Health Chain Connect

Mr. Prasad Sonawane[1], Mr. Anup Sonawane[2], Miss. Aditi Pahadi[3], Miss. Chandrakala Mahale[4], Mr. Rohan Lokhande[5], Miss. Devyani Girase[6]

Lecturer and HOD, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2,3,4,5,6]
Mahavir Polytechnic, Nashik, Maharashtra, India

Abstract*: Electronic medical records are medical records of patient stored digitally on the internet. Patient information is stored in the blockchain, and this information is stored as a block of data in the blockchain. Encrypted using the AES algorithm used to encrypt all patient data. Blockchain networks are used in healthcare to exchange patient information and increase the efficiency, security, and transparency of medical information sharing in healthcare. Security, decentralized and transparency, the three main features of blockchain technology, make all applications secure and inaccessible to unauthorized persons.*

Keywords: Medical records, Blockchain, Data encryption

I. INTRODUCTION

Patient records are transitioning from paper to electronic formats for better security and accessibility. Electronic Health Records (EHR) store a patient's health info digitally, making it easier to manage and share across. Healthcare providers. Blockchain, a decentralized ledger system, ensures secure and unalterable data recording by linking information in a chain of blocks. Blockchain enhances accountability and security in healthcare by storing data across a network, making it resistant to tampering. An architecture using blockchain and edge nodes manages EHR data access. Hospitals register patients and encrypt their data for security using AES algorithm. Hash values are generated for data and stored on the blockchain for verification. Other hospitals request access to patient data via the cloud using a private key. Patient authentication is done through OTP sent to their phone number. Any change in data during transmission triggers alerts and requires verification.

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 the 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

II. LITERATURE SURVEY

- It will reach zeta bytes by 2020. However, according to the U.S. Department of Health and Human Services, there were more than 2,181 medical data breaches between 2009 and 2017, resulting in 176,709,305 medical records. Therefore, protecting EHR data has become an important issue in eHealth. Although encryption solves some key security and privacy concerns for EHRs, access control is particularly vulnerable to

IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, March 2024

exploitation due to the fragmentation and fragmentation of EHR data and the relationship between data owners and data users.

- Therefore, it is important to provide flexible and granular access solutions to EHR data. Recently, blockchain has been viewed as a promising solution for EHR data management. The security structure of the blockchain-based infrastructure can provide evidence of all access to the EHR. In particular, all access events can be verified and recorded via consensus before being added to the blockchain. However, from an EHR perspective, blockchain-based solutions always have two disadvantages.

- First of all, although blockchain can ensure the integrity of information, it does not have the necessary control system to include the work done by different participants.

- Second, the block size on the blockchain is too limited to accommodate EHR files containing images (such as x-rays, CT scans, and MRIs) and/or video (such as ultrasounds).

- This article presents an integrated approach to managing EHR data using blockchain and edge nodes to facilitate access. Specifically, the Hyper ledger Composer Fabric blockchain implements smart contracts programmed with Access Control Lists (ACLs) to implement self-management of EHR data and record legitimate access events on the blockchain for monitoring and accountability purposes. Through collaboration, end nodes store EHR data and participate in the management of Behavior Based Access Control (ABAC) of EHR data using rules defined in Authoritative Abbreviation Language (ALFA) 1. ALFA maps directly to Extensible Access Control Markup Language (XACML) and provides a concise description.

- Additionally, hash summaries are used to maintain the integrity of EHR data stored on end nodes, helping to identify changes in the EHR. Additionally, once self-destructing URLs are defined in the smart contract containing the addresses of EHR data at the edge of the queue that will be sent back to the editor state when access rights to the ACL are executed. Clinicians then use these URLs to access EHR data from end nodes. Therefore, only users who take advantage of behavior-based management can access EHR data requests.

- This paper presents a hybrid architecture that uses blockchain and edge nodes to facilitate data access management for EHRs. Specifically, the hyper ledger Composer.

- Web blockchain implements smart contracts programmed using Access Control Lists (ACLs) to implement self-based management and security legal access of EHR data. Events are entered into the blockchain for traceability and accountability. End nodes collaboratively store EHR data and add behavior-based access control (ABAC) to EHR data using rules defined in the Authorization Acronym Language (ALFA).

- ALFA maps directly to Extensible Access Control Markup Language (XACML) and provides concise instructions. Additionally, hash summaries are used to maintain the integrity of EHR data stored in the queue, which helps identify changes to the EHR. Additionally, when self-destructing URLs are sent to the smart contract containing the addresses of EHR data on the end nodes, these URLs are sent back to expert treatment upon completion of the ACL access policy. Clinicians then use these URLs to access EHR data from end nodes. Therefore, only users who take advantage of behavior-based management can access EHR data requests

III. RESEARCH METHODOLOGY

Information Management: Implement a comprehensive system for managing patient information securely, ensuring that all datais accurately recorded, stored, and accessible only to authorized individuals or entities.

Block Production: Utilize blockchain technology to create blocks containing hashed patient data, ensuring that each block is securely linked to the previous one, forming an immutable chain of records.

Attribute-Based Encryption (ABE): Employ attribute-based encryption techniques to control access to patient information based on specific attributes or criteria, such as roles, departments, or privileges, ensuring that only authorized users can view or modifydata.

Hash Signature Verification: Utilize hash functions and digital signatures to verify the authenticity and integrity of patient data,ensuring that any changes to the data are detectable and traceable.

Remote Information Access: Develop mechanisms for accessing patient information remotely, allowing healthcare providers toretrieve data securely from any location, enhancing convenience and flexibility in patient care.

Role-Based Access Management (RBAC): Implement role-based access control mechanisms to regulate access to patient information based on the roles and responsibilities of healthcare professionals, ensuring that each user has appropriate permissions to perform their duties while maintaining data security and confidentiality.

IV. IMPLEMENTATION OF PROPOSED SYSTEM

We offer an integrated system that helps manage access to EHR data using blockchain and edge nodes. From the reference diagram, we first list the following areas included in the architecture. The main and important purpose of our organization is to deliver patients' medical information to hospitals and provide safe information.

- **Patient:** The patient is the entity whose EHR data is accessed. The patient can type in access rights to the EHR data he/she owns. Healthcare Providers: Healthcare providers (such as doctors and nurses) are organizations that need access to EHR data from patients. Physicians often ask for permission to reach the patient.
- **Smart Sensor/Imaging Device:** A smart sensor is a device that records the patient EHR Equipment that collects and transmits data to medical facilities. Edge node. Imaging equipment. May include X-rays, CT scans, MRIs, and ultrasounds, which generate HER information about the patient. EHR Data: EHR data is patient data that is accessible by authorized healthcare providers.
- **An Edge node:** An edge node is a computing and storage device used to store EHR data and enforce access control policies.
- **A Blockchain:** Blockchain is used as controller for compliance with infrastructure, control management policies and access verification.
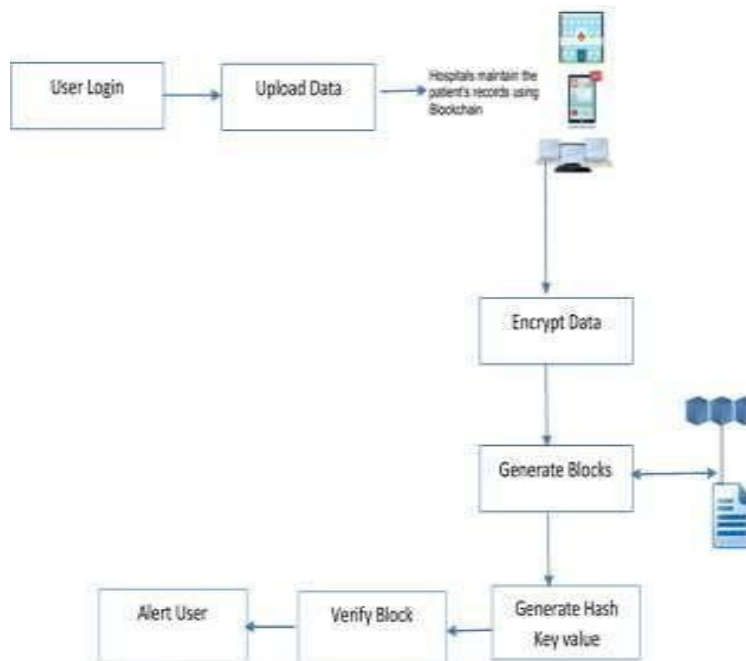

Fig. 1. Block Diagram

V. CONCLUSION

We proposed a hybrid architecture that uses blockchain and edge nodes to implement attribute-based access control for EHR data. Health information management provides high security for patient information by eliminating intermediaries in the chain of evidence. The system is changing the way hospitals use patient information and improve care. Electronic Health Records (EHR) make everything easier and more convenient, in addition to making information and data entry accurate and secure, EHR is now considered one of the most popular medical equipment that improves all aspects of Treatment and provides accuracy. Information and speed for patients

VI. ACKNOWLEDGMENT

REFERENCES

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

[2]. Trisha Torrey. [online]. URL: 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 for developing countries to solve interoperability and security issues of electronic health information? - 2018 IST-Africa Week Conference (IST-Africa). IB, 2018, p.

[4]. Hyperledger model. [online]. Available at: https://www.hyperledger.org/projects/fabric

[5]. NIST, "Guidelines for the Design and Evaluation of Process-Based Access Control (ABAC)," Tech. Representative NISTSpecial Publication 800-162, 2014.

[6]. Wikipedia Contributor, -Alpha (xacml) - Wikipedia, the free encyclopedia, - 2018. [online]. New information: https://en.wikipedia.org/wiki/ ALFA(XACML)

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

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

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

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