Fine-grained and Efficient Access Control in E-health Environment

Tiantian Miao[1], Jian Shen[1,2], Xin Jin[1], Jin-Feng Lai[3]

[1] School of Computer & Software, Nanjing University of Information Science & Technology, China
[2] Security Research Center, Peng Cheng Laboratory, China
[3] School of Information and Communication Engineering, University of Electronic Science and Technology of China, China
mtt_0106@126.com, s_shenjian@126.com, ndghtxx@163.com, lcf2018@uestc.edu.cn

Abstract

With the rapid development of cloud storage technology, more and more hospitals and research institutions would like to upload the patient's electronic medical record (EMR) to the cloud. However, the problems of privacy protection maybe occur if the patient's private data be obtained by a malicious user. To solve this problem, a fine-grained and efficient access control protocol in the e-health environment is proposed. For one thing, ciphertext-policy attribute-based encryption (CP-ABE) strategy are utilized to conduct fine-grained access control, which guarantees the private data only can be accessed by legal users. For another thing, an optimized access control structure is designed for the reduction of computing and communication overhead. Note that unlike traditional access control protocols. Moreover, counter and the decryption test are employed in this paper to limit the access times and help cloud justify whether the data requester has permission to decrypt the requested data, which contribute to resisting denial of service attacks (DoS). Analysis result demonstrates that the proposed protocol performs well in terms of security and efficiency.

Keywords: Access control, Privacy protection, CP-ABE, E-health environment

1 Introduction

In recent years, with the increasing improvement of living standards and quality, people's awareness of safety and health has been continuously enhanced. As a result, more and more medical data is introduced and traditional medical models have been unable to meet people's requirements, and then e-health has come into being [1]. In e-health environment, patient's medical data (such as EMR) is uploaded to the cloud, and users (such as doctors, research institutions as well as family members of patients) can access the patient's data for further treatment. However, there are not always legal users who want to access patients' private data. Malicious adversaries may also hope to gain other's private message actuated by ulterior motives, which brings bad influence on the data owners [2]. Therefore, a fine-grained access control protocol is necessary for avoiding user privacy being obtained by malicious attackers.

Attribute-based Encryption (ABE) technologies are the natural choice as the solution of the above problems, which executes the access policy defined on the attribute during the encryption process, and give the data consumer access right to the corresponding data according to the attributes of the recipient. In 2005, the concept of ABE [3] is first formally proposed by Sahai and Water based on the concept of Identity-based Encryption (IBE) [4]. However, the ABE proposed in [3] requires a fixed threshold and cannot accommodate complex access strategies. Later, ciphertext-policy attribute-based encryption (CP-ABE) and key-policy attribute-based encryption (KP-ABE) are proposed by Goyal et al. [5]. In the KP-ABE, the ciphertext is associated with the attribute, and the key is associated with the access policy [6-9]. In the CP-ABE, the ciphertext is associated with the cipher-defined access policy, and the key is associated with the attribute [10-13]. Since CP-ABE allow encryptors to freely choose the attribute set for a certain data, CP-ABE is more suitable than KP-ABE for scenarios with high access control requirements in the e-health environment.

However, current access control protocols [14-22] not always simultaneously meet the requirements of efficiency and security. On the one hand, the resources of users in e-health environment are limited, and the process of encryption and decryption may bring heavy burden to the data owner and the data consumer respectively. On the other hand, the malicious adversary may cheat the cloud to get patient's private data without the permission of the data owner, or even

*Corresponding Author: Jin-Feng Lai; E-mail: lcf2018@uestc.edu.cn

DOI: 10.3966/160792642019122007014

continuously sends duplicate request information to the cloud server, maliciously encroaching on the resources of the cloud server and interfering with the normal operations of legitimate users.

To solve the problems of the above problems, a fine-grained and efficient access control protocol in the e-health environment is proposed, and the main contributions of the proposed protocol are listed as follows:

(1) *An access* structure *with attribute ranking is proposed.* Note that the relationship between attribute and ciphertext is often not one-to-one. The overhead of computation and communication increases with the increasing of the complexity of the access structure. In this paper, a simplified access structure with attribute ranking is designed to simplify the access structure and further reduce user's overhead.

(2) *Decryption test is supported to authenticate the legitimacy of users.* Few of current access control protocols al-low the cloud to justify the validity of the data consumer, which increases the risk that user privacy message will be compromised. To avoid this problem, the decryption test is employed to prevent malicious users from accessing the medical data of the patient.

(3) *Denial of service attack resistance is supported.* In reality, a malicious user can send thousands of request message to launch denial of service attack, and further interfere with the normal behaviors of valid users. Therefore, the access times in this paper is limited to resist the DoS attacks.

The remainder of this paper is organized as follows: In Section 2, some preliminaries for this paper are briefly introduced. In Section 3, the system model and our scheme are defined. In Section 4, the optimized access control structure and our scheme are described in detail. In Section 5, the security and performance analyses are presented. Finally, the conclusion of this paper is covered in Section 6.

2 Preliminaries

To help readers have a better understanding of this paper, preliminary knowledge is introduced in this chapter, including bilinear pairing, access structure and linear secret sharing schemes.

2.1 Bilinear Pairing

Given two cyclic multiplicative groups $\mathbb{G}_1$ and $\mathbb{G}_T$ with large prime order q. Let $g \in \mathbb{G}_1$ be the generator of group . A weil pairing is a valid map $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow$ $\mathbb{G}_T$ if it satisfies the four properties as follows:

(1) Bilinearity: For any g and $h \in \mathbb{G}_1$, a and $b \in \mathbb{Z}_q^*$, $\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$ holds.

(2) Non-degeneracy: If g is a generator of group $\mathbb{G}_1$, $\hat{e}(g, g) \neq 1$ holds.

(3) Computability: For any g and $h \in \mathbb{G}_1$, there is always an efficient polynomial-time algorithm can compute $\hat{e}(g, h)$.

2.2 Access Structure [23]

Let $U = \{U_1, U_2, \ldots, U_n\}$ denote a set of parties. A collection $\mathbb{A} \in 2^U$ is monotone if for any $B \in \mathbb{A}$ and $C \in 2^U$: if $B \in C$ then $C \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection $\mathbb{A}$ of nonempty subsets of U, ie. $\mathbb{A}\, 2^u \setminus \{0\}$. Then, the sets in $\mathbb{A}$ are called authorized sets; Otherwise, called unauthorized sets.

2.3 Linear Secret Sharing Schemes (LSSS) [24]

Let U denote the attribute universe. An LSSS includes ($\mathbb{M}$, ρ), where $\mathbb{M}$ is a $l \times n$ matrix over $\mathbb{Z}_q^*$, and ρ maps a row of $\mathbb{M}$ to an attribute in U. An LSSS is composed of two steps as follows:

(1) *Share*($\mathbb{M}$, ρ) is used to share the secret value s. Given a random vector $v = \{s, y_2, y_3, \ldots, y_n\}$, where $y_2, y_3, \ldots, y_n \in \mathbb{Z}_q^*$, compute $\lambda_x = \mathbb{M}_x \cdot v$ as a share of the secret s.

(2) *Reconstruction* ($\lambda_1, \lambda_2, \ldots, y_l$, ($\mathbb{M}$, ρ)) is used to recover the secret value s Let S be the authorized set, then there are constants $\{w_i\}_{i \in S}$ such that $\sum_{i \in S} \omega_i\, \mathbb{M}_i$ (1, 0, …, 0), then we have $\sum_{i \in S} \omega_i \lambda_i = s$.

We say that $S \in \{1, 2, \ldots, l\}$ satisfies the access structure ($\mathbb{M}$, ρ) if there exits $\{w_i\}_{i \in S}$ such that $\sum_{i \in S} \omega_i$ $\mathbb{M}_i$ = (1, 0, …, 0); Otherwise, $S \in \{1, 2, \ldots, l\}$ is an unauthorized set.

3 Definitions

In this section, definitions of the system model and our schemes are given as follows:

3.1 Definition of System Model

The system model of our access control scheme is given as in Figure 1. The system is comprised of four entities: the attribute authority, the cloud, the data owners (DO) and the user.

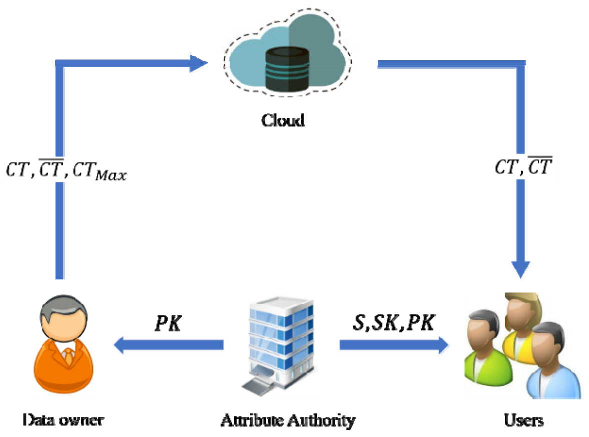


Figure 1. The system model

The attribute authority is a fully trust party, which is employed for managing all attributes and generating the public key and the secret key for each user.

The cloud is honest but curious, which is employed for storing data owner's data.

The data owner defines the access policies and outsource data in ciphertext format to the cloud.

The users request the data from the cloud, and they can decrypt the data if and only if their attribute set satisfies the access policy.

3.2 Definition of Our Scheme

The proposed scheme is composed of the following four algorithms:

(1) $SetUp(1^{\lambda}) \rightarrow (PK, MSK)$: Given a security parameter λ as input, output the public key *PK* and the master secret key *MSK*.

(2) $KeyGen(PK, MSK, S) \rightarrow (PU_C, PR_C, SK)$ can be further divided into two steps:

(a) $KeyGen() \rightarrow (PU_C, PR_C)$: Given some random elements as input, output the key pair $\{PU_C, PR_C\}$.

(b) $KeyGen(PK, MSK, S) \rightarrow (SK)$: Given the PK, the *MSK* and a set of attribute *S* as input, output the corresponding secret key *SK*.

(3) $Enc(PK,\ (\mathbb{M},\ \rho),\ max,\ m,\ r) \rightarrow (CT, \overline{CT}, CT_{Max})$: Given the *PK*, the access policy $(\mathbb{M}, \rho)$, the maximum access times *max*, the data *m* and a random element *r* as input, output the corresponding ciphertext $(CT, \overline{CT}, CT_{Max})$.

(4) $Dec(CT, \overline{CT}, CT_{Max},\ \mathbb{M},\ PK, SK) \rightarrow (m)$: can be further divided into two steps:

(a) $DecTest(\overline{CT},\ \mathbb{M}, PK, SK) \rightarrow (r^*)$: Given the $\overline{CT}$, $\mathbb{M}$, *PK* and *SK* as input, output the value r^*.

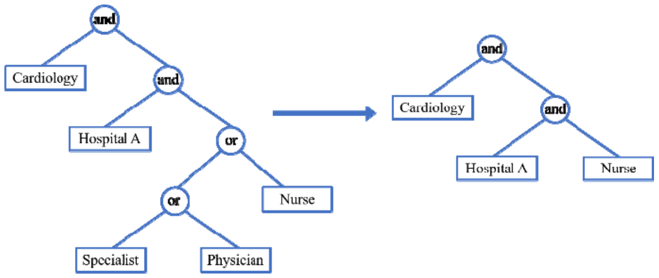
(b) $DecData(CT,\ \mathbb{M}, PK, SK) \rightarrow (m)$: Given the *CT*, $\mathbb{M}$, *PK* and *SK* as input, output the data *m*.

4 The Proposed Scheme

In this section, the access structure with attribute ranking employed is first introduced, and then the design details of the proposed scheme are given.

4.1 The Access Structure with Attribute Ranking

Here, the access structure with attribute ranking is described in detail, which simplifies the conditional access structure. To understand this section well, an example of the access structure with attribute ranking is given as Figure 2.



(a) The traditional access structure (left)

(b) The access structure with attribute ranking (right)

Figure 2. The access structure

Note that the left figure of Figure 2 can be seen as a traditional access structure, while the right figure of Figure 2 can be seen as the access structure with attribute ranking. And the access policy of Figure 2(a) is {*Cardiology*} and {*HospitalA*} and {{*Specialist*} or {*Physician*} or {*Nurse*}} which is very complex. To simplify the access policy, we set the relationship of *Specialist*, *Physician*, *Nurse* as *Specialist* > *Physician* > *Nurse*. In this case, *Specialist* attribute includes all privileges of *Physician* attribute and *Nurse* attribute, *Physician* attribute includes all privileges of *Nurse* attribute. Hence, the access structure can be reduced as {*Cardiology*} and {{*HospitalA*} and {*Nurse*}}, which is much easier to manage than the access policy of the traditional structure. Note that we assume that the result of attribute ranking is known by all participants in this system.

4.2 Design Details of Our Scheme

Let $U = |U| \in \mathbb{Z}_q^*$ be the size of attribute universe, $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$ be a bilinear map, and *g* be a generator of $\mathbb{G}_1$, where $\mathbb{G}_1$ and $\mathbb{G}_T$ are two cyclic multiplicative groups of prime order *q*. Then, based on the description of definition in Section 3.2, the design details of our scheme are given as follows:

(1) $SetUp(1^{\lambda}) \rightarrow (PK, MSK)$: This algorithm is executed by the attribute authority to generate the public key *PK* and the master secret key *MSK*. In this algorithm, the attribute authority takes the security

parameter λas input, selects random elements $a, a, x_0 \in \mathbb{Z}_q^*, u, h_1, ..., h_U \in \mathbb{G}_1$, and outputs the *PK* as Eq. (1) as well as the *MSK* as Eq. (2).

$$PK = \{U, g, g^a, \hat{e}(g, g)^a, h_1, ..., h_U, S_0\} \quad \textbf{(1)}$$

$$MSK = g^a \quad \textbf{(2)}$$

Note that in Eq. (1), we compute S_0 as $S_0 = g^{-u^{x_0}}$.

(2) $KeyGen\,(PK, MSK, S) \rightarrow (PU_c, PR_c, SK)$: This algorithm is executed by the cloud to generate its key pair (PU_c, PR_c), and the attribute authority to generate users' secret key *SK*. It includes the following two steps:

(a) $KeyGenC \rightarrow (PU_c, PR_c)$: The cloud randomly selects two primes $c, f \in \mathbb{Z}_q^*$, and calculates $\eta = c \times f$, $\phi(\eta) = (c-1)(f-1)$. Then, a large integer *e* is selected and *d* is calculated. Note that $\gcd(\phi(\eta), e) = 1$, $1 < e < \phi(\eta)$ and $d \equiv e^{-1} \bmod \phi(\eta)$. Finally, the cloud publics $PU_c = \{e, \eta\}$ and keeps $PRC_c = \{d, \eta\}$ secret.

(b) $KeyGen\,(PK, MSK, S) \rightarrow (SK)$: The attribute authority takes the public key *PK*, the master key *MSK* and users attribute set $S \subseteq 2^U$ as input, and computes

$$K = g^{\alpha} g^{at}, K' = g^t, K_i = S_i^{u^{x0} - u^{x_i}} h_x^t \quad \textbf{(3)}$$

where $t, \{x_i\}_{i \in s} \in \mathbb{Z}_q^*$ are random elements, $x_i < x_0$ and $S_i = g^{u^{x_i}}$. Then, the secret key *SK* is set as Eq. (4):

$$SK = \{K, K', \{K_i\}_{i \in S}\} \quad \textbf{(4)}$$

(3) $Enc\,(PK, (\mathbb{M}, \rho\,),\ \max, m, r) \rightarrow (CT, \overline{CT}, CT_{Max})$: This algorithm is executed by the data owner to generate the ciphertext. In this algorithm, the data owner takes the public key *PK* the access structure $(\mathbb{M}, \rho\,)$, the maximum access times *max*, the data *m* and the random element for decryption test *r* as input. Note that $\mathbb{M}$ denotes a $l \times n$ access matrix, and ρ represents the mapping relationships between the row of $\mathbb{M}$ and the attribute.

(a) The data owner first encrypts the maximum access times as Eq. (5):

$$C_{\max} = \max^e \bmod \eta \quad \textbf{(5)}$$

(b) The data owner then encrypts the data *m* and the element *r* for decryption test. Firstly, it randomly selects two vector $v = (s, y_2, y_3, ..., y_n)$ and $\overline{v} = (\overline{s}, \overline{y}_2, \overline{y}_3, ..., \overline{y}_n)$, where $y_2, y_3, ..., y_n \in \mathbb{Z}_q^*$ are used to share the encryption secret $s \in \mathbb{Z}_q^*$ and $\overline{y}_2, \overline{y}_3, ..., \overline{y}_n \in \mathbb{Z}_q^*$ are used to share the encryption secret $\overline{s} \in \mathbb{Z}_q^*$. Then, for $i = 1, 2, ..., l$, the data owner computes $\lambda_i = \mathbb{M}_i \cdot v$ and, where $\mathbb{M}_i$ represents the *i*-th row of the access matrix $\mathbb{M}$. Finally, the data owner computes *CT* as Eq. $CT = \{C = m \cdot \hat{e}(g, g)^{as}, C' = g^s, C_i = g^{a\lambda_i} h_{\rho(i)}^{-s}\}, \overline{CT}$ as Eq. (7), and sends $\{CT, \overline{CT}, C_{\max}\}$ to the cloud.

$$CT = \{C = m \cdot \hat{e}(g, g)^{as}, C' = g^s, C_i = g^{a\lambda_i} h_{\rho(i)}^{-s}\} \quad \textbf{(6)}$$

$$\overline{CT} = \{\overline{C} = r \cdot \hat{e}(g, g)^{a\overline{s}}, \overline{C'} = g^{\overline{s}}, \overline{C_i} = g^{a\overline{\lambda}_i} h_{\rho(i)}^{-\overline{s}}\} \quad \textbf{(7)}$$

(4) $Dec\,\{CT, \overline{CT}, C_{Max}\ \ \mathbb{M}\ \ PK, SK) \rightarrow (m)$: This algorithm is executed by the cloud to limit the access times of the data *m*, and the users to access the content of *m*. For the cloud, it first decrypts the maximum access times *max* as Eq. (8)

$$\max = C_{\max}{}^d \bmod \eta \quad \textbf{(8)}$$

Then, it initializes a counter $count = 0$, whose value denotes the times that the data *m* has been accessed. Finally, it computes $count = count + 1$ when a user is verified to be a valid user. For the users, they first find coefficients $\{\omega_i \mid i \in S\}$ such that $\sum_{i \in s} \omega_i\ \mathbb{M}_i = (1, 0, ..., 0)$, and then do the following two steps:

(a) $DecTest\,(CT,\ \mathbb{M}, PK, SK) \rightarrow (r^*)$: This step is used for decryption test. It takes $\overline{CT}$, $\mathbb{M}$, *PK*, *SK* as input, finds valid coefficients $\{\overline{\omega_i} \mid i \in S\}$, and then returns $r^* = \overline{C} / \overline{E}$, where

$$E = \frac{\hat{e}(\overline{C'}, K)}{\hat{e}(\prod_{i \in s} \overline{C_i}^{\omega_i}, K)\, \hat{e}(\overline{C'}, \prod_{i \in s} (K_{\rho(i)} S_0)^{\omega_i})} \quad \textbf{(9)}$$

If $r^* = r$ and *count* < *max*, the users are authorized to access the data *m* and go to the following step.

(b) $DecData\,(CT, \mathbb{M}, PK, SK) \rightarrow (m)$: After receiving the ciphertext *CT*, the users take the *CT*, $\mathbb{M}$, *PK* and *SK* as input, compute

$$\overline{E} = \frac{\hat{e}(\overline{C'}, K)}{\hat{e}(\prod_{i \in s} C_i^{\omega_i}, K)\, \hat{e}(C', \prod_{i \in s} (K_{\rho(i)} S_0)^{\omega_i})} \quad \textbf{(10)}$$

and recover the data as $m = C / E$

5 Evaluation

In this section, the security and the performance of the proposed scheme are discussed in detail. Moreover, the proposed scheme is compared with related schemes, and the results of comparison demonstrate the superiority of our scheme.

5.1 Security Analysis

Here, the security analysis is given in terms of correctness, confidentiality and DoS resistance.

***Theorem 1*: The proposed scheme is correct.**

Proof: The correctness of our scheme means the data *m* can be accessed by all valid users, which requires that $\max = {C_{\max}}^{d} \bmod \eta$, $r = \overline{C} / \overline{E}$ and $m = C / E$. Then, the above three equations are proved as follows:

Firstly, the prove of $\max = {C_{\max}}^{d} \bmod \eta$ is given as Eq. (11)

$$\begin{aligned} & {C_{\max}}^{d} \bmod \eta \\ & = (\max{}^{e} \bmod \eta)^{d} \bmod \eta \\ & = \max{}^{ed} \bmod \eta \\ & = \max \end{aligned} \tag{11}$$

From Eq. (11), we can see that any user has the opportunity to access the data m if it has not been accessed max times.

Secondly, the prove of $r = \overline{C} / \overline{E}$ is presented as Eq. (12), Eq. (13) and Eq. (14)

$$\begin{aligned} \overline{E} & = \frac{\hat{e}(\overline{C'}, K)}{\hat{e}(\prod_{i \in s} \overline{C_i}^{\omega_i}, K)\, \hat{e}(\prod_{i \in s} (K_{\rho(i)} S_0)^{\omega_i})} \\ & = \frac{\hat{e}(g^{\bar{s}}, g^{a}, g^{at})}{\hat{e}(\prod_{i \in s} (g^{a\overline{\lambda_i}} h_{\rho(i)}^{-\bar{s}})^{\omega_i}, g^{t})\, \hat{e}(g^{\bar{s}}, \prod_{i \in s} (S_i h_x^{t} S_0)^{\omega_i})} \\ & = \frac{\hat{e}(g^{\bar{s}}, g^{a}) \hat{e}(g^{\bar{s}}, g^{at})}{\hat{e}(\prod_{i \in s} g^{a\bar{s}}, g^{t})\, \hat{e}(\prod_{i \in s} h_{\rho(i)}^{-\bar{s}\omega_i}, g^{t})\, \hat{e}(g^{\bar{s}}, \prod_{i \in s} (S_i h_x^{t} S_0)^{\omega_i})} \\ & = \frac{\hat{e}(g^{\bar{s}}, g^{a})}{\hat{e}(\prod_{i \in s} h_{\rho(i)}^{-\bar{s}\omega_i}, g^{t})\, \hat{e}(g^{\bar{s}}, \prod_{i \in s} {}_{\rho(i)}^{t\omega_i})\, \hat{e}(g^{\bar{s}}, \prod (S_i S_0)^{\omega_i})} \\ & = \frac{\hat{e}(g^{\bar{s}}, g^{a})}{\prod_{i \in s} (S_i S_0)^{\omega_i})} \end{aligned} \tag{12}$$

Furthermore,

$$S_0^{-1} = g^{u^{x0}} = (g^{u^{xi}})^{u^{x0} - u^{xi}} = (S_i)^{u^{x0} - u^{xi}} \tag{13}$$

Hence, $\overline{E} = \hat{e}(g^{\bar{s}}, g^{a})$, and then

$$r = \frac{\overline{C}}{\overline{E}} = \frac{r \cdot \hat{e}(g, g)^{a\bar{s}}}{\hat{e}(g^{\bar{s}}, g^{a})} = r \tag{14}$$

From Eq. (12), Eq. (13) and Eq. (14), we can see that any valid user can pass the decryption test, and get the cipertext of the data *m*.

Finally, the proof of $m = C / E$, which is similar to that of $r = \overline{C} / \overline{E}$, is given as Eq. (15) and Eq. (16)

$$\begin{aligned} \overline{E} & = \frac{\hat{e}(\overline{C'}, K)}{\hat{e}(\prod_{i \in s} C_i^{\omega_i}, K)\, \hat{e}(\prod_{i \in s} (K_{\rho(i)} S_0)^{\omega_i})} \\ & = \frac{\hat{e}(g^{\bar{s}}, g^{a}, g^{at})}{\hat{e}(\prod_{i \in s} (g^{a\lambda_i} h_{\rho(i)}^{-s})^{\omega_i}, g^{t})\, \hat{e}(g^{s}, \prod_{i \in s} (S_i h_x^{t} S_0)^{\omega_i})} \\ & = \frac{\hat{e}(g^{\bar{s}}, g^{a}) \hat{e}(g^{\bar{s}}, g^{at})}{\hat{e}(\prod_{i \in s} g^{as}, g^{t})\, \hat{e}(\prod_{i \in s} h_{\rho(i)}^{-s\omega_i}, g^{t})\, \hat{e}(g^{s}, \prod_{i \in s} (S_i h_x^{t} S_0)^{\omega_i})} \end{aligned} \tag{15}$$

$$= \hat{e}(g^{s}, g^{a})$$

and

$$m = \frac{C}{E} = \frac{m \cdot \hat{e}(g, g)^{as}}{\hat{e}(g^{s}, g^{a})} = m \tag{16}$$

Therefore, any valid user can access to the data *m*, and further, the correctness of the proposed scheme is proved.

***Theorem 2*: The proposed scheme can prevent data from being accessed by unauthorized users.**

Proof: The confidentiality of the proposed scheme requires that the data *m* will not be accessed by illegal users. To satisfy the requirement of confidentiality, we do the following two things:

For one thing, the data *m* is outsourced to the cloud in the form of ciphertext $CT = \{C = m \cdot \hat{e}(g, g)^{as}$, $C' = g^{s}, C_i = g^{a\lambda_i} h_{\rho(i)}^{-s}\}$, and only those users whose attribute set $S \in 2^{U}$ satisfy the access policy are qualified to decrypt the data m by computing Eq. (17).

$$m = \frac{m \cdot \hat{e}(g, g)^{as}\, \hat{e}(\prod_{i \in s} C_i^{\omega_i}, K')\, \hat{e}(C', \prod_{i \in s} (K_{\rho(i)} S_0)^{\omega_i})}{\hat{e}(g^{s}, g^{a}, g^{t})} \tag{17}$$

In Eq. (17), the *S* of $\prod_{i \in S} C_i^{\omega_i}$ denotes the access policy of the data *m*, while the *S* of $\prod_{i \in S} (K_{\rho(i)} S_0)^{\omega_i}$ denotes the attribute set of the user. Not that if and only if the above two *S* are equal, the Eq. (17) holds. Therefore, any user whose attribute set dose not satisfy the access policy, could not access the data *m*.

For another, to further improve the confidentiality of the proposed scheme, the decryption test is employed to prevent unauthorized users from getting the data *m* and help the cloud to decide which user is malicious. Most of the current related schemes directly deliver the ciphertext of data *m* to the users without verifying whether they are valid or not, which bring potential hazards to users privacy. To resolve the problem, we encrypt a random number *r* as $\overline{CT} = \{\overline{C} = r \cdot \hat{e}(g, g)^{a\bar{s}}$,

$C' = g^{\bar{s}}, \overline{C_i} = g^{a\lambda_i} h_{\rho(i)}^{-\bar{s}}\}$. Only valid users who could correctly decrypt the r by computing Eq. (18) can get the cipertext $CT = \{C = m \cdot \hat{e}(g,g)^{as}, C' = g^{s}, C_i = g^{a\lambda_i} h_{\rho(i)}^{-s}\}$. from the cloud, and further compute data *m*.

$$r = \frac{r \cdot \hat{e}(g,g)^{as}\, \hat{e}(\prod_{i \in s} \overline{C_i}^{\omega_i}, K)\, \hat{e}(\overline{C'}, \prod_{i \in s} (K_{\rho(i)} S_0)^{\omega_i})}{\hat{e}(g^{s}, g^{a}, g^{t})} \quad \textbf{(18)}$$

***Theorem 3*: The proposed scheme can resists the DoS attack.**

Proof: DoS attack refers to attackers maliciously send the cloud extensive data and requests message to occupy the resources of the cloud. As a result, the cloud can not respond to requests from valid users in time. To solve the problem, we assume *max* to be the maximum access times, and *count* to be the number that the data *m* has been accessed. If a user wants to get *m*, the cloud should first check whether *count* < *max*. If yes, set *count* = *count* + 1 and continue the scheme; Otherwise, abort the it. Hence, the proposed access scheme can resist the DoS attack.

5.2 Performance Comparison

In this section, our scheme is compared with the related works in terms of security and performance. To show the results of comparison clearly, the comprehensive comparison according to important features, such as privacy protection, DoS resistance, decryption test, attribute ranking and expressiveness is presented in Table 1. From the Table 1, we can conclude that: (1) All schemes in Table 1 can support privacy protection; (2) Only the scheme in [26], the scheme in [28] and our scheme are able to support the attribute ranking, which reduces the complexity of the access policy; (3) LSSS access policies are supported in [28-29] and our scheme, but only AND access policies are realized in the other three related schemes; (4) Only the scheme in [29] and our scheme support decryption test while the former can not resist the DoS attacker.

Table 1. Comparisons of CP-ABE Schemes

Schemes	Privacy protection	Dos Resistance	Decryption Test	Attribute Ranking	Expressiveness
[25]	√	×	×	×	AND
[26]	√	×	×	√	AND
[27]	√	×	×	×	AND
[28]	√	×	×	√	LSSS
[29]	√	×	√	×	LSSS
Our Scheme	√	√	√	√	LSSS

Then, we further compare the proposed scheme with the related scheme in [29] and the results of the comparison are given in Table 2. Here, Pair, Exp, $|I|$ and $|S|$ are used to denote a bilinear pairing option, an exponentiation operation, the size of minimum authorized set in traditional access structure, and the size of minimum authorized set in the proposed access structure with attribute ranking, respectively. Note that the size of minimum authorized set is determined by the complexity of access structure and $|S| \leq |I|$. From the Table 2, we can know that: (1) In encryption, $7|I|+4$ exponentiation operations are needed in the scheme in [29], which is near to 2 times more that of our scheme; (2) In decryption test and decryption phase, $|I|+2$ bilinear pairing operations and $2|I|$ exponentiation operations are required in the scheme in [29], while only constant bilinear pairing operations and $2|I|$ exponentiation operations are required in our scheme. Therefore, from the above analysis, we can conclude that the proposed scheme has a better performance than the related schemes.

Table 2. Performance comparisons between CP-ABE schemes supporting decryption test

Schemes	Encryption Cost	Decryption test cost		Decryption phase cost	
	Exp	Pair	Exp	Pair	Exp
[29]	$7\|I\|+4$	$\|I\|+2$	$2\|I\|$	$\|I\|+2$	$2\|I\|$
Our Scheme	$4\|S\|+5$	3	$2\|S\|$	3	$2\|S\|$

6 Conclusion

In this paper, a fine-grained and efficient access control in e-health environment is proposed. In the proposed scheme, we first employ the decryption test to decide the validity of the users and stipulate only those users who pass the decryption test are qualified to access the data *m*, which prevents the data from malicious users. Then, the maximum access times and counter are employed to limit the access times, which can resists the DoS attack. Moreover, to reduce the complexity of access policy, an access structure with attribute ranking is designed, which makes it easy for the data owner to manage the access policy. Finally, the security analysis and the performance comparison also demonstrate that the proposed scheme performs better in terms of security and the performance.

Acknowledgments

This work is supported by the National Science Foundation of China under Grant No. 61672295, No. 61672290, No. 61772280 and No. U1405254, the Foundation of Guizhou Provincial Key Laboratory of Public Big Data, Guangxi Key Laboratory of Cryptography and Information Security under Grant No. GCIS201715, the Peng Cheng Laboratory Project of Guangdong Province PCL2018KP004, the State Key Laboratory of Information Security under Grant No. 2017-MS-10, the 2015 Project of six personnel in Jiangsu Province under Grant No. R2015L06, the CICAEET fund, and the PAPD fund.

References

[1] W. Joosen, K. Wuyts, R. Scandariato, G. Verhenneman, Integrating Patient Consent in E-Health Access Control, *International Journal of Secure Software Engineering*, Vol. 2, No. 2, pp. 1-24, April, 2011.

[2] Y. Liu, Y. Zhang, J. Ling, Z. Liu, Secure and Fine-Grained Access Control on E-Healthcare Records in Mobile Cloud Computing, *Future Generation Computer Systems*, Vol. 78, No. P3, pp. 1020-1026, January, 2018.

[3] A. Sahai, B. Waters, Fuzzy Identity-based Encryption, *International Conference on the Theory & Applications of Cryptographic Techniques*, Aarhus, Denmark, 2005, pp. 457-473.

[4] A. Shamir, Identity-Based Cryptosystems and Signature Schemes, in: G. R. Blakley, D. Chaum (Eds.), *Proceedings of Crypto '84, Lecture Notes in Computer Science 196*, Springer-Verlag, 1985, pp. 47-58.

[5] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, *Proceedings of the 13th ACM conference on Computer and Communications Security*, Alexandria, VA, USA, 2006, pp. 89-98.

[6] F. Han, J. Qin, H. Zhao,. Hu, A General Transformation from KP-ABE to Searchable Encryption, *Future Generation Computer Systems*, Vol. 30, pp. 107-115, January, 2014.

[7] C.-J. Wang, Y. Liu, J.-T. Kim, An IND-CCA2 Secure Key-Policy Attribute-Based Key Encapsulation Scheme, *Journal of Internet Technology*, Vol. 11, No. 5, pp. 619-625, September, 2010.

[8] J. Kim, W. Susilo, F. Guo, M. H. Au, S. Nepal, An Efficient KP-ABE with Short Ciphertexts in Prime Ordergroups under Standard Assumption, *Acm on Asia Conference on Computer & Communications Security*, Abu Dhabi, United Arab Emirates, 2017, pp. 823-834.

[9] Z. Guan, J. Li, L. Zhu, Z. Zhang, X. Du, M. Guizani, Toward Delay-Tolerant Flexible Data Access Control for Smart Grid with Renewable Energy Resources, *IEEE Transactions on Industrial Informatics*, Vol. 13, No. 6, pp. 3216-3225, December, 2017.

[10] J. Lai, R. H. Deng, Y. Li, Fully Secure Cipertext-Policy Hiding CP-ABE, *International Conference on Information Security Practice & Experience*, Guangzhou, China, 2011, pp. 24-39.

[11] F. Guo, Y. Mu, W. Susilo, D. S. Wong, V. Varadharajan, CP-ABE With Constant-Size Keys for Lightweight Devices, *IEEE Transactions on Information Forensics & Security*, Vol. 9, No. 5, pp. 763-771, May, 2014.

[12] V. Odelu, A. K. Das, Y. S. Rao, S. Kumari, M. K. Khan, K.-K. R. Choo, Pairing-based CP-ABE with Constant-size Ciphertexts and Secret Keys for Cloud Environment, *Computer Standards & Interfaces*, Vol. 54, No. P1, pp. 3-9, November, 2017.

[13] V. Odelu, A. K. Das, M. K. Khan, K.-K. R. Choo, M. Jo, Expressive CP-ABE Scheme for Mobile Devices in IoT Satisfying Constant-Size Keys and Ciphertexts, *IEEE Access*, Vol. 5, pp. 3273-3283, February, 2017.

[14] D. R. Kuhn, E. J. Coyne, T. R. Weil, Adding Attributes to Role-Based Access Control, *Computer*, Vol. 43, No. 6, pp. 79-81, June, 2010.

[15] J. Hur, D. K. Noh, Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22, No. 7, pp. 1214-1221, July, 2011.

[16] J. Dong, Q. Zhao, Security Access Control Policy of Information System under Multi-domain Mode, *International Journal of Internet Protocol Technology*, Vol. 11, No. 1, pp. 44-50, May, 2018.

[17] S. Ruj, M. Stojmenovic, A. Nayak, Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds, *IEEE Transactions on Parallel & Distributed Systems*, Vol. 25, No. 2, pp. 384-394, February, 2014.

[18] D. He, N. Kumar, H. Shen, J.-H. Lee, One-to-many Authentication for Access Control in Mobile Pay-TV Systems, *Science China Information Sciences*, Vol. 59, No. 5, pp. 052108, May, 2016.

[19] J. B. Bernabe, J. L. H. Ramos, A. F. S. Gomez, TACIoT: Multidimensional Trust-aware access Control System for the Internet of Things, *Soft Computing*, Vol. 20, No. 5, pp. 1763-1779, May, 2016.

[20] A. Ouaddah, H. Mousannif, A. A. Elkalam, A. A. Ouahman, Access Control in The Internet of Things: Big Challenges and New Opportunities, *Computer Networks*, Vol. 112, pp. 237-262, January, 2017.

[21] H. Zhong, W. Zhu, Y. Xu, J. Cui, Multi-authority Attribute-Based Encryption Access Control Scheme with Policy Hidden for Cloud Storage, *Soft Computing*, Vol. 22, No. 1, pp. 243-251, January, 2018.

[22] Z. Qiu, Z. Zhang, S. Tan, J. Wang, X. Tao, Hierarchical Access Control with Scalable Data Sharing in Cloud Storage,

Journal of Internet Technology, Vol. 20, No. 3, pp. 663-676, May, 2019.

[23] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy Attribute-based Encryption, *IEEE Symposium on Security & Privacy*, Berkeley, CA, USA, 2007, pp. 321-334.

[24] A. Beimel, Secure Schemes for Secret Sharing and Key Distribution, Ph. D. Thesis, *Technion-Israel Institute of technology*, Haifa, Israel, 1996.

[25] J. Li, K. Ren, B. Zhu, Z. Wan, Privacy-aware Attribute-based Encryption with User Accountability, *International Conference on Information Security*, Pisa, Italy, 2009, pp. 347-362.

[26] H. Li, D. Liu, K. Jia, X. Lin, Achieving Authorized and Ranked Multi-Keyword Search over Encrypted Cloud Data, *IEEE International Conference on Communications (ICC)*, London, United Kingdom, 2015, pp. 7450-7455.

[27] T. V. X. Phuong, G. Yang, W. Susilo, Hidden Ciphertext Policy Attribute-Based Encryption under Standard Assumptions, *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 1, pp. 35-45, January, 2016.

[28] B. Li, D. Huang, Z. Wang, Y. Zhu, Attribute-based Access Control for ICN Naming Scheme, *IEEE Transactions on Dependable and Secure Computing*, Vol. 15, No. 2, pp. 194-206, March-April, 2018.

[29] J. Lai, R. H. Deng, Y. Li, Expressive CP-ABE with Partially Hidden access Structures, *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, Seoul, South Korea, 2012, pp. 18-19.

Biographies

Tiantian Miao received the B.E. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2018. She is currently working toward the M.E. degree in NUIST, Nanjing, China. Her research interests include data access control and privacy preserving in cloud computing.

Jian Shen received the Ph.D. degrees in computer science from Chosun University, South Korea, in 2012. Since 2012, he has been a Professor with the Nanjing University of Information Science and Technology, Nanjing, China. His research interests include public cryptography, cloud computing, data auditing and sharing, and information security systems.

Xin Jin received the B.E. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2017. He is currently working toward the M.E. degree in NUIST, Nanjing, China. His research interests include computer and network security, access control and cloud computing security.

Jin-Feng Lai is currently with the School of Information and Communication Engineering, University of Electronic Science and Technology of China. He has authored or coauthored over 100 refereed papers in journals, conferences, and workshop proceedings about his research areas within four years. His research interests include multimedia communications, sensor-based healthcare, and embedded systems. He is a member of the IEEE CIRCUITSAND SYSTEMS and the IEEE Communications Societies.