Flexible Access Control Mechanism for Cloud stored EHR using Consortium Blockchain

Eben Exceline C

Vellore Institute of Technology: VIT University

Sivakumar Nagarajan (✉ nsivakumar@vit.ac.in)

Vellore Institute of Technology: VIT University <https://orcid.org/0000-0002-8945-6412>

Research Article

Keywords: Consortium Blockchain, Cloud computing, Data Integrity, Data Privacy, Fine-grained access control, Smart Contracts, Electronic Health Record

Posted Date: April 12th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-397642/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Flexible Access Control Mechanism for Cloud stored EHR using Consortium Blockchain

C. Eben Exceline, Dr. Sivakumar Nagarajan
School of Information Technology and Engineering, VIT, Vellore, India
ebencse@gmail.com, nsivakumar@vit.ac.in

Abstract

The persevering pursuit of security has proved historically limiting the implementation of significant design improvements for Electronic Health Records (EHR). Such a vital requirement for these kinds of technical development is revamped now. This is because the patients are motivated by personalization and data science to participate in the health information sharing. The implementation of cloud computing has already shown substantial benefits for both clinical organizations and patients in managing electronic health records. The prime security issue of cloud-based electronic health records is that the patient is physically unable to own a medical record whereas a clinical organization can maintain one for them. The latter may collude with centralized cloud servers. So, there is a vulnerability of such records being tampered with in order to hide the medical malpractices. So, maintaining data integrity and data privacy becomes a significant challenge when deploying cloud computing. Therefore, in this paper, a consortium blockchain-based cloud-stored electronic health record is proposed which provides data integrity, data privacy, storage scalability, and fine-grained access control. Each process in outsourcing electronic health records to the cloud is incorporated as a transaction in a consortium ethereum blockchain through smart contracts. Through smart contracts, an attribute-based contract key is generated for the users that can decrypt the encrypted data stored in the cloud. The attribute-based contract key allows only users who are authorized to access the information ensuring data privacy and fine-grained access control. Moreover, the proposed scheme is proved to provide tamper-proof although the medical records are controlled by a group of clinical organizations.

KeyWords: Consortium Blockchain, Cloud computing, Data Integrity, Data Privacy, Fine-grained access control, Smart Contracts, Electronic Health Record.

1. Introduction

The electronic health record (EHR) systems that store and access patient health information has become a significant developing technology to enhance the efficiency of healthcare services. It is so since EHR is less error-prone, but at the same time, it is reliable. In the early days, the EHR was just maintained by different clinical organizations, and it isn't helpful for information sharing. The patients lack quick access to their past health data even though the records belong to them. When they visit other clinical organizations they are not able to provide their comprehensive previous medical history to the healthcare professional taking care of them. So the patients should take again medical tests which were already taken in the previous clinic. This is merely a waste of resources. The complexities of interoperability between various clinical systems pose an intense obstacle to EHR sharing. For better EHR information accessing and accomplish information sharing, centralized servers were set up that gives extraordinary comfort to patients and even clinical organizations.

Such a centralized server technology called cloud computing is a service-oriented architecture that addresses the interoperability issues with relatively low cost in a virtual environment. Cloud-based technology provides infrastructure, platform, and software. They provide services to share the data between various clinical organizations. Stealing sensitive information from EHRs outsourced to the cloud is increasingly becoming common as a result of inadequate security structures. First, EHRs outsourced to the cloud are typically handled by individual clinical organizations, ensuring that all private documents are kept in a database held by the organization responsible for producing the medical records. Second, once the data is outsourced to the cloud, there is no control over the data. The patient cannot keep track of the users who are accessing the data, the full trust relies on the cloud server. Third, malicious clinical organizations can collude with the cloud server and modify the health information stored in it leading to data integrity issues. The inadequacy mentioned above in EHR security structures raises a range of security, safety, and control problems that evolving technologies need to tackle.

The emerging blockchain technology can be successfully used to manage access control where different users can store and access data while the data remains private (Zyskind, Nathan, & Pentland, 2015). Blockchain is a decentralized, distributed, and immutable system that has a distributed ledger adopting an append-only data structure. All data appended are broadcasted on all the nodes in the network, so blockchain is easily verifiable and

tamper-resistant. Blockchain was initially designed as a cryptocurrency infrastructural component to make financial transactions called Bitcoin (Nakamoto, n.d.). A public distributed ledger records the transfer of Bitcoin from one account to another account. Anyone in the network can validate the transaction by verifying which accounts hold the particular Bitcoin. Nowadays, there are many other blockchain infrastructures, namely Ethereum (Buterin, 2009) and Hyperledger Fabric (Cachin, 2016). These infrastructures allow everyone to participate in the generation of blockchain-based applications. Blockchain is designed to record only the transactions of cryptocurrency, but EHR contains large images and unstructured data, which is difficult to store in blockchain. So EHR can be stored in an external cloud or Interplanetary file storage (IPFS) system. The access control is made through blockchain that improves scalability.

Blockchain is categorized as a public blockchain, private blockchain, and consortium blockchain according to the needs of real-world applications. Public blockchain cannot be adopted for securing EHR because the data are stored in a public ledger leading to data privacy breaches. Private blockchain provides perfect privacy for securing EHR, yet the trust relies on the single party who is controlling the network. Moreover, the vital requirement of EHR is to share among various clinical organizations, which is difficult under a single authority. A consortium blockchain is controlled by a group of users. It provides better privacy than public blockchain as well as solves the interoperability problem found in a private blockchain. So in this paper, the proposed system stores EHR in the cloud. The access control is made through consortium blockchain. Moreover, the proposed system designed an attribute-based key generation contract. It generates a key for the requestor who wants to access data in EHR. The attribute-based contract key allows the requestor to access the health data in EHR stored in the cloud. The user key attributes should satisfy the attributes used to encrypt the medical records. Thus the proposed system ensures data integrity, data privacy, fine-grained access control, and scalability

1.1 Motivation

Storing and accessing EHR in centralized servers leads to unauthorized modification and accessing confidential data of patients, denial of service, system failure, and breach of user privacy. The blockchain-based EHR proved to provide data integrity and data privacy but there is no option to give access to particular data for particular users. The failures mentioned in the existing cloud-based EHR and blockchain-based EHR prompted the work in this paper to arrive at a novel secured consortium blockchain-based cloud-stored EHR sharing framework.

1.2 Contribution

The following are the contribution of this paper:

- A) A consortium blockchain-based EHR with cloud storage is proposed. It provides data integrity, data privacy, scalability, interoperability, and fine-grained access control.
- B) The system designed six smart contracts named providers: provider relation contract, user-provider relation contract, access control contract, data encryption contract, key generation contract, and permission contract.
- C) The patient deploys the access control contract according to the keywords in his/her EHR.
- D) Through a key generation contract, an attribute-based contract key is generated. This is for the blockchain users to access patient EHR stored in the cloud. It provides data privacy and fine-grained access control over EHR.
- E) The smart contract is designed to encrypt the data, first fragment the EHR according to the searching keywords. Then it encrypts the data using inner product encryption (IPE) with the access control structure derived by the patient before being outsourced to the cloud. IPE hides the access control structure along with the data. It increases the security of EHR outsourced to the cloud.

The rest of the paper is organized as follows: Section 2 describes the background information on applying blockchain cloud-stored EHR. The detailed description of the proposed work is described in section 3. In section 4, the proposed work is implemented and it is compared with similar approaches. Finally, the last section contains the conclusion.

2. Preliminaries

2.1 Blockchain Technology

The formal definition of blockchain is given by (Marco & Karim, 2017) as

‘A blockchain is an open distributed ledger which can effectively record transactions between two parties in a verifiable and permanent manner.’

Blockchain is a peer-to-peer network consists of nodes. Every node is involved in the mutual validation of digital transactions, by storing the same blockchain copy. To be validated by peer nodes, each new transaction is broadcast over the network. Most nodes in the network must verify the transaction that is to be added to the blockchain. It is difficult to tamper with the transactions that are updated to the blockchain because the hash of the transactions is added in the block. Moreover, each block is represented by its hash value and it is chained with the previous block hash value.

As per the real-world needs, the existing blockchain systems can be divided into three categories: Public blockchain, private blockchain, and consortium blockchain (Zheng Xie). A public blockchain is permissionless in which all records are available in public. Anyone who has a blockchain account can participate in the system and have access to the information. A private blockchain is called a centralized network because the system is entirely managed by an entity. A consortium blockchain is a partly de-centralized structure because it is controlled by various clinical organizations. In consortium blockchain, information can be accessed by certain nodes that come from approved clinical organizations.

2.2 Pairing based cryptography:

Definition of bilinear maps

Let G_1 and GT be cyclic groups of the same prime order. A bilinear map from $G_1 \times G_1$ to GT is a function $e: G_1 \times G_1 \rightarrow GT$.

The map should fulfill the properties which are the following.

- 1 Bilinear: A map $e: G_1 \times G_1 \rightarrow GT$ is bilinear if $e(P^a, Q^b) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and all $a, b \in \mathbb{Z}$.
- 2 Non –degenerate: If P is a generator of G_1 then $e(P, P)$ is a generator of GT .
- 3 Computable: To compute $e(P, Q)$ for any $P, Q \in G_1$ there should be an efficient algorithm (Boneh & Franklin, 2001).

Bilinear maps are called pairing because it pairs elements from G_1 and G_1 to GT . Pairing-based cryptography takes two points from elliptic curve group G_1 and outputs from multiplicative abelian group GT . Pairing has a special property called bi-linearity. It is suitable for cryptography.

2.3 Decisional Bilinear Diffie Hellman (DBDH)

DBDH is to compute $e(g, g)^{abc}$ and decisions are made whether $Z = e(g, g)^{abc}$ where a, b and c are uniform random elements of $\mathbb{Z}_p$. g is the generator of G_1 , e is the bilinear map and Z is a random element of GT (Chatterjee & Sarkar, 2011).

The advantage of an adversary A to solve DBDH is defined as

$$ADV(A) = \{pr[A(g, g^a, g^b, g^c, Z) \rightarrow 1 \mid Z = e(g, g)^{abc}] - pr[A(g, g^a, g^b, g^c, Z) \rightarrow 1 \mid Z \text{ is random}]\}$$

The Decision Bilinear Diffie-Hellman (DBDH) assumption holds in the pairing group if the advantage of any polynomial-time adversary is negligible in solving the DBDH problem.

2.4 Inner Product Encryption:

The following four polynomial-time algorithms comprise an IPE scheme with a hierarchical access structure (Katz, Sahai, & Waters, 2013):

Setup ($\lambda \rightarrow pp, msk$) $\rightarrow pp, msk$: A clinical organization runs this randomized algorithm that takes the input security parameter λ and generates public parameters pp and master secret key msk .

User key generation ($pp, msk, A \rightarrow SK$): This algorithm is run by the clinical organizations to take the attributes of the user A as input and issue the secret key for the user sk . If the user is registered under different clinical organizations the user collects sk from the other clinical organizations. Then combines them to form the secret key SK .

Encryption ($M, T \rightarrow CT$): This algorithm is run by the clinical provider to generate ciphertext CT by taking message M and access structure T as input.

Decryption ($CT, SK \rightarrow M$): This algorithm is run by the user who requests the medical records. It takes CT and secret key SK as inputs and check the inner product between the secret key attributes and attributes in the access structure used to generate the ciphertext. If the inner product between the vector formed from the attributes of the secret key and the vector generated from the attributes of the access structure should be zero then the algorithm outputs M otherwise output a null value.

3. Related work

In this section, discussion based on different research papers in cloud-based EHR and accessed through blockchain is done. The primary goal of these papers was to establish blockchain networks that provided access controls for medical data. This allowed patients to track their personal medical information more carefully and helped them such that they made their data tamper-proof. According to the three categories of blockchain, the discussion is done.

3.1 Public blockchain with cloud storage

A public blockchain was deployed to share and access EHR to provide data integrity (Cao, Zhang, Liu, Zhang, & Neri, 2019). As data was stored in a public ledger and anyone could enter a public blockchain to make transactions perfect data privacy could not be achieved. But data privacy could be improved when the patients could have full control over their medical records by developing an agreement between the requestor and the patient through smart contracts. Although the users who were entering the network, modified data could not be traceable. To provide data privacy the requestor had to authenticate themselves to the data owner and complex logic query-based search encryption was adopted in (Chen, Lee, Chang, Choo, & Zhang, 2019) scheme.

3.2 Private blockchain with cloud storage

The risk of data privacy in distributing patients' medical records beyond one organization was solved by the permission granted blockchain-based framework (Xia, Sifah, Smahi, Amofa, & Zhang, 2017)(Xia, Sifah, Asamoah, et al., 2017). The architecture used the immutability and built-in transparency of blockchain to tackle access management issues associated with confidential information outsourced to the cloud. In order to avoid 51% attack in the private blockchain, (L. Zhu, Wu, Gai, & Choo, 2019) employed a trusted authority to vote for validating the updated medical records and adopted public key encryption to encrypt the EHR. The scheme assured high user privacy but lacked data privacy. Data privacy could be improved when public-key encryption was used to encrypt the EHR by deploying certificate authority (Fan, Wang, Ren, Li, & Yang, 2018). The transactions on EHR were distributed and stored in different blockchain nodes after encryption to achieve high data privacy (Kaur, Alam, Jameel, Mourya, & Chang, 2018). The scheme stored EHR on both cloud and blockchain, which resulted in high computational cost and less scalability. Dagher et al. proposed the Ancile framework, which assured data privacy by storing the data reference hash value in the blockchain, and queries were made through private transactions by utilizing proxy re-encryption. The Ancile Framework used a smart contract named the classification Contract (CLC) feature for enforcing access control mechanisms for the different roles of users like patients, organizations on the blockchain that allowed for inequality of roles that could be applied to according to the users' necessity. The scalability of this system is affected when more users were introduced to the network because of the time it took to scan global contracts such as the CLC (Dagher, Mohler, Milojkovic, & Marella, 2018). Thwin et al. also developed a proxy re-encryption scheme that deployed a gateway server to generate re-encryption keys according to the access control list and to re-encrypt the data to share with the requester (Thwin & Vasupongayya, 2019). The drawback of the scheme was the trust relied on the gateway server.

For securing EHR in blockchain-based EHR (H. Wang & Song, 2018), used attribute-based encryption (ABE) to encrypt the data and identity-based signature to check the authenticity of data entered in the blockchain. The scheme used ABE to achieve fine-grained access control. The identity-based signature used to validate the authorized users was not sufficient because the single attribute was checked for validation. The scheme was computationally expensive because it applied two varying encryption techniques, and it required a special searchable mechanism to search particular data in the EHR. Ciphertext-policy ABE was adopted to provide fine-grained access control for the EHR stored in the cloud (S. Wang, Wang, & Zhang, 2019). However, in this scheme, a patient needed high computational power to manage all the attributes of the user. (Yang & Yang, 2017) developed attribute-based signcryption, which combined encryption and signature scheme. Medical records were encrypted using the attributes required to decrypt the message and the owner of the medical record had to sign in order to validate the data. The drawback of the scheme was identifying management by a single authority that was the patient. Multiple authorities were employed to develop attribute-based signatures for the users of EHR (Guo, Shi, Zhao, & Zheng, 2018), and the system stated that the privacy of the data could be ensured when the patient had close attention to their medical records.

3.3 Consortium blockchain with cloud storage

A consortium blockchain was adopted to assist the access of cloud-stored EHR provided interoperability between various clinical organizations. Hospitals, medical research institutions, universities, medical insurance companies,

and government agencies form the consortium (Hylock & Zeng, 2019). These parties were trusted authority to control the transactions done in the blockchain. Hylock et al. adopted a proxy re-encryption scheme to give access permission to the users accessing the EHR. The cloud was deployed to store and act as a proxy to re-encrypt the EHR for the data requester (Y. Wang, Zhang, Zhang, & Wang, 2019). The scheme adopted searchable encryption and conditional proxy re-encryption to grant flexible data access to the EHR requester. When proxy re-encryption was adopted the trust relied on the proxy. Consortium blockchain could be applied to biomedical research and make collaborative decision making which improved the quality of healthcare delivery for the patients (X. Zhu, Shi, & Lu, 2019). The consensus-driven services and value sharing provided by the scheme enabled clinical organizations, individuals, and health-relevant industries to share the system's increasing value and acquire a range of healthy, secure, trustworthy, high-quality, affordable, conveniently payable, and on-demand resources. The Zhu et al. scheme developed a health cloud crypto coin to fund the miners to compete for block mining. The medical data was encrypted using a public-key encryption scheme which provided user privacy but it lacked data privacy.

The following observations are drawn from the existing literature:

- a) All the literature discussed in this paper stored patient's medical records in the cloud and integrated blockchain to assist the access control mechanisms to provide data integrity where the cloud did not provide.
- b) Some of the existing literature used proxy re-encryption, where the cloud acted as a proxy and re-encrypted the data again and sent it to the requestor. Again a trusted environment was developed so that the users had to trust the third-party cloud.
- c) Some literature used attribute-based encryption (ABE) or identity-based encryption (IBE) to encrypt the medical records before it was outsourced to the cloud. Although ABE provided fine-grained access control to the users in closed private blockchain identity management fell on a single authority which was cumbersome.
- d) Most of the literature adopted private blockchain. Although private blockchains had the advantage of high data privacy, they were intuitive against the goal of decentralization and allowed only limited members to access the EHR resulting in interoperability issues.
- e) Besides, personal user information was leaked in a private blockchain; access control architecture still required the property of allowing access to the relevant part of the EHR system only by certain users.
- f) Consortium blockchain provided interoperability and control participation of the users on the network, but the access control mechanism should provide more user privacy and fine-grained access control.
- g) In some literature patients were responsible to deploy all the smart contracts and for the key generation which required high computational power.

4. Proposed system

The functioning of the proposed system is explained in this section. First, the overview of the system is discussed and the components involved in the system are introduced. Then the detailed operation of the system is explained.

4.1 Overview

The overall proposed architecture is explained in Figure 1. The proposed blockchain-based cloud-stored EHR consists of the following steps.

1. A group of clinical organizations joins together to form a consortium blockchain network. This is to monitor the access of the cloud-stored patients' EHR and to maintain the privacy and interoperability of the data. The trust among the organizations is maintained by the provider-provider relationship contract.
2. The EHR of patients is fragmented and stored according to the search keywords in the cloud. The hash of the keywords and the location is stored in the blockchain.
3. The fragmented EHR is encrypted using Inner Product Encryption before being outsourced to the cloud. The access control structures used to encrypt the patient's data are deployed through a smart contract that runs on the patient node.
4. The key generation smart contract generates an attribute-based contract key for the user.
5. The user who wants to request EHR data submits an attribute-based contract key, makes a query with the keywords, and the needed access permission (read/write) through the blockchain. The signature of the requestor signs the queries.

6. The user-provider smart contract checks whether the user is from a valid registered clinical organization, the designation of the user, and the relationship of the patient whose data has been queried is checked.
7. If the attribute-based contract key of the requestor satisfies the attribute associated with the ciphertext stored in the cloud, the requestor can decrypt the data and can make modifications if write permission is granted.
8. The hash of the modified data, along with the query, is documented as a transaction in the blockchain with the requestor's signature and the clinical organization's signature to which the requestor belongs.
9. The patient whose medical record is queried then validate the modification by adding his/her digital signature.
10. Each transaction is validated by the signature of the patient, the signature of the requestor, the signature of the health provider the requestor belongs, the query, and the hash of the modified data.
11. After the transaction is validated, the block is mined to add the block to the chain. The data modified is permanently stored in the cloud if it is validated in the blockchain otherwise the modified data is removed from the cloud.

4.2 System components:

The proposed system contains the following components:

- a) Patient: the EHR owner to whom the medical records belong.
- b) Users: who makes query request. Users involve nurses, doctors, lab technicians, patients, etc.
- c) Clinical organizations: they form the consortium, which involves hospitals, health insurance companies, medical research organizations, pharmacies, etc.
- d) Cloud storage: where the EHR is fragmented according to the search keywords, IPE encrypted, and stored.
- e) Ethereum Blockchain: it is the network controlled by various clinical organizations and it is accountable for storing the hash of the data in the blockchain, encrypting the data, and key generation for the users.
- f) Search keywords: these are the attributes of a medical record - for example, department, prescription, lab report, diagnosis, etc.

Figure 1. System Architecture of Blockchain assisted Cloud-stored EHR

4.3 Smart contracts:

A smart contract is a term used in the blockchain is a series of digitally specified agreements, including protocols through which the parties make certain commitments (Szabo & The, 2018). Smart contracts are used in many cases for validating the legitimacy of contracts between two or more parties to the contract. The proposed blockchain-assisted cloud-stored EHR consists of six smart contracts: provider-provider contract, user-provider contract, Access control contract, IPE encryption contract, key generation contract, and permission contract.

4.3.1 Provider-provider contract:

This contract is responsible for developing a consortium. The clinical organizations join together to form the consortium and are responsible for validating the medical data being stored on the cloud. Only valid clinical organizations in the consortium will be able to sign the data modified by the requestor. Moreover, this contract is responsible for transaction validation and block mining.

4.3.2 User-provider contract:

The user-provider contract is responsible for user registration. This contract allows the user to submit the attributes and checks whether the user is registered under a valid provider in the consortium. Moreover, the contract is responsible for the validation of the modified data which was done by the user. If a user registered under a provider updates data in the EHR stored in the cloud, the data is validated only when the query transaction is signed by the user and the clinical organization the user belongs to.

4.3.3 Access control contract:

This contract is deployed in the patient node. The patient is responsible for controlling his/her medical records through which the patient is allowed to choose the users who can access the medical records by selecting the attributes. After the patient selects the attributes an access structure is generated. The contract stores the search keyword and the corresponding access structure such that the medical records stored under the keyword should be encrypted only by the particular access structure.

4.3.4 IPE encryption contract:

This contract fragment the medical records of the patient according to the search keywords. And the contract encrypts the data outsourced to the cloud according to the keyword and the access control specified by the user. Encryption should be done every time the data is updated in the cloud. It is executed by the clinical organization that is in the consortium verified by the provider-provider contract and the patient whose data is modified should be registered under the provider. It accepts the access control generated by the patient from the access control contract and encrypts the data.

4.3.5 Key generation contract:

Through this contract, a key is generated for the users according to their attributes submitted during the registration. This attribute contract key is used to decrypt the data stored in the cloud which is in encrypted form. The requestor can decrypt the requested data only if the attributes in the key satisfy the attributes used to encrypt the data. The contract checks whether the user who requests the key is registered under a valid clinical organization then it issues the key to the requested user.

4.3.6 Permission contract:

The permission contract is deployed in each patient node. When a requestor submits a query, it is sent to the patient. This contract then checks whether the requestor is a valid user under the clinical organization the patient is registered. If the requestor is a valid user, then access permission is granted to access the EHR by signing the query. After the permission is granted for the requestor, the query is diverted to the cloud storage, the cloud reply back with the encrypted data, which is stored under the queried keyword. The requestor can decrypt the data using the secret attribute key, which is received through the key generation contract.

4.4 System Architecture

This subsection describes the main operations of blockchain-based cloud-stored EHR. They are 1. user registration, 2. key generation, 3. EHR encryption, 4. accessing EHR, and 5. validating the updated EHR.

4.4.1 User registration

User registration is the process of adding a new node to the system of storing and access EHR outsourced to the cloud. Before the user has been registered to the system, they should create an Ethereum wallet and receive the Ethereum address. In the registration phase, the user who wants to access the EHR of patients submits their attributes, such as the designation, department, and clinical organization the user belongs to. If the user is a patient, then the patient has to submit to which hospital he/she is taking treatment. The patient can register in more than one clinical organization. By user registration, the user-health provider relation is made through the user-provider smart contract. Each user is identified by a globally unique identifier that is used for the validation process and the whole medical records of the patient are stored under this identifier. The public key generated by the during Ethereum wallet creation is the identity of the user. After user registration, the key structure is designed for each user as shown in figure 2. After that, the setup algorithm is run by the organizations in the consortium which outputs public parameters and master secret key.

Figure 2. Example key structure for patients and doctors

Setup Algorithm:

1. Select P a large prime number.
2. Compute g the generator of the cyclic group.
3. Form an array containing elements of Z_p .
4. Input d, i , and j where d is the depth of the key structure, i be the maximum level of the access structure and j be the number of attributes in the universe.
5. Choose random elements $\alpha_{1,1}, \alpha_{1,2}, \dots, \alpha_{i,j}, \beta_1, \beta_2, \gamma$ from Z_p .
6. Form two cyclic groups G, GT of the same order P .
7. Compute $g_{i,j} = g^{\alpha_{i,j}}$ which forms the group elements.
8. Compute $u = e(g, g)^{-\gamma}$.
9. Form $msk = (\alpha_{1,1}, \alpha_{1,2}, \dots, \alpha_{i,j}, \beta_1, \beta_2, \gamma)$
10. Form $PP = (G, GT, P, u, g_{i,j}, g^{\beta_1}, g^{\beta_2}, g^{1/\beta_1}, g^{1/\beta_2})$

4.4.2 User key Generation

Through the key generation contract, the user key is generated. It can be done only by the organizations in the consortium and the users should be registered under the provider. It takes the key structure of the user, pp , and msk as the input from the user-provider contract and outputs attribute-based keys for the users. The attribute-based key is

$$SK = g^{\gamma + r \sum_{i=1}^n \sum_{j=1}^m \alpha_{i,j} (K_{i,j})^{r_{i,j}}}, g^{(\gamma + r_1)/\beta_1}, g^{(\gamma + r_2)/\beta_2}$$

Key generation Algorithm:

1. If (provider in consortium and user under provider)
2. Input key structure of the user.
3. Generates an array of $K_{d,j} = (k_{1,1}, k_{1,2}, \dots, k_{1,j}, k_{2,1}, \dots, k_{d,j})$ from the key structure.
4. $K_{i,j} = Hash(K_{d,j})$

5. Choose randomly r from Z_p
6. Choose randomly r_1, r_2
7. Choose randomly $r_{1,1}, \dots, r_{i,j}$
8. Get input g from PP generated in the setup algorithm.
9. Get input msk from setup algorithm
10. Input n and m
11. For $i=1$ to n where n is the maximum level of access structure,
For $j=1$ to m where m is the number of attributes in the system
Calculate $D = SUM(\alpha_{i,j}(K_{i,j})^{r_{i,j}})$
12. Calculate $h = g^{(v+r_1)/\beta_1}, f = g^{(v+r_2)/\beta_2}$
13. Output $SK = g^{v+r \cdot D}, h, f$

4.4.3 Encrypting the EHR:

Encryption of patient medical records is done on the provider's node. Before encryption, the medical records are fragmented according to the search keywords. The search keywords are hierarchically arranged as shown in figure 3 so that for the contents under each keyword, access control can be designed by the patients as in figure 4. The proposed system adopted a monotonic tree access control structure. The content under the search keywords is encrypted using the attributes of the access control structure. For example, if the keyword is ECG, then the patient can design access control over the data within the keyword such as only the doctors from the cardiology department, and the lab technicians who take ECG report can make access to the data. Under the diagnosis keyword, the doctors of the cardiology department and the nurses of the particular hospital where the patient gets treatment can access the data. The access control was implemented using the access control smart contract. The proposed system adopted the access control mechanism designed as in (Exceline, Norman, Exceline, & Norman, 2019) which deployed NOT gate to reduce the user rejection time complexity. In the access control structure, the leaf nodes are the attributes needed to decrypt the medical record. And other non-leaf nodes are gates. Each node is determined by its threshold value. The threshold value t_x of each node ranges between $0 \leq t_x \leq num_x + 1$. Where num_x is the number of children node for node x . The threshold value for the nodes are set as follows.

- When the node is an AND gate then $t_x = num_x + 1$
- When the node is an OR gate then $t_x = num_x$
- When the node is a NOT gate then $t_x = 1$
- When the node is a leaf node then $t_x = 0$

Figure 3. Hierarchically fragmented medical records

Figure 4. Example access control structure

The provider can encrypt the data only if the patient is registered under the provider which can be checked through the user-provider contract. The access structure got from the patient deployed for the access structure contract. The access structure is converted to a two-dimensional array. That one dimension defines the level of the access structure and the other dimension defines the presence of attributes or gates in the access structure. For example, the matrix for the access structure for figure 4 is

$$W = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

The encryption algorithm takes access control W , and message M as input. It randomly chooses t , and s which is the element of Z_p^{ij} and compute the ciphertext as

$$CT = u^t \cdot M, g^t, g_{1,1}^t \cdot g^{sw_{1,1}}, g_{1,2}^t \cdot g^{sw_{1,2}} \dots \dots \dots, g_{n,m}^t \cdot g^{sw_{n,m}}$$

$$CT = C, C_0, C_{1,1}, \dots, C_{i,j}$$

Encryption Algorithm:

1. Input M
2. Choose t, s from Z_p^{ij}
3. Input PP from setup algorithm
4. Input W
5. $W_{i,j} = HASH(W)$
6. Calculate $C = u^t \cdot M, C_0 = g^t$
7. For $i=1$ to m
For $j=1$ to n
Calculate $C_{i,j} = g_{i,j}^t \cdot g^{sw_{i,j}}$
8. Output $CT = C, C_0, C_{i,j}$

4.4.4 Accessing the EHR:

The requestor who makes a query for the data in EHR submits the keyword related to their search. The requestor is validated by the user-provider contract. If the person is registered under a valid health provider and if the user received the attribute key through a key generation contract the access permission to the data is given by the patient whom the data is queried. The data in the cloud is made available to the requestor for accessing. Only if and only if the attributes of the user contract key matches the access control used to encrypt the data can decrypt and make changes. The decryption process takes the user attribute contract key and the ciphertext and outputs the original data, which was queried. The decryption algorithm takes the ciphertext and the attribute-based contract key as input and output the plaintext the requestor queried. The decryption equation is given by

$$C \cdot (e(g^\gamma, \prod_{i,j=1}^{n,m} (g_{i,j}^t \cdot g^{sw_{i,j}})^{K_{i,j}}) \cdot e(g^{\gamma+r \cdot \sum_{i=1}^n \sum_{j=1}^m \alpha_{i,j} \cdot K_{i,j}}, g^t)) = M$$

Decryption Algorithm:

1. Input CT, SK
2. $C_r = 1$
3. For $i=1$ to m
For $j=1$ to n
Calculate $C_r = C_r \cdot C_{i,j}$
Calculate $D = \sum_{i=1}^n \sum_{j=1}^m \alpha_{i,j} \cdot K_{i,j}$
4. Calculate $Y = g^{\gamma+r \cdot D}$
5. Apply pairing to generate $e(g^\gamma, C_r)$
6. Apply pairing to generates $e(Y, g^t)$
7. Calculate $M = C \cdot e(g^\gamma, C_r) \cdot e(Y, g^t)$

4.4.5 Validating the Process

If the requestor decrypts the data and updates the data, the data should be validated. The requestor who updated the data, the patient whom the data is updated and the provider to whom the requestor and the patient are registered should sign on the hash of the updated data. And the transaction is broadcasted on the blockchain. The transaction

is validated by the organizations in the consortium by checking the signatures on the hash value. After is validated by the consortium the transaction is updated in the block and made available to all the users in the system.

5. Implementation and Comparative Analysis

5.1 Implementation

Using the Ethereum open-source blockchain platform the proposed blockchain-assisted cloud-stored EHR system is implemented. A consortium blockchain based on Ethereum was developed on a Dell system with Intel i5 CPU 2.30 GHz, 16GB RAM, Linux Ubuntu system, and Windows 10 operating system. The simulation of smart contracts designed in the proposed system is coded with solidity programming language version 0.4.24 in the Remix integrated development environment. Then it is tested on the Rinkeby test network of Ethereum. An Ethereum Geth client is created under Linux Ubuntu operating system. The quorum nodes are initialized to form a consortium and the smart contract is deployed. The system comprises 4 health organizations, 20 health practitioners, 50 patients, and a total of 100 EHR participants who can request and access the EHR of the patients outsourced to the cloud. The proposed system developed an inner product encryption scheme using Java programming language with external java pairing-based cryptography (JPBC) library and it is combined with smart contracts using web3.js library.

5.2 Computational complexity

The computational complexity of the proposed blockchain assisted cloud-stored EHR is computed in this section. The computational cost of each algorithm is calculated according to the number of group elements, the number of pairing operations, the number of point multiplication done on the group, and the number of exponentiation operations done on the group. Table 1. shows the comparison of the computational complexity of each algorithm of the proposed system with other systems that adopted ABE to encrypt the medical record. Compared with the other two schemes that adopted ABE, the computational cost of encryption, and decryption algorithm of the proposed scheme is efficient. As we adopted the hierarchical key structure the key generation and PP cost are higher compared with the other two schemes but the hierarchical key structure provides flexible access to EHR.

Table 1. The comparison of the computational complexity of the proposed system

Algorithm	(H. Wang & Song, 2018)	(S. Wang et al., 2019)	Proposed System
Setup	$2 G + G_T $	$2 G + G_T $	$dU G + G_T $
Key generation	$j(G) + 2 G $	$j(G) + 2 G $	$dj(G) + 2 G $
Encryption	$nm(G) + G + G_T $	$3 G + G_T $	$nm(G) + G_T $
Decryption	$nm(G) + 3e$	$m(G) + 3e$	$nm(G) + 2e$

Where G, G_T are the two groups of same prime order p , U denotes the number of attributes in the Universe, d denotes the key structure depth, j denotes the number of attributes in the key structure, n denotes access structure depth, m denotes the number of attributes in the access structure, e denotes the pairing operation, bracket denotes point multiplication and ' $'$ ' denotes exponentiation operation.

5.2.1 Setup Algorithm Cost:

The computational cost to generate master secret key msk and public parameters PP depends on the number of exponentiation operations done to form the group elements in the group G . The number of exponentiation operations depends on the maximum depth of the key structure d and the number of attributes of the user in the universe U . One exponentiation operation is done on the group G_T . Therefore the computational cost for the setup algorithm is $dU|G| + |G_T|$.

5.2.2 Key generation Algorithm Cost:

The computational cost of generating the attribute-based contract key consists of two exponentiation operations in group G for the depth of the key structure d and dj point multiplication for the number of attributes in each depth of the key structure. So the computational cost for generating the attribute-based secret key for a user is $dj(G) + 2|G|$. The key generation cost is high compared to other schemes because the proposed scheme adopted the hierarchical key structure and multiple values for attributes.

5.2.3 Encryption Algorithm Cost:

The computational cost of encrypting the generated medical record depends on the depth of the access structure n and the number of attributes m present in the access structure. The encryption cost is calculated as $nm(G) + |G_T|$ because it performs nm point multiplication in the group G and one exponentiation in the group G_T . The encryption cost is low compared to other schemes because the number of exponentiation operation done for the attributes present in the access structure is less.

5.2.4 Decryption Algorithm Cost:

The computational cost of decrypting the medical record under a keyword is related to the number of key structure attributes that match the number of access structure attributes. The decryption cost is $nm(G) + 2e$ because it performs nm point multiplication in the group G and two pairing operations. The decryption cost of our scheme is low compared with the other two schemes. This is because the number of pairing operations done is small. The pairing operations done on the other two schemes are three while the proposed scheme is only two.

5.2.5 Comparison of execution time complexity:

Figure 5 shows the execution time of each algorithm proposed in the scheme concerning the number of attributes. The execution time of each algorithm is determined based on the attributes used to derive the attribute-based contract key and the attributes used to derive the ciphertext. The setup algorithm execution time is determined regarding the number of attributes present in the universe and the key generation algorithm execution time is determined by the number of attributes present in the users' key structure. Whereas the encryption algorithm and the decryption algorithm execution time is determined by the number of access tree attributes. The execution time of each phase is calculated concerning the number of attributes in the access structure and key structure such as 5,10,15 and 20. The execution time of each algorithm increases almost linearly based on the number of attributes.

Figure 5. The execution time of each algorithm in the proposed system

Figure 6 compares the execution time complexity of the proposed scheme with two other schemes (S. Wang et al., 2019) and (H. Wang & Song, 2018) that adopted attribute-based encryption to store and access EHR outsourced to the cloud. The (Thwin & Vasupongayya, 2019) scheme implemented ABE of (H. Wang & Song, 2018). Both

the schemes adopted basic ciphertext policy ABE of (Bethencourt, Sahai, & Waters, 2007). But the (H. Wang & Song, 2018) adopted the tree access structure to encrypt the message while (S. Wang et al., 2019) adopted a linear access structure. Compare with the other two schemes the proposed scheme in this paper shows low execution time complexity. The (H. Wang & Song, 2018) scheme adopted ABE shows that the execution time increases very high with an increase in the number of users resulting in scalability breach. The execution time of (S. Wang et al., 2019) scheme increases constantly little regarding the number of attributes but the overall execution time is more compared with the execution time of the proposed scheme in this paper. Because the execution time of (S. Wang et al., 2019) and (H. Wang & Song, 2018) is high due to three exponentiation operations done on the group for encryption algorithm and the decryption cost consists of three pairing operation and one exponentiation operation. The proposed scheme contains only point multiplication operation and one exponentiation operation in the encryption algorithm and only two pairing operation and point multiplication operations in the decryption algorithm. Because the proposed scheme calculates only the inner product of the vector derived from the attributes of the user, the overall execution time of the system is reduced compared with other schemes.

Fig 6. Comparison of execution time

5.3 Security Analysis

This subsection describes how the proposed blockchain assisted cloud-stored HER system effectively fulfills the security requirement of EHR.

5.3.1 Data Privacy:

Data privacy can be achieved only when the patient has full control over the EHR. In our proposed framework, data privacy is maintained by storing EHR in the cloud and not in the blockchain's public ledger, and the patient is allowed to choose the user by designing the access structure to access his / her EHR. Although the network is controlled by clinical organizations in the consortium, the access permission for the requestor is generated by the patient through the permission contract designed in the proposed system thus ensuring data privacy. Moreover, EHR is fragmented, to provide high data privacy such that the patient can provide access to a specific part of EHR to a particular user.

5.3.2 Data Integrity:

The proposed system maintains data integrity on cloud-stored EHR by providing flexible EHR access to the user through consortium blockchain. The distinction between the cloud-based approach and the consortium blockchain-assisted EHR is that once the data outsourced to the cloud is authenticated and the block is connected to the blockchain, the data can not be changed even though the consortium itself includes a malicious health organization.

5.3.3 User Privacy:

User privacy can be maintained by hiding the identities of the user to others who are in the network and to the cloud. As the proposed system adopts IPE, the attributes of the user are also hidden to other users and the cloud.

So tracing of identities of the users is not possible in the proposed blockchain-assisted cloud-stored EHR ensuring high user privacy.

5.3.4 Interoperability:

Interoperability is assured when many users from anywhere can able to access the EHR of patients. In a private blockchain, only limited users can be involved. As the proposed system adopts consortium blockchain and many organizations join together to form the consortium the system provides high interoperability compares to other schemes. Moreover, the system allows the patient to register with more than one provider so that they can share their EHR with multiple doctors to get efficient healthcare.

5.3.5 Fine-grained access control:

According to the search keywords, the tree access structure and hierarchically fragmented medical records provide greater fine-grained access control over other schemes for the users within the blockchain network. Access to specific records for a particular requestor can be provided by fragmenting the medical records. The requestor doesn't want to access a patient's entire record. Only the specific relevant data can be viewed and accessed by the requestor. This provides the users with the versatility to access the EHR.

5.3.6 Scalability:

The proposed blockchain-assisted cloud-stored EHR is based on a variety of concepts designed to encourage scalability. The blockchain stores only the hash of keywords and the hash of modified data, which requires very little storage space. Clinical organizations are maintaining their cloud and allow other organizations in the consortium to access their cloud. Moreover, the users attribute key generation and encryption of medical data of the patient is done on the organization's node. Organizations would already be equipped with high computational power thus the proposed system ensures scalability in terms of storage and computation.

5.3.7 Comparison of Security properties

Table 2 demonstrates the comparison of the proposed scheme's security properties with other blockchain-assisted cloud-stored EHR. From the table, the proposed scheme satisfies all the security properties needed for the secure sharing of EHR among various clinical organizations and users. All the schemes which adopted blockchain to assist access control of medical record to provide high data integrity. Using private blockchain for accessing EHR makes users trust a single authority and identity management is difficult. So the proposed system adopted a consortium blockchain formed by clinical organizations and the trust between each provider relies on the provider-provider smart contract. The attributes of the users are maintained by various clinical organizations in the consortium so identity management is not difficult in the proposed system.

Table 2. Comparison of security properties with other schemes

Schemes	Single Trusted Authority	Trust on cloud	Data Privacy	Data Integrity	User Privacy	Scalability	Fine-grained access control
(Dagher et al., 2018)	Yes	Yes	Yes	Yes	No	No	No
(Thwin & Vasupongayya, 2019)	Yes	-	No	Yes	No	Yes	Yes
(S. Wang et al., 2019)	Yes	Yes	Yes	Yes	No	Yes	Yes
(Yang & Yang, 2017)	Yes	-	Yes	Yes	No	Yes	Yes
(H. Wang & Song, 2018)	Yes	-	No	Yes	No	Yes	No
(Y. Wang et al., 2019)	No	Yes	Yes	Yes	Yes	Yes	No
(X. Zhu et al., 2019)	Yes	-		Yes	No	Yes	No

(L. Zhu et al., 2019)	Yes	-	No	Yes	Yes	Yes	No
(Nguyen, Pathirana, Ding, & Seneviratne, 2019)	No	-	Yes	Yes	No	Yes	No
Proposed system	No	Yes	Yes	Yes	Yes	Yes	Yes

5.4 Limitations and Recommendations:

This subsection discusses the limitation of the proposed blockchain-based cloud-stored EHR and gives an idea to overcome the limitation. They are as follows,

1. As the proposed system uses cloud storage, there is a need to trust the third party cloud server. There is a possibility for a single point of failure by crashing the cloud storage. Due to this, a breach in the availability of the data in the storage system occurs.
2. IPFS (the interplanetary file system) may be implemented instead of storing EHR in the cloud. IPFS is a distributed, peer-to-peer storage system that provides secure data storage by generating a data hash value. These hash values, which can not be modified, are stored in the blockchain. Furthermore, as the storage system is decentralized there is no need to trust a single authority.

Conclusion

In this paper, a novel blockchain-assisted cloud-stored EHR is proposed that ensures data privacy, user privacy, data integrity, and fine-grained access control. The proposed system adopted a consortium blockchain that controls the user group registered under various clinical organizations. Deploying consortium blockchain to store the search keywords and updated medical records hash value ensured high data privacy and integrity. The EHR of the patient is fragmented according to the search keywords stored in the blockchain gives access to specific records for a particular user. An attribute-based contract key is generated for the users to access the encrypted EHR outsourced to the cloud provided fine-grained access control over medical records. An inner product encryption algorithm is developed to encrypt the medical records which are to be outsourced to the cloud which also hides the access structure used to encrypt the medical record ensuring user privacy. Furthermore, the proposed system is efficient compared with similar approaches due to the low execution time complexity. As a future work IPFS, a decentralized, distributed storing system, can be deployed to store EHR, and access can be done through blockchain, which avoids the trust on third party cloud.

References

- Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. *Proceedings - IEEE Symposium on Security and Privacy*, 321–334. <https://doi.org/10.1109/SP.2007.11>
- Boneh, D., & Franklin, M. (2001). *Identity-Based Encryption from the Weil Pairing*. 213–229.
- Buterin, B. V. (2009). *A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM*. (January), 1–36.
- Cachin, C. (2016). *Architecture of the Hyperledger Blockchain Fabric **.
- Cao, S., Zhang, G., Liu, P., Zhang, X., & Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Information Sciences*, 485, 427–440. <https://doi.org/10.1016/j.ins.2019.02.038>
- Chatterjee, S., & Sarkar, P. (2011). *Identity based encryption*. Springer Science & Business Media.
- Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems*, 95, 420–429. <https://doi.org/10.1016/j.future.2019.01.018>
- Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for

- access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, 39(December 2017), 283–297. <https://doi.org/10.1016/j.scs.2018.02.014>
- Exceline, C. E., Norman, J., Exceline, C. E., & Norman, J. (2019). *EAI Endorsed Transactions Biometric based Multi-Authority Inner Product Encryption for Electronic Health Record*. 5(20), 1–13.
- Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). SYSTEMS-LEVEL QUALITY IMPROVEMENT MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *Journal of Medical Systems*, 42, 1–11. <https://doi.org/10.1007/s10916-018-0993-7>
- Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems. *IEEE Access*, 6, 11676–11686. <https://doi.org/10.1109/ACCESS.2018.2801266>
- Hylock, R. H., & Zeng, X. (2019). A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. *Journal of Medical Internet Research*, 21(8), e13592. <https://doi.org/10.2196/13592>
- Katz, J., Sahai, A., & Waters, B. (2013). Predicate encryption supporting disjunctions, polynomial equations, and inner products. *Journal of Cryptology*, 26(2), 191–224. <https://doi.org/10.1007/s00145-012-9119-4>
- Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *Journal of Medical Systems*, 42(8). <https://doi.org/10.1007/s10916-018-1007-5>
- Marco, I., & Karim, L. (2017). The Truth About Blockchain. *Harvard Business Review*. Harvard University.
- Nakamoto, S. (n.d.). *Bitcoin : A Peer-to-Peer Electronic Cash System*. 1–9.
- Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. *IEEE Access*, 7, 66792–66806. <https://doi.org/10.1109/ACCESS.2019.2917555>
- Szabo, N., & The, I. (2018). *Smart Contracts : Building Blocks for Digital Markets*. (c), 1–11.
- Thwin, T. T., & Vasupongayya, S. (2019). Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. *Security and Communication Networks*, 2019. <https://doi.org/10.1155/2019/8315614>
- Wang, H., & Song, Y. (2018). *BAB 2 PITA ezahan*. <https://doi.org/10.1007/s10916-018-0994-6>
- Wang, S., Wang, X., & Zhang, Y. (2019). A Secure Cloud Storage Framework With Access Control Based on Blockchain. *IEEE Access*, 7, 112713–112725. <https://doi.org/10.1109/access.2019.2929205>
- Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019). Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain. *IEEE Access*, 7, 136704–136719. <https://doi.org/10.1109/access.2019.2943153>
- Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. *IEEE Access*, 5(July), 14757–14767. <https://doi.org/10.1109/ACCESS.2017.2730843>
- Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information (Switzerland)*, 8(2). <https://doi.org/10.3390/info8020044>
- Yang, H., & Yang, B. (2017). A Blockchain-based Approach to the Secure Sharing of Healthcare Data. *Norwegian Information Security Conference*. Retrieved from <https://ojs.bibsys.no/index.php/NISK/article/view/462>
- Zhu, L., Wu, Y., Gai, K., & Choo, K. K. R. (2019). Controllable and trustworthy blockchain-based cloud data management. *Future Generation Computer Systems*, 91, 527–535. <https://doi.org/10.1016/j.future.2018.09.019>
- Zhu, X., Shi, J., & Lu, C. (2019). Cloud health resource sharing based on consensus-oriented blockchain technology: Case study on a breast tumor diagnosis service. *Journal of Medical Internet Research*, 21(7).

<https://doi.org/10.2196/13767>

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, 180–184.
<https://doi.org/10.1109/SPW.2015.27>

Author Biograph

Figures

Figure 1

System Architecture of Blockchain assisted Cloud-stored EHR

Figure 2

Example key structure for patients and doctors

Figure 3

Hierarchically fragmented medical records

Figure 4

Example access control structure

Figure 5

The execution time of each algorithm in the proposed system

Figure 6

Comparison of execution time