Dynamic permission access control model based on privacy protection

Qikun Zhang1 · Liang Zhu1 · Kunyuan Zhao1 · Yimeng Wu2 · Baohua Jin1 · Jianyong Li1 · Yinghui Meng1 · Sikang Hu3

Accepted: 20 June 2022 / Published online: 3 August 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
Access control technology is one of the key technologies to ensure safe resource sharing. Identity authentication and authority distribution are two key technologies for access control technology to restrict unauthorized users from accessing resources, and only authorised legal users can access resources. However, user privacy protection and frequent permission changes are two thorny issues that need to be solved urgently by access control technology. In this paper, a dynamic access control model based on privacy protection is proposed to deal with these problems. Compared with existing access control technologies, the main advantages of this paper are as follows: (1) Encrypt and hide the attributes of entities, and use attribute-based identity authentication technology for identity authentication, which not only achieves the purpose of traditional identity authentication, but also ensures the attributes and privacy of entities are not leaked; (2) Binding resource access permissions with entity attributes, dynamically assigning and adjusting resource access control permissions through changes in entity attributes, making resource access control more fine-grained and more flexible. Security proof and performance analysis show that the proposed protocol is secure under the hardness assumption of the discrete logarithm problem and the decision bilinear Diffie–Hellman problem. Compared with the cited references, this model has the advantages of low computational complexity, short computational time, and low communication overhead.

Keywords Privacy protection · Access control · Attribute-based encryption · Information security · Hidden attribute authentication

1 Introduction
The innovation and development of artificial intelligence, big data and 5G technology have promoted the birth of new applications such as smart community, smart transportation and smart city. One of its core technologies is secure resource sharing, information exchange and transmission among multiple entities. Access control is a core technology that guarantees secure resource sharing and information exchange among entities. Under the access control technology, only the legitimate terminal that meets the access policy can access the resources of the network platform. The security of system resources is improved, but the flexibility of access to system resources is enhanced. In recent years, there has been more and more research on access control technology. These studies are applied to medical, industrial, corporate and personal fields. On this basis, many access control schemes have been proposed, such as early autonomous access control and mandatory access control, later identity-based access control and recent research hotspot attribute-based access control, etc. Many practical problems have been solved by them.

However, with the progress of network technology, access control technology is also facing new challenges. The vast and complex data exchange increases the threat to data security and increases the risk of terminal privacy leakage. It is difficult to realize the hierarchical division and classified storage of resources. In the process of resource sharing, the terminal needs to undertake huge computing and communication tasks. In addition, it is still difficult to solve the problem of terminal member revocation or terminal attribute weight

1 School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China
2 School of Architecture and Environmental Engineering Zhengzhou Technical College, Zhengzhou 450000, China
3 School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China
A PP-DPAC model is proposed in this paper. The advantages of this model are as follows:

1. Hidden attribute authentication. Terminal members need to be authenticated before participating in resource sharing. By improving the traditional attribute-based authentication scheme, a terminal identity authentication scheme with hidden attributes is proposed in this paper. In the scheme, not only the identity information of the terminal is hidden, but also the attribute information of the terminal is hidden by algorithm. In this way, the leakage of personal privacy can be avoided.

2. Dynamic and fine-grained access control. Each terminal member has a different number of attributes. Different attribute number combinations correspond to different access permissions. Terminal members access resources at the corresponding level or lower level according to their attribute permissions. When terminal members have lower permissions, they can access higher-level resources by upgrading their permissions. In other words, authenticated terminal members can upgrade or downgrade their permissions to access multiple levels of resources.

3. High security. Shared resources need to be encrypted before being stored. Then it is uploaded to the resource sharing storage platform. When terminal members obtain resources, they not only need to verify identity, but also need to have enough attribute weights to calculate the decryption key and decrypt the ciphertext. This double guarantee mechanism can resist collusion attacks and has high security.

2 Related work

With the development and application of various new technologies, the application scenario of access control is also expanding. However, the existing access control technology is difficult to meet the requirements of complex application scenarios, such as cloud computing, edge computing and industrial Internet of things (IoT). In recent years, many scholars have carried out in-depth research on access control technology in combination with specific application scenarios. An access control protocol combined with blockchain is proposed in [1,2]. Blockchain has the characteristics of decentralization, which can better solve the third-party trust problem. At the same time, blockchain technology is used to record the attribute information of the terminal members, which not only facilitates the management of the terminal, but also enhances the security of the system. The algorithm part of the scheme adopts a modular design. This method not only facilitates the later management and maintenance, but also improves the flexibility of the scheme. In [3], an access control scheme supporting data privacy protection and policy hiding is proposed. A flexible access structure is designed in the scheme. LSSS matrix combined with policy hiding can better ensure the security of data access. At the same time, not only user revocation is supported in this scheme, but also it is efficient and lightweight. The computing and communication load of the terminal is reduced. Finally, the security and performance of the scheme are analyzed, and the feasibility of the scheme is analyzed through simulation experiments. In [4,5], an efficient access control scheme based on privacy protection is proposed. The characteristics of hash function and the structure of binary tree are used to limit the decision-making process of the model. A binary search tree based on hash function is used to protect the attributes of terminal members, so the risk of user privacy leakage is reduced. At the same time, this method is also applied to the server to effectively process requests from various terminals. In [6,7], a secure access control scheme based on attribute signcryption is proposed. Under the assumption of discrete logarithm theory, the attribute hiding and zero knowledge proof technology are used in this scheme, which can not only protect the privacy of terminal members, but also reduce the leakage of attributes in the process of data sharing. In addition, the server is used to partially decrypt the ciphertext resources. The computing tasks of the terminal members are effectively reduced.

An anonymous cloud assisted Internet of things access control scheme is proposed in [8]. In the scheme, the fine-grained access control combined with attribute encryption...
technology is realized. At the same time, a confusion strategy is proposed to fuzzy the user’s privacy information. The correctness of the scheme is verified by formal verification. In [9], a new cryptographic access control framework is proposed. The programme supports the establishment of multiple authority centres. A new security encryption strategy is adopted, which is bound with ciphertext to resist known attacks. Users no longer use private key signature verification, but adopt a more convenient attribute token. Although this method is convenient and lightweight, there is still a risk of token leakage. In [10,11], a flexible multi authority data storage scheme is proposed. This scheme does not need an authority center to distribute the key. At the same time, a series of attributes are used to realize flexible data storage, which completely eliminates the security risks caused by key distribution. In addition, the computing task of the terminal is transferred to the assistant node, which reduces the load of the terminal node. A ciphertext strategy for media cloud is proposed in [12,13]. Compared with other attribute based encryption schemes, this scheme has better performance. Legitimate users only need two hash operations when switching access to resources, which greatly reduces the calculation time. At the same time, the scheme also supports user revocation, which is easy to expand and maintain in later work. In [14], an access control scheme supporting attribute hiding is proposed. By hiding the attributes, the scheme can better protect the privacy information of terminal members. In addition, an attribute location mechanism is also proposed, which can help authorized terminals locate attribute information and decrypt resources. The final simulation comparison shows that the efficiency of this scheme is better.

In [15,16], a user and attribute revocable access control scheme is proposed. In the scheme, the revocation of the user or the user’s attributes is supported, and the terminal members cannot access the original resources after revocation. At the same time, in the scheme, users can add or reduce attributes according to their own needs, and the amount of calculation is small in this process. Through the security analysis of the scheme, the scheme can effectively resist known attacks. In [17], a fine-grained access control scheme based on attribute and blockchain is proposed. In this scheme, a cooperation mechanism is applied, which can authorize users in emergency, and this mechanism can be verified. The outsourcing method is adopted to build a trusted node to perform the main computing and communication tasks, and writes the information into the blockchain through transaction. A resource sharing scheme combining blockchain and ABE is proposed in [18]. In this scheme, data providers can set access policies for shared data ciphertext to achieve fine-grained access control. At the same time, the data demander communicates directly with the data provider, and the data provider can provide the key for the legitimate data demander. In addition, the keyword search function is also supported. The server locates resources and returns information according to the keywords provided by the data demander. In [19], a secure and efficient access control scheme is proposed. The encryption process of this scheme is fast and lightweight computing is realized by outsourcing the decryption process. The scheme has better performance.

In [20,21], an access control scheme for smart medicine is proposed. The scheme combines CP-ABE technology to realize the security protection of data and privacy. Improving the low efficiency and low security scheme makes it more suitable for the security protection of medical data. An access control scheme for Internet of things is proposed in [22]. In the scheme, the terminal device encrypts its own data and then uploads it to the server, which solves the problem of over authorization by the third party or the entrusted node. At the same time, the unauthorized operation of the application can be limited, so the privacy information of the terminal device can be protected. Finally, it is proved that the scheme is secure. An access control model in smart health application scenario is proposed in [23]. In this system, when the smart health record is encrypted, the attribute value of the access policy is hidden and only the attribute name is displayed, which well protects personal privacy. It uses a small number of bilinear pairs to complete the decryption of smart health records, which greatly improves the efficiency of decryption. In [24], a cross domain access control scheme for cloud sharing is proposed. Combined with blockchain technology, the scheme not only solves the problem of single point of failure, but also can trace the access records of the terminal. At the same time, by extending the traditional scheme, a cross domain cooperation mechanism is designed through smart contract, which can realize the cooperative operation of multiple trust institutions and generate decryption keys for users. The analysis shows that the scheme has good performance. In [25], a proactive dynamic secure data scheme is proposed. It uses attribute-based access control to protect the private information of financial users. In order to protect the integrity and security of data, the client is used as the core method to effectively avoid the impact of unexpected operation on the server. In addition, due to data access restrictions based on configuring user attributes, this model can continue to provide a high level of security.

An access control scheme based on blockchain smart contract is proposed in [26]. In this scheme, multiple smart contracts are designed, such as the master contract, to manage the access control of data among users. The authentication management contract is used to authenticate the identity of terminal members and store registration records. Intelligent detection contract is used to detect illegal behaviors in the system and punish users. In addition, the consumption of computing and communication energy can be reduced to a certain extent. In [27], an access control scheme for fog computing scenario is proposed. It aims to reduce the cost
of calculation and ensure the confidentiality of data. In this scheme, the fog device bears the main computational cost of the encryption and decryption stages. Therefore, the calculation cost of the sender and the receiver will be reduced, which greatly improves the efficiency of data exchange. At the same time, the user’s private key is generated through multi-authority, which enhances data security. In [28], a secure and efficient access control scheme using smart contract is proposed. Different from the previous attribute-based access control, this scheme carries out safe and efficient data sharing by setting up multiple smart contracts. The most important is the smart contract for access control, which completes the established security policy by setting the access rights of resources and verifying the identity information of terminal members. In addition, there is a judgment contract and a registration contract. Judgment contract is mainly to punish the violations in the process of system operation. The registration contract is used to manage the information of the terminal. In [29], a fine-grained access control scheme with decentralized capability is proposed. In this scheme, resources are stored on their own devices instead of other third-party large storage devices. At the same time, the access control of resources is based on the user’s identity. The management of user rights is realized through smart contract. Finally, the feasibility of the scheme is proved. In [30], a traceable access control protocol supporting emergency authorization is proposed. In the scheme, smart contracts are used to define some rules to deal with emergencies, and the duration of emergency visits is also regulated. In addition, patients can also restrict the distribution of permissions for personal health records.

By reading the above references, researchers have made a lot of contributions to data sharing and access control. At the same time, there are some shortcomings, such as the privacy leakage of terminal members, the lack of clear classification of shared resources, and the problem of user authority revoking. To solve these problems, we proposed a dynamic permission access control model based on privacy protection (PP-DPAC), and optimized it in terms of personal privacy information protection, lightweight and security. Through comparative analysis, the effect of this scheme is better.

3 Basic theory

For ease of understanding, the symbols and related descriptions used in this paper are shown in Table 1.

3.1 Bilinear mapping

In this section, we will introduce the basic knowledge of bilinear mapping used in this paper.

Let $G_1$ and $G_2$ be two groups on elliptic curve, where $G_1$ is an additive group and $G_2$ is a multiplicative group. They all have large prime order $q(q \geq 2^\ell + 1)$ satisfying the safety parameter $\ell$. Let $g_1$ is the generator of $G_1$, that means $G_1 = \langle g_1 \rangle$. It is difficult to solve the discrete logarithm problem of $G_1$ and $G_2$, $e$ is called admissible pairing, if $e : G_1 \times G_1 \rightarrow G_2$ satisfies the follow properties:

1. bilinearity: For any element $\mu, \nu \in G_1$ and element $a, b \in \mathbb{Z}_q^*$, $e(a\mu, b\nu) = e(\mu, \nu)^{ab}$ can always be calculated;
2. Non-degeneracy: For any element $\mu, \nu \in G_1$, there is always $e(\mu, \nu) \neq 1$;
3. Computability: For any two elements $\mu, \nu \in G_1$, $e(\mu, \nu)$ can always be calculated in polynomial time.

**Inference 1** For all $\mu_1, \mu_2, \nu \in G_1$, there is $e(\mu_1 + \mu_2, \nu) = e(\mu_1, \nu)e(\mu_2, \nu)$.

**Definition 1** Discrete Logarithm Problem (DLP). Given an equation $Y = aQ$, where $Y, Q \in G_1$ and $a < Q$. If $a$ and $Q$ are given, it is easy to calculate $Y$. But if $Y$ and $Q$ are given, it will be difficult to calculate $a$.

**Definition 2** Inverse Computational Diffie–Hellman (ICDH) Problem: The ICDH problem is given $g_1, ag_1$ and $abg_1$, for some $a, b \in \mathbb{Z}_q^*$ to compute $(ab/a)g_1$.

3.2 Lagrange interpolation theorem

Generally, If we know that function $y = f(x)$ passes through different $n + 1$ points $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n).$ We can...
Dynamic permission access control model… 195

construct a polynomial \( y = P_n(x) \) with the highest degree of \( n \). The polynomial passes through these \( n + 1 \) points. Therefore, it satisfies formula \( P_n(x_k) = y_k \), \( k = 0, 1, \ldots, n \).

So we can calculate the value \( P_n(\xi) \) at any point \( \xi \), where \( \xi \neq x_i \), \( i = 0, 1, 2, \ldots, n \). \( P_n(\xi) \) can be used as an approximation of the exact value \( f(\xi) \). We call this method the interpolation method, where \( P_n(\xi) = y_k \), \( k = 0, 1, \ldots, n \) is the interpolation condition. Interval \([a, b] \) is the minimum interval of \( x_i \), \( a = \min\{x_0, x_1, \ldots, x_n\}, b = \max\{x_0, x_1, \ldots, x_n\} \).

**Application form** Suppose there are \( n \) points \((x_0, y_0), (x_1, y_1), \ldots, (x_{n-1}, y_{n-1})\) in plane space. We can construct function \( f(x) \) through these \( n \) points. The implementation is shown below.

Let set \( D_n \) be a set of subscripts with respect to the point \((x, y)\), where \( D_n = \{0, 1, \ldots, n - 1\} \) and construct \( n \) polynomials \( p_j(x), j \in D_n \). For any \( k \in D_n \), there are \( p_k(x) \) and \( B_k = \{i \mid i \neq k, i \in D_n\} \), so that

\[
p_k(x) = \prod_{i \in B_k} \frac{x - x_i}{x_k - x_i}
\]

where \( p_k(x) \) is a polynomial of degree \( n - 1 \) and satisfies \( p_k(x_m) = 0 \) and \( p_k(x_x) = 1 \) for any \( m \in B_k \), so that \( L_n(x) = \sum_{j=0}^{n-1} y_j p_j(x) \). The interpolation polynomial \( L_n(x) \) of the above form is called Lagrange interpolation polynomial.

**Access control system model**

The main idea of the model are as follows: The resources stored in the shared database have different security levels. Terminal members have different levels of access rights. Only the terminal members meeting the access rights can decrypt the corresponding resources. In the model, terminal members are divided into two categories, one is data sharers, and the other is data acquirers. A terminal member can be either a data sharer or a data acquirer. Data sharers first set access rights according to the confidentiality level of resources. Then it calculates the encryption key according to the access rights and encrypts the resources to obtain the ciphertext. Finally, the ciphertext resources and the corresponding description information are uploaded to the resource sharing platform. The data requester first checks whether its attribute weight meets the access rights. Then it requests access and downloads ciphertext resources. Finally, it calculates the decryption key according to its attribute weight and decrypts the downloaded ciphertext resources. Data requesters can upgrade or revoke their attributes according to the access rights of the target resources. This method can not only flexibly and dynamically restrict resource access, but also make the resource access control between entities more secure and efficient. The dynamic permission access control model based on privacy protection is shown in Fig. 1.

**Certificate authority** (CA) Generate public/private key pairs for the resource storage service platform and terminal devices. At the same time, it authenticates the identity and attributes of terminal members, and distributes the corresponding attribute weights for each terminal.

**Resource storage service platform** (RSSP) Publish each terminal’s attribute sequence, identity and its public key, and provide a public display platform for terminals to publish information such as plaintext keywords for shared ciphertext resources, ciphertext information description, and ciphertext encryption attribute weights.

**Ciphertext database** (CD) Store ciphertext resource information shared by each terminal.

## 5 Access control protocol

### 5.1 Initialization

In this work, assuming that the information sharing network contains a certification authority CA and \( n \) terminal members. CA is mainly used to verify terminal identity and generate system parameters and system master keys. The set of \( n \) terminal members is denoted as \( U = \{u_1, u_2, \ldots, u_n\} \), and the corresponding identity set is \( ID = \{id_{u_1}, id_{u_2}, \ldots, id_{u_n}\} \). The sequence of constraint attributes for all access to network resources is \( Attr_seq = A_1 | A_2 | \ldots | A_i | A_j | \ldots | A_R \), where \( i < j, A_i < A_j(i, j, R \in N^*) \). The corresponding constraint attribute set is \( Attr_set = \{A_1, A_2, \ldots, A_R\} \). And the attribute sequence of the terminal member \( u_i \) is \( attr_seq_i = a_{u_{i,1}} | a_{u_{i,2}} | \ldots | a_{u_{i,n}}| (1 \leq i \leq n) \), and the corresponding ordered attribute set is \( attr_set_i = \{a_{u_{i,1}}, a_{u_{i,2}}, \ldots, a_{u_{i,j}}, \ldots, a_{u_{i,n}}\} \), where \( a_{u_{i,j}} < a_{u_{i,j+1}} \) \( Attr_set_i \subseteq Attr_set \). \( r \) denotes the number of attributes of terminal member \( u_i \).

Assuming \( G_1 \) and \( G_2 \) are an additive group and a multiplicative group on the elliptic curve of prime order \( q \), respectively. The discrete logarithm over \( G_1 \) and \( G_2 \) are difficult, \( g_1 \in G_1 \) is a generator of \( G_1 \). Parameter \( e : G_1 \times G_1 \rightarrow G_2 \) is a computable bilinear mapping. \( H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^* \), \( H_2 : G_1 \rightarrow \mathbb{Z}_q^* \) are two hash functions.

**KeyGen** \( KeyGen(1^l) \rightarrow (PK_E, SK_E) \): The CA can run \( KeyGen(1^l) \) to generate public/private key pairs \((SK_E, PK_E) \) for the entity, where \( SK_E \in \mathbb{Z}_q^* \) and \( PK_E = SK_E g_1 \).

The CA runs the \( KeyGen \) \((1^l) \) to obtain a public/private key pair \((SK_CA, PK_CA) \), where \( SK_CA \in \mathbb{Z}_q^* \) and \( PK_CA = SK_CA g_1 \). At the same time, CA runs \( KeyGen(1^l) \) to generate public key and private key for RSSP and each terminal member in the system respectively. Then CA distributes them through secure channel. Suppose the public/private key pair...
of RSSP is \((SK_{RSSP}, PK_{RSSP})\), where \(SK_{RSSP} \in \mathbb{Z}_q^*\), 
\(PK_{RSSP} = g^{SK_{RSSP}}\). The public/private key pair of the 
terminal member \(u_i \in U\) (1 ≤ \(i \leq n\)) is \((sk_{ui}, pk_{ui})\), where \(sk_{ui} \in \mathbb{Z}_q^*\), 
\(pk_{ui} = g^{sk_{ui}}\). The system parameters are 
\(params = (PK_{CA}, PK_{RSSP}, q, G_1, G_2, g, e, H_1, H_2)\).

5.2 Hidden attribute authentication

(1) CA broadcasts the attribute sequence set for accessing 
network resources and corresponding sequence numbers 
\([A_1, S_1], (A_2, S_2), \ldots, (A_R, S_R)\), where \(A_i (1 \leq i \leq R)\) represents attribute, \(S_i\) represents the serial number corresponding to the attribute \(A_i\).

(2) Each terminal user \(u_i (1 \leq i \leq n)\) with an ordered 
attribute set \(attr_{set_i} = \{a_{ui,1}, a_{ui,2}, \ldots, a_{ui,r}\}\), where \(a_{ui,j} < a_{ui,j+1} (1 \leq j < r)\), chooses a random positive 
integer \(s_{ui} \in \mathbb{Z}_q^*\) and calculates 
\(\vartheta_{i,0} = s_{ui} PK_{CA}\), \(\vartheta_{i,1} = s_{ui} a_{ui,1} g, \vartheta_{i,2} = s_{ui} a_{ui,2} g, \ldots, \vartheta_{i,r} = s_{ui} a_{ui,r} g, \vartheta_{i} = s_{ui} H_2(\vartheta_{i,1} || \vartheta_{i,2} || \ldots || \vartheta_{i,r}) PK_{CA}\). Then, \(u_i\) sends \([id_{ui}, pk_{ui}, ai, \vartheta_{i,0}, (\vartheta_{i,1}, S_1), (\vartheta_{i,2}, S_2), \ldots, (\vartheta_{i,r}, S_r)\] to CA.
(3) After receiving the messages \(\{id_{u_i}, pk_{u_i}, o_i, \vartheta_{i,0}, (\vartheta_{i,1}, S_1), (\vartheta_{i,2}, S_2), \ldots, (\vartheta_{i,r}, S_r)\}\), CA calculates \(\eta_i = SK_{CA}^{-1}o_i = s_u H_2(\vartheta_{i,1}||\vartheta_{i,2}||\cdots||\vartheta_{i,r})g_1\) and \(\psi_i = SK_{CA}^{-1}o_Ak_i = s_u g_1a_{u_i,k}(k=1,2,\ldots,r)\). Then, CA verifies the identity of \(u_i\) by the equation \(H(id_{u_i})\eta_i = ?H_2(\vartheta_{i,1}||\vartheta_{i,2}||\cdots||\vartheta_{i,r})pk_{u_i}\) and \(H_2(\psi_i ||\psi_{i'} ||\cdots||\psi_r) = ?H_2(\vartheta_{i,1}||\vartheta_{i,2}||\cdots||\vartheta_{i,r})\). If it holds, CA selects a random numbers \(i_{CA,k} \in \mathbb{Z}_q^* (1 \leq k \leq r)\) for each attribute \(a_{u_i,k}\), CA computes \(c_{i,k} = i_{CA,k}^2\psi_i\) and its signature \(\delta_i = SK_{CA}(i_{CA},a_{u_i,1} + i_{CA}a_{u_i,2} + \cdots + i_{CA}a_{u_i,r})g_1\). (Note that for any attributes \(a_{u_i,j}\) and \(a_{u_i,k}\) of different terminals \(u_i\) and \(u_l(i \neq l)\), if \(j = k\), then \(i_{CA,j} = i_{CA,k}\). Then, CA sends messages \(\{PK_{CA}, \delta_i, (\vartheta_{i,1},\vartheta_{i,2},\ldots,\vartheta_{i,r})\}\) to the register terminal \(u_l\).

(4) After receiving the messages \(\{PK_{CA}, \delta_i, (\vartheta_{i,1},\vartheta_{i,2},\ldots,\vartheta_{i,r})\}\) from CA, \(u_l(1 \leq i \leq n)\) calculates \(T_{i,1} = s_{u_i}^{-1}c_{i,1} = i_{CA,1}a_{u_i,1}g_1, T_{i,2} = s_{u_i}^{-1}c_{i,2} = i_{CA,2}a_{u_i,2}g_1, \ldots, T_{i,r} = s_{u_i}^{-1}c_{i,r} = i_{CA,r}a_{u_i,r}g_1\) and \(\mu_i = (T_{i,1} + T_{i,2} + \cdots + T_{i,r})\). Then, \(u_l\) verifies the identity of CA and attribute weight \(T_{i,k}\) of \(a_{u_i,k}(1 \leq k \leq r)\) by equation \(e(\delta_i, g_1) = e(\mu_i, PK_{CA})\). If it holds, \(u_l\) obtains the attribute weight \(T_{i,k}\) corresponding to each of its attribute \(a_{u_i,k}(1 \leq k \leq r)\). Each terminal member has successfully registered.

(5) Due to the service characteristics of RSSP and its direct connection with CA, it can obtain all the attributes \(\{A_1, A_2,\ldots, A_K\}\) of the system. Then, according to the above steps, RSSP can calculate all attribute weights \(T_{i,1} = i_{CA,1}A_1g_1, T_{i,2} = i_{CA,2}A_2g_1, \ldots, T_{i,r} = i_{CA,r}A_rg_1\).

(6) Finally, according to the messages \(\{id_{u_j}, pk_{u_j}, o_j, \vartheta_{j,0}, (\vartheta_{j,1}, S_1), (\vartheta_{j,2}, S_2), \ldots, (\vartheta_{j,r}, S_r)\}\) sent by \(u_j\), CA sends the information \(\{pk_{u_j}, S_1, S_2,\ldots, S_r\, j\}\) of each \(u_j\) to RSSP, where the attribute serial number \(S_1, S_2,\ldots, S_r\) of \(u_j\) corresponds to the network attribute serial number \(S_1, S_2,\ldots, S_r\).  

5.3 Calculation of access permissions for shared resources

Data sharer \(u_j(1 \leq j \leq n)\) sets corresponding access permissions according to the security level of shared resources. Only terminal members with the attribute set \(attr_{set,j} = \{a_{u_1,j}, a_{u_2,j},\ldots, a_{u_i,j},\ldots, a_{u_r,j}\}(j, t \in \mathbb{N}^*, t \leq r)\) can access the resource \(m_{u_j,i} \in M^* (M^* is the plaintext space). The calculation of resource access permissions is as follows:

(1) \(u_j\) randomly selects the encryption parameter \(\beta_{u_i,m} \in \mathbb{Z}_q^*\) and uses the encryption parameter to calculate the encryption key \(k_{u_j,m} = H_2(\beta_{u_i,m}g_1)\). Then \(u_j\) encrypts resource \(m_{u_j,i}\) to obtain ciphertext \(c_{i,m} = k_{u_j,m} \oplus m_{u_j,i}\) and sets the attribute weight according to the confidentiality of resource \(m_{u_j,i}\). Only the terminal member that meets the attribute weight can access and decrypt resource \(m_{u_j,i}\). Assume that access to resource \(m_{u_j,i}\) requires \(r\) different attribute weights. The attribute serial number corresponding to the \(r\) attribute weights is \((S_1, S_2,\ldots, S_r)\). \(u_j\) calculates \(h = \beta_{u_i,m}PK_{RSSP}, H_1(c_{i,m})\) and signature \(\sigma_{i,m} = sk_{u_j}^{-1}H_1(\text{keyword}_{d,m} || S_1 || S_2 || \ldots | | S_{j-1} || | | h || | | c_{i,m})\). Then \(u_j\) sends the message \(\{id_{u_j}, pk_{u_j}, (S_1, S_2,\ldots, S_{r-1}), h, \sigma_{i,m}, c_{i,m}, \text{keyword}_{d,m}, H_1(c_{i,m})\} to the RSSP.

(2) After receiving the message \(\{id_{u_j}, pk_{u_j}, (S_1, S_2,\ldots, S_{r-1}), h, \sigma_{i,m}, c_{i,m}, \text{keyword}_{d,m}, H_1(c_{i,m})\}\), it first calculates hash values \(H_1(c_{i,m})\) and \(e(\sigma_{i,m}, pk_{u_j}) = e(H_1(\text{keyword}_{d,m} || S_1 || S_2 || \ldots | | S_{j-1} || | | h || | | c_{i,m})\) to verify the integrity of ciphertext resources and the legitimacy of terminal member \(u_j\)’s identity respectively. If it is correct, RSSP calculates the encryption key \(k_{u_j,m} = H_2(\text{SK}_{RSSP}^{-1}h)\) and randomly selects \(t - 1\) random numbers \(b_1, b_2,\ldots, b_{t-1} \in \mathbb{Z}_q^*\) to construct the polynomial \(f(x) = b_1x^{t-1} + b_2x^{t-2} + \cdots + b_{t-1}x + k_{u_j,m}\). Then it inputs the hash value \(H_2(T_{i,1}), H_2(T_{i,2}),\ldots,H_2(T_{i,r})\) of the attribute weight corresponding to the attribute serial number to the polynomial \(f(x)\). \(f(x)\) outputs \(t\) function values \(\{f_{i,1}, f_{i,2},\ldots, f_{i,t}\}\). Finally, the RSSP publishes the information \(\{id_{u_j}, pk_{u_j}, f_{i,1}, f_{i,2}, S_{r-1},\ldots, f_{i,t}, S_{r-1}, \text{keyword}_{d,m}\}\) on the public information sharing platform, and the ciphertext \(c_{i,m}\) is stored in the ciphertext database CD.

5.4 Decryption and acquisition of resources

(1) The data acquirer \(u_j(1 \leq j \leq n)\) searches the ciphertext resource \(c_{i,m}\) and the attribute serial number \((S_{j,1}, S_{j,2},\ldots, S_{j,r})\) corresponding to the ciphertext resource \(c_{i,m}\) on the public information sharing platform according to the keyword \(\text{keyword}_{d,m}\). If the data acquirer \(u_j\) has the attribute \(a_{u_1,j}, a_{u_2,j},\ldots, a_{u_r,j}\) corresponding to the attributes serial number \((S_{j,1}, S_{j,2},\ldots, S_{j,r})\), \(u_j\) has the access right to access the resource. \(u_j\) calculates \(\sigma_{j,m} = sk_{u_j}^{-1}H_1(S_{j,1} || S_{j,2} || \ldots | | S_{j,r} || | | \text{keyword}_{d,m})g_1\) and sends the message \(\{id_{u_j}, pk_{u_j}, (S_{j,1}, S_{j,2},\ldots, S_{j,r}), \sigma_{j,m}, \text{keyword}_{d,m}\}\) to RSSP to apply for access to the resource.

(2) After receiving the message \(\{id_{u_j}, pk_{u_j}, (S_{j,1}, S_{j,2},\ldots, S_{j,r}), \sigma_{j,m}, \text{keyword}_{d,m}\}\) sent by \(u_j\), it will match the attribute serial number set \((S_{j,1}, S_{j,2},\ldots, S_{j,r})\) in the sent message with the serial number \((S_{j,1}, S_{j,2},\ldots, S_{j,r})\) \(t \leq r\) published on the information sharing platform (that is, whether \(u_j\) has the attribute access rights it claims). If it matches, RSSP calculates \(\phi_{j,m} = \)
If $u_j$ upgrade membership attributes, it can obtain the corresponding level of resource access permissions. Suppose the current attribute set of terminal member $u_j$ is $\text{attr set}_j = \{a_{u_j,1}, a_{u_j,2}, \ldots, a_{u_j,r}\}$, and it can only access low-level shared resources. The process of revoking the access of $u_j$ is as follows:

1. $u_j$ sends $\{\text{id}_{u_j}, pk_{u_j}, \alpha_j, \beta_{j,0}, (\beta_{j,r+1}, S_{r+1})\}$ to CA.

2. After receiving the messages $\{\text{id}_{u_j}, pk_{u_j}, \alpha_j, \beta_{j,0}, (\beta_{j,r+1}, S_{r+1})\}$, CA verifies the identity of $u_j$ by calculating whether $H_2(\beta_{j,r+1}) = \text{SK}_{CA}^{-1}\delta_j$ and the attribute weight $\text{sk}_{CA}(\delta_j, \chi_{j,r+1})$. If the verification is successful, CA sends $\{PK_{CA}, \delta_j, \chi_{j,r+1}\}$ to $u_j$.

3. After receiving the message $\{PK_{CA}, \delta_j, \chi_{j,r+1}\}$, $u_j$ calculates $\chi_{j,r+1} = \text{SK}_{CA}^{-1}\chi_{j,r+1} = \text{SK}_{CA}^{-1}(\text{id}_{u_j}, \text{sk}_{CA}(\delta_j, \chi_{j,r+1}) + 1)$ and verifies whether the identity of CA and the attribute weight hold. If the verification is successful, $u_j$ obtains the attribute weight $\text{sk}_{CA}(\delta_j, \chi_{j,r+1})$ and can only access low-level shared resources.

6.2 Permission revocation

When terminal members are punished, such as reduced trust or illegal operations, certain specific resource access rights may be cancelled. Suppose the current attribute set of terminal member $u_j$ is $\text{attr set}_j = \{a_{u_j,1}, a_{u_j,2}, \ldots, a_{u_j,r}\}$ and it can only access lower-level shared resources. The process of revoking attribute $a_{u_j,r}$ of $u_j$ is as follows:

1. CA broadcasts a notice. The notice is the attribute $a_{u_j,r}$ of the terminal member $u_j$ is revoked.

2. After receiving the notification, RSSP updates the information of $u_j$ in the information sharing platform, that is, cancels the $S_{r+1}$ item in the $u_j$ column.

3. CA selects a random numbers $\tilde{t}_{CA,r} \in \mathbb{Z}_q^{\beta_{CA,r}}$ for the attribute $a_{u_j,r}$ of each $u_i (1 \leq i \leq n, i \neq j)$, CA computes $\tilde{t}_{CA,r} = \tilde{t}_{CA,r} \beta_{j,r} (1 \leq i \leq n, i \neq j)$ and its signature $\tilde{s}_{CA} = SK_{CA}^{-1}\tilde{t}_{CA,r} + 1$. Then, CA broadcasts messages $\{PK_{CA}, \delta_{CA}, (\tilde{t}_{1,r}, \tilde{t}_{2,r}, \ldots, \tilde{t}_{j-1,r}, \tilde{t}_{j+1,r}, \ldots, \tilde{t}_{n,r})\}$ to all the register terminal $u_j$.

4. After receiving the messages $\{PK_{CA}, \delta_{CA}, (\tilde{t}_{1,r}, \tilde{t}_{2,r}, \ldots, \tilde{t}_{j-1,r}, \tilde{t}_{j+1,r}, \ldots, \tilde{t}_{n,r})\}$, CA verifies the identity of $u_j$ by equation $\text{sk}_{CA}(\tilde{t}_{j,r}, PK_{CA}) = e(\tilde{t}_{j,r}, PK_{CA})$. If it holds, $u_j$ obtains the attribute weight $\tilde{t}_{j,r}$ corresponding to its attribute $a_{u_j,r}$ and updates the previous attribute weight $\tilde{t}_{j,r}$ with $\tilde{t}_{j,r}$. At this time, $u_j$ cannot calculate the new attribute weight $\tilde{t}_{j,r}$, and $u_j$ can only access low-level shared resources.
Through the above authority update process, the access authority of terminal members to access certain shared resources can be dynamically upgraded or downgraded.

7 Correctness and security analysis

In this section, we discussed the PP-DPAC protocol. The first is the proof of the correctness of the PP-DPAC protocol, then the security of the PP-DPAC protocol is analyzed.

7.1 Correctness

The following theorem proves the correctness of PP-DPAC protocol.

**Theorem 1** If any terminal member \( u_j (1 \leq i \leq n) \) has a legal attribute sequence set \( \text{attr}_{r,\text{set}} = \{ a_{u,i}, a_{u,i+1}, \ldots, a_{u,n} \} \), it can satisfy the correctness of the equation \( H_1(id_{u_i})\eta_i = ?H_2(\theta_{i,1} \parallel \theta_{i,2} \parallel \cdots \parallel \theta_{i,r})pk_{u_i} \) and \( e(\delta_i, g_1) = e(\mu_i, PKCA) \), then complete the registration.

**Proof** Since \( \delta_i = SKCA(\mu_{CA},a_{u,i} + \mu_{CA},a_{u,i+1} + \cdots + \mu_{CA},a_{u,n})g_1 \), \( o_i = s_{u_i}H_2(\theta_{i,1} \parallel \theta_{i,2} \parallel \cdots \parallel \theta_{i,r})PKCA \), \( T_{i,r} = s_{u_i}a_{u,i}g_1 \), \( \chi_{i,k} = SKCA(\mu_{CA},a_{u,i},r)g_1 \), \( T_{i,r} = s_{u_i}a_{u,i}g_1 \), \( \mu_i = (T_{i,1} + T_{i,2} + \cdots + T_{i,r}) \) pairings, it is proved as follows:

\[
H_1(id_{u_i})\eta_i = H_1(id_{u_i})SKCA^{-1}o_i \\
P(i)CA = H_1(id_{u_i})SKCA^{-1}s_{u_i}H_2(\theta_{i,1} \parallel \theta_{i,2} \parallel \cdots \parallel \theta_{i,r})g_1 \\
= sk_{u_i}H_2(\theta_{i,1} \parallel \theta_{i,2} \parallel \cdots \parallel \theta_{i,r})pk_{u_i}e(\delta_i, g_1) \\
= e(SKCA(\mu_{CA},a_{u,i} + \mu_{CA},a_{u,i+1} + \cdots + \mu_{CA},a_{u,n})g_1 \parallel \mu_{CA},a_{u,i+1} + \cdots + \mu_{CA},a_{u,n})SKCA \\
= e((\mu_{CA},a_{u,i} + \mu_{CA},a_{u,i+1} + \cdots + \mu_{CA},a_{u,n})g_1, PKCA) \\
= e(T_{i,1} + T_{i,2} + \cdots + T_{i,r}, PKCA) \\
= e(\mu_i, PKCA)
\]

According to the above two equations, if terminal members have a legal set of attributes, they can verify successfully and complete registration.

**Theorem 2** If any terminal member \( u_j \) has a legal attribute weight set \( \{ T_{j,1}, T_{j,2}, \ldots, T_{j,r} \} \), it can satisfy the correctness of the equation \( e(\sigma_{j,m}, pk_{u_j}) = e(\phi_{j,m}, g_1) \) and the key \( k_{u_i,m} \). It can obtain the plaintext resource.

**Proof** Since \( \sigma_{j,m} = sk_{u_j}H_1(S_{j,1} \parallel S_{j,2} \parallel \cdots \parallel S_{j,r} \parallel \text{keyword}_{d,m}g_1 \), \( \phi_{j,m} = H_1(S_{j,1} \parallel S_{j,2} \parallel \cdots \parallel S_{j,r} \parallel \text{keyword}_{d,m}g_1 \), and according to the properties of the bilinear pairings, it is proved as follows:

\[
e(\sigma_{j,m}, pk_{u_j}) = e(sk_{u_j}H_1(S_{j,1} \parallel S_{j,2} \parallel \cdots \parallel S_{j,r} \parallel \text{keyword}_{d,m}g_1, pk_{u_j}) \\
= e(sk_{u_j}H_1(S_{j,1} \parallel S_{j,2} \parallel \cdots \parallel S_{j,r} \parallel \text{keyword}_{d,m}g_1, pk_{u_j})^{k_{u_j}} \\
= e(H_1(S_{j,1} \parallel S_{j,2} \parallel \cdots \parallel S_{j,r} \parallel \text{keyword}_{d,m}g_1, sk_{u_j}^{-1}pk_{u_j}) \\
= (\mu_i, PKCA) \\
= e(\phi_{j,m}, g_1)
\]

After the above equation is verified, the terminal member obtains \( (y_{u,k}, T_{j,k})(k = 1, 2, \ldots, r) \) from the RSSP, and \( u_j \) calculates the decryption key. Then \( u_j \) restores the \( (r-1) \) degree polynomial \( f(x) = b_{1,1}x^{r-1} + b_{2,1}x^{r-2} + \cdots + b_{1,1}x + k_{u,m} \) by using the polynomial \( g(x) = \sum_{j=1}^{r}y_{u,j} = \prod_{i=0}^{r-1}T_{j,(i)}^{-1}H_{i}(T_{j,(i)}) \) according to the Lagrange theorem. Since \( T_{j,k} = T_{j,k} = (k = 1, 2, \ldots, r) \) and \( y_{u,k} \) is the same, \( u_j \) can get \( g(0) = k_{u_m} \). So Theorem 2 is proved.

7.2 Security analysis

**Theorem 3** For any terminal member \( u_i (1 \leq i \leq n) \), if it has attribute \( a_{u,i} \), it can get the attribute weight \( T_{i,r} \) corresponding to the attribute \( a_{u,i} \).

**Proof** For terminal member \( u_i \) with attribute \( a_{u,i} \), it can calculate \( \theta_{i,0} = s_{u_i}PKCA \theta_{i,1} = s_{u_i}a_{u,i}g_1 \), \( \theta_{i,1}=s_{u_i}a_{u,i+1}g_1 \), \( \theta_{i,2}=s_{u_i}a_{u,i+2}g_1 \), \( \cdots \), \( \theta_{i,r}=s_{u_i}a_{u,n}g_1 \), \( o_i = s_{u_i}H_2(\theta_{i,1} \parallel \theta_{i,2} \parallel \cdots \parallel \theta_{i,r}) \) PKCA. After receiving the message \( \{ id_{u_i}, pk_{u_i}, o_i, \theta_{i,0}, \theta_{i,1}, \theta_{i,2}, \ldots, \theta_{i,r} \} \) from the terminal member \( u_i \), CA calculates \( \eta_i = SKCA^{1}_{CA} \theta_{i,1} = s_{u_i}H_2(\theta_{i,1} \parallel \theta_{i,2} \parallel \cdots \parallel \theta_{i,r})g_1 \), \( \psi_k = SKCA^{1}_{CA} \theta_{i,0} \), \( s_{u_i}g_1a_{u,k}(k = 1, 2, \ldots, r) \) and verifies the identity of \( u_i \) by the equation \( H_1(id_{u_i})\eta_i = ?H_2(\theta_{i,1} \parallel \theta_{i,2} \parallel \cdots \parallel \theta_{i,r})pk_{u_i} \), \( H_2(\theta_{i,1} \parallel \theta_{i,2} \parallel \cdots \parallel \theta_{i,r}) \). Then CA selects a random numbers \( i_{CA,k} \in \mathbb{Z}^n_1(1 \leq k \leq r) \) for each attribute \( a_{u,i,k} \) and calculates \( \chi_{i,k} = ic_{CA,k} \theta_{i,k} \). After receiving the messages \( \{ PKCA, \delta_i, \chi_{i,1}, \chi_{i,2}, \ldots, \chi_{i,r} \} \) from CA, \( u_i \) can obtain attribute weight \( T_{i,r} \) corresponding to the attribute \( a_{u,i} \) by calculating \( T_{i,r} = s_{u_i}^{-1} \chi_{i,r} \), \( ic_{CA,r}a_{u,i}g_1 \).

**Theorem 4** If the terminal member \( u_j (1 \leq j \leq n, i \neq j) \) does not have attribute \( a_{u,j,r} \), it cannot obtain the attribute weight \( T_{j,r} \) corresponding to the attribute \( a_{u,j,r} \).

**Proof** if the terminal member \( u_j \) wants to obtain the attribute weight \( T_{j,r} \), it needs to calculate the attribute weight \( T_{j,r} \) (Due to \( T_{j,r} = T_{i,r} \)). It can intercept the dialogue between...
CA and $u_i$ in network communication to obtain information such as $\chi_{i,r}$, $\theta_{i,r}$. Then $u_j$ tries to calculate $T_{i,r}$. But because $s_{u_i}$ is a private parameter of $u_i$, $u_j$ cannot calculate $T_{i,r}$. Assume that $u_j$ can calculate $T_{i,r}$ from $\chi_{i,r}$ and $\theta_{i,r}$. Here is $\chi_{i,r} = cACA_k \theta_{i,r}$, $T_{i,r} = s_{u_i} - \chi_{i,r} = cACA_k a_{u_i,r} g_1$, $\theta_{i,r} = s_{u_i} a_{u_i,r} g_1$. Let $a g_1 = \theta_{i,k}, a b g_1 = \chi_{i,k}$. $b = cACA_k$, the terminal member $u_j$ constructs algorithm $A$ to calculate $cACA_k$ and $T_{i,r} = cACA_r a_{u_i,r} g_1 = a_{u_i,r} b g_1$. Solving $\theta_i$ is equivalent to solving the ICDH problem. The ICDH problem is a difficult assumption, so $u_j$ cannot calculate attribute weight $T_{i,r}$ through $\chi_{i,r}$ and $\theta_{i,r}$. The above proof shows that only legal terminals have legal attributes to obtain corresponding attribute weights, and illegal terminals or illegal attributes cannot obtain correct attribute weights.

\[ \mathbf{Theorem 5} \quad \text{Any terminal member } u_j (1 \leq j \leq n, i \neq j) \text{ with an attribute set } att_r t_{i,j} = \{a_{u_{i,j}}, a_{u_{i,j}}, ..., a_{u_{j,j}}\} (j, r \in N^*, r < R) \text{ can decrypt the resources of higher confidentiality level by upgrading to obtain attributes } a_{u_{j,j+1}}. \]

\[ \mathbf{Proof} \quad \text{According to Theorem 3, if terminal member } u_j (1 \leq j \leq n, i \neq j) \text{ has an attribute set } att_r t_{i,j} = \{a_{u_{i,j}}, a_{u_{i,j}}, ..., a_{u_{j,j}}\} (j, r \in N^*, r < R), \text{ it can obtain an attribute weight set } (T_{ij,1}, T_{ij,2}, ..., T_{ij,r}). \text{ Then combined with the attribute sequence set obtained from the information sharing platform, } \text{r points } (y_{u_{i,j}}, T_{ij,i}) (i = 1, 2, ..., r) \text{ can be formed. Then} \]

\[ u_j \text{ restores the } (r - 1) \text{ degree polynomial } f(x) = b_{ij,1}x^{r-1} + b_{ij,2}x^{r-2} + ... + b_{ij,r}x \text{ by using the polynomial } g(x) = \sum_{i=1}^{r} y_{u_{i,j}} \prod_{\sigma \neq 1, \sigma \neq i}^{r} \frac{x - T_{ij,\sigma}}{T_{ij,\sigma} - T_{ij,i}} \text{ (} t = r) \text{ according to the Lagrange interpolation theorem. That is, } g(x) = f(x), \text{ u_j calculates the decryption key } k(0) = k_{u_{i,j}}. \text{ In the same way, terminal members with attributes can restore r degree polynomial } f(x) = b_{ij,1}x^{r} + b_{ij,2}x^{r-1} + b_{ij,3}x^{r-2} + ... + b_{ij,r}x + k_{u_{i,j}} \text{ after upgrading. Then } u_j \text{ calculates the decryption key } k(0) = k_{u_{i,j}} \text{ to decrypt higher-level resources according to } g(x) = \sum_{i=1}^{r} y_{u_{i,j}} \prod_{\sigma \neq 1, \sigma \neq i}^{r} \frac{x - T_{ij,\sigma}}{T_{ij,\sigma} - T_{ij,i}} \text{ (} t = r + 1). \]

\[ \mathbf{Theorem 6} \quad \text{Any terminal member, if it is downgraded, u_j cannot decrypt the resources of the corresponding sensitivity level before the downgrade.} \]

\[ \mathbf{Proof} \quad \text{if terminal member } u_j (1 \leq j \leq n, i \neq j) \text{ has an attribute set } att_r t_{i,j} = \{a_{u_{i,j}}, a_{u_{i,j}}, ..., a_{u_{j,j}}\} (j, r \in N^*, r < R), \text{ it can obtain an attribute weight set (} T_{ij,1}, T_{ij,2}, ..., T_{ij,r}) \text{. Then combined with the attribute sequence set obtained from the information sharing platform, } \text{r points } (y_{u_{i,j}}, T_{ij,i}) (i = 1, 2, ..., r) \text{ can be formed. Then according to the Lagrange interpolation theorem } g(x) = \sum_{i=1}^{r} y_{u_{i,j}} \prod_{\sigma \neq 1, \sigma \neq i}^{r} \frac{x - T_{ij,\sigma}}{T_{ij,\sigma} - T_{ij,i}} \text{ (} t = r), \text{ u_j can calculate the decryption key } x = g(0). \text{ When the level of } u_j \text{ decreases, his attribute authority parameter changes to } (T_{ij,1}, T_{ij,2}, ..., T_{ij,r}). \text{ The last point formed by the combination will become } (y_{u_{i,j}}, T_{ij,r}) \text{ different from the previous (} y_{u_{i,j}}, T_{ij,r} \text{). According to the Lagrange interpolation theorem } g(x) = \sum_{i=1}^{r} y_{u_{i,j}} \prod_{\sigma \neq 1, \sigma \neq i}^{r} \frac{x - H_{2}(T_{ij,\sigma})}{H_{2}(T_{ij,\sigma}) - H_{2}(T_{ij,i})} \text{ (} t = r), \text{ the calculated decryption key is } x = g(0). \text{ Because of } x \neq x, \text{ the degraded terminal members cannot decrypt the resources of the original sensitivity level.} \]

\[ \mathbf{Theorem 7} \quad \text{For different members to collude with different attribute combinations, this model can resist by registering and calculating permissions. In other words, this model can resist collusion attacks.} \]

\[ \mathbf{Proof} \quad \text{For this model, the attribute serial number set } (S_{j,1}, S_{j,3}, S_{j,4}, ..., S_{j,t}) \text{ of } u_j \text{ will be sent directly to RSSP by CA during the registration process. Suppose } u_j \text{ wants to access the resource whose attribute serial number set is } (S_{j,1}, S_{j,2}, S_{j,3}, ..., S_{j,t}). \text{ It needs to form the attribute sequence set (} S_{j,1}, S_{j,2}, S_{j,3}, ..., S_{j,t}) \text{ together with the conspirators. Then } u_j \text{ calculates } \sigma_{j,m} = s_{k_{u_j}^{-1}} H_{1}(S_{j,1}) S_{j,2} S_{j,3} ... S_{j,t} \text{ together with } \text{the platform } (S_{j,1}, S_{j,2}, S_{j,3}, ..., S_{j,t}) \text{ in the sent message with the platform (} S_{j,1}, S_{j,2}, S_{j,3}, ..., S_{j,t}) \text{ (} t \leq r) \text{ published on the information sharing platform. If it matches, RSSP calculates } \phi_{j,m} = H_{1}(S_{j,1}) S_{j,2} S_{j,3} ... S_{j,t} \text{ and verifies the identity of } u_j \text{ by calculating whether equation } e(\sigma_{j,m}, p_{ka}) = e(\phi_{j,m}, g_1) \text{ holds. If the equation holds, RSSP will provide the ciphertext } c_{i,m} \text{ 's link corresponding to the keyword } \text{keyword}_{i,m} \text{ to } u_j. \text{ However, the actual value calculated by the RSSP is } \phi_{j,m} = H_{1}(S_{j,1}) S_{j,2} S_{j,3} ... S_{j,t} \text{. Since } \phi_{j,m} \neq \phi_{j,m}, e(\sigma_{j,m}, p_{ka}) 
eq e(\phi_{j,m}, g_1), \text{ u_j cannot get the ciphertext link. In other words, this model can resist collusion attacks.} \]

\[ \text{Anti-man-in-the-middle attack} \quad \text{Analysis of anti-man-in-the-middle attacks will be discussed in two parts. During the authentication phase, adversary } A \text{ can obtain messages } (id_{u_i}, p_{ka}, \alpha_i, \theta_{i,0}, (\theta_{1,1}, S_1), (\theta_{1,2}, S_2), ..., (\theta_{i,r}, S_i)) \text{ and } \{ PK_{CA}, \delta_i, (\chi_{i,1}, \chi_{i,2}, ..., \chi_{i,r}) \} \text{ on the common channel. According to Theorem 4, because } s_{u_i} \text{ is a private parameter of } u_i. \text{ At the same time, it cannot be cracked to get } \text{ic}_{CA,k}. \text{ u_j cannot calculate } T_{i,r}. \text{ In the resource decryption stage, } A \text{ can obtain the ciphertext resource link on the public channel and download the ciphertext } c_{i,m}. \text{ According to Theorem 6, } A \text{ has no attribute weight } T_{i,r}, \text{ so the key } x = g(0) \text{ cannot be recovered by constructing polynomial } g(x) = \sum_{i=1}^{r} y_{u_{i,j}} \prod_{\sigma \neq 1, \sigma \neq i}^{r} \frac{x - H_{2}(T_{ij,\sigma})}{H_{2}(T_{ij,\sigma}) - H_{2}(T_{ij,i})}. \text{ Therefore, this protocol can resist man-in-the-middle attacks.} \]
Table 2  Security features of four models

| Models          | Policy update | Anti-middleman attack | Hide attribute authentication | Anti-collusion attacks |
|-----------------|---------------|------------------------|-------------------------------|------------------------|
| Zhang et al. [34] | No            | Yes                    | No                            | Yes                    |
| Liu et al. [32] | No            | Yes                    | No                            | Yes                    |
| Gao et al. [33] | No            | Yes                    | No                            | No                     |
| Guo et al. [31] | Yes           | Yes                    | No                            | Yes                    |
| Ours            | Yes           | Yes                    | Yes                           | Yes                    |

Table 3  Execution time of each algorithm

| The algorithm                                      | Execution time (ms) |
|----------------------------------------------------|---------------------|
| Modular inverse operation ($T_{inv}$)              | $T_{inv} \approx 0.0042$ |
| Multiplication operation ($T_{mul}$)              | $T_{mul} \approx 0.0011$ |
| Exponentiation operation ($T_{exp}$)              | $T_{exp} \approx 6.6432$ |
| Elliptic curve point addition ($T_{pa-ecc}$)      | $T_{pa-ecc} \approx 0.003$ |
| Elliptic curve point multiplication ($T_{sm-ecc}$) | $T_{sm-ecc} \approx 0.0036$ |
| Hash operation ($T_h$)                             | $T_h \approx 0.0001$ |
| Bilinear pairing ($T_{bp}$)                        | $T_{bp} \approx 4.3183$ |
| Bilinear pairing point addition ($T_{pa-bp}$)      | $T_{pa-bp} \approx 0.014$ |
| Bilinear pairing scalar multiplication ($T_{sm-bp}$)| $T_{sm-bp} \approx 0.2038$ |

8 Performance analysis

Performance analysis is an important aspect of evaluating the efficiency of the model. In this section, we comprehensively evaluate our model in terms of security features, time complexity and computational consumption. In addition, according to the information provided in literature [31], we compare the models of literature [31–34] with our model, and the results show that our model is more efficient.

In terms of security features, we compare this model with the other four models as shown in Table 2. Hidden attribute authentication is a unique security feature of this model. The identity and attribute privacy of terminal members are protected, and the security of the system is improved. In addition, this model also has great advantages in the other three security features.

In terms of time costs, we use the Java programming language and the Java-based encryption library JPBC library (the library version is JPBC-2.0.0). The configuration of the computer is the processor is Intel(R) Core(TM) 2 i5-7500 3.4Ghz, running Windows 10 operating system. On this basis, through a large number of tests, we obtained the time data of various operations, as shown in Table 3. In terms of operation, compared with bilinear operation and exponentiation operation, addition operation and multiplication operation consume very short time, which is negligible in performance analysis.

Suppose $r$ represents the size of the terminal attribute set, $n$ represents the number of access tree nodes, $|l|$ represents the number of rows of the matrix, $|c|$ represents the number of columns of the matrix, $t$ represents the size of the attribute set required by the access policy, $|k|$ represents the number of revoked users. Based on this, we establish a calculation complexity analysis table, as shown in Table 4.

In order to facilitate quantitative analysis of the computational time consumption of the five models, suppose the number of access tree nodes is $n = 10$. The number of rows and columns of the matrix is $|l| = |c| = 5$. The number of revoked users is $|k| = 0$. Based on this, we compare and analyze the three different stages of the five models, as shown in Figs. 2, 3, and 4.

It can be seen from Fig. 2 that in the keyGen stage, our model consumes the least computational time. Followed by the model of Gao et al. [33], the model of Zhang et al. [34], and the model of Guo et al. [31]. The scheme of Liu et al. [32] consumes the most computational time. Among the five models, the model of Liu et al. [32], the model of Guo et al. [31], and the model of Zhang et al. [34] have a faster increase in computing time consumption as the attributes of terminal members increase, and they are not suitable for large-scale attribute application scenarios.
Table 4: Computational complexity of our model and the models in the other four protocols

| Models              | keyGen                  | Encrypt                                      | Decrypt                                      |
|---------------------|-------------------------|----------------------------------------------|----------------------------------------------|
| Zhang et al. [34]   | \((2 + r)T_{\text{exp}} + T_{\text{mul}}\) | \((2 + 3 | l |)T_{\text{exp}} + (1 + 2 | l |)T_{\text{mul}}\) | \(rT_{\text{exp}} + rT_{\text{mul}} + (1 + 2r)T_{\text{hp}}\) |
| Liu et al. [32]     | \((7 + r)T_{\text{exp}} + 2T_{\text{mul}}\) | \((3 + 3 | l | + 4 | k |)T_{\text{exp}} + (1 + 2 | l | + | k |)T_{\text{mul}}\) | \((2 + 2r + 2 | k |)T_{\text{exp}} + (2 | k | + 2r)T_{\text{mul}} + (1 + 2r + 2 | k |)T_{\text{hp}}\) |
| Gao et al. [33]     | \((1 + | l |)T_{\text{exp}}\) | \((2 + 1 | l | + | c |)T_{\text{exp}} + (2 + 1 | l | + | c |)T_{\text{mul}}\) | \(rT_{\text{mul}} + (1 + r)T_{\text{hp}}\) |
| Guo et al. [31]     | \((5 + r)T_{\text{exp}} + 2T_{\text{mul}}\) | \((4 + | l | + | c |)T_{\text{exp}} + (1 + | l | + | c |)T_{\text{mul}}\) | \((1 + 2r)T_{\text{exp}} + 2T_{\text{mul}} + 3T_{\text{hp}}\) |
| Ours                | \(2(r + 1)T_{\text{pa-ec}} + rT_{\text{inv}} + 2T_{\text{hp}} + (r + 1)T_{\text{mul}} + T_{\text{h}}\) | \(2T_{\text{pa-ec}} + T_{\text{inv}} + T_{\text{mul}} + 3T_{\text{h}}\) | \((r + 1)T_{\text{mul}} + T_{\text{inv}} + T_{\text{pa-ec}} + 4T_{\text{h}}\) |

As can be seen from Fig. 3, in the encryption phase, the calculation time consumption of the five schemes is independent of the number of attributes of terminal members. The model of Guo et al. [31] consumes the most computational time. Followed by the model of Gao et al. [33], the model of Liu et al. [32], and the model of Zhang et al. [34]. Among them, Liu et al. [32]’s model and Zhang et al. [34]’s model consume almost the same calculation time. Our model consumes the least computational time.

It can be seen from Fig. 4 that in the decryption stage, the model of Liu et al. [32] consumes the most computational time. Followed by the model of Zhang et al. [34], the model of Guo et al. [31], and the model of Gao et al. [33]. Our model consumes the least computational time.

9 Conclusion

In order to solve the problem of privacy leakage in access control, improve the security of the data-sharing system. Based on the analysis of current research results and existing problems of access control, a dynamic permission access control model based on privacy protection is proposed in this paper. Firstly, a hidden attribute authentication method is proposed. The identity information of terminal members can be hidden, and the attribute information can also be hidden. The personal privacy of users is greatly protected. Meanwhile, a dynamic, flexible and fine-grained access policy is proposed, which allows users to access resources with different sensitivity levels through upgrading or downgrading. In addition, a...
dual authentication mechanism is proposed. Terminal members need to be authenticated first, then calculate the correct key with their own attributes, finally decrypt the resource with the key. Under this mechanism, collusion attacks can be resisted. Finally, the correctness and security of the model are proved, and the performance of the model is analyzed. The results show that this model has higher security and better performance.

Acknowledgements This work is supported by National Natural Science Foundation of China under Grant (Nos. 61772477, 61971380, U1804263 and 62072037), and the Key Technologies R&D Program of Henan Province (Nos. 212102210089, 212102210171, 212102210075), and the Key scientific research project plans of higher education institutions in Henan Province (Grant No. 21zx014).

Funding The authors have not disclosed any funding.

Declarations

Conflict of interest The authors have not disclosed any competing interests.

References

1. Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2019). A novel attribute-based access control scheme using blockchain for IoT. *IEEE Access*, 7, 38431–38441.
2. Zhang, Q., Zhu, L., Li, Y., Ma, Z., Yuan, J., Zheng, J., & Ai, S. (2021). A group key agreement protocol for intelligent internet of things system. *International Journal of Intelligent Systems*, 37, 1–24. https://doi.org/10.1002/int.22644.
3. Zhong, H., Zhu, W., Xu, Y., & Cui, J. (2018). Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage. *Soft Computing*, 22(1), 243–251.
4. Xu, Y., Zeng, Q., Wang, G., Zhang, C., Ren, J., & Zhang, Y. (2020). An efficient privacy-enhanced attribute-based access control mechanism. *Concurrency and Computation: Practice and Experience*, 32(5), e5556.
5. Ma, Y., Shen, M., Zhao, Y., Li, Z., Tong, X., Zhang, Q., & Wang, Z. (2021). Opponent portrait for multiagent reinforcement learning in competitive environment. *International Journal of Intelligent Systems*, 36, 1–14. https://doi.org/10.1002/int.22594.
6. Xu, Q., Tan, C., Fan, Z., Zhu, W., Xiao, Y., & Cheng, F. (2018). Secure multi-authority data access control scheme in cloud storage system based on attribute-based signcryption. *IEEE Access*, 6, 34051–34074.
7. Zhang, Q., Zhu, L., Wang, R., Li, J., Yuan, J., Liang, T., & Zheng, J. (2021). Group key agreement protocol among terminals of the intelligent information system for mobile edge computing. *International Journal of Intelligent Systems*, 2021, 1–20. https://doi.org/10.1002/int.22544.
8. Nasiraei, H., & Ashouri-Talouki, M. (2020). Anonymous decentralized attribute-based access control for cloud-assisted IoT. *Future Generation Computer Systems*, 110, 45–56.
9. Zhu, Y., Yu, R., Ma, D., & Chu, W. C. (2019). Cryptographic attribute-based access control (ABAC) for secure decision making of dynamic policy with multiauthority attribute tokens. *IEEE Transactions on Reliability*, 68(4), 1330–1346.
10. Sandor, V. K., Lin, Y., Li, X., Lin, F., & Zhang, S. (2019). Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage. *Journal of Network and Computer Applications*, 129, 25–36.
11. Li, Y., Yao, S., Zhang, R., & Yang, C. (2021). Analyzing host security using D-S evidence theory and multisource information fusion. *International Journal of Intelligent Systems*, 36, 1053–1068. https://doi.org/10.1002/int.22330.
12. Li, H., Deng, L., Yang, C., & Liu, J. (2020). An enhanced media ciphertext-policy attribute-based encryption algorithm on media cloud. *International Journal of Distributed Sensor Networks*, 16(2), 1550147720908196.
13. Zhang, Q., Li, Y., Wang, R., Liu, L., Tan, Y. -a., & Hu, J. (2021). Data security sharing model based on privacy protection for blockchain-enabled industrial Internet of Things. *International Journal of Intelligent Systems*, 36, 94–111. https://doi.org/10.1002/int.22293.
14. Hao, J., Huang, C., Ni, J., Rong, H., Xian, M., & Shen, X. S. (2019). Fine-grained data access control with attribute-hiding policy for cloud-based IoT. *Computer Networks*, 153, 1–10.
15. Imine, Y., Lounis, A., & Bouabdallah, A. (2018). Revocable attribute-based access control in multi-authority systems. *Journal of Network and Computer Applications*, 122, 61–76.
16. Zhang, N., Xue, J., Ma, Y., Zhang, R., Liang, T., & Tan, Y.-A. (2021). Hybrid sequence-based Android malware detection using natural language processing. *International Journal of Intelligent Systems*, 36, 5770–5784. https://doi.org/10.1002/int.22529.
17. Zhang, Y., Li, B., Liu, B., Wu, J., Wang, Y., & Yang, X. (2020). An attribute-based collaborative access control scheme using blockchain for IoT devices. *Electronics*, 9(2), 285.
18. Wang, S., Zhang, Y., & Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access*, 6, 38437–38450.
19. De, S. J., & Ruij, S. (2020). Efficient decentralized attribute access control for mobile clouds. *IEEE Transactions on Cloud Computing*, 8(1), 124–137.
20. Rana, S., & Mishra, D. (2020). Efficient and secure attribute based access control architecture for smart healthcare. *Journal of Medical Systems*, 44(5), 1–11.
21. Li, Y., Wang, X., Shi, Z., Zhang, R., Xue, J., & Wang, Z. (2021). Boosting training for PDF malware classifier via active learning. *International Journal of Intelligent Systems*, 37, 1–19. https://doi.org/10.1002/int.22451.
22. Yan, H., Wang, Y., Jia, C., Li, J., Xiang, Y., & Pedrycz, W. (2019). IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT. *Future Generation Computer Systems*, 95, 344–353.
23. Zhang, Y., Zheng, D., & Deng, R. H. (2018). Security and privacy in smart health: Efficient policy-hiding attribute-based access control. *IEEE Internet of Things Journal*, 5(3), 2130–2145.
24. Qin, X., Huang, Y., Yang, Z., & Li, X. (2021). A Blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. *Journal of Systems Architecture*, 112, 101854.
25. Qiu, M., Gai, K., Thuraisingham, B., Tao, L., & Zhao, H. (2018). Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. *Future Generation Computer Systems*, 80, 421–429.
26. Sultana, T., Almogren, A., Akbar, M., Zauri, M., Ullah, I., & Javaid, N. (2020). Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. *Applied Sciences*, 10(2), 488.
27. Wang, Q., Lv, G., & Sun, X. (2019). Distributed access control with outsourced computation in fog computing. In *2019 Chinese control and decision conference (CCDC)* (pp. 2446–2450). IEEE.
28. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*, 6(2), 1594–1605.
29. Xu, R., Chen, Y., Blasch, E., & Chen, G. (2018). Blendcac: A blockchain-enabled decentralized capability-based access control for iots. In 2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData) (pp. 1027–1034). IEEE.

30. Rajput, A. R., Li, Q., Ahvanooey, M. T., & Masood, I. (2019). EACMS: Emergency access control management system for personal health record based on blockchain. *IEEE Access*, 7, 84304–84317.

31. Guo, L., Yang, X., & Yau, W. C. (2021). TABE-DAC: Efficient traceable attribute-based encryption scheme with dynamic access control based on blockchain. *IEEE Access*, 9, 8479–8490.

32. Liu, Z., Xu, J., Liu, Y., & Wang, B. (2019). Updatable ciphertext-policy attribute-based encryption scheme with traceability and revocability. *IEEE Access*, 7, 66832–66844.

33. Gao, S., Piao, G., Zhu, J., Ma, X., & Ma, J. (2020). TrustAccess: A trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain. *IEEE Transactions on Vehicular Technology*, 69(6), 5784–5798.

34. Zhang, Y., He, D., & Choo, K. K. R. (2018). BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT. *Wireless Communications and Mobile Computing, 2018*, 2783658. https://doi.org/10.1155/2018/2783658.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Qikun Zhang received the Ph.D. degree in computer science and technology from Beijing Institute of Technology, P.R. China, in 2013. He is currently an assistant professor at Computer and Communication Engineering in Zhengzhou University of Light Industry, Zhengzhou, China. His research includes information security and cryptography.

Liang Zhu is a graduate student at the School of Computer and Communication Engineering in Zhengzhou University of Light Industry, Zhengzhou, China. His research includes information security and cryptography.

Kunyuan Zhao is a graduate student at the School of Computer and Communication Engineering in Zhengzhou University of Light Industry, Zhengzhou, China. His research includes information security and cryptography.

Yimeng Wu received the Master degree in Computing (Knowledge Management) from Dublin Institute of Technology, Ireland, in 2012. She is currently a lecturer at School of architecture and environmental engineering in Zhengzhou Technical College, Zhengzhou, China. Her research includes information system management and knowledge management.

Baohua Jin received the Masters degree in computer science and technology from Huazhong University of Science and Technology, P.R. China, in 2003. He is a professor at the School of Computer and Communication Engineering in Zhengzhou University of Light Industry, Zhengzhou, China. His current research topics include computer engineering and applications, information communication and processing.
Jianyong Li received his M.S. degree in Computer Science and Technology from Huazhong University of Science and Technology, P.R. China in 2001. He is currently a professor in College of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou, China. His research interest includes artificial intelligence and network control.

Yinghui Meng received the M.S. and Ph.D. degrees in computer science and technology from Northeastern University in 2010 and 2014, respectively. He is an assistant professor with the School of Computer and Communication Engineering. His current research interest includes localization problem for wireless sensor networks.

Sikang Hu received the Ph.D. degree in computer science and technology from Beijing Institute of Technology, P.R. China, in 2009. He is currently a lecturer at Beijing Institute of Technology, Beijing, China. His research includes information security and software engineering.