Black box-assisted fine-grained hierarchical access control scheme for epidemiological survey data

Xueyan Liu[1], Ruirui Sun[1,*], Linpeng Li[1], Wenjing Li[1], and Tao Liu[2]
[1] College of Computer Science and Engineering, Northwest Normal University
Lanzhou,Gansu, China
[2] China Telecom WanWei Information Technology Co., LTD
Lanzhou, Gansu, China
[e-mail: 18919805672@.189.cn]
[*]Corresponding author: Ruirui Sun
[e-mail: srr6694@163.com]

Received May 31, 2023; revised July 10, 2023; accepted August 19, 2023; published September 30, 2023

Abstract

Epidemiological survey is an important means for the prevention and control of infectious diseases. Due to the particularity of the epidemic survey, 1) epidemiological survey in epidemic prevention and control has a wide range of people involved, a large number of data collected, strong requirements for information disclosure and high timeliness of data processing; 2) the epidemiological survey data need to be disclosed at different institutions and the use of data has different permission requirements. As a result, it easily causes personal privacy disclosure. Therefore, traditional access control technologies are unsuitable for the privacy protection of epidemiological survey data. In view of these situations, we propose a black box-assisted fine-grained hierarchical access control scheme for epidemiological survey data. Firstly, a black box-assisted multi-attribute authority management mechanism without a trusted center is established to avoid authority deception. Meanwhile, the establishment of a master key-free system not only reduces the storage load but also prevents the risk of master key disclosure. Secondly, a sensitivity classification method is proposed according to the confidentiality degree of the institution to which the data belong and the importance of the data properties to set fine-grained access permission. Thirdly, a hierarchical authorization algorithm combined with data sensitivity and hierarchical attribute-based encryption (ABE) technology is proposed to achieve hierarchical access control of epidemiological survey data. Efficiency analysis and experiments show that the scheme meets the security requirements of privacy protection and key management in epidemiological survey.

Keywords: Epidemiological survey, Hierarchical attribute-based encryption, Characteristic value, Multi-authority, Black box.

The work was supported by Foundation Items: The National Natural Science Foundation of China (No. 62262060, 61662071, 62241207). Industrial support plan project of Gansu Provincial Department of Education (2022CYZC-17). Gansu Science and Technology Program(22JR5RA158).

http://doi.org/10.3837/tiis.2023.09.013 **ISSN : 1976-7277**

1. Introduction

In recent years, the COVID-2019 has received widespread attention, and the overall epidemic situation is characterized by strong infectivity, rapid spread and high risk. Epidemiological survey is one of the main means of epidemic prevention and control. Epidemic risk points can be effectively identified through epidemiological survey, which can facilitate precise identification of the close contacts. And then they can take isolation measures, delimit disinfection scope and timely interrupt virus transmission channels. It plays a decisive role in analyzing epidemic transmission mode, determining transmission generations, calculating incubation period and studying and judging the transmission of asymptomatic infections.

In the process of epidemiological survey, the disease control and other epidemiological staff collected relevant information by investigating the case's personal information, social relations, action trajectory, exposure and medical treatment. The epidemiological survey information shall be sorted and analyzed to form an epidemiological survey report for subsequent sharing by multiple parties. However, on the one hand, epidemiological survey data includes personal basic information, disease and health information, social relationship information and other relevant private information. The risk of disclosure is increased due to the high openness of these private information. Disclosure will directly lead to secondary injury to epidemiological survey objects and hinder the smooth implementation of epidemic prevention and control. On the other hand, epidemiological survey data will be applied to different institutions such as disease control and community and each department will pay different attention to epidemiological survey data. This situation is prone to ultra vires access and privacy disclosure. Therefore, authorization management of hierarchical access control should be conducted for users according to the sensitivity of the data to more timely control the epidemic and slow down its spread.

Attribute-based encryption (ABE) [1] can embed access policies in ciphertext or keys, support data sharing and implement fine-grained access control. It has been applied in various fields such as cloud computing, enabling access control and authorization and reducing the communication and computing burden in data sharing. There are two types of ABE: ciphertext-policy ABE (CP-ABE) [2] and key-policy ABE (KP-ABE) [3]. CP-ABE schemes [4, 5] allow data owners to precisely control access to data for only authorized users, which is more suitable for data security sharing of epidemiological survey. However, due to the large number of institutions involved in epidemiological survey process, different access permissions, there are some shortcomings when using the existing CP-ABE [6] for epidemiological survey data sharing and privacy protection. Firstly, attributes and keys management depend on a central authority in a single authority CP-ABE scheme [7]. Although this method is convenient for managing keys, as the number of users increases, it can easily cause bottleneck problems, and the single authority scheme will be affected by centralized attacks, leading to system paralysis [8]. However, epidemiological survey involves multiple institutions in charge of different data, and a single authority cannot meet their needs. Secondly, in the general CP-ABE schemes [9, 10], only access control of a single type of permission is considered. In the epidemiological survey, the data sensitivity is different due to the different confidentiality degree of the institutions to which the data belong and the importance of data properties. Thus, it needs to grant different permissions to different users according to the data sensitivity, so as to conduct fine-grained hierarchical access control, avoid unauthorized access, prevent access without relevant permission and protect the privacy of epidemiological survey data. In addition, many existing CP-ABE schemes have a positive correlation between the size of ciphertext and access policy. Storage and computing cost will also increase as access policies increase, which will

lead to excessive communication burden and reduced the sharing efficiency. Therefore, the current access control technology cannot meet the requirements of decentralized management of multiple institutions, multi-user and hierarchical access control.

To solve these problems, we propose a black box-assisted hierarchical access control scheme for epidemiological survey data. Our scheme uses hierarchical ABE technology to realize hierarchical access control of epidemiological survey data, thereby improving the efficiency of encryption and decryption. Besides, according to the confidentiality degree of the data institution and the importance of data properties, a sensitivity classification method is proposed. With the help of black box, a multi-attribute authority management mechanism without a master key and a trusted center is established to solve the bottleneck problem, avoid the authority deception of trusted center, reduce the storage load and prevent the disclosure of the master key.

1.1 Motivation and contribution

In the context of epidemiological survey, the security of its data and the privacy of its objects have become increasingly prominent. Therefore, privacy protection of epidemiological survey data based on access control has become a new research need. Data owners prevent unauthorized users from obtaining epidemiological survey data to protect these data's privacy. They want to set different permissions for different users of different institutions involved in epidemiological survey according to the sensitivity of the data. Many attribute authorities, namely, the institutions to which the epidemiological data belong, also participate in epidemiological survey. The collusion between dishonest attribute authorities will also cause the disclosure of private information. Thus, the collusion attack of multiple attribute authorities needs to be resisted. Accordingly, an access control scheme without trusted authority based on hierarchical ABE should be designed. This scheme supports multi-permission management for the smooth implementation of epidemiological survey and the security of epidemiological survey data.

Our main work is to propose a hierarchical ABE access control scheme with multiple attribute authorities. Firstly, a special threshold key generation method is designed on the basis of Zhang's scheme [11] and the characteristics of matrix eigenvalue [12]. The difference from Zhang's scheme [11] is that our scheme does not directly recover the secret value. That is to say, the system public key is generated without obtaining the master key to prevent the leakage of the master key and resist collusion from multi-attribute authorities in our scheme. They jointly manage and distribute of the key and each authority only knows its own sub-secret and cannot obtain the sub-secret information of other authorities. Thus, the attribute authority can generate key without obtaining the master key. Secondly, our scheme proposes a sensitivity classification method due to the different confidentiality degree of the institution to which epidemiological survey data belongs and the importance of the data properties and then divides the multiple access permissions. Furthermore, the access structure of hierarchical access tree is adopted in our scheme to encrypt data at one time for providing multiple permissions. When the data user gives out an access request, the user can obtain the data information within the corresponding permission range when his attribute set meets access structure.

The following are our main contributions:

1) Our scheme supports multi-attribute authority management and multi-permission data sharing. Additionally, we have designed a sensitivity division method based on the confidentiality of data institutions and the importance of data properties, which allows user to

assign different permissions to different institutions, enabling multi-permission access control. When users from different institutions access the data, they must obtain the corresponding permissions while satisfying the access policy based on their attribute sets. It effectively addresses privacy protection and access control challenges.

2) It is based on a secret sharing mechanism and utilizes a special threshold of eigenvalues in our scheme to enable multi-attribute authority management. We propose a key generation method. In this method, each attribute authority has its own initial sub-secret, which is assisted by the black box to generate its own sub-key. They jointly generate the key without obtaining the master key and having the trusted center. It avoids the deception of the central authority, solves the bottleneck problem in the single-authority scheme and resists the collusion attack between multi-attribute authorities.

3) We use hierarchical attribute-based encryption technology and hierarchical access tree structure, which only stores the lowest level ciphertext without establishing multiple access structures, saving storage space. At the same time, multiple permissions can be encrypted with one-time encryption, and the cost of encryption time can be reduced without multiple encryptions.

1.2 Related Work

- **Multi-attribute authority ABE**

In most existing ABE schemes, single center authority (CA) distributes and manages user keys, but that will lead to many security problems [13]. In 2007, Chase [14] proposed the first ABE scheme where multiple attribute authorities are jointly responsible for distributing keys and managing attributes to avoid single point attack, but it needs to a CA. Lin et al. [15]'s scheme support multiple attribute authorities to jointly participate in key generation to resist the single point attack. In the multi-attribute authority scheme proposed by Lewko and Water [16], to prevent user collusion, a global user identity is introduced. Although the scheme can resist user collusion attacks, multiple malicious authorities can obtain user attributes when they track user's GID collaboration, which damages user's privacy. For effective privacy protection, a decentralized attribute-based encryption scheme is designed by Tao et al. [17] based on medical blockchain, which can provide effective privacy protection and avoid single point failure. Li et al. [18]'s scheme can make encryption faster and more efficient through the offline encryption. The user will generate the transformed key and hand it over to the honest but curious cloud service provider. So the ciphertext can be decrypted quickly and safely.

- **Hierarchical ABE**

Generally, if data owners want to share much data, they need define different access policies, which may be intricate. With the increase of shared data, it is very easy to cause problems such as heavier ciphertext storage burden and computing overload. In view of this, Gentry et al. [19] first put forward the concept of hierarchical encryption. Wan et al. [20] use hierarchical ABE to encrypt data stored on the cloud. Later, many scholars have proposed hierarchical ABE schemes. Shen et al. [21] proposed a hierarchical scheme but a trusted center is required. Yang et al. [22] applied attribute-based encryption method with Computer-aided Design (CAD) of assembly model, which can protect the content privacy of CAD model and realize hierarchical access control of collaborative design scenes in cloud manufacturing. Sammy et al. [23]'s scheme uses the elliptic curve cryptography, which can help reduce complexity. Besides, they provide dynamic attributes and a user-centric access policy, allowing multiple authorities to manage the attributes and realize data and user authentication. Ying et al. [24] designed a distributed CP-ABE scheme to realize data sharing. They set multiple blockchain nodes to jointly manage the user nodes' attribute keys and effectively protect the privacy of users.

At present, multi-attribute authority ABE schemes and hierarchical ABE schemes are mostly used in medical, cloud computing and other fields, but there is less research on access control in epidemiological survey. Due to the requirement to realize decentralized management of multiple institutions and provide multi-user and hierarchical access control in the process of epidemiological survey, the combination of multi-attribute authority ABE scheme and hierarchical ABE scheme is crucial for data sharing and privacy protection in epidemiological survey.

2. Preliminaries

2.1 Bilinear Maps

Let G_1 and G_T be two multiplicative cyclic group, p be their prime order and g_1 be a generator of G_1, a bilinear mapping $e: G_1 \times G_1 \to G_T$ satisfies the following properties:

(1) Bilinearity: For $\forall g_1 \in G_1, \forall u, x \in Z_p^*$, it has $e(g_1^u, g_1^x) = e(g_1^x, g_1^u) = e(g_1, g_1)^{ux}$.

(2) Non-degeneracy: There $\exists g_1 \in G_1$ such that $e(g_1, g_1) \neq 1$.

(3) Computability: For $\forall g_1 \in G_1$, there is an efficient computation $e(g_1, g_1)$.

2.2 Decisional Bilinear Diffie Hellman (DBDH) Assumption

Let G_1 and G_T be two groups with prime order p, the generator $g_1 \in G_1$ and $x, y, z, w \in Z_p^*$. A bilinear mapping $e: G_1 \times G_1 \to G_T$. If not one adversary can distinguish between $(g_1^x, g_1^y, g_1^z, e(g_1, g_1)^{xyz})$ and $(g_1^x, g_1^y, g_1^z, e(g_1, g_1)^w)$ with a negligible advantage in the polynomial time, then the DBDH assumption holds.

2.3 Access Structure

Let the set of all participants in the system be $F = \{F_1, F_2, \ldots, F_n\}$,the collection is said to be monotonous. For $\forall K_1, K_2$, if $K_1 \in \mathbb{N}$ and $K_1 \subseteq K_2$, then $K_2 \in \mathbb{N}$. If $\mathbb{N} \neq \varnothing$ is the monotonous collection and is a subset of F, then the sets in $\mathbb{N}$ is the authorized set. Otherwise, it is the unauthorized set.

2.4 Lagrange Interpolation Theorem

Let there be polynomial $f(x)$ of degree m of x, give its $m+1$ different points $(x_i, f(x_i))$, then we can determine that the unique $f(x)$ value of x is as shown in (1):

$$f(x) = \sum_{1 \le h \neq i < n}^{n} f(x)\left(\prod_{1 \le h \neq i \le n} \frac{x - x_h}{x_j - x_h}\right). \tag{1}$$

The Lagrange coefficient [25] is in (2):

$$\Delta_{i,s_x'}(x) = \prod_{i \in s, i \neq j}^{n} \frac{x - j}{i - j}, \text{ where: } i, s \in Z_p^*. \tag{2}$$

2.5 Hierarchical Access Tree

Hierarchical access tree [13] is composed of many access structures enabling to realize Hierarchical access control through dividing different permissions.

Suppose Γ is a hierarchical tree with l access levels. Its root node is (x, y), x represents the node level in Γ, y represents the order of the grade where the nodes in Γ are located. As shown in **Fig. 1**, the nodes are described as: $R=(1,1)$, $A=(2,2)$, $B=(2,3)$, $C=(3,2)$, $D=(3,3)$, $E=(4,1)$, $F=(4,2)$, $G=(4,3)$.

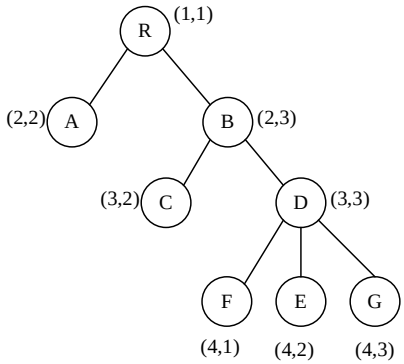

Fig. 1. Hierarchical access tree node

In order to describe Γ, the following formula is defined:

(1) (x, y): It denotes a node in the access tree Γ. If (x, y) is a leaf node, it denotes an attribute. Otherwise, it denotes a threshold gate. In Fig. 1, A, C, E, F and G are the leaf nodes, which denote the attributes. R, B and D are non-leaf nodes, which denote the threshold gates.

(2) $attr(x, y)$: It denotes an attitude associated with the leaf node (x, y) in Γ.

(3) $k_{(x,y)}$: It denotes the threshold value of (x, y).

(4) $index(x, y)$: It denotes a unique value associated with (x, y) in Γ.

(5) (x_h, y_h): It denotes level nodes of Γ, there are l levels of nodes in Γ, which denote l hierarchy. In **Fig. 1**, (x_1, y_1) is the highest, (x_4, y_4) is the lowest.

(6) $parent(x, y)$: It denotes the parent node of (x, y) in Γ.

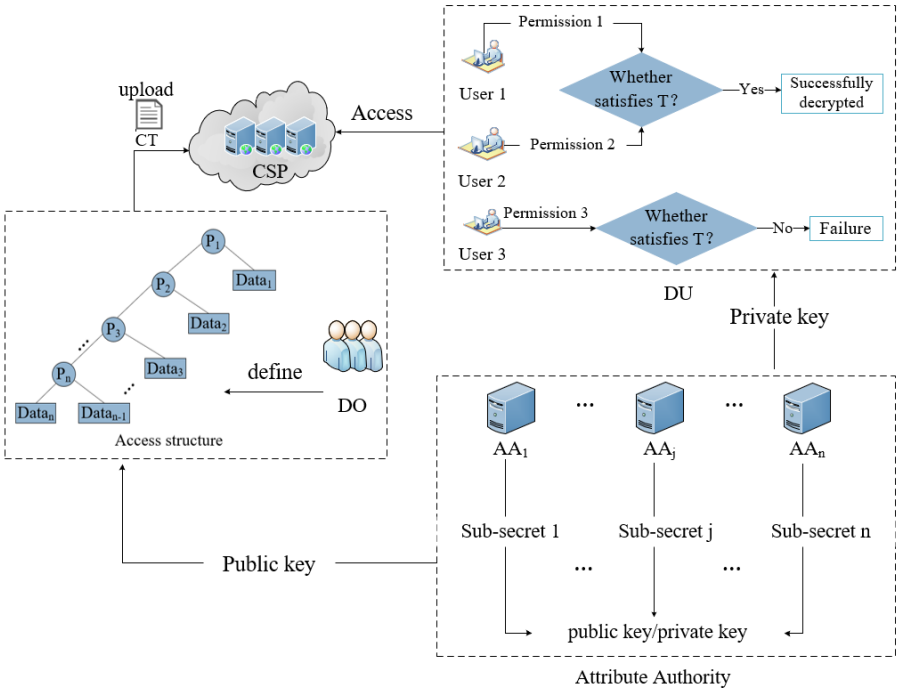

Fig. 2. System model

3. System Framework

3.1 System Model

Our system includes four entities: Attribute Authorities $(AA_j)(j=1,2,\ldots,n)$, Cloud Server Provider (CSP), Data Owner (DO) and Data User (DU), as shown in **Fig. 2**.

(1) Attribute Authority (AA_j): Each AA_j is not completely trusted and their work is separated from each other. In our scheme, each institution involved in epidemiological survey acts as the attribute authority, jointly managing attributes and keys. Each AA_j mainly implements *AAsetup* algorithms and *keygen* algorithms.

(2) Data Owner (DO): The DO is responsible to collect epidemiological survey data, define access structure and upload ciphertext to the CSP.

(3) Cloud Server Provider (CSP): In the system, CSP can provide encrypted storage and transportation functions. CSP is not fully trusted. Although it will execute the assignments and return the correct results, CSP also wants to know more sensitive information.

(4) Data user (DU): Only When DU's attribute set meets access structure, DU can obtain the data within permissions, then get corresponding the data.

3.2 Hierarchical ABE Scheme

The details of the hierarchical ABE scheme is shown as below:

(1) $Globalsetup(\kappa)\rightarrow GP$. The system returns global public parameter GP through the input security parameter κ.

(2) $AAsetup(GP) \to PK$. Each AA_j inputs GP to return system public key PK .

(3) $keygen(PK, GP, S) \to SK$. AA_j inputs public key PK , system parameter GP , user attribute set S and gets user's private key SK .

(4) $Encrypt(GP, M, PK, \Gamma) \to CT$. DO inputs GP , the l level data $M = \{m_1, m_2, \ldots, m_l\}$, PK and hierarchical access structure Γ to return the ciphertext CT .

(5) $Decrypt(CT, GP, SK) \to M$. DU inputs CT , GP , SK . If S meets the entire access policy, it can obtain all data in M . If it only meets the partial access policy, only gets partial access permission of M .

3.3 Security Model

The security model is described under the DBDH assumption which is the choice between adversary A and challenger B in our scheme. It is a chosen-plaintext-attack (CPA) secure symmetric encryption algorithm based on the model in literature [13], the analysis is as follows:

Init: A submits the challenge access structure Γ_0 and the corrupted authorities C_A to algorithm H .

GlobalSetup: B runs $Globalsetup$ algorithm, obtains GP and sends it to A.

AASetup: For the corrupted authorities, B sends system public and secret keys (PK, SK) to A. Otherwise, B sends system public keys PK .

Phase 1: A sends an attribute set T to B for q times secret keys queries, where $T \neq \Gamma_0$.

Challenge: A submits the two messages m_0, m_1 ,which are equal length. B randomly chooses $\mu \in \{0,1\}$ through $Encrypt$ algorithm to obtain ciphertext CT_μ . B returns CT_μ to A.

Phase 2: Repeated Phase 1 adaptively.

Guess: Finally, A outputs the guess $\hat{\mu} \in \{0,1\}$. If $\hat{\mu} = \mu$, A wins the security game. So A can win the game which is defined as shown in (3):

$$Adv_{IND-CPA}(A) = \left| \Pr\left[\hat{\mu} = \mu\right] - \frac{1}{2} \right|. \tag{3}$$

4. Scheme Construction

In this section, we will present the concrete construction of our access control scheme. We design a black box-aided key generation method based on matrix eigenvalue to resist collusion attack. Multiple attribute authorities jointly manage and distribute keys without obtaining the master key. Furthermore, a sensitivity classification method that provides multiple permissions is proposed to ensure that different data users from different institutions have different permissions, protect the user privacy and avoid unauthorized access. Finally, the access structure of hierarchical access tree is adopted in our scheme to encrypt different permissions to realize hierarchical access control of epidemiological survey data.

4.1 A black box-aided special threshold key generation method based on matrix eigenvalue

Suppose there are n attribute authorities, and each $AA_j (j = 1,2,\ldots,n)$ randomly chooses the initial secret information $a_j \in Z_p^* (1 \le j \le n)$. The details are as follows:

(1) Sub-secret generation: AA_j sends a_j to the black box. Black box calculates:

1) $\lambda_j = h^{a_j} \pmod p$, h is automatically generated by the black box $h \in Z_p$. Then, take λ_j as the element to generate a diagonal matrix $\Lambda = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$.

2) AA_j randomly generate an n dimensional column vector $\overrightarrow{p_j}$ and sends it to the black box. The black box verifies the linear correlation of n column vectors. If they are uncorrelated, the n order invertible matrix P can be generated, the similarity matrix $M = P\Lambda P^{-1}$ can be calculated and its standard ortho-normalization can be performed to obtain the eigenvector vector group $\vec{Q}$: $\overrightarrow{q_1}, \overrightarrow{q_2}, \ldots, \overrightarrow{q_n}$, $\overrightarrow{q_j}$ is the sub-secret.

(2) Sub-key distribution: Black box randomly selects n different numbers $x_1, x_2, \ldots, x_n$ less than p, sends the sub-key $(x_j, \overrightarrow{q_j})$ to AA_j and sets the polynomial of order t.

(3) Reconstruct secret share: Each AA_j sends their respective sub-key $(x_j, \overrightarrow{q_j})$ to the black box, which calculates the corresponding characteristic value λ_j and sends the secret share (x_j, λ_j) to each AA_j.

(4) Calculate the corresponding key: t AA_j calculate and broadcast $e(g_1, g_1)^{\lambda_j}$, ${g_1}^{\lambda_j}$ using Lagrange interpolation to obtain:

$$e(g_1, g_1)^{\lambda} = \prod_{j=1}^{t} (e(g_1, g_1)^{\lambda_j})^{s(j)}$$

$$= e(g_1, g_1)^{\sum_{j=1}^{t} \lambda_j \cdot s(j)}$$

$${g_1}^{\lambda} = \prod_{j=1}^{t} ({g_1}^{\lambda_j})^{s(j)} = {g_1}^{\sum_{j=1}^{t} \lambda_j \cdot s(j)}$$

Where $s(j) = \prod_{\substack{l=1 \\ l \ne j}}^{n} \frac{-x_l}{x_j - x_l}$.

4.2 A data sensitivity classification method with multiple permissions

In the process of epidemiological survey, to achieve hierarchical access control, it is necessary to set different permissions for the users with different attribute set. Before DO encrypts the data, a sensitivity hierarchy model is established for epidemiological survey data. The hierarchical model is divided into two layers: at the first level, the confidentiality degree of the institution to which the data belongs is different, which is set according to national laws and regulations. Second, the confidentiality of different data varies according to the importance of the attribute. The division details are as follows:

(1) First level sensitivity factor: There are l data institutions $I_1, I_2, \cdots, I_l$, and the corresponding sensitivity factors are $f_1, f_2, \cdots, f_l$, then the sensitivity factors satisfy $\sum_{i=1}^{l} f_i = 1$, $0 < f_i < 1$, and the higher the privacy, the smaller the f_i.

(2) Second level sensitivity factor: There is a group of data $D(Att_1, Att_2, \cdots, Att_k)$, Att_i represents the attributes of the $i\text{-}th$ kind data and the corresponding sensitivity factor is $e_j = Info(w_1, w_2, \cdots, w_k)$, where $Info$ is a weighting function, $w_1, w_2, \cdots, w_k$ represent the weight of various influencing factors that form data sensitivity, such as legal definition, application scenarios, impact, etc. Similarly, the higher the privacy, the smaller the e_j.

Integrate (1) and (2) to obtain data sensitivity: $\mathrm{Im}_{ij} = f_i \cdot e_j$.

(3) Permission setting: Each sensitivity is assigned a corresponding permission flag $P_i \to \mathrm{Im}_{ij}$, which meets partial order relation $P_1 > P_2 > \cdots > P_l$. When the user gets P_i, he also obtains smaller permissions $P_i, P_{i+1}, \cdots, P_l$.

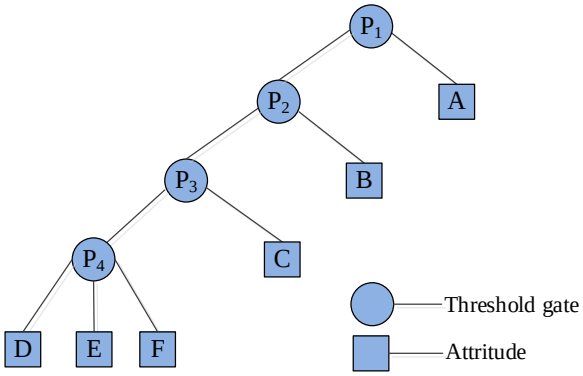

Fig. 3. Example of four permissions

Hierarchical access structure is designed according to data sensitivity and permission marks to realize the function of encrypting multiple permissions at one time. As shown in **Fig. 3**, if the user obtains permission P_1, he can obtain A, B, C, D, E, F. If he obtains permission P_4, only D, E and F can be obtained.

4.3 Black box-assisted fine-grained hierarchical access control scheme for epidemiological survey data

Our scheme's overview is shown in **Fig. 4**. It has the following five algorithms: *Globalsetup*, *AAsetup*, *keygen*, *Encrypt*, *Decrypt*. The details are as follows:

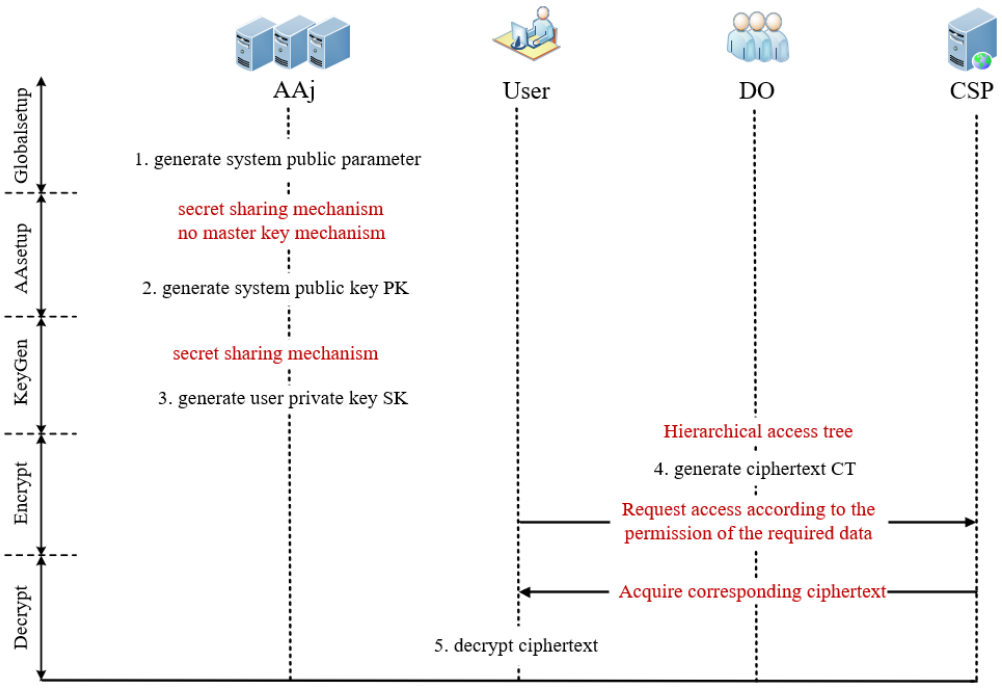

Fig. 4. The overview of our scheme

(1) $Globalsetup(\kappa) \to GP$. The algorithm inputs a security parameter κ, returns the system parameter $GP:\{e,g,p,G_0,G_T,H\}$, where, G_0 and G_T are the multiplication cycle groups with prime order p. A bilinear mapping $e:G_0 \times G_0 \to G_T$ and the generator of $g \in G_0$. Suppose our system has n attribute authorities $AA=\{AA_j \mid j=1,2,\ldots,n\}$. The hash function $H:\{0,1\}^* \to G_0$.

(2) $AAsetup(GP) \to PK$. Each AA_j executes the algorithm and ouputs the system public key PK . Each AA_j randomly selects $a_j \in Z_p$, uses the special threshold key generation method based on eigenvalues proposed in Section 4.1, AA_j share $\lambda \in Z_p$, and cooperate to publish the following system public key:

$$PK=\left\{e(g,g)^{\lambda}, g^{\lambda}\right\}$$

(3) $keygen(PK,GP,S) \to SK$.

1) AA_j randomly selects $v_i, r_i \in Z_p^* \ (i \in S)$, where S represents the user's attribute set. In combination with the method proposed in Section 4.1, each AA_j selects $r_{ij} \in Z_p^* \ (i \in S)$ and broadcasts $g^{r_{ij}}$. At least t AA_j jointly calculate:

$$D_{1,i} = \prod_{j=1}^{t} (g^{\lambda_j} \bullet g^{r_{ij}})^{s(j)}$$
$$= g^{\sum_{j=1}^{t} \lambda_j \bullet s(j) + \sum_{j=1}^{t} r_{ij} \bullet s(j)}$$
$$= g^{\lambda + r_i}$$
$$D_{2,i} = \prod_{j=1}^{t} (g^{r_{ij}} H(i)^{v_i})^{s(j)}$$
$$= g^{\sum_{j=1}^{t} r_{ij} \bullet s(j)} H(i)^{v_i}$$
$$= g^{r_i} H(i)^{v_i}$$
$$D_{3,i} = g^{v_i}$$

2) So DU's private key is:

$$SK = \{D_{1,i} = g^{\lambda + r_i}, D_{2,i} = g^{r_i} H(i)^{v_i}, D_{3,i} = g^{v_i}\}.$$

(4) $Encrypt(GP, M, PK, \Gamma) \to CT$. The DO shares l kinds of data $M = \{m_1, m_2, \ldots, m_l\}$, sets permission $P = \{P_1, P_2, \ldots, P_l\}$ according to the data sensitivity classification method with multiple permissions in Section 4.2, then builds a hierarchical access structure Γ. Firstly, DO encrypts M through symmetric encryption algorithm as following: $CT_P = \{E_{P_1}(m_1), E_{P_2}(m_2), \ldots, E_{P_l}(m_l)\}$. Then, encrypts the permissions P according to the access structure Γ.

1) DO sets the level node $(x_h, y_h)(h = 1, 2, \ldots, l)$ in the access control tree, select l random numbers $b_1, b_2, \ldots, b_l \in Z_p$. Then, he calculates the ciphertext at the level nodes as follows:

$$\overline{C}_h = P_h e(g, g)^{\lambda b_h}, \overline{C}_h' = g^{b_h}$$

2) DO randomly selects polynomials $q_{(x,y)}$ from root node R to each node in Γ. The order of the polynomials is $d_{(x,y)} = t_{(x,y)} - 1$ and $t_{(x,y)}$ is the threshold value. DO sets polynomial $q_R(0) = q_{(x,y)}(0) = b_1$ of the root node R. For $\forall (x, y) \neq R$, if it is a leaf node, then $q_{(x,y)}(0) = q_{(x_k, y_k)}(0) = b_k$. Otherwise, $q_{(x,y)}(0) = q_{parent(x,y)}(index(x, y))$.

3) The leaf nodes ciphertext: Y is the set of leaf nodes in Γ. For $\forall (x, y) \in Y$, ciphertext is:

$$C_{(x,y)} = g^{q_{(x,y)}(0)}, \overline{C}_{(x,y)} = H(attr(x, y))^{q_{(x,y)}(0)}$$

4) Transport nodes ciphertext: X is transport nodes set in Γ. For $\forall (x, y) \in X$, ciphertext is:

$$\widehat{C}_{(x,y),h'} = e(g, g)^{\lambda (q_{(x,y)}(0) + q_{(x,y),h'}(0)}$$

5) DO output complete ciphertext:

$$CT = \{\Gamma, CT_P, \overline{C}_h = P_h e(g, g)^{\lambda b_h}, \overline{C}_h' = g^{b_h}, \forall (x, y) \in Y : C_{(x,y)} = g^{q_{(x,y)}(0)},$$
$$\overline{C}_{(x,y)} = H(attr(x, y))^{q_{(x,y)}(0)}, \forall (x, y) \in X : \widehat{C}_{(x,y),h'} = e(g, g)^{\lambda (q_{(x,y)}(0) + q_{(x,y),h'}(0)}\}$$

(5) $Decrypt(CT, GP, SK) \to M$.

1) If $(x, y) \in Y$, we let $i = attr(x, y)$. If $i \notin S$, define $DecNode(CT, SK, (x, y)) = null$.

Otherwise, we can compute:

$$\begin{aligned} DecNode(CT, SK, (x,y)) &= \frac{e(D_{2,i}, C_{(x,y)})}{e(D_{3,i}, \overline{C}_{(x,y)})} \\ &= \frac{e(g^{r_i} H(i)^{v_i}, g^{q_{(x,y)}(0)})}{e(g^{v_i}, H(attr(x,y))^{q_{(x,y)}(0)})} \\ &= \frac{e(H(i), g)^{v_i q_{(x,y)}(0)} \cdot e(g,g)^{r_i q_{(x,y)}(0)}}{e(H(i), g)^{v_i q_{(x,y)}(0)}} \\ &= e(g,g)^{r_i q_{(x,y)}(0)} \end{aligned}$$

2) If $(x,y) \notin Y$, set *chi* as the child node and let $F_{chi} = DecNode\left(CT, SK, \left(x,y\right)\right)$, then, we can compute as follows:

$$\begin{aligned} F_{chi} &= \prod_{chi \in s_{(x,y)}} (e(g,g)^{r_i q_{(x,y)}(0)})^{\Delta_{i,s_{(x,y)'}(0)}} \\ &= \prod_{chi \in s_{(x,y)}} (e(g,g)^{r_i q_{parent(chi)}(index(chi))})^{\Delta_{i,s_{(x,y)'}(0)}} \\ &= \prod_{chi \in s_{(x,y)}} e(g,g)^{r_i q_{(x,y)}(i) \Delta_{i,s_{(x,y)'}(0)}} \\ &= e(g,g)^{r_i q_{(x,y)}(0)}. \end{aligned}$$

$i = index(chi), s_{(x,y)}{}' = \{index(chi) : chi \in s_{(x,y)}\}$, Where $\Delta_{i,s(x,y)'}$ is the Lagrange coefficient. Then performs the following decryption operation:

a) If S satisfies part or the whole access structure Γ, we can obtain as follows:

$$\begin{aligned} B_h &= DecNode(CT, SK, (x_h, y_h)) \\ &= e(g,g)^{r_i q_{(x_h, y_h)}(0)} \\ &= e(g,g)^{r_i b_h} \\ F_h &= \frac{e(\overline{C}_h{}', D_{1,i})}{B_h} \\ &= \frac{e(g^{b_h}, g^{\lambda + r_i})}{e(g,g)^{r_i b_h}} \\ &= e(g,g)^{\lambda b_h} \end{aligned}$$

b) If S contains lower authorization nodes, calculate through transport node $\widehat{C}_{(x,y),h'}(h' = 1,2,\ldots)$ as follows:

$$\begin{aligned} F_{h+1,h'} &= \frac{\widehat{C}_{(x,y),h'}}{F_h} \\ &= \frac{e(g,g)^{\lambda(b_h + q_{(x,y),h'}(0))}}{e(g,g)^{\lambda b_h}} \\ &= e(g,g)^{\lambda q_{(x,y),k'}(0)} \end{aligned}$$

c) Calculate corresponding permissions P_h:

$$\frac{\overline{C}_h}{F_h} = \frac{P_h e(g,g)^{\lambda b_h}}{e(g,g)^{\lambda b_h}} = P_h$$

d) According to the obtained permission P_h, the data $m_h = D_{P_h}$ (CT_h) within the permission range in the shared data M is obtained.

5. Security analysis

5.1 Security proof

Theorem 1: If the DBDH assumption is valid, no adversary can break our proposed scheme in a certain probability polynomial time, then our scheme is IND-CPA secure.

Proof: Suppose that an adversary A will attack our scheme with a non-negligible advantage ε in polynomial time, a polynomial time algorithm H can attack the DBDH assumption with a non-negligible advantage $\frac{\varepsilon}{2}$.

The challenger B randomly selects $x, y, z \in Z_p^*$, $\eta \in \{0,1\}$, $e(g,g)^{xyz} \in G_T$. Let a bilinear mapping $e: G_0 \times G_0 \to G_T$, the generator $g \in G_0$. If $\eta = 0$ is established, B sends $(X,Y,Z,W) = (g^x, g^y, g^z, e(g,g)^{xyz})$ to H. Otherwise, sends $(X,Y,Z,W) = (g^x, g^y, g^z, e(g,g)^w)$ to H. After receiving (X,Y,Z,W), H plays the following security games with A:

Initialization: A submits the challenge access structure Γ_0 and a list of corrupted authorities C_A to H.

GlobalSetup: H randomly chooses $AA_j^* \in \{AA_1, AA_2, \ldots, AA_n\}$

(1) If $AA_j \in C_A$, H randomly chooses a number $w_j \in Z_p$, uses the key generation method based on eigenvalue to calculate $f_j = h^{w_j}$. Then, he uses Lagrange interpolation to calculate $e(g,g)^f$ and g^f, simulator H sends $< f_j, e(g,g)^f, g^f, w_j >$ to the adversary.

(2) If $AA_j \notin C_A$, H randomly chooses $w_j \in Z_p$, calculates $f_j = g^{w_j} = g^b$. Simulator H randomly chooses $w_j' \in Z_p$ and calculates $f_j = g^{w_j'+a}$. If $AA_j = AA_j^*$, $e(g,g)^{\lambda} = e(g,g)^{f+ab}$. If AA_j is honest, H sends PK to A.

Phase 1: A sends B attribute set T to ask for the key, where $T = \{\varpi \in \Gamma\} \notin \Gamma_0$.

(1) For $AA_j \in C_A$, H chooses the random number $r_i \in Z_p$, $v_i \in Z_p$ and uses the key generation method based on eigenvalues to calculate SK.

(2) For $AA_j \notin C_A$, H randomly chooses $r_i \in Z_p$, $v_i' \in Z_p$ and calculate $D_{1,i} = g^{f+r_i}$, $D_{2,i} = g^{r_i} H(i)^{v_i'}$, $D_{3,i} = g^{v_i'}$. Simulator H randomly chooses $v_i'' \in Z_p$, if $AA_j = AA_j^*$, $D_{1,i} = g^{f+r_i}$, $D_{2,i} = g^{r_i} H(i)^{v_i''+a}$, $D_{3,i} = g^{v_i''+a}$. If $AA_j \neq AA_j^*$, simulator H randomly chooses $r_i' \in Z_p$, sets $r_i = r_i' - a$, $f = f' + ab$, calculates $D_{1,i} = g^{f'+ab+r_i'-a} = g^{f'+ab+r_i'-a}$. For $\varpi \in T$, $D_{2,i} = g^{r_i'-a} H(i)^{v_i''+a} = g^{r_i'} / A \cdot H(i)^{v_i''+a}$, H sends SK to A.

Challenge: B receives m_0, m_1 from A and randomly chooses $\hat{\mu} \in \{0,1\}$ to obtain ciphertext $CT_{\mu} = \{C_k' = g^{s_k} = g^c = C, \tilde{C}_k = m_{\mu} \cdot e(g,g)^{f \cdot s_k} = m_{\mu} \cdot e(g,g)^{f \cdot c} = m_{\mu} \cdot We(g,g)^{f \cdot c}\}$. B sends CT_{μ} to A.

Phase 2: Repeated Phase 1.

Guess: Finally, A outputs his guess $\hat{\mu} \in \{0,1\}$. If $\hat{\mu} = \mu$, simulator H outputs 0, so $W = e(g,g)^{xyz}$. Otherwise, outputs 1, $W \in G_T$.

Probability Analysis: The correct ciphertext can be decrypted if $W = e(g,g)^{xyz}$, so $\Pr[B(g, g^x, g^y, g^z, W = e(g,g)^{xyz}) = 0] = \varepsilon + \frac{1}{2}$. If $W \in G_T$, the information of μ cannot be learned, so, $\Pr[C(g, g^x, g^y, g^z, W = e(g,g)^w) = 0] = \frac{1}{2}$. Finally, B's advantage in solving DBDH problems is $Adv_{IND-CPA}(A) = \frac{\varepsilon}{2}$, where, ε is a non-negligible advantage, so its advantages cannot be ignored.

Theorem 2: Our scheme can resist multiple authority collusion attacks.

Proof: We propose a special threshold key generation method based on eigenvalue based on the secret sharing scheme of Zhang et al. [11]. In *keygen* phase, there is no master key, and each AA_j can only obtain part of its own information, so that AA_j cannot get the complete SK to resist multiple authority collusion.

Theorem 3: Our scheme can resist user collusion attacks.

Proof: Only when S meets access structure, DU can get P_h . When users with different permissions conspire, because different users randomly choose different v_i , part of the user's key $D_{2,i} = g^{r_i} H(i)^{v_i}$ is different, so user collusion cannot obtain the user's key. Therefore, the scheme can resist collusion attacks from users.

5.2 System robustness

In our system, attribute authority is not fully trusted, and there are some malicious attribute authorities that will prevent from running the system normally. Since our scheme uses the (t,n) special threshold key generation method to manage and generate user keys, the robustness of the system depends on (t,n) . Suppose the attacker can crash some AAs. The probability of the system being attacked satisfies the Bernoulli distribution $\sum_{n-t+1}^{n} \binom{i}{n} p^i (1-p)^{n-i}$ when the probability of the single AA crash is p . In **Fig. 5**, when n is taken as 7 and 14 respectively, the probability of the system being attacked is different with p .

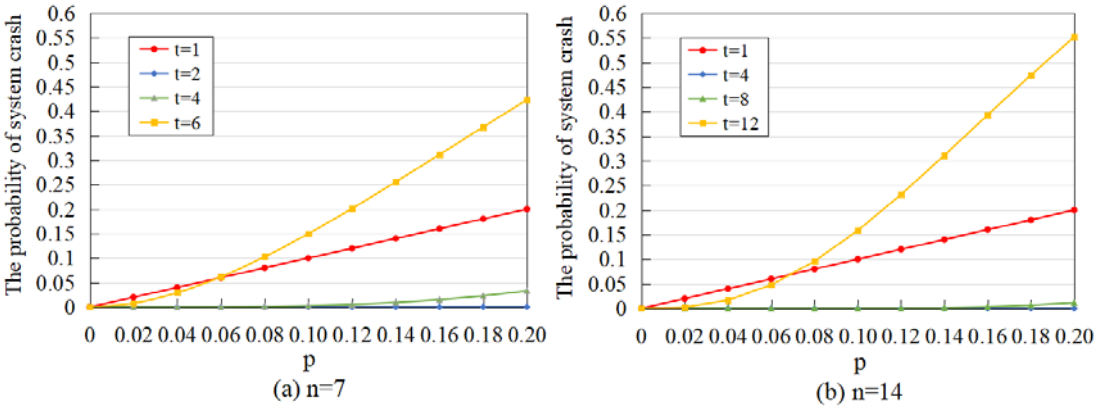

Fig. 5. The probability of system being attacked changes with p

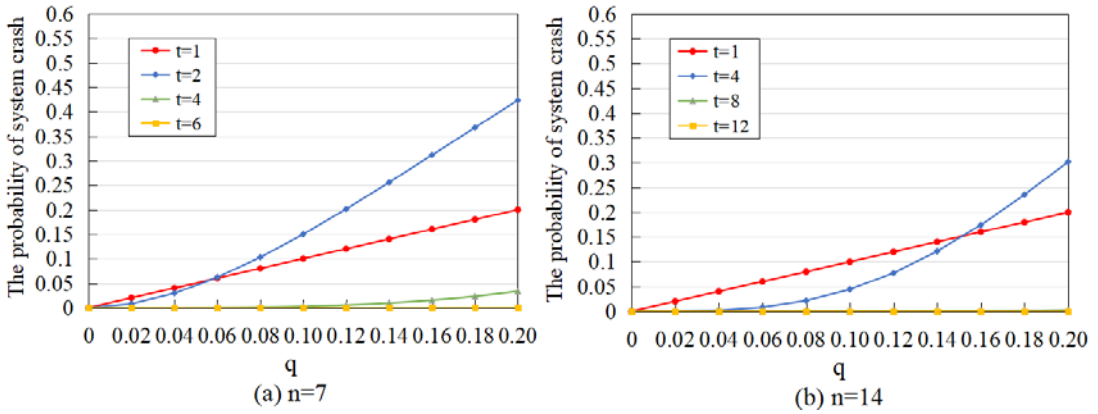

Fig. 6. The probability of system being attacked changes with q

In addition, the attacker can control the system if he can control t attribute authorities. Suppose the probability that the attacker can control a single attribute authority is q, the probability of the system crash being attacked meets the Bernoulli distribution $\sum_{t}^{n}\binom{i}{n}q^{i}(1-q)^{n-i}$. As shown in **Fig. 6**, the probability of the system being attacked changes with q and n is 7 and 14 respectively.

In **Fig. 5** and **Fig. 6**, the robustness of our scheme is more significant. The probability of the system being attacked is lower as t gets closer to n.

6. Performance Analysis

This section presents a comparison between our scheme with related schemes [2], [13], [20], [26] and [27] in term of the functions, computational overhead and storage costs. The relevant notations are described in **Table 1**.

Table 1. Notations

Notations	Description
E_p	The bilinear pairing operations time
E_{G_0}	Exponential computation time in G_0
E_{G_T}	Exponential computation time in G_T
T	Transport nodes set
S_i	The set of the least interior nodes satisfying Γ
$\|*\|$	The number of elements in *
L_*	The bit-length of element in *
A_u	The user attribute set
A_{C_i}	The ciphertext attribute set
l	The number of data types

6.1 Functional comparison

The functions of our scheme and schemes [2], [13], [20], [26] and [27] are analyzed and compared in **Table 2**. Amongst them, schemes [2] and [26] are of CP-ABE type. The access structure increases linearly with data types, while ciphertext storage cost also increases, which will result in greater storage burden. Compared with scheme [20], a sensitivity classification method is designed to set different access permissions in our scheme. Meanwhile, we propose a special threshold key generation method based on matrix eigenvalue to establish a multi-attribute authority management mechanism without a master key. This way avoids the collusion of dishonest attribute authorities, which is not found in other schemes. Moreover, our scheme and scheme [13] are of H-CP-ABE type and both use hierarchical access tree access structure, which can reduce storage burden and improves the efficiency of the scheme. The other feature is to design a data sensitivity classification method with multiple permissions, which enables it to realize hierarchical access control. In summary, our scheme can meet privacy protection and access control requirements in epidemiological survey and is feasible.

Table 2. Functional comparison

Scheme	Type	Access structure	Muti-authority	No master key	Multi-permission	Resist collusion
[2]	CP-ABE	Access tree	×	×	×	×
[13]	H-CP-ABE	Hierarchical access tree	√	×	√	√
[20]	H-A-SBE	Hierarchical access tree	√	×	×	×
[26]	CP-ABE	And gate	×	×	×	√
[27]	MA-ABE	LSSS	√	×	×	√
Ours	H-CP-ABE	Hierarchical access tree	√	√	√	√

6.2 Computational cost

Suppose our system need to share l hierarchical data $M=\{m_1,m_2,\ldots,m_l\}$. The access order decreases gradually with the number of levels. According to the characteristics of hierarchical access tree, each level of ciphertext attribute set is expressed as $\{A_{C_1},A_{C_2},\ldots,A_{C_l}\}$, where $A_{C_1}\supseteq A_{C_2}\supseteq\ldots\supseteq A_{C_l}$.

As shown in **Table 3**, the size of ciphertext in scheme [2], [26] and [27] is positively correlated to the number of attributes and data types Different access structures need to be established according to different levels of data. which will result in higher computational costs. We use the hierarchical access tree structure to encrypt data and designs an authorization algorithm for multiple permissions. This algorithm can encrypt multiple permissions at a time. Thus, it does not need to establish an access structure for each level. Compared with schemes [2], [26] and [27], our scheme greatly saves the computational cost.

Table 3. Computational cost

Scheme	Encryption	Decryption	Keygen
[2]	$[2(\lvert A_{C_1}\rvert+\lvert A_{C_2}\rvert+\ldots+\lvert A_{C_l}\rvert)+l]E_{G_0}+lE_{G_T}$	$l(2\lvert A_u\rvert+1)E_p+[2(\lvert S_1\rvert+\lvert S_2\rvert+\ldots+\lvert S_l\rvert)+2l]E_{G_T}$	$2(\lvert A_u\rvert+1)E_{G_0}$
[26]	$[3(\lvert A_{C_1}\rvert+\lvert A_{C_2}\rvert+\ldots+\lvert A_{C_l}\rvert)+2l]E_{G_0}+lE_{G_T}$	$l(2\lvert A_u\rvert+1)E_p+[(\lvert S_1\rvert+\lvert S_2\rvert+\ldots+\lvert S_l\rvert)+3l]E_{G_T}$	$(2\lvert A_u\rvert+3)E_{G_0}$
[27]	$[3(\lvert A_{C_1}\rvert+\lvert A_{C_2}\rvert+\ldots+\lvert A_{C_l}\rvert)+2l]E_{G_0}+lE_{G_T}$	$l(3\lvert A_u\rvert+1)E_p+[(\lvert S_1\rvert+\lvert S_2\rvert+\ldots+\lvert S_l\rvert)+3l]E_{G_T}$	$2(\lvert A_u\rvert+2)E_{G_0}$
Ours	$(2\lvert A_{C_1}\rvert+l)E_{G_0}+(k'\lvert T\rvert+l)E_{G_T}$	$(2\lvert A_u\rvert+1)E_p+(2\lvert S_1\rvert+2l+k'\lvert T\rvert)E_{G_T}$	$4\lvert A_u\rvert E_{G_0}$

6.3 Storage cost

Table 4 presents a comparison in term of the PK, MSK, SK and CT sizes of our scheme with those of schemes [2], [26] and [27]. In our scheme, we design a special threshold key generation method based on matrix eigenvalue with the help of black box, which can establish a multi-attribute authority management mechanism without trusted center and master key and take up less storage space. However, the schemes [2], [26] and [27] requires layered encryption of data at multiple levels, which aggravates the burden of ciphertext storage. Our scheme encrypts the data by using the hierarchical ABE, it only needs to store attribute ciphertext. When the data types and user attributes increase, our storage cost is lower than that in schemes [2], [26] and [27].

Table 4. Storage cost

Scheme	PK	MSK	SK	CT
[2]	$3L_{G_0}+L_{G_T}$	$L_{Z_p}+L_{G_T}$	$(3\lvert A_u\rvert+1)L_{G_0}$	$[2(\lvert A_{C_1}\rvert+\lvert A_{C_2}\rvert+\ldots+\lvert A_{C_l}\rvert)+l]L_{G_0}+lL_{G_T}$
[26]	$2L_{G_0}+L_{G_T}$	$4L_{Z_p}$	$(2\lvert A_u\rvert+3)L_{G_0}$	$[3(\lvert A_{C_1}\rvert+\lvert A_{C_2}\rvert+\ldots+\lvert A_{C_l}\rvert)+2l]L_{G_0}+lL_{G_T}$
[27]	$2L_{G_0}+L_{G_T}$	$3L_{Z_p}$	$2(\lvert A_u\rvert+2)L_{G_0}$	$[3(\lvert A_{C_1}\rvert+\lvert A_{C_2}\rvert+\ldots+\lvert A_{C_l}\rvert)+2l]L_{G_0}+lL_{G_T}$
Ours	$L_{G_0}+L_{G_T}$	-	$4\lvert A_u\rvert L_{G_0}$	$(2\lvert A_{C_1}\rvert+l)L_{G_0}+(k'\lvert T\rvert+l)L_{G_T}$

6.4 Experiment simulation

We carried out some experimental simulations to evaluate our scheme. Our scheme is implemented on Windows 10 operating system, 8.00 GB RAM laptop and 2.60 GHz CPU. The Java language and the Pairing-Based Cryptography (PBC) library [28] are applied to implement cryptographic algorithm. The operations on prime-order groups are implemented by Type A pairing, which is provided by Java Pairing-Based Cryptography Library (JPBC). The access policy what we use in the experiments is the access tree. The experimental results are as follows.

The encryption and decryption times are shown in **Fig. 7** in our scheme and schemes [2], [26] and [27]. We use the hierarchical access tree to encrypt data and does not need to establish different access structures according to different levels of permission that reduces computational cost. The encryption and decryption times increase slowly when the number of attributes increases, but they increase rapidly in other schemes with $l = 4$. Our scheme is more efficient than other three schemes.

A similar phenomenon can be observed from **Fig. 8**. We fix user attributes $A_u = 30$ and we observe the encryption and decryption times vary as l changes. With the increase of l, its exponential operation rises. Then, computational cost increases slowly in our scheme, on the contrary, they rise rapidly in schemes [2], [26] and [27]. Thus, the time efficiency of our scheme is more prominent.

In our scheme, the access structure of hierarchical access tree is used for encryption and decryption. It does not need to establish multi-level access structure and store multi-level ciphertext. The establishment of a master key-free system in our scheme can reduce the storage cost. According to the analysis of (a) and (b) in **Fig. 9**, as data types and attributes increase, our scheme has less storage burden.

According to the abovementioned conclusions, our scheme has more significant advantages in computing and storage costs than schemes [2], [26] and [27]. Our scheme fully utilizes the characteristics of hierarchical access tree to provide a finer division of different permissions and more efficient services for the smooth process of epidemiological survey.

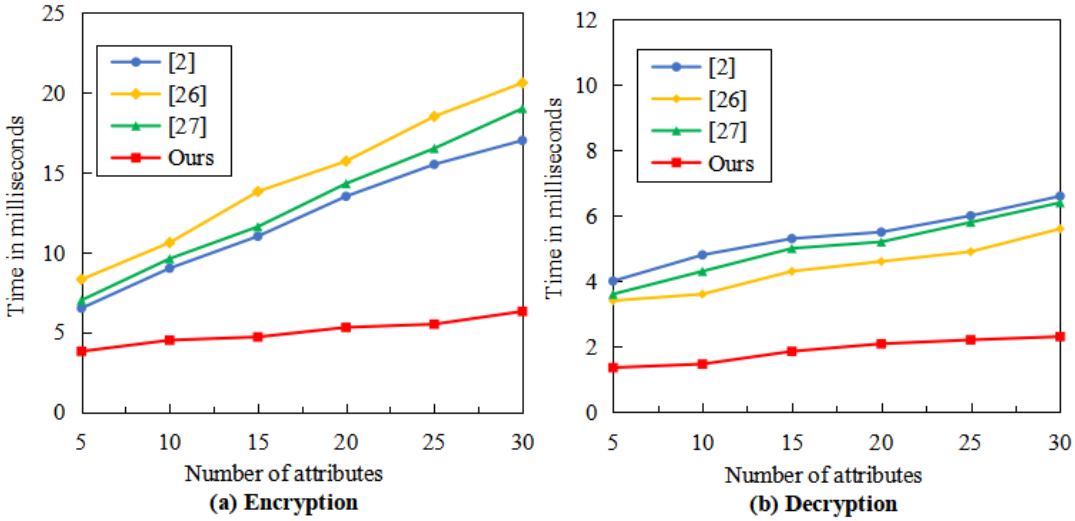

Fig. 7. The comparison of encryption/decryption time ($l = 4$)

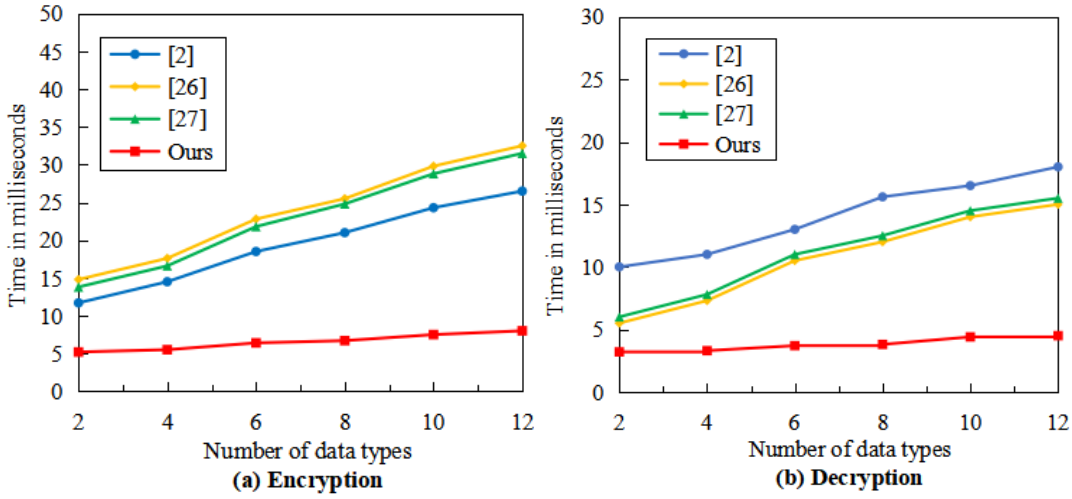

Fig. 8. The comparison of encryption/decryption time ($|A_u|=30$).

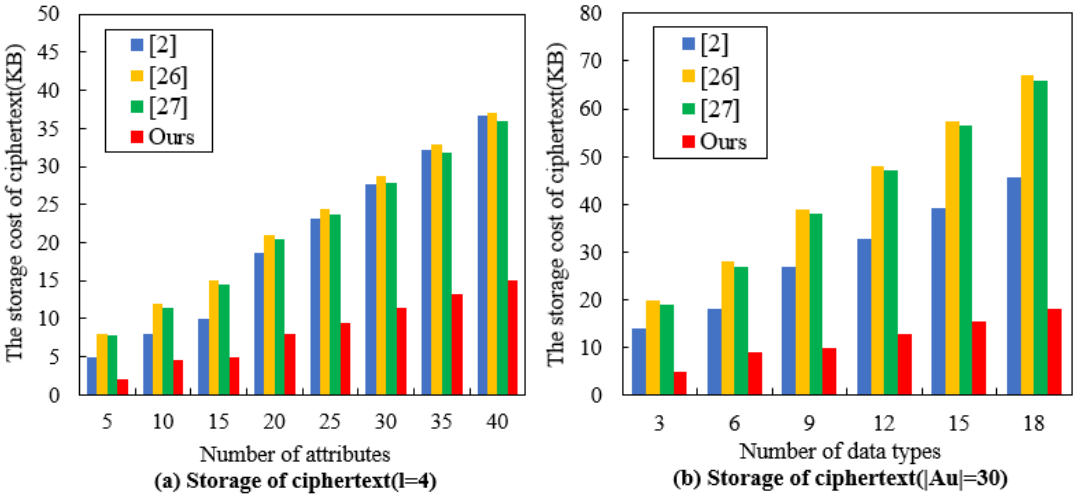

Fig. 9. The comparison of storage cost of ciphertext

7. Conclusion

Data privacy protection in epidemiological survey is explored based on the hierarchical access tree structure to ensure smooth operation of this survey. A data sensitivity classification method with multiple permissions is designed according to the confidentiality degree of the institution to which the data belongs and the importance of the data properties. Different permissions are set using hierarchical access tree structure to improve encryption efficiency and realize privacy protection. Combined with the characteristics of matrix eigenvalue, multi-attribute authority management mechanism is established without a trusted center to prevent fraud of a single authority center. Public and private keys are distributed without obtaining the master key by using secret sharing mechanism to avoid key disclosure. Our scheme is proven

to be secure under the DBDH assumption. In the future work, more comprehensive access control methods will be considered, such as access structure change and access structure hiding, to better protect the privacy of epidemiological survey data.

Reference

[1] A. Sahai, B. Waters, "Fuzzy identity-based encryption," in *Proc. of The 24th Annual International Conference on Theory and Applications of Cryptographic Techniques*, pp. 457-473, 2005. Article (CrossRef Link).

[2] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-Based encryption," in *Proc. of 2007 IEEE Symposium on Security and Privacy*, pp. 321-334, 2007. Article (CrossRef Link).

[3] V. Goyal, O. Pandey, A. Sahai, W. Brent, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. of the 13th ACM Conference on Computer and Communications Security*, pp. 89-98, 2006. Article (CrossRef Link).

[4] Ba, X. Hu, Y. Chen, Z. Hao, X. Li, X. Yan, "A blockchain-based CP-ABE scheme with partially hidden access structures," *Security and Communication Networks*, vol. 2021, pp. 1-16, Nov. 2021. Article (CrossRef Link).

[5] Z. Zhang, X. Ren, "Data security sharing method based on CP-ABE and blockchain," *Journal of Intelligent & Fuzzy Systems*, vol. 40, no. 2, pp. 2193-2203, Jan. 2021. Article (CrossRef Link).

[6] X. Liu, Y. Xia, W. Yang, F. Yang, "Secure and efficient querying over personal health records in cloud computing," *Neurocomputing*, vol. 274, pp. 99-105, Jan. 2018. Article (CrossRef Link).

[7] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1265-1277, Jun. 2016. Article (CrossRef Link).

[8] J. Tao, L. Ling, "Practical medical files sharing scheme based on blockchain and decentralized attribute-based encryption," *IEEE Access*, vol. 9, pp. 118771-118781, 2021. Article (CrossRef Link).

[9] Y. He, H. Wang, Y. Li, K. Huang, V. C. M. Leung, F. Yu, Z. Ming, "An efficient ciphertext-policy attribute-based encryption scheme supporting collaborative decryption with blockchain," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2722-2733, 15 Feb. 2022. Article (CrossRef Link).

[10] H. Wang J. Liang, Y. Ding, S. Tang, Y. Wang, "Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health," *Computer Standards & Interfaces*, vol. 84, pp. 103696, 2023. Article (CrossRef Link).

[11] Y. Zhang, W. Li, G. Zhao, et al. "Research on Secret Sharing Scheme Without Trusted Center Based on Eigenvalue," *Journal of Electronics & Information Technology*, vol. 40, no. 11, pp. 2752-2757, 2018. Article (CrossRef Link).

[12] Y. Zhang, W. Li, L. Chen, W. Bi, T. Yang, "Verifiable special threshold secret sharing scheme based on eigenvalue," *Journal on Communications*, vol. 39, pp. 169-175, 2018. Article (CrossRef Link).

[13] X. Liu, X. Yang, Y. Luo, L. Wang and Q. Zhang, "Anonymous electronic health record sharing scheme based on decentralized hierarchical attribute-based encryption in cloud environment," *IEEE Access*, vol. 8, pp. 200180-200193, 2020. Article (CrossRef Link).

[14] M. Chase, "Multi-authority Attribute-Based Encryption," in *Proc. of TCC 2007: Theory of Cryptography*, pp. 515–534, 2007. Article (CrossRef Link).

[15] H. Lin, Z. Cao, X. Liang, J. Shao, "Secure threshold multi authority attribute-based encryption without a central authority," *Information Sciences*, vol. 180, pp. 2618-2635, 2010. Article (CrossRef Link).

[16] A. Lewko, B. Waters, "Decentralizing attribute-based encryption," in *Proc. of Advances in Cryptology- EUROCRYPT 2011*, pp. 568-588, 2011. Article (CrossRef Link).

[17] J. Tao and L. Ling, "Practical medical files sharing scheme based on blockchain and decentralized Attribute-based encryption," *IEEE Access*, vol. 9, pp. 118771-118781, 2021. Article (CrossRef Link).

[18] S. Li and H. Zhang, "Online/Offline attribute-based encryption with multi-authority access control," in *Proc. of International Computer Conference on Wavelet Active Media Technology and Information Processing*, pp. 426-433, 2021. Article (CrossRef Link).
[19] C. Gentry, A. Silverberg, "Hierarchical ID-based cryptography," in *Proc. of Advances in Cryptology- ASIACRYPT 2002*, pp. 548-566, 2002. Article (CrossRef Link).
[20] Z. Wan, R H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 743-754, Apr. 2012. Article (CrossRef Link).
[21] J. Shen, D. Liu, Q. Liu, X. Sun and Y. Zhang, "Secure authentication in cloud big data with hierarchical attribute authorization structure," *IEEE Transactions on Big Data*, vol. 7, no. 4, pp. 668-677, Oct. 2021. Article (CrossRef Link).
[22] Y. Yang, F. He, S. Han, Y. Liang, Y. Cheng, "A novel attribute-based encryption approach with integrity verification for CAD assembly models," *Engineering*, vol. 7, pp. 787-797, 2021. Article (CrossRef Link).
[23] F. Sammy, S. Maria Celestin Vigila, "An efficient blockchain based data access with modified hierarchical attribute access structure with CP-ABE using ECC scheme for patient health record," *Security and communication networks*, vol. 2022, pp. 1-11, Mar. 2022. Article (CrossRef Link).
[24] Ying Z, Si Y, Ma J, et al. Z. Ying, Y. Si, J. Ma, X Liu, "Blockchain-based distributed EHR fine-grained traceability scheme," *Journal on Communications*, vol. 42, pp. 205-215, 2021. Article (CrossRef Link).
[25] A. Saidi, O. Nouali, A. Amira, "SHARE-ABE: an efficient and secure data sharing framework based on ciphertext-policy attribute-based encryption and Fog computing," *Cluster Comput*, vol. 25, pp. 167–185, 2022. Article (CrossRef Link).
[26] X. Yan, X. He, T. Liu, Q. Ye, J. Yu, Y. Tang, "Traceable attribute-based encryption scheme with key-delegation abuse resistance," *Journal on Communications*, vol. 41, pp. 150-161, 2020. Article (CrossRef Link).
[27] X. Yan, X. Yuan, Q. Zhang, Y. Tang, "Traceable and weighted attribute-based encryption scheme in the cloud environment," *IEEE Access*, vol. 8, pp. 38285-38295, 2020. Article (CrossRef Link).
[28] V. Lynn, "PBC Library," 2016. [Online]. Available: https://crypto.stanford.edu/pbc.

Xueyan Liu received the B.S. and M.S. degrees in Northwest Normal University, in 2001 and 2004, respectively. In 2016, she received the PH.D. degree in Lanzhou University of technology. She has been working in Northwest Normal University since July 2001, and now she is an associate professor and master tutor. She has published some wonderful articles and she is a reviewer of some journals. She also hosts and participated in several National Natural Science Foundation projects. Her main research interests include cryptographic, information security, and Internet of things security. Her e-mail ID is liuxy@nwnu.edu.cn.

Ruirui Sun received B.S. degree in Henan Normal University, Xinxiang, Henan, in 2021. She is currently pursuing the M.E. degree with the Northwest Normal University, Lanzhou, China. Her research interests include attribute-based cryptography and information security. She is the corresponding author and her e-mail ID is srr6694@163.com.

Linpeng Li received the B.E. degree in engineering from Henan University of Technology, Henan, China, in 2021. He is currently pursuing the M.E. degree with the Northwest Normal University, Lanzhou, China. His research interest is the Internet of Vehicles, blockchain. His e-mail ID is llp201716040121@163.com.

Wenjing Li received the B.E. degree in engineering from the Northwest Normal University, Lanzhou, China, in 2022. She is currently pursuing the M.E. degree with the Northwest Normal University, Lanzhou China. Her research interests include attribute-based cryptography and information security. Her e-mail ID is 17339915388@163.com.

Tao Liu is with the China Telecom WanWei Information Technology Co., LTD, Lanzhou 730070, China. He is currently a senior system designer. His main research interests are big data security and blockchain. His e-mail ID is 18919805672@189.cn.