Research Article

Jie Cai* and Jun Wang

Data sharing platform and security mechanism based on cloud computing under the Internet of Things

https://doi.org/10.1515/comp-2022-0256
received April 21, 2022; accepted August 9, 2022

Abstract: Under the background of the rapid development of information technology, people's data and information security problems are becoming increasingly serious. Data and information can be leaked in daily Internet access or communications. When doing data sharing, the security mechanism of the data sharing platform should be analyzed. This article aims to study how to analyze the security mechanism of cloud computing-based data sharing platforms in the Internet of Things era. This article presented an attribute-based encryption (ABE) algorithm, a detailed interpretation of the attribute-based encryption algorithm, and analyzed security problems in data sharing in cloud computing. The experimental results showed that the ABE algorithm takes an average of 11 s with five trials, while the other two methods take 51.8 and 31.6 s. ABEs take less time for different encryption numbers under the same data than the other two methods and are more efficient than the other two methods. Thus, attribute-based encryption algorithms should have more advantages.

Keywords: Internet of Things, cloud computing, data sharing platform, encryption algorithm

1 Introduction

With the development and popularization of cloud computing, the storage, computing, and other services provided by cloud platforms are favored increasingly by individuals and small- and medium-sized enterprises. Despite the growing development of cloud service technology, most users are still hesitant to share confidential data on public cloud platforms due to personal privacy issues. To protect data privacy, various methods of encryption have emerged. However, encryption increases the difficulty and cost of data processing and even limits the advanced capabilities provided by cloud services, such as data sharing. As a highly integrated and comprehensive application of the new generation of information technology, the Internet of Things (IoT) has the characteristics of strong penetration, great driving effect, and good comprehensive benefits. It is another promoter of the development of the information industry after the computer, the Internet, and the mobile communication network.

Data security and data privacy in the public cloud have always been the most concerning issues for users because the cloud data are vulnerable to attack and snooping. For example, a malicious server may try to analyze the data to obtain some decision information, or a curious service administrator may somehow spy on private data, such as identity information, etc. An effective solution is that the data owner (DO) outsources the encrypted data to the cloud service provider (CSP). Although the encryption mechanism can effectively protect the privacy of data, it limits the quality of cloud services to some extent. Therefore, data sharing, an important feature in cloud storage, will face severe challenges.

The innovation of this article is that: (1) It introduces the relevant theoretical knowledge of the IoT and cloud-based data sharing. The attribute-based encryption (ABE) algorithm is proposed, which analyzes how the ABE algorithm plays a role in solving the security problem based on cloud computing. (2) It compares the ABE algorithm with the encryption algorithm of the traditional encryption algorithm. Through the analysis, we can know that the ABE algorithm's working time is shorter than other methods, and its working efficiency is higher than other methods.

* **Corresponding author: Jie Cai,** School of Intelligent Engineering, NanJing City Vocational College, Nanjing 211200, Jiangsu, China, e-mail: caijie@ncc.edu.cn
Jun Wang: Software Development Department, BDStar Intelligent & Connected Vehicle Technology Co., Ltd. (BICV), Nanjing 211100, Jiangsu, China, e-mail: steedgallop@sina.com

2 Related work

With the development of information technology, the application of the IoT and cloud computing has become increasingly extensive. Jin L found that data sharing is not only very convenient but also particularly cost-effective, so it has become an attractive service provided by cloud computing platforms. As a potential technology for data sharing, ABE has attracted a lot of attention. However, existing ABE solutions are not only expensive but also have low security. Therefore, he addressed this challenging problem by proposing a new attribute-based data sharing scheme suitable for mobile users with limited resources in cloud computing. Although the scholar proposed a specific solution, the solution has not been demonstrated in practice, so the feasibility is unknown [1]. Xue et al. found that according to the current state of the medical industry, it is difficult to verify, store, and synchronize clinical data, so clinical data sharing has become a challenging task. This results in high resource and time costs for verification. To solve this problem, he proposed a block-based medical data sharing model, which has the advantages of decentralization, high security, collective maintenance, and tamper resistance. It can make data sharing more convenient, safe, and fast, and better match different types of medical institutions. Although the scholar described the advantages of his proposed model, he did not specify how to apply it to medical information [2]. Liu et al. found that in a secure data sharing system, a keyword search for encrypted files is a basic requirement of users. While traditional searchable encryption techniques can provide privacy protection, two key issues still need to be considered. He proposed a scheme called "Verifiable Search Encryption with Aggregated Keys." In this scheme, after the user obtains such a key, it can be used to verify the security of the server. However, the scholar did not describe how to verify the security of the server [3]. Jiang et al. discovered that mobile crowd sensing (MCS) is a new approach to sensing using embedded sensors. However, the traditional MCS architecture often has the problems of high operating costs and poor scalability of centralized servers, and data sharing can effectively reduce the cost of servers. He proposed a novel P2P-based MCS architecture, where sensory data are saved and processed locally in user devices and shared among users in a P2P manner. Scholars put forward corresponding measures for the problem, but there is no specific experiment to show whether the measures are reliable [4]. Xue et al. found that privacy protection and secure data sharing have become a very challenging issue. Existing secure access control schemes consume too many computing resources, which may therefore not be suitable for real-time applications. Therefore, he proposed a cryptography-based mechanism for fine-grained access control. The results show that complex computations are securely outsourced to cloud servers with confidentiality and privacy protection. Although the scholars came to a conclusion, they did not elaborate on the experimental process [5]. Ascoli et al. found that most people have not embraced data sharing applications, so he discusses how publicly available repositories can benefit both data producers and end users. He outlined the practical ways for resource developers to maximize the research impact of data-sharing platforms for contributors and users. However, the scholar did not specifically introduce how data sharing benefits data producers [6].

3 Cloud data sharing mechanism based on attribute-based encryption algorithm

3.1 Basic concepts of IoT and cloud computing data sharing

The proposal of the IoT breaks the traditional idea of separating equipment and information transmission, truly realizes the communication between things, and embodies the unified concept of the Internet, which is of great significance [7]. If information is included in the communication application of the IoT, the number of communication connections that may be involved may reach billions, which provides a large space for information transmission.

Data sharing is to allow users who use different computers and different software in different places to read other people's data and perform various operations and analyses. The degree of data sharing reflects the level of information development of a region and a country. The higher the degree of data sharing, the higher the level of information development. By realizing data sharing, more people can use existing data resources more fully, which reduces the corresponding costs of repetitive labor and data collection, and focuses on the development of new applications and system integration [8]. Since the data provided by different users may come from different channels, the data content, data format, and data quality are very different. Data sharing becomes very difficult, and the data format cannot be converted or information

may be lost after conversion. Due to intractable problems such as these, data flow and sharing in various departments and various software systems are severely hindered [9].

With the rapid development of computer level and communication technology, the application of the IoT in e-commerce, power monitoring, military and national defense, and other confidential fields has become increasingly extensive, and the sharing and exchange of information occupies an increasingly important position. Data communication is the main information exchange method, which is essential to ensure the security of data communication in the IoT [10].

Cloud computing can provide reliable basic software and hardware, abundant network resources, low-cost construction, and management capabilities, and is a concentrated expression of information technology development and service model innovation. A few years ago, people were hesitant about whether cloud computing and the IoT were new technologies and whether they were necessary for the development. Now, the industry has developed a high degree of recognition of cloud computing and the IoT. It can also be seen from Google trends that cloud computing has gone through a journey from scratch, as shown in Figure 1.

As shown in Figure 1, cloud computing and IoT have become one of the hottest topics of the moment. More mature cloud computing and IoT products such as Baidu Cloud and Alibaba Cloud have sprung up like mushrooms after a spring rain and have become an indispensable part of people's work, studies, and life [11]. IoT is a kind of network that connects any item to the Internet through information sensing equipment and according to the agreed protocol to exchange and communicate information, to realize intelligent identification, positioning, tracking, monitoring, and management. Increasingly, users are hosting their data on these cloud computing and IoT storage platforms for management. However, cloud computing and IoT security issues are increasingly prominent.

Cloud computing security is one of the most important issues affecting the development of cloud computing. Cloud computing not only includes security issues existing in existing IT systems but also faces new security risks based on cloud computing characteristics [12]. Concerns about security and data protection have become a stumbling block to the popularization of cloud computing services, especially concerns about data confidentiality, integrity, and compliance with regulations, as well as business confidentiality and data protection. However, current security technologies are based on traditional network structures and applications and cannot fully

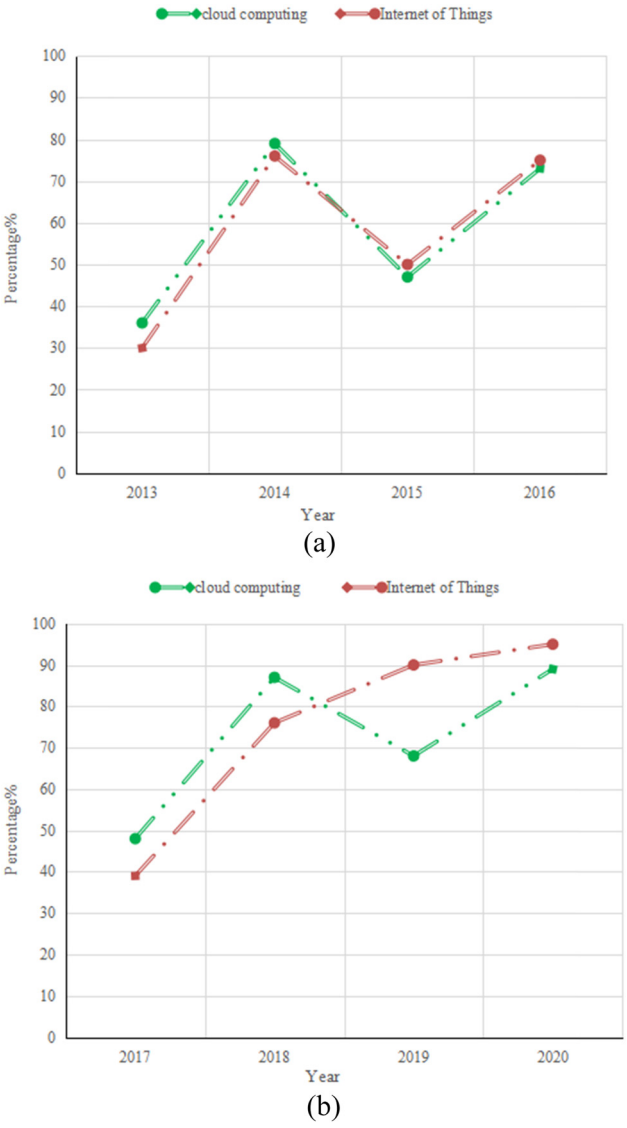

Figure 1: Cloud computing and IoT search index in Google. (a) 2013–2016 Cloud computing and IoT search index in Google; (b) 2017–2020 cloud computing and IoT search index in Google.

adapt to the new features of cloud computing such as borderless risk and shared risk [13], as shown in Figure 2.

As shown in Figure 2, on the one hand, most existing data sharing encryption schemes do not consider the communication overhead and workload of DOs and users; on the other hand, performing computations on encrypted shared data in the cloud has not been effectively addressed. In particular, the realization of influence maximization in social networks still faces significant challenges [14]. Now, information sharing is just in its infancy, and all aspects are not comprehensive, especially in law and regulations, there are still large loopholes, and there are increasingly lawbreakers, and they will increasingly use their drawbacks to harm the society.

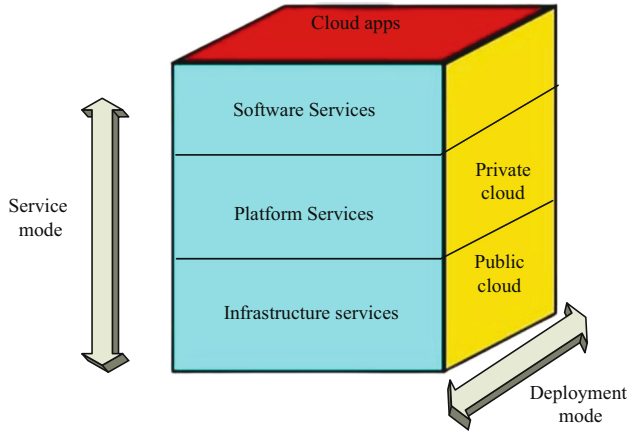

Figure 2: Cloud computing classification model.

3.2 Security issues of cloud computing-based data sharing platform under the IoT

3.2.1 Data transmission security issues

The continuous increase of data and sharing users will cause the workload of the DO to become quite large. Another alternative method is that the DO directly sends the decryption key to the user [15,16]. There are two types of keys: symmetric keys and asymmetric keys. Symmetric key encryption, also known as private key encryption or session key encryption algorithm, means that the sender and receiver of information use the same key to encrypt and decrypt data. Its biggest advantage is the fast encryption/decryption speed, which is suitable for encrypting large amounts of data. However, since the decryption key is usually bound to the identity information of the DO, this method will reveal all privacy of the DO. Therefore, none of the existing methods can simultaneously satisfy the DO's need for data security and workload issues. In these solutions, cloud services are only responsible for providing cloud storage, and their powerful computing power is not fully utilized [17].

3.2.2 Security issues brought about by shared technology

Usually, public CSPs have high-performance servers and powerful database software. The emergence of these public CSPs can effectively solve the problems of limited storage capacity and low computing power of personal and small enterprises. In the cloud environment, DOs outsource data to CSPs [18]. In real scenarios, most of the DOs are mobile terminal users, who will generate a large amount of data in real time when they use mobile devices with limited storage and low processing power. To obtain more storage space, DOs have to outsource the data to the public cloud. Mobile terminal users pay data transmission fees according to data traffic, so it is necessary for mobile terminal users to reduce communication overhead.

3.2.3 Defects in traditional public key infrastructure technology (KPT)

Cloud storage services provided by most cloud providers are not completely trustworthy to users. Furthermore, the traditional public KPT can ensure data confidentiality by encrypting data [19]. Public key infrastructure (PKI) is a system that uses public key technology to realize the security of e-commerce, and it is a kind of infrastructure, which is used to ensure the security of network communication and online transactions. However, there are several major defects in PKI technology. First, the data sender needs to know the valid public key certificates of all data receivers, which brings a large user management burden to the data sender; second, each data recipient needs a copy of the encrypted data, which results in data redundancy. At the same time, the encryption time is proportional to the number of data recipients, which brings about problems such as encryption time and communication consumption. Therefore, traditional encryption technology and access technology are not suitable for this new cloud data sharing model.

In short, traditional methods have various system bottlenecks, inflexible strategies, incomplete failure mechanisms, and high system overhead [20,21]. Based on the current research situation of the industry and the current application environment of cloud computing, this article proposes an efficient, flexible, and secure cloud data sharing model – the cloud data sharing model based on attribute encryption. This chapter mainly introduces the mathematical knowledge related to ABE. It explains the basic mechanism of attribute encryption and the calculation steps of attribute encryption scheme using various strategies.

3.3 ABE

ABE is embedded in the ciphertext because of the policy, which means that the DO can decide which attributes can access the ciphertext by setting the policy. It is equivalent

to making an encrypted access control on these data whose granularity can be refined to the attribute level. Elliptic curve encryption in cryptography uses limited elliptic curves. The finite elliptic curve represents the following equation:

$$b^2 = a^3 + ax + b. \tag{1}$$

All coefficients are elements of some finite field E_q. The most common of these is the following equation:

$$E_q(x, y)b^2 = a^3 + ax + b(\text{mod } q). \tag{2}$$

In crowd-sensing scenarios, DOs continuously generate and collect data over time. After a certain period of time, the data will exceed their own storage and processing capacity, so it is necessary to proxy the data to cloud management. At the same time, with the development of cloud computing, outsourcing data storage, management, and analysis to CSPs has become a necessary requirement for individuals and enterprises. However, DOs face a dilemma when sharing sensitive encrypted outsourced data with others. The access control system model based on attribute-based encryption algorithm is shown in Figure 3.

As shown in Figure 3, the participants include the authorization organization, the data sender, and the data user. Given the importance of privacy protection, encryption methods are widely used to protect the privacy of DOs when performing advanced functions on the cloud and should address privacy concerns. However, in the past, it was very difficult to perform functions on ciphertext encrypted with traditional cryptography tools. After the data are encrypted, the advanced functions provided by the cloud service will be limited, which reduces the quality of the cloud service to a certain extent. In addition, the needs of sharing users are often not limited to secure sharing, they need to perform computational functions on the shared data. However, after the data are encrypted, the implementation of complex computations such as influence maximization computation in social networks will face enormous challenges. The influence maximization problem is a function based on social network data mining, which aims to select a set of seed nodes, which has the greatest influence on the whole network through propagation. This technique has attracted a lot of research in the field of data mining.

The purpose of password control and key security management strategy is to ensure that appropriate and effective control measures are used to protect the confidentiality, authenticity, or integrity of information, and the main content includes the password control strategy. In the key policy scheme, the data user generates an access control policy based on his own attribute set, the authority calculates the user key according to the control policy, and the data sender uses the attribute set to encrypt the ciphertext. When the ciphertext attribute set satisfies the access control policy, the user can decrypt it. The control strategy is constructed into a tree structure as shown in Figure 4.

As shown in Figure 4, let the attribute set be P, the root node of the access tree T be R; the set pair accesses

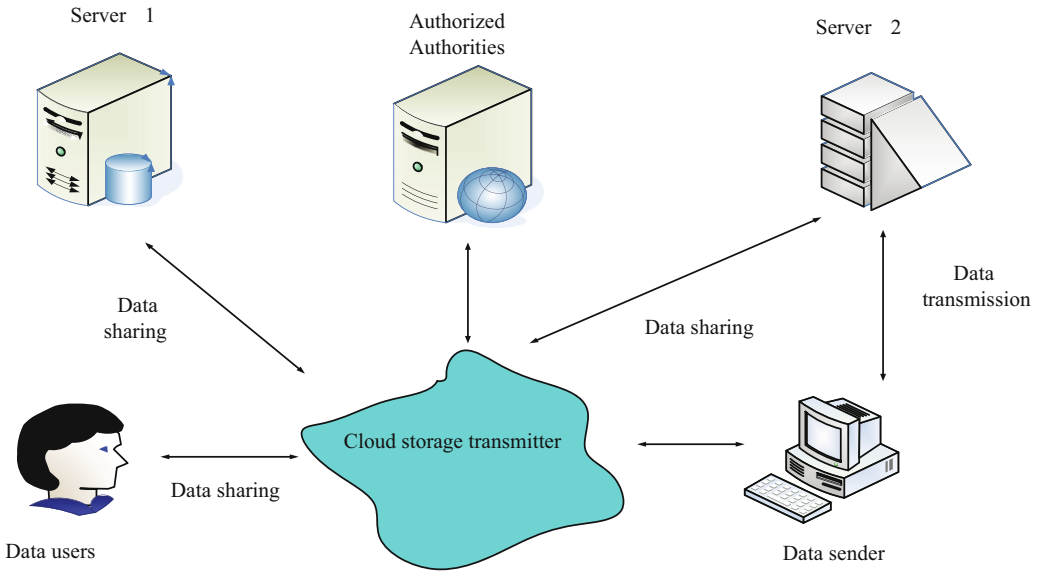

Figure 3: Attribute-based encryption algorithm.

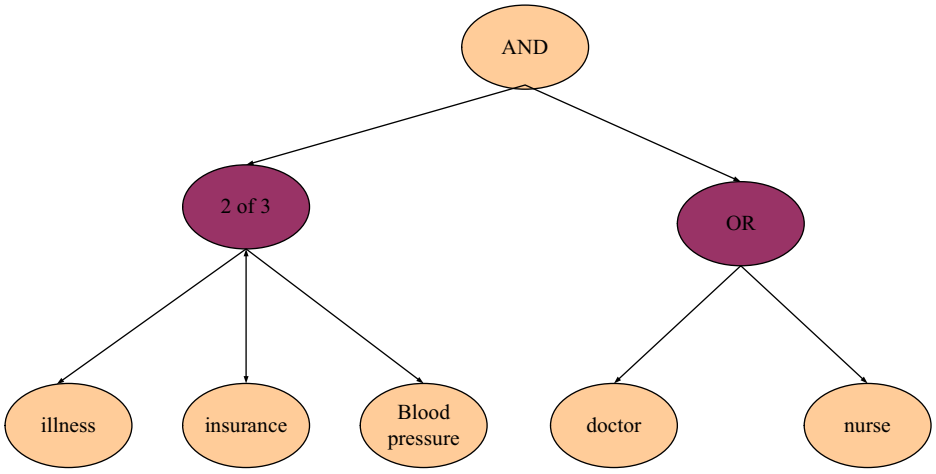

Figure 4: Access control tree.

tree T node; the difference between the ciphertext strategy ABE and the basic ABE mechanism lies in the KeyGen and decrypt steps. KeyGen is the abbreviation of KeyGenerator, which is generally referred to as the registration machine, which is a tool for piracy to generate the registration code required for software registration.

KeyGen: Generates a degree term for each node of a machine of T from top to bottom, such as the following equation:

$$P_a(0) = p_{\text{parent}(a)(\text{index}(a)),\text{othrewise}}. \tag{3}$$

Decrypt: It is a bottom-up recursive process, when x is a leaf node and as in the following equation:

$$F_a = e(D_a, E_i), i \in A_C. \tag{4}$$

In the ciphertext strategy scheme, the access control strategy T is specified by the data sender, and the control strategy adopts the same tree structure as the key strategy scheme. Its leaf node is $L(T) = A_{\text{ct}}$; the user key is associated with attribute set A_{ct}.

3.4 Data sharing system model

The degree of data sharing reflects the level of information development in regions and countries. The higher the degree of data sharing, the higher the level of information development. To realize data sharing, we must first establish a unified legal data exchange benchmark, standardize the data form, and use user-specified data benchmarks as much as possible. By implementing data sharing, more people can make full use of the existing data resources, which reduces the duplication of labor and the corresponding costs of data collection, and focuses on the development of new applications and system integration.

The data sharing system model consists of four parts: DO, CSPs, sharing users, and trusted third parties, as shown in Figure 5.

As shown in Figure 5, the data model accurately describes the shared system, data structure, data relationships, and semantic constraints. It defines the static characteristics, dynamic behavior, and dependency rules of the shared system at a higher level of abstraction, and is the core and foundation of the shared system. The data sharing system model includes the following parts: DO: Encrypt and outsource private data to the public cloud. Furthermore, it often wants to share its private data stored in the cloud with other authorized users. DO shares data with authorized users by defining a sharing policy and sends the sharing policy to a trusted third party to verify the sharing request.

CSP: Provides public cloud services. It has high-performance machines and powerful database software to store and manage data. The CSP also forwards the sharing user's sharing request to a trusted third party to verify the user's permission. In addition to this, CSP also provides upload, storage, and download services.

Attribute authority k generates master and public keys for each attribute it manages. Two exponents $v_{k,i}, v_{k,i}^* \in Z_q$ are randomly selected for attribute i, whose master key is the following equation:

$$\text{MSK}_{k,i}(v_{k,i}, v_{k,i}^*). \tag{5}$$

Key generation: Each data user needs to authenticate the identity to the authority that obtains the attribute key. The data user submits the identity number to the attribute authority k, and the authority verifies the identity of the

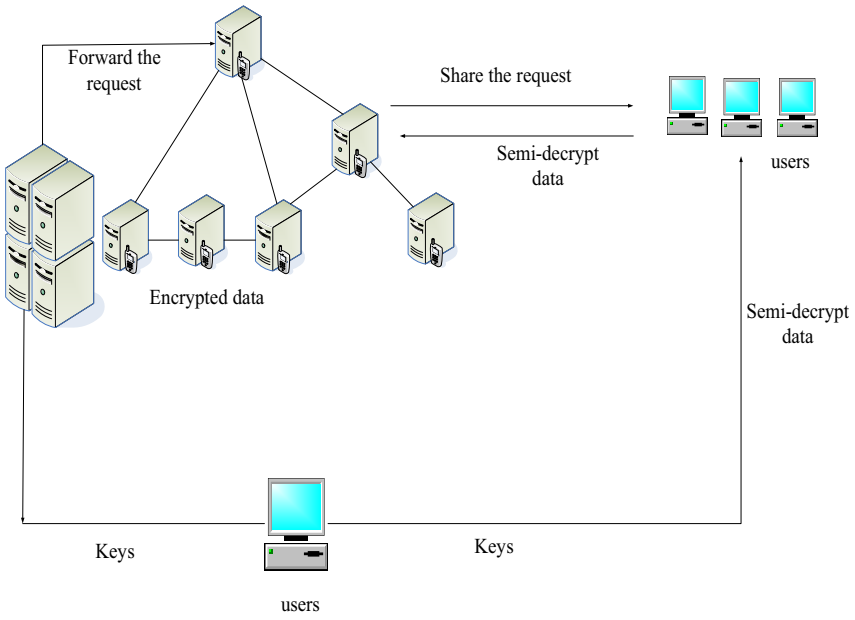

Figure 5: Key policy cloud data storage and sharing model.

data user through the identity authentication mechanism. If the data user GID is a legitimate user, the authority k assigns the user the attribute key associated with the requested attribute set.

The data encryption algorithm inputs the plain text m, the access control policy T, the global public parameters GPPs, and the public key PKs related to the leaf nodes of the tree T. The maximum coefficient of the polynomial is p_a, and p_a is the threshold value defined by the node, so that:

$$p_a(0) = \begin{cases} s, a = R \\ p^*_{\text{parent}(a)(\text{index}(a)), \text{othrewise}}. \end{cases} \tag{6}$$

Only the data users whose attribute set satisfies the access policy specified by the ciphertext CT can correctly decrypt the information m, and then use the key m to decrypt the symmetric encrypted data.

If the attribute set of the data user satisfies the access control tree T, then it can be calculated as:

$$A = e(g, H(\text{GID}))^{p_R(0)} = e(g, H(\text{GID}))^s. \tag{7}$$

Finally, the plaintext information $m = C/(A^*/A)$ can be decrypted.

ABE technology solves the system bottleneck and data redundancy problems caused by traditional technology. In the process of decryption, the user inputs the key embedded in the policy and the ciphertext embedded in the attribute set into the decryption algorithm. In this way, the matching between the policy and the attribute set is realized.

3.5 Privacy protection scheme of nonlinear mapping order preserving encryption

Cloud storage supports uploading and downloading of any type of data (text, multimedia, log, binary, etc.). It can provide a powerful meta-information mechanism, and developers can use general and custom meta-information mechanisms to define resource attributes. However, the realization of data sharing, an important function of cloud storage, has not been effectively solved. Most of the existing solutions focus on the control of users' access rights without considering the communication overhead and workload problems between DOs and users in data sharing. In practical scenarios, users who use public cloud services often need to pay expensive communication fees, and the computing processing power is relatively low.

Order-preserving encryption has become an important tool for building searchable encryption systems, which allows efficient query operations on ciphertexts, which is very much in line with the requirements for operational security and confidentiality in cloud environments. The research of outsourced data query and data mining under privacy protection makes order-preserving encryption very promising in encrypted data search. After the encrypted data are stored on the remote server, the comparison operation is performed by sending another encrypted data, and the security of the data and query can be ensured during all operations, as shown in Figure 6.

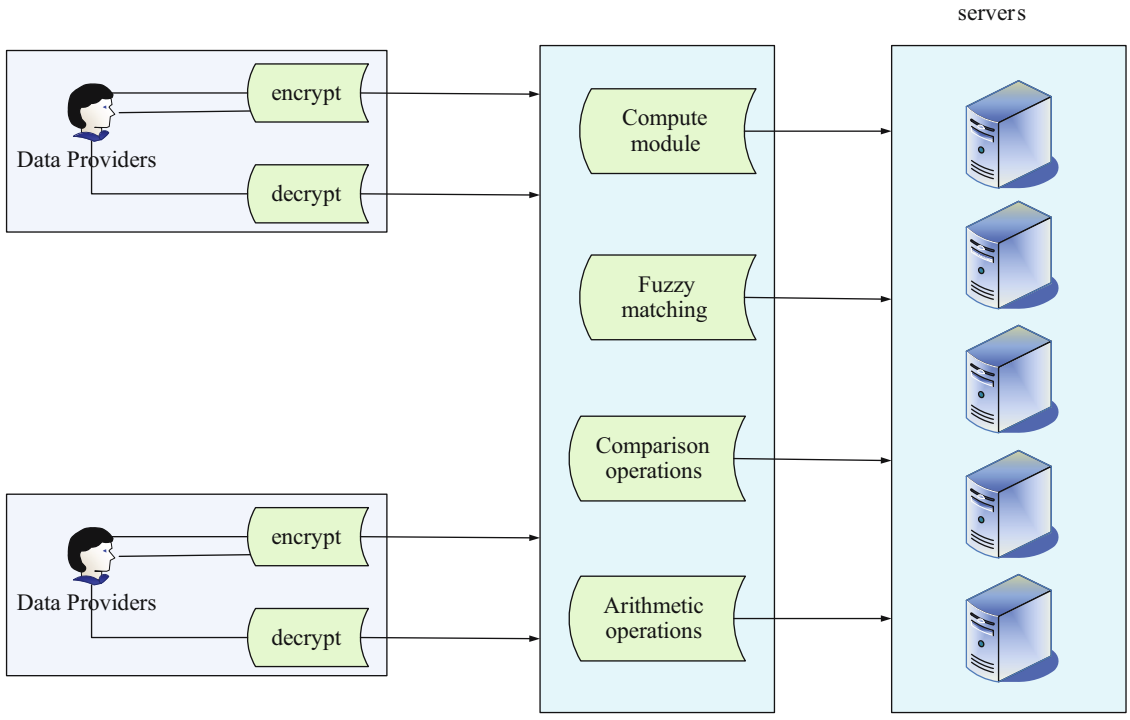

Figure 6: Problem model.

As shown in Figure 6, users and data providers can protect the privacy of data by encrypting confidential data and parameters. If this problem cannot be effectively solved, users will not be able to use the computing resources of cloud computing to process confidential data, and the advantages of cloud computing will be weakened. The advantages of cloud computing are ultra-large scale, virtualization, high reliability, versatility, high scalability, on-demand services, and extremely cheap.

Divide the original plaintext space M into a series of 1 s, as in the following equation:

$$M = \bigcup_{i=1}^{m} D_i = \bigcup_{i=1}^{m} [l_i, r_i]. \tag{8}$$

It divides the ciphertext space C into a series of intervals $C_i = [l_i', r_i']$, so one lets $l_i', r_i' \in Z$ satisfy the following conditions, as in the following equation:

$$C = \bigcup_{i=1}^{m} C_i = \bigcup_{i=1}^{m} [l_i', r_i']. \tag{9}$$

For different intervals, people use different encryption functions $\mathrm{Enc}_i(a)$ to map different values to the target space $C_i = [l_i', r_i']$. The overall process is as shown in the following equation:

$$a \in D_i = [l_i, r_i] \rightarrow \mathrm{Enc}_i(a) \in C_i. \tag{10}$$

The sparse interval extends to a small extent into the ciphertext space, so the ciphertext is almost uniformly distributed. To realize the division, this article gives these parameters as follows:

$$P = (a_{\min}, a_{\max}, [T_i], d_{\min}). \tag{11}$$

$a_{\min}$ and $a_{\max}$ are the starting points of the plaintext, and $[T_i]$ represents the set of dense intervals. To break the data distribution, $d_{\min}$ is the smallest length interval one can set. The specific division method: people make the plaintext space as the following equation:

$$M = R_1 + T_1 + R_2 + T_2 + \cdots + T_n + R_{n+1}, \tag{12}$$

where R_{n+1} is the sparse interval, people randomly choose integers to divide the interval into equal intervals, and for the dense interval $T_i = [l_i, r_i]$, people divide it into the following equation:

$$T_i = d_{\min} + n \cap \ldots \cap d_{\min}. \tag{13}$$

3.6 Data sharing platform security

In terms of time overhead, the ABE only needs to encrypt the file when uploading the file for the first time, which

can save the user's time. In addition, the sizes of the plaintext file and the ciphertext file are not much different. For simple access control structure, the difference is 4 kB, and for complex access control structure, the difference is 30 kB. Storage overhead can be ignored in ABEs.

If the order-preserving encryption scheme is correct, it must meet the following conditions:

$$\forall m \in D, \exists \mathrm{Dec}(k\mathrm{Enc}(a_1) \succ \mathrm{Enc}(a_2)), \tag{14}$$

$$\text{if } a_1 \succ a_2 (a_1, a_2 \in D), \mathrm{Enc}(a_1) \succ \mathrm{Enc}(a_2). \tag{15}$$

If two adjacent numbers are not in the same interval, the intersection of the two intervals is a_0, then $E(a_1) \prec E(a_0)$, $E(a_0) \prec E(a_2)$, then $E(a_1) \prec E(a_2)$, so the scheme is order-preserving. To sum up, the order preservation scheme is correct. When A passes the average distance, there is the following formula:

$$d = \frac{(\mathrm{Enc}(a_k) - \mathrm{Enc}(a_1))}{(k-1)}. \tag{16}$$

When guessing the value of a, since the scheme is a nonlinear map $b = ax^3 + b$, the ciphertext is very different from the reference function, such as the following equation:

$$f(a) = E\mathrm{nc}(a_1) + (a - a_1)d. \tag{17}$$

When two adjacent points are in the same interval, as in the following equation:

$$d' = x_i(a_i + 1)^3 + b_i - a_j(a_i)^3 - b_j. \tag{18}$$

It makes it difficult for A to judge the size of the range. Therefore, the dominant probability of A is the following equation:

$$\mathrm{Adv}(A) = |pr[b' = b] - 0.5| = \varepsilon. \tag{19}$$

In practical applications, it is of great significance to ensure the forward and backward security of data. For example, in transactions between companies, it must be possible to ensure that newly joined partners can only obtain the information after joining and cannot obtain the previous information. The algorithm in this article can satisfy the above characteristics.

Cloud computing is an emerging computing model, which involves large-scale, distributed computing of multiple data sources. Computing devices can provide users with the computing power they need, and users can move their business to the cloud to reduce investment. People can store data files in the cloud environment to realize data sharing, which is the data sharing system. When users outsource their own information data to cloud servers, the security of records and access control face great challenges.

To solve the aforementioned problems, people can encrypt the data files in the data sharing system based on cloud computing. Traditional encryption techniques are not suitable for data sharing systems. Symmetric encryption is very efficient, but requires a system to manage access control. In ABEs, the access control policy depends on the attributes of the user, the environment, or the data itself, and data files can also be encrypted. Attribute-based encryption algorithms can use access control policies to access encrypted data, and the user's private key and ciphertext are associated with attributes. The overall framework of the data sharing platform is shown in Figure 7.

As shown in Figure 7, with the development of technology, the speed of online information and circulation is accelerated, and the efficiency is getting higher and higher, and increasingly enterprises, governments, and individuals are engaged in network-related activities such as e-commerce. Network-based business cooperation and data exchange are becoming increasingly important in the government's science and technology departments or in e-government, technology business, etc., between government departments. Due to shared and interconnected network resources, the Internet faces various security threats, such as information theft, illegal alterations, malicious deception, disguise, etc. More secure data sending and sharing is essential for the development of data exchange technology.

4 Experiment based on attribute-based encryption algorithm

4.1 Experiment preparation based on attribute-based encryption algorithm

The experimental environment of this article is built on Cygwin, which simulates the Linux environment under Windows system, and the memory capacity is 4 GB. Their implementation is on a 512-bit finite field, and the experimental code is written based on the cpabe-0.11 library and the Kpabe library, among which the ABE is less efficient. People first encrypt the file symmetrically, and then encrypt the symmetric encryption key using the attribute-based encryption algorithm, which uses the 128-bit AES encryption algorithm. This article compares the ABE

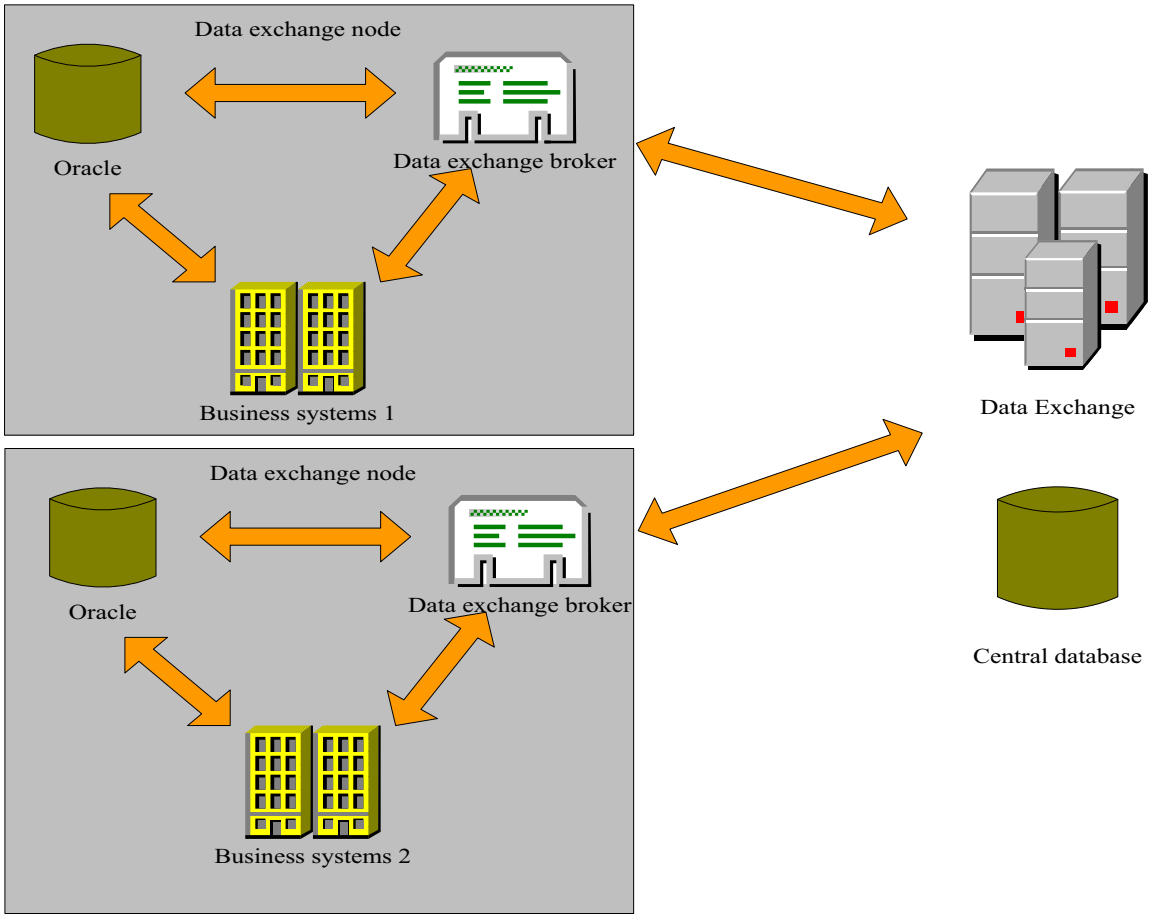

Figure 7: Schematic diagram of the structure of the data exchange center.

mentioned in the article with other classical encryption schemes including Popa'13 and Liu'16.

To test the key generation time, encryption time, and decryption time of the scheme, two text files (1 and 5 MB) were used for testing. The linear relationship between the key generation time and the number of attributes is shown in Figure 8.

As shown in Figure 8, for the encryption algorithm, the running time changes with the change of the leaf nodes in the access structure tree. The encryption efficiency of the ABE is clearly better than that of Popa'13 and Liu'16, because Popa'13 and Liu'16 need to perform a second operation when the ABE performs an exponentiation operation, as shown in Figure 9.

As shown in Figure 9, for the decryption algorithm, the most expensive is the bilinear mapping. The modified scheme is more efficient than the original scheme because Popa'13 and Liu'16 perform quadratic bilinear mapping while ABE performs one bilinear mapping. The comparison chart of ciphertext and key update time is shown in Figure 10.

As shown in Figure 10, the ABE is slightly better than Popa'13 and Liu'16 in both ciphertext update and key update. Because in ABEs, there is a linear relationship between the time cost of each step of user revocation and the number of authorized authorities, the number of allowed authorities is fixed at system initialization. The time required to update the ciphertext and update the key with this scheme is very small and constant.

4.2 Performance of ABEs and Popa'13 and Liu'16 algorithms

People use 100 data to test the actual performance of the three algorithms, test the execution time of the three algorithms, and their average efficiency, as shown in Tables 1–3.

As shown in Tables 1–3, clearly, compared with Popa'13 and Liu'16, due to the reduction of the number of exponentiations in the ABE, the efficiency is significantly

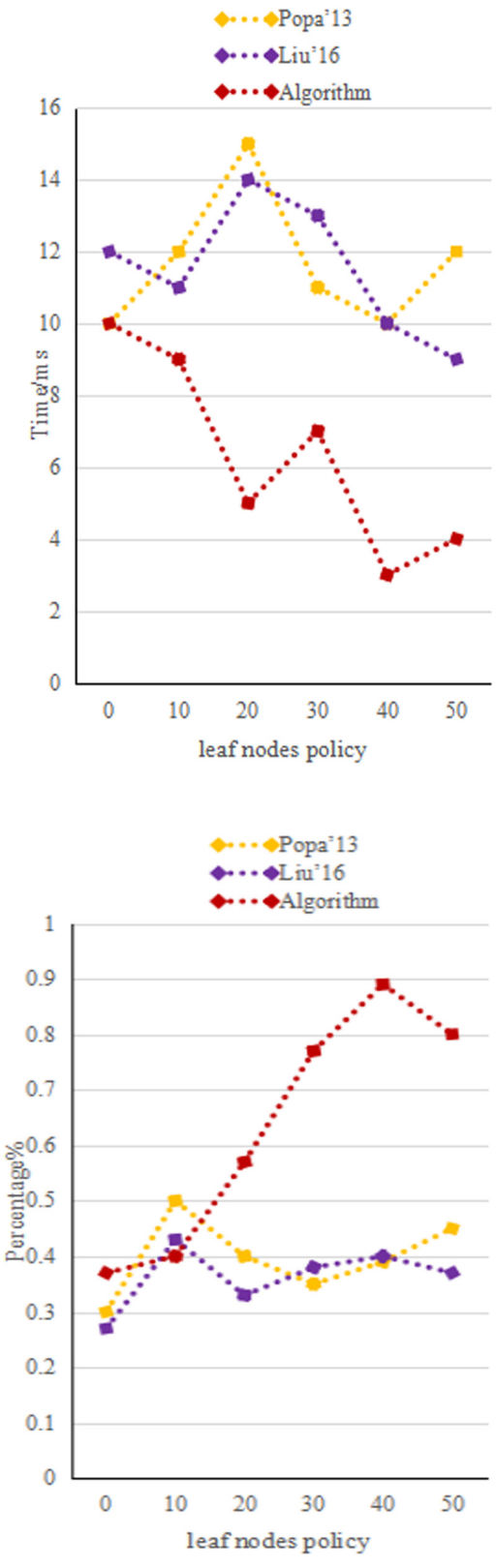

Figure 8: Comparison of (a) key generation time and (b) encryption efficiency of the three algorithms.

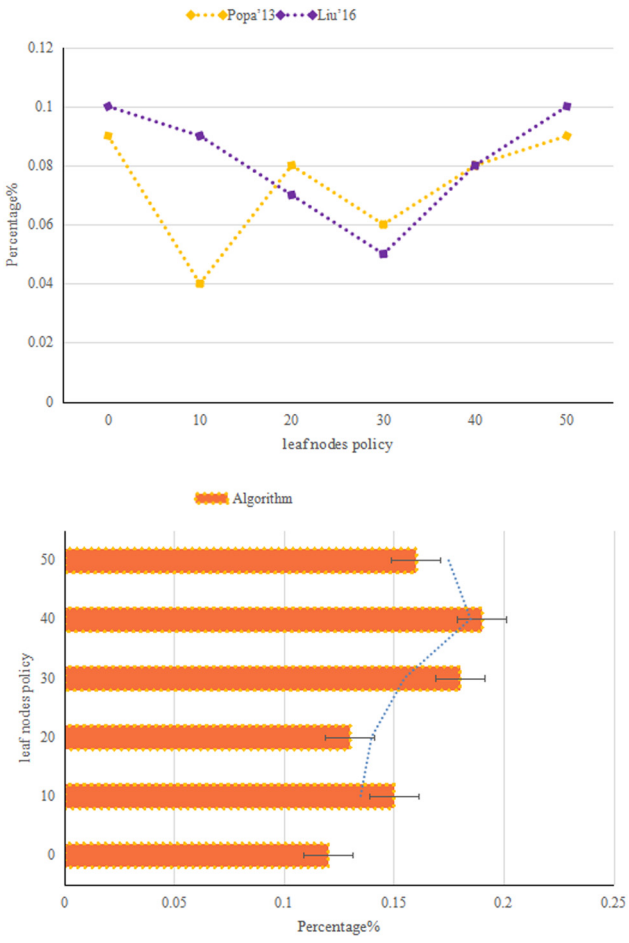

Figure 9: Comparison of decryption efficiency of three algorithms.

higher than the original scheme. The efficiency of Popa'13's scheme is worst, the remaining two schemes have the same efficiency, the scheme execution time is short, and the efficiency is high. The ABE achieves an ideal security state, and compared with the Liu'16 algorithm, the ABE achieves higher security. Although ABEs lose the ordering encryption properties used to directly compare ciphertext data, they do not achieve the same ideal security as Popa'13's scheme. However, it is distributed and data frequency improves the security of the encryption scheme. The comparison of the order-preserving encryption of the three encryption algorithms is shown in Table 4.

As shown in Table 4, in the context of increasingly mature cloud computing and distributed computing technologies, cloud computing provides economically convenient services for individuals and enterprises and provides power for development in all fields. This article provides a detailed analysis of the data access control system model based on cloud storage services. The model

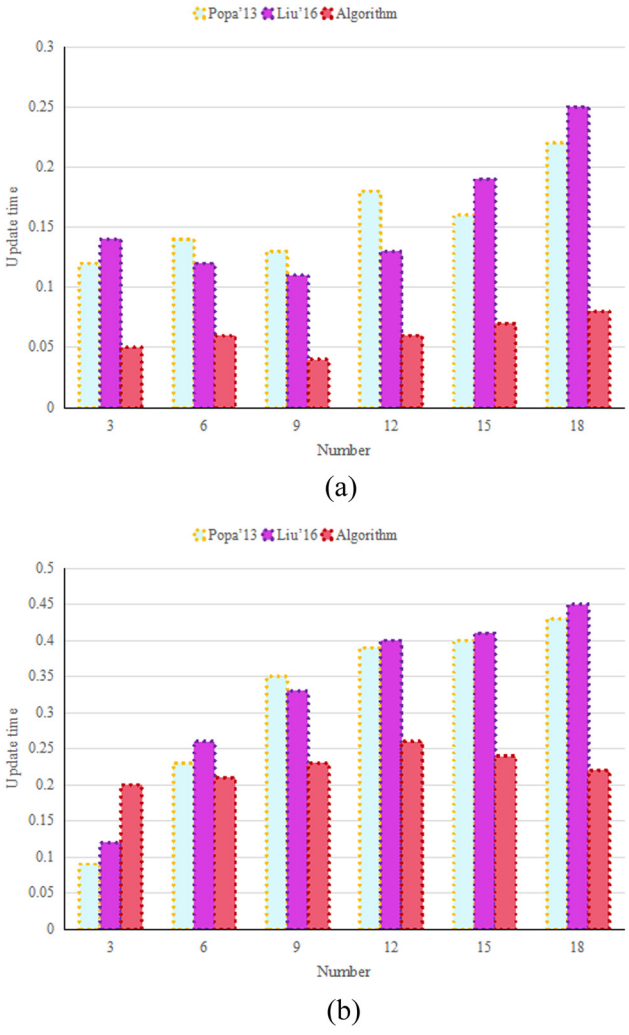

Figure 10: Comparison of ciphertext and key update time. (a) Comparison of ciphertext update time and (b) comparison of key update time.

Table 1: Popa'13 time and efficiency required for different encryption numbers under the same data

Encrypted number	Execution time (ms)	Effectiveness (%)
1	40	25
2	53	18
3	56	16
4	59	17
5	51	20
Average time	51.8	19.2

needs to allow only the allowed data users to decode and access the data. And it also analyzed that the current access control technology cannot be well applied to the cloud data sharing scheme. Its main disadvantages are the reliance on reliable third party: the large management burden of data providers, data redundancy, data sharing, and a series of security issues.

Table 2: Time and efficiency required by Liu'16 for different encryption numbers under the same data

Encrypted number	Execution time (ms)	Effectiveness (%)
1	30	33.3
2	35	28.5
3	33	30.3
4	31	32.2
5	29	34.5
Average time	31.6	31.6

Table 3: Time and efficiency of ABE under different encryption numbers under the same data

Encrypted number	Execution time (ms)	Effectiveness (%)
1	12	83.3
2	10	87
3	11	90.9
4	13	76.9
5	9	87.5
Average time	11	90.0

Table 4: Comparison of order-preserving encryption of three encryption algorithms

Algorithm	Efficiency class	Security level	Programmability
ABEs	O(n)	SA,IND-DNCPA	high
Popa'13	O($n$log$n$)	IND-0CPA	Low
Liu'16	O(n)	SR-CPA	high

5 Conclusions

This article analyzes and summarizes the difficulties of the existing encryption schemes in solving the secure sharing and computability of external data, and the existing impact maximization schemes in maximizing the impact of encrypted data in the cloud environment. In view of the problem of high computing and communication cost DOs and sharing users, the scheme of attribute-based encryption algorithm for data security sharing is put forward. In Section 3, this article provides a clear interpretation around the concept of cloud computing and data sharing and provides a detailed description of the ABEs. In Section 4, the ABE and traditional two-encryption

algorithm are compared, the experiments proved that ABE, whether on working time or work efficiency, is more efficient than the traditional two encryption algorithms. Therefore, ABE can be well used in the IoT under cloud computing-based data sharing platform security mechanism research. This is very meaningful, but because the author's strength is limited, there are some loopholes in many contents.

Conflict of interest: Authors state no conflict of interest.

Data availability statement: This article does not cover data research. No data were used to support this study.

References

[1] L. Jin, Y. Zhang, X. Chen, and X. Yang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Comput. Sec.*, vol. 72, no. JAN, pp. 1–12, 2018.

[2] T. F. Xue, Q. C. Fu, C. Wang, and X. Y. Wang, "A medical data sharing model via blockchain," *Zidonghua Xuebao/Acta Auto Sin.*, vol. 43, no. 9, pp. 1555–1562, 2017.

[3] Z. Liu, T. Li, P. Li, C. F. Jia, and J. Li, "Verifiable searchable encryption with aggregate keys for data sharing system," *Future Gener. Comput. Syst.*, vol. 78, no. PT.2, pp. 778–788, 2017.

[4] C. Jiang, L. Gao, L. Duan, and J. Huang, "Scalable mobile crowdsensing via peer-to-peer data sharing," *IEEE Trans. Mob. Comput.*, vol. 17, no. 4, pp. 898–912, 2017.

[5] K. Xue, J. Hong, Y. Ma, D. S. L. Wei, P. Hong, and N. Yu, "Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing," *IEEE Netw.*, vol. 32, no. 3, pp. 7–13, 2018.

[6] G. A. Ascoli, P. Maraver, S. Nanda, S. Polavaram, and R. Arma, "Win-win data sharing in neuroscience," *Nat. Methods*, vol. 14, no. 2, pp. 112–116, 2017.

[7] L. Liu, W. Kong, Z. Cao, and J. Wang, "Analysis of one certificateless encryption for secure data sharing in public clouds," *Int. J. Electron. Inf. Eng.*, vol. 6, no. 2, pp. 110–115, 2017.

[8] B. Marwick and S. Birch, "A standard for the scholarly citation of archaeological data as an incentive to data sharing," *Adv. Archaeolog Pract.*, vol. 6, no. 2, pp. 1–19, 2018.

[9] H. Zhao and D. Nan, "Dynamic analysis of stochastic Cohen–Grossberg neural networks with time delays," *Appl. Math. Comput.*, vol. 183, no. 1, pp. 464–470, 2017.

[10] P. Mark, "International data-sharing norms: from the OECD to the general data protection regulation (GDPR)," *Hum. Genet.*, vol. 137, no. 8, pp. 575–582, 2018.

[11] M. Segler, T. Kogej, C. Tyrchan, and M. P. Waller, "Generating focused molecule libraries for drug discovery with recurrent neural networks," *Acs Cent. Sci.*, vol. 4, no. 1, pp. 120–131, 2018.

[12] B. M.Knoppers and Y.Joly, "Introduction: the why and whither of genomic data sharing," *Hum. Genet.*, vol. 137, no. 8, pp. 569–574, 2018.

[13] M. Sepehri, A. Trombetta, and M. Sepehri, "Secure Data Sharing in Cloud Using an Efficient Inner-Product Proxy Re-Encryption Scheme," *J. Cyber Secur. Mobil.*, vol. 6, no. 3, pp. 339–378, 2018.

[14] A. Thorogood and B. M. Knoppers, "Can research ethics committees enable clinical trial data sharing? *Ethics Med. Public. Health*, vol. 3, no. 1, pp. 56–63, 2017.

[15] J. Montgomery, "Data sharing and the idea of ownership," *N. Bioeth.*, vol. 23, no. 1, pp. 81–86, 2017.

[16] M. M. Mello, L. Van, and S. N. Goodman, "Clinical trial participants' views of the risks and benefits of data sharing," *N. Engl. J. Med.*, vol. 378, no. 23, pp. 2202–2211, 2018.

[17] K. B. Read, L. Amos, L. M. Federer, A. Logan, and K. G. Akers, " Practicing what we preach: developing a data sharing policy for the journal of the medical library association," *J. Med. Lib. Assoc. JMLA*, vol. 106, no. 2, pp. 155–158, 2018.

[18] C. H. George, S. C. Stanford, S. Alexander, G. Cirino, J. R. Docherty, and M. A. Giembycz, "Updating the guidelines for data transparency in the British Journal of Pharmacology – data sharing and the use of scatter plots instead of bar charts," *Br. J. Pharmacol.*, vol. 174, no. 17, pp. 2801–2804, 2017.

[19] H. Rodriguez and S. R. Pennington, "Revolutionizing precision oncology through collaborative proteogenomics and data sharing," *Cell*, vol. 173, no. 3, pp. 535–539, 2018.

[20] K. Bhuvaneshwar, A. Belouali, S. Rao, A. Alaoui, Y. Gusev, and R. Clarke, "Abstract 2604: The Georgetown Database of Cancer (G-DOC): A web-based data sharing platform for precision medicine," *Cancer Res.*, vol. 77, no. 13 Supplement, pp. 2604–2604, 2017.

[21] T. Doel, D. I. Shakir, R. Pratt, M. Aertsen, J. Moggridge, and E. Bellon, "GIFT-Cloud: A data sharing and collaboration platform for medical imaging research," *Comput. Methods Prog. Biomed.*, vol. 139, no. Complete, pp. 181–190, 2017.