International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

eHealth Data Access Management with Privacy Protection by using Blockchain Technology and Attribute based Encryption

Ashmila KP

Assistant Professor, Vimal Jyothi Engineering College

Abstract: ***eHealth is a connection of health related organisations to transfer medical data. Medical data are the private information of each patient. People consults so many doctors, each of them stores prescriptions in their servers. Sharing of medical data through any unsecure media causes unauthorised access or misuse of information. The usage of blockchain and attribute based encryption allows the secure sharing of medical and personnel data between health organizations, establishing trust among parties involved. However, due to the replication of the blockchain on multiple nodes, a significant amount of storage space is required, which may not have an immediate purpose. To address this issue, the proposed solution combines the Ethereum blockchain with IPFS distributed storage technology to create a data sharing platform that prioritizes data security. The proposed model uses Attribute-based encryption (CP-ABE). Which is considered as more secure than traditional public-key encryption.***

Keywords: eHealth data; Ethereum; CP-ABE; IPFS

1. Introduction

People consults so many doctors, each of them stores prescriptions in their servers. Sharing of medical data through any unsecure media causes unauthorised access or misuse of information. eHealth is a connection of health related organizations to transfer medical data. The importance of eHealth is, its ability to give patients an access to their medical data and control its usage. Sharing of medical data through any unsecure media causes unauthorised access or misuse of information.

Blockchain technology can be used to salve these issues. By using blockchain technology, every transaction is stored cryptographically. The transactions in blockchain can't be delete or modified. But, blockchains are not perfect for storing large files. IPFS is file storing and sharing system. It stores and shares data efficiently. It stores data and corresponding hashes stored in the blockchain. So, the proposed system combines the features of both ethereum and IPFS technologies. Data privacy is a big concern for each person. To increase security, each person's provide access policy over the data before stored into the blockchain. Attribute Based Encryption is a cryptographic tool to provide access control.

a) Blockchain

Blockchain is a technology used to store and share data. Blockchain uses a distributed network to create a growing list of ordered transaction records. it is called blocks. Each block contains transations and it is validated by the participants in the network, by using consensus mechanism. Transactions in blockchain considered as permanent, because it prevents alteration. Transparency is the main characteristics of blockchain technology. [1] It is a connection of individual blocks and data transferred in between the blocks, and the blocks form the network. There are different type blockchain are there, private and public.

b) ETHEREUM

Ethereum is the public blockchain technology. Ethereum is considered as a series of protocols. every code in the ethereum executed on the Ethereum virtual machine EVM. [2] The protocols have the characteristics of decentralization. Ethereum have the distributed property, it ensures the property of consistency. The transaction process is open and transparent. The data storage and sharing is safe, and the information will not be altered. Its smart contract function provides efficiency to the ethereum blockchain.

c) IPFS

IPFS is known as inter planettary file system and is one of the best distributed file storage systems. [3] every node in the IPFS network is independent. The nodes are not depend on other nodes. When the datas are stored in the IPFS system, the IPFS system identify a unique hash value of the data according to the property of the data or information. The data is stored permanently in the IPFS network. If we want to retrieve the data, we need to use the hash value, then the user can obtain the data from the IPFS network.

d) ABAC

Attribute Based Encryption is a cryptographic technology to provide access control. Here, with each attribute a user secret key and cipher text is associated. [4] There are two types of attribute based encryption, Ciphertext Policy At-tribute Based Encryption (CPABE) and Key Policy Attribute Based Encryption (KPABE). In CPABE, a user key with a set of attributes is used to store and retrieve data. Whereas, in KPABE, a user private key with an access structure is used. In this proposed model, a CPABE based access control is used. Because here the persons can set a set of attributes to their particular data. When any other persons try to retrieve the data, only those whose attributes satisfies the given attributes at the time of encryption can only access the data. It prevents the unauthorised access. Depending on the attributes are managed by a single or multi authority, CPABE categorised into two types, single

authority CPABE and multi authority CPABE.

2. Related Works

Health records are crucial for the effective and efficient management of healthcare services. However, as you have mentioned, the current state of health record storage is fragmented and not interconnected. This results in a lack of patient mobility and makes it challenging for patients to access their data and control its use. Several approaches were introduced for efficient sharing of eHealth data.

A blockchain used 'medichain' model was proposed by Rahul et al [5]. This model uses the blockchain to store the entire data of patients. Merkle tree and hash values are also used to check the data is tampered or not. This system tries to remove all the problems related to the sharing and storing medical or healthcare data. The method uses a method called on chain storage. But the blockchain have storage issues and scalability problem. Onchain storage is expensive. A hybrid chain based EHR sharing scheme is proposed by Yi Sun [6]. Here the private datas are stored in the private chain and non-private data are stored in the public chain. Only licensed users can access the private data, and the non-private data can be shared with medical institutions for medical development. The model also uses offchain storage, and only data hashes are stored in the chain, and the smart contracts are automatically manage the EMR request, approval and usage process. The particular system uses hybrid chain was very novel.

An ABE based eHealth data storage model was proposed by Yingwen Chen [7] .They introduce the consortium blockchain. After patients upload data to medical institutions. The medical institution blur some sensitive data by using kanonimity technique. Then, the keywords are extracted from the dataset and form the index. They design a model based on searchable encryption to encrypt the dataset and the index. The entire encrypted dataset is uploaded to the cloud. The data set is managed by the medical institution itself. The encrypted data are uploaded to the consortium blockchain platform. Each medical institution act a node in the network. They develop smart contract for the blockchain network. One of the interfaces is designed for data users to query with the keyword index.

Sun Jianjun and Li Ming [8] propose a system that secure PHR by using patient access control. Their system uses both permissioned and permissionless blockchains and uses an IPFS system for data storage. The patients, doctors, hospitals, and other health care related organizations are registered on the blockchain. The hash values of EHR are stored in the blockchcain. Mahesh Kayastha and Shakir Karim [3] propose a system to storing and sharing patient Health Information using Ethereum Blockchain and Inter Planetary File System (IPFS) based Application Model. In this proposed model, for a decentralized application they utilizes Ethereum blockchain and Inter Planetary File System (IPFS). Based on their findings, they argue that blockchain technologies offer a more effective option for public and private healthcare institutions, as well as medical practitioners, to securely store and share patient records, which can lead to the delivery of timely and quality healthcare services.

3. eHealth data access management using ethereum blockchain and attribute based encryption

The architecture of this proposed system contains an attribute-based access control model, InterPlanetary File System, and an ethereum blockchain. Here there are two modules are there: User and an Admin. Users can be divided into two types: who can be doctors and patients. The blockchain technology used for the proposed model is Ethereum blockchain technology.
The proposed model consists of the following modules:

- Blockchain and User Registration
- Data Access from Blockchain
- Data Transaction Record on Blockchain

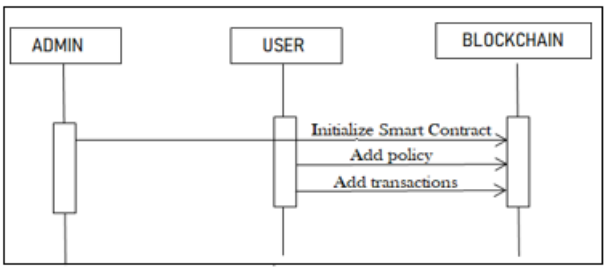

Figure 1: Smart contract and Policy

The implementation of the proposed system using blockchain technology requires the installation of a smart contract in the blockchain network. The first step is to choose an appropriate blockchain network, such as Ethereum, and connect to it, either through a node or a web interface. Once connected, the next thing is to develop the smart contract code, which defines the system's rules, logic, and behavior. The smart contract code is develop using the programming languages such as Solidity, and it is then compiled to bytecode. The compiled code is deployed to the network using a specialized transaction called a con- tract deployment transaction, which creates an immutable instance of the smart contract on the blockchain. After the smart contract is developed, it is interacted with through transactions that invoke its methods or functions. These transactions are broadcast to the network and are processed by the blockchain nodes according to the rules defined by the consensus mechanism. This ensures that the system operates in a decentralized, trustless, and transparent manner.

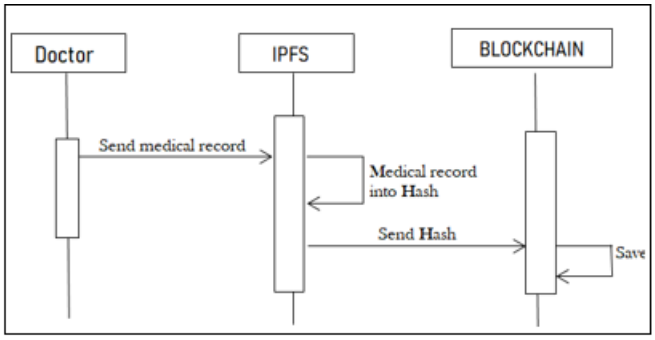

Figure 2: Data Transaction Record on Blockchain

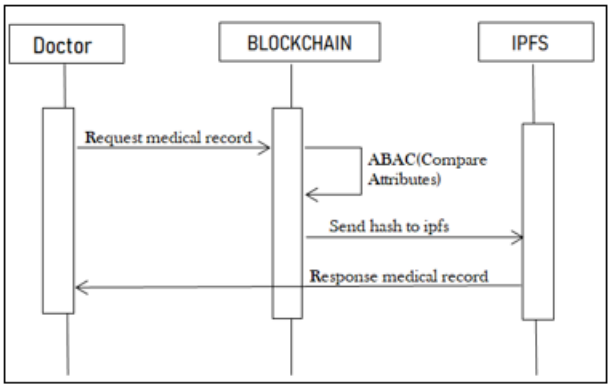

Figure 3: Data Access from Blockchain

First, the medical records are uploaded to IPFS and a hash address is generated. After that the hash address is stored on the blockchain. If a doctor uploads medical records, they are first encrypted using attribute-based encryption before being stored on IPFS. IPFS uses the SHA256 algorithm twice to convert the original data into a hash address that is then encoded using Base58. The resulting hash address is 33 bytes long and is used to replace the original medical information. Finally, the hash address is stored in the blockchain and the medical data is stored in the corresponding block. When doctor uploads medical records the system uses CPABE to encrypt the particular data. There are mainly four algorithms in this scheme:

1) Setup (): This step take a random number, the thresh-old value t and an attribute id aid. This step produces a public key PK and a master key MK.
2) Encrypt (PK, M, A): This step takes the public key PK, a message M, and an access structure A. This step encrypt M and produce a ciphertext CT.
3) Key Generation (PK, MK, S): This step takes the public key PK, master key MK, and a set of attributes S that describe the key. The output is the secret key SK.
4) Decrypt (CT, PK, SK): This step takes the public key PK, ciphertext CT, which contains an access policy A, and secret key SK as the input. The algorithm decrypt the ciphertext CT and return message M.

Accessing medical information using attribute- based access control is a multi step process that begins with a doctor requesting access to a patient's medical data. The request is then sent to the attribute-based access control system, which is responsible for ensuring that only correct doctors have the access to the medical data. To determine whether the requesting doctor has the necessary access rights, the attribute-based access control system compares the attributes associated with the doctor's account to the required attributes for accessing the medical data. These attributes may include things like the doctor's specialty, level of clearance, or any other relevant information that is necessary to ensure the security of the patients health care data. If the requesting doctor's attributes match the required attributes for accessing the medical data, the blockchain network transfers the hash value of the medical data to the IPFS. The hash address serves as a unique identifier for the medical data and allows IPFS to locate and retrieve the relevant information requested by the doctor. By Using the hash address, IPFS calculates and retrieves the relevant medical data requested by the doctor. This process ensures that the patients data is kept confidential and secure.

4. Performance Evaluation

The performance of the proposed method is analysed by comparing it with the existing methods. We analyse the performance in terms of Transaction cost and Time complexity. In Ethereum, a constant amount of gas is required for each transaction block. This means that every transaction must have a certain amount of gas allocated to successfully completed, and an equal amount of gas is used as the cost of create a new block. This gas limit ensures that the network remains stable and prevents any single transaction from using an excessive amount of resources. The proposed system uses ethereum+IPFS technology for

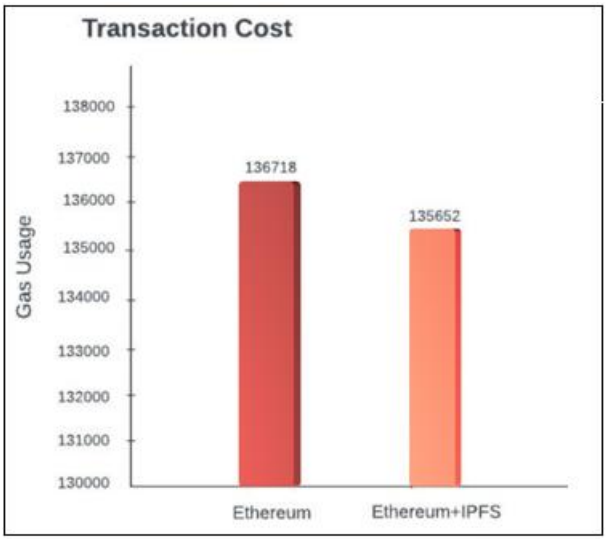

Figure 4: Transaction cost

medical data storage. That means, At the time of eHealth data storage, the data stored in the IPFS file system and the corresponding hash value is stored in the blockchain. From the given figure 1, it shows that ethereum+IPFS storage system uses less gas than ethereum storage system. If we can reduce the gas usage, we can optimize the performance and efficiency of the smart contracts.

The proposed system uses attribute based encryption. Attribute based access control (ABAC) systems can use various encryption algorithms such as CAMELLIA-256-CBC, AES-256-GCM, AES-256-CTR, and AES-128-CBC. However, based on their running time, these algorithms can be divided into different categories. From the figure 2, it is given that CAMELLIA-256-CBC uses more running time, while AES-128-CBC and AES-256-CTR uses less running time. Compared to AES-128-CBC ialgorithm, AES-256-CTR offers additional security with greater key sizes and more rounds. The AES 128 uses 10 rounds. But AES 256 uses 14 rounds.

5. Conclusion

The sharing of healthcare data is a very important thing in eHealth. Because sharing of health data is not that much secure. However, sharing patient data between healthcare organizations can be risky without a trusted system in place. To address this issue, this system combines blockchain technology with IPFS and attribute based access control, to

provide secure and private storage of medical information. With ABAC, patient data is kept confidential and the patient is recognized as the owner of their data.

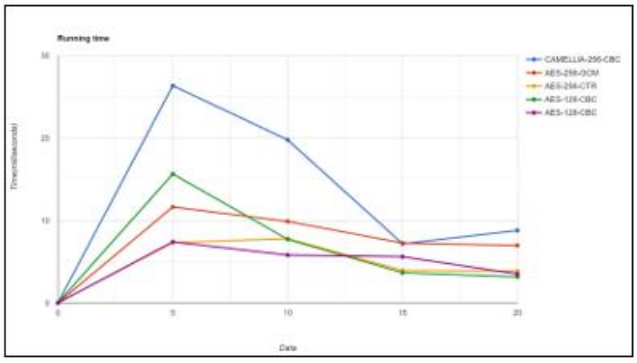

Figure 5: Time complexity

Furthermore, to avoid the storage issue of the blockchain. This system utilizes the InterPlanetary File System (IPFS) for storage. The combination of IPFS and blockchain provides a better solution to the storage issue often faced by blockchain systems. By leveraging these technologies, this system offers a secure and efficient solution for storage and sharing of healthcare data.

References

[1] P. Xi, X. Zhang, L. Wang, W. Liu, and S. Peng, "A review of blockchain-based secure sharing of healthcare data," *Applied Sciences*, vol. 12, no. 15, p. 7912, 2022.

[2] Z. Sun, D. Han, D. Li, X. Wang, C.-C. Chang, and Z. Wu, "A blockchain-based secure storage scheme for medical information," *EURASIP Journal on Wireless Communi- cations and Networking*, vol. 2022, no. 1, p. 40, 2022.

[3] M. Kayastha, S. Karim, R. Sandu, and E. Gide, "Ethereum blockchain and inter-planetary file system (ipfs) based application model to record and share patient health information: An exemplary case study for e-health edu- cation in nepal," in *2021 19th International Conference on Information Technology Based Higher Education and Training (ITHET)*, pp. 1–7, IEEE, 2021.

[4] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. Tsai, and C.-R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE journal of biomedical and health informatics*, vol. 24, no. 8, pp. 2169–2176, 2020.

[5] R. Johari, V. Kumar, K. Gupta, and D. P. Vidyarthi, "Blosom: Blockchain technology for security of medical records," *ICT Express*, vol. 8, no. 1, pp. 56–60, 2022.

[6] J. Dong, H. Wu, D. Zhou, K. Li, Y. Zhang, H. Ji, Z. Tong,

[7] S. Lou, and Z. Liu, "Application of big data and artificial intelligence in covid-19 prevention, diagnosis, treatment and management decisions in china," *Journal of Medi- cal Systems*, vol. 45, no. 9, p. 84, 2021.

[8] Y. Chen, L. Meng, H. Zhou, and G. Xue, "A blockchain- based medical data sharing mechanism with attribute- based access control and privacy protection," *Wire- less Communications and Mobile Computing*, vol. 2021, pp. 1–12, 2021.

[9] S. Jianjun, L. Ming, and M. Jingang, "Research and application of data sharing platform integrating ethereum and ipfs technology," in *2020 19th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)*, pp. 279– 282, IEEE, 2020.