible Access Control Markup Language (XACML) and provides succinct representation. In Addition, hash digest is used to protect the integrity of EHR

Data stored in the edge nodes, which helps detect any alteration of EHR. Furthermore, one-time self-destructing urls, containing the addresses of EHR data on the edge nodes, are referenced in smart contracts, which will be returned to the healthcare providers after the successful execution of the ACL access policy. The healthcare providers then use the urls to access EHR data from edge nodes. Therefore, only eligible users who pass the attribute-based access control imposed by edge nodes can access the requested EHR data.

Methodology

1. HER Records
2. Block Generation.
3. Attribute based encryption.
4. Hashing Signature verification.
5. Remote Records Fetching.
6. Role based access control

Working:

We illustrate the hybrid architecture to facilitate access control of EHR data by using both block chain and edge node. By referring to Fig., we first enumerate the following entities which take part in the architecture.

The main and basic goal of our system is to provide Health records of patients to hospitals provide Security to Data.

• Patient: A patient is an entity who owns the EHR data to be accessed. A patient may specify the access policies for the EHR data he/she owns.

• Healthcare provider: A healthcare provider (e.g., doctor and nurse) is an entity who needs to access EHR data owned by patients. A healthcare provider actively seeks access authorizations from patients.

• Smart sensor/imaging equipment: A smart sensor is a device which collects EHR data from patients and sends it to the edge node. Imaging equipment may include X-ray, CT scan, MRI, and ultrasound, which generate HER data from patients.

• EHR data: An EHR data is a piece of information owned by a patient, and can be accessed by authorized healthcare providers.

• Edge node: An edge node is a computing and storage device which stores EHR data and imposes attribute-based access control policies.

• Block chain: Block chain is utilized as the controller of the architecture which manages access control policies and serves as a tamper-proof access log.

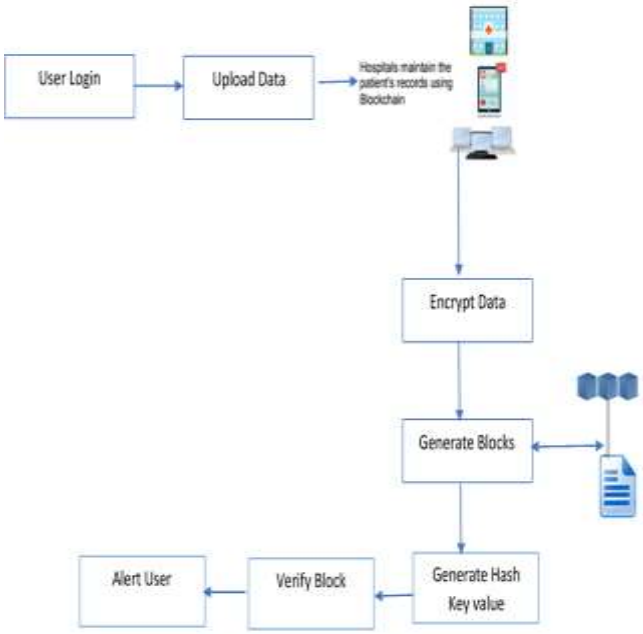

Fig. 1. Block Diagram

Conclusion

We propose a hybrid architecture of using both block chain and edge nodes to impose attribute-based access control of EHR data. Health record management system provide high security for patient information by removing intermediaries from the validation chain. This system enhance revolutionize how hospital use patient record and improve healthcare services. The electronic health record (EHR) made everything more easy and comfortable plus the entered data and information more accurate and safety, EHR now is considered as one of the most popular health technologies, it improved all the aspects of health care plus providing accurate information and fast access regarding the patients.

References

[1] IDC. [Online]. Available: https://www.emc.com/analyst-report/ digital-universe-healthcare-vertical-report-ar.pdf

[2] Trisha Torrey. [Online]. Available: https://www.verywellhealth.com/ who-has-access-to-your-medical-records-2615502

[3] G. Kamau, C. Boore, E. Maina, and S. Njenga, "Blockchain technology: Is this the solution to emr interoperability and security issues in developing countries?" in 2018 IST-Africa Week Conference (IST-Africa). IEEE, 2018, pp. Page–1.

[4] Hyperledger Fabric. [Online]. Available: https://www.hyperledger.org/ projects/fabric

[5] NIST, "Guide to Attribute Based Access Control (ABAC) Definition and Consideration," Tech. Rep. NIST Special Publication 800-162, 2014.

[6] Wikipedia contributors, "Alfa (xacml) — Wikipedia, the free encyclopedia," 2018. [Online]. Available: https://en.wikipedia.org/wiki/ ALFA (XACML)

[7] 1ty.me. [Online]. Available: https://1ty.me/

[8] [Online]. Available: http://www.my-signals.com/

[9] Wikipedia contributors, "Hyperledger — Wikipedia, the free encyclopedia," https://en.wikipedia.org/wiki/Hyperledger, 2019.

[10] [Online]. Available: https://www.nist.gov/news-events/news/2015/08/ nist-releases-sha-3-cryptographic-hash-standard

[11] W. Li, M. Nejad, and R. Zhang, "A blockchain-based architecture for traffic signal control system," IEEE ICIOT, 2019.

[12] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD). IEEE, 2016, pp. 25–30.

[13] D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in IFIP International Conference on Distributed Applications and Interoperable Systems. Springer, 2017, pp. 206–220.

[14] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of Medical Systems, vol. 40, no. 10, p. 218 (8 pages), 2016.

[15] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare:medrec prototype for electronic health records and medical research data," in Proceedings of IEEE Open & Big Data Conference, vol. 13, 2016, p. 13.

[16] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE Access, vol. 6, pp. 11 676–11 686, 2018.

[17] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.

[18] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in 2015 IEEE Security and Privacy Workshops. IEEE, 2015, pp. 180–184.

[19] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," IEEE Access, vol. 6, pp. 38 437–38 450, 2018.

[20] H. Guo, E. Meamari, and C.-C. 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.

[21] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, 2016.