International Journal on Cybernetics & Informatics (IJCI) Vol.13, No.4, August 2024

# Empowering Healthcare: A Blockchain-Based Secure and Decentralized Data Sharing Scheme with Searchable Encryption

Seyedmohammad Nouraniboosjin[1], Melika Yousefi[2], Sadaf Meisami[3], Melina Yousefi[4], and Sajad Meisami[2]

[1]Worcester Polytechnic Institute, Worcester, USA
[2]Illinois Institute of Technology, Chicago, USA
[3]Kharazmi University, Tehran, Iran
[4]Isfahan University of Technology, Isfahan, Iran

**Abstract.** Medical care is one of the most important parts of human lives, and now with the invention of the internet of things(IOT) and cloud computing streamlining the treatment process is becoming a main topic of research. The problem is the sensitivity of the medical data which raises concerns about data privacy in the system. storing vast amount of patients' data in the cloud which is controlled by a single trusted third party is common nowadays but, this manner poses great privacy risks and security concerns because it makes it possible for the cloud to use the stored data for illegal purposes. In this paper we try to answer this question that 'how to resolve these problems using the blockchain technology?'. we propose a novel protocol that combines Blockchain technology and cryptographic primitives such as ring signature and searchable encryption in order to remove the need for a trusted third party and providing an efficient privacy preserving access control mechanism. Also when it comes to the applications of the blockchains in areas other than cryptocurrencies, combining this technology to other cryptographic primitives can lead to unique features. In this paper we used ring signatures in order to protect the patients' privacy and also by using the blockchain technology we were able to eliminate the need for a trusted third party and provide security for a searchable encryption scheme.

**Keywords:** Blockcchain, IOT, privacy, cryptography, searchable encryption

## 1 Introduction

The corona virus epidemic has affected people's lives in many aspects in different parts of the world. Also, the spread of its different variants makes it difficult to treat and deal with. Comprehensive research is done to produce a vaccine, and medical and biological methods are also used to diagnose and treat this disease. At the same time as this disease spreads, the best way to deal with it is monitoring and controlling .As a result of this, it is inevitable to use new technologies to deal with the corona virus. Technologies such as: artificial intelligence, big data , blockchain, 5G internet ,etc. can be used to diagnose and track this disease[12].

Recent advances in communication technology have provided the basis for the use of new methods of telemedicine and can respond to the increasing need for access to medical services. Also,In the case of epidemic, the need for remote treatment increases dramatically, in order to avoid unnecessary movements of patients and the spread of the virus. therefore, the use of IOT, cloud computing and blockchains should take priority in hospitals[4].

Suppose that the patient stores their data on a cloud server to use telemedicine technology so that doctors and health care providers can provide online and remote services.This requires full trust in the server, because patients have uploaded their health data to the cloud, and the Server may behave dishonestly. For example, selling patient's data to drug

Bibhu Dash et al: COMSCI, IOTCB, AIAD, EDU, MLDA, EEEN - 2024
pp. 47-55, 2024. IJCI – 2024
DOI:10.5121/ijci.2024.130405

companies, or add fake data to a patient's history, or remove specific data from a patient's file. On the other hand, patients or doctors may also behave dishonestly.

In this paper we introduced a novel architecture for the blockchain network that is capable of recording the transaction history of health providers and patients while preserving the privacy.

### 1.1 organization

section 2 will describe the related work involved in this research. Section 3 covers the security and privacy challenges that we address in our work. Sections 4 provides an overview of the system model, while section 5 explains the structure of our scheme in detail. Section 6 discusses the security and privacy of the proposed model, and section 7 provides a conclusion.

## 2 related work

when it comes to storing data on a cloud, Lots of potential parties want to use the data for different applications. Take the data stored on social networks like Instagram for example, it's quit easy to use this data to anticipate the needs of the customers and emerging trends or pharmaceutical companies can use the patients' health records for producing new medicines. In this case the patient's privacy is crucial. Although this data is useful for lots of purposes, there is always the possibility of revealing this important and private data and invading the privacy of the patient. As a result of this some solutions are purposed by researchers.

k-anonymity[9] is one of the methods that is used to protect the personally identifiable information. In this scheme any recorded data is indistinguishable from at least k1 other important recorded data, However this method is vulnerable against background knowledge attack[11].

In order to protect data against background knowledge attack the concept of differential privacy[6] has been proposed. In this method a zero mean noise is added to the data before forwarding it for the client. This method is not appropriate for medical goals since noisy data is usable in medical diagnoses.

Fully homomorphic encryption[7] is another scheme that allows us to evaluate the functions on the encrypted data, but due to its heavy computations it is not suitable for IOT devices.

Blockchain[15] technology was introduced in 2008 for the first time. With their transparent and immutable structure, blockchains provide a good potential for the management of cloud based services.Researchers have proposed schemes to use blockchain in health data[17] [14] [1],for example in [16] authors use blockchain to share electronic health records. In this scheme the admin issues the transactions that contain the uploading and downloading data and these transactions are recorded on the blockchain by the miners, but the main problem with this scheme is full trust in the admin. Another scheme is proposed by[8] that utilizes the blockchain technology in internet of things ,although it is less dependent on full nodes but the privacy of the users has not been considered. In recent years some other schemes[13, 18] are proposed that utilize the applications of blockchains in the management of the medical data.

## 3 Security and privacy challenges

Due to their nature and direct impact on the well-being of patients, electronic health records are of the great importance. As a result of this, the underlying system responsible

for managing this records should take security and privacy considerations into account. An immutable and transparent distributed ledger would help us to meet this considerations but still we need to address some challenges.

### 3.1 Security

To start, we need to provide some clear definitions to asses our scheme accordingly.

**Definition 1 (Privacy).** *A scheme is called privacy preserving if its public data does not reveal any thing about the private data of the users[5].*

**Definition 2 (Authentication).** *In authentication we can verify the correctness of the identity of the users. In other words, only valid users are able to make changes on the blockchain[2] .*

**Definition 3 (integrity).** *Integrity means that the downloaded data is exactly the uploaded one and it's guarded against improper information modification or destruction[2].*

### 3.2 searching in encrypted data

In our scheme we utilize searchable encryption that allows miners of the blockchain network search in data without threatening the security and confidentiality of the messages. a searchable encryption scheme usually consists of these functions[3].

- KeyGen(s): Gets the security parameter and generates the public key private key pair.
- PEKS($A_{pub}$, W): Takes the public key and the keyword and generates searchable encrypted keywords S.
- Trapdoor(W,$A_{priv}$): Takes private key and the keyword and generates the trapdoors $T_w$.
- Test($A_{pub}, T_w, s$): Tests if the keyword for the trapdoor and the encrypted keyword are the same or not.

  This primitive also brings about it's own challenges and security considerations.

- completeness: When a doctor sends a keyword to the miners, miners have to find all the co responding files. For their own benefits, some miners may refuse to perform complete search. This is because a miner gets his reward after processing and submitting the information. Therefore it's essential to design a system which guarantees the completeness of the search results.
- keyword guessing attack (KGA): Using the public key of the searchable encryption $PK_{peks}$ and a valid trapdoor $T_W$ of of keyword $W$ and set of possible keywords $\{W_1, W_2, ..., W_{|W|}\}$ attacker can perform keyword guessing attack[19]:
  - set i=1.
  - create searchable encrypted data $C = PEKS(PK_{peks}, W_i)$
  - Now if the $TEST(C, T_W, PK_{peks})$ is equal to 1 our guess is correct if not increment i and do the previous step again.
- data injection attack[21]: when the server wants to send the data to doctors may inject some faulty data and this may cause serious errors in the diagnose and treatment process.

# 4 System model

In this section we introduce the different parts of our system. As shown in figure 1 our scheme has five main parts.

1. control center
2. storage unit
3. miners
4. patients
5. doctors

## 4.1 Control center

This unit is a backbone to our scheme, initialization of the protocol and submitting new users are the responsibilities of the control center. When a doctor or a patient wants to use our network needs to get the control center's permission. When a member signs up to the network Control center adds their public key to the public key table in the distributed ledger.

## 4.2 storage unit

All the collected data from patients is stored in storage unit.

## 4.3 miners

Miners are individual parties that compete with each other in maintaining and updating our distributed ledger. Processing the transactions and running the smart contracts are done by miners in the blockchain network.

## 4.4 patients

Electronic health records of the patients are collected by their smart phones and sent to the storage unit. Patients are data owners in our scheme.

## 4.5 doctors

As data users, doctors send download requests to the control center and after their request is granted by the control center the required data is forwarded for the doctors.

# 5 Proposed Scheme

In this section we explain our scheme in detail.

## 5.1 Data uploading phase

Our goal is to set up a network that patients are able to get the permission to upload their data from the blockchain network. On one hand it's necessary to authenticate the patients in advance and digital signature is a way to do so, on the other hand the privacy of the patients is important and through using the conventional digital signature schemes the identity of the patients is revealed. Therefore we use ring signature in order to authenticate the patients. This is because ring signature allows the patients to prove their membership in a set(legitimate patients) without revealing their identity.

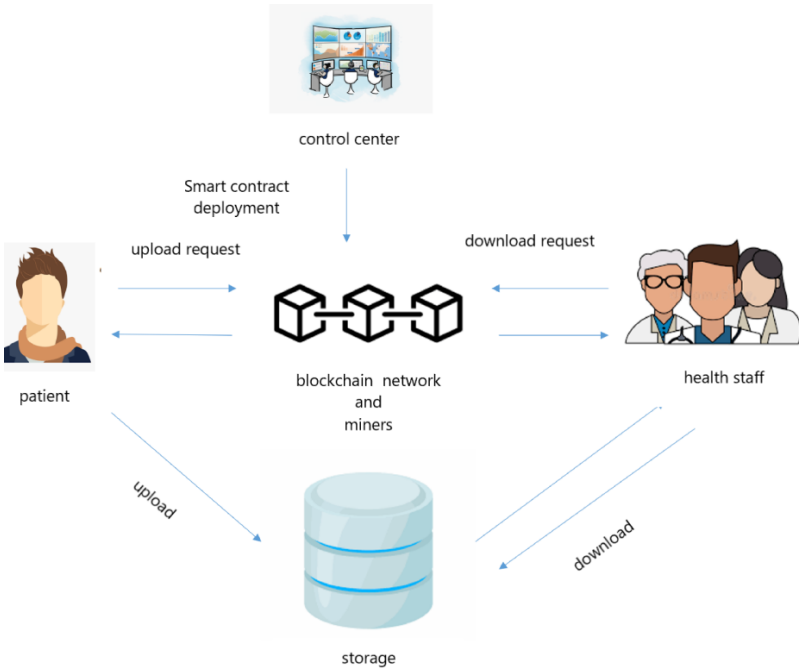


**Fig. 1.** proposed scheme:In our scheme all the parties send transactions to the blockchain network

**Table 1.** List of abbreviation and acronyms

| abbreviation/acronyms | definition |
|---|---|
| H(.) | hash function |
| C | cipher text |
| $W_i$ | keyword |
| PK | public key |
| ED | expiration date of a transaction |
| S | ring signature |
| $C_E$ | the set of encrypted keywords |
| Tx | transaction |
| Results | the results of the search |
| valid PKs | the set of valid public keys |
| L | distributed ledger memory |
| Enc(.) | encryption function |
| verif(.) | verification function |
| cipherG(.) | searchable encryption function |
| Dtrapdoor | trapdoor generation function |
| FuzzTest(.) | fuzz test function |
| ExactTest(.) | exact test function |

**Upload Transaction** Assume that the data is collected from the sensors and is ready to be uploaded in the cloud. Firstly, the patient needs to encrypt the data, to do so, encrypts the original data using a symmetric encryption scheme and gets $C_1$ and then encrypts the key $K_{sym}$ using the public key of the doctor. Also to be stored in the distributed ledger the patients gets the hash of the data.

$$C_1 \leftarrow Enc(M, K_{sym})$$

$$C_2 \leftarrow Enc(K_{sym}, PK_{doctor})$$

$$C = C_1||C_2$$

$$H_M = H(M)$$

Now the patient should issue the ring signature. In our scheme we use [10] because it's privacy preserving, efficient and secure. In order to issue this signature first we choose two multiplicative cyclic groups $G_1$ and $G_2$ of the same order $q$. $P$ and $Q$ are two random members of $G_1$ and $G_2$ and $e$ is a bilinear map from $G_1 \times G_1$ to $G_2$:

- the patient chooses $n-1$ points from $G_1$
- computes $h_i = H(A_i, H_M, pk_1, pk_2, .., pk_n)$
- chooses a random $t \in Z^*$ and computes:
  $A_p = tP - \sum_{i-p}^{n}(h_i pk_i + A_i), h_p = H(A_p, H_M, pk_1, ..., pk_n), B = (t + h_p S_p)Q$
- the ring signature is $S = \{A_1, ..., A_n, B\}$

After ring signature, the patients creates searchable encrypted keywords that lets the miners to search in encrypted data while revealing nothing about the data itself. In this scheme we use [19] because it is secure against keyword guessing attack. Keywords encompasses the necessary information about the patient. In order to create the searchable encrypted keyword, the patient first chooses the key words and the and uses $pk_{PEFKS}$ to encrypt them.

$$C_i =\leftarrow CipherG(W_i, pk_{PEFKS})$$

$$C_E = \{C_1, C_2, ..., C_m\}$$

After creating $C_E$ , the patient sends a transaction to the blockchain network. The transaction contains $C_E$,$S$,$PK_{doctor}$ and$H_M$ as a request to upload the data.

**Upload transaction validation** Upon receiving the upload request transaction the miners follow the algorithm 1 to grant the upload request.

**Algorithm 1** upload request validation

**input:**$T_x(C_E, H_M, S, PK_{doctor})$
**output:** upload permission
**if** $A_1, A_2, ..., A_n \in validPKs$& $verif(S) == 1$ **then**
$L \leftarrow L \bigcup Tx$ **Else** $return0$
**end if**

**Table 2.** Comparison of different Schemes.

| Scheme | Searchable Encryption | Privacy preserving | Decentralized structure |
|---|---|---|---|
| Meisami[13] | - | ✓ | ✓ |
| Xia [18] | - | ✓ | ✓ |
| Yang [20] | ✓ | ✓ | - |
| Nguyen[16] | - | - | ✓ |
| He [8] | - | - | ✓ |
| proposed scheme | ✓ | ✓ | ✓ |

### 5.2 Data downloading phase

**Download request** Assume that a doctor wants to download the data of his patient. Firstly, the keywords and their trapdoors should be determined. In the next step, the doctor sends a transaction to the blockchain network containing the following information.

- TD : trapdoors
- $PK_d$: doctors public key
- $\sigma$ : digital signature

**Download transaction validation** Miners validate the download request by following the algorithm 2.

**Algorithm 2** Download request validation

**input:**$T_x(TD, PK_d, \sigma)$
**output:** download permission
**if** Verif($\sigma$)==1 **then**
  **for** *each* $Tx \in L$
  **if** $FuzzTest(TD) == 1$ & $ExactTest(TD) == 1$ & $blocknumber \leq ED$ **then**

$$Results \leftarrow Results \bigcup Tx$$

  **end if**
**end if**

### 5.3 Public key table

updating the public key table is one of the responsibilities of the control center. When a doctor or a patient wants to use the network the miners process their transaction only if the public key(s) used by them is in the public key table. In a case that a doctor or patient shows faulty behaviour control center immediately deletes their public key from the table.

## 6 security and privacy analysis

### 6.1 Comparison

In this section first we compare our scheme with other schemes in the literature from privacy distributed structure and the capability of searching in the encrypted data. The blockchain is used in [13] and [18], and in [13] a off-chain secure channel is established between the doctor and the patient, but in [18] a public key encryption is used in the blockchain network. But still none of the papers used searchable encryption in their scheme. [20] is a data sharing scheme that utilizes the searchable encryption primitive but in a centralized system.

### 6.2 security analysis

In this section we asses our scheme from different

- privacy: As mentioned before we have used the ring signature to authenticate the clients. As a result of this, while processing the transactions the miners are not able to reveal the identity of the patients.
- Authentication: In our scheme the clients of the network (the doctors and the patients) need to be signed up by the control center in advance. Therefore it is not possible for an illegitimate user to send a transaction to the network because the valid public keys are stored in the blockchain and they do not have access to the private keys.
- integrity: Before sending an encrypted data to the storage unit, the patients store the hash value of that data on the distributed ledger. As a result of this, it is impossible to manipulate the data because upon receiving the data from the storage unit the doctors check the hash value of the data with the stored one on the blockchain.
- completeness: the completeness of the search results is one of the biggest challenges. In order to save time and computational power, the miner may refuse to search the ledger completely. In such cases, since they have access to trapdoors, other miners and members of the network are able to do the searching and realize that the search results are not complete and do not accept the block.

## 7 conclusion

Such as all other networks, in electronic health record sharing systems security and the privacy are of the great importance. The proposed schemes can be used only if they guarantee this security and privacy aspects. Due to its nature health data has a great impact on the patients well-being, therefore outsourcing this data is quit challenging. In this paper we proposed a scheme that uses the decentralized structure of the blockchain networks to eliminate the trust in third parties and also, searchable encryption is used to let the miners of the network search freely in the encrypted data. For the future steps using multiparty computation schemes or zere-knowledge proofs in designing such systems should be considered.

## References

[1] Rayan Anwar Abutaleb, Saad Said Alqahtany, and Toqeer Ali Syed. “Integrity and privacy-aware, patient-centric health record access control framework using a blockchain”. In: *Applied Sciences* 13.2 (2023), p. 1028.

[2] Elaine B Barker et al. “Recommendation for Key Management-Part 1: General (Revised)(March 2007 edition)”. In: (2007).

[3] Dan Boneh et al. “Public key encryption with keyword search”. In: *International conference on the theory and applications of cryptographic techniques*. Springer. 2004, pp. 506–522.

[4] Antonio Celesti et al. “Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds”. In: *Sensors* 20.9 (2020), p. 2590.

[5] Tore Dalenius. “Towards a methodology for statistical disclosure control”. In: *statistik Tidskrift* 15.429-444 (1977), pp. 2–1.

[6] Cynthia Dwork. “Differential privacy: A survey of results”. In: *International conference on theory and applications of models of computation*. Springer. 2008, pp. 1–19.

[7] Craig Gentry. *A fully homomorphic encryption scheme*. Stanford university, 2009.
[8] Songlin He et al. "Decentralizing IoT management systems using blockchain for censorship resistance". In: *IEEE Transactions on Industrial Informatics* 16.1 (2019), pp. 715–727.
[9] Kristen LeFevre, David J DeWitt, and Raghu Ramakrishnan. "Mondrian multidimensional k-anonymity". In: *22nd International conference on data engineering (ICDE'06)*. IEEE. 2006, pp. 25–25.
[10] Chia-Chen Lin, Chin-Chen Chang, and Yao-Zhu Zheng. "A Ring Signature Based Anonymity Authentication Scheme for Group Medical Consultation". In: *Symmetry* 12.12 (2020), p. 2009.
[11] Ashwin Machanavajjhala et al. "l-diversity: Privacy beyond k-anonymity". In: *ACM Transactions on Knowledge Discovery from Data (TKDD)* 1.1 (2007), 3–es.
[12] Elliot Mbunge et al. "A critical review of emerging technologies for tackling COVID-19 pandemic". In: *Human behavior and emerging technologies* 3.1 (2021), pp. 25–39.
[13] Sajad Meisami, Mohammad Beheshti-Atashgah, and Mohammad Reza Aref. "Using Blockchain to Achieve Decentralized Privacy In IoT Healthcare". In: *arXiv preprint arXiv:2109.14812* (2021).
[14] Sajad Meisami et al. "Combining blockchain and IOT for decentralized healthcare data management". In: *arXiv preprint arXiv:2304.00127* (2023).
[15] Satoshi Nakamoto and A Bitcoin. "A peer-to-peer electronic cash system". In: *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf* 4 (2008).
[16] Dinh C Nguyen et al. "Blockchain for secure ehrs sharing of mobile cloud based e-health systems". In: *IEEE access* 7 (2019), pp. 66792–66806.
[17] Venkatesh Upadrista, Sajid Nazir, and Huaglory Tianfield. "Secure data sharing with blockchain for remote health monitoring applications: a review". In: *Journal of Reliable Intelligent Environments* 9.3 (2023), pp. 349–368.
[18] QI Xia et al. "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain". In: *IEEE Access* 5 (2017), pp. 14757–14767.
[19] Peng Xu et al. "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack". In: *IEEE Transactions on computers* 62.11 (2012), pp. 2266–2277.
[20] Yang Yang and Maode Ma. "Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds". In: *IEEE Transactions on Information Forensics and Security* 11.4 (2015), pp. 746–759.
[21] Yupeng Zhang, Jonathan Katz, and Charalampos Papamanthou. "All your queries are belong to us: The power of file-injection attacks on searchable encryption". In: *25th {USENIX} Security Symposium ({USENIX} Security 16)*. 2016, pp. 707–720.