Hindawi
Advances in Multimedia
Volume 2023, Article ID 9807598, 1 page
https://doi.org/10.1155/2023/9807598

Retraction

Retracted: A New Attribute Encryption Anonymity Algorithm in Cloud Computing Environment

Advances in Multimedia

Received 15 August 2023; Accepted 15 August 2023; Published 16 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] C. Zhao and Y. Chen, "A New Attribute Encryption Anonymity Algorithm in Cloud Computing Environment," *Advances in Multimedia*, vol. 2022, Article ID 8786035, 10 pages, 2022.

Hindawi
Advances in Multimedia
Volume 2022, Article ID 8786035, 10 pages
https://doi.org/10.1155/2022/8786035

Research Article

A New Attribute Encryption Anonymity Algorithm in Cloud Computing Environment

Cuirong Zhao and Yan Chen

Anhui Wenda University of Information Engineering, Hefei 231201, Anhui, China

Correspondence should be addressed to Yan Chen; chen12345202204@163.com

Received 26 May 2022; Accepted 29 June 2022; Published 21 July 2022

Academic Editor: Qiangyi Li

In order to solve the security problem of privacy information exposed by plaintext access strategy in cloud computing environment, this paper proposes a new attribute encryption anonymity algorithm which can be hidden and updated. The algorithm proposed in this paper hides the access policy attribute information through a randomized technology, which can support full hiding of the policy, and the prevention and control are more flexible. The experimental results show that, compared with the previous decryption algorithms, under the premise of the same attributes, the encryption time decreases in a few seconds. When the number of attributes is 1, the encryption time decreases by 10 s, and when the number of attributes is 10, the encryption time decreases by about 100 s, and the efficiency is greatly improved.

1. Introduction

While the network era brings many conveniences to social production and life, it also virtually brings human society into the information age. Information has become an important resource for the development of all fields of today's society. To some extent, various activities in modern society rely more and more on information resources. However, with the realization of information resource sharing, hidden dangers of information security begin to appear. Some criminals will even use illegal means to spy on the information of individuals, enterprises, and even the government in order to obtain more useful information. Even if the owner of information and data hides the identification information that can identify an individual before sharing the data, the risk of privacy disclosure will also increase. Therefore, how to ensure that the privacy information in the data is not disclosed in the process of data release is the focus of this study. Therefore, in order to protect the privacy of data information, this study proposes a new attribute encryption anonymity algorithm that can be hidden and updated. Compared with the traditional decryption algorithm, this algorithm has further improved its efficiency and security.

2. Literature Review

Data anonymization is the main technology to realize privacy protection. After making some changes to the privacy information of the original data, the attacker cannot infer a specific individual, so as to realize the protection of personal privacy. Anonymous operation methods mainly include suppression, generalization, anatomization, slicing, and disassociation. Among them, generalization is the most common anonymization method. Its essence is to replace the original attribute value with a wider range of fuzzy values, so as to realize the fuzzy replacement of data without violating the original semantics. Although the generalization operation will reduce the data accuracy, it fully realizes the role of protecting privacy [1].

Aiming at the problem of privacy protection in the process of data publishing, new data publishing principles and privacy protection algorithms have been proposed. Bouchaala et al. proposed the k-anonymity model, which divides the records in the original data into multiple equivalent groups. After anonymizing the data, some attribute values of several records belonging to the same equivalent group are the same, and then the data are published with

relatively low accuracy after anonymization, so as to solve the problem of privacy disclosure caused by link attack [2]. Aiming at the shortcomings of k-anonymity model, Zhang, Z. proposed ℓ–diversity model with constraints on sensitive attributes to resist possible homogeneous attacks and background knowledge attacks [3]. The model adds constraints on the basis of k-anonymity. Each equivalence group contains at least ℓ different sensitive attribute values, which makes the attacker infer that the confidence of an individual's sensitive information is up to $1/\ell$. In addition, the t-closeness model proposed by Sarma et al. requires data anonymity, so that the distribution of sensitive attribute values contained in each equivalence group is close to that in the original data, and the difference between the two distributions cannot exceed m [4]. Invariance model requires that, after data generalization, each equivalence group contains at least m records, and the data records in all equivalence groups must have different sensitive attribute values. Although many improved models have been proposed, k-anonymity model is still the most widely studied anonymous model. It is one of the effective methods to prevent privacy disclosure caused by link attack and has been highly concerned by the majority of researchers [5].

Li et al. proposed attribute encryption of key policy as a deformation of traditional attribute encryption algorithm. The access structure of the algorithm is designed based on monotonic structure; Mike proposes an algorithm that prohibits the cooperation of all parties. The ultimate goal is to realize the attribute encryption algorithm with anticollusion key strategy. The algorithm uses the tree infrastructure to create an access strategy when encrypting data. At the same time, the algorithm adopts the linear secret sharing scheme and the idea of monotonous traversal of items to establish an attribute encryption algorithm [6]. In order to ensure the security of the distributed algorithm and store the data on the untrusted server, Mike proposed another improved algorithm of attribute encryption, attribute encryption of ciphertext strategy. In this algorithm, the key generation algorithm uses the user's attribute set to generate the decryption key. Each ciphertext contains an access policy. The access control is based on the tree structure of "and" gate and "or" gate as the policy prototype of the algorithm [7]. If the user wants to decrypt, he needs to check whether the access structure in the ciphertext matches his own attribute set. At the same time, the algorithm adopts a novel attribute key randomization technology to realize anticollusion. In addition, the feasibility of the algorithm is similar to the role-based access control algorithm; that is, if a data owner wants to encrypt information, they need to arrange a threshold access structure for its attributes while encoding information. The access structure is used to encode information, and its ultimate goal is that people who access the structure can access the data in the algorithm. The drawback is that its security proof is based on the general group model. In order to improve the efficiency of encryption and decryption, a new attribute encryption algorithm is proposed, which reduces the amount of computation by providing faster encryption/decryption algorithm and shortening the ciphertext size. However, in the standard model, its security proves that it can only achieve selective security under the deterministic bilinear Diffie-Hellman assumption. A more secure attribute encryption of ciphertext strategy is constructed. This algorithm can achieve strong security under three static assumptions. The disadvantage is that the algorithm involves complex order groups, and the efficiency needs to be improved [8].

3. Attribute Encryption Algorithm with Hidden and Updatable Policy

3.1. Attribute Based Encryption of Hidden Access Policy. This section will give the HP-CP-ABE solution in the cloud environment. In order to reduce the consumption of user decryption calculation, a permission verification stage is added before decryption operation. This stage is to check whether the decryption user is legally authorized, and the computational complexity of this stage is far less than that of a decryption operation.

Abe has always been the best when it comes to safe sharing of data. However, these policies only focus on the security of data and do not care about the protection of user privacy. In some applications, access to permissions may contain sensitive information about the owner or user of the information. For example, a patient may want to share his or her medical record (PHR) with some doctors and family members, but he or she may not want others to know about his or her condition. If the patient encrypts the PHR using the traditional ABE program, even if the malicious user cannot obtain the content of the PHR, the user's personal information can be obtained, as shown in Figure 1. Since the access rules include "heart attack" and "DC hospital," a malicious user can predict that the owner's data will have a heart attack and receive treatment at the DC hospital [9].

In order to design a secure data sharing scheme suitable for cloud environment, the following problems need to be solved: how to protect the privacy of users while ensuring the confidentiality of data and how to design a fast authority verification mechanism to verify whether users have decryption authority and help users decrypt quickly when hiding access policies. The model of how to reduce the length of the private key, meet the resource constrained environment, and facilitate storage is shown in Figure 2.

The attribute based encryption system of the hidden access policy of ciphertext policy in the cloud environment consists of the four following parts, cloud server, authority center, data owner, and data user, as shown in Figure 2.

The scheme consists of the four following algorithms: system initialization algorithm, private key generation algorithm, encryption algorithm, and decryption algorithm [10].

System initialization (setup): take global attribute set U and security parameter K as the input of the algorithm to obtain public parameter PK and system master key MK.

Keygen: take the public parameter PK, master key MK, and user attribute set $L \subset U$ as the input of the algorithm to obtain the user's private key SK_L.

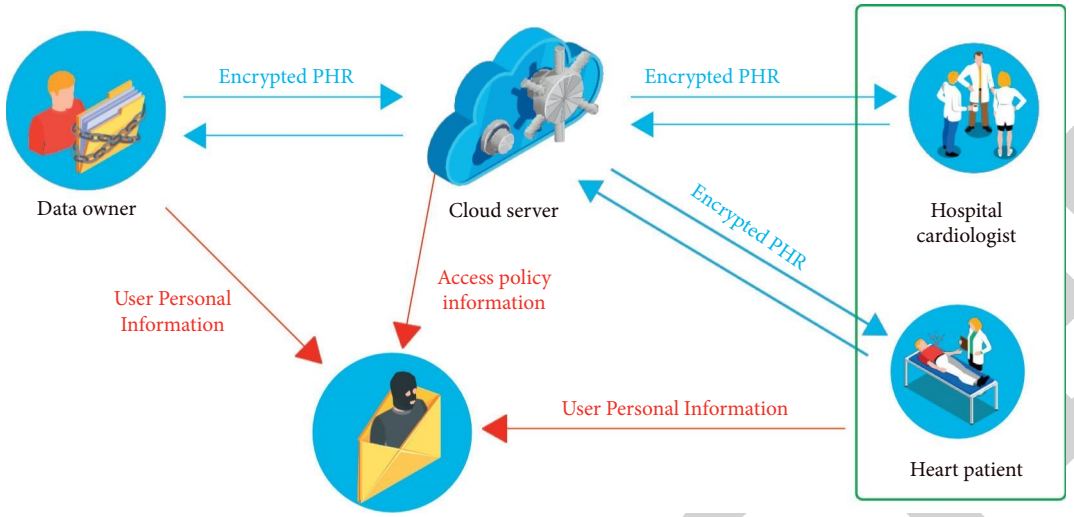

Figure 1: Traditional CP-ABE information disclosure model.

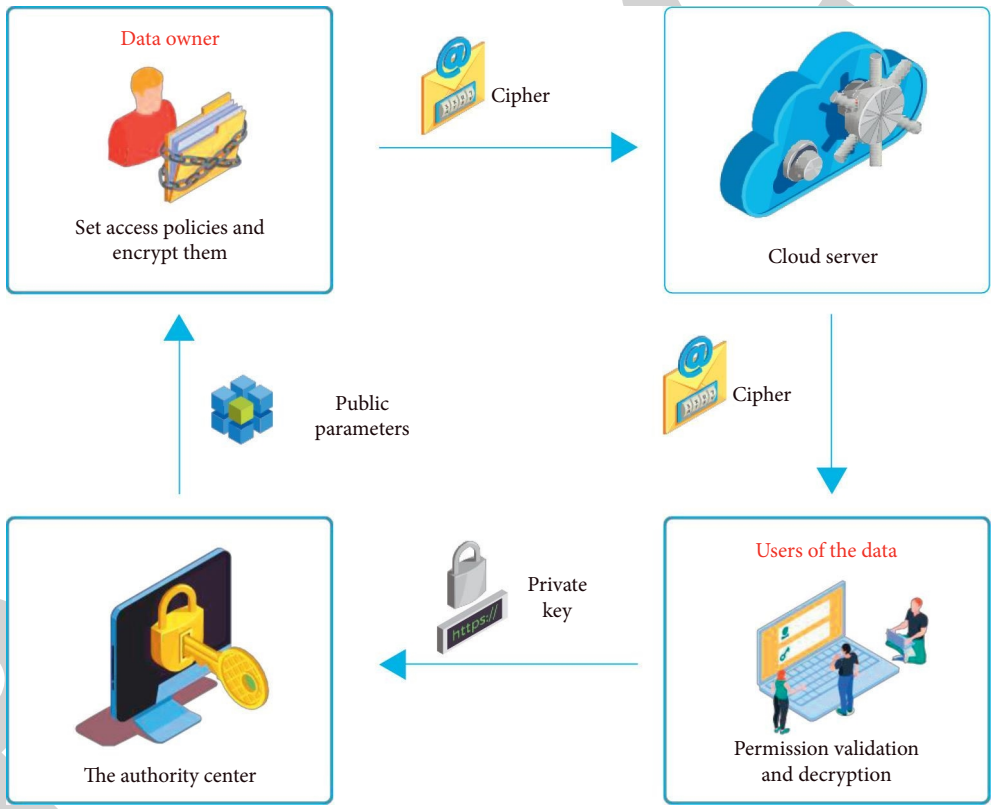

Figure 2: HP-CP-ABE solution model in cloud environment.

Encryption: take plaintext message M, system public parameter PK, and access policy W as algorithm input to obtain ciphertext CT_W.

Decryption: the decryption algorithm includes two stages: permission verification stage and decryption stage. Enter the system public key PK and private key SK_L, and the algorithm runs authority verification to check whether the decrypted user attribute set meets the secret access policy. If the test passes, the decryption phase is carried out and message M is output; otherwise, the algorithm aborts [11].

3.2. Basic Scheme. System setup is as follows: let g be a random generator of group G, and then select randomly, as shown in the following formula:

$$\begin{aligned} &u, w, h_o, h_1, \ldots, h_n \in G \\ &z_1, z_2, z_3, a_{ij} \in Z_p \end{aligned}. \tag{1}$$

We have that $i \in [1, n]$, $j \in [1, k_i]$, and the next calculation is as shown in the following formula:

$$\begin{cases} y_1 = g^{z_1} \\ y_2 = g^{z_2} \\ y_3 = g^{z_3} \\ A = e(u, y_1) \end{cases}. \tag{2}$$

The generation of public parameter PK and master key MK is as follows:

$$PK = \langle g, \omega, h_0, h_1, h_2, \ldots, h_n, y_1, y_2, y_3, A \rangle, \tag{3}$$

$$MK = \langle u, z_1, z_2, z_3, \{a_{i,j}\}_{i \in [1,n], j \in [1,k_i]} \rangle. \tag{4}$$

Private key generation (keygen) is as follows: enter the user's attribute set, as shown in the following formula:

$$L = \{L_1, L_2, \ldots, L_n\}. \tag{5}$$

Then calculate as shown in the following formula:

$$k_i = h_0^{t_i} \cdot h_i^{a_{i,j}}. \tag{6}$$

It should be noted here that $\sum_{i=1}^{n} t_i = 1$. Finally, $r_1, r_2 \in Z_p$ is randomly selected and calculated as shown in the following formula:

$$\begin{cases} sk_{1,i} = k_i^{r_1} \\ sk_2 = g^{r_1 z_1 z_2 + r_2 z_1 z_3} \\ sk_3 = g^{r_1 z_1} \\ sk_4 = g^{r_2 z_1} \\ sk_5 = u w^{r_2} \end{cases}. \tag{7}$$

Then, consider the following:

$$SK_L = \langle \{sk_1\}_{i \in [1,n]}, sk_2, sk_3, sk_4, sk_5 \rangle. \tag{8}$$

Encryption is as follows: the data owner formulates an access policy, as shown in the following formula:

$$W = \{W_1, W_2, ..., W_n\}. \tag{9}$$

We have that $W_i \in Att_i$; then select the random value $s_{1,i}, s_{2,i} \in Z_p$, where $i \in [1, n]$, and then $s_1 = \sum_{i=1}^{n} s_{1,i}, s_2 = \sum_{i=1}^{n} s_{2,i}$. Finally, if the attribute meets $v_{i,j} \in W_i$, then calculate $C_{i,j} = h_0^{s_{1,i}} h_1^{a_{i,j} s_1} y_2^{s_{2,i}}$. Otherwise, select a random element from group G, and C_3 can be expressed as follows:

$$C_3 = \{C_{i,j}\}_{(1 \le i \le n, a \le j \le k_i)}. \tag{10}$$

According to the above formula, we have

$$CT = \{C_1, C_2, C_3, C_4, C_5\}. \tag{11}$$

Decryption is as follows: the user enters his own private key SK_L. If its attribute list L meets the access policy, it can be decrypted correctly; otherwise, the algorithm will abort. The decryption process is shown in the following formula:

$$M = \frac{C_5}{\prod_{i=1}^{n} e(sk_{1,i}, C_1) \cdot e(sk_5, C_1) \cdot e(sk_2, C_2) / \prod_{i=1, v_{i,j} \in W_i}^{n} e(C_{i,j}, sk_3) \cdot e(C_4, sk_3).} \tag{12}$$

3.3. Improvement Scheme. There are many improvements in this scheme; for example, the length of private key and ciphertext is too large, the consumption of decryption operation is too high, and there is no authority verification. On this basis, this section will give an improvement scheme to solve the above problems.

System setup is as follows: the algorithm randomly selects a generator g of group G and then selects $u, w, h_o, h_1, \ldots, h_n, t_1, t_2, t_3 \in_R G$, as shown in the following formula:

$$\begin{cases} A_1 = g^{t_1} \\ A_2 = g^{t_2} \\ A_3 = g^{t_3} \\ A = e(u, A_1) \end{cases}. \tag{13}$$

Select $a_{i,j} \in Z_p$ randomly for each attribute in U and calculate $T_{i,j} = h_i^{a_{i,j}}$, as shown in the following formula:

$$\begin{cases} i \in [1, n] \\ j \in [1, k_i] \end{cases}. \tag{14}$$

The generation of public parameter PK and master key MK is shown in the following formulas:

$$PK = \langle g, w, h_0, A_1, A_2, A_3, A, \{T_{i,j}\}_{i \in [1,n], j \in [1,k_i]} \rangle, \tag{15}$$

$$MK = \langle u, t_1, t_2, t_3, \{a_{i,j}\}_{i \in [1,n], j \in [1,k_i]} \rangle. \tag{16}$$

Keygen is as follows: this algorithm is divided into two stages. The first stage is to generate a unique label for the user, and the second stage is to generate a private key for the user.

To generate the private key, the user submits its property set $L = \{L_1, L_2, ..., L_n\}$. Then the authority center performs the following operations: first, run the label generation algorithm and define a function, as shown in the following formula:

$$H_n(L) = h_0 \prod_{i=1}^{n} T_{i,j} = h_0 \prod_{i=1}^{n} h^{a_{i,j}}. \tag{17}$$

Then select $r_1, r_2 \in Z_p$ randomly and calculate as follows:

$$\begin{cases} D_0 = K_L = \omega_k \\ D_1 = uH_n(L)^{r_1} w^{r_2} \\ D_2 = g^{r_1 t_1 t_2 + r_2 t_1 t_3} \\ D_3 = g^{r_1 t_1} \\ D_4 = g^{r_2 t_1} \end{cases}. \tag{18}$$

Then, we have

$$SK_L = \langle D_0, D_1, D_2, D_3, D_4 \rangle. \tag{19}$$

Encryption is as follows: the data owner formulates an access policy $W = \{W_1, W_2, \ldots, W_n\}$. The maximum number of users supported by the access policy is T, and then the random integer $r \in Z_p$ is selected. For an authorized user, the data owner converts the attribute of u_i into a binary array and sends r to the authority center. Next, the authority center runs the label generation algorithm to return $K_{u_i}^r$ to the data owner. The final calculation is shown in the following formula:

$$\begin{cases} C_0 = A_1^r \\ C_1 = A_1^{s_1} \\ C_3 = \left\{C_{i,j}\right\}_{v_{i,j} \in W} = \left\{h_0^{s_1} T_{i,j}^{s_1} A_2^{s_{2,i}}\right\} \\ C_4 = w^{s_1} A_3^{s_2} \\ C_5 = A^{s_1} \cdot M \\ C_i^{\bullet} = e\left(A_1, K_{u_i}^r\right) \\ C_i^n = m_i \oplus C_i^{\bullet} \end{cases}. \tag{20}$$

Then, we have

$$CT = \langle \{C_1, C_2, C_3, C_4, C_5\}, \{C_i^{\bullet}, C_i^n\}_{i \in [1,t]} \rangle = \langle CT_1, CT_2 \rangle. \tag{21}$$

Decryption is as follows: this algorithm consists of two stages. First, the user's permission must be verified, and then the ciphertext can be decrypted. The specific operation is as follows.

First, calculate as follows:

$$m_k = e(D_0, C_0) \oplus C_k^{\bullet}. \tag{22}$$

Consider the following calculation:

$$M = \frac{C_5}{e(D_1, C_1) \cdot e(D_2, C_2) / e\left(D_3, \prod_{i=1,(i,j) \in m_k}^{n} C_{i,j}\right) \cdot e(D_4, C_4).} \tag{23}$$

As can be seen from Figures 3–6, the scheme in this paper should be more efficient in terms of time consumption in the stages of private key generation, ciphertext generation, authority verification, and decryption, especially in the stages of authority verification and decryption. This is extremely beneficial to the efficient decryption of users [12].

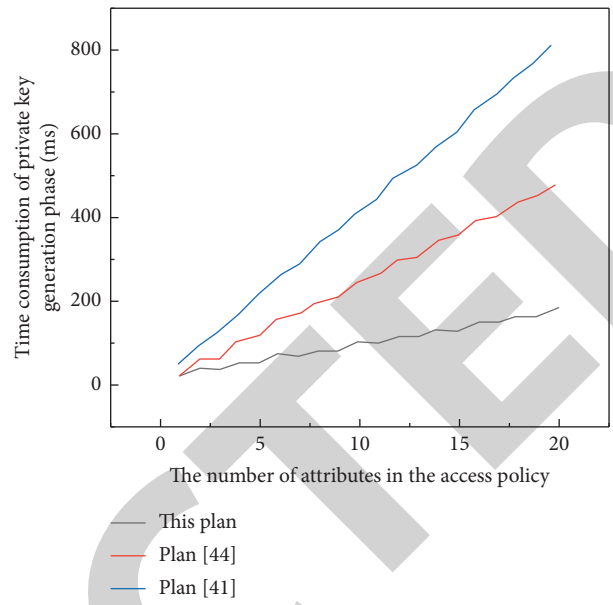

Figure 3: Time consumption of private key generation algorithm.

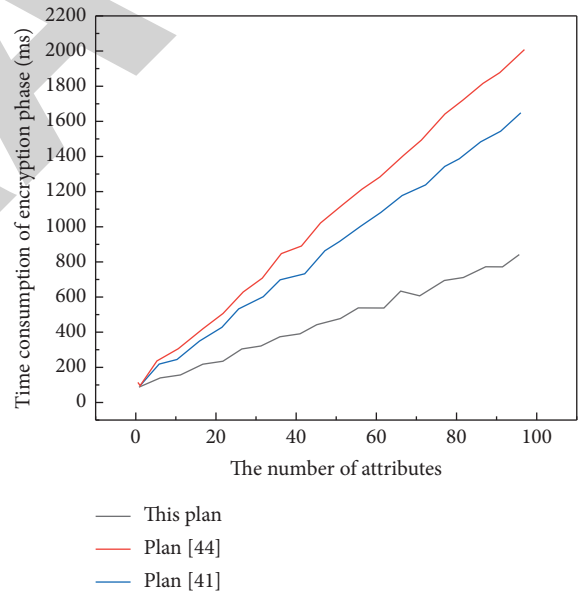

Figure 4: Time consumption of encryption algorithm.

This chapter first gives the preliminary design of an HP-CP-ABE scheme under prime order group and then extends the scheme. Compared with the existing schemes, the extended scheme has obvious advantages in the length of private key, the amount of computation required for authority verification, and the amount of bilinear pair computation required for decryption. Finally, it is proved that the extended scheme is IND-sCP-CPA safe under the deterministic n-BDHE hypothesis and D-linear hypothesis.

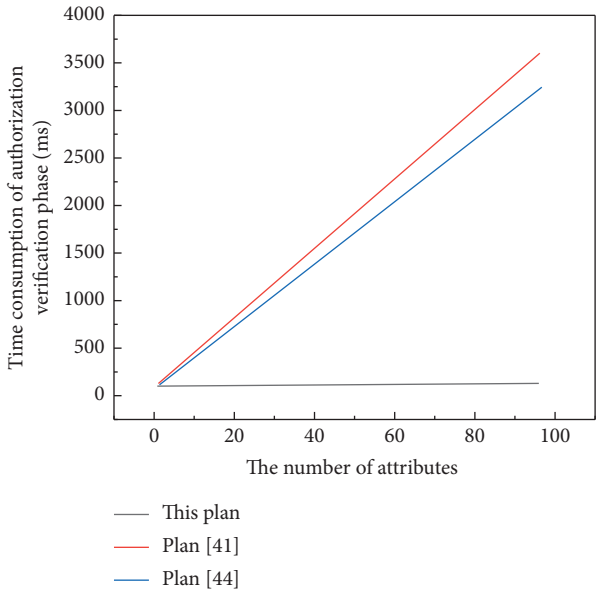

Figure 5: Time consumption of authority verification.

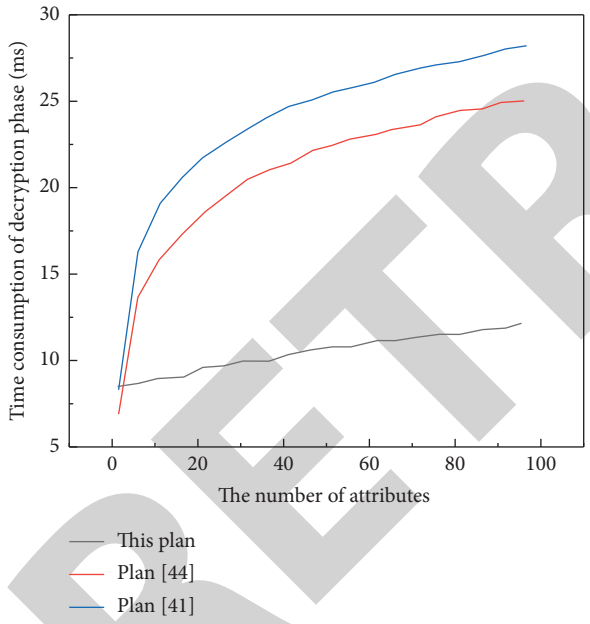

Figure 6: Time consumption of decryption algorithm.

4. Policy Hiding and Verifiable Attribute Encryption Algorithm

4.1. Algorithm Model. In smart medicine, if the medical staff (data owner) actively changes the encryption method (access policy) in order to obtain benefits, resulting in the leakage of patient (data user) information, it is necessary to verify whether the access structure in the ciphertext has been tampered with. In addition, in the existing attribute encryption algorithms, the access structure in the ciphertext stored on the cloud server exists in the form of plaintext or only hides part of the attribute information, so it directly exposes the patient's attribute information. Therefore, in order to solve the above problems, this paper constructs an attribute encryption algorithm supporting policy hiding and policy verification [13]. As shown in Figure 7, this paper shows an algorithm model diagram of a policy concealable and verifiable attribute encryption algorithm, which mainly includes five entities: private key generation center, cloud server, data owner, auditor, and data user.

Private Key Generation Center. The private key generation center is a trusted source. It is responsible for unrestricted public access to algorithms and key generators. When a user registers a file with a private manufacturer, the manufacturer reassigns the user a personal identity based on the behavior.

ECS. ECS is an honest but curious server provider, which is responsible for storing the ciphertext of the data owner. At the same time, ECS can also obtain additional sensitive information from this process [14].

Data Owner. The data owner owns the plaintext message and then sends the plaintext message to the auditor in the form of ciphertext. The data owner defines the access structure and encrypts its health data under the structure. In addition, the data owner needs to generate additional information for the auditor to check the authenticity of the strategy.

Auditor. The auditor is a trusted group, which is mainly responsible for checking whether the access structure in the ciphertext transmitted by the data owner is consistent with the predefined access policy. At the same time, due to the lack of private key information, the auditor cannot decrypt the ciphertext.

Data Users. Data users are groups that can access plaintext information. Therefore, the data user can obtain the corresponding ciphertext when sending a request to the ECS, but the data user can recover the message if and only if the data user has the authorization attribute. Otherwise, decryption fails [15].

When users want to access the ciphertext CT files stored on ECS, they can directly download them to the encrypted CT. In traditional attribute encryption algorithms, the input format of plaintext can be directly represented as character attributes of user data. Therefore, decryption can only be achieved when the user behavior set satisfies the entry criteria. However, in this algorithm, the behavior embedded in the template is hidden, so not all data users can know whether their process satisfies the incoming template. However, at the model hiding point of this algorithm, only legitimate users can make accurate decisions [16].

4.2. System Performance Analysis

User Privacy Security. In the algorithm in this chapter, the attribute mapping function ρ can be restored correctly only when the user attribute set meets the specified access policy. Otherwise, if irrelevant attribute sets are input into algorithm 2 in this chapter, the calculation will return a random value instead of the correct line number, and the next

algorithm 3 cannot recover the correct attribute mapping function, so as to effectively resist dictionary attack. Therefore, adversary A cannot obtain any sensitive information about attributes from the access structure with (M, ACF) in the ciphertext; that is, ACF-Check algorithm cannot increase the advantage of adversary A to break through the algorithm, so the algorithm in this chapter can protect the privacy and security of users [17].

Specifically, Table 1 gives the comparison table of symbol meanings involved in the algorithm in this paper. This algorithm sets the bit size of cyclic group G_1, G_2, G_T to 5121024 and 3072 bits, respectively.

Figure 8 shows the encryption time efficiency analysis diagram of the attribute encryption algorithm whose strategy can be hidden and verified. From this diagram, it can be intuitively seen that the time consumption of the encryption process in the two algorithms increases linearly with the increase of the number of attributes. At the same time, it can also be concluded that, on the premise of the same number of attributes, the algorithm in this paper has obvious advantages compared with the traditional algorithm [18].

Figure 9 shows the decryption time efficiency analysis diagram of the attribute encryption algorithm whose strategy can be hidden and verified. Similarly, the time consumption of the two algorithms increases linearly with the increase of the number of attributes. On the premise of the same number of attributes, the decryption algorithm in this chapter reduces the calculation time of symmetric operation compared with the decryption algorithm of the traditional algorithm, so the algorithm in this chapter also has some advantages.

The algorithm proposed in this paper has the advantages of highly expressive access structure, fully hidden policy, and ensuring the authenticity of access policy on prime order bilinear groups. Compared with other related works, the algorithm in this paper is more suitable for solving the problem of data privacy disclosure caused by the intentional change of access policy by the data owner, so as to realize the operability in practical application [19].

4.3. Result Discussion. As an extension of cloud computing, cloud storage has the advantages of resource sharing, low management cost, and scalability. Therefore, it can provide users with efficient and fast storage and computing services. Electronic medical system can help patients obtain, manage, and share their health data, which helps to predict a variety of diseases and improve the quality of medical services. With the continuous expansion of the existing medical data scale, the development of e-medicine based on cloud storage is becoming more and more rapid [20]. However, some cloud security problems also follow, such as data confidentiality and flexible access control. As a cryptographic primitive, attribute encryption can solve the fine-grained access control of health data, which effectively solves the above problems, so it is more suitable for electronic medical treatment. The existing attribute encryption algorithms for e-medicine have achieved a series of research results, but they still face some new challenges in access control, such as policy privacy disclosure, dynamic policy update, and illegal policy change. Specifically, the access policy in plaintext may expose the privacy information in the access policy. The real-time sharing of data needs a flexible access control encryption. The user's malicious change of policy requires a third party to verify the authenticity of the access policy [21].

The research focus of this paper is to design a new algorithm supporting privacy protection and dynamic sharing, which is an attribute encryption algorithm of ciphertext strategy applied to realize policy full hiding and flexible data sharing in e-medicine. In this algorithm, policy full hiding is realized by randomizing the attribute information in the access structure. In the recovery process, the attribute mapping function is recovered by using the positioning mechanism of Bloom filter [22]. In addition, the data user generates the conversion key for dynamically changing the access policy for the personal health file cloud, so as to outsource it to the personal health file cloud to update the ciphertext. Finally, based on the assumption of deterministic q-order bilinear Diffie-Hellman problem, it is proved that the algorithm is safe. An attribute encryption algorithm with full policy hiding and verification is proposed, which ensures full policy hiding and policy authenticity in e-medicine. In addition, a third-party "auditor" is introduced to check whether the access policy is tampered with before and after encryption. Then, the algorithm is proved to be selective and secure under the deterministic parallel bilinear Diffie-Hellman assumption. Performance analysis shows that the proposed algorithm has certain practical value for electronic medical system [23].

Modern society is in a period of rapid development of information and intelligence, which not only makes life convenient and fast but also brings new problems. The leakage of personal privacy information has become unprecedentedly common. The vast majority of people have been harassed by marketing, telephone and e-mail, and even online fraud. This also makes people realize the importance of protecting personal privacy information. How to ensure not only the confidentiality of information but also the privacy of users has become the focus of cryptographers' research [24]. For this purpose, this paper proposes HP-CP-ABE scheme and its extended research scheme through attribute based encryption scheme as follows.

In order to improve decryption decisions and reduce user inaccuracy, an authorization authentication mechanism is introduced; the number of input private keys is constant, which is not only convenient for storage but also suitable for limited resources; the performance of the process is determined by simulation. The results show that the process performs well in the decryption and approval process. Finally, conceptual stability and anonymity are demonstrated based on the determinant n-DBHE theory and D-linearity assumption, with the expansion of the study of encryption the hidden policy control behavior. Following the jury's decision, the HP-CP-ABE protocol was developed. In the process of hiding both access and posting tags, comparison with appropriate policies shows that these policies do not lose their effectiveness when conscious of protecting consumer

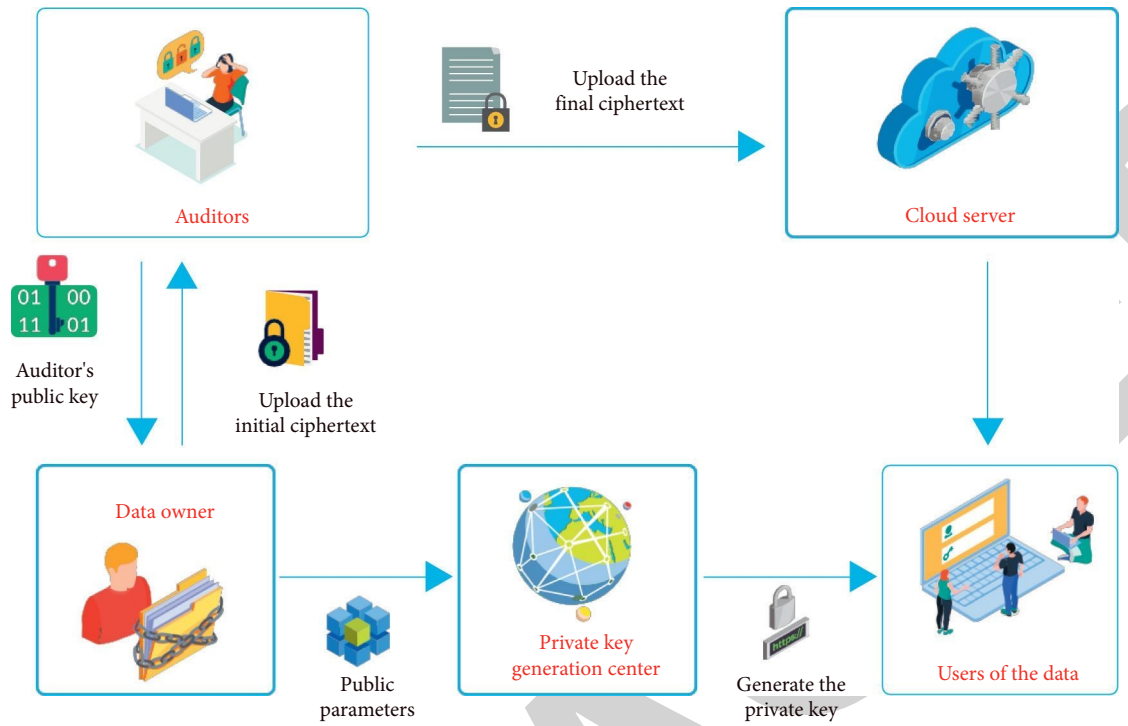

Figure 7: Attribute encryption algorithm model with hidden and verifiable policy.

Table 1: Comparison of symbols.

Symbol	Meaning
U	Number of attributes in the domain
S	Number of attributes in the user attribute set
l	Number of attributes in access policy
$\|M\|$	Bit length of access matrix
$\|L_l\|$	Bit length of value l
$\|h\|$	Bit length of hash function
m	Size of cuckoo filter

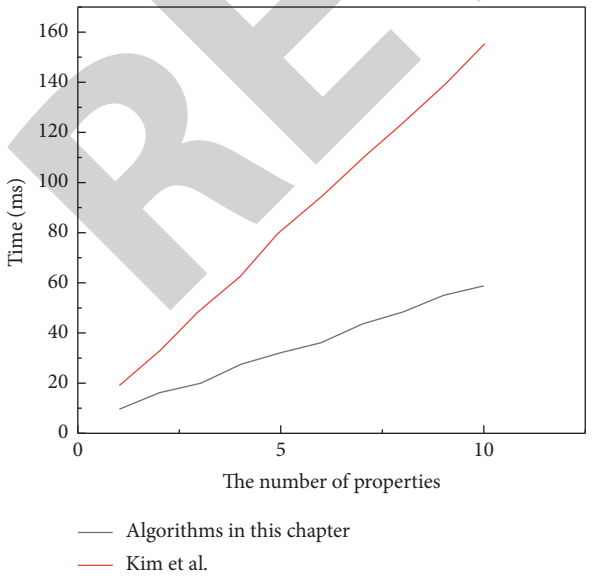

Figure 8: Encryption time of attribute encryption algorithm with hidden and verifiable policy.

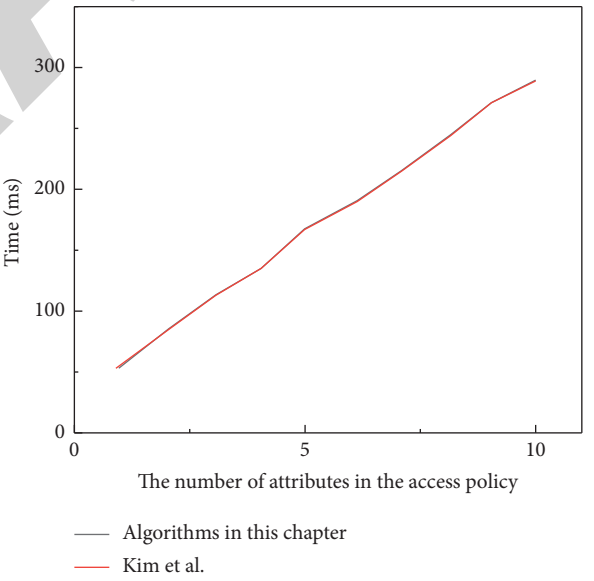

Figure 9: Decryption time of attribute encryption algorithm with hidden and verifiable policy.

privacy. Finally, conceptual stability is clearly defined according to our static assumption.

5. Conclusion

As we all know, under the same security conditions, the cryptographic scheme under prime order group is much more efficient than that under composite order group. At the same time, the scheme supporting flexible access structure has a wider application scenario. The first scheme given in

this paper is based on prime order group, but it only supports relatively simple and gate access structure. Although the second scheme supports a more flexible LSSS access structure, it is based on composite order group construction. Therefore, the construction of anonymous schemes supporting flexible access structure under prime order groups is worthy of further research. In addition, quantum computer is developing at an amazing speed. Google has made many achievements in the research field of quantum computer. Maybe quantum computer can become a reality in the near future. This will be a fatal blow to the existing public key cryptosystem, and the previously extremely secure scheme may be captured in a few seconds. Therefore, it is of great significance to construct a privacy-preserving cryptographic scheme against quantum attacks. At present, most cryptographic schemes focus on theoretical research and often cannot meet the needs of industry. Although theoretical research is important, combined with practical application, the design of cryptographic scheme to meet industrial needs should also be paid attention to. To sum up, the focus of future research can be carried out in depth around the following aspects:

(1) Design HP-CP-ABE scheme supporting flexible access policy under prime order group to meet more complex requirements. For example, HP-CP-ABE scheme supporting LSSS access structure is constructed under prime order group.

(2) Design HP-CP-ABE scheme which can resist quantum attack. Take the difficult problems on the lattice as the reduction object of the CP-ABE scheme for privacy protection, such as LWE problem, to ensure that the security of the scheme is trustworthy even after the advent of quantum computer, which is a far-reaching research significant and challenging problem for cryptographers.

(3) Design HP-CP-ABE scheme meeting industrial needs. In modern society, information leakage occurs from time to time. Combined with practical problems, such as artificial intelligence and privacy protection in smart cities, we take solving these problems as the goal of scheme construction and build a scheme that meets the actual needs.

Data Availability

The labeled data set used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported by the Anhui Provincial Education Department Natural Science Research Project: Research on Intelligent Inspection and Monitoring System of Substation Based on Mobile Robot (no. KJ2021A1193), andAnhui Natural Science Project: Research on Facial Emotion Recognition Algorithm Based on Integrated Depth Neural Network (no. XZR2020A02).

References

[1] X. Yan, G. He, J. Yu, Y. Tang, and M. Zhao, "Offline/online outsourced attribute-based encryption with partial policy hidden for the internet of things," *Journal of Sensors*, vol. 2020, no. 7, pp. 1–11, 2020.

[2] M. Bouchaala, C. Ghazel, and L. A. Saidane, "Trak-cpabe: a novel traceable, revocable and accountable ciphertext-policy attribute-based encryption scheme in cloud computing," *Journal of Information Security and Applications*, vol. 61, no. 3, Article ID 102914, 2021.

[3] Z. Zhang, P. Zeng, B. Pan, and K. K. R. ChooChoo, "Large-universe attribute-based encryption with public traceability for cloud storage," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10314–10323, 2020.

[4] R. Sarma, C. Kumar, and F. A. Barbhuiya, "Pac-fit: an efficient privacy preserving access control scheme for fog-enabled iot," *Sustainable Computing: Informatics and Systems*, vol. 30, no. 2, Article ID 100527, 2021.

[5] W. L. Tai, Y. F. Chang, and W. H. Huang, "Security analyses of a data collaboration scheme with hierarchical attribute-based encryption in cloud computing," *International Journal on Network Security*, vol. 22, no. 2, pp. 212–217, 2020.

[6] H. Li, K. Yu, B. Liu, C. Feng, Z. Qin, and G. Srivastava, "An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1949–1960, 2022.

[7] X. Yan, X. Yuan, Q. Zhang, and Y. Tang, "Traceable and weighted attribute-based encryption scheme in the cloud environment," *IEEE Access*, vol. 8, pp. 38285–38295, 2020.

[8] R. Zhang, G. Liu, S. Li, Y. Wei, and Q. Wang, "Absac: attribute-based access control model supporting anonymous access for smart cities," *Security and Communication Networks*, vol. 2021, no. 1, pp. 1–11, 2021.

[9] S. Wang, H. Wang, J. Li et al., "A fast cp-abe system for cyber-physical security and privacy in mobile healthcare network," *IEEE Transactions on Industry Applications*, vol. 56, p. 1, 2020.

[10] D. Ramesh, R. Mishra, and M. C. Trivedi, "Pcs-abe (t,n): a secure threshold multi authority cp-abe scheme based efficient access control systems for cloud environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 4, pp. 9303–9322, 2021.

[11] S. K. Selvi, "Renewable keyword for data store application in secure cloud storage using enhanced hyper elliptical curve cryptography," *International Journal of Innovative Research in Science Engineering and Technology*, vol. 9, no. 1, pp. 13268–13275, 2020.

[12] J. Yu, G. He, X. Yan, Y. Tang, and R. Qin, "Outsourced ciphertext-policy attribute-based encryption with partial policy hidden," *International Journal of Distributed Sensor Networks*, vol. 16, no. 5, Article ID 155014772092636, 2020.

[13] N. Muhammad and J. Mohd ZainMohd Zain, "Access control: ciphertext policy - attribute based encryption in cloud computing," *Journal of Physics: Conference Series*, vol. 1830, no. 1, Article ID 012019, 2021.

[14] B. F. Begam and M. Sasiskala, "Attribute based Encryption in cloud computing - a Review," *International Journal of Computer Applications*, vol. 174, no. 19, pp. 36–38, 2021.

[15] H. Li, L. Deng, C. Yang, and J. Liu, "An enhanced media ciphertext-policy attribute-based encryption algorithm on media cloud," *International Journal of Distributed Sensor Networks*, vol. 16, no. 2, Article ID 155014772090819, 2020.
[16] S. K. Panda, "Secure dynamic groups data sharing with modified revocable attribute-based encryption in cloud," *International Journal of Nano and Biomaterials*, vol. 8, no. 4, pp. 9508–9512, 2021.
[17] T. Siddhardha, Murugaanandam, D. S. Nithin, and V. Raghuveer, "Re-distributed multi-authority attribute based encryption in cloud using cp-abe algorithm," *IOP Conference Series: Materials Science and Engineering*, vol. 994, no. 1, p. 012008, Article ID 012008, 2020.
[18] Z. Cao and O. Markowitch, "Comment on "circuit ciphertext-policy attribute-based Hybrid Encryption with verifiable Delegation in cloud computing"," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 2, pp. 392-393, 2021.
[19] W. Zhang, Z. Zhang, H. Xiong, and Z. Qin, "Phas-hekr-cp-abe: partially policy-hidden cp-abe with highly efficient key revocation in cloud data sharing system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 1, pp. 613–627, 2021.
[20] X. Ren, C. Li, X. Ma et al., "Design of multi-information fusion based intelligent electrical fire detection system for green buildings," *Sustainability*, vol. 13, no. 6, p. 3405, 2021.
[21] D. Selva, B. NagarajNagaraj, D. PelusiPelusi, R. ArunkumarArunkumar, and A. Nair, "Intelligent network Intrusion prevention Feature Collection and Classification algorithms," *Algorithms*, vol. 14, no. 8, p. 224, 2021.
[22] X. Liu, J. Liu, J. Chen, and F. Zhong, "Degradation of benzene, toluene, and xylene with high gaseous hourly space velocity by double dielectric barrier discharge combined with Mn3O4/activated carbon fibers," *Journal of Physics D: Applied Physics*, vol. 55, no. 12, p. 125206, Article ID 125206, 2022.
[23] R. Huang, P. Yan, and X. Yang, "Knowledge map visualization of technology hotspots and development trends in China's textile manufacturing industry," *IET Collaborative Intelligent Manufacturing*, vol. 3, no. 3, pp. 243–251, 2021.
[24] H. Xie, Y. Wang, Z. Gao, B. P. GanthiaGanthia, and C. V. TruongTruong, "Research on frequency parameter detection of frequency shifted track circuit based on nonlinear algorithm," *Nonlinear Engineering*, vol. 10, no. 1, pp. 592–599, 2021.