International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Decentralized Data Access Control Mechanism for Healthcare Sector based on Blockchain Security

R. Vidhya[1], R. Sathya[2]

[1]ME Student, Sir Issac Newton College of Engineering and Technology, Nagappattinam, Tamilnadu, India

[2]Assistant Professor, Department of Computer Science and Engineering, Sir Isaac Newton College of Engineering & Technology, Nagappattinam, Tamilnadu, India

Abstract: ***Objective: Electronic health records possess the patient's medication details and their health history. The health records attract the attention of the attackers' as it possesses invaluable information. Loss of electronic health record leads to a wrong medication or surgery. Healthcare systems provide fewer security measures to secure the health records. In traditional electronic health records (EHRs), medical-related information is generally separately controlled by different hospitals and thus it leads to the inconvenience of information sharing. Cloud-based EHRs solve the problem of information sharing in the traditional EHRs. However, cloud- based EHRs suffer the centralized problem, i.e., cloud service center and key-generation center. Proposed work focus on creating a new EHRs paradigm which can help in dealing with the centralized problem of cloud - based EHRs. The solution is to make use of the emerging technology of blockchain to EHRs (denoted as blockchain-based EHRs for convenience). First, define the system model of blockchain-based EHRs in the setting of blockchain. In addition, the authentication issue is very important for EHRs. However, existing authentication schemes for blockchain-based EHRs have their own weak points. Here also propose an authentication scheme for blockchain-based EHRs. Our proposal is Role based signature scheme with multiple authorities which can resist collusion attack. Also implement cryptography methods for secure data storage and time based access control method to enhance the data access control. Furthermore, proposed scheme is provably secure in the random oracle model and has more efficient signing and verification algorithms than existing authentication schemes.***

Keywords: blockchain, data privacy, decentralized access control, decentralized identifier, self sovereign identity

1. Introduction

EHRs are an information system which maintains medical records in the process of patients' treatment or health management. In EHRs, all medical related data are digitized and stored in the server of hospital. Then, when a patient goes back to the hospital, he or the hospital can search previous information, including names of the patient and doctor, time, diagnosis, and so on. As an important application in the medical field, EHRs have attracted wide attention. However, there exist many problems in traditional EHRs. First of all, generally, medical-related data are independently stored in different hospitals or research institutions since they have their own independent database. Therefore, when a patient transfers from a hospital to another one, he needs to obtain medical examinations once again. This obviously will lead to waste of medical information resources and increase patients' body and financial burdens. Secondly, in EHRs systems, only the authorities, such as hospitals, have data. Hence, if there is a dispute between hospital and patient, then the hospital will always win since it can tamper the medical records or even delete them. It is not fair for patients. In order to solve the problem of information sharing in the traditional EHRs, researchers introduced the notion of could based EHRs. The cloud-based EHRs are one of the application of could computing technology. In cloud-based EHRs systems, there still needs a cloud service provider who plays the role of authority. All medical-related data, from doc tor, pharmacy, diagnostic laboratory, insurance center, and so on, will be uploaded to the cloud server. Then, users can search and download useful information from could server. If several organizations share a same cloud server, then they can share the data with a convenient way.

Next, when patients transfer from a hospital to another one, the new hospital can obtain patients' medical related data from the cloud and thus they have no need to, once again, get medical examinations. Therefore, cloud-based EHRs solve the problem of information sharing in the traditional EHRs. In addition, in cloud-based EHRs, all data are only maintained by the authority, i.e., cloud service provider, and thus the hospitals and other organizations could tamper the medical-related data only when they collude with the authority.

In this project propose a secure data sharing scheme for dynamic members. Firstly, we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager. Secondly, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.. Finally, our scheme can achieve fine efficiency, which means previous users need not to update their private keys for the situation either a new user joins in the group or a user is revoked from the group.

2. Cloud Computing

Cloud computing technology consists of the use of computing resources that are delivered as a service over a network. In cloud computing model users have to give access to their data for storing and performing the desired business operations. Hence cloud service provider must provide the trust and security, as there is valuable and sensitive data in huge amount stored on the clouds. There are concerns about flexible, scalable and fine grained access control in the cloud computing.

Cloud computing is consistently growing and there are many main cloud computing providers including Amazon, Google, Microsoft, Yahoo and many others who are offering solutions including Software-as-a-Service, Platform-as-a-Service, Storage-as-a- Service and Infrastructure-as-a-Service. In addition, considering the possibility to substantially minimizing expenses by optimization and also maximizing operating as well as economic effectiveness, cloud computing is an excellent technology. Furthermore, cloud computing can tremendously boost its cooperation, speed, and also range, thus empowering a totally worldwide computing model on the internet infrastructure. On top of that, the cloud computing has advantages in delivering additional scalable, fault tolerant services.

Cloud computing handles resource management in a better way since the user no longer needs to be responsible for identifying resources for storage. If a user wants to store more data they request it from the cloud provider and once they are finished they can either release the storage by simply stopping the use of it, or move the data to a long-term lower-cost storage resource. This further allows the user to effectively use more dynamic resources because they no longer need to concern themselves with storage and cost that accompany new and old resources.

Cloud computing service models are all inside in the cloud sing and laptops, desktops, phones and tablets are acts like clients to get services from the cloud. Servers provide services to clients according to their request or pay base. Cloud computing provides a shared pool of configurable IT resources on demand, in which needs minimal effort of management to get better services. Services are based on various agreement SLA (Service Level Agreement) between service providers and consumers.

The term “cloud”, as used in this white paper, appears to have its origins in network diagrams that represented the internet, or various parts of it, as schematic clouds. “Cloud computing” was coined for what happens when applications and services are moved into the internet “cloud.” Cloud computing is not something that suddenly appeared overnight; in some form, it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications. Many companies are delivering services from the cloud. Some notable examples include the following:

Google:
Has a private cloud that it uses for delivering Google Docs and many other services to its users, including email access, document applications, text translations, maps, web analytics, and much more.

Microsoft:
Has Microsoft® Office 365online service that allows for content and business intelligence tools to be moved into the cloud, and Microsoft currently makes its office applications available in a cloud.

Hashing is the process of changing the arbitrary and variable size input to a fixed size output. There are different functions that perform hashing of different level. MD5 algorithm is widely used for hashing purposes and it provides a 128 nit or 32 symbols long hash value. MD5 is the latest algorithm in the series while before that Md2, Md3, and Md4 also existed. The algorithm was designed to be used as a cryptographic hashing algorithm but it faces some problems that reduce the production of unique hash value and hence it faces some vulnerability. SHA (Secure Hashing Algorithm) is another cryptographic hash function that yields 160 bit hash value consisting of 40 hexadecimal characters. The algorithm could not resist the collusion attacks against it and its usage has declined. In this time several new algorithms have also been proposed, including SHA 3, and SHA 256.

3. Blockchain Technology

Blockchain technology has revolutionized the way we store and share data by providing a secure and decentralized system. Cloud data storage and data sharing have become increasingly popular in recent years due to the convenience and accessibility they offer. However, these systems often come with security concerns, such as the risk of data breaches, unauthorized access, and data manipulation.

Blockchain-based cloud data storage and data sharing can address these security concerns by providing a tamper-proof and transparent system. This technology allows data to be stored in a decentralized network of nodes, making it virtually impossible for any single party to manipulate the data. Additionally, the data can be encrypted and distributed across the network, ensuring that even if one node is compromised, the data remains safe.

Furthermore, blockchain-based cloud data storage and data sharing provide an incentive mechanism for users to contribute their storage space to the network. Users are rewarded for their contribution with cryptocurrency tokens, creating a self-sustaining and decentralized system. Overall, blockchain-based cloud data storage and data sharing provide a secure, transparent, and incentivized system for storing and sharing data. This technology has the potential to revolutionize the way we handle and store sensitive information, making it an exciting development in the world of data management.

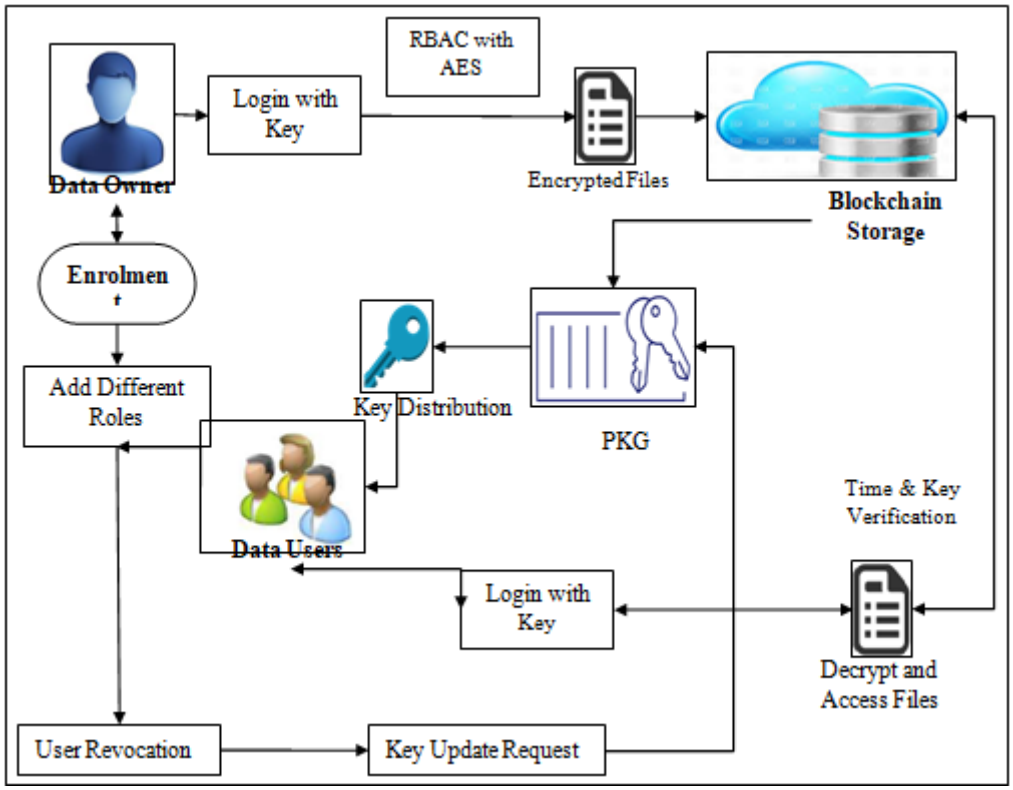

Figure 1: System overview

The storage scheme of medical data uses blockchain based cloud storage technology to achieve safe storage and sharing. In this module, create a local Cloud and provide priced abundant storage services. Data storage and access control are the main transactions in the medical blockchain. It would be optimal to be able to hold all medical data on the blockchain. Once get space from cloud the users can upload to share data in the cloud. In this work, the cloud storage can be implementing with high secure using block chain technology. Proposed secure data sharing framework provides communication between group owner and group members. Group Owner takes charge of followings,

- System parameters generation
- User registration
- User revocation

Therefore, the group owner is fully trusted by the other parties. The Group owner is the admin. The group owner has the logs of each and every process in the cloud. The group owner is responsible for user registration and also user revocation too.

Blockchain Technology

Transaction initiation: A transaction is initiated by a user who wants to send digital assets to another user on the blockchain.

The transaction includes information such as the amount of assets being transferred and the recipient's address.

Verification: The transaction is broadcast to all nodes (or validators) on the blockchain network, who verifies the transaction's validity. This involves checking the user's digital signature to confirm their identity and ensuring that the user has sufficient assets to complete the transaction.

Block creation: Once a certain number of verified transactions have been collected (often referred to as a block), a new block is created. This block includes a hash of the previous block, creating a chain of blocks (hence the term blockchain).

Consensus: The nodes on the network work together to reach consensus on the validity of the new block. This often involves using a consensus algorithm, such as Proof of Work or Proof of Stake , to determine which nodes can add the new block to the chain.

Block addition: Once consensus has been reached, the new block is added to the blockchain, and the transactions within the block are considered confirmed and final.

Mining (optional): In PoW-based blockchains, mining is a process where nodes compete to solve a complex mathematical problem to earn a reward for adding a new block to the chain. This incentivizes nodes to participate in the network and secure the blockchain.

Node synchronization: Each node on the network updates its copy of the blockchain to include the new block, ensuring that all nodes have a consistent and up-to-date copy of the blockchain.

These steps are repeated for every new transaction that is initiated on the blockchain, ensuring that the blockchain remains secure, transparent, and immutable.

Data Upload with Encryption

Group owner is a cloud client who registers with the CSP (Cloud Service Provider). Owner outsources data to cloud in encrypted form. Group owner anonymously get authenticated to cloud while getting duly authenticated. It is

the duty of the Group owner to prevent the admission of malicious group owner's to cloud. The encrypted data is uploaded to the cloud by the group owner. The group owner can encrypt the file using AES encryption technique. The choice of encryption is of the group owner.

Attribute Based Encryption
Setup (λ, U) → (PK, MK): The setup algorithm takes as input a security parameter λ and a universe description U, which defines the set of allowed attributes in the system. It outputs the public parameters PK and the master secret key MK.

Encrypt (PK, M, S) → CT: The encryption algorithm takes as input the public parameters PK, a message M and a set of attributes S and outputs a ciphertext CT associated with the attribute set.

KeyGen (MK, A) → SK: The key generation algorithm takes as input the master secret key MK and an access structure A and outputs a private key SK associated with the attributes.

Decrypt (SK, CT) → M: The decryption algorithm takes as input a private key SK associated with access structure A and a ciphertext CT associated with attribute set S and outputs a message M if S satisfies A or the error message ⊥ otherwise.

Role Based Access Control
RBAC is nothing more than the idea of assigning system access to users based on their role within an organization. The system needs of a given workforce are analyzed, with users grouped into roles based on common job responsibilities and system access needs. Access is then assigned to each person based strictly on their role assignment. With tight adherence to access requirements established for each role, access management becomes much easier.

Role Based Access Control
The Data User is provided with Role-based Access Control policy. In our proposed system, the privileges of the Data User are reduced and the DU can only download data from the cloud. In the proposed system, to protect the sensitive information the Data Owner specifies their own access privacy policies. Access can be restricted to certain information. Apart from this, it also helps the customer to increase his confidence and provides continuous data access with the touch of a button from anywhere at any time.
U, R, P, and S (users, roles, permissions and sessions respectively),
P A ⊆ P x R, a many-to-many permission to role assignment relation,
U A ⊆ U x R, a many-to-many user to role assignment relation,
user: $S \to U$, a function mapping each session s_i to the single user user (s_i) (constant for the session's lifetime), and roles: $S \to 2^R$, a function mapping each session s_i to a set of roles $roles\ (s_i) \subseteq \{r|(user\ (s_i), r) \in UA\}$ (which can change with time) and session s_i has the permissions $U_{r \in roles\ (s_i)}\{P|(p, r) \in PA\}$

3.4.4 Data Access
User must be authenticated to access the service from cloud. The commonly used security mechanism for data access is to check username and password pair. User provides the username and password to the cloud server and then cloud server checks the authenticity of user. If user is authorized service provider will allow user to search file from cloud otherwise the user will not allowed to search files. User can be extracting the stored data anywhere from cloud storage. If a new member is added to the group, this system can be granted access to the file and sharing the group key to the added member wherein he can directly download the decrypted data file, when they are downloading the file a secret key is generated and sent to their own mobile number, using that key user can download the data.

3.4.5 User Revocation
User revocation is performed by the group owner through a public available revocation list, based on which group owner can encrypt the data files and ensure the confidentiality against the revoked users. Revoked users are not permitted to decrypt the data shared on the cloud after the revocation. The remaining users need to update their group keys to avoid unwanted data access made by removed users. New granted users can get present group key and learn all the content data files stored by group owner.

4. Conclusion

Blockchain technology maximizes security and accessibility. The technology can be used in many different areas of the healthcare system, such as for storing and sharing medical records and insurance information both in healthcare venues and in mobile applications and remote monitoring systems, and for clinical trials. This research work provides efficient access control policy based on users role also implement secure encryption using AES encryption algorithm. The cloud storage requires secure access control to preserve privacy of data. Here propose a RBAC based model which allows an organization to store data securely in a public cloud. The proposed (Role Based Access Control with Encryption) model performs the user revocation and decryption operations efficiently.

References

[1] Tao, Jiyu, and Li Ling. "Practical medical files sharing scheme based on blockchain and decentralized attribute-based encryption." IEEE Access 9 (2021): 118771-118781.
[2] Madine, Mohammad Moussa, AmmarAymanBattah, IbrarYaqoob, Khaled Salah, Raja Jayaraman, Yousof Al-Hammadi, SasaPesic, and SamerEllahham. "Blockchain for giving patients control over their medical records." IEEE Access 8 (2020): 193102-193115.
[3] Kim, Beomseok, Woonseob Shin, Dong-Yeop Hwang, and Ki-Hyung Kim. "Attribute-based access control (ABAC) with decentralized identifier in the Blockchain-based energy transaction platform." In 2021 International Conference on Information Networking (ICOIN), pp. 845-848. IEEE, 2021.
[4] Park, Young-Hoon, Yejin Kim, and Junho Shim.

"Blockchain-based privacy-preserving system for genomic data management using local differential privacy." Electronics 10, no. 23 (2021): 3019.

[5] Manoj, T., KrishnamoorthiMakkithaya, and V. Narendra. "A blockchain based decentralized identifiers for entity authentication in electronic health records." Cogent Eng 9, no. 1 (2022): 2035134.

[6] Cruz, Jason Paul, Yuichi Kaji, and Naoto Yanai. "RBAC-SC: Role-based access control using smart contract." Ieee Access 6 (2018): 12240-12251.

[7] Kumar, Randhir, and RakeshTripathi. "Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model." Journal of Ambient Intelligence and Humanized Computing 12 (2021): 2321-2338.

[8] Capraz, Seval, and Adnan Ozsoy. "Personal data protection in blockchain with zero-knowledge proof." Blockchain Technology and Innovations in Business Processes (2021): 109-124.

[9] Ferrey, A. E., Hughes, N. D., Simkin, S., Locock, L., Stewart, A., Kapur, N., Gunnell, D. Hawton, K. (2016). Changes in parenting strategies after a young person's self-harm: a qualitative study.