Blockchain-Based Electronic Health Records Sharing Scheme with Data Privacy Verifiable

Insaf BOUMEZBEUR* **and Karim ZAROUR**

LIRE laboratory, Faculty of NTIC, University Constantine2- Abdelhamid Mehri, Nouvelle ville Ali Mendjli BP67A, Constantine, Algeria.
E-mail(*): insaf.boumezbeur@univ-constantine2.dz

* Author to whom correspondence should be addressed; Tel. +213 (0) 31 78 31 69

Received: July 16, 2021/Accepted: November 22, 2021/ Published online: December 5, 2021

Abstract

We proposed architecture for sharing electronic health records. This work is based on an encryption mechanism to encrypt the health data, access control to ensure the privacy and confidentiality of health records. The proposed scheme has used a storage mechanism combining cloud and blockchain. The cloud server stores the encrypted health records, while the blockchain retains traceable log information and encryption keys. The proposal is an adequate solution to share the electronic health record securely. Our solution allows integrity, privacy, and confidentiality to ensure efficient protection of sharing electronic health records.

Keywords: Blockchain; Privacy; Cloud computing; Encryption; Electronic Health Record (EHR)

Introduction

The rapid growth of network information technology is also used in the healthcare field. The storing of patient's sensitive health data into Electronic Health Records (EHRs) has evolved rapidly. The EHR is a longitudinal electronic record of patient health information created by one or more interactions in any care delivery environment [1]. It comprises all required information about a patient, including the patient's basic information, demographic data, medical history, clinical and hospital data, providers' written notes, medications, and other patient-related data collected from multiple providers incorporating evidence-based methods to make informed decisions.

The sharing of such records can enhance the accuracy of the doctor's diagnosis and encourage the advancement of medical research. In addition, because the EHR can be acquired and maintained by various licensed health care professionals and transferred electronically among providers, the EHR can safeguard patient health. The growing usage of EHR systems by different healthcare organizations has considerably led to the gathering of sensitive health data. Besides treatments received by patients, patient health data may be utilized for additional reasons to enhance health outcomes and decrease related expenditures [2].

On another side, the EHR technology creates some issues, and it becomes easy to hack the data if the prior precautions have not been taken. As it is a new way of storing data, staff need proper training to use it. Electronic health records contain crucial and critical patient-related medical data, requiring safe storage, sharing, retrieval, and scope. The confidentiality of such data must be protected at all times, and access to such information must be cleared. Privacy is one of the main challenges limiting e-health providers from obtaining patient confidence and adopting e-health systems fully [3]. It also enables individuals to decide how their e-healthcare information is maintained and utilized by doctors and other users in areas outside healthcare. In addition, the success of e-healthcare and the fulfillment of its promises is reflected in safeguarding the privacy of patients' identifiable health information.

Blockchain technology has gained extensive interest from the healthcare industry due to its huge commercial potential and numerous applications. It can modernize the EHR exchanges by delivering a secure approach for medical, which can be an excellent solution for EHR and health data transfer. This technology is a form of distributed database that provides a secure, decentralized framework for the controlled diffusion of patient's EHRs in the healthcare sector.

In health care, multiple parties need to collaborate on the administration of individual EHR blockchains. It has been extensively practiced in current healthcare systems. More precisely, the present research has largely focused on securing patients' EHR, Personal Health Record (PHR), and medical data [3-8], mobile healthcare application [9], electronic prescription system [10, 11], traceability of COVID-19 Pandemic [12], and telemedicine industry [13].

Benefits of Blockchain in Healthcare

Blockchain promises to bring significant potential in the healthcare sector such as [14]:

- ✓ Secure data is saved and shared across a variety of parties.
- ✓ National data interoperability, as well flexible and quick invoicing and payment options
- ✓ Improve better patient information access.
- ✓ Enhance transparency and traceability.
- ✓ Guarantee data privacy and security.
- ✓ Validate the correctness of billing management.

Related Work

Ying et al. [4] presented a lightweight PHR system with strategy updating based on attribute-based encryption (CP-ABE). Instead of retrieving the entire ciphertexts, the PHR owners had to generate an updated key and upload it to the cloud server. However, the amount of processing required by the data owner can be increased to some level.

Blockchain-based searchable encryption for EHRs sharing scheme using blockchain is proposed by Chen et al. [5]. The authors used the blockchain to store the index for EHRs generated via complex logic expressions utilizing specified smart contracts. In this scheme, the real EHRs are stored in public cloud servers, while an index for each EHR is calculated using a complicated logic expression. This index is then recorded in the blockchain, giving data owners complete ownership over their information. Furthermore, this method enables effective EHR sharing among various users, with users obtaining permission privileges by authenticating themselves with the data owners.

A blockchain security framework (BSF-EHR) to secure and store EHRs effectively is proposed by Abunadi and Kumar [7]. BSF-EHR offers patients access to extensive, consistent records and free access to EHRs. With this framework, the patients can independently manage, download and share their EHRs.

Based on the consortium blockchain, the work of Qin et al. [8] provided a secure sharing protocol for electronic medical records combining the cloud and consortium blockchain. The cloud server is utilized to save the ciphertext of the original medical records, while the blockchain retains verifiable log information and medical record index. The authors have categorized the medical institutions in medical treatment combinations and improved the preselection node mechanism of the PBFT consensus algorithm to enhance the reliability and security of the system.

Liang et al. [9] have created and implemented a mobile healthcare system for exchanging personal health data between individuals and healthcare providers. This application can safely collect health data, exchange them with healthcare and insurance providers, and synchronize them with cloud services. The authors utilized the blockchain network to assure data integrity, individual data ownership, and data privacy.

With a particular healthcare system, Ramani et al. [15] proposed a blockchain-based secure and effective data access method for the patient and the doctor to protect the confidentiality and privacy of the patients set by the elliptic curve cryptography (ECC). The proposed system is also capable of safeguarding patients' privacy. This scheme's security research reveals that it can withstand well-known attacks while retaining system integrity.

Zhao et al. [16] utilize access control technology, information entropy technology, and blockchain technology to improve medical data security, improve data integrity, promote the exchange of trusted data, and decentralize medical data management so that patients have more control over data sharing and privacy protection.

Our objective was to realize blockchain-based EHR sharing that incorporates integrity, privacy, and confidentiality to protect health data efficiently.

Material and Method

In contrast to the the solutions available in the scientific literature, we have used the encryption key to enforce the confidentiality of the EHR. Moreover, unlike the proposals by Chen et al. [5], Kumar [7], Liang et al. [9], Ramani et al. [15], and Zhao et al. [16], we have used hybrid encryption to guarantee patient privacy and EHR confidentiality. Furthermore, we have used the smart contract in our solution, which is not the case in the solutions of Abunadi and Kumar [7], Qin et al. [8], and Liang et al. [9], to ensure access control.

The Proposed System

To fulfill the needs for blockchain in shared EHR systems, we propose a blockchain-based security scheme for sharing EHRs to preserve patient's privacy and ensure data integrity. Figure 1 shows the difference between the traditional EHR system and the proposed scheme.

In the conventional EHR system:
(1) The patient visits the doctor.
(2) Then, the doctor treats the patient.
(3) After therapy, the doctor uploads the EHR to the server.
(4) For future use, the doctor can download the EHR.

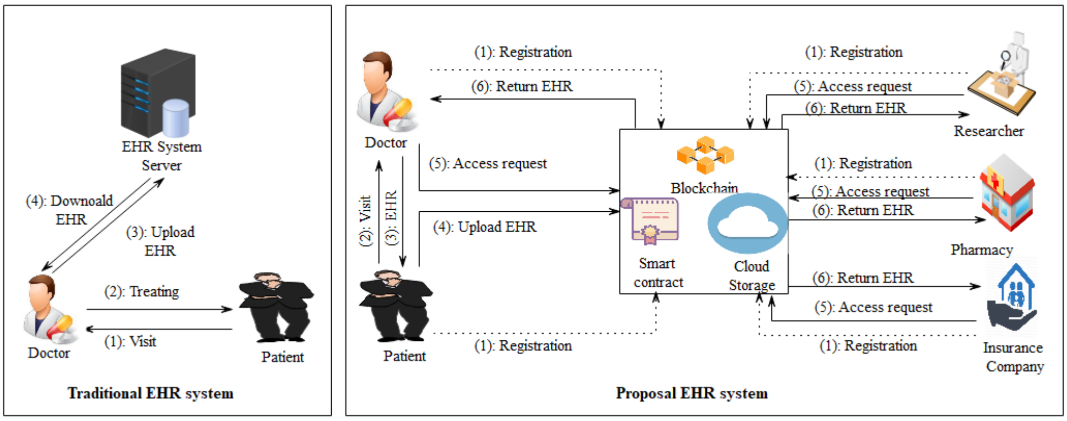


Figure 1. Architecture overview of the proposed solution

Our approach may be portrayed as revolutionary secure EHRs of patients, which institutions or patients may confidentially share. In which the patient can manage, download, and exchange his/her EHRs autonomously.

In the proposed scheme:
(1) All users must be registered to the system to generate and store keys.
(2) The patient visits doctors in hospitals or medical institutions for healthcare treatment.
(3) He/she obtains his/her electronic health records, including individual private health data that will be generated after the examination.
(4) The patient uploads the encrypted files directly to the cloud storage and submits the healthcare data to the blockchain.
(5) The user (maybe pharmacy, physician, or researcher) sends requests to get access to the file.
(6) User receives the encrypted files from the health cloud to get the original file.

Thus, the patient can only access his/her EHR records for the access control procedure, and no one else can read the details. Moreover, the doctor may only review the EHR of patients whom he/she has treated. Finally, a doctor or other users can only access EHR that he/she has the owner permission to see it.

Architectural Description

Our architecture contains the following components: actors (patient, doctor, pharmacist, analyst, physician, or researcher), cloud storage, blockchain, an encryption mechanism, smart contract, electronic health record, and a web portal.

Actors. In the proposed system, the actors concerned are:

- Patient: who visits doctors in hospitals or medical institutions for healthcare treatment. He/she obtains his/her electronic health records, including individual private health data that will be generated after their consultation and treatment.
- Doctor: via a web application, he/she can write prescriptions, consult the patient's medical record with his/her consent, or add an observation if necessary.
- Other users such as pharmacists, analysts, physicians, or researchers have obtained authorization from the appropriate data owner to view the healthcare record data. The pharmacist, for example, obtains patient prescriptions to provide medications to patients.

Electronic Health Record (EHR). It is critical to remember that the EHR has all required patient information acquired from various sources. They are built to be portable between organizations. If you have an EHR, it will have information from all clinicians you have encountered. Furthermore, because the EHR contains all of a patient's health information illustrated in Figure 2, it is a significant data source that must be carefully secured. Further, distributed EHR sharing allows patients to access their medical information online easily, controlling their health care. The patients can actively engage in the coordination of their treatment by giving their health information to other clinicians as part of the process of managing their health information.

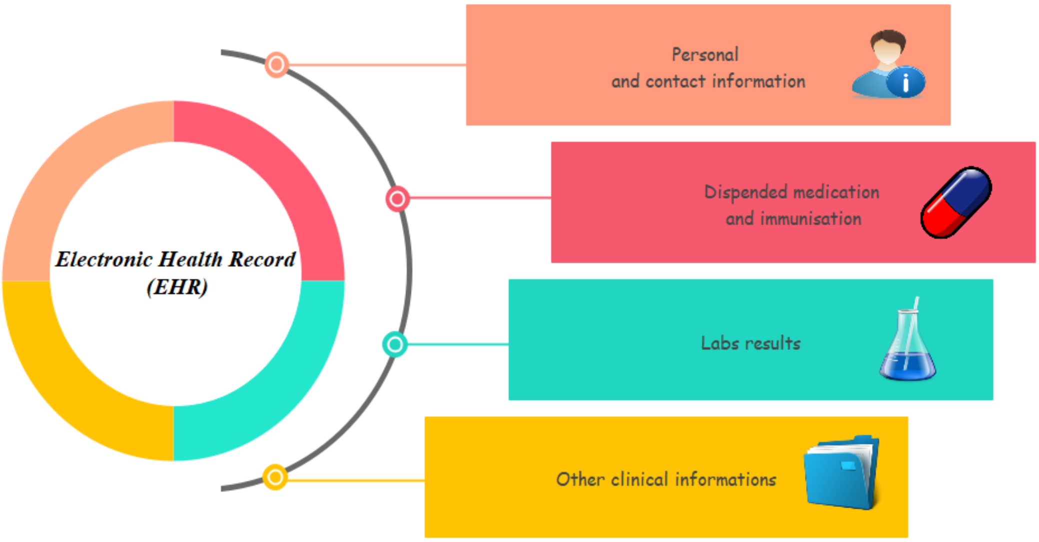

Electronic Health Record (EHR)
Personal and contact information
Dispended medication and immunisation
Labs results
Other clinical informations

Figure 2. The compenent of EHR

When comparing EHR with Electronic Medical Record (EMR), we can state that EHR is an inter-organizational system that contains data from all clinicians and health organizations engaged in a patient's treatment. While EMR provides data from a single health institution, this is highly beneficial for all clinicians and employees who may use this information to treat a patient. Furthermore, unlike EMRs that are local and internal, such as those used in a clinic or hospital, EHRs enable information sharing and are interoperable. To put it another way, EMRs are not interoperable, which is also their major flaw. Table 1 shows the difference between the EHR and the EMR.

Table 1. Difference between EHR and EMR

Indicator	EHR	EMR
Content	Clinicians' and laboratories' medical data	Medical data obtained from an internal clinical system
Accessibility	Interoperable (inter-organizational system)	Internal organization with limited access
Source data	Clinician or analyst from a variety of sources	A single provider's clinician
function	Organizational information exchange	Internal medical record
Use cases	Used for medical decision making, analytics, research, communications between physicians and patients	Used only to diagnose and treat patients.
Data management capabilities	The information available in real-time	Historical data tracking
Data sharing capabilities	Multiple teams may quickly exchange and access information over the internet	There is no exchange of information across teams

EHR requirements are:

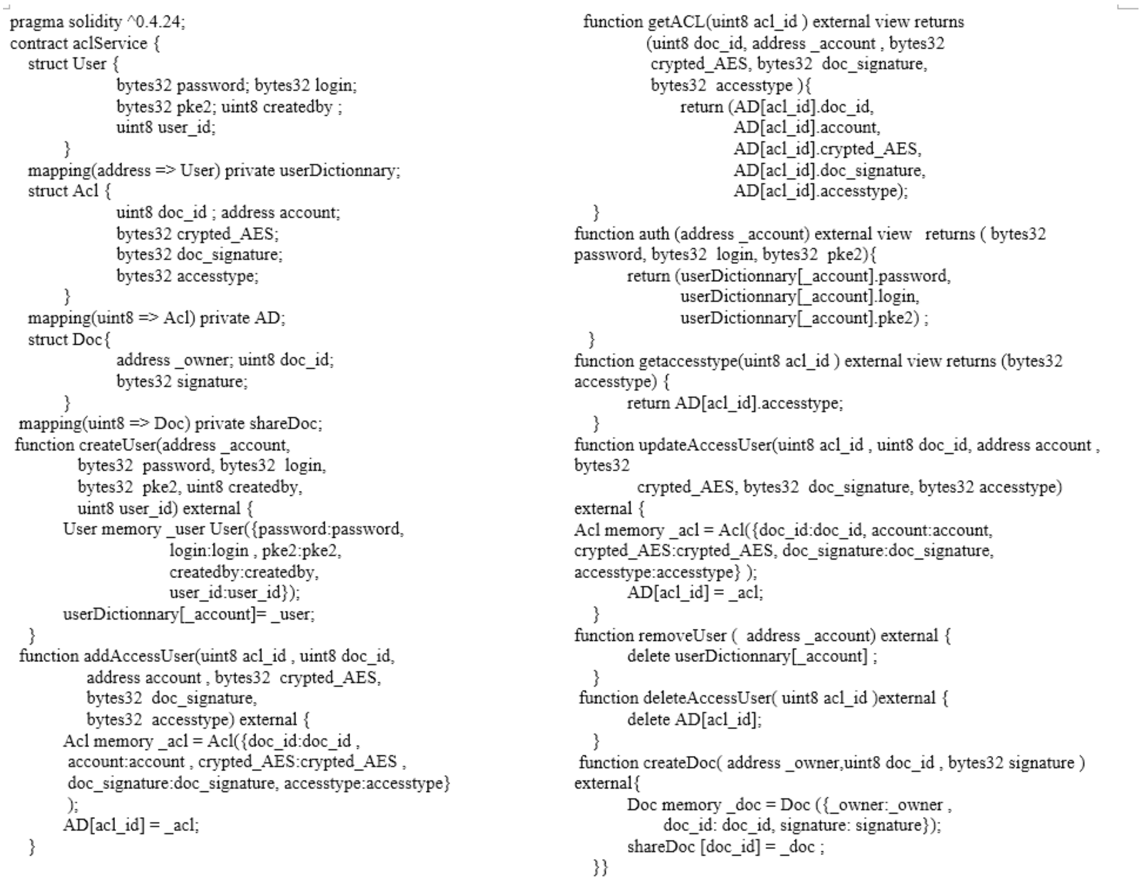
- *Privacy and security:* In the healthcare setting, security and privacy are meant to give patients the authority to control their medical information by issuing authorization.
- *Access control:* Only authorized health providers and patients should have access to medical information. Patients should be able to view their data and control who has access to it.
- *Data sharing:* Because the patient's treatment is dispersed across multiple health care providers, medical records must be exchanged; as a result, the data must be shared with other medical institutions and the government.
- *Data Integrity and Availability:* The term "integrity" refers to the data's efficiency and consistency. It results in the fact that data has not been harmed due to unapproved usage in EHR.

Blockchain. In the field of healthcare, blockchain offers several applications and uses. The ledger technology allows for the secure transfer of patient health information, the management of the pharmaceutical supply chain, and the assistance of healthcare researchers in unlocking genetic code. We used blockchain to retain an incorruptible, decentralized, and transparent log of all patient data. It is ripe for securing electronic health records.

Moreover, while blockchain is transparent, it is also private, concealing any individual's identity behind complex and secure protocols to protect medical data sensitivity. The technology's decentralized nature allows patients, doctors, and healthcare professionals to share the same information quickly and securely. The Ethereum blockchain was chosen because it enables the execution of smart contracts, allowing decentralized applications to be built on top of it. Ethereum was the first blockchain platform to introduce the notion of smart contracts, which is why smart contract-based decentralized healthcare applications are so popular.

Smart contract. It is a code executable, modular and reusable, developed and installed into the blockchain to affect any task when specific conditions are met. It allows anonymous participants to conduct transactions and agreements without requiring a central institution, external enforcement, or legal system. In other words, we have chosen the Smart Contract to connect with the blockchain and healthcare providers based on their needs and manage the patient's healthcare information by controlling the healthcare record's access control. It is also used to check and verify all of a user's access rights and user authentication. The smart contract is essential for implementation since it executes or performs the agreement between the many parties engaged in the system. By generating the codes, a smart contract may be established, and these codes describe the agreement signed by the patient. The contract sends a transaction to be placed on the blockchain when it has been validated. The proposed scheme's smart contract is shown in Figure 3. Our scheme uses Remix as a smart contract development tool, produces smart contracts in the Solidity language, and deploys the produced contracts on the Ethereum test network Rinkeby. The cost of deploying a contract

(DeployContract), adding a user (AddUser), removing a user (RemoveUser), adding an EHR (AddEHR), and removing an EHR (RemoveEHR) were all investigated.



```
pragma solidity ^0.4.24;
contract aclService {
   struct User {
               bytes32 password; bytes32 login;
               bytes32 pke2; uint8 createdby ;
               uint8 user_id;
       }
   mapping(address => User) private userDictionnary;
   struct Acl {
               uint8 doc_id ; address account;
               bytes32 crypted_AES;
               bytes32 doc_signature;
               bytes32 accesstype;
       }
   mapping(uint8 => Acl) private AD;
   struct Doc{
               address _owner; uint8 doc_id;
               bytes32 signature;
       }
  mapping(uint8 => Doc) private shareDoc;
 function createUser(address _account,
          bytes32  password, bytes32  login,
          bytes32  pke2, uint8 createdby,
          uint8 user_id) external {
        User memory _user User({password:password,
                      login:login , pke2:pke2,
                      createdby:createdby,
                      user_id:user_id});
        userDictionnary[_account]= _user;
   }
  function addAccessUser(uint8 acl_id , uint8 doc_id,
           address account , bytes32  crypted_AES,
           bytes32  doc_signature,
           bytes32  accesstype) external {
        Acl memory _acl = Acl({doc_id:doc_id ,
         account:account , crypted_AES:crypted_AES ,
         doc_signature:doc_signature, accesstype:accesstype}
         );
        AD[acl_id] = _acl;
   }
```

```
  function getACL(uint8 acl_id ) external view returns
           (uint8 doc_id, address _account , bytes32
            crypted_AES, bytes32  doc_signature,
            bytes32  accesstype ){
                return (AD[acl_id].doc_id,
                        AD[acl_id].account,
                        AD[acl_id].crypted_AES,
                        AD[acl_id].doc_signature,
                        AD[acl_id].accesstype);
   }
function auth (address _account) external view   returns ( bytes32
password, bytes32  login, bytes32  pke2){
        return (userDictionnary[_account].password,
                userDictionnary[_account].login,
                userDictionnary[_account].pke2) ;
   }
function getaccesstype(uint8 acl_id ) external view returns (bytes32
accesstype) {
        return AD[acl_id].accesstype;
   }
function updateAccessUser(uint8 acl_id , uint8 doc_id, address account ,
bytes32
          crypted_AES, bytes32  doc_signature, bytes32 accesstype)
external {
Acl memory _acl = Acl({doc_id:doc_id, account:account,
crypted_AES:crypted_AES, doc_signature:doc_signature,
accesstype:accesstype} );
        AD[acl_id] = _acl;
   }
function removeUser (  address _account) external {
        delete userDictionnary[_account] ;
   }
 function deleteAccessUser( uint8 acl_id )external {
        delete AD[acl_id];
   }
 function createDoc( address _owner,uint8 doc_id , bytes32 signature )
external{
        Doc memory _doc = Doc ({_owner:_owner ,
              doc_id: doc_id, signature: signature});
        shareDoc [doc_id] = _doc ;
   }}
```

Figure 3. The Smart contract code

Cloud storage. We have used to store the encrypted EHRs uploaded by the patient.

Web Portal. The portal is the first level of security. It allows access to certain functions and EHR information by associating a user name and a password. Patients will access information about their health data and some information that health care providers transmit to them. Other actors have access to the applications intended for them according to their role in the EHR process.

Encryption mechanism. With symmetric encryption, there is just one key used to encrypt and decrypt data. Algorithms employing this technique are highly fast but not as strong as with asymmetric encryption. Asymmetric encryption is considered more secure as it does not involve sharing keys, but it takes more time than symmetric encryption and tends to be slower. Therefore, we have opted for combining symmetric and asymmetric encryption. The reason to use hybrid encryption is that Symmetric encryption is used to transform the plaintext to ciphertext. This makes use of the symmetric encryption speed. To take advantage of asymmetric encryption's security, the asymmetric key is used to encrypt the symmetric key, ensuring that only the intended receiver may decrypt the symmetric key.

Access control ensures the confidentiality and integrity of EHR. Medical information should then be accessible only to authorized healthcare specialists and patients. Patients should obtain their data and provide control over who can access it. The patient specified in the smart contract makes such access decisions. If a third party or unknown entity attempts to access the system, the smart contract will reject the request, and the system will be terminated.

The user retrieving health data must have the patient's permission and approval access. In addition, the patient is the only one who has the access right access privileges to alter or add the doctor's information, and they may only add one other person to see the patient's record. The smart contract verifies the access right before getting the health data to ensure that the doctor has access to the patient's data. The system sends a false message and aborts the session if the doctor does not have access control.

Scenario

All actors go through the web portal to interact with the system. Each user must be registered to the system to generate and store keys. Figure 4 illustrates these interactions:

1: The patient visits the doctor in hospitals or medical institutions.

2: The patient obtains his/her electronic health records, including individual private health data generated after the interactions with the doctor.

3: The patient accesses the portal through his user ID and password.

4: The patient adds his EHR to the system.

5: The patient adds a user's access right to his/her EHR according to the user's role.

6: After encryption, the EHR will be uploaded as an encrypted form to the cloud storage.

7: The patient Uploads the encrypted key and other information to the blockchain.

8: All transactions request are saved to the blockchain

9: Users send an access request to the system with key information to retrieve EHR.

10: The smart contract verifies the access user and decrypts the encrypted key

11: Retrieves encrypted EHR from the cloud and decrypt it

12: The user downloads the EHR and consults it.

13: The user can make a change in patient EHR according to his/her access.

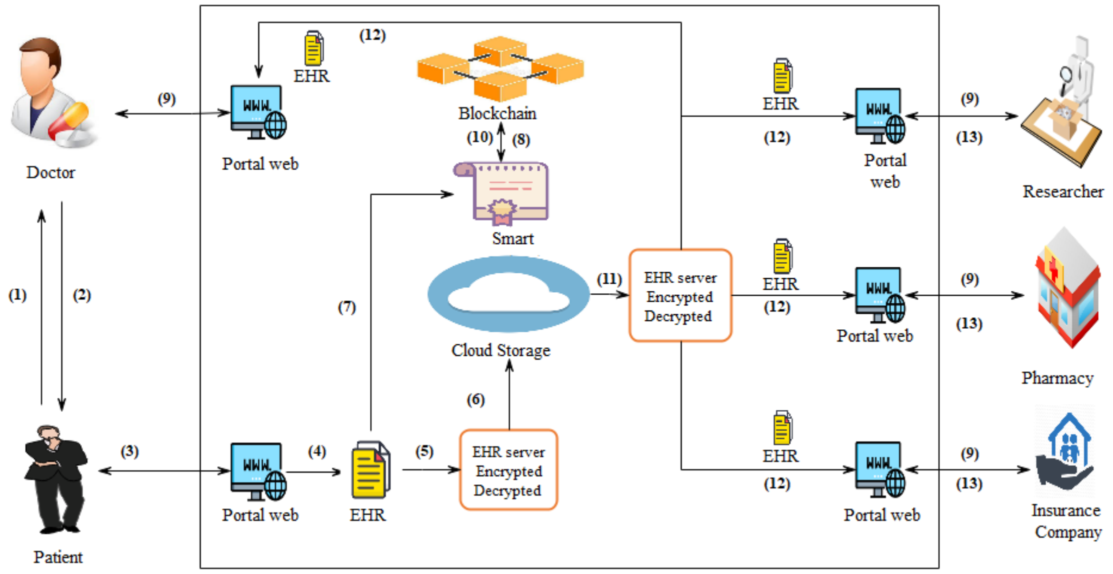


Figure 4. Interactions in the system

Prototype Implementation and Transaction Fees

The feasibility and practicality of the proposed architecture is shown using the following scenario:

- The patient consults a doctor.
- The doctor examines and diagnosis the patient.
- Patient logs into the system.
- The patient can upload his/her record or update it in case if it previously exists.
- The patient can add, update or remove access users for his/her record.

- The patient can view his health record as well as the record user's list.

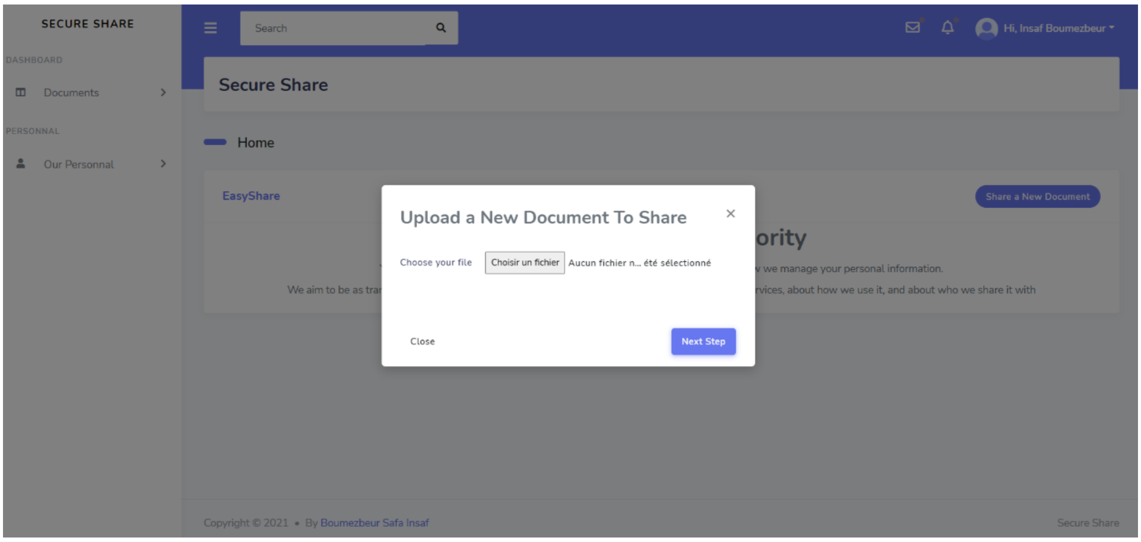
The transaction fees in Ethereum are determined in 'ETH,' which is the Ethereum coin, which includes units such as *wei* and *gwei* connected with it. The product of gas consumed and gas price is the transaction cost for a transaction. It could be expressed in the following way:

$$\text{Transaction Fee} = \text{gasUsed} * \text{gasPrice}$$

Results

Prototype Implementation

After the patient accesses the system by inserting his/her email and password, he adds his health record illustrated in Figure 5, and he must add an access role for his/her record. If the user does not exist in the user list, the patient can add it by inserting his/her name and email. After that, he can give him access according to the user role, as shown in Figure 6. Then the health record will be encrypted and uploaded as an encrypted form to the cloud.



Upload a New Document To Share

Choose your file [Choisir un fichier] Aucun fichier n... été sélectionné

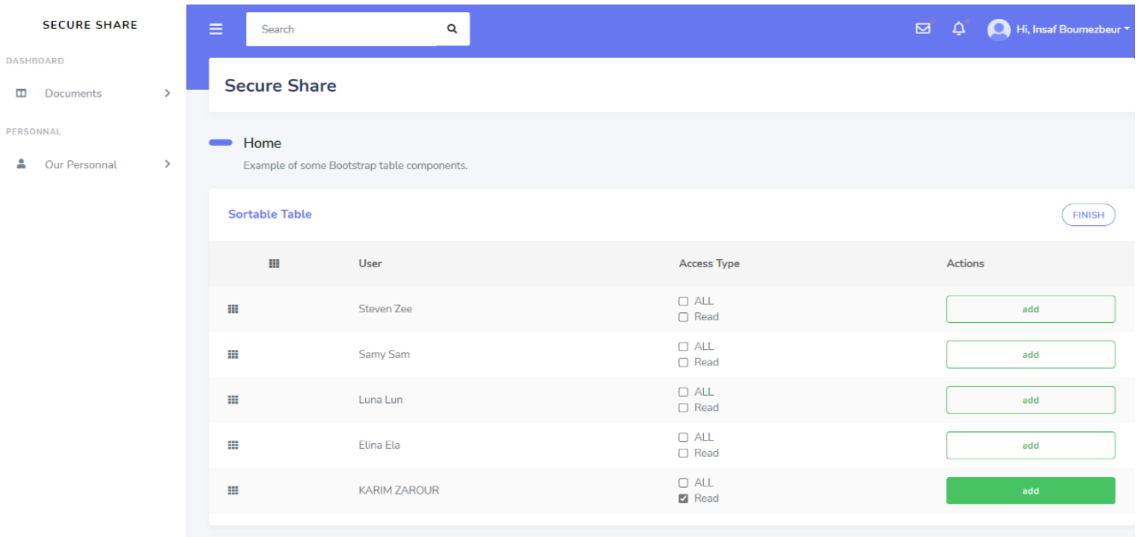
ority

We aim to be as tra… …v we manage your personal information.

…rvices, about how we use it, and about who we share it with

Copyright © 2021 • By Boumezbeur Safa Insaf — Secure Share

Figure 5. Upload a health record

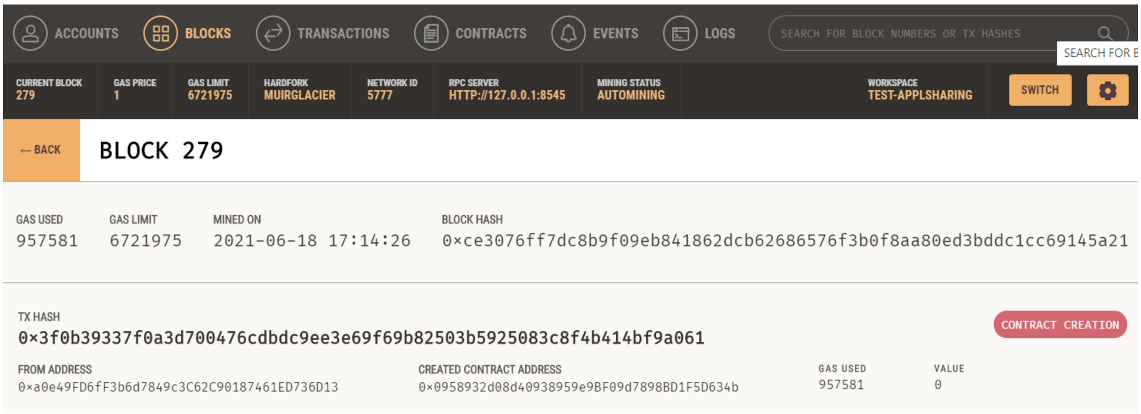


Example of some Bootstrap table components.

▦	User	Access Type	Actions
▦	Steven Zee	□ ALL □ Read	add
▦	Samy Sam	□ ALL □ Read	add
▦	Luna Lun	□ ALL □ Read	add
▦	Elina Ela	□ ALL □ Read	add
▦	KARIM ZAROUR	□ ALL ☑ Read	add

Figure 6. Adding users access

All operations in the system are saved as a transaction in the blockchain. For example, Figures 7 and 8 show an Ethereum transaction to deploy a smart contract that calculates gas used for each block, as well as, a screenshot of the Etherscan website (etherscan.io), which displays transaction details and fees.



CURRENT BLOCK 279
GAS PRICE 1
GAS LIMIT 6721975
HARDFORK MUIRGLACIER
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:8545
MINING STATUS AUTOMINING
WORKSPACE TEST-APPLSHARING

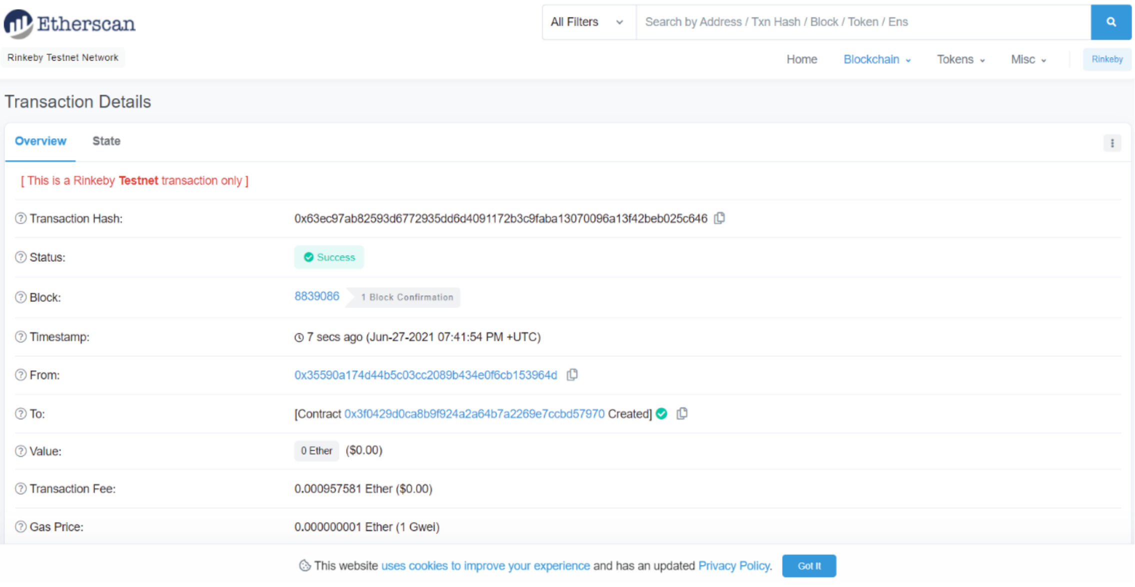
BLOCK 279

GAS USED	GAS LIMIT	MINED ON	BLOCK HASH
957581	6721975	2021-06-18 17:14:26	0×ce3076ff7dc8b9f09eb841862dcb62686576f3b0f8aa80ed3bddc1cc69145a21

TX HASH
0×3f0b39337f0a3d700476cdbdc9ee3e69f69b82503b5925083c8f4b414bf9a061
CONTRACT CREATION

FROM ADDRESS	CREATED CONTRACT ADDRESS	GAS USED	VALUE
0×a0e49FD6fF3b6d7849c3C62C90187461ED736D13	0×0958932d08d40938959e9BF09d7898BD1F5D634b	957581	0

Figure 7. Ethereum blockchain block (captured 18/06/2021)



Transaction Details

[This is a Rinkeby **Testnet** transaction only]

Transaction Hash:	0x63ec97ab82593d6772935dd6d4091172b3c9faba13070096a13f42beb025c646
Status:	Success
Block:	8839086 1 Block Confirmation
Timestamp:	7 secs ago (Jun-27-2021 07:41:54 PM +UTC)
From:	0x35590a174d44b5c03cc2089b434e0f6cb153964d
To:	[Contract 0x3f0429d0ca8b9f924a2a64b7a2269e7ccbd57970 Created]
Value:	0 Ether ($0.00)
Transaction Fee:	0.000957581 Ether ($0.00)
Gas Price:	0.000000001 Ether (1 Gwei)

This website uses cookies to improve your experience and has an updated Privacy Policy.

Figure 8. Transaction example from the Etherscan (captured 27/06/2021)

Test Results

Test results of the compiled contract are obtained directly from the Ethereum test network Rinkeby, as shown in the example in Figure 8. The cost of deploying the contract, addUser, removeUser, addEHR and removeEHR are shown in Table 2. The deploy contract operation is done at the startup step at 0.000958 Ether. The addUser operation is done during the EHR sharing to add an access user to EHR, and the cost of the operation is 0.000042 Ether. Furthermore, once the patient deletes a user from the system, the removeUser action is conducted to remove the user's authorization, and the cost of the operation is 0.000027 Ether.

On the other hand, the patient to add new EHR and their user access list uses AddEHR, and the operation will cost 0.000106 Ether. While RemoveEHR operation is used to delete the encrypted EHR and their authorized users, the cost of this operation is 0.000017 Ether. The function executions are inexpensive. The execution costs of these functions vary depending on the lengths of the various inputs, such as attribute information and other associated data.

Table 2. Smart contract fee test

Operations	Gas used	Cost (ether)
DeployContract	957581	0.000958
AddUser	42192	0.000042
RemoveUser	27314	0.000027
AddEHR	106285	0.000106
RemoveEHR	17141	0.000017

Discussion

Our results show that the executions of smart contract functions are inexpensive, implying that blockchain technology could be cost-effective for EHR sharing while ensuring the privacy, confidentiality, and integrity of these shared EHRs. Several authors are widely proposed blockchain-based systems in the healthcare field to secure the sharing of health data. Contrary to Zhao et al. [16], which saves all blockchain records, this article uses cloud storage technologies to relieve the strain on blockchain storage and meet real-world deployment requirements. Chen et al. [5] created a system that needs the patient to give the private key to the doctor for data access; however, the transmission mechanism cannot guarantee the privacy of the private key, and hostile nodes may gain access to it. Our proposal has used a hybrid encryption mechanism to provide more security to gain from each encryption benefit as long as the encryption keys are completely secure. In our scheme, the original EHR is encrypted and then outsourced to the cloud server. This overcomes the problem of limited blockchain storage capacity and significantly minimizes the risk of privacy information in the original electronic health data being disclosed.

Unlike each of several previously solutions [4, 8, 7, 9, 15], our solution used the smart contract to store the encryption key securely, verified user authentification, and assured user access control.

Our proposed scheme protects the patient's privacy by allowing granular access control over his or her EHR data to be specified using smart contracts (Figure 3). Furthermore, it operates based on a decentralized network structure with no single point of failure. Our solution safeguards EHR data against security threats such as unauthorized access. It is based on the roles of the defined users, as shown in Figure 6. As a result, malicious users will be unable to access EHR data. It also gives high-speed, secure access to EHR data according to the patient's preferences. Indeed, it ensures the availability of EHR data items without the need for any third-party validation. Table 3 gives some differences between the traditional EHR system and Blockchain-based EHR system.

Table 3. Comparison traditional EHR system vs. blockchain EHR system

Feature	Traditional EHR system	Blockchain-based EHR system
Decentralisation	Low	High
Security	Medium	High
Transparency	Low	High
Immutability	No	High
Veracity	Low	High

Table 4 demonstrates the comparison of the proposed system to other current works presented in this paper regarding blockchain, smart contract, access control, privacy, integrity, hybrid encryption, healthcare data, and key encryption. '✓' and '✗' to denote that the features are available or not.

Table 4 shows that all schemes can meet the attributes of privacy preservation and integrity, but not all solutions can provide access control, which is a critical security goal in an EHR sharing system. We observed that smart contracts are only utilized by a few works, while hybrid encryption is only used by Qin et al. [8]. Through comparison, our scheme performs better than these similar studies in terms of functions such as privacy protection, access control, and data integrity. Moreover, it presents a feasible alternative for updating existing e-health systems, including hybrid encryption, encryption keys, and smart contract.

Table 4. Comparison of the proposed framework with related work

System	Blockchain-based	Smart contract	Access control	Privacy preservation	Integrity	Hybrid encryption	Encryption key
[4]	✗	✗	✓	✓	✓	✗	✗
[5]	✓	✓	✗	✓	✓	✗	✗
[7]	✓	✗	✓	✓	✓	✗	✗
[8]	✓	✗	✗	✓	✓	✓	✗
[9]	✓	✗	✓	✓	✓	✗	✗
[15]	✓	✗	✓	✓	✓	✗	✗
[16]	✓	✓	✓	✓	✓	✗	✗
[17]	✓	✓	✓	✓	✓	✗	✗
Our solution	✓	✓	✓	✓	✓	✓	✓

Nonetheless, this work has some limitations:

- There is a possibility that the EHR could be intercepted while it is being encrypted.
- It is challenging to demonstrate stakeholders' satisfaction empirically due to the diversity of their professional and technological backgrounds and their reluctance to change, which may condition the solution's success.

As future work, we envisage several possible extensions or improvements to our system, such as security. Indeed, given the number of medical transactions, specific attacks on the blockchain can stop the entire system.

Conclusions

A sharing electronic health record scheme to store EHRs effectively and securely, using cloud computing and blockchain technology was successfully implemented. Two encryption methods were successfully combined to ensure data sharing and user data privacy. The proposal used a system in a cloud environment to decrease the load on blockchain, improve efficiency and security, and use a specified smart contract on blockchain to replace the centralized server. Additionally, we have assessed that our proposed scheme could satisfy privacy, confidentiality, integrity, and access control criteria.

Conflict of Interest

The authors declare that they have no conflict of interest.

Acknowledgments

The PRFU project partially supports this research under the number C00L07UN250220200002.

References

1. HIMSS. [updated unknown; cited 2021 Jun 17]. Available from: https://www.himss.org/

2. Yue L, Nortey RN, Adjeisah M, Agbedanu PR, Lui X. Blockchain Enabled Privacy Security Module for Sharing Electronic Health Records (EHRs). International Journal of Computer and Communication Engineering 2019;8(4):155-168. doi: 10.17706/ijcce.2019.8.4.155-168
3. Bajrić S. Data Security and Privacy Issues in Healthcare. Applied Medical Informatics 2020;42(1):19-27.
4. Ying Z, Jang W, Cao S, Liu X, Cui J. A lightweight cloud sharing PHR system with access policy updating. IEEE Access. 2018;6:64611-64621. doi: 10.1109/ACCESS.2018.2877981
5. Chen L, Lee WK, Chang CC, Choo KKR, Zhang N. Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Systems. 2019;95:420-429. doi: 10.1016/j.future.2019.01.018
6. Pournaghi SM, Bayat M, Farjami Y. MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. Journal of Ambient Intelligence and Humanized Computing 2020;11:4613-4641. doi: 10.1007/s12652-020-01710-y
7. Abunadi I, Kumar RL. BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients. Sensors. 2021;21(8):2865. doi: 10.3390/s21082865
8. Qin Q, Jin B, Liu Y. A Secure Storage and Sharing Scheme of Stroke Electronic Medical Records Based on Consortium Blockchain. BioMed Research International 2021;2021:6676171. doi: 10.1155/2021/6676171
9. Liang X, Zhao J, Shetty S, Liu J, Li D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). 2017, pp. 1-5. doi: 10.1109/PIMRC.2017.8292361
10. Zarour K, Fetni MO, Belagrouz S. Towards Electronic Prescription System in a Developing Country. Applied Medical Informatics 2021;43(1):56-67.
11. Lupşe OS, Stoicu-Tivadar L. Extracting and Structuring Drug Information to Improve e-Prescription and Streamline Medical Treatment. Applied Medical Informatics. 2018;40(1-2):7-14.
12. Reegu FA, Daud SM, Alam S, Shuaib M. Blockchain-based Electronic Health Record System for efficient Covid-19 Pandemic Management. Preprints 2021, 2021040771. doi: 10.20944/preprints202104.0771.v1
13. Ahmad RW, Salah K, Jayaraman R, Yaqoob I, Ellahham S, Omar M. The role of blockchain technology in telehealth and telemedicine. International Journal of Medical Informatics 2021;148:104399. doi: 10.1016/j.ijmedinf.2021.104399
14. Theodouli A, Arakliotis S, Moschou K, Votis K, Tzovaras D. On the design of a blockchain-based system to facilitate healthcare data sharing. 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). 2018, pp. 1374-1379. doi: 10.1109/TrustCom/BigDataSE.2018.00190
15. Ramani V, Kumar T, Bracken A, Liyanage M, Ylianttila M. Secure and efficient data accessibility in blockchain based healthcare systems. 2018 IEEE Global Communications Conference (GLOBECOM). 2018, pp. 206-212, doi: 10.1109/GLOCOM.2018.8647221
16. Zhao Y, Cui M, Zheng L, Zhang R, Meng L, Gao D, et al. Research on electronic medical record access control based on blockchain. International Journal of Distributed Sensor Networks 2019;15(11):1550147719889330. doi: 10.1177/1550147719889330
17. Xia QI, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 2017;5:14757-14767. doi: 10.1109/ACCESS.2017.2730843