HiLL PUBLISHING

Advances in Computer and Communication, 2024, 5(3), 158-164
https://www.hillpublisher.com/journals/acc/
ISSN Online: 2767-2875

A Medical Data Storage and Sharing Model Based on Blockchain

Yaqiong Zhang*, Hui Zhang

School of Information Engineering, Yulin University, Yulin 719000, Shaanxi, China.

How to cite this paper: Yaqiong Zhang, Hui Zhang. (2024) A Medical Data Storage and Sharing Model Based on Blockchain. *Advances in Computer and Communication*, 5(3), 158-164.
DOI: 10.26855/acc.2024.07.001

Received: May 31, 2024
Accepted: June 30, 2024
Published: July 30, 2024

***Corresponding author:** Yaqiong Zhang, School of Information Engineering, Yulin University, Yulin 719000, Shaanxi, China.

Abstract

Aiming to address the issues of centralized storage, low sharing efficiency, and privacy disclosure of medical data, this paper proposes a security sharing model for medical data based on blockchain technology. The model utilizes bilinear mapping for authentication, enabling bidirectional authentication between patients and hospitals. By combining AES and ABE encryption algorithms for fine-grained access control of medical data, the model employs searchable encryption technology to facilitate secure search of medical data. The effectiveness of the proposed authentication scheme is analyzed using BAN logic, considering storage overhead and computational cost. The results indicate that the security model presented in this article fulfills various security requirements during the authentication process, ensuring secure sharing of medical data. Furthermore, in terms of accessibility, the average communication time and cost are reduced, meeting the integrity, privacy, and availability requirements for medical data storage and sharing.

Keywords

Medical data; Data Storage; Data Sharing; Blockchain; BAN logic; Bilinear mapping

1. Introduction

With the continuous development of technologies such as the Internet of Things, AI, and blockchain, smart healthcare is also gradually advancing Wearable devices, smart sensors, and other devices generate a large amount of medical data for the convenience of data sharing, more and more medical institutions are starting to store medical data on cloud servers. However, medical data involves a large amount of patient privacy information. Once the cloud server is attacked or accessed by unauthorized users during the sharing process, it may cause medical data to be tampered with or patient privacy information to be leaked. Therefore, it is very important to ensure that medical data stored in the cloud server is not accessed by unauthorized users [1, 2].

It proposes a fine-grained access control scheme based on a ciphertext policy attribute encryption algorithm to solve the privacy leakage problem in the process of electronic medical record sharing [3]. The attribute encryption scheme based on ciphertext strategy not only achieves fine-grained data access control but also encrypts electronic medical records. It combines blockchain and attribute encryption to achieve secure sharing of medical data. Firstly, encrypt medical data and store the ciphertext on a cloud server [4, 5]. Then, the storage address of the encrypted data and medical-related information is uploaded to the blockchain, which not only ensures efficient data storage but also alleviates the storage overhead of the blockchain. Secondly, in order to address the issues of medical data privacy and signer identity leakage, while also ensuring the authenticity and trustworthiness of medical data sources, this scheme combines Attribute-Based Encryption (ABE) and Attribute-Based Signature (ABS).

Blockchain organizes data into specific block structures, which form a chain structure in chronological order. By using consensus algorithms and cryptographic techniques, it ensures the integrity and security of the data [6]. Due to its decentralized architecture, blockchain is suitable for providing accurate information [7]. Deploying efficient

authentication and authorization mechanisms ensures security and privacy while overcoming performance bottlenecks in query records. This makes it convenient for patients to query data, thereby improving the operational efficiency of medical institutions [8].

Based on the above research, a blockchain-based model for the secure storage and sharing of medical data is proposed in this paper, which uses Attribute-Based Encryption (ABE) and Attribute-Based Signature (ABS).

2. Related Knowledge

2.1 Attribute-based encryption

ABE originates from Fuzzy Identity Based Encryption. The idea of ABE is to associate ciphertext and keys with the set of attributes and access structure [9]. Only when the set of attributes satisfies the access structure can decryption be successful.

2.2 Searchable encryption

When data is stored on an untrusted server, in order for the server to not be able to understand the content of the data, it is necessary to encrypt the data before storing it. In order to achieve keyword retrieval on encrypted data, searchable encryption (SE) is proposed. SE is divided into symmetric searchable encryption (SSE) and asymmetric searchable encryption (ASE) [10]. The difference between the two is that SSE uses symmetric encryption algorithms, with the same encryption and decryption keys, while ASE uses asymmetric encryption algorithms.

2.3 Bilinear mapping

G and G_T are two multiplicative cyclic groups of order prime p, g∈G. Define a bilinear mapping e: $G \times G \to G_T$ that satisfies bilinear, computability, and nondegeneracy [11].

(1) Bilinear: for$\forall x, y \in G, \exists \alpha, \beta \in Zp$, such that equation $e(x^{\alpha}, y^{\beta}) = e(x, y)^{\alpha\beta}$ is established.

(2) Computability: for $\forall x, y \in G$,, there exists an effective algorithm to compute e(x, y).

(3) Non degeneracy: $\exists g \in G$, such that $e(g, g) \neq 1$.

3. Security Sharing Architecture

3.1 System model

The medical chain model simplifies existing systems and helps reduce the average communication time required for patients and hospitals to retrieve and access distributed medical information. The model deploys an authentication method based on the Burrows Abadi Needham (BAN) logic, maintaining third-party trust between data providers and users, and reducing the communication time cost of the system. The system architecture based on blockchain is shown in Figure 1, which includes the Certification Authority (CA), user layer, and processing layer. The hash value of each medical record in each hospital is stored in encrypted form on the blockchain network.

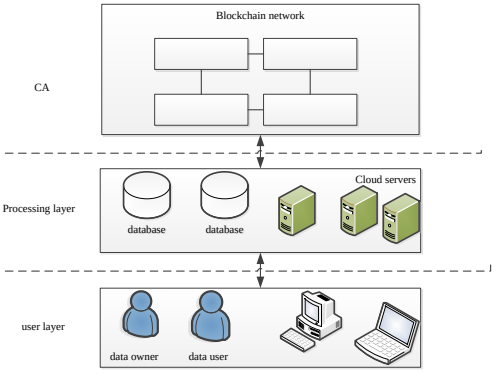

Figure 1. System Model of the Secure Storage.

(1) CA is responsible for creating and publishing digital certificates for entities connected to the blockchain

network. The public key used by the patient is generated by CA, with the aim of standardizing information sharing on decentralized networks and using the patient's private key to decrypt data when needed. CA is responsible for checking the operational status of the system. So, detecting and removing malicious nodes on the system is also the responsibility of the CA. CA is also an Attribute authorization (AA). AA is responsible for managing user attributes and generating user attribute keys.

(2) The processing layer includes hospital servers and databases. These databases store patient-related data such as past medical records, examination reports, and prescriptions, as well as hospital data such as treatment provided by doctors, treatment time, accounts, etc. The corresponding hash values of these data are stored in encrypted form on the blockchain network. The alliance chain network is a chain structure formed by these records, where each record represents the medical data of a specific hospital.

(3) The user layer includes all patients, doctors, devices, and other users. Patients (data owners, DO) are medical data owners who use symmetric encryption algorithms to encrypt medical data and store it on the blockchain. Simultaneously set access control policies for symmetric encryption keys and search keywords, and upload them to the blockchain. Data users (DU) are medical staff or researchers, users generate keyword search trapdoors, and blockchain nodes perform search matching. When the keyword matches and the data user's attributes meet the access control policies set by the patient, the data user can obtain the key used to decrypt the medical data ciphertext, thereby decrypting the medical data ciphertext.

3.2 Medical data upload process

Due to memory limitations in blockchain storage, all hospitals will store medical record data in the main node of the consortium chain in the form of ciphertext, medical record hash values, digital summaries, and their cloud storage locations. M is the hash value of each hospital, used to encrypt medical record summaries; L represents the cloud storage location of medical records. L should always encrypt and send to the blockchain network using the hospital's public key. The following are the steps for this algorithm:

Input: Medical records for each hospital

Output: Transaction results of medical data

Step 1: Generate the corresponding Epubkey {Mac||H(M)||L};

Step 2: Save the corresponding information generated in Step 1 to the medical alliance chain;

Step 3: Process all transactions and broadcast them to the blockchain network;

Step 4: Update records and output records that reflect medical data.

3.3 Security authentication mechanism

Table 1. Symbol Description

Symbol	Description
H1	hospital 1
H2	hospital 2
G1	P-order additive group
G2	P-order multiplicative group
e	bilinear pairing
q	Large prime numbers
P	G1 generator
H	The secure hash function of G1
h	The secure hash function of G2
E(.)	encryption algorithm
tc	Current timestamp
H(M)	H2 Medical Database Hash Value
Mac	Medical Data Summary
L	Position index of H2

The mechanism for sharing medical records on the medical chain requires storing medical record information on the blockchain network. When hospital H1 needs medical record information from hospital H2, H1 sends a request to the blockchain network using H1's data and private key, and the medical records update the data to the main node MN of the consortium chain network. The super node SN on the network is responsible for key management and attribute generation. The security authentication of the medical chain is divided into three stages: initialization, registration, and authentication. Table 1 shows the symbol explanations used by the security authentication mechanism.

(1) Initialization stage

The medical chain super node SN generates a key pair and provides system parameters for further processing. The system parameters are represented as (L, A1, A2, q, P, e, H, h). Then, use the consensus mechanism of the medical chain to generate public-private key pairs.

(2) Registration stage

Hospital H1 creates a unique identification ID and a random number R on the network, creates the required hospital data request record R1, forms a parameter Parameter=(ID, R, R1), and sends this parameter to the super node on the medical chain network. After receiving the parameters, the super nodes on the medical chain calculate the QID and SID and send the parameters to H2 through a secure channel, represented as formula (1):

$$\mathrm{QID} = \mathrm{H}(\mathrm{ID} \oplus \mathrm{R} \oplus \mathrm{R1}), \mathrm{SID} = \mathrm{QID} * \mathrm{SSN}, \mathrm{Parameter} = (\mathrm{SID}, \mathrm{QID}) \quad (1)$$

After receiving the parameters, H2 securely stores them for future use.

(3) Certification stage

After selecting a random number in H1, calculate X, X ', QID, r, s, U, and W as shown as formula (2). Then, H1 sends timestamp parameters to the master node on the blockchain network.

$$\begin{gathered} \mathrm{X} = \mathrm{x} * \mathrm{P}, \\ \mathrm{X}' = \mathrm{x} * \mathrm{QMN}, \\ \mathrm{QID} = \mathrm{H}(\mathrm{ID} \oplus \mathrm{R} \oplus \mathrm{R1}), \\ \mathrm{r} = \mathrm{H}\big(\mathrm{ID}\big|\big|\mathrm{R}\big|\big|\mathrm{QID}\big|\big|\mathrm{QSN}\big|\big|\mathrm{X}\big|\big|\mathrm{X}'\big|\big|\mathrm{tc}\big), \\ \mathrm{s} = \mathrm{h}(\mathrm{X}||\mathrm{X}'||\mathrm{tc}||\mathrm{R1}), \\ \mathrm{U} = \mathrm{SID} + \mathrm{x} * \mathrm{r} * \mathrm{QID} = \mathrm{W} = \mathrm{ESID}(\mathrm{ID}, \mathrm{R}, \mathrm{U}) \end{gathered} \quad (2)$$

The main node starts validation after receiving the timestamp. If it is found to be invalid, reject it. Otherwise, the master node starts calculating a secure hash and decrypts it using the hospital H1 public key to obtain the ID, R, and U, and then creates validation parameters. If the conditions are not met, the master node selects a random number. In addition, the master node will also calculate the session key and verification key, and send the parameters to hospital H1. The calculation formula is as formula (3):

$$\begin{gathered} \mathrm{y} \in \mathrm{Z} * \mathrm{q}, \mathrm{X}' = \mathrm{SMN} * \mathrm{X}, \mathrm{s} = \mathrm{h}(\mathrm{X}||\mathrm{X}'||\mathrm{tc}||\mathrm{R1}), \mathrm{e}(\mathrm{U}, \mathrm{P}) = \ (\mathrm{QID}, \mathrm{QSN} \ + \mathrm{r} * \mathrm{xP}) \ , \mathrm{T} = \mathrm{y} * \mathrm{P}, \mathrm{V} = \mathrm{y} * \mathrm{X} = \mathrm{x} * \mathrm{y} * \\ \mathrm{P}, \mathrm{M} = \mathrm{EQID}(\mathrm{R}||\mathrm{L}||\mathrm{|}(\mathrm{M})||\mathrm{Mac}), \mathrm{SK} = \mathrm{h}(\mathrm{X}, \mathrm{X}, \mathrm{T}, \mathrm{V}), \mathrm{AK} = (\mathrm{W}, \mathrm{Tc}, \mathrm{X}, \mathrm{X}, \mathrm{T}, \mathrm{V}), \mathrm{Parameter} = (\mathrm{T}, \mathrm{AK}, \mathrm{M}) \end{gathered} \quad (3)$$

After receiving the timestamp parameter, H1 immediately calculates V and verifies whether it is true: V=x. T and h (X, X, T, V). Reject the request if it does not pass validation. Otherwise, decrypt M using H1's private key to obtain R, L, M, and Mac. At this point, H1 and the master node have obtained all information related to medical records, hospital H2 location index, and patients through verification.

3.4 Data security sharing process

This scheme adopts attribute-based searchable encryption technology for the secure sharing of medical data. The process of sharing medical data is as follows:

(1) System initialization stage

Enter a security parameter k and generate the system's public parameter pp. The public key APK and private key ASK of the attribute authorization center AA is also obtained.

(2) Key generation stage

Enter the public parameter PP, private key ASK of attribute authorization center AA, and user attribute set ξ, Thus outputting the user's private key SKu.

(3) Data encryption stage

Encrypt the original medical data using a symmetric encryption algorithm, upload the ciphertext to IPFS (Distributed File Storage System) for storage, IPFS returns its storage address u, and then use CP-ABE to encrypt the symmetric encryption key. Meanwhile, encrypt the keyword kw. Finally, store the summary of the data ciphertext, IPFS storage address u, symmetric encryption key encryption result, and keyword ciphertext on the blockchain.

(4) Data search stage

Enter the public parameter PP, user's key SKu, and keyword w to obtain trapdoor Tw. Upload it to a blockchain node, and if the keyword uploaded by the user matches successfully, return the encrypted medical data key ciphertext CT and the storage address u of the medical data in IPFS.

(5) Data user decryption stage

Firstly, the data user obtains the key ciphertext CT from the blockchain. If the data user's attributes meet the access control policy set by the data owner, the data user can decrypt the ciphertext and obtain the decryption keyσfor medical data ciphertext. Finally, the data user DU downloads the ciphertext Cw based on the download address u. After obtaining Cw, use the decrypted key σ to decrypt ciphertext Cw to obtain medical data plaintext M.

4. Model Analysis

4.1 Validity check of the authentication mechanism

This section uses BAN logic to verify and analyze the previous verification process. Figure 2 shows the working principle of using the BAN logic verification protocol.

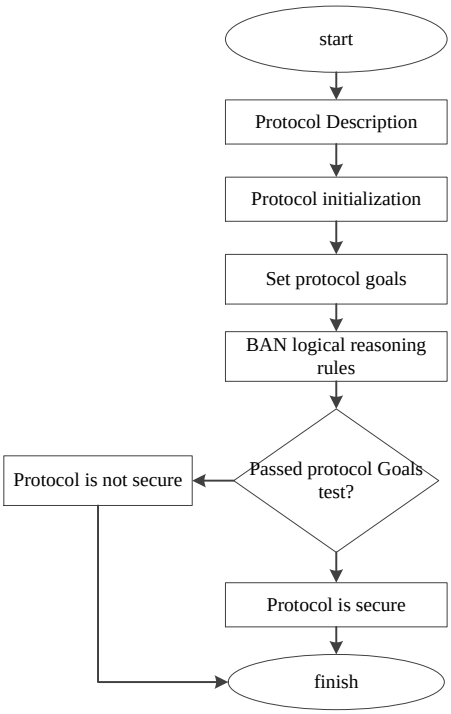

Figure 2. BAN logic verification flowchart.

When applying BAN logic to validate the proposed algorithm model, it can be found that the time required for identity authentication between hospital H1 and master node MN on the blockchain is of discrete logarithmic order. Therefore, the proposed protocol achieves high efficiency while also establishing secure session keys for storing and sharing data on the medical chain.

By analyzing storage capacity and key storage requirements, storage overhead can be calculated. In this article, the length of the qth order additive group is 1024, the length of the qth order multiplicative group is 512, the length of G1 is 512, the length of large prime numbers is 160, and the timestamp is 34. The requirement for calculating H1 storage key {SID+R+R1}=1024+64+42=1130. The private key of the master node requires 155 bits of storage space

on the blockchain.

4.2 Analysis of the correctness of the model

Next, the correctness of the model will be analyzed using deductive methods. After receiving the parameters (W, X, R1, tc) sent by H1, medical nodes on the blockchain need to perform authorization confirmation and accuracy calculation. Assuming QID is l, QSN is m, SID is n, and SSN is o, then there are:

$$E(U,P)=e(l,m+r*x*P)=e(n+x*r*l,P)=e(l*o+x*r*l,P)=e(l*o,P)*e(x*r*l,P)=e(l,P*o+x*r*P)=e(l,m+r*x*P)$$

The above derivation demonstrates the correctness of the model.

4.3 Analysis of the performance of the model

The performance of this model will be analyzed from the perspectives of storage overhead and computational cost.

By analyzing storage capacity and key storage requirements, storage overhead can be calculated. In this article, the length of the q-order additive group is 1024bit, the length of the q-order multiplicative group is 512bit, the length of G1 is 512bit, the length of large prime numbers is 160bit, and the timestamp is 34bit. So the requirement for the H1 storage key is {SID+R+R1}=1024+64+42=1130b. The private key of the master node requires 155 bits of storage space on the blockchain. On cloud storage with huge storage resources, the storage space used in this model is not large, so it can be said that the cost is relatively low.

The computational cost of the model was evaluated by using a platform configured with 8KB RAM, 128KB ROM, and 7.38 MHz Atmega 128 L microcontrollers. In terms of time, bilinear pairing is used, and the TinyOS library is used for RAM and ROM. The computational time cost is TG (mul)+1TG (add)+1TG (exp)+2Th, resulting in approximately 10.53 seconds.

5. Conclusions

In order to solve the problem of difficulty in sharing medical data among medical institutions and address the issue that existing blockchain-based architectures cannot be directly applied to the medical field, this article integrates blockchain and cloud storage technologies to provide a model for secure storage and sharing of medical data. Based on the decentralization and secure transmission characteristics of blockchain and network models, a medical chain architecture for medical data sharing was designed using bilinear mapping, ABS, and ABE. This architecture ensures the security of data storage and sharing, while also exhibiting good performance in terms of cost and computation time.

Funding

This work was supported by the Yunlin Municipal Science and Technology Bureau of research projects (CXY-2021-94-03 and CXY-2021-94-02).

References

[1] Xue T F, FU Q C, Wang Z. Research on medical data sharing model based on blockchain [J]. Acta Automatica Sinica, 2017, 43(9):1555-1562.

[2] Zhang J, Xue N, Huang X. A secure system for pervasive social network-based healthcare [J]. IEEE Access, 2016, 12:9239-9250.

[3] Saini A, Zhu Q Y, Singh N, et al. A smart-contract-based access control framework for cloud smart healthcare system. IEEE Internet of Things Journal, 2021, 8(7): 5914-5925. DOI: 10.1109/JIOT.2020.3032997.

[4] Sun J, Yao X M, Wang S P, et al. Block chain-based secure storage and access scheme for electronic medical records in IPFS. IEEE Access, 2020, 8: 59389-59401. DOI: 10.1109/ACCESS.2020.2982964.

[5] Wang H, Zhou M M, Li X. Security storage model of medical information based on blockchain [J]. Computer Science, 2019, 46(12):174-179.

[6] Lee J S, Chew C J, Liu J Y, et al. Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract. Journal of Information Security and Applications, 2022, 65: 103117. DOI: 10.1016/j.jisa.2022.103117.

[7] Yuan F, Wang Y. Blockchain: The state of the art and future trends [J]. Acta Automatica Sinica, 2016, 26:481-494.

[8] Li L, Wu Y, Yang Z K. Medical electronic medical record sharing scheme based on partition block chain [J]. Computer Application, 2022, 42(1):183-190.

[9] Luo W J, Wen S L, Cheng Y. Blockchain-based electronic health record sharing scheme [J]. Journal of Computer Applications 2020, 40(1):157-1615.

[10] Ahmed F, Hussein N, Gustavo R. A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform [J]. Cognitive Systems Research, 2018, 52:1-11.

[11] Castro M, Liskov B. Practical byzantine fault tolerance [J]. Symposium on Operating Systems Design & Implement, 1999, 47:173-186.