INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research

International Journal of Autonomous and Adaptive Communications Systems

ISSN online: 1754-8640 - ISSN print: 1754-8632
https://www.inderscience.com/ijaacs

Access control method of laboratory cloud data based on internet of things technology

Liuyang Wang, Yangxin Yu

DOI: 10.1504/IJAACS.2023.10052878

Article History:

Received:	17 April 2020
Accepted:	01 September 2020
Published online:	17 March 2023

Copyright © 2023 Inderscience Enterprises Ltd.

Access control method of laboratory cloud data based on internet of things technology

Liuyang Wang* and Yangxin Yu

Faculty of Computer & Software Engineering,
Huaiyin Institute of Technology,
Huai'an 223003, China
Email: liuyang@mls.sinanet.com
Email: 381536880@qq.com
*Corresponding author

Abstract: In order to solve the problems of low access efficiency and poor security in the access control method of laboratory cloud data in the environment of internet of things, this paper proposes the access control method of laboratory cloud data based on internet of things technology. It decomposes the data in the laboratory cloud database into the minimum attributes, encrypts the attributes of the acquired laboratory cloud data, and generates the minimum granularity key that meets the access tree constraints. It combines the internet of things technology and proxy re encryption technology, maps the access structure and attribute set through hash function, encrypts the symmetric key with CP-ABE scheme, and realises the number of laboratory clouds According to the access control method. The simulation results show that the minimum memory cost of the proposed method is 524 bytes, and the highest efficiency is about 98%.

Keywords: internet of things technology; laboratory cloud data; access control; hash function; key encryption; CP-ABE scheme; minimum granularity key.

Reference to this paper should be made as follows: Wang, L. and Yu, Y. (2023) 'Access control method of laboratory cloud data based on internet of things technology', *Int. J. Autonomous and Adaptive Communications Systems*, Vol. 16, No. 1, pp.31–47.

Biographical notes: Liuyang Wang received his Master degree in Nanjing University of Science & Technology in 2009. He is currently an Associate Professor in the Faculty of Computer & Software Engineering of Huaiyin Institute of Technology. His research interests include information management and information system, intelligent information processing, data mining.

Yangxin Yu received his Master degree in Suzhou University in 2007. He is currently a Professor in the Faculty of Computer & Software Engineering of Huaiyin Institute of Technology. His research interests include information management and information system, intelligent information processing, knowledge organisation.

Copyright © 2023 Inderscience Enterprises Ltd.

1 Introduction

With the rise and continuous development of new technologies such as cloud computing, internet of things and big data, using them to obtain infrastructure services (IAAs), platform services (PAAS) and software services (SaaS) has become a common way of using network resources (Yan et al., 2016; Zhao et al., 2016). Laboratory cloud data security is one of the main challenges of cloud computing, and laboratory cloud data access control is one of the most important methods to ensure data security (Zheng et al., 2016). In the access control of laboratory cloud data, data resources are often not directly controlled by users. In this complex access security environment, how to ensure the security and efficiency of cloud data access control has become a hot issue in this field (Zhao et al., 2019; Yu et al., 2016).

Peng et al. (2016a) put forward a cloud data access control method for cloud storage experiment. Through the data owner to protect the rights and release the secret key for different users, the corresponding attribute conditions are set for the data ciphertext, and the decryption ability of the method is determined by the corresponding attribute. Liu Qiang et al. also carry out research on the laboratory cloud data access control technology. Combined with the management requirements of the laboratory cloud data, a new access control model is designed and proposed. The model can effectively access the cloud data of the laboratory, but the encryption level of the data needs to be strengthened, and the information security is difficult to guarantee. Cao et al. (2019) proposes a method of cloud data access control in the laboratory. Under the prospect of continuous development of cloud computing technology, the automatic operation and maintenance system of data centre construction can better adapt to the needs of new environment, so as to achieve the purpose of cloud data access control in the laboratory. This method can realise the access control of cloud data in the laboratory, but the operation process of this method is complex and it is difficult to improve the work efficiency. Liu et al. (2016a) put forward an access control method based on encryption system in private cloud environment. This method introduces the traditional access control principle and typical model, analyses the application characteristics in the private cloud environment, on this basis, proposes the access control application scheme based on the encryption system, and analyses its application process. This method can guarantee the security of cloud data resources in the laboratory, but it is not suitable for the general use because of its little consideration on the control of cloud data in the laboratory.

Based on the above problems, this paper proposes the access control method of laboratory cloud data based on internet of things technology. By introducing the technology of internet of things and encrypting and authorising the laboratory cloud data, the access control analysis of the laboratory cloud data is completed. Through the simulation experiment, it is verified that the proposed method can effectively access the laboratory cloud data and ensure the security of the laboratory cloud data.

2 Attribute decomposition and encryption of laboratory cloud data

2.1 Attribute decomposition of laboratory cloud data

In the access control of laboratory cloud data, the method of attribute decomposition is adopted to decompose the data in the laboratory cloud database to the minimum attribute. Attribute decomposition is to ensure that when there is no dynamic encryption key, the decomposed attributes cannot be obtained at the same time. The privacy constraint rules of single attribute are implemented by separate dynamic encryption, while the privacy constraint with association relationship needs dynamic encryption of its attributes in the mode of attribute decomposition.

Supposing that there is a data relationship pattern of P in the laboratory cloud data, and its privacy constraint rule is Y, $\forall U = \{U_1, U_2\}$. When the positive attribute of the privacy constraint rule of P is satisfied, U_1 stores the encrypted attribute, and U_2 stores the non-encrypted attribute, and $U_1 \cap U_2 \cong \hbar, U_1 \cup U_2 = P,$ then $\forall y_i \in Y,$ and $y_i \notin U_2$.

When the laboratory cloud data is stored, the attribute $U = \{U_1, U_2\}$ of the data will be mapped to all the physical layers including the P attribute to achieve the connection of the laboratory cloud data.

Let $P = \{p_1, p_2, \ldots, p_n\}$ be the initial relationship of laboratory cloud data, and $U = \{U_1, U_2\}$ be its positive attribute decomposition.

Then the physical layer decomposition attribute is $P' = \{r, p_1, p_2, \ldots, p_n\}$, where r is the encryption attribute of P decomposition to U_1.

The decomposition of the data in the cloud database of the laboratory requires the least amount of computation, so the efficiency of data decomposition will be improved. Assuming that the size of laboratory cloud data is *size* p_i, the amount of U_1 data in attribute decomposition is:

$$size\ U_1 = \sum p_{i \in u^{size(p_i)}} \tag{1}$$

The minimum encryption case attribute decomposition of laboratory cloud data satisfies that there is no positive attribute decomposition is less than positive attribute decomposition, and the minimum attribute decomposition of data in laboratory cloud database can be completed.

Due to the large amount of data accessed by the laboratory cloud data, a large number of different nature keys will be generated when decomposing the data relationship attributes of the cloud data. If each key is stored, the storage space of the system will be increased. Therefore, the laboratory cloud data attributes need to be encrypted to save storage space and ensure the security of access.

2.2 Encryption of laboratory cloud data attributes

Laboratory cloud data access control is a logical structure to describe ciphertext access control strategy, which is mainly used to set authorised access set and unauthorised access set of encrypted data (Guo et al., 2017). Attribute encryption mainly combines access structure and identity encryption to ensure fine-grained access control of data.

Let $P = \{P_1, P_2, \ldots, P_n\}$ represent the set of n participants, and $\Gamma \in 2^P$ represent the set of subsets of each participant. Supposing that the set Γ is monotonic, where Γ needs to satisfy the following constraints:

For any B and C, let B ∈ Γ and B ⊆ C. Therefore, a single access structure is mainly composed of non empty participants and a subset of participants, namely:

$$\Gamma \subseteq 2^{\{P_1, P_2, \cdots, P_n\}} \tag{2}$$

Among them, the set of Γ in the access structure is called authorised set (Zhang et al., 2018a), and the set in different access structures is called unauthorised set.

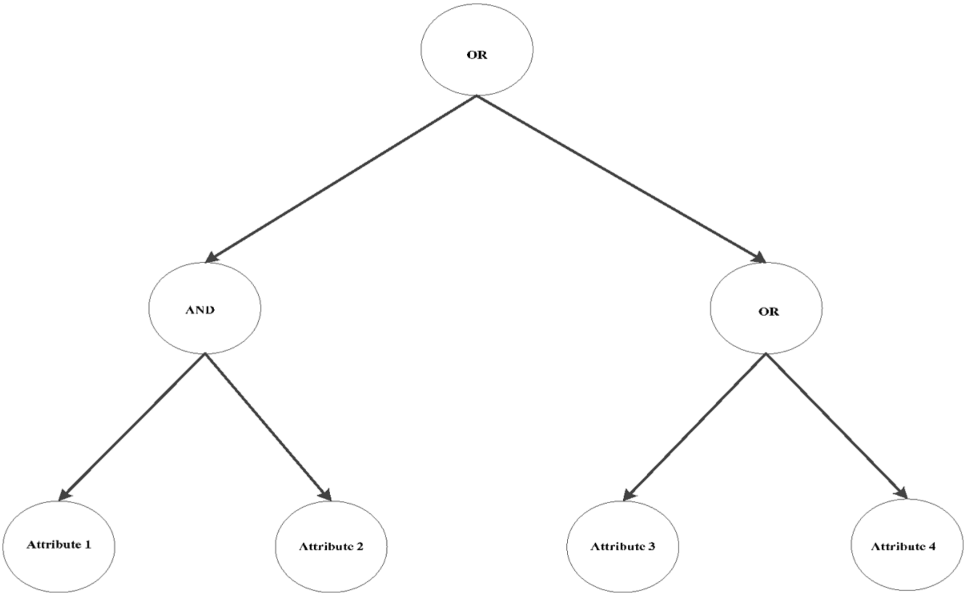
In the laboratory cloud data access control based on the internet of things technology, the system threshold is set to t, the attribute set associated with the identity user is w, and the attribute set associated with the ciphertext is w^*. If $|w \cap w^*| \geq t$, it shows that w can satisfy the corresponding access structure and realise the decryption of ciphertext. When the ciphertext is formed, the attribute set can be divided into two types, namely:

- for authorised access set, the user's attribute set needs to meet the following constraints: $|w \cap w^*| \geq t$
- for unauthorised access to the set, the user's property set needs to meet the following constraints (Wang and Yin, 2017): $|w \cap w^*| < t$.

After the encryption of lab cloud data attributes, the access to lab cloud data is often restricted by the threshold constraints of data attributes, which leads to the failure of smooth access to lab cloud data. Therefore, this paper analyses the constraints of the laboratory cloud data through the access tree constraints, in order to have the ability of user attribute level revocation in the access control of the laboratory cloud data, and to ensure the access control rights of users.

Let T represent the access tree, and the non-leaf nodes of each access tree can be represented by the (k_x, num_x) threshold structure, where, num_x represents the number of child nodes of node x (Han et al., 2016), and k_x represents the corresponding threshold. The specific structure of the access tree is shown in Figure 1.

Figure 1 Access tree structure



Let T represent the access tree whose root node is *r*, and T_x represent the subtree whose root node is *x* (Sun and Zhang, 2016). Through correlation analysis, it can be seen that there is the same form between the T_x and T_r. Let the attribute set *w* meet the access tree T_x, at this time:

$$T_x = 1 \tag{3}$$

Recursive calculation is required. The specific calculation steps are as follows:

Step 1: assuming that *x* represents a non-leaf node. The value of T_{x^*} of all child nodes x^* in *x* is estimated. Only when the number of child nodes is more than k_x, T_{x^*} returns 1.

Step 2: assuming that *x* represents leaf node. When the attribute attr(*x*) associated with leaf node *x* is an element in attribute set *w*, that is, attr(*x*) ∈ *w*, the value of T_{x^*} returns 1.

On the basis of the above analysis, the Lagrangian difference formula is used for calculation.

Let *f*(*x*) represent a polynomial of order *n*. Supposing that different points (x_i, $f(x_i)$) of the polynomial *f*(*x*) are given. Then, formula (3) is used to determine the corresponding polynomial of any *x*, that is:

$$f(x) = \sum_{i=1}^{n} f(x_i) \left(\prod_{1 \le k} (x - x_k) / (x_i - x_k) \right) \tag{4}$$

The Lagrange coefficient can be expressed as:

$$\Delta_{i,x}(x) = \prod_{i \in S} \frac{x - j}{i - j} \tag{5}$$

The whole secret sharing scheme based on Lagrange interpolation formula (Song et al., 2016) is mainly composed of the following three parts, respectively:

(1) System initialisation:

Let the secret distributor of the laboratory cloud data be D, and the shared secret information be s. The secret share space and the secret space all exist on the finite field Z_p, $P = \{P_1, P_2, \ldots, P_n\}$ represents *n* participants. Let *p* represent a large prime number, and the threshold value represent *t*. In the finite field, *n* numbers $d_1, \ldots, d_c$ with different values are selected, and them are set as the identity of participants.

(2) Formation of sub secret:

The secret distributor D needs to choose a polynomial of order *t* – 1, which is as follows:

$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \bmod p \tag{6}$$

Where $a_0 + a_1 + \cdots + a_{t-1}$ represents a random number, and *f*(*x*) needs to meet the following constraints:

$$f(x) = s \tag{7}$$

The secret shares of participants can be calculated by the following formula:

$$x_i = f(d_i) \bmod p \tag{8}$$

(3) Secret reconstruction:

Assuming that there are t* participants to reconstruct the shared secret, it needs to select the set P* of t* participants from t* participants, where the set of t participants can be expressed in the following form:

$$\mathrm{P}^* = \left\{ P_1^*, \cdots, P_t^* \right\} \tag{9}$$

Where, the shared secret information s can be calculated by the following formula, namely:

$$s = \begin{cases} f(0) \\ \sum_{i=1}^{t} x_t \end{cases} \prod_{i=1}^{t} \frac{0 - d_j}{d_t - d_j} \bmod p \tag{10}$$

In the process of laboratory cloud data attribute encryption, ciphertext is mainly composed of attribute set representation (Liu et al., 2016b), private key and access structure, which determines whether users can unlock ciphertext. After the attribute decomposition, encryption and constraint acquisition of laboratory cloud data, this paper introduces the internet of things technology to realise the access control method of laboratory cloud data.

3 Access control method for laboratory cloud data based on internet of things technology

The internet of things includes a variety of information sensing devices, which can realise the functions of identification, control and tracking between the network terminal and its detection object. This paper introduces the internet of things technology, multiplies the public key parameters corresponding to the attribute values of each laboratory cloud data, and sets the result as ciphertext, so as to realise the fixed length ciphertext. Based on the internet of things technology, laboratory cloud data cryptosystem can be divided into symmetric cryptosystem and asymmetric cryptosystem.

In the symmetric encryption algorithm, the data sender encrypts the plaintext through the encryption key, and sends out the ciphertext formed at the same time. After receiving the ciphertext, the receiver needs to use the previously encrypted key to decrypt it. The encryption process is shown in Figure 2.

After the above ciphertext encryption is completed, hash function is used to map the access structure and attribute set of laboratory cloud data, which effectively reduces the number of public key and main private key in the system (Zhang et al., 2018b; Zhu et al., 2016).

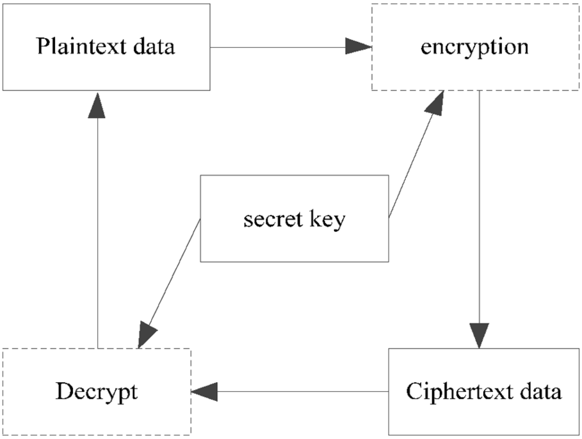
Let $W = \{W_1, \cdots, W_n\}$ to represent a set of attribute names, $V_i = \{V_{i,1}, \cdots, V_{in}\}$ represent a set of possible values of attribute W_i, and n_i represent the number of all possible values of attribute W_i. The user's attribute set can be expressed as:

$$u = (u_1, \cdots, u_n) \tag{11}$$

The laboratory cloud data access structure can be expressed as:

$$\mathrm{S} = (s_1, \cdots, s_n) \tag{12}$$

Figure 2 Ciphertext encryption process



Based on the internet of things technology, the mapping process of laboratory cloud data attribute set is as follows:

Step 1: Initialise the whole algorithm

By running the DBDH parameter generator with safety parameters, two groups with prime number of order q are generated, which are G_1 and G_T, respectively

$$\mathrm{Y} = e\left(g, g_1\right) \tag{13}$$

On the basis of the above analysis, a public key parameter matrix (Xu et al., 2016a; Jiang and Tang, 2017) composed of element group elements is formed, which is shown as follows:

$$\mathrm{T} = \begin{pmatrix} t_{0,1}, L, t_{0,m} \\ t_{1,1}, L, t_{1,m} \end{pmatrix} \tag{14}$$

$$g^T = \begin{pmatrix} g^{t_{0,1}}, L, g^{t_{0,m}} \\ g^{t_{1,1}}, L, g^{t_{1,m}} \end{pmatrix} \tag{15}$$

Step 2: Key formation algorithm

The message MP in the system is entered. The message belongs to the corresponding access structure. At the same time, the corresponding hash value is calculated:

$$h = H\left(u_1 \| \cdots \| u_n\right) \tag{16}$$

On the basis of the above analysis, $r \in Z_q$ is randomly selected and the private key of the corresponding user is calculated by the following formula:

$$SK_u = \begin{cases} \left\{SK_1, SK_2\right\} \\ g_1^y \left(\prod_{i \in [1,m]} g^{t_{i,j}}\right), g^r \end{cases} \tag{17}$$

Step 3: Encryption algorithm

On the basis of the above operations, if $r \in Z_q$ is selected randomly, then:

$$C_1 = \begin{cases} M \cdot Y^s \\ g^s \end{cases} \tag{18}$$

Then the output ciphertext is expressed as:

$$\mathrm{C} = \{S, C_1, C_2, C_3\} \tag{19}$$

Step 4: Decryption algorithm

Input MP, ciphertext $\mathrm{C} = \{S, C_1, C_2, C_3\}$ and C. If it needs to calculate and output the plaintext data M as follows, then there are:

$$\mathrm{M} = \frac{C_1 \cdot e(C_3, SK_2)}{e(C_2, SK_1)} \tag{20}$$

Where, ciphertext C and decryption key SK_U are expressed as (Xu et al., 2016b; Peng et al., 2016b):

$$\mathrm{C} = \left\{ S, C_1 = M \cdot Y^s, C_2 = g^s, C_3 = \left(\prod_{i \in [1,m]} g^{t_{i,j}} \right)^s \right\} \tag{21}$$

After the laboratory cloud data is decrypted, the attribute set mapping of the laboratory cloud data is completed by the following formula:

$$\frac{C_1 \cdot e(C_3, SK_2)}{e(C_2, SK_1)} = \begin{cases} \dfrac{C_1 \cdot e(C_3, g^r)}{e\left(C_2, g_1^y \left(\prod_{i \in [1,m]} g^{t_{i,j}}\right)\right)} \\ \dfrac{M \cdot e(g, g_1)^{sy} \cdot e\left(\prod_{i \in [1,m]} g^{t_{i,j}}\right)}{e(g, g_1) \cdot e\left(\prod_{i \in [1,m]} g^{t_{i,j}}\right)} \\ M \end{cases} \tag{22}$$

After mapping lab cloud data attributes, authorisation can be given to multiple users according to the different access rights granted. However, the process includes one-time decryption and dynamic encryption, which is time-consuming. Therefore, access control methods need to be verified to ensure the smooth implementation of access control of cloud data in the laboratory.

In order to verify the effectiveness of the above scheme, it is necessary to prove the security in the attack game that challenges the pre selection of access structure, and whether there is an attacker A who wins the game without neglecting the advantages. The specific operation process is as follows (Bai et al., 2019; He et al., 2018):

(1) Initialisation:

Attacker A needs to select and send the corresponding access structure to the challenger.

(2) Establishment stage:

Input:

$$\mathrm{BGen}\left(1^{k}\right)=\left\{q,G_{1},G_{T},g,e\right\} \tag{23}$$

Where

$$\mathrm{Z}=e\left(g,g\right)^{abc} \tag{24}$$

Select a hash function containing cryptographic features (Han and Wang, 2016), and express it in the following form:

$$\mathrm{T}^{*}=\begin{pmatrix} t^{*}{}_{0,1},L,t^{*}{}_{0,m} \\ t^{*}{}_{1,1},L,t_{*1,m} \end{pmatrix} \tag{25}$$

Calculate $h^{*}=H\left(s_{1}^{*}\left\|\cdots\right\|s_{N}^{*}\right)$, and set:

$$g^{T}=\begin{pmatrix} g^{t_{0,1}},L,g^{t_{0,m}} \\ g^{t_{1,1}},L,g^{t_{1,m}} \end{pmatrix} \tag{26}$$

Where

$$g^{t_{h_{i},j}^{*}}=g_{h_{i,j}}^{t^{*}-b} \tag{27}$$

$$g^{t_{h_{i},j}^{-*}}=g_{h_{i,j}}^{t_{-*}} \tag{28}$$

The main public key can be expressed as:

$$\mathrm{MP}=\left(q,G_{1},G_{T},g,e,g_{1}=g^{\alpha},Y=e\left(g,g\right)^{ab},g^{T},H\right) \tag{29}$$

Then the primary private key can be expressed in the following forms:

$$\mathrm{MS}=\left\{h^{*},T_{*}\right\} \tag{30}$$

In the query phase, for the list of arbitrary attributes published by the attacker:

$$\mathrm{U}=\left\{u_{1},u_{2},\cdots,u_{n}\right\} \tag{31}$$

The decryption key of the associated property set can be expressed as:

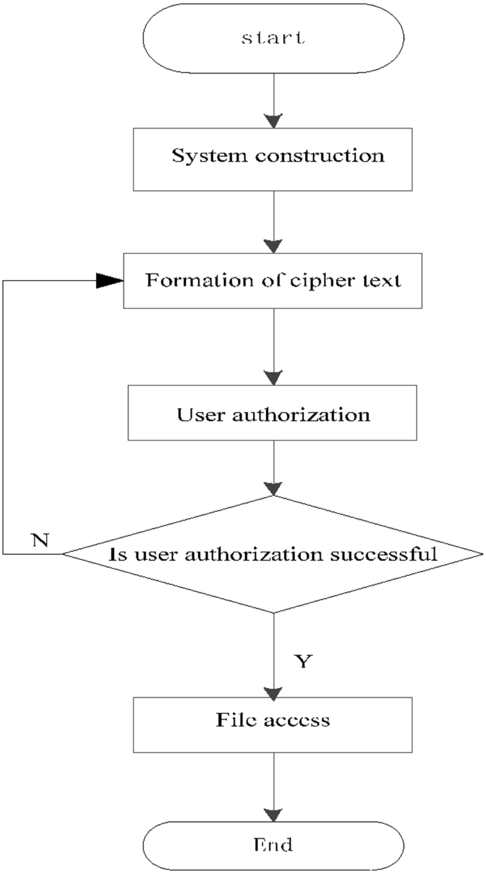
$$SK_{u}=\left\{SK_{1}=g^{r\cdot x+sum\cdot r\cdot b-sum^{-1}\cdot x\cdot a},SK_{2}=g^{r-sum^{-1}-a}\right\} \tag{32}$$

Where

$$x=\sum_{i\in[1,m]}t_{h,j} \tag{33}$$

The laboratory cloud data access control method based on the internet of things technology will select the hybrid encryption constitution to complete the safe and efficient data sharing access, that is, first use the symmetric key encryption algorithm to encrypt the data file (Wang, 2019), and then use the CP-ABE scheme to encrypt the symmetric key, to ensure that the symmetric key can only be accessed by the authorised legitimate users. The specific operation flow is shown in Figure 3. It is shown that:

Figure 3 Flow chart of access control processing



In the process of user revocation, the internet of things technology and proxy re encryption technology are combined to transfer most of the computing cost in the user attribute process to the cloud service to complete, effectively reduce the cost of the owner, and realise the access control of cloud data in the laboratory. By combining internet of things technology and proxy re encryption technology, the access structure and attribute set are mapped through hash function, so as to reduce the number of public key and main private key in the system; by using CP-ABE scheme to encrypt symmetric key, ensure that the symmetric key is authorised to be accessed by legitimate users, and realise the access control method of laboratory cloud data based on internet of things technology.

4 Simulation experiment

4.1 Experimental environment and parameter setting

In order to verify the comprehensive effectiveness of the proposed cloud data access control method based on the internet of things technology, a simulation experiment is needed. The Windows XP operating system is selected for the experiment. The hardware is Intel Pentium processor 3.0 GHz and 512 MB memory. My-Apriori-1 algorithm is implemented by Microsoft Visual Studio vc2005. Symmetric encryption adopts 128 bit AES encryption algorithm based on Openssl-1.0.0 library. In the whole experiment process, the network delay in the data transmission process is ignored, and the research method is applied to a laboratory.

4.2 Experimental scheme

In order to verify the comprehensive performance of the proposed method, the experiment chooses to access and control the cloud data of a laboratory. The size of the accessed database is 10 GB, and 75 data attributes are selected for access control. By comparing the methods of this paper, Peng et al. (2016a), Cao et al. (2019) and Liu et al. (2016a), the experimental analysis is made with the storage cost of access control, the operation efficiency of access control method, the encryption time of access control method and the stability of access control method as the experimental indicators.

- *storage space overhead*: the smaller the storage space used for lab cloud data access is, the better the performance of this access method is
- *operation efficiency*: when it accesses and controls the laboratory cloud data, the higher the efficiency of operation is, the faster the speed is, which proves that this method is more effective
- *encryption time*: when encrypting lab cloud data attributes, the shorter the encryption time is, the better the effect of access method is
- *the stability of access control method*: the higher the equilibrium value is, the better the stability of representative access method is.

4.3 Analysis of experimental results

4.3.1 Storage overhead analysis of different access control methods

In order to verify the effectiveness of the proposed method, the experiment compares the storage cost of the proposed method, the methods in Liu et al. (2016a), Guo et al. (2017) and Zhang et al. (2018a) and analyses it under the same attribute value quantity environment. The experimental results are shown in Table 1.

Analysis of the experimental data in Table 1 shows that with the continuous increase of the number of attribute values, the storage space overhead of the four access control methods is also changing, and there is a certain gap. Among them, when the number of attribute values is changing, the storage space overhead of the proposed method changes little, and remains below 620 bytes all the time; while the other three access control methods are always in the increasing trend, and far higher than the storage space overhead of the proposed method when the number of attribute values is changing. This is because the proposed method introduces the internet of things technology, encrypts the laboratory cloud data attributes, combines the access structure and identity encryption to ensure the fine-grained access control of the data, so as to ensure that the storage space of the proposed method is small and the effectiveness of the proposed method is verified.

Table 1 Storage space overhead of different access control methods (byte)

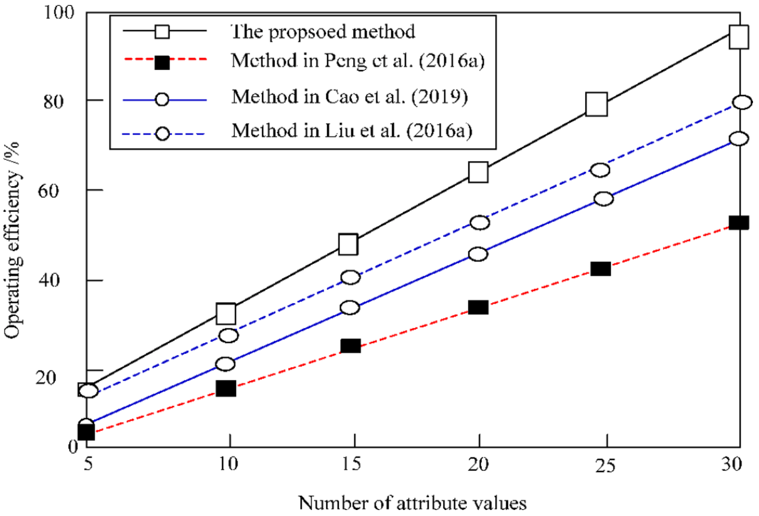
Number of attribute values	*The proposed method*	*Method in Peng et al. (2016a)*	*Method in Cao et al. (2019)*	*Method in Liu et al. (2016a)*
5	524	789	1012	1285
10	530	796	1068	1360
15	536	810	1104	1485
20	541	818	1159	1556
25	547	830	1188	1689
30	550	845	1207	1750
35	556	858	1284	1843
40	562	870	1305	1969
45	568	884	1359	2024
50	572	895	1423	2130
55	577	908	1488	2284
60	589	920	1520	2348
65	594	935	1574	2450
70	602	946	1598	2596
75	618	958	1635	2687

4.3.2 Operation efficiency analysis of different access control methods

In order to verify the effectiveness of the proposed method, the operation efficiency of the four access control methods is compared. The higher the operation efficiency is, the better the comprehensiveness of this method is. The experimental results are shown in Figure 4.

Analysis of Figure 4 shows that there is a certain gap in the efficiency of cloud data access control using four methods. Among them, the efficiency of using the proposed method to access cloud data in the laboratory is the highest, up to about 98%, while the highest efficiency of the other three methods is about 79%, 75% and 53%, respectively. Compared with this, the operation efficiency of the proposed method is improved by about 19%, 23% and 45%, respectively. Through the analysis of data, it can see that the operation efficiency of the proposed method is high. This is because the optimised CP-ABE scheme is adopted in the proposed method, which makes the public key parameters corresponding to each attribute value multiply, and sets them as ciphertext. At the same time, the hash function containing the cryptographic characteristics is used for access structure and attribute set mapping, which effectively reduces the quantity of public key and the main private key in the system, and then improve the operation efficiency of the proposed method.

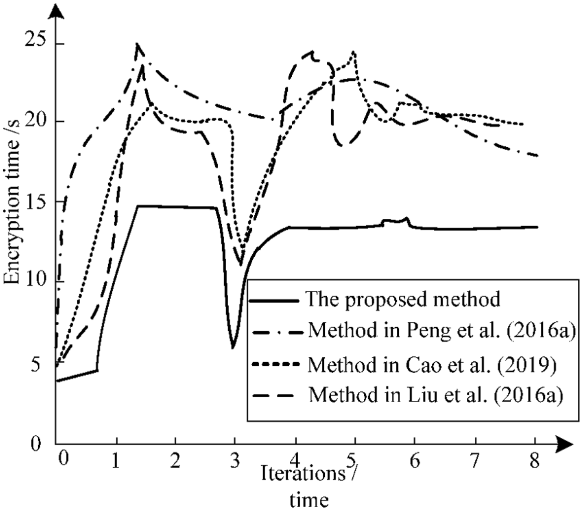
Figure 4 Comparison of operation efficiency of different access control methods (see online version for colours)



4.3.3 Analysis of encryption time for different access control methods

In order to verify the feasibility of the proposed method, the experiment analyses the time-consuming of four access control methods for laboratory cloud data encryption, and the comparison results are shown in Figure 5.

Figure 5 Comparison results of encryption time of different control methods

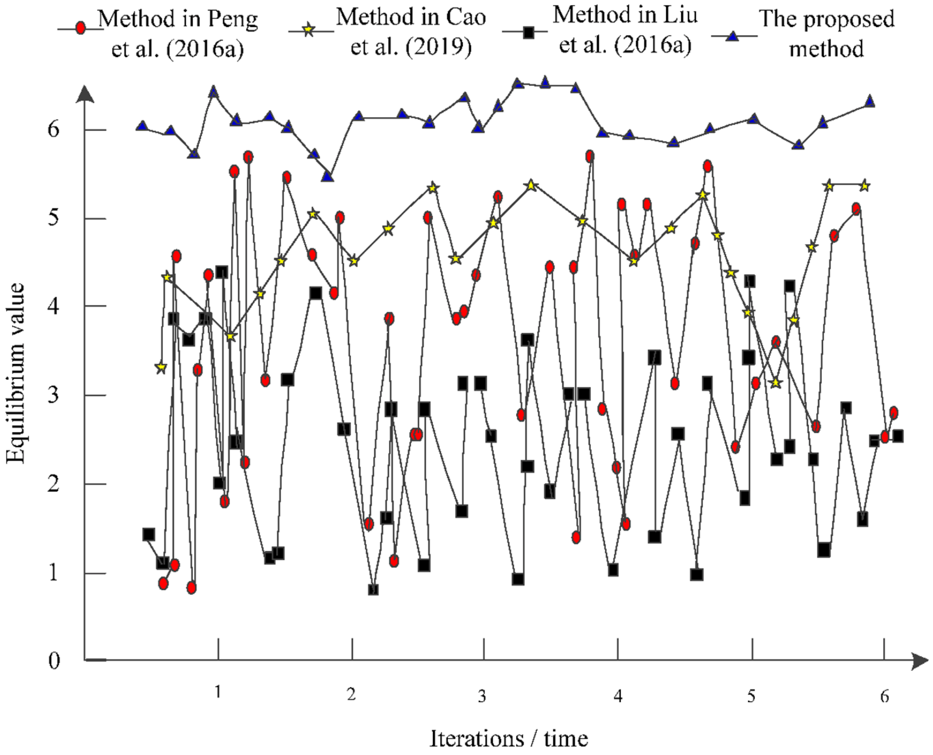


Analysis of Figure 5 shows that the encryption time of the four access control methods changes with the number of iterations, and the encryption time is different. Among them, the encryption time of the proposed method is always less than that of the other three methods, and is always less than 15s. However, the encryption time of the access control methods in Peng et al. (2016a), Cao et al. (2019) and Liu et al. (2016a) fluctuates many times and is always higher than that of the proposed method. This is because the proposed method divides the ciphertext into two categories before encrypting the data ciphertext, encrypting the ciphertext satisfying the conditions, thus improving the encryption speed and verifying the scientific validity of the proposed method.

4.3.4 Stability analysis of different access control methods

In order to further verify the comprehensive performance of the proposed method, the experiment analyses the stability of the four methods in the laboratory cloud data access control, and measures the stability of the method according to the balance value. The greater the balance value is, the better the effect is. The experimental results are shown in Figure 6.

Figure 6 Stability comparison of different access control methods (see online version for colours)



From the analysis of Figure 6, it can be seen that there are some differences in the stability of access control with four methods. Among them, the equilibrium value of the proposed method is large, always greater than 5, while the equilibrium value of the other three methods is always lower than the proposed method, and the fluctuation range of the other three methods is large, so it can be determined that the proposed method has the best stability in the laboratory cloud data access, which verifies the comprehensive effectiveness of the proposed method.

5 Conclusions

In view of the problems of traditional laboratory cloud data access control methods, such as long encryption time, high storage cost and low operation efficiency, this paper designs and proposes a laboratory cloud data access control method based on internet of things technology. By decomposing and encrypting the laboratory cloud data, improving the user's attribute level revocation ability, introducing the internet of things technology, and combining the hash function to access the laboratory cloud data, the laboratory cloud data access control based on the internet of things technology is realised. Through the experiment, the following conclusions are obtained:

- the proposed method can effectively save the data space cost when accessing the cloud data of the control laboratory, and is always lower than 620 bt
- the efficiency of the proposed method is high when it is used for access control, and the highest efficiency is 98%
- when the proposed method is used for access control, it takes less time to encrypt the laboratory cloud data, and it is always less than 15 s
- the equilibrium value of the proposed method is always greater than 5 in the access control of cloud data in the laboratory, which verifies the stability of the access control.

Due to the limitation of time conditions, the proposed method still has some disadvantages. In the future, the following aspects will be focused on:

- The proposed method has some limitations. In the future, it will further expand the scope of research and reduce the amount of calculation.
- Later, we will focus on how to effectively improve the privacy protection ability and security of access control scheme without reducing the efficiency of access control.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant No. 61602202.

References

Bai, C.Z., Wang, H.J., Han, C. and Zhang, S.H. (2019) 'Control strategy of water drop hovering configuration based on piecewise constant thrust', *Journal of Beijing University of Aeronautics and Astronautics*, Vol. 45, No. 3, pp.560–566.

Cao, Z.H., Cai, X.H., Gu, M.H., Gu, X.Z. and Li, X.W. (2019) 'Android permission management and control scheme based on access control list mechanism', *Computer Applications*, Vol. 39, No. 11, pp.3316–3322.

Guo, H.Y., Fang, J. and Li, D. (2017) 'Multi-source streaming data real-time storage system based on load balancing', *Computer Engineering and Science*, Vol. 39, No. 4, pp.641–647.

Han, W.C., Gao, H.k., Liu, L., Guo, L. and Xu, J. (2016) 'Authorization control design of pipeline integrity management system', *Oil and Gas Storage and Transportation*, Vol. 35, No. 9, pp.928–931.

Han, X.J. and Wang, D.W. (2016) 'Simulation of quantitative work-in-progress (WIP) control strategies for supply chain storage system radio frequency identification', *Control Theory and Applications*, Vol. 33, No. 4, pp.453–459.

He, Y.N., Liu, L.L., Cai, Q.Y., Zhao, N.Q. and Zheng, Y.J. (2018) 'Structural classification of hybrid control strategies in research design', *Chinese Journal of Epidemiology*, Vol. 39, No. 7, pp.999–1002.

Jiang, S.L. and Tang, Y.H. (2017) 'M/g/1 queuing system with multilevel adaptive vacations and min(n, v)-policy control', *System Science and Mathematics*, Vol. 37, No. 8, pp.1866–1884.

Liu, J., Xiang, J.W., Han, W. and Gao, Y. (2016b) 'Flight quality prediction based on adaptive pilot optimal control model', *Flight Mechanics*, Vol. 34, No. 5, pp.82–85.

Liu, X.P., Luo, X.Y. and Yang, H. (2016a) 'HBase-based high-efficiency traffic data cloud indexing technology', *Control Engineering*, Vol. 23, No. 4, pp.560–564.

Peng, L., Cai, G.W., Kong, L.G., Chen, C., Du, J.B. and Duan, J. (2016b) 'Control strategy for photovoltaic hydrogen storage grid connection', *Power Construction*, Vol. 37, No. 9, pp.56–61.

Peng, W.P., Liu, X.Z., Guo, H.R. and Song, C. (2016a) 'Research on cross-domain security access control model based on trust', *Computer Application Research*, Vol. 33, No. 6, pp.1791–1796.

Song, Y., Zhang, T.T. and Jiang, W. (2016) 'Pest management model based on pulse control', *Journal of Fuzhou University: Natural Science Edition*, Vol. 44, No. 2, pp.156–163.

Sun, C.H. and Zhang, B.S. (2016) 'Research on emergency control model of disease transmission based on target immunity', *Management Review*, Vol. 28, No. 8, pp.167–174.

Wang, J.W. and Yin, X.C. (2017) 'Attribute-based encryption scheme for ciphertext policy with weighted attribute revocation', *Computer Applications*, Vol. 37, No. 12, pp.3423–3429.

Wang, Z.H. (2019) 'Simulation of efficient data storage method for wireless sensor networks', *Computer Simulation*, Vol. 7, pp.376–379.

Xu, S.W., Tang, Z.Q., Wang, D.L. and Zhao, X. (2016a) 'Series braking control strategy for electric commercial vehicles', *Journal of Gansu Agricultural University*, Vol. 51, No. 4, pp.113–120.

Xu, X.W., Zhao, W.Q., Zhang, J.B., Wang, Y.P., Chang, B.L. and Yang, J.M. (2016b) 'Research on additional control strategies for ormoc-naga DC project in the Philippines', *Power System Technology*, Vol. 40, No. 9, pp.2810–2816.

Yan, X.C., Chen, Y., Zhai, Y.C., Lan, J.L. and Huang, K.X. (2016) 'An efficient CP-ABE cloud data access control scheme', *Small Microcomputer System*, Vol. 37, No. 10, pp.2155–2161.

Yu, H.w., Zheng, C., Wang, Y., Tang, W.D., Ma, Z.B. and Xu, J.H. (2016) 'Historical data service optimization scheme in smart grid dispatch control system', *Automation of Electric Power Systems*, Vol. 40, No. 19, pp.113–118.

Zhang, K., Ma, J.F., Zhang, J.W., Ying, Z.B., Zhang, T. and Liu, X.M. (2018a) 'Online/offline accountable attribute encryption scheme', *Computer Research and Development*, Vol. 55, No. 1, pp.216–224.

Zhang, Y.P., Lian, G., Zhiwei and Xing, Z.W. (2018b) 'Aircraft launches a strategy of controlling waiting for punishment of parking spaces', *Journal of Harbin Institute of Technology*, Vol. 50, No. 3, pp.39–45.

Zhao, B., He, J.S., Zhang, Y., Ji, X.R. and Xuan, X.G. (2016) 'Rough set-based authorization rules knowledge discovery in access control', *Journal of Beijing University of Posts and Telecommunications*, Vol. 39, No. 2, pp.48–52.

Zhao, Z.Y., Wang, J.H., Zhu, Z.Q. and Sun, L. (2019) 'Attribute-based encryption scheme for IoT data security sharing', *Computer Research and Development*, Vol. 56, No. 6, pp.1290–1301.

Zheng, Z.H., Zhang, M.A., Dai, X.M. and Wang, X.A. (2016) 'Efficient agent-based encryption-based cloud storage access control scheme', *Electronic Technology Application*, Vol. 42, No. 11, pp.99–101.

Zhu, W., Zhong, P. and Wu, X.Y. (2016) 'Multi-state frequency stability and unit control strategy after DC connection', *Chinese Journal of Electrical Engineering*, Vol. 36, No. 22, pp.6122–6130.