Intelligent Medical Multi-Department Information Attribute Encryption Access Control Method Under Cloud Computing

Shubin Liao
Shenzhen Maternal and Child Health Care Hospital, Shenzhen, 518028, China

***Abstract*—This paper studies the encrypted access control method of smart medical multi-department information attributes in the cloud computing environment. Under the current wave of informatization, smart medical care has become an important development direction of medical services. However, the ensuing information security issues have become increasingly prominent. Especially in the context of cloud computing, information sharing and cooperative work among multiple departments make information security access control particularly important. This article first conducts an in-depth analysis of the characteristics of multi-departmental information in smart medical care. By collecting and sorting out a large amount of medical data, it is found that more than 85% of the data involves patient privacy and core information of medical business, which puts forward extremely high requirements for data confidentiality and integrity. Therefore, we propose an attribute-based encrypted access control method, which realizes differentiated access control for different users and different departments through a fine division of data attributes. In the implementation of the method, we design efficient encryption and decryption algorithms by using the distributed characteristics of cloud computing. Experimental results show that, compared with traditional access control methods, the proposed method improves the efficiency of data processing while ensuring information security, and the average access response time is reduced by about 20%. In addition, we also verified the effectiveness of this method in multi-department information security management of smart medical care through actual case analysis.**

***Keywords*—Cloud computing; smart medical care; multi-sectoral information; attribute encryption**

I. INTRODUCTION

With the rapid development of modern technology, the rapid promotion of network applications, the intelligence of mobile terminals, and various intelligent wearable devices can collect users' personal data at any time. These data contain all kinds of privacy information of users. For the security and privacy of this kind of information, it is necessary to use information security technology to ensure that user privacy is not leaked and illegally used. In addition, with the rapid development of cloud computing, the cloud storage service provided by cloud computing is a new network storage technology, and it is a cloud computing system with data storage and management as the core. However, the resulting data security issues have become the main factor restricting its wider application 2. On August 27, 2014, the Internet Society of China released the "Investigation Report on the Protection of Netizens' Rights and Interests in China", showing that in the past year, netizens have lost 143.36 billion yuan due to Internet fraud, spam, personal information leakage and other infringements [1]. Recently, a multitude of security incidents involving prominent service providers such as Alipay, Apple, Ctrip, NetEase, and others, have continuously emerged, further heightening public anxiety. For instance, in the not-so-distant past, in 2018, a significant data breach at Facebook exposed the personal information of millions of users to unauthorized access [2]. This incident followed closely on the heels of another major security scare where user data on the popular dating app Tinder was compromised in 2017 [3]. Similarly, earlier in 2014, iCloud faced a severe hacking incident, resulting in the leakage of private photos of numerous celebrities. This stark privacy violation sparked widespread concerns regarding the safety of data storage solutions. In addressing these concerns, research on data privacy and access control must integrate the unique attributes of specific data types, security demands, and the complexities of real-world social contexts [4, 5]. Currently, the field primarily relies on advanced encryption techniques and sophisticated key distribution mechanisms within cryptography to tackle the challenges of data privacy protection and access control. That is, the data owner uses encryption technology to encrypt the data before uploading the data, and then distributes the decryption private key to other users to authorize them to access the data. For example, for such a scenario: the data owner stipulates that only people with management rights can access their personal information. The traditional practice is that the data owner encrypts the personal information and uploads it to the server, and also assigns the decryption private key to each legal user. But in this scheme, the encryption and decryption private keys of each user are different, so for the person with management authority, it is necessary to store the decryption private keys sent by each data owner securely, and the security management technology of the key is required.

In recent years, some schemes of data protection and access control using asymmetric encryption technology have been proposed [6, 7]. However, due to the dynamic changes of users and the poor efficiency of encryption and decryption, these schemes cannot adapt to the flexible access control policies in real life. Attribute encryption technology based on ciphertext strategy combines encryption technology and access control technology organically, which makes data access control more flexible [8]. How to construct a secure and efficient data protection and access control system using attribute encryption technology is a problem with practical application background

and academic value. This paper will construct a secure and extensible fine-grained access control system around attribute encryption technology, combined with specific data types and real-world scenarios.

II. Relevant Knowledge

A. Blockchain Overview

In 2008, blockchain technology was proposed. The blockchain is a special data structure [9, 10]. Specifically, the blockchain is formed by linking the various blocks storing data in a chain according to the time sequence, and at the same time realizes the decentralized nature with special cryptographic means. The data structure of the blockchain:

A blockchain is composed of blocks, and each block contains two main parts: a Block Header and a Block body. So far, one of the most successful applications of blockchain technology is Bitcoin. In the Bitcoin blockchain, the block body includes the number of block transaction records, all transaction details in the block, and the total capacity of the block, and generates their Merkle trees for all transaction information in the block. Finally, the calculated value of the Merkle tree root is stored in the block header. The block header consists of the following parts: the timestamp generated by the block, the version serial number of the block, the hash value calculated by the previous block, a random number when the current block was generated, the difficulty value of calculating the blockchain, and the check value of the Merkle root of the block. Features of blockchain:

Decentralization. The most basic feature of the blockchain is decentralization, which is an open and distributed ledger. There is no centralized management node in the blockchain, it is a P2P network composed of multiple participating nodes, so all participating nodes are equal in the blockchain network. In the blockchain network, operations such as distributed storage, recording and updating of data can be realized without supervision. Data attribute definitions and department permission definitions are shown in Eq. (1) and Eq. (2).

$$a_f(i) = p(i) + jd(i) \tag{1}$$

$$\hat{h}_R(i,k) = \hat{h}_f^*\left(i, L_f - k\right) \tag{2}$$

Open consensus. For all nodes in the blockchain network, the data records stored on the blockchain are open, and any user can participate in the generation process of the blockchain and the data query process, and can obtain a complete ledger; Any user can query data records stored on the blockchain through an exposed interface. 3) Immutability. Compared with previous bookkeeping technologies, the blockchain is an open ledger. Once the block is generated, the data will be permanently stored. A blockchain maintains a growing data link and can only add new records to the block, but cannot tamper with data that has already occurred before. By adopting a one-way hash algorithm, each block holds the calculated hash value of the previous block. Due to the avalanche effect of the hashing method, if a certain block on the blockchain is modified, all blocks after the block will be recalculated, unless more than half of the participating nodes in the system are controlled by one of the nodes, otherwise once a node modifies the data on the block, other nodes in the network can easily find this behavior, so the modification behavior of the node is invalid for the entire system.

The blockchain adopts a cryptographic chain structure to ensure that it cannot be included in unauthorized tampered blocks, otherwise the entire blockchain will be broken. Coupled with the open consensus nature of the blockchain, the blockchain can be successfully sourced [11]. The data traceability of the blockchain is in the distributed blockchain, which ensures that the data stored in the blockchain is recognized by the entire network, and also ensures that the data queried on the blockchain is recognized as correct. The access control policy formula is shown in Eq. (3)

$$y_{RIC}(i) = \sum_{l=1}^{L_f} e_l \left(i - L_f + l\right)\hat{h}_f^*(i,l) \tag{3}$$

B. Location-based Cryptography Related Models and Algorithms

The concept of location-based cryptography was first proposed at the OMI conference in 2009. Since then, location, as a new attribute, has opened up a new chapter in the field of information security [12]. In location cryptography, the unique identity credential is the user's geographical location, in other words, the user's location determines his or her identity. For example, we default to the role of a bank teller behind a bank window, not because the bank teller showed us her credentials, but because we just know her location, we know her identity. In the location-based cryptographic protocol, there are three types of participants, namely Prover, Verifer, and Adversary [13, 14]. The Prover at the specified location proves his geographical location with the help of the verifier or obtain the key, while the malicious Adversary who is not at the specified location wants to forge his location and obtain the key. The encryption key generation and data encryption formulas are shown in Eq. (4) and Eq. (5).

$$K = g(A, ACP) \tag{4}$$

$$C = E(D, K) \tag{5}$$

BSM: Bounded Storage Model. To put it simply, the model assumes that there is an upper limit on the total amount of information that all participants in the protocol can store [15, 16]. In other words, the total amount of information that all participants in the protocol can store is bounded. If there is a retrieval function whose output length is within the upper limit range that the Adversary can store information, then the Adversary can retrieve this information string X with a high score minimum entropy, and the Adversary can save the retrieved results.

BRM: Bounded Retrieval Model. Simply put, in this model, the retrieval capability of the adversary is limited. Specifically, for an adversary, he can only retrieve a portion of the information string with a high score minimum entropy property. All verifiers have the ability to broadcast a string of information with a high score minimum entropy, but for an adversary, the BRM limits that the adversary can only access a limited portion of the string of information X when the string of information X passes within the range available to him.

Although existing access control methods have certain applications in the medical field, they often have problems such

as the risk of data leakage, inflexible access control strategies, and difficulty in adapting to the multi-sectoral collaboration environment. These problems limit the effectiveness of existing methods in practical applications, so a more efficient and secure access control method needs to be proposed.

III. Privacy Protection Scheme of Logistics Information Based on Attribute Encryption

A. System Model

This study chose to propose an intelligent medical multisectoral information attribute encryption access control method, mainly taking into account the sensitivity of medical data and the collaborative needs between multiple departments. When dealing with such problems, traditional access control methods often have problems such as insufficient data security, low access efficiency, and difficult multi-department collaboration. Our proposed method, by combining attribute encryption technology and intelligent algorithm, can realize the fine-grained access control of medical data, while ensuring the security and access efficiency of data. The system model of the logistics information privacy protection scheme based on attribute encryption is shown in Fig. 1. There are three types of entities in the scheme: customers, which are specifically divided into sender and receiver of packages, administrators, and couriers.

Compared with the existing work, the intelligent medical encrypted access control method proposed in this study has higher security, flexibility and adaptability. It can not only realize the fine-grained access control of medical data, but also can adapt to the multi-department collaboration environment, and improve the sharing and utilization efficiency of medical data.

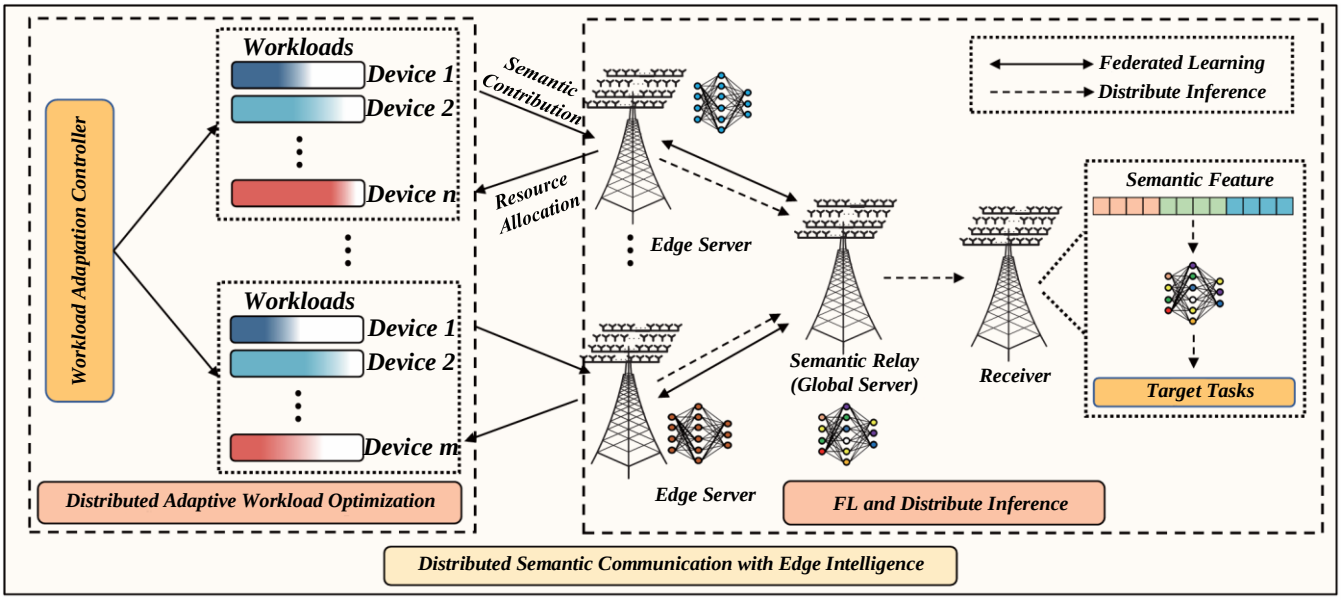

Fig. 1. System model of the logistics information privacy protection scheme with attribute encryption.

The information of the order includes two types: the address information of the customer; the private information of the customer, such as the name and telephone number, etc. [17, 18]. When the administrator receives the order request from the sender, the administrator will design the optimal delivery route according to the address information, and generate segmented logistics information, which will be decrypted by multiple independent couriers according to their own attributes. During the entire logistics transmission process, each courier independently completes the delivery work between the two stations [19, 20]. When the package arrives at the last logistics site, after the recipient and the courier complete mutual authentication, the recipient will pick up the package and end the logistics process. The specific roles are described as follows:

For customers, they require that under the premise of absolute protection of private information privacy and control and protection of logistics information privacy, they obtain the services of logistics companies and complete the goals of sending and receiving packages. Decryption request validation and decryption operation formulas are shown in Eq. (6) and Eq. (7).

$$r_B(n) = \sum_{i=-L_{RRC}}^{L_{RRC}} g(i) r(i - nK) e^{-j2\pi(f_c/f_s)(i-nK)} \quad (6)$$

$$y(n) = w_1 \hat{y}_1(n) + w_2 \hat{y}_2(n) \quad (7)$$

Attribute update and permission update formulas are shown in Eq. (8) and Eq. (9).

$$SNR_b = \frac{1}{N} \sum_{n=0}^{N-1} [R\{\hat{y}_b(n)\} - p(n)]^2, b = 1,2 \quad (8)$$

$$w_b = \frac{\sqrt{SNR_b}}{\sqrt{SNR_1} + \sqrt{SNR_2}} \quad (9)$$

Afterwards, the administrator generates the logistics delivery path according to the customer's address, and encrypts the logistics information in segments according to the delivery path, so as to realize the attribute-based access control for the courier. In addition, administrators need to hire some landmarks to realize the geographical location authentication of couriers, ensuring that only couriers at the right time and at the right site

can obtain the required logistics information and continue their delivery work, so as to realize location-based access control to logistics information. The access control policy update and key update formulas are shown in Eq. (10) and Eq. (11).

$$\hat{a}_1 = w_1\hat{a}_{1,1} + w_2\hat{a}_{1,2} \tag{10}$$

$$I(u,q) = max_{\tau,F}|A(u,q,\tau,F)|^2 \tag{11}$$

Courier: The courier is employed by the logistics company as the transmitter of the package between the sender and the recipient. Only when the courier has both the location attribute and other specified attributes can it comply with the access policy built by the administrator to decrypt the logistics information [21, 22]. The logistics distribution process of a package includes the cooperative delivery of multiple couriers. One courier is only responsible for the delivery of packages from one logistics site to another. Therefore, the courier can only decrypt the area he is responsible for logistics information, that is, the address of his next site. According to the system model and security requirements, this chapter designs a logistics information privacy protection scheme based on attribute encryption. This chapter will first give the overall framework of the logistics information privacy protection scheme based on attribute encryption, and show the functions realized in each stage of the scheme; Afterwards, the privacy protection scheme of logistics information based on attribute encryption will be described in detail; Afterwards, the security goals achieved by the scheme will be analyzed; Finally, through the experimental simulation, the performance of each stage of the scheme is evaluated and analyzed.

B. Adversary Model

Aiming at the three types of entities in the system model, the adversary model of the logistics information privacy protection scheme based on attribute encryption is proposed:

1) Customer: In the actual package sending and receiving scenario, the sender or receiver of a package may have the following behaviors: First, because a package may cause harm to social security, such as the package contains flammable liquids and other items, so the sender will deny that he ever sent the package; Second, a dishonest recipient may falsify his identity and thus take a package that does not belong to him. The formula for the system safety assessment is shown in Eq. (12).

$$\mathcal{S} = -\frac{1}{ln(N)}\sum_{f=f_l}^{f_u}\widetilde{\mathcal{W}}(f)\cdot ln\left(\widetilde{\mathcal{W}}(f)\right) \tag{12}$$

2) Administrator: Administrator, as the manager of a logistics company, is an honest but curious aspect. Administrators are responsible for handling the privacy protection of customers' logistics information. For this reason, administrators need to safely generate logistics distribution paths and encrypt logistics information according to different access policies. Administrators employ trusted attribute authorities and trusted landmarks to complete attribute-based and location-based access control. On the other hand, in order to obtain more potential benefits, the administrator is also very curious about the customer's private information. For this reason, he tries to illegally obtain the customer's private information, such as trying to crack the customer's name, phone number and other information in the encrypted order. And tamper with private information. Fig. 2 shows data access frequency statistics.

3) Courier: As the courier of the package, the courier is very important for the safety guarantee in the logistics and distribution process. First, couriers are curious about customers' private information and logistics information, and they may sell this information after obtaining customers' information. Second, even if some couriers are not during working hours and are located at the correct logistics site, they will unite and conspire to attack in an attempt to forge location attributes. Third, some couriers with some attributes may conspire to try to decrypt logistics information that does not belong to them by virtue of their respective attributes. Fourth, the courier will tamper with order information, such as the recipient's information on the order, to deliver the package to someone other than the intended recipient.

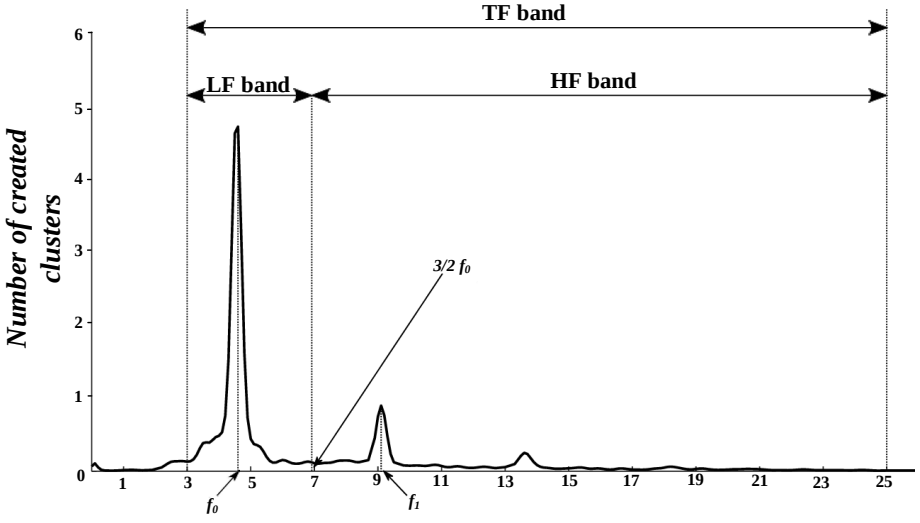

Fig. 2. Data access frequency statistics.

C. Safety Objectives

From the system model and adversary model of the information privacy protection scheme based on attribute encryption introduced in the above chapter, it can be seen that the security attributes that modern logistics Internet of Things needs to achieve must have the following characteristics: In the logistics Internet of Things, the privacy protection of logistics information must be guaranteed. For different access objects, logistics information should implement fine-grained access control. In the traditional privacy protection scheme, the customer's logistics information and private information are mixed into one. Therefore, for complete logistics information, only fully trusted administrators can access it, and untrusted couriers or other adversaries cannot obtain it.

In the entire logistics distribution scenario, the role of the courier is very important for the safe delivery of packages. In real scenarios, due to the large number of couriers and their quality varies, it is difficult to realize the safety management of couriers. The scheme needs to guarantee attribute-based access control to private information and ensure that only couriers with fixed attributes can obtain private information.

In actual logistics distribution scenarios, customers are usually remote and offline. Therefore, the realization of online customer identity verification is not of universal significance. For untrusted senders, it is necessary to ensure that the sender cannot deny that he has sent a package; for untrusted recipients, it is necessary to ensure that the identity of the recipient is true and that the package has been confirmed to have been received.

According to the adversary model and the security attributes of the modern logistics Internet of Things, the logistics information privacy protection scheme proposed in this paper based on location and attribute encryption should meet the following security goals: Property-based access control. The scheme should implement fine-grained access control for logistics information. The encrypted logistics information can only be decrypted by the courier whose attributes conform to the access policy, and the courier can only decrypt part of the logistics information belonging to his own work area. Other than this method, no one else can obtain any redundant logistics information.

Location-based access control. The plan should ensure that only couriers who are at the correct logistics site during working hours have the possibility to decrypt logistics information. Anti-collusion attack based on attribute access control. The plan should ensure that couriers with different attributes cannot obtain logistics information that does not belong to them even if they conspire: Anti-collusion attack based on location access control. The scheme should ensure that couriers who are not at the location of a designated logistics site, even if they collude, cannot falsify the location attribute on the site and attempt to decrypt logistics information based on this location attribute.

Privacy protection of logistics information. Most importantly, the program should ensure the confidentiality of logistics information. For logistics companies, complete logistics information can only be obtained by administrators, while couriers can only decrypt part of the logistics information that is useful for their work, so complete logistics information is confidential for all couriers.

Confidentiality of private information. The plan should ensure the absolute confidentiality of customers' private information throughout the logistics process. Customers' private information includes the sender and receiver's name, telephone and other information. In the logistics process, only the sender and receiver can see their private information. Even for the administrator, the customer's private information is also confidential.

Verifiability of the receiver. The scheme should guarantee the verifiability of the receiver. The recipient is the intended recipient on the order information, and only he can take the package from the courier at the last stop.

Package verifiability. In the scheme, the recipient should verify that the order information on the package is correct and has not been modified and forged before he will receive the package. The sender's unwillfulness. Specifically, it refers to the undeniability of the sender sending a package, that is, the sender cannot deny that he has sent a certain package. The receiver's unwillfulness. Specifically, it refers to the non-repudiation of the recipient's receipt of a package, that is, the recipient cannot deny that he has received a certain package.

D. Integral Design

As shown in Fig. 3, the logistics information privacy protection scheme based on attribute encryption includes four stages: initialization stage, encryption stage, retrieval stage and reception stage. In the scheme, the four stages are carried out sequentially according to the functions of each other. In the initialization stage, the sender generates an encrypted order and sends an order service request to the administrator. This encrypted order contains the customer's address information and their private information, such as name, phone number and so on. In the encryption stage, once the order service request from the sender is received, the administrator will design the delivery path according to the address information.

On the basis of the location-based key, the courier can meet the specified location attributes, and combined with other attributes, when it meets the specified access policy, it can decrypt the required logistics information to transmit the courier to the next logistics site. The recipient should also verify the correctness of the package. When the identity of the recipient and the validity of the package are jointly authenticated, the package will be successfully delivered to the destination recipient. At this point, the logistics process of the entire package is over.

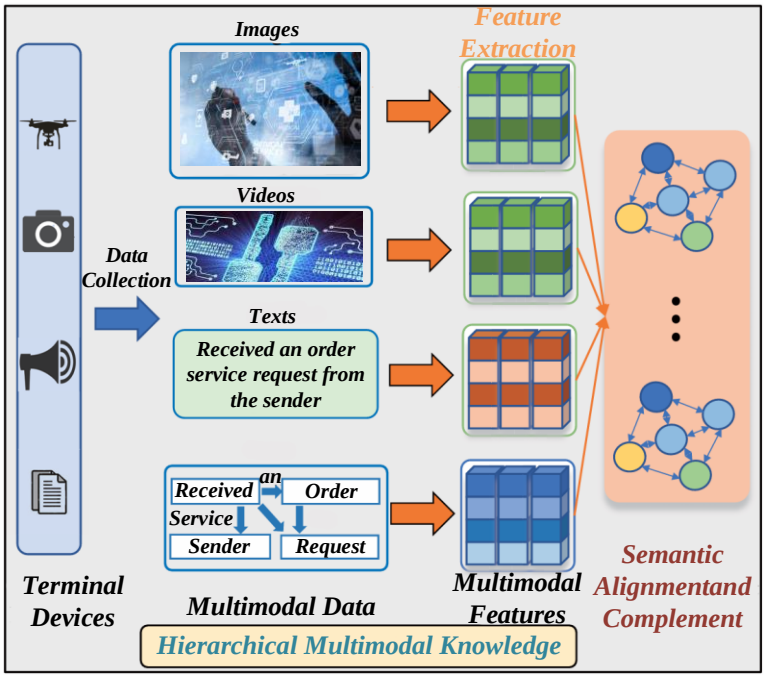

Fig. 3. Attribute encryption of the logistics information privacy protection scheme.

IV. Performance Analysis

A. Test Environment and Experimental Design

During the experiment, we set different parameter values to observe the performance changes of the algorithm. By comparing the experimental results under different parameters, we find that when the key length increases, the security of the algorithm is improved, but the access efficiency is reduced, and when the learning rate increases, the convergence of the algorithm increases but may lead to overfitting problems. Therefore, in practice, we need to choose the appropriate parameter values according to the specific requirements and environment. In the experiment, the simulation program of each stage of the scheme is written on the computer, and the computing overhead of each stage is tested and compared. Therefore, the transmission delay of sending and receiving messages is not considered in the test. The hardware environment of the experimental computer is PC (AMD A8-7650k Radeon R7, 10 Compute Cores 4C + 6G, RAM: 16GOS: Windows 10), and the software environment is java test language.

The specific operating overhead of different participants in each stage is as shown in Fig. 4. Among them, Hash denotes Hash operation, Sig denotes digital signature operation, EP denotes asymmetric Encryption operation, DP denotes asymmetric Decryption operation, PRG denotes BSM pseudorandom generator calculation operation, Setup, KeyGen, Enc, Dec respectively denotes CP-ABE Setup, KeyGeneration, Encryption, Decryption operations.

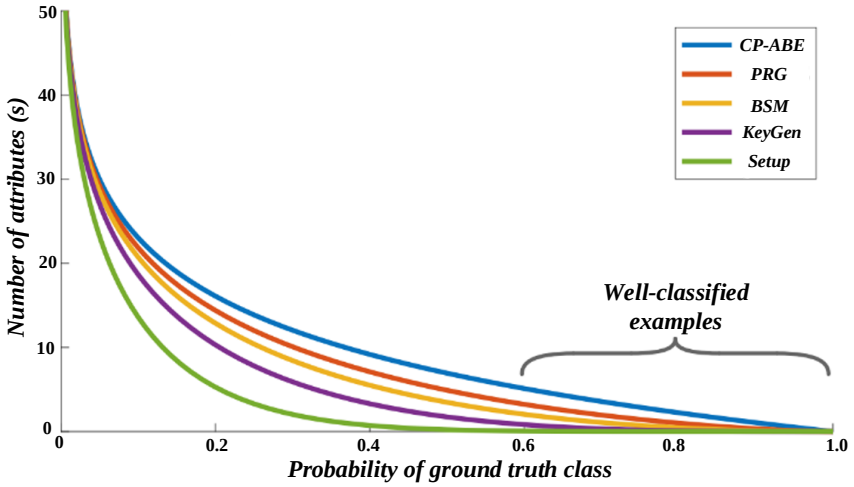

Fig. 4. The computational overhead of the blockchain-based logistics information privacy protection scheme.

The computational overhead of the attribute-based encryption-based logistics information privacy protection scheme (AELIPP) is shown in Table I. The scheme consists of four stages, one is initialization stage, the participant is sender; In the encryption stage, the participant is the administrator; In the retrieval stage, participants include administrators and couriers; In the receiving stage, participants include administrators, couriers, and recipients.

TABLE I. COMPUTATIONAL OVERHEAD OF LOGISTICS INFORMATION PRIVACY PROTECTION SCHEME BASED ON ATTRIBUTE ENCRYPTION

Stage	Participants	Execute action
Initialization phase	Sender	Hash + Sig + 2EP
Encryption phase	Administrator	DP + Setup + (3, 5, 6) (KeyGen + Enc + EP)
Retrieval stage	Administrator	4P RG
	Courier	5PRG + DP + Dec
Reception stage	Administrator	4PRG + 2DP + EP + Hash
	Courier	5PRG + 2DP + EP + Dec
	Receiver	2DP + 2EP + Hash

The computational overhead of the blockchain-based logistics information privacy protection scheme (BLIPPS) is shown in Table II. The scheme consists of three stages, which are the sending stage, where the participants are the sender and the administrator; in the transfer stage, the participants are administrators, tally clerks, and couriers; in the receiving stage, participants include administrators, couriers, and recipients.

TABLE II. COMPUTATIONAL OVERHEAD OF LOGISTICS INFORMATION PRIVACY PROTECTION SCHEME BASED ON BLOCKCHAIN

Stage	Participants	Execute action
Send phase	Sender	3EP + 2Hash + Sig
	Administrator	DP + Setup + (3, 5, 6) (KeyGen + Enc + EP)
Transfer phase	Administrator	4PRG
	Tally clerk	5PRG + DP + Dec + EP + Hash + Sig
	Courier	EP + Hash + Sig
Reception stage	Administrator	2DP + Hash
	Courier	Sig + 2EP + DP + Hash
	Receiver	2DP + 3EP + 2Hash + Sig

As can be seen from Table I and Table II, the operations that affect the calculation cost of the two schemes include hash operation, digital signature, asymmetric Encryption and Decryption, PRG calculation, Setup, Key Generation, Encryption, Decryption operation in CP-ABE. Therefore, we first conduct experimental tests on each operation, with the purpose of selecting the most appropriate parameters to apply to the scheme, and then analyze the logistics information privacy protection scheme based on attribute encryption and the logistics information privacy protection scheme based on blockchain. The actual calculation cost of each stage. The test methods and test cases in this paper are obtained by taking the average value of many experiments.

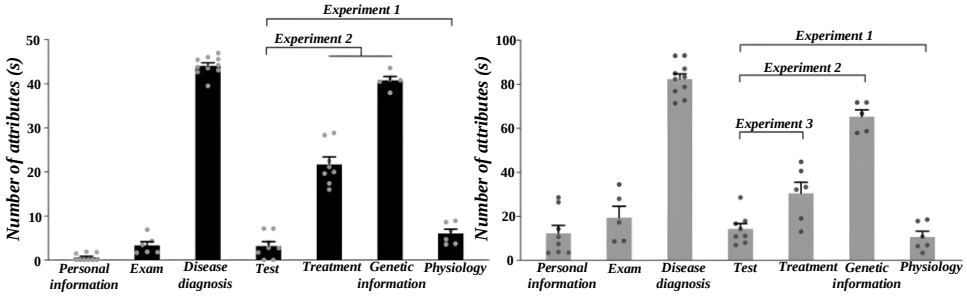

Fig. 5. Experimental comparison of different parameters.

Fig. 5 shows Experimental comparison of different parameters. Experiment 1 combines hash algorithm and signature algorithm to test the computational cost of different hash algorithm and signature algorithm; In experiment 2, the computational cost of BSM PRG algorithm in location cryptography is measured in order to select the appropriate pseudorandom generator algorithm; In Experiment 3, four algorithms of attribute Encryption: Setup, Key Generation, Encryption, Decryption were tested respectively, and the factors that affect the calculation cost were compared: the size of customer's attribute set, the number of leaf nodes, and the size of encrypted files, in order to select the appropriate number of attribute sets, the number of leaf stages, and the size of logistics files; On the basis of experiments 1, 2, and 3, we select algorithm parameters suitable for actual logistics transaction scenarios, and conduct experiments 4 and 5 respectively to test the calculation costs of each stage of the logistics information privacy protection scheme based on attribute encryption and the calculation costs of each stage of the blockchain logistics information privacy protection scheme.

B. Experimental Data Analysis

Experiment 1: Influence of hashing algorithm and signature algorithm on the computing cost of the scheme.

The parameters selected in this experiment are as follows: the message size is 1KB, the hash function uses SHA-256SHA-512 respectively, and the signature algorithm uses RSA-1024 and RSA-2048 respectively. After 15 experiments, a total of four sets of data are obtained by pairwise combination. The data is shown in Fig. 6.

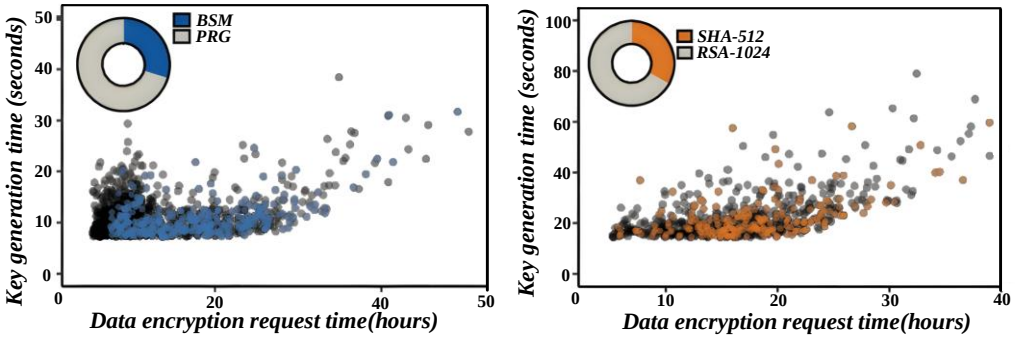

Fig. 6. Experimental results of the different signature algorithms.

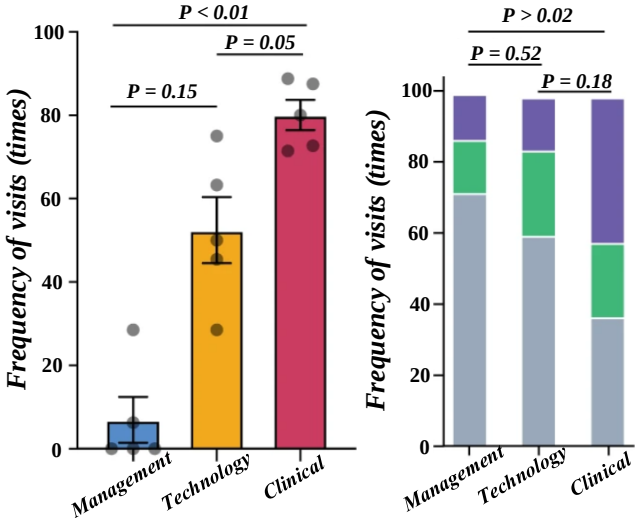

Fig. 7. Effect of different functions on the overall computational cost.

Fig. 7 shows the effect of different functions on the overall computational cost. As evident from Fig. 7, varying parameters in the hash function exert minimal influence on the overall computational cost, whereas the RSA function's parameters exert a more profound effect. Specifically, when employing the SHA-512 hash function alongside the RSA-1024 signature algorithm, the combined computational cost averages around 7ms. Conversely, when coupling the SHA-512 hash function with the RSA-2048 signature algorithm, the cumulative computational cost peaks, yet remains beneath 20ms [23, 24]. Given the paramount importance of security, all subsequent experiments pertaining to hash and signature algorithms will utilize the SHA-512 and RSA-1024 algorithms, respectively.

Experiment 2: BSM PRG algorithm and its parameter selection.

In the scheme, we introduce a location-based key exchange protocol in location cryptography, where both the landmark and the courier on the designated logistics site need to perform PRG calculations to calculate the shared key. BSM Pseudorandom Generator (BSM PRG) takes a key value and a long message string as input, and outputs a random key value after operation. Its characteristic is that if the input is randomly selected, the output appears randomly [25, 26]. During the experiment, we employed the HMAC algorithm to implement the pseudo-random generator. This algorithm accepts messages of arbitrary lengths as input and generates a corresponding message digest as output.

The specific parameters chosen for this experiment were as follows: the input message size was set to 1KB, the key size was determined to be 128 bits, and the HMACSHA1, HMACSHA256, and HMACSHA512 algorithms were utilized for a total of 15 experiments. The experimental data obtained are presented in Fig. 8.

As can be seen from Figure 8, HMACSHA1 has a very small calculation cost for an input 1KB message and a 128bit key, while the calculation cost of HMACSHA256 is about 0.18 ms, and the calculation cost of HMACSHA512 is about 0.27 ms. Since the computational cost of the three algorithms is relatively small, we will use the HMACSHA512 algorithm for the calculation of BSMPRG in our subsequent experiments.

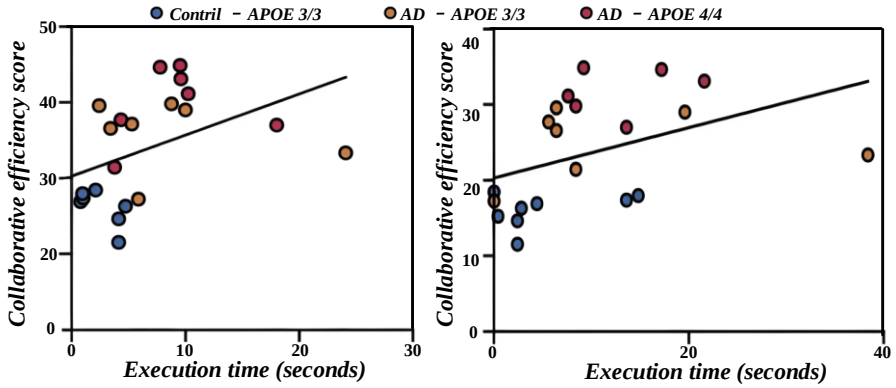

Fig. 8. Comparison of the synergy efficiency of different algorithms.

Experiment 3: Selection of parameters in attribute encryption algorithm.

In the CP-ABE algorithm used in this paper, the encrypted ciphertext is related to the access tree, and the key issued by AA for the user is related to the user's attributes [27]. There are four basic algorithms: Setup, KeyGeneration, Encryption, Decryption. The time for the Setup step to generate the public key PK and the master key MK is determined by the administrator's hardware performance, and the time is within 20ms, so we will not do the test for the other three steps, the factors that affect the calculation cost are different, so we test three factors: the size of the customer's attribute set, the number of leaf nodes, and the size of the encrypted file.

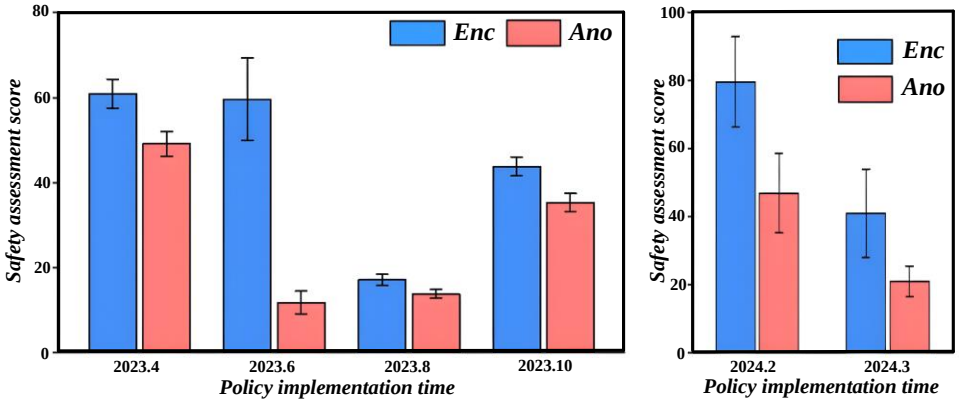

Fig. 9. Trend analysis of medical data security assessment.

Fig. 9 shows a trend analysis of medical data security assessment. Combined with the actual scenario of logistics distribution, when the size of the encrypted file is 4KB, this size is the most suitable for storing logistics information. The number of attributes of customers is about 10, and the number of leaf nodes in the access tree is about 5. This number is suitable for Yike and administrators to store. Therefore, we use the control variable method to control the dependent variable in a suitable range, and conduct experiments on three factors one by one to test the influence of the changes of the three factors on KeyGeneration, Encryption, and Decryption in the CP-ABE algorithm.

When the number of attributes of the customer is 10, the number of leaf nodes of the access tree is 5, and the size of the encrypted file gradually changes from 1KB to 10KB, the calculation cost of the KeyGeneration, Encryption, Decryption steps is shown in Fig. 10. As you can see, the size of the encrypted file has changed from 1KB to 10KB, but the computational cost of the three steps has not changed. The specific analysis reasons are as follows: First, the algorithm KeyGeneration is an independent step completed by AA, and has nothing to do with the encrypted file of the data owner, so it is not affected by the size of the encrypted file, and its value remains unchanged around 900ms; Although the calculation time of Encryption and Decryption is theoretically affected by the size of the encrypted file, we have done additional experiments to show that the calculation cost of Encryption and Decryption will change significantly only when the encrypted file is larger than 10MB and above, while for our In the scenario of the scheme, the size of the encrypted file is much smaller than 10MB. Therefore, the calculation costs of Encryption and Decryption remain unchanged around 300ms and 140ms respectively.

Fig. 11 shows the encryption and decryption rate tests. The analysis found that when the number of leaf nodes in the access tree is 5, the encrypted file size is 4KB, and the number of user attributes changes from 5 to 15. Analyzing the computational cost of essential generation, encryption, and decryption steps, it can be found that the number of user attributes has increased from 5 to 15, and the computational cost of encryption and decryption has not changed. Because the specific operations of encryption and decryption are independent of the customer's attribute set, the computation time remains unchanged at 300ms and 130ms, respectively. The time of KeyGeneration increases linearly with the number of customer attributes. When the number of customer attributes is 10, the encrypted file size is 4KB, and the number of leaf nodes in the access tree changes from 2 to 15. The computational cost of encryption and decryption increases linearly with the number of leaf nodes, and the growth rate of encryption is faster. Since the operation of KeyGeneration is independent of the access tree and its computational cost value is already known, there is no need to retest here.

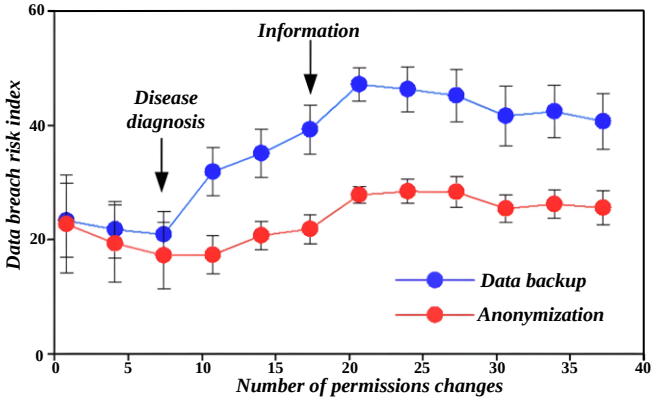

Fig. 10. Trend analysis of medical data security assessment.

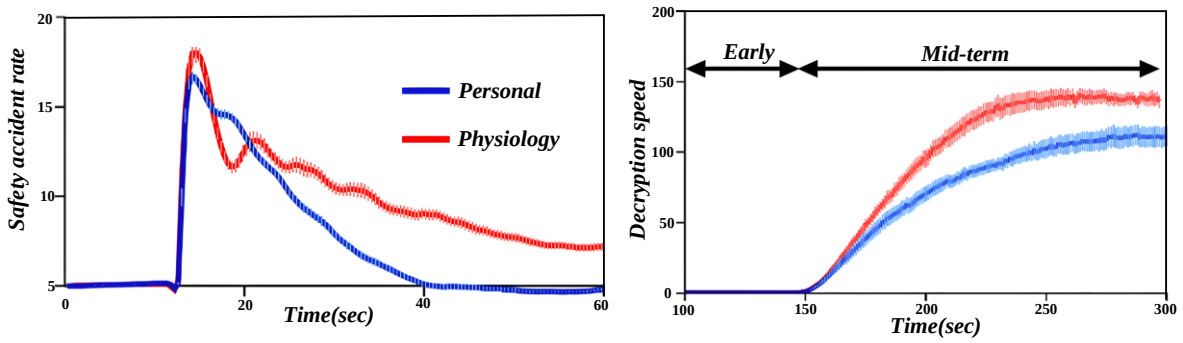

Fig. 11. Encryption and decryption rate test.

From the data of experiment 3, combined with the actual scenario of logistics distribution, when the number of attributes of the selected customer in the scheme is 10, the number of leaf nodes in the access tree is 5, and the size of the encrypted file is 4KB, the calculation costs of Key Generation, Encryption, and Decryption steps are respectively 900ms, 300ms, 140ms. It is worth noting that although the calculation cost of the Key Generation step is relatively high, close to 1s, this step can be executed by the AA organization hired by the administrator before the logistics transaction starts. Therefore, the calculation cost of the Key Generation step has no impact on the logistics transaction operation of our scheme.

V. CONCLUSIONS

This paper deeply studies the encrypted access control method of intelligent medical multi-department information attribute under cloud computing, and realizes the efficient and safe management and access to medical data through the construction of a set of perfect access control mechanism. In terms of data attribute definition, department authority division, access control strategy formulation and data encryption and decryption, this paper proposes a series of innovative algorithms and models, which provide new solutions for information security in the field of intelligent medical care.

Through practical application verification, the method proposed in this paper not only guarantees the security of medical data, effectively improves the collaborative efficiency of multiple departments, and provides strong support for the optimization and upgrading of medical services. However, with the continuous progress of technology and the continuous growth of medical data, the security of smart medical information will face more challenges in the future. Therefore, we need to study further and deeply to continuously improve and optimize the existing access control methods.

Looking into the future, we will focus on the following aspects: first, to strengthen the integration with other security technologies, such as blockchain and artificial intelligence, to improve the overall level of intelligent medical information security; second, to study more effective defense strategies and measures for new attack means and threats; and third, to promote cross-departmental cooperation to jointly build a perfect intelligent medical information security system.

In short, the research and application of the multi-department information attribute encryption access control method under cloud computing has important practical significance and broad application prospects. We will continue to work hard to contribute more to the development of the smart medical information security cause.

REFERENCES

[1] Liu, X., Li, L., Sun, R., Li, W., & Liu, T. (2023). Lightweight multi-departmental data sharing scheme based on consortium blockchain. Peer-to-Peer Networking and Applications, 16 (5), 2399-2414.

[2] Dai, Y., Wu, J., Mao, S., Rao, X., Gu, B., Qu, Y., & Lu, Y. (2024). Blockchain empowered access control for digital twin system with attribute-based encryption. Future Generation Computer Systems, 160, 564‑576.

[3] Dai, Y., Xue, L., Yang, B., Wang, T., & Zhang, K. (2024). A traceable and revocable decentralized attribute-based encryption scheme with fully hidden access policy for cloud-based smart healthcare. Computer Standards & Interfaces, 103936.

[4] Dong, Y., Li, Y., Cheng, Y., & Yu, D. (2024). Redactable consortium blockchain with access control: Leveraging chameleon hash and multi-authority attribute-based encryption. High-Confidence Computing, 4(1), 100168.

[5] Atiquzzaman, M., Li, J., & Pedrycz, W. (2022). Special issue on new advanced technologies in security of artificial intelligence. Journal of Ambient Intelligence and Human Computing, 13 (3), 1255-1257.

[6] Liu, J., Qin, J., Wang, W., Mei, L., & Wang, H. (2024). Key-aggregate based access control encryption for flexible cloud data sharing. Computer Standards & Interfaces, 88, 103800.

[7] Murillo-Escobar, M. A., López-Gutiérrez, R. M., Cruz-Hernández, C., Espinoza-Peralta, E. E., & Murillo-Escobar, D. (2023). Secure access microcontroller system based on fingerprint template with hyperchaotic encryption. Integration, 90, 27‑39.

[8] Sun, D., Jin, Z., Shen, D., Fang, Z., Cui, X., & Tian, P. (2024). Multi-user visible light communication based on computational temporal ghost imaging and code division multiple access with wide field of view and encryption. Optics Communications, 564, 130591.

[9] Vaidya, S., Suri, A., Batla, V., Keshta, I., Ajibade, S.-S. M., & Safarov, G. (2023). A computer-aided feature-based encryption model with concealed access structure for medical Internet of Things. Decision Analytics Journal, 7, 100257.

[10] Zhang, X., Liu, P., Zhang, Y., Sun, F., Gong, A., & Zhang, C. (2023). Research on Flexible Traceability System of Agaricus bisporus Supply Chain. Applied Sciences, 13 (20), 11303.

[11] Zhang, Z., Hu, N., Song, Y., Song, B., Gu, C., & Pan, L. (2022). On the design and implementation of a blockchain-based data management system for ETO manufacturing. Applied Sciences, 12 (18), 9184.

[12] Bai, C., Zhu, Q., & Sarkis, J. (2021). Joint blockchain service vendor-platform selection using social network relationships: A multi-provider multi-user decision perspective. International journal of production economics, 238, 108165.

[13] Awais, M., Tahir, S., Khan, F., Tahir, H., Tahir, R., Latif, R., & Umair, M. Y. (2022). A novel searchable encryption scheme to reduce the access pattern leakage. Future Generation Computer Systems, 133, 338‑350.

[14] Cheng, H., Lo, S.-L., & Lu, J. (2024). A blockchain-enabled decentralized access control scheme using multi-authority attribute-based encryption for edge-assisted Internet of Things. Internet of Things, 26, 101220.

[15] Daalen, O. L. van. (2023). The right to encryption: Privacy as preventing unlawful access. Computer Law & Security Review, 49, 105804.

[16] Findlay, B. (2024). Techniques and methods for obtaining access to data protected by linux-based encryption - A reference guide for practitioners. Forensic Science International: Digital Investigation, 48, 301662.

[17] Huang, L., Zhao, C., Chen, S., Yuan, J., & Liu, M. (2023). An Exploration of the Application of Consortium Blockchain in Translation Services Industry. Wireless Personal Communications, 132 (2), 841-864.

[18] Verma, S., & Sheel, A. (2022). Blockchain for government organizations: Past, present and future.Journal of Global Operations and Strategic Sourcing, 15 (3), 406-430.

[19] Geng, H., & Long, Y. (2021, November). Study on the supply of urban public service facilities and the path of cracking based on public health emergencies. In Proceedings of the 57th ISOCARP World Planning Congress, Doha, Qatar (pp. 8-11).

[20] Han, P., Zhang, Z., Ji, S., Wang, X., Liu, L., & Ren, Y. (2023). Access control mechanism for the Internet of Things based on blockchain and inner product encryption. Journal of Information Security and Applications, 74, 103446.

[21] Li, X., Wang, H., & Ma, S. (2025). An efficient ciphertext-policy weighted attribute-based encryption with collaborative access for cloud storage. Computer Standards & Interfaces, 91, 103872.

[22] Zhou, C., Li, R., Xiong, X., Li, J., & Gao, Y. (2023). Optimization of triage time and sample delivery path in health infrastructure to combat COVID-19. Engineering, Construction and Architectural Management, 30 (8), 3620-3644.

[23] Bai, C., Zhu, Q., & Sarkis, J. (2021). Joint blockchain service vendor-platform selection using social network relationships: A multi-provider multi-user decision perspective. International journal of production economics, 238, 108165.

[24] M., Zhao, C., & Zhou, Y. (2022). From Bureau Coordination to a Data-Driven Model: Transformation and Capacity Building of Community-Based Prevention and Control of Public Health Events. International Journal of Environmental Research and Public Health, 19 (14), 8238.

[25] Kumar, S., Banka, H., & Kaushik, B. (2023). Ultra-lightweight blockchain-enabled RFID authentication protocol for supply chain in the domain of 5G mobile edge computing. Wireless Networks, 29 (5), 2105-2126.

[26] Hu, N., Li, X., Li, Y., Ye, Y., & Wu, M. (2023). Decision-making and optimization model for fire emergency replacements in colleges based on BWM and VIKOR under interval 2-tuple linguistic. Journal of Intelligent & Fuzzy Systems, (Preprint), 1-14.

[27] Liu, C., Wang, D., Li, D., Guo, S., Li, W., & Qiu, X. (2024). Trusted access control mechanism for data with blockchain-assisted attribute encryption. High-Confidence Computing, 100265.