J Med Syst (2018) 42: 152
https://doi.org/10.1007/s10916-018-0994-6

SYSTEMS-LEVEL QUALITY IMPROVEMENT

Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain

Hao Wang[1] · Yujiao Song[1]

Received: 3 March 2018 / Accepted: 12 June 2018 / Published online: 5 July 2018

Abstract
To achieve confidentiality, authentication, integrity of medical data, and support fine-grained access control, we propose a secure electronic health record (EHR) system based on attribute-based cryptosystem and blockchain technology. In our system, we use attribute-based encryption (ABE) and identity-based encryption (IBE) to encrypt medical data, and use identity-based signature (IBS) to implement digital signatures. To achieve different functions of ABE, IBE and IBS in one cryptosystem, we introduce a new cryptographic primitive, called combined attribute-based/identity-based encryption and signature (C-AB/IB-ES). This greatly facilitates the management of the system, and does not need to introduce different cryptographic systems for different security requirements. In addition, we use blockchain techniques to ensure the integrity and traceability of medical data. Finally, we give a demonstrating application for medical insurance scene.

Keywords EHR · Attribute-based cryptosystem · Blockchain · Cloud storage

Introduction

With the rapid development of information technology, more and more medical institutions use electronic information systems, which produce massive medical information data every day. To improve the quality of hospital services and decrease patients' cost, making better use of medical information data has gradually become a hot research topic. The management of medical information data has brought new challenges to the medical institutions.

As a patient, the personal electronic health record (EHR) [13] is an electronic, personal medical health record that contains all personal health related information such as personal medical records, medical images, medical treatment, medications, experience reports, family history of genetic disease, etc. The use of EHR can help people to prevent diseases and improve the cure rate.

In the early days, EHR data was only mastered by various medical institutions, it is not conducive to data sharing. To make better use of EHR data and achieve better data sharing, some centralized data centers were set up. This provides great convenience for patients and medical institutions. For example, a patient may refer other doctors at the time of transfer and patients' medical records may also provide important support for research conducted by medical institutions, pharmaceutical companies and the like. In particularly, the use of big data technology makes the medical personalization service more realistic.

However, the establishment of medical data center requires high construction costs and professional technical support. Fortunately, cloud storage technology can provide a good solution. Cloud storage is essentially a cloud computing system with a large storage capacity. It extends from cloud computing and evolves. Cloud storage technology has its advantages of fast transmission, good sharing, storage capacity, low cost, easy access, dynamic association. As an important technology to support the development of smart medical services, cloud storage can serve as a platform for information sharing between remote hospitals and solve the problem of remote collaborative diagnosis [19].

This article is part of the Topical Collection on *Blockchain-based Medical Data Management System: Security and Privacy Challenges and Opportunities*

✉ Hao Wang
wanghao@sdnu.edu.cn

Yujiao Song
songyujiaosdnu@163.com

[1] School of Information Science and Engineering, Shandong Normal University, Jinan, China

Currently, cloud storage plays a crucial role in the medical information system. By storing EHR data on a cloud server, EHR data can be efficiently and conveniently shared among different medical institutions. Medical cloud system not only provides great convenience for doctors and patients, but also helps patients to better control their own condition. However, when users store EHR data on the cloud server, the data will suffer a variety of security threats [2], involving the privacy of the data, the integrity of the data, and the authentication of the data.

Our contribution

To solve these security problem, achieving confidentiality, authentication, integrity of medical data, and supporting the sharing of confidential data, we propose a cloud-based EHR system uses attribute-based cryptosystem and blockchain technology. In this system, we use ABE and IBE to encrypt data, ensuring fine-grained access control for encrypted data, and use IBS to implement digital signatures. To achieve different functions of attribute-based encryption (ABE), identity-based encryption (IBE) and identity-based signature (IBS) in one cryptosystem, we introduce a new cryptographic primitive, called combined attribute-based/identity-based encryption and signature (C-AB/IB-ES). This greatly facilitates the management of the system, and does not need to introduce different cryptographic systems for different security requirements. In addition, we use blockchain technology to ensure that the medical data cannot be tampered with, and the data sources can be traced. Finally, we give a demonstrating application for medical insurance scene.

Related work

EHR system

In order to improve medical service, increase the cure rate, reduce the cost, the modern health record systems have been widely used [11, 16]. EHR system can bring a lot of advantages, including precise recording, tracking disease, information sharing, data analysis, and so on. However, the security and privacy issues hindered the promotion of EHR system to some extent. In recent years, more and more attention has been paid to the security and privacy issues of EHR systems [1, 3, 20–22, 27, 39].

Attribute-based cryptosystem

Attribute-based cryptosystem is a special class of public-key cryptosystem, in which the attribute of user can be used as its public key. Since the identity information can be regarded as a special attribute, the attribute-based cryptosystem contains identity-based cryptosystem impliedly.

The concept of identity-based cryptography was proposed by Shamir in 1984 [29]. Until several years later, Boneh and Franklin [5] introduced the first identity-based encryption (IBE) scheme using bilinear maps in 2001. After that, the researchers carried out a lot of research on identity-based encryption [4, 17, 36, 37], identity-based signature [26], identity-based signcryption [6, 7] and so on. In 2005, Sahai and Waters proposed the concept of fuzzy identity-based encryption [28], which can be regarded as the embryonic form of attribute-based encryption (ABE). Then, Goyal et al. [12] gave the formal definition of ABE. In the past decade, ABE has been fully studied [14, 18, 23, 31–34].

Blockchain

Blockchain technology originated in the groundbreaking essay “Bitcoin: A Peer-to-Peer E-Cash System”, which is published on a cryptographer mailing list by Satoshi nakamoto in 2008 [25]. The invention of blockchain makes bitcoin to be the first digital currency, which solves the double spending problem without the need of trusted authority or central server. Blockchain is a type of append-only distributed ledger that is maintained by a group of nodes through consensus protocols. The main purpose of the blockchain is to decentralize and prevent information tampering. At present, many researchers are trying to use blockchain in different fields, such as Internet of Things [15], healthcare [40], electronic voting [24, 35], cloud computing [9], and so on.

Organization

We introduce the blockchain technology as the fundamental tool in Section “Blockchain technology”, and describe the concept of combined attribute-based/identity-based encryption and signature in Section “Combined attribute-based/identity-based encryption and signature”. Then, we introduce the design of our secure cloud-based EHR system in Section “Secure cloud-based EHR system”. In Section “A specific C-AB/IB-ES scheme”, we propose a specific C-AB/IB-ES scheme, and analyze its security. In Section “Application in insurance claims”, we introduce how to use our secure cloud-based EHR system in insurance claims scene. Finally, we give the conclusion in Section “Conclusion”.

Blockchain technology

Blockchain is a kind of chained data structure which is composed of data blocks linked by cryptography

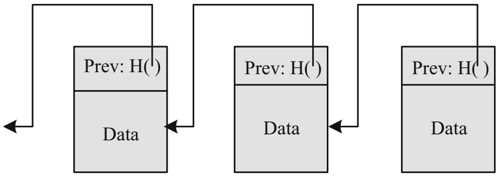

Fig. 1 Blockchain

hash function (e.g. SHA-256). Due to the security of cryptography hash function, this structure is hard to be tampered with. In general, a blockchain uses the chained data structure to store data, uses the consensus protocol between distributed nodes to generate and update data, uses the cryptography method to ensure the security, and uses automated scripting code to run intelligent contracts. With the increasing popularity of digital cryptocurrencies, blockchain has drawn great attention from government departments, financial institutions, technology companies and capital markets.

At present, the blockchains are usually divided into three categories, namely: public blockchains, coalition blockchains, and private blockchains. In a public blockchain system, anyone in the world can participate in the generation of blockchains, and can read the contents on the blockchain. The Bitcoin and the Ethereum are typical public blockchains. In a consortium blockchain system, consensus process is controlled by a set of pre-selected nodes, who make up a consortium for the common purpose. In a private blockchain, the write permissions are kept centralized to one organization, while the read permissions may be public or restricted to an arbitrary extent. The blockchain system used in this paper belongs to the consortium blockchain.

From the point of structure, blockchain is an ordered list of blocks, each block refers to a previous block, resulting in a blockchain. Once a block has been created and attached to the blockchain, the transactions in that block can not be changed or restored. The structure shown in Fig. 1:

The core of blockchain technology is the consensus mechanism, which ensures that all consensus nodes in the network agree upon a consistent global state of the blockchain. A blockchain network usually consists of data producers, consensus nodes, and data pool. When data producers want to write the data on blockchain, they first submit their data to the data pool. Then consensus nodes in the consensus network will capture the data from the data pool. After verifying the captured data, the consensus node runs the consensus protocol and selects the bookkeeping node. The bookkeeping node is responsible for writing data to the blockchain. The working process of the blockchain can be shown in Fig. 2.

Combined attribute-based/identity-based encryption and signature

Syntax

In order to achieve different functions of ABE, IBE and IBS in one cryptosystem, we introduce a primitive, called combined attribute-based/identity-based encryption and signature (C-AB/IB-ES), which is an extension of combined encryption and signature [8] in identity-based and attribute-based setting. A C-AB/IB-ES scheme shares setup and key generation algorithm in one system, and same public parameters and secret keys are used in three different functions of C-AB/IB-ES scheme. It comprises a tuple of algorithms (**Setup**, **KeyGen**, **Encrypt**, **Decrypt**, **Sign**, **Verify**), such that (**Setup**, **KeyGen**, **Encrypt**, **Decrypt**) forms ABE or IBE scheme and (**Setup**, **KeyGen**, **Sign**, **Verify**) forms IBS scheme. We describe these algorithms as follows:

Setup(λ)$\rightarrow$ PP, MSK: inputs security parameter λ, and outputs public parameters PP and master secret key MSK.

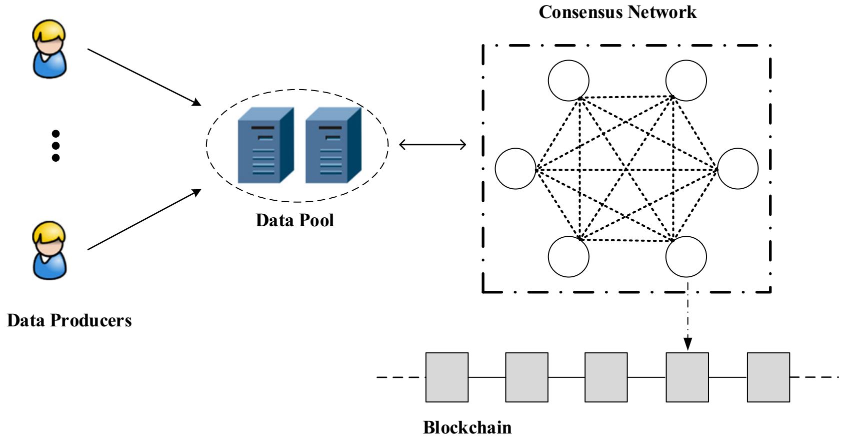

Fig. 2 Blockchain Network

KeyGen$(PP, MSK, I_{key}) \rightarrow SK_{I_{key}}$: inputs PP, MSK, key index I_{key}, and returns a private secret key $SK_{I_{key}}$ associated with I_{key}.

Encrypt$(PP, I_{enc}, m) \rightarrow CT_{I_{enc}}$: inputs PP, message m, encryption index I_{enc}, and returns a ciphertext $CT_{I_{enc}}$ associated with I_{enc}.

Decrypt$(PP, SK_{I_{key}}, CT_{I_{enc}}) \rightarrow m$: inputs PP, $CT_{I_{enc}}$, $SK_{I_{key}}$, and returns message m if $f(I_{key}, I_{enc}) = 1$, that is, I_{key} and I_{enc} satisfy the presupposition conditions f.

Sign$(PP, SK_{I_{key}}, m) \rightarrow \sigma$: inputs PP, $SK_{I_{key}}$, message m, and outputs a signature σ. Note, the signature σ usually contains the description of I_{key}.

Verify(PP, σ, m): inputs PP, σ, m, and outputs 1 if the signature is valid and 0 otherwise.

Note, when I_{key} represents an identity id, I_{enc} represents an identity id', the tuple (**Setup**, **KeyGen**, **Encrypt**, **Decrypt**) forms an IBE scheme, and $f(I_{key}, I_{enc}) = 1$ denotes $id = id'$. When I_{key} represents an attributes set S, I_{enc} represents an access structure $\mathbb{A}$, the tuple (**Setup**, **KeyGen**, **Encrypt**, **Decrypt**) forms a (ciphertext-policy) ABE scheme, and $f(I_{key}, I_{enc}) = 1$ denotes $S \in \mathbb{A}$. Furthermore, in the signing function, we set I_{key} represents an identity id, therefore the tuple (**Setup**, **KeyGen**, **Sign**, **Verify**) forms an IBS scheme.

Security model

We define the security in two aspects: confidentiality and unforgeability.

Confidentiality

The security game (IND-CPA for IBE/ABE) is defined as follows:

- *Setup*: The challenger $\mathcal{C}$ calls **Setup**$(1^\kappa) \rightarrow$ (PP, MSK), and gives PP to adversary $\mathcal{A}$.
- *Phase-1*: $\mathcal{A}$ queries a key index I_{key} to $\mathcal{C}$, and gets $SK_{I_{key}} \leftarrow$ **KeyGen**(PK, MSK, I_{key}) from $\mathcal{C}$.
- *Challenge*: $\mathcal{A}$ submits two messages m_0^*, m_1^* ($|m_0^*| = |m_1^*|$) and an encryption index I_{enc}^* to $\mathcal{C}$. Then, $\mathcal{C}$ selects $b \overset{R}{\leftarrow} \{0, 1\}$, runs $CT^* \leftarrow$ **Encrypt**(PP, I_{enc}^*, m_i^*) and forwards CT^* to $\mathcal{A}$. We restrict that all key indexes $I_{key,i}$ queried in Phase-1 satisfy $f(I_{key,i}, I_{enc}^*) \neq 1$.
- *Phase-2*: $\mathcal{A}$ queries the private key as in Phase 1. We also restrict that all key indexes $I_{key,j}$ queried in Phase-2 satisfy $f(I_{key,j}, I_{enc}^*) \neq 1$.
- *Guess*: $\mathcal{A}$ outputs a bit b'.

For the IBE/ABE component of the C-AB/IB-ES scheme, the advantage of $\mathcal{A}$ in breaking indistinguishable game under chosen-plaintext attacks (IND-CPA) is defined as

$$Adv_{\mathcal{A}}^{\text{IND-CPA}}(\kappa) := Pr[b' = b] - 1/2.$$

Definition 1 (IND-CPA Secure) A C-AB/IB-ES scheme is IND-CPA secure if $Adv_{\mathcal{A}}^{\text{IND-CPA}}(\kappa)$ is negligible for any PPT adversary.

Unforgeability

The security game (EUF-CMA for IBS) is defined as follows:

- *Setup*: The challenger $\mathcal{C}$ calls **Setup**$(1^\kappa) \rightarrow$ (PP, MSK), and forwards PP to adversary $\mathcal{A}$.
- *Queries*: $\mathcal{A}$ can query the oracles
  - $\mathcal{O}_{KeyGen}(id)$: $\mathcal{C}$ calls **KeyGen**$(PK, MSK, id) \rightarrow SK_{id}$, and forwards SK_{id} to $\mathcal{A}$.
  - $\mathcal{O}_{Sign}(id, m)$: $\mathcal{C}$ calls **Sign**$(PP, SK_{id}, m) \rightarrow$ σ, and forwards σ (contains id) to $\mathcal{A}$.
- *Forgery*: In the end, $\mathcal{A}$ outputs (m^*, σ^*), where σ^* contains id^*. $\mathcal{A}$ wins if:
  - $\mathcal{A}$ has not queried oracle $\mathcal{O}_{Sign}$ for (id^*, m^*).
  - $\mathcal{A}$ has not queried oracle $\mathcal{O}_{KeyGen}$ for id^*.
  - **Verify**$(PP, \sigma^*, m^*) = 1$

For the IBS component of a C-AB/IB-ES scheme, the advantage of $\mathcal{A}$ in breaking existential unforgeability game under chosen message attacks is defined as

$$Adv_{\mathcal{A}}^{\text{EUF-CMA}}(\kappa) := Pr[\mathcal{A} \text{ wins}].$$

Definition 2 (EUF-CMA Secure) A C-AB/IB-ES scheme is EUF-CMA secure if $Adv_{\mathcal{A}}^{\text{EUF-CMA}}(\kappa)$ is negligible for any PPT adversary.

Secure cloud-based EHR system

In order to achieve confidentiality, authentication, integrity of medical data, and support the sharing of confidential data, our cloud-based EHR system uses C-AB/IB-ES scheme and blockchain. There are five types of entities in our system: key generation center (KGC), hospitals, patients, medical clouds, data consumers (including medical research institute, insurance company, etc.).

In this system, patients authorize their data access policy (with their signature) to the hospital according to their actual need, and submit the signed authorization letters to the blockchain data pool to wait for the consensus nodes processing. The hospital will encrypt patients medical data under the specified access policy, and submit the encrypted data with hospitals signature to the data pool. The consensus nodes will keep monitoring the data pool, and capture the matched authorization letter (submitted by the patients) and encrypted data (submitted by the hospital). They will verify the corresponding signature to ensure that the data are complete and authorized by the patients. Then, the consensus nodes will perform a consensus protocol to select a bookkeeping node. The bookkeeping node will submit the encrypted data to the medical cloud and write the description of the data along with the address of the data in the cloud to the blockchain.

The specific operation of our scheme is as follows (as shown in the Fig. 3):

0. KGC runs the **KeyGen** algorithm to generate users private keys.

0-1: It generates identity keys for signing in IBS used by data producers (including hospitals, patients, etc.).

0-2: It generates attribute keys for decrypting in ABE used by data consumers (including medical research institute, insurance company, etc.).

1. The patients run **Sign** algorithm on authorization letter to state their data sharing policies (attached their signatures).

1-1: The patients send signed the authorization letter to the hospitals to authorize their data sharing policies.

1-2: In the meantime, they submitted the authorization letter to the data pool of the blockchain system, and waited for the consensus nodes to collect this authorization letter.

2. The hospital runs **Encrypt** algorithm to encrypt patients' data according to the data access policy authorized by patients, and runs **Sign** algorithm on this encrypted data to authenticate the authenticity of data, then it submits the encrypted data with related description and signature to the data pool of the blockchain.
3. The consensus nodes extract matched encrypted data and authorization letter from the data pool, and run **Verify** algorithm to verify the hospital's signature and patient's signature. Then, they perform a consensus protocol to select a bookkeeping node.
4. The bookkeeping node submits the encrypted data to the medical cloud and get the data access address form the cloud.
5. Then, the bookkeeping node write the description of the encrypted data along with the data address in the specified format to the blockchain.
6. The data consumers can browse the content of the blockchain and obtain the data address according to their requirements.
7. Then, the data consumers download the corresponding encrypted data and run the **Decrypt** algorithm to decrypt the encrypted data using their private keys.

A specific C-AB/IB-ES scheme

Construction

Our scheme is constructed on the basis of the Waters' CP-ABE [38].

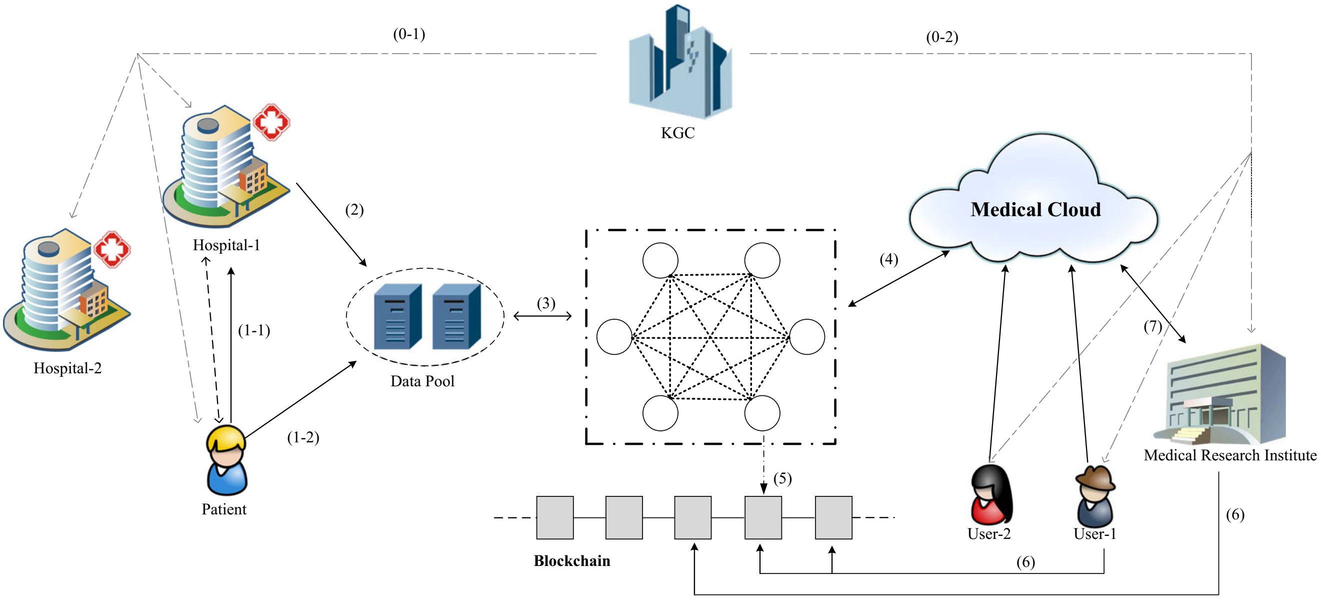

Fig. 3 Secure Cloud-Based EHR System

Setup(1^λ): It first selects a bilinear group G of prime order p, a generator g of G and a cryptographic hash function $h(\cdot)$: $\{0,1\}^* \rightarrow G$, which maps arbitrary values uniformly to G. Then, it randomly chooses $\alpha, a \in Z_p$, and outputs the public parameters $PP = (g, e(g,g)^\alpha, g^a, h(\cdot))$, the master secret key $MSK = g^\alpha$.

KeyGen$_{ATT}(PP, MSK, S) \rightarrow SK_S$: The key generation algorithm for attributes chooses $t \in Z_p$ randomly, and computes the private secret key $SK_S = \{K_0, K_1, \{K_{S,x}\}_{x \in S}\}$, where

$$K_0 = g^\alpha g^{at}, K_1 = g^t, \forall x \in S \;\; K_{S,x} = h(x)^t.$$

KeyGen$_{ID}(PP, MSK, id) \rightarrow SK_{id}$: The key generation algorithm for identities chooses $t \in Z_p$ randomly, and computes the private secret key $SK_{id} = \{K_0, K_1, K_{id}\}$, where

$$K_0 = g^\alpha g^{at}, K_1 = g^t, K_{id} = h(id)^t.$$

Encrypt$_{ATT}(PK, (M, \rho), m) \rightarrow CT$: In the input of the encryption algorithm for ABE, the encryption index is represented by an LSSS access structure (M, ρ), where M is an $l \times n$ matrix, function ρ associates rows of M to attributes. It selects a vector $\vec{v} = (s, y_2, ..., y_n) \in Z_p^n$ randomly. For $i = 1$ to l, it calculates $\lambda_i = \vec{v} \cdot M_i$, where M_i is the vector corresponding to the ith row of M. In addition, it chooses $r_1, r_2, ..., r_l \in Z_p$ randomly.

The ciphertext $CT = \{(M, \rho), C_0, C_1, \{(C_{2,i}, C_{3,i})\}_{i \in [1,l]}\}$, where

$$\begin{aligned} &C_0 = m \cdot e(g,g)^{\alpha \cdot s}, C_1 = g^s, \\ &(C_{2,1} = g^{a\lambda_1} h(\rho(1))^{-r_1}, C_{3,1} = g^{r_1}), ..., \\ &(C_{2,l} = g^{a\lambda_l} h(\rho(l))^{-r_l}, C_{3,l} = g^{r_l}). \end{aligned}$$

Encrypt$_{ID}(PP, id, m) \rightarrow CT$: The encryption algorithm for IBE chooses $r \in Z_p$ randomly. The ciphertext

$$CT = \{C_0 = m \cdot e(g,g)^{\alpha \cdot s}, C_1 = g^s, C_2 = g^{as} h(id)^{-r}, C_3 = g^r\}.$$

Decrypt$_{ATT}(PP, SK_S, CT)$: Let $I \subset \{1, 2, ...l\}$ be $I = \{i : \rho(i) \in S\}$. If S satisfies the access structure, we can find a set of constants $\{\omega_i \in Z_p\}_{i \in I}$, such that $\sum_{i \in I} \omega_i \lambda_i = s$. The decryption algorithm for ABE computes

$$\begin{aligned} A &= e(K_0, C_1) = e(g^\alpha g^{at}, g^s) = e(g,g)^{\alpha s} \cdot e(g,g)^{ats}, \\ B &= \prod_{i \in I} (e(K_1, C_{2,i}) \cdot e(K_{S,\rho(i)}, C_{3,i}))^{\omega_i} \\ &= \prod_{i \in I} (e(g^t, g^{a\lambda_i} h(\rho(i))^{-r_i}) \cdot e(h(\rho(i))^t, g^{r_i}))^{\omega_i} \\ &= e(g,g)^{at \sum_{i \in I} \lambda_i \omega_i} \\ &= e(g,g)^{ats}, m = C_0 \cdot B/A. \end{aligned}$$

Decrypt$_{ID}(PP, SK_{id}, CT)$: The decryption algorithm for IBE computes

$$\begin{aligned} A &= e(K_0, C_1) = e(g^\alpha g^{at}, g^s) = e(g,g)^{\alpha s} \cdot e(g,g)^{ats}, \\ B &= e(K_1, C_2) \cdot e(K_{id}, C_3) \\ &= e(g^t, g^{as} h(id)^{-r}) \cdot e(h(id)^t, g^r) \\ &= e(g,g)^{ats}, m = C_0 \cdot B/A. \end{aligned}$$

Sign$(PP, SK_{id}, m) \rightarrow \sigma$: First, it chooses $t', \tau \in Z_p$ randomly, and re-randomize the secret key:

$$K_0 = g^\alpha g^{at'}, K_1 = g^{t'}, K_{id} = h(id)^{t'}.$$

Then, it computes:

$$\begin{aligned} &S_0 = K_0 \cdot g^{a\tau} = g^\alpha g^{a(t'+\tau)}, \\ &S_1 = K_1 = g^{t'}, \\ &S_2 = g^\tau, \\ &S_3 = K_{id} \cdot h(m)^\tau = h(id)^{t'} \cdot h(m)^\tau, \end{aligned}$$

The signature is:

$$\sigma = (id, S_0, S_1, S_2, S_3).$$

Verify(PP, σ, m): It first computes

$$\begin{aligned} e(S_0, g) &= e(g,g)^\alpha \cdot e(g,g)^{a(t'+\tau)}, \frac{e(S_1, g^a h(id)) e(S_2, g^a h(m))}{e(S_3, g)} \\ &= \frac{e(g,g)^{at'} e(g, h(id))^{t'} e(g,g)^{a\tau} e(g, h(m))^\tau}{e(g, h(id))^{t'} e(g, h(m))^\tau} \\ &= e(g,g)^{a(t'+\tau)}, \end{aligned}$$

then verifies

$$\frac{e(S_0, g) e(S_3, g)}{e(S_1, g^a h(id)) e(S_2, g^a h(m))} \overset{?}{=} e(g,g)^\alpha$$

If the equality holds, it outputs 1, otherwise it outputs 0.

Security analysis

Confidentiality

Theorem 1 *Our C-AB/IB-ES scheme is IND-CPA secure in the random oracle model.*

Our scheme uses the design framework of Waters' ABE. The only difference is that in our scheme, we use a hash function $h(\cdot)$ instead of the public parameter $h_1, ..., h_U$. This brings three advantages, short public parameters, large universe of attribute, easy to support IBE. In the random oracle model, we can preset the return value of the hash function $h(\cdot)$, therefore the security of our scheme can be reduced to the security of the Waters' scheme.

Unforgeability

Theorem 2 *Our C-AB/IB-ES scheme is EUF-CMA secure.*

The design of the IBS part of our C-AB/IB-ES scheme is based on the ideas of Gentry and Silverberg [10], that is, any two layer HIBE scheme can be transformed into an IBS scheme. Our IBE scheme can be easily extended to a HIBE scheme, the key delegation algorithm can be constructed as follows: (For simplicity, we give an example of two-layer HIBE.)

Delegate$(PK, SK_{id_1}, id_2) \rightarrow SK_{id_1:id_2}$: For $SK_{id_1} = \{K_0, K_1, K_{id_1}\}$, where $K_0 = g^{\alpha} g^{at}$, $K_1 = g^{t}$, $K_{id_1} = h(id_1)^{t}$. It first chooses $t', \tau \in Z_p$ randomly, and re-randomize the secret key:

$$K_0 = g^{\alpha} g^{at'}, K_1 = g^{t'}, K_{id} = h(id_1)^{t'}.$$

Then, it computes:

$$K_0' = K_0 \cdot g^{a\tau} = g^{\alpha} g^{a(t'+\tau)},$$

$$K_1' = K_1 = g^{t'}, K_2' = g^{\tau},$$

$$K_{id}' = K_{id} \cdot h(id_2)^{\tau} = h(id_1)^{t'} \cdot h(id_2)^{\tau}.$$

The new key is:

$$SK_{id_1:id_2} = (K_0', K_1', K_2', K_{id}').$$

Therefore, the security of our scheme can be reduced to the security of HIBE, which has been proved to be secure in Theorem 1. The IBS part of our C-AB/IB-ES scheme is EUF-CMA secure.

Application in insurance claims

With the rapid development of medical insurance business, the number of insured persons has risen straightly, and insurance claim events have also increased. But at the same time, we can easily find out that during the actual insurance claims, there are many cases of medical insurance fraud through tamper with the medical records, there are also many cases of refusing claims because the medical records are incomplete.

Medical record is the real record of the patient's health information on the file, including the patient's condition and treatment process. It can be said that the medical record is an important basis for the insurance company to pay for the medical expenses when auditing the claims. However, the traditional case management system has some problems, and the authenticity of the case is threatened. For example, after an agreement has been reached between a patient and some member of the hospital, they forges the patient's medical record and then illegally receives a claim. Due to the above problems, we must ensure the timeliness, completeness and especially authenticity of medical records.

Our secure EHR system can provide a good solution. Only the actual medical records can guarantee the transparency of the insurance claims process and provide better service for insurance claims. In this system, as the medical record data is generated, the blockchain records the medical record information at any time, and the medical record information on the blockchain cannot be modified afterwards. The consensus node controlled by the insurance company in the consensus network gets data in real time. Therefore, this also ensures the integrity and authenticity of medical records. At the time of the claim, the insurance company can gain access to the encrypted medical record data to complete the claim.

We give an example for medical insurance scene. There are three types of entities in this process that are patients, hospitals and insurance companies. The work flow of this system is as follows (as shown in the Fig. 4):

0. All participants register private keys from the KGC, where the patients and the hospitals obtain identity keys for signing using IBS, and the insurance companies obtains attribute keys for decrypting using ABE;
1. The patient authorizes the data access policy to the hospital, including the policy that allows the insurance company to access data;
2. The hospital encrypts the medical record according to the data access policy and submits it to the blockchain data pool;
3. The blockchain consensus nodes verify the legitimacy of the source of the medical record data, on one hand the encrypted data are stored on the medical cloud and on the other hand the relevant descriptions of medical records are written on the blockchain;
4. The patient submits a claim to the insurance company. After the insurance company gets the application, it searches the blockchain for the existence of the medical record and obtains the address information of the medical record in the cloud storage. Because the insurance company's attributes comply with the patient's prescribed access policy, the corresponding encrypted file can be downloaded and decrypted using its private key. Based on the medical record information to be reviewed, the insurance companies complete the claims.

In this system, the decentralization of the blockchain ensures that medical records are completed by various medical institutions, thereby avoiding the possibility of a single institution being controlled or bribed to record the accounts. The data on the blockchain is also traceable. Because the data written to the blockchain is accompanied by a complete copy of the timestamp, the data on the blockchain can not be tampered with. The existence of the blockchain provides strong support for medical insurance claims.

Our system can also support smart contracts for automatic claims settlement [30]. It needs to run a

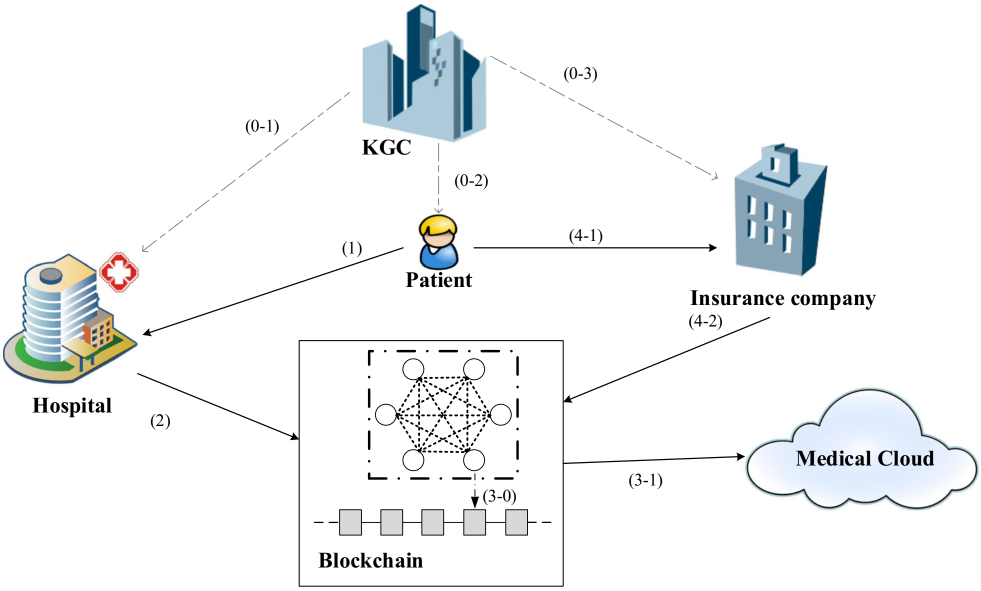

Fig. 4 Medical insurance scene

smart contract between the patients, the hospitals, and the insurance companies. When the patient reaches the claim conditions, the patient will automatically receive compensation from the fund pool. This process does not even require the existence of a traditional insurance company.

Conclusion

In this paper, we pay attention to the security of the EHR system, and propose a secure cloud-based EHR system. To achieve different functions of encryption and signature in one cryptosystem, we introduce the C-AB/IB-ES scheme. This greatly facilitates the management of the system, and does not need to introduce different cryptographic systems for different security requirements. To ensure the integrity and traceability of medical data, we use the blockchain techniques. In addition, we give a demonstrating application for medical insurance scene.

In the future, we will study the deployment of smart contracts on our system and build an automated insurance claim contract on Ethereum.

Funding This study was funded by the National Natural Science Foundation of China (No.61602287, No.61672330, No.61572294), and the Primary Research & Development Plan of Shandong Province (No. 2018GGX101037).

Compliance with Ethical Standards

Conflict of interests Authors declares that they have no conflict of interest.

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Akinyele, J. A., Pagano, M. W., Green, M. D., Lehmann, C. U., Peterson, Z. N. J., and Rubin, A. D., Securing electronic medical records using attribute-based encryption on mobile devices. In: SPSM'11, Proceedings of the 1st ACM Workshop Security and Privacy in Smartphones and Mobile Devices, Co-located with CCS 2011, October 17, 2011. Chicago, pp. 75–86, 2011.
2. Alemȧn, J. L. F., Seňor, I. C., Lozoya, P. O., and Toval, A., Security and privacy in electronic health records: A systematic literature review. *J. Biomed. Inform.* 46(3):541–562, 2013.
3. Alshehri, S., Radziszowski, S. P., and Raj, R. K., Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. In: Workshops Proceedings of the IEEE 28th International Conference on Data Engineering, ICDE 2012, Arlington, VA, USA, April 1-5, 2012, pp. 143–146, 2012.
4. Boneh, D., and Boyen, X., Efficient selective-id secure identity-based encryption without random oracles. In: Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings, pp. 223–238, 2004.
5. Boneh, D., and Franklin, M. K., Identity-based encryption from the weil pairing. In: Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings, pp. 213–229, 2001.
6. Boyen, X., Multipurpose identity-based signcryption (A swiss army knife for identity-based cryptography). In: Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings, pp. 383–399, 2003.
7. Boyen, X., Identity-based signcryption. In: Practical Signcryption, pp. 195–216, 2010.
8. Chen, C., Chen, J., Lim, H. W., Zhang, Z., and Feng, D., Combined public-key schemes: The case of ABE and ABS. In: Provable Security - 6th International Conference, ProvSec 2012, Chengdu, China, September 26-28, 2012. Proceedings, pp. 53–69, 2012.
9. Dong, C, Wang, Y., Aldweesh, A., McCorry, P., and van Moorsel, A., Betrayal, distrust, and rationality: Smart counter-collusion contracts for verifiable cloud computing. In: Proceedings of the

2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017, pp. 211–227, 2017.

10. Gentry, C., and Silverberg, A., Hierarchical id-based cryptography. In: Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings, pp. 548–566, 2002.
11. Goroll, A. H., Simon, S. R., Tripathi, M., Ascenzo, C., and Bates, D. W., Case report: Community-wide implementation of health information technology: The massachusetts ehealth collaborative experience. *JAMIA* 16(1):132–139, 2009.
12. Goyal, V., Pandey, O., Sahai, A., and Waters, B., Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006, pp. 89–98, 2006.
13. Hȧyrinen, K., Saranto, K., and Nykȧnen, P., Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *I. J. Med. Inf.* 77(5):291–304, 2008.
14. Hohenberger, S., and Waters, B., Online/offline attribute-based encryption. In: Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings, pp. 293–310, 2014.
15. Huang, H., Chen, X., Qianhong, W., Huang, X., and Shen, J., Bitcoin-based fair payments for outsourcing computations of fog devices. *Fut. Gen. Comp. Syst.* 78:850–858, 2018.
16. Krist, A. H., Peele, E., Woolf, S. H., Rothemich, S. F., Loomis, J. F., Longo, D. R., and Kuzel, A. J., Designing a patient-centered personal health record to promote preventive care. *BMC Med Inf. .Decis. Making* 11:73, 2011.
17. Lewko, A. B., and Waters, B., New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings, pp. 455–479, 2010.
18. Lewko, A. B., and Waters, B., New proof methods for attribute-based encryption Achieving full security through selective techniques. In: Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings, pp. 180–198, 2012.
19. Li, M., Yu, S., Ren, K., and Lou, W., Securing personal health records in cloud computing Patient-centric and fine-grained data access control in multi-owner settings. In: Security and Privacy in Communication Networks - 6th Iternational ICST Conference, SecureComm 2010, Singapore, September 7-9, 2010. Proceedings, pp. 89–106, 2010.
20. Li, M., Yu, S., Zheng, Y., Ren, K., and Lou, W., Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Trans. Parallel Distrib. Syst.* 24(1):131–143, 2013.
21. Li, X., Ibrahim, M. H., Kumari, S., Sangaiah, A. K., Gupta, V., and Choo, K.-K. R., Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. *Comput. Netw.* 129:429–443, 2017.
22. Li, X., Niu, J., Kumari, S., Wu, F., and Choo, K.-K. R., A robust biometrics based three-factor authentication scheme for global mobility networks in smart city. *Fut. Gen. Comp. Syst.* 83:607–618, 2018.
23. Li, X., Niu, J., Liao, J., and Liang, W., Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update. *Int. J. Commun. Syst.* 28(2):374–382, 2015.
24. McCorry, P., Shahandashti, S. F., and Hao, F., A smart contract for boardroom voting with maximum voter privacy. In: Financial Cryptography and Data Security - 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers, pp. 357–375, 2017.
25. Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system, 2008.
26. Paterson, K. G., and Schuldt, J. C. N., Efficient identity-based signatures secure in the standard model. In: Information Security and Privacy, 11th Australasian Conference, ACISP 2006, Melbourne, Australia, July 3-5, 2006, Proceedings, pp. 207–222, 2006.
27. Bo, Q., Deng, H., Wu, Q., Domingo-Ferrer, J., Naccache, D., and Zhou, Y., Flexible attribute-based encryption applicable to secure e-healthcare records. *Int. J. Inf. Sec.* 14(6):499–511, 2015.
28. Sahai, A., and Waters, B., Fuzzy identity-based encryption. In: Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, pp. 457–473, 2005.
29. Shamir, A., Identity-based cryptosystems and signature schemes. In: Advances in Cryptology, Proceedings of CRYPTO ’84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings, pp. 47–53, 1984.
30. Underwood, S., Blockchain beyond bitcoin. *Commun. ACM* 59(11):15–17, 2016.
31. Wang, H., He, D., Shen, J., Zheng, Z., Yang, X., and Au, M. H., Fuzzy matching and direct revocation: a new CP-ABE scheme from multilinear maps. *Soft Comput.* 22(7):2267–2274, 2018.
32. Wang, H., He, D., Shen, J., Zheng, Z., Zhao, C., and Zhao, M., Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing. *Soft Comput.* 21(24):7325–7335, 2017.
33. Wang, H., Zheng, Z., Wu, L., and He, D., New large-universe multi-authority ciphertext-policy ABE scheme and its application in cloud storage systems. *J. High Speed Netw.* 22(2):153–167, 2016.
34. Wang, H., Zheng, Z., Wu, L., and Li, P., New directly revocable attribute-based encryption scheme and its application in cloud storage environment. *Clust. Comput.* 20(3):2385–2392, 2017.
35. Wang, Z., Zhang, H., Song, X., and Zhang, H., Consensus problems for discrete-time agents with communication delay. *Int. J. Control Autom. Syst.* 15(4):1515–1523, 2017.
36. Waters, B., Efficient identity-based encryption without random oracles. In: Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, pp. 114–127, 2005.
37. Waters, B, Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings, pp. 619–636, 2009.
38. Waters, B., Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings, pp. 53–70, 2011.
39. Yan, H., Li, X., and Li, J., Secure personal health record system with attribute-based encryption in cloud computing. In: 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Guangdong, China, November 8-10, 2014, pp. 329–332, 2014.
40. Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W., Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* 40(10):218,1–218,8, 2016.