International Journal for Housing Science and Its Applications
Publish August 3, 2025. Volume 46, Issue 3 Pages 1283-1293

https://doi.org/10.70517/ijhsa46399

Optimization of Data Protection and Privacy Encryption Algorithms for Open Big Data Environment

Kezhi Zhen[1,*], Zhaozhen Zeng[1], Chaoyun Luo[1], Lin Feng[1], Ming Wu[1] and Guosong Fan[1]
[1] China Tobacco Guizhou Industrial Co., Ltd., Guiyang, Guizhou, 550001, China
Corresponding authors: (e-mail: 17708541846@163.com).

Abstract Data protection and privacy encryption technology face heavy challenges in the billing big data environment. In this paper, after combing the current problems of privacy protection and data encryption, RSA homomorphic encryption algorithm is combined with CP-ABE attribute encryption protection algorithm to construct RSA+CP-ABE hybrid encryption mechanism. In order to explore the optimization effect of RSA+CP-ABE hybrid encryption algorithm, the security and performance of hybrid encryption algorithm in this paper are analyzed. The hybrid encryption algorithm of RSA+CP-ABE in this paper improves the security while maintaining the diffusivity and obfuscation.The encryption time of RSA+CP-ABE algorithm is comparable to that of the original RSA algorithm, while the decryption time is significantly reduced.The RSA+CP-ABE algorithm improves the key security and decryption speed.The encryption efficiency of the RSA+CP-ABE scheme is comparable to that of the RSA scheme. The encryption efficiency of RSA+CP-ABE scheme is reduced compared with that of RSA scheme, but the degree of efficiency improvement is reasonable and can meet the practical applications.

Index Terms RSA homomorphic encryption, CP-ABE attribute encryption, data protection, privacy encryption

I. Introduction

In the big data environment, the problem of data privacy leakage is increasingly serious [1]. With the rapid progress of information technology, the collection, preservation and manipulation of individual data are pervasive, which undoubtedly increases the risk of personal privacy exposure, and thus it is crucial to enhance data privacy protection [2]-[4]. In the context of data-driven era, a series of privacy-enhancing techniques have been widely adopted to safeguard personal information, such as information de-identification, identity hiding, differential privacy, and full homomorphic encryption [5]-[7]. There is a natural conflict between the protection of personal privacy and the accessibility of information [8]. On the one hand, in order to maintain privacy security, it is necessary to rely on technological strategies, such as information de-identification and anonymization, to reduce the risk of individual data being exposed [9], [10]. On the other hand, computation and evaluation may need to rely on processed and highly accurate information data, which also affects data availability [11], [12].

However, when dealing with large-scale datasets, conventional information encryption techniques may encounter performance limitations, resulting in encryption activities that take too much time to adapt to usage environments with stringent demands for immediate response [13]-[15]. At the same time, the security of some encryption techniques is challenged with the possibility of decryption as computational power increases and cryptography research advances [16], [17]. In order to meet these challenges, one must continuously research and optimize information encryption techniques [18]. By improving cryptographic encoding techniques and utilizing high-performance devices such as GPUs and TPUs, encryption efficiency can be significantly improved [19]. At the same time, improved multitasking capabilities also accelerate the encryption speed, ensuring protection measures while speeding up the encryption process [20], [21]. Data deformation processing technique protects privacy without affecting the analysis results, prevents data leakage by replacing and deleting sensitive information, and is widely used in test development [22], [23].

Literature [24] analyzes the current status and characteristics of the application of data encryption technology in computer network communication security, points out the current threats to network security, and discusses the data encryption technology applied to network communication security, as well as the application of data encryption technology in computer network communication security. Literature [25] discusses the architecture, concepts and deficiencies of cloud computing based on the literature review, elucidates the research challenges and future directions of privacy protection in cloud computing environment by proposing a privacy protection framework, and provides corresponding privacy protection laws to make up for the technical deficiencies. Literature [26] examines

various types of data encryption algorithms, including asymmetric and symmetric encryption, and based on literature review and empirical analysis, analyzes the role of data encryption algorithms in data security and emphasizes the importance of robust encryption measures. Literature [27] proposed an enhanced hybrid security algorithm that aims to provide better security for big data in cloud environment and introduced is hybrid matrix hash key generation algorithm and anonymous multi-fusion shuffling algorithm. Literature [28] proposes a method for data privacy encryption, Dynamic Data Encryption Strategy (D2ES), which aims to selectively encrypt data and use privacy classification methods under time constraints in order to maximize the scope of privacy protection, proves the effectiveness of D2ES and effectively provides evidence for privacy enhancement. Literature [29] proposed a BD security and privacy protection model based on image encryption algorithms, aiming to improve the protection capability of the privacy protection model, and verified the correctness of the research direction, which pointed out the way forward for the reform and optimization of the BD security and privacy protection model.

In order to improve the effect of data protection and privacy encryption mechanism in big data environment, this paper takes RSA homomorphic encryption algorithm as the base method and embeds CP-ABE attribute encryption algorithm into the original RSA algorithm to construct RSA+CP-ABE hybrid encryption algorithm. In order to understand the encryption security and performance of the optimized RSA+CP-ABE hybrid encryption algorithm, relevant experiments are conducted to compare the performance of RSA+CP-ABE hybrid encryption algorithm with the original RSA encryption algorithm in terms of diffusion and obfuscation, as well as the encryption/decryption time of the two. Finally, the encryption efficiency of the RSA+CP-ABE hybrid encryption scheme is evaluated by simulating the computation process of resource-limited users and servers using two metrics, namely, user efficiency improvement metrics and relative additional overhead metrics.

II. Establishment of privacy protection mechanism based on hybrid encryption

II. A.Privacy Protection and Data Encryption in Big Data Environment

II. A. 1) Data privacy breaches

In the big data environment, the problem of data privacy leakage is becoming increasingly serious. With the rapid progress of information technology, the collection, preservation and manipulation of individual data are pervasive, which undoubtedly increases the danger of personal privacy exposure. For example, in the disposal of a petition case of an enterprise, the imperfect security measures for data transmission and storage led to the leakage of private information, resulting in adverse consequences. Therefore, it is crucial to strengthen data privacy protection.

II. A. 2) Efficiency and Security Challenges of Data Encryption Algorithms

When dealing with large-scale datasets, conventional message encryption techniques may encounter performance limitations, resulting in encryption activities that take too much time to adapt to usage environments with stringent demands for immediate response. At the same time, with the increase in computational power and advances in cryptography research, the security of some encryption techniques is also challenged, and the possibility of decryption exists. In order to meet these challenges, there is a need for continuous research and improvement of information encryption techniques.

II. A. 3) Conflict between privacy protection and data availability

In the context of the data-driven era, a series of privacy-enhancing techniques, such as information de-identification, identity concealment, differential privacy, and full homomorphic encryption, have been widely adopted while safeguarding personal information. There is a natural conflict between the protection of personal privacy and the accessibility of information. On the one hand, in order to maintain privacy security, it is necessary to rely on technological strategies, such as information de-identification and anonymization, to reduce the risk of individual data being exposed. On the other hand, computation and evaluation may need to rely on processed and highly accurate information data, which also affects the availability of data.

II. B.RSA Homomorphic Cryptographic Protection Methods

There are two main types of traditional encryption algorithms: symmetric encryption algorithms and asymmetric encryption algorithms. In symmetric encryption algorithms, the same key is used for encryption and decryption, i.e., the same secret key is used to encrypt and decrypt the same password. Asymmetric encryption has two keys, and public and private keys. The public and private keys exist in pairs. If the original text is encrypted with the public key, it can only be decrypted with the corresponding private key. This algorithm is called asymmetric encryption algorithm because the encryption and decryption do not use the same key. The key for asymmetric encryption is a long string of random numbers obtained through a series of algorithms, usually the longer the length of the random numbers, the more secure the encrypted information. It is possible to derive the public key from the private key through a

series of algorithms, i.e., the public key exists based on the private key. However, it is not possible to deduce the private key from the public key in reverse, the process is one-way. This section introduces one of the most commonly used asymmetric encryption algorithms, the RSA encryption algorithm.

RSA encryption algorithm is currently the most representative encryption algorithm based on public key cryptosystem [30], [31]. Due to the perfect theory of the algorithm, high security strength, and the concept of easy to understand and implement, it makes RSA encryption algorithm has become a public key cryptosystem algorithm with extremely wide application. While being widely used in practice, its technology has become more and more mature, and its security performance has been greatly improved and perfected. Although the RSA encryption algorithm has gained affirmation and recognition, and has a wide range of applications in real life.

RSA encryption algorithm is a kind of packet cipher, which has three core parameters: modulus n, public key exponent e, and private key exponent d. Modulus n is the core, which is an integer between 0 and n-1. n has been proved to be very secure when it is a 1024-bit binary number, and it can be 2048 bits in important occasions. RSA algorithm adopts the power modulus operation because it requires that the encrypted plaintext is of value M<n, and if the binary length of the plaintext is greater than the modulus n, the plaintext will be grouped according to certain rules before encrypting each group. If the binary length of the plaintext is greater than the binary length of the modulus n, the plaintext is first grouped according to certain rules and then each group is encrypted. The length of the group requires that the number of bits of the binary value of each group is less than n, that is, the size of the group must be less than or equal to $\log_2(n)+1$ bits. For example, M=190, modulo n=3×5=15, the binary of n is 1111, a 4-bit binary. the binary of M is 10111110, and since M>n, the grouping of M needs to be encrypted. The binary of M is divided into two groups {1011, 1110} which are sent using key for RSA encryption respectively, and the receiver recovers M by combining the two groups of numbers {1011, 110} obtained from decryption.

Where both the sender and receiver know the value of the modulus n and the public key index e, e satisfies $\gcd(\phi(n),e)=1$. $1<e<\phi(n)$. $\phi(n)$ refers to the Euler function of n. $\gcd(\phi(n),e)=1$ refers to the greatest common divisor between $\phi(n)$ and e. l. Only the receiver knows the value of the private key exponent d. Therefore, the public key of the public-key encryption algorithm is PU={e, n}, and the private key is PR={d, n}.For the RSA cryptographic algorithm to be able to be used for public-key encryption, it must fulfill the following Condition:

(1) One can find e, d, and n such that for all M<n, there is $M^{ed}=Mmodn$.

(2) It is relatively easy to compute M^e and C^d for all M<n.

(3) It is infeasible to determine d from e and n.

The mathematical properties and description of the decryption phase of the RSA encryption algorithm are as follows:

$$M^{ed}=C^d(modn) \tag{1}$$

It is known that $ed\equiv 1(mod\,\phi(n)),\varnothing(n)=(p-1)\times(q-1)$. Then there exists an integer h such that $ed\equiv(1+h\times\phi(n))$, by Euler's theorem:

$$M^{ed}=M^{1+h\times\phi(n)}=M\times(M^{\phi(n)})^h\equiv n\times(1)^h(modn)\equiv Mmodn \tag{2}$$

The way the encryption algorithm encrypts a plaintext message $C=M^emodn$, it follows that there exists an integer k such that:

$$C=M^e-kn \tag{3}$$

Bringing the above ciphertext message C into the ciphertext message decryption formula $M=C^dmodn$ yields:

$$M=(M^e-kn)^d\,modn \tag{4}$$

Expanding the right-hand side of the above equation with the binomial theorem yields Equation (5) ($C_d^t(0\le i\le d)$ $C_d^t(0\le i\le d)$ is a binomial coefficient and is an integer):

$$(M^e-kn)^d=C_d^0M^{ed}(-kn)^0+C_d^1M^{e(d-1)}(-kn)^1+\cdots+C_d^dM^0(-kn)^d \tag{5}$$

From equation (5), it can be found that since the second term of the expansion is a multiple of n, the proof is simplified to prove that $M^e\cdot d=M(modn)$ is true, and since $ed\equiv 1(mod\,\phi(n))$, then $ed\equiv 1+h\times\phi(n)$. From the above conclusion, we can get equation (6):

$$M^{1+h\times\varnothing(n)}=M(modn) \tag{6}$$

The proof of Eq. (6) needs to be divided into two cases:

n and M are mutually prime: by Euler's theorem we get $M^{\phi(n)} = kn+1$ which can be obtained by subjecting it to the binomial expansion theorem:

$$M^{\varnothing(n)} \times M = (kn+1) \times M(modn) = M \tag{7}$$

Thus it is proved that Eq. (6) holds.

n and M are not mutually prime: Since the modulus $n = p \times q$, M must be equal to either kp or kq. In the case of M=kp, for example, k and q are then necessarily mutually prime. If k and q are not mutually prime, then there is:

$$k = tq, n = tqp = tn \tag{8}$$

But according to the specification of the RSA encryption algorithm, $M \in (0.....n-1)$ and M<n's, so k and q must be mutually prime. Since k and q are mutually prime and p and q are mutually prime, then we have kp and q must be mutually prime, and according to Euler's theorem, formula (9) holds:

$$(kp)^{q-1} \equiv 1(modq) \tag{9}$$

Further inference leads to equation (10):

$$[(kp)^{q-1}]^{h(p-1)} \times kp \equiv kp(modq) \tag{10}$$

That is, $(kp)^{ed} \equiv kp(modq)$, which is obtained by further inference:

$$(kp)^{ed} = kp + tq \tag{11}$$

Clearly, t is divisible by q, i.e., $t = t^{'} p$, can be obtained:

$$(kp)^{ed} = kp + t^{'} pq \tag{12}$$

Since $n = kp, N = pq$, this finally leads to Eq. (13):

$$M^{ed} \equiv M(modn) \tag{13}$$

Thus it is proved that equation (6) holds and thus the decryption method in the RSA encryption algorithm is fully proved.

II. C.CP-ABE Attribute-Based Encryption Protection Methods

Let P be the set of all attributes $\{p1, p2 \cdots pn\}$, then each user's attribute $P^{'}$ is a non-empty subset $P^{'} \subset \{p1, p2 \cdots pn\}$ of the set of attributes P, and N attributes can be used to identify 2^n users, and this is where the user attributes come in.

II. C. 1) Bilinear Mapping

Since CP-ABE cryptography uses the prototype of bilinear mapping as a technique, we first introduce some theoretical foundations related to the group of bilinear mappings: let $G0$ and $G1$ be two multiplicative cyclic groups of order prime p, and g be the generating element of $G0$, $e: G0 \times G0 \to G$. The bilinear map e has the following properties:

(1) Bilinearity: for any $u, v \in G0$ and any $a, b \in Zp$, we have $e(u^a, v^b) = e(u, v)^a b$.

(2) Non-degeneracy: $e(g, g) \neq 1$.

We call $G0$ a bilinear group if both the group operation in $G0$ and the bilinear map $e: G0 \times G0 \to G1$ are efficiently computable. The bilinear mapping e has symmetry since $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

II. C. 2) CP-ABE encryption algorithm design

The CP-ABE algorithm consists of four basic algorithms and operations [32], [33], namely Setup, Encrypt, KeyGen, and Decrypt.

Setup: the input of the setup algorithm has only implicit security parameters and outputs the public parameter PK and the master key MK.

Encrypt (PK, M, A): the inputs to the encryption algorithm are the public parameter PK, the plaintext and the access structure on the full set of attributes. The algorithm encrypts the plaintext and produces the ciphertext CT,

which can decrypt the message only if the user holds the set of attributes that satisfy the access structure. We assume that the ciphertext implies the access structure.

KeyGen (MK, S): the input to the key generation algorithm is the master key MK and the set of attributes describing the private key, and the output is the private key SK.

Decrypt (PK, CT, SK): the input to the decryption algorithm is the public parameter PK, the ciphertext CT containing the access policy and the private key SK generated from the set of attributes. If the set satisfies the access structure then the algorithm decrypts the ciphertext CT to return the message.

The detailed encryption algorithm is as follows:

Suppose that $G0$ is a bilinear mapping group of order prime p, while the parameter g is the generating element of the mapping group $G0$, and $e: G0 \times G0 \to G1$ is a bilinear mapping. The security parameter k determines the size of the group. At the same time, we define the Lagrange coefficients $\Delta i, s, i \in Zp$, and S is an element of the set Zp: $\Delta i, s(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$. The hash function $H: \{0,1\}^* \to G0$ is randomoracle.This function maps any property described by a binary string to a random group element. For CP-ABE is constructed as follows:

The SetupSetup algorithm chooses a bilinear mapping $G0$ with generating element g and order of prime p, with indices $\alpha, \beta \in Zp$. Generate public key $PK = G0, g, h = g^{\beta}, e(g,g)^{\alpha}$ and master key $MK = \beta, g^{\alpha}$.

The Encrypt(PK, M, T) encryption algorithm encrypts the message M under the access structure tree T. The algorithm first chooses a polynomial qx for each node x (including leaf nodes) of the access structure tree T. The polynomials are chosen from the top down, starting from the root node R of the tree. The degree dx of the polynomial qx at node x is 1 less than the threshold value kc at that node, i.e., $dx = kc - 1$.

The algorithm chooses random numbers $s \in Zp$ starting from the root node R and sets $qr(0) = s$. The algorithm then chooses randomly dr points on the polynomial qr to completely define qr. For the other vertices x, let $qx(0) = qparent(x)(index(x))$ and randomly choose the other dx vertices to completely define qx.

Let the set Y of all leaf nodes in T, then compute the ciphertext under the given tree access structure T:

$$CT = (T, \tilde{C} = Me(g,g)^{\infty}, C = h^{s}, \forall y \in Y: C_y = g^{\varphi(0)}, C_y^{'} = H(att(y))^{\varphi(0)}) \tag{14}$$

The input to the KeyGen (MK, S) key generation algorithm is the set of attributes S and the output is the key labeled by S. The algorithm first chooses the random number $r \in Zp$ and then chooses the random number $rj \in Zp$ for each $j \in S$. Finally the private key is computed:

$$SK = (D = g^{(\alpha + r)/\beta}, \forall j \in S: D_j = g^{r} H(j)^{rj}, D_j^{'} = g^{rj}) \tag{15}$$

Decrypt(PK, CT, SK) Our decryption algorithm is a recursive algorithm. For ease of discussion, we present the simple form of the decryption algorithm. We first define the recursive algorithm Decrypt(PK, CT, x), which takes as input the ciphertext $CT = (T, \tilde{C}, C, \forall y \in Y: C_y, C_y^{'})$, the private key SK associated with the set of attributes S, and node x in T.

When node x is a leaf node, let $i = att(x)$ if $i \in S$:

$$\begin{aligned} DecryptNode(CT, SK, x) &= \frac{e(D_i, C_x)}{e(D_i^{'}, C_x^{'})} \\ &= \frac{e(g^{r}.H(i)^{ri}, g^{q_x(0)})}{e(g^{ri}, H(i)^{q_x(0)})} \\ &= e(g,g)^{rq_x^{(0)}} \end{aligned} \tag{16}$$

If $i \notin S$, then $DecryptNode(CT, SK, x) = \perp$.

We now consider the recursive case when x is a non-leaf node. The algorithm $Decrypt(PK, CT, x)$ works as follows: for all child nodes z of x, compute $Fz = DecryptNode(CT, SK, z)$. Let Sx be the set of child nodes z of size kx that satisfy $Fz \neq \perp$. If no such set exists, then this node is not satisfied and the function returns on.

Otherwise, we compute:

$$
\begin{aligned}
F_x &= \prod_{z\in S(x)} F_z^{\Delta i_z^i(0)}, \text{among}, i = index(z), S_x^{'} = \{index(z) : z \in S_x\} \\
&= \prod_{z\in S(x)} \left(e(g,g)^{r\cdot q_{z(0)}}\right)^{\Delta_{i,s_x^{'}}(0)} \\
&= \prod_{z\in S(x)} \left(e(g,g)^{r\cdot q_{parent(z)(index(z))}}\right)^{\Delta_{i,s_x^{'}}(0)} \\
&= \prod_{z\in S(x)} e(g,g)^{rq_{z(i)}(\Delta i,s_x^{'}(0))} \\
&= e(g,g)^{r\cdot q_x(0)} (\text{Using polynomial interpolation})
\end{aligned}
\tag{17}
$$

and return the result.

After defining the Decryptl function, we define the decryption algorithm. The algorithm first calls $DecryptNode(CT, SK, R)$, where R is the root node of the tree T. If the tree satisfies S, we decree:

$$
A = DecryptNode(CT, SK, R) = e(g,g)^{rq_R(0)} = e(g,g)^{rs} \tag{18}
$$

The algorithm is now decrypted by the following calculation:

$$
\tilde{C} \Big/ \left(\frac{e(C,D)}{A}\right) = \tilde{C} \Big/ \left(\frac{e(h^s, g^{(\alpha+r)/\beta}}{e(g,g)^{rs}}\right) = M \tag{19}
$$

II. D.Hybrid encryption mechanism of RSA+CP-ABE

We combine RSA homomorphic encryption algorithm and CP-ABE attribute-based encryption algorithm to propose a reliable data protection scheme based on categorical hybrid encryption at the privacy level to ensure that the user's privacy is not violated.

In the big data environment, sensitive private data must be stored in the form of encrypted ciphertext in the cloud service, and this security means is the most basic for privacy data protection. Further, if most of the cloud data is stored in the form of encrypted ciphertext in the cloud, many computing services cannot be executed because the ciphertext cannot be decrypted, and the services are difficult to be provided to the users due to the ciphertext limitation. Cloud storage is only one aspect of what cloud service providers offer, and the main SaaS and PaaS will suffer as a result. The user encrypts the data homomorphically, stores the ciphertext in the cloud, and operates on the data in the cloud, and for the platform, all operations are based on the ciphertext, and the decryption key is held only by the user, and cannot be known by the service provider. Homomorphic encryption realizes the user's private data protection in this way.

Homomorphic encryption cannot read and utilize other people's network resources, and if you want to share information with others, you have to use attribute-based encryption. CP-ABE attribute-based encryption can be used to realize the access control and authentication of users' outgoing packet data, and this technology can effectively solve the problem of revoking users' privileges and so on in the access control.

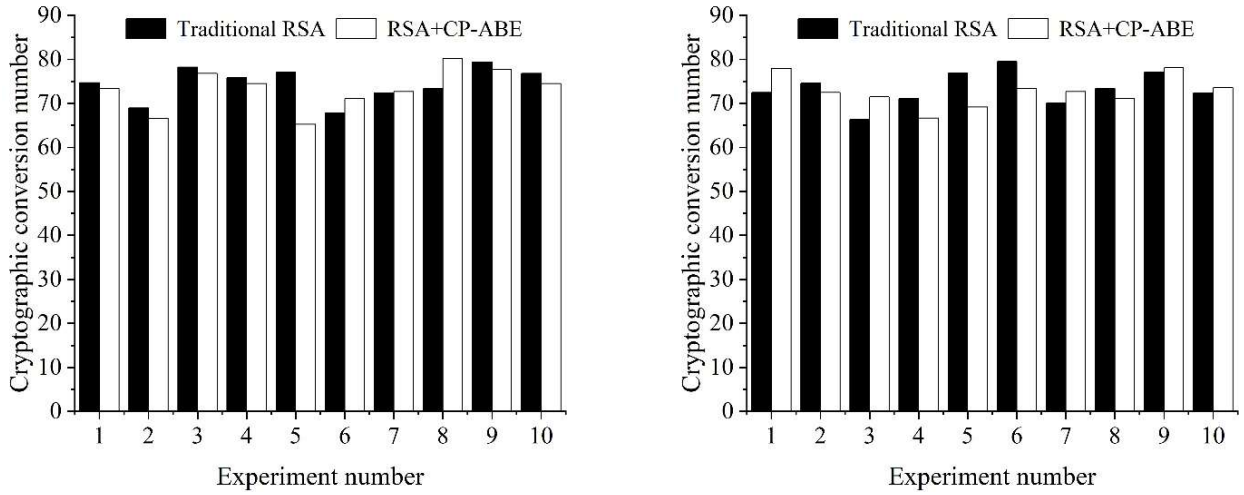
The combination of the two encryption methods not only ensures the security of important data, but also realizes the sharing of network resources.

III. Security and performance analysis

III. A. Security analysis

For the improved hybrid encryption algorithm, since the two keys used are uncorrelated, the attacker is unable to obtain all the keys in the encryption process by derivation even if he gets one key. If the attacker wants to take an exhaustive key attack, since the length of the key used is 128bit, the best case scenario is 1 while the worst case scenario is 2^k, and according to the calculation the average complexity is 2^{127}, i.e., the attacker needs to make 2^{127} attempts on average to crack the key. In this paper, the optimization method to add a key independent of the initial key, further increasing the complexity of the key cracking, the attacker needs to make an average of 2^{255} attempts to crack the key to the current computing power to crack the key at least hundreds of millions of years, even if cracked out, the price paid is far more than the value of the data itself. The comparison of diffusivity and obfuscation of the traditional RSA algorithm and the improved hybrid RSA+CP-ABE encryption algorithm for encrypting 128bit plaintext is shown in Fig. 1, where 10 experiments were conducted for each. Fig. (a) shows the results of diffusivity comparison and Fig. (b) shows the results of obfuscation comparison.

From Fig. 1, it can be seen that by changing one plaintext, the diffusivity range of the improved hybrid encryption algorithm is 73±7, and the diffusivity range of the traditional RSA algorithm is 74±6. By changing one key, the obfuscation range of the improved hybrid encryption algorithm with RSA+CP-ABE is 73±5, and the obfuscation range of the traditional RSA algorithm is 73±7. From this it can be seen that the improved algorithm doesn't reduce the original RSA algorithm's the improved algorithm does not reduce the scalability and obfuscation of the original RSA algorithm, but also improves the security of the symmetric key.



(a) Diffusivity comparison

(b) Confusing comparison

Figure 1: Experiment results

Using CP-ABE algorithm based on attribute encryption to encrypt the key of RSA algorithm for transmission, it can guarantee the security of symmetric key very well.The comparison results of key length and confidentiality years under the same security strength of CP-ABE algorithm and RSA algorithm are shown in Table 1. From the table, it can be seen that CP-ABE algorithm only needs a very short key change to achieve a high degree of secrecy.

Table 1: CP-ABE and RSA confidentiality level comparison

Confidentiality level	RSA key length	CP-ABE key length	Time of secrecy
96	2048	192	2020
128	3072	256	2040
144	4096	288	2050

III. B. Encryption and decryption time analysis

First of all, the decryption time of the RSA algorithm is tested, due to the fast encryption and decryption speed of the RSA algorithm, in order to be able to see the trend of its encryption and decryption speed, the amount of data is put into 60MB, and the results of the comparison between the encryption and decryption time of the traditional RSA algorithm and the improved RSA+CP-ABE algorithm are shown in Table 2.

As can be seen from Table 2, in terms of encryption time consumed, the improved RSA+CP-ABE algorithm is similar to the pre-improvement, almost the same. Because, the simplified column mixing operation in the improved RSA+CP-ABE algorithm does not change the original computation amount, which is still 2 times multiplication operation and 4 times dissimilarity operation. Therefore, the CP-ABE encryption protection method is used to improve the security of the key without affecting the encryption speed of the RSA algorithm, and the optimization method is effective. In terms of decryption time consumption, the improved RSA+CP-ABE algorithm shows a significant reduction in time consumption compared to the pre-improvement period, and the decryption time consumption is reduced by 5.1, 11.1, 12.6, 22.5, 28.2, and 32.2ms when the data volume is 10, 20, 30, 40, 50, and 60MB, respectively. Because the optimized column mixing operation reduces the computation of inverse column mixing operation during decryption. Therefore, the improved RSA+CP-ABE algorithm improves the decryption speed while increasing the key security and the optimization method is effective.

Table 2: Time-consuming comparison between RSA+CP-ABE and the traditional RSA

Data volume/MB	10	20	30	40	50	60
Traditional RSA encryption/ms	32.5	70.2	115.6	150.3	223.4	275.6
Traditional RSA decryption/ms	33.7	71.5	110.4	144.7	212.7	264.3
RSA+CP-ABE encryption/ms	30.4	71.5	113.7	147.9	220.9	270.2
RSA+CP-ABE decryption/ms	28.6	60.4	97.8	122.2	184.5	232.1

III. C. Evaluation of the efficiency of encryption schemes

In order to evaluate the efficiency of the RSA+CP-ABE scheme, we conducted experimental simulations using C++ as the programming language, and all experiments were run on a machine configured with Windows 10, a 3.40GHz Intel i7 CPU and 24GB RAM in order to simulate the computational processes of both the resource-limited user and the server. If the computational processes of both users and servers are run on the same machine, then the experimental results can reflect the difference in the amount of computation between the two sides. However, if the experiments are run on different machines, one machine runs the computation of the user side and the other runs the computation of the server side, this will lead to the experimental results are also affected by the different computation speeds of the different machines, so the experiments are only run on the same machine and the changes in communication efficiency do not need to be considered since the RSA+CP-ABE scheme does not introduce any additional communication overheads. Also in terms of experimental data, randomly generated matrices of real numbers are used for the experiments. The main symbols used in the experiments are shown in Table 3.

Table 3: The symbols and definitions used in the experiment

Symbol	Definition
t_o	The time cost of calculating the original outsourcing task
t_{cs}	The time required for the server to calculate the encryption of the outsourcing task
t_{c1}	The time required by the user to generate the key and encrypt the original task
t_{c2}	The time required by the user to decrypt and validate the results
t_c	$t_c=t_{c1}+t_{c2}$
i_c	User efficiency index
i_{cs}	Server efficiency indicator
i_{ec}	Relative additional cost indicator

The main purpose of the experiment is to demonstrate the improvement of task outsourcing on user efficiency, so the main performance metric is selected as $i_c = \frac{t_o}{t_c}$, which is the ratio of the user's time to process the task locally to the time to perform the computation after the user has outsourced the task, as the user efficiency improvement metric. This value should be a positive number greater than 1, which represents the user's computational overhead is smaller than it was by outsourcing the task. There is also a server efficiency metric $i_{cs} = \frac{t_o}{t_{cs}}$ to be considered, which represents the efficiency impact that the encryption scheme gives to the server in processing tasks. This value should ideally be close to 1, which indicates that there is no increase in the computational overhead required by the server to process encrypted tasks compared to processing the original outsourced tasks, which also saves the user the price of renting server resources. The final relative additional overhead metric to be considered $i_{ec} = \frac{t_c + t_{cs} - t_o}{t_o}$ represents the total time overhead required for both the user and the server to complete the task. Change in time overhead, the smaller this value the better.

In order to show the experimental results more clearly, the traditional AES algorithm is introduced to be compared together with the traditional RSA and the improved RSA+CP-ABE encryption scheme in this paper, and the experimental results of the efficiency evaluation are shown in Table 4, and the results of the efficiency evaluation of the traditional RSA and the improved RSA+CP-ABE encryption scheme in this paper are shown in Fig. 2. In Table 4 the running time is listed, this time is obtained by running 20 times to take the average value, the dimension of the matrix is set as *m*: *n*: *s*=4:5:6, and the number of iterations for verification is taken as *l*=40, *l*=70, and *l*=100, which corresponds to the three cases of efficiency prioritization, compromise, and verification prioritization,

respectively. The server efficiency metric i_{cs} close to 1 means that the server does not have an increased computational overhead due to the fact that it is dealing with an encryption task as compared to dealing with the original. $t_{c1}<t_{c2}$ means that the computation results in a greater time overhead for decryption and validation than generating the key and encrypting the original data.

As can be seen from Fig. 2, the user efficiency improvement metric i_c is increasing with increasing data size, and the corresponding relative additional overhead metric i_{ec} is decreasing. In addition, as the number of authentication iterations increases, the user efficiency improvement metric i_c decreases, while the relative extra overhead metric i_{ec} increases. Further compared to the RSA encryption scheme, the efficiency of the RSA+CP-ABE scheme decreases, but the efficiency improvement is comparable, which is reasonable because the RSA+CP-ABE scheme includes not only multiplicative perturbations but also additive perturbations to correct the intrinsic security flaws in the RSA scheme. Thus the RSA+CP-ABE encryption scheme is not only more privacy secure, but also efficient enough to meet the needs of practical applications.

Table 4: The evaluation and analysis of the efficiency of the encryption schemes

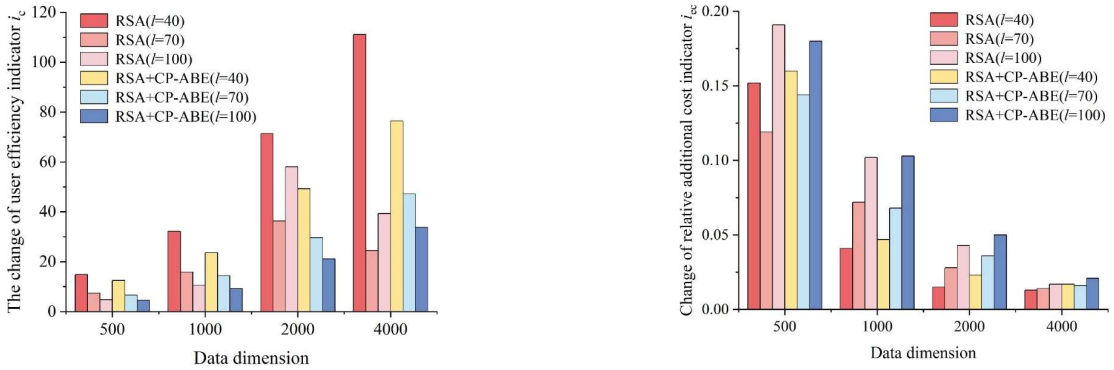
Validation iteration number	m	Traditional AES	Traditional RSA					
		t_o	t_{cs}	t_{c1}	t_{c2}	i_c	i_{cs}	i_{ec}
l=40	500	1158	1256	25	72	14.85	0.92	0.152
	1000	9579	9675	74	248	32.15	0.99	0.041
	2000	84728	84786	296	918	71.32	1.00	0.015
	4000	301987	303056	689	2086	111.07	1.00	0.013
l=70	500	1145	1126	24	157	7.39	1.00	0.119
	1000	9683	9768	90	549	15.87	0.99	0.072
	2000	84722	84725	296	2086	36.39	1.00	0.028
	4000	304069	303026	689	4689	58.09	1.00	0.014
l=100	500	1133	1114	25	230	4.82	1.00	0.191
	1000	9108	9178	74	812	10.59	0.99	0.102
	2000	84597	84786	310	3175	24.49	1.00	0.043
	4000	305346	302869	689	7125	39.33	1.01	0.017
Validation iteration number	m		RSA+CP-ABE					
			t_{cs}	t_{c1}	t_{c2}	i_c	i_{cs}	i_{ec}
l=40	500		1250	48	72	12.45	0.93	0.160
	1000		9623	152	275	23.59	1.00	0.047
	2000		84963	623	1135	49.29	1.00	0.023
	4000		303152	1506	2546	76.39	1.00	0.017
l=70	500		1138	48	154	6.66	1.01	0.144
	1000		9674	141	559	14.41	1.00	0.068
	2000		84893	623	2268	29.63	1.00	0.036
	4000		302578	1497	5064	47.14	1.00	0.016
l=100	500		1087	48	226	4.53	1.04	0.180
	1000		9063	154	857	9.25	1.00	0.103
	2000		84795	642	3398	21.15	1.00	0.050
	4000		302684	1520	7610	33.81	1.01	0.021

IV. Conclusion

In this paper, we combine the RSA same-stage encryption algorithm with CP-ABE attribute encryption algorithm to construct the RSA+CP-ABE hybrid encryption algorithm to enhance data protection and privacy encryption effect. The security and performance of the hybrid encryption algorithm in this paper are verified through relevant experiments.

The diffusivity range of this paper's RSA+CP-ABE hybrid encryption algorithm is 73±7, and the obfuscation range is 73±5, which does not reduce the original scalability and obfuscation of the RSA algorithm and improves the security of symmetric keys.The encryption time consumed by the RSA+CP-ABE algorithm is similar to that by the traditional RSA algorithm, while the decryption time consumed is significantly reduced, and the reduction of decryption time consumed increases with the increase of the data volume, the data volume increases with the

increase of the data volume. When the data volume is 10, 20, 30, 40, 50, 60MB, the decryption time is reduced by 5.1, 11.1, 12.6, 22.5, 28.2, 32.2ms respectively, and the RSA+CP-ABE algorithm improves the decryption speed while improving the key security. The user efficiency improvement metrics are increasing with the increase of data size, and the relative extra overhead metrics are decreasing.The efficiency of the RSA+CP-ABE scheme decreases compared to the RSA scheme, but the degree of efficiency improvement is reasonable and sufficient to meet the practical requirements.



(a) The change of user efficiency indicator i_c (b) The change of relative additional cost indicator i_{ec}

Figure 2 The change of i_c and i_{ec} with different data volume

References

[1] Jegorova, M., Kaul, C., Mayor, C., O'Neil, A. Q., Weir, A., Murray-Smith, R., & Tsaftaris, S. A. (2022). Survey: Leakage and privacy at inference time. IEEE Transactions on Pattern Analysis and Machine Intelligence, 45(7), 9090-9108.

[2] Nayak, S. K., & Ojha, A. C. (2020). Data leakage detection and prevention: Review and research directions. Machine learning and information processing: proceedings of ICMLIP 2019, 203-212.

[3] Felix, A., Abdullahi, A., Momoh, J., Ikpaya, I. D., & Juliet, I. O. (2025, February). Strengthening Data Privacy and Protection in Nigeria: Recommendations for a Comprehensive Approach. In 8th URSI-NG Annual Conference (URSI-NG 2024) (pp. 27-38). Atlantis Press.

[4] Yanamala, A. K. Y., & Suryadevara, S. (2023). Advances in Data Protection and Artificial Intelligence: Trends and Challenges. International Journal of Advanced Engineering Technologies and Innovations, 1(01), 294-319.

[5] Gutta, C. (2024). Strengthening Data Privacy Laws in the Age of IoT. Interdisciplinary Studies in Society, Law, and Politics, 3(1), 1-3.

[6] Ping, H. (2022). Network information security data protection based on data encryption technology. Wireless Personal Communications, 126(3), 2719-2729.

[7] Zhao, B., Chen, W. N., Wei, F. F., Liu, X., Pei, Q., & Zhang, J. (2024). PEGA: A privacy-preserving genetic algorithm for combinatorial optimization. IEEE Transactions on Cybernetics, 54(6), 3638-3651.

[8] Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications policy, 41(10), 1027-1038.

[9] Saurabh, S. (2024). The Digital Personal Data Protection Act of 2023: Strengthening Privacy in the Digital Age. Int'l JL Changing World, 3, 77.

[10] Chamorro, R. E. E., Cabrita, C. M. M., & Lima, J. S. V. (2025). Strengthening personal data protection through the creation of a regulatory body. Salud, Ciencia y Tecnología-Serie de Conferencias, (4), 611.

[11] Amal Chandra, C. (2024). Strengthening India's Cybersecurity and Data Privacy Landscape: A Comprehensive Overview. Indian Journal of Public Administration, 70(3), 466-478.

[12] Binjubeir, M., Ahmed, A. A., Ismail, M. A. B., Sadiq, A. S., & Khan, M. K. (2019). Comprehensive survey on big data privacy protection. Ieee Access, 8, 20067-20079.

[13] Li, X. (2020, June). Application of data encryption technology in computer network communication security. In Journal of Physics: Conference Series (Vol. 1574, No. 1, p. 012034). IOP Publishing.

[14] Liu, G. (2022). The application of data encryption technology in computer network communication security. Mobile information systems, 2022(1), 3632298.

[15] Alloghani, M., Alani, M. M., Al-Jumeily, D., Baker, T., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2019). A systematic review on the status and progress of homomorphic encryption technologies. Journal of Information Security and Applications, 48, 102362.

[16] Ma, H., & Zhang, Z. (2020). A new private information encryption method in internet of things under cloud computing environment. Wireless Communications and Mobile Computing, 2020(1), 8810987.

[17] Chen, H., Hu, H., Sun, B., Zhao, H., Qie, Y., Luo, Z., ... & Li, F. (2022). Dynamic anti-counterfeiting labels with enhanced multi-level information encryption. ACS Applied Materials & Interfaces, 15(1), 2104-2111.

[18] Wu, Y., Chen, X., & Wu, W. (2023). Multiple stimuli-response polychromatic carbon dots for advanced information encryption and safety. Small, 19(10), 2206709.

[19] Gollagi, S. G., Srividya, R., Kumar, G. S., & Pareek, P. K. (2021, December). A novel image encryption optimization technique. In 2021 International Conference on Forensics, Analytics, Big Data, Security (FABS) (Vol. 1, pp. 1-6). IEEE.

[20] Lee, C. C., Tseng, H. C., Liu, C. C., & Chou, H. J. (2021). Using aes encryption algorithm to optimize high-tech intelligent platform. WSEAS Transactions on Business and Economics, 18, 1572-1579.

[21] Selvaraj, J., Lai, W. C., Kavin, B. P., & Seng, G. H. (2023). Cryptographic encryption and optimization for internet of things based medical image security. Electronics, 12(7), 1636.
[22] Zhang, Z. (2024). Optimization of data packet encryption algorithm in network link transport layer. Journal of Cyber Security Technology, 8(1), 53-70.
[23] Abed, Q. K., & Al-Jawher, W. A. M. (2023). An image encryption method based on lorenz chaotic map and hunter-prey optimization. Journal Port Science Research, 6(4), 332-343.
[24] Yang, W. (2021, September). Optimization of Data Encryption Technology in Computer Network Communication. In Journal of Physics: Conference Series (Vol. 2037, No. 1, p. 012070). IOP Publishing.
[25] Sun, P. J. (2019). Privacy protection and data security in cloud computing: a survey, challenges, and solutions. Ieee Access, 7, 147420-147452.
[26] Oladoyinbo, T. O., Oladoyinbo, O. B., & Akinkunmi, A. I. (2024). The Importance Of Data Encryption Algorithm In Data Security. Current Journal of International Organization of Scientific Research Journal of Mobile Computing & Application (IOSR-JMCA), 11(2), 10-16.
[27] Sumithra, R., & Parameswari, R. (2022). Data privacy and data protection security algorithms for big data in cloud. International journal of health sciences, 6(S2), 7613-7621.
[28] Gai, K., Qiu, M., & Zhao, H. (2017). Privacy-preserving data encryption strategy for big data in mobile cloud computing. IEEE Transactions on Big Data, 7(4), 678-688.
[29] Hua, B., Wang, Z., Meng, J., Xi, H., & Qi, R. (2023). Big data security and privacy protection model based on image encryption algorithm. Soft Computing, 1-13.
[30] Kazi Naimur Rahman,Monowar Wadud Hridoy,Md Mizanur Rahman,Md Rifatul Islam & Semonti Banik. (2024). Highly secured and effective management of app-based online voting system using RSA encryption and decryption. Heliyon,10(3),e25373-e25373.
[31] Sagi Sreevibhu & Teendra Pavan Kumar. (2024). Application of Integrated RSA Encryption in Remote Data Integrity Check. Journal of Research in Science and Engineering,6(8),32-37.
[32] Shumin Xue & Chengjuan Ren. (2019). Security Protection of System Sharing Data with Improved CP-ABE Encryption Algorithm under Cloud Computing Environment. Automatic Control and Computer Sciences,53(4),342-350.
[33] T Siddhardha,Siddhardha T,Murugaanandam,Sri Nithin D & Raghuveer V. (2020). Re-Distributed Multi-Authority Attribute Based Encryption in Cloud Using CP-ABE Algorithm. IOP Conference Series: Materials Science and Engineering,994(1),012008-.