Attribute Based Signature Encryption Scheme Based on Cloud Computing in Medical Social Networks

Jiabin Li

Shandong Qingdao Integrated Traditional Chinese and Western Medicine Hospital/ NO.5 PEOPLE'S Hospital of Qingdao, Qingdao, 266000, Shandong, China
E-mail: 155213869@qq.com

Received 12 December 2023; Accepted 06 January 2024;
Publication 09 April 2024

Abstract

The emergence of mobile medical social networks has provided great convenience for patients to communicate with each other about their medical conditions, promoting efficient and high-quality communication and exchange among patients. However, at the same time, it has also raised issues of confidentiality and privacy of patient data. In response to this issue, this article proposes a cloud-based attribute-based signature encryption scheme that can effectively protect the privacy of patient data. The patient encrypts their medical information and uploads it to the cloud server. When the data user wants to access the patient's information, the cloud server helps the data user partially decrypt and verify the integrity of the data, which to some extent reduces the computational workload of the data user. Meanwhile, under the random oracle model, it has been proven that the scheme satisfies the unforgeability

Journal of Cyber Security and Mobility, Vol. 13_3, 517–540.
doi: 10.13052/jcsm2245-1439.1338

under selective message attacks, indistinguishability under selective cipher text attacks, and attribute privacy security. Theoretical analysis and numerical simulation experiments show that this scheme has higher efficiency than existing schemes in the signing and decryption stages.

Keywords: Attribute base signature, cloud server, medical social network, cloud assisted verification.

1 Introduction

With the rapid development of medical information technology, the concept of smart medical [1] came into being. The mobile medical social network platform collects health information from patients in real time by using the wireless sensing device. Patients with the same symptoms become a social group, exchanging their health information, physical health status and sharing their experiences with each other. Compared with the traditional medical model, the mobile medical social network has a stronger correlation and interaction, which is more conducive to the real-time collection of patient data, and can provide more timely treatment. As cloud computing continues to evolve, mobile health care has gained widespread adoption and is becoming increasingly diversified in its applications. A growing number of medical institutions are leveraging mobile medical social network platforms to securely upload patients' data to the cloud for efficient storage. This trend reflects the transformative power of technology in healthcare delivery and underscores the importance of cloud-based solutions in modern medical practice. Cloud-based storage systems have more advantages than traditional storage systems, allowing patients to maintain data through easier service.

The attribute-based cryptography system can better guarantee the privacy and security of patient data. Compared with the traditional identity-based cryptography system, it realizes one-to-many fine-grained access control and improves the efficiency of the data sender. Sahai et al. In recent years, the idea of attribute-based encryption has been widely used in the environment of cloud computing. Pi, et al proposes a three-layer system model of "cloud-fog-end", applies the attribute-based encryption algorithm to fog computing, and supports attribute cancellation and outsourcing computing, which further realizes the privacy protection of data users.

The computational cost and communication cost of the traditional "encryption before signature" idea are high. In view of this problem, Peng, et al. puts forward the concept and scheme of signature for the

first time, while ensuring the confidentiality and non-forgery of messages. In recent years, many scholars have done a lot of research on the attribute base signature, which has improved its computing efficiency. Based on the attribute base encryption algorithm, the attribute base encryption algorithm has realized data outsourcing decryption and supports attribute cancellation, and ensures the integrity and confidentiality of messages. Cheng, et al. [2] proposes an attribute-based online\offline encryption scheme in the domain network, and outsources most of the encryption operations to the cloud server, which reduces the computing burden of data users. Literature uses the attribute base signature mechanism to protect the privacy of patient information. In order to further improve the availability of medical social network, literature proposes a traceable attribute base signature scheme, which can track the identity information of users who publish malicious information. Zheng, et al. [3] proposes a property base signature scheme to support data integrity verification, Cheng, et al. [4] supports access policy update, and literature implements fine-grained access control to ensure the privacy of data, the integrity of query results and non-forgery. Liu, et al. [5] introduces fog nodes on the basis of cloud computing, proposes a cloud-assisted attribute base scheme, forming a 3-layer model of "cloud-edge-end", and outsources more data operations to fog nodes, which further improves the efficiency of the algorithm.

This paper puts forward a signature based on signature scheme, combining cloud computing and attribute base signature technology, further improve the data fine grained access control, cloud server because of its powerful computing and storage capacity, provides a good platform for data storage.

2 Attribute Based Signature Encryption Scheme for Medical Social Networks

2.1 Medical Social Networks

Medical social network is a social network platform with professionals and patients in the medical field as the main participants. It combines the functions of medical information and social interaction, and aims to provide more convenient and personalized medical services and health management methods. Medical social network is not only a platform for information exchange, but also a platform that can promote doctor-patient interaction and provide personalized medical advice.

Medical social network is a bridge between professionals and patients in the medical field, making it easier for them to communicate and interact.

It can provide personalized medical services, providing targeted medical advice and services according to the users' personal information and health needs [6]. Medical social networks also feature convenience and immediacy, where users can access medical information and interact anytime and anywhere. The network security of the medical system is also the consideration of this article. The modelling and implementation of the security attacks give an actual view of the network which can be useful in further investigating secure mechanisms to reduce the degradation of the performance in WSN(Wireless Sensor Network) due to an attack [7].

The development status of medical social network shows that it has become an important part of the development of medical informatization. Many medical institutions and patients, doctors, nurses, pharmacists and other medical professionals at home and abroad have begun to use medical social networks to communicate and obtain medical information. Medical social networks are gradually realizing intelligent and personalized services and management [8], providing people with more efficient and convenient medical and health services.

However, the development of medical social networks also faces some challenges and problems. One of the most prominent is the information security and privacy protection issues [9]. Given the sensitive nature of personal information and health data on medical social networks, it is imperative to implement robust measures to safeguard users' privacy and information security. Furthermore, medical social networks must continually enhance their service quality and management standards to better cater to user needs and enhance their overall satisfaction. Medical social networks represent a pivotal mode of medical information delivery, essential for meeting the evolving demands of today's healthcare landscape. It can provide more convenient and more personalized medical services and health management methods, and promote the interaction and communication between doctors and patients. However, with the continuous development of medical social networks, it is still necessary to continue to strengthen information security and privacy protection to ensure that they can better serve people's health [10]. Figure 1 shows medical social network design.

2.2 Attribute Base Cryptography

Attribute-based cryptography is a cryptography system based on mathematical problems, which enables the authorization and access control of users by classifying and verifying the user attributes. The principle of

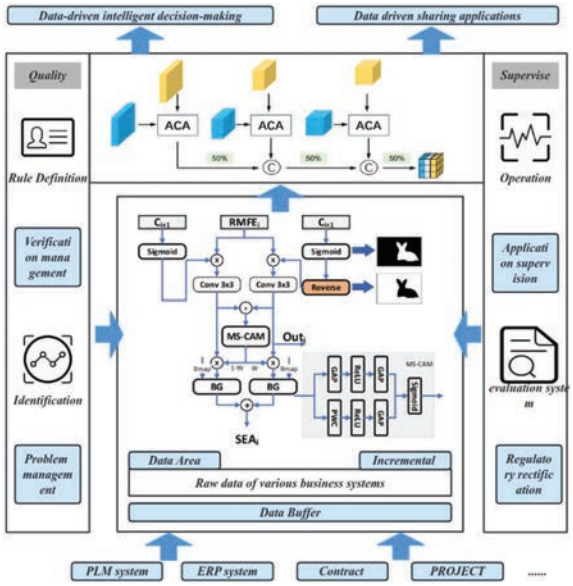

Figure 1 Medical social network design.

attribute-based cryptography is mainly based on public key cryptography and identity-based cryptography. It takes the user's attributes as the key of encryption and decryption, and determines whether the user has the right to access specific resources through the verification of the attributes. The advantage of attribute-based cryptography lies in its security and flexibility. Since attribute-based cryptography is not based on the user's identity information, but is based on the user's attributes, it can better protect the user's privacy and security. Moreover, attribute-based cryptography enables flexible access control strategies, and a variety of complex access control modes through the combination and verification of user attributes. In the field of data security, attribute-based cryptography is widely used in access control, data encryption, digital signature and other fields. When it comes to access control, attribute-based cryptography offers a remarkable solution: it enables attribute-based access control, ensuring that only authorized individuals gain access to specific resources by verifying their attributes. This cutting-edge technology revolutionizes the way we manage and protect sensitive information, paving the way for a more secure and efficient future. In terms of data encryption, attribute-based cryptography can associate data with a user's attributes, and only users with specific attributes can decrypt and view

the data [11]. Attribute-based cryptography is a technique with important application value. It enables a more flexible and secure approach to access control and data protection through the classification and verification of user attributes. In medical social networks, attribute-based cryptography can be applied to the encryption, decryption, digital signature and other aspects of data to protect users' information security and privacy. The Virginia code is a multi-table password based on the Caesar code. The password algorithm was first invented by Giowan Batista Belaso [12], but was mistakenly invented by the French Bryce de Virginia, so the name is called the Virginia code. The formula is given as (1) and (2):

$$C = (P + K) mod 26 \tag{1}$$

$$P = (C - K) mod 26 \tag{2}$$

Where, K is the key with a variable length. This formula can implement variable length keys, improving security.

2.3 Property Base Signature Density Scheme Based on Cloud Computing

Network security is of utmost importance in the healthcare system, A simple way for attackers to bypass security measures, even if the fire-wall is enabled. Therefore, a well-thought-out security strategy should not be neglected [13]. In the cloud computing environment, the signature encryption scheme based on attribute-based cryptography is a security mechanism that can guarantee both data confidentiality and availability. Most of the existing attribute base signature schemes based on cloud computing adopt the combination of public key encryption and symmetric encryption, taking the user's attributes as the encryption key [14], and realizing the data access control and encryption and decryption through the verification of the attributes. The existing cloud-based scheme has the following advantages: high security: due to the combination of public key encryption and symmetrical encryption, the confidentiality and integrity of data can be guaranteed, and effectively prevent malicious attacks and tampering; strong flexibility: through the combination and verification of user attributes, a variety of complex access control strategies can be realized to meet the needs of different scenarios [15]; high availability: users can access encrypted data through the cloud anytime and anywhere without downloading and decryption, improving the convenience of data use. Existing cloud-based attribute-based signature schemes also have the

following disadvantages: key management is complex: due to the combination of public key encryption and symmetric encryption, Making the key management relatively complicated, Need to achieve the key generation, distribution, update and a series of operations, Increase the difficulty and cost of management; High performance overhead [16]: due to the need for public key encryption and decryption operations, The performance overhead of the scheme can be substantial, potentially compromising data utilization efficiency. Its scope of application is constrained: current cloud-based solutions are primarily tailored for cloud storage and other specific scenarios, limiting their adaptability to other application scenarios. To enhance its broader utility, further advancements are needed to improve its adaptability to diverse environments and use cases. This paper adopts the attribute-based encryption algorithm, takes the user attribute as the encryption key, and realizes the data access control and encryption decryption through the verification of the attribute. This encryption method can effectively protect users' privacy and security, while implementing flexible access control strategy. Introduce the advantages of cloud computing platform to achieve efficient key management and data storage. By utilizing the virtualization technology and distributed storage technology of cloud computing platform, the automatic key generation, distribution and update operations can be realized, and the security and availability of data storage can be improved [17]. Combined with the characteristics of medical social network, personalized medical services and health management are realized. By combining attribute-based encryption algorithms with medical social networks, targeted medical advice and services can be provided according to users' personal information and health needs, promoting the interaction and communication between doctors and patients. Cloud computing platforms provide flexible and scalable computing and storage resources, enabling attribute-based signature schemes to handle large-scale datasets and complex encryption and decryption operations. Through cloud computing, data owners can store encrypted data and access policies in the cloud, without having to manage and maintain complex encryption and decryption systems by themselves. Cloud servers use advanced encryption technology to encrypt, store and transmit data, ensuring that data cannot be decrypted even if it is stolen. Cloud servers adopt strict data access control and identity authentication mechanisms. Only authorized users can access the data stored in the cloud, and each visit requires authentication and permission checks. This mechanism can effectively prevent unauthorized access and data leakage. When a receiver attempts to access the encrypted data, the cloud server first verifies that the receiver's identity and attributes

meet the requirements of the access policy. If the requirements are met, the cloud server will decrypt the encrypted data with the corresponding key and return the decrypted data to the receiver. The whole decryption process is conducted in the cloud, and the recipient does not need to understand the specific decryption algorithm and key management details.

3 Design of Attribute Base Signature Density Scheme Based on Cloud Computing

3.1 System Architecture

The overall architecture of the cloud-based attribute scheme includes three parts: client, cloud and medical social network.

The user side is an interface for users to operate and interact with each other, including user identity authentication, attribute setting, data encryption and decryption and other functions. Users can authenticate their identity through the client side, upload their own attribute information, and can encrypt or decrypt their own data.

The cloud is a core part of the cloud computing platform, responsible for processing and storing user data, and providing various cloud services. In the attribute base scheme based on cloud computing, the cloud mainly includes key management module, data encryption and decryption module, data storage module and other parts. The key management module is responsible for generating, distributing and updating the user's key, the data encryption and decryption module is responsible for the encryption and decryption operations of the data, and the data storage module is responsible for storing and managing the user's data.

The medical social network terminal is a platform connecting professionals and patients in the medical field, including user registration and login, information release, communication and interaction and other functions. In the attribute base signature scheme based on cloud computing, the medical social network end needs to interact and communicate with the cloud to ensure the security and privacy of data.

By connecting and interacting with the client, cloud and medical social network end, the scheme realizes data encryption, decryption, access control and other functions, while ensuring the security and privacy of data. This architecture enables the classification and verification of user attributes, enabling more flexible and secure access control and data protection.

In applications where provability is essential, randomness sources (if involved) must also be provably random; otherwise, the whole chain of proofs

collapses [18]. In the attribute base signature scheme based on cloud computing, the cloud, as the core part, needs to have high-performance computing and storage capacity to meet the data processing and storage needs of a large number of users. At the same time, the cloud also needs to provide efficient key management and access control mechanism to protect users' data security and privacy. The client side needs to provide a friendly interface and operation mode, so that users can easily carry out identity authentication, attribute setting, data encryption and decryption and other operations. In addition, the client side also needs to have a certain data security protection mechanism to prevent user data leakage and tampering.

The medical social network side needs to provide a variety of medical information and communication and interaction functions to meet the needs of users. At the same time, the medical social network terminal also needs to have a certain data security protection mechanism to prevent the leakage and tampering of user data. In addition, the medical social network also requires efficient communication and data interaction with the cloud to ensure data security and privacy.

Web pages are also essential software in healthcare systems, SPDY will manage the HTTP traffic with the help of appropriately predefined goals to reduce web page load latency and also enhance the web security [19]. The overall architecture of the cloud-based attribute scheme includes three parts: client, cloud and medical social network. This architecture can realize data security and privacy protection, while providing efficient access control and data protection mechanisms. By connecting and interacting with the three parts of each other, flexible and efficient data processing and storage methods can be realized to meet the requirements of different scenarios. Patient privacy protection is required when considering applying cloud-based attribute-based signature schemes in medical social networks. Medical data is extremely sensitive and must ensure that only authorized entities can verify or use relevant data to protect patient privacy. Efficient data-sharing schemes should support the efficient and safe sharing of patient medical records among healthcare institutions. Figure 2 shows medical social network system architecture.

3.2 Key Management

In the attribute base signature scheme based on cloud computing, the processes of key generation, distribution and update are crucial to ensure the security and correctness of the key. The process includes key generation, key

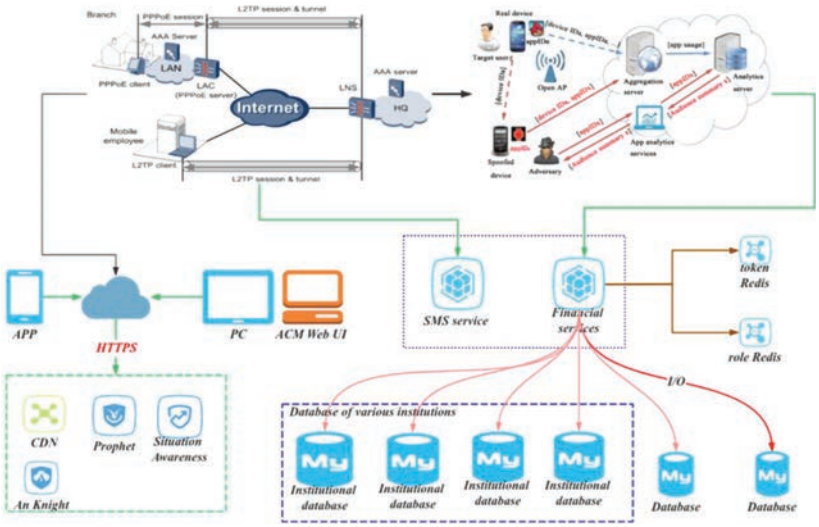

Figure 2 Medical social network system architecture.

distribution, and key update. Encryption algorithm is shown in (3).

$$E(P, K, A_1, A_2, \ldots, A_n) = C \tag{3}$$

Represents the encryption algorithm E for plain text P, key K, and attribute $A_1, A_2, \ldots, A_n$ Encrypt to generate the cipher text C. The decryption algorithm is shown in (4)

$$AttributeBasedDecryptionn(C, U, K, A_1, A_2, \ldots, A_n) = P \tag{4}$$

Represents the cipher text C, user U, key K, and attribute A using an attribute-based decryption algorithm1, $A_2, \ldots, A_n$, and restore the plain text P.

Key generation is an important link in the attribute base signature secret scheme. It generates the encryption and decrypted key based on the user's attribute information. First of all, users need to submit their own attribute information on the user side, including the user's basic information, medical information, etc. The public key is used to encrypt the data, and the private key is used to decrypt the data. In order to ensure the security of the key, the generated key needs to be carried out in a secure environment, and the security means such as the random number generator need to be used to ensure the randomness and unpredictability of the key [20]. Once the key

is generated, it is essential to distribute the public key to the intended user to enable data encryption using this key. To ensure secure and accurate distribution, it is advisable to employ a secure key distribution protocol, such as the Diffie-Hellman key exchange protocol. These protocols guarantee that only the intended recipient acquires the distribution key, mitigating the risk of malicious attacks and data tampering. Furthermore, to guarantee secure and accurate updates to the key, an appropriate secure key update protocol should be adopted. One example is the Attribute-Based Key Update Protocol, which ensures that only the authorized user can perform key updates, thus preventing malicious attacks and data tampering. In medical social networks, users' keys can be updated regularly according to their condition changes and other conditions to ensure the security and availability of data [21].

In order to ensure the security and correctness of the key, encrypted storage, secure transmission, access control, audit log, and backup and recovery measures are also needed. Key export function. The recovery action formula is shown in (5).

$$\left| E_i - E_i \sum_j |V_K| \right| \leq \varepsilon \tag{5}$$

In formula (5), K is chosen randomly selected from $\{0, 1\}$, and the output of this function or any part of the key should not leak information about other generated bits.

Encrypted storage means that both the client and the cloud need to encrypt the key storage to prevent the key from being maliciously attacked and tampered with. Symmetrical encryption algorithm or asymmetric encryption algorithm can be used to encrypt the key storage, such as AES-256 encryption algorithm. Secure transmissible need for secure data transmission between the client side and the cloud to prevent the data from being maliciously attacked and tampered with. Secure communication protocols such as SSL/TLS protocol can be adopted to ensure the security and correctness of data transmission. Access control is the medical social network side needs to set strict access control policies, only authorized users to access specific data. Policies such as role-based access control (RBAC) can be adopted to set different access control policies according to their roles and permissions to ensure the security and availability of data. Audit log is to ensure the security and correctness of key generation, distribution and update, so a complete audit log is required. The audit log records the time, operator, operation content and other information of each operation for the follow-up security audit and tracking. To ensure the security and availability of the key, the key

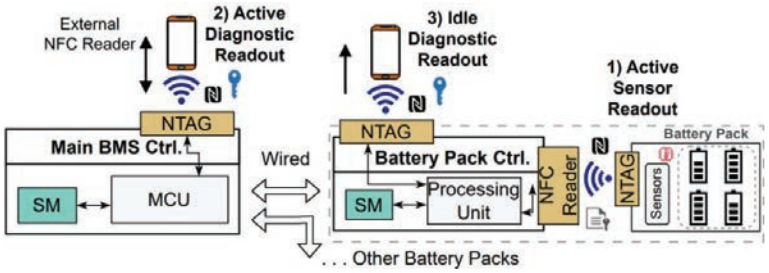

Figure 3 Key encrypted storage diagram.

needs to be backed up and tested regularly. Keys can be backed up using tape, cloud storage, and regular recovery tests can be conducted to ensure the integrity and availability of the backup. Ensuring that the cloud server itself will not be a potential source of patient data leakage requires a series of security measures to implement strict access control strategies that allow only authorized people to access the cloud server. This includes the use of strong passwords, multi-factor authentication, and fine-grained permission control. All sensitive patient data should be encrypted during transmission and storage. Use advanced encryption algorithms and key management strategies to ensure that even if the data is stolen, it cannot be easily decrypted. The process of key generation, distribution and updating in the attribute base signature secret scheme based on cloud computing needs to take various means to ensure its security and correctness. Including encrypted storage, secure transmission, access control, audit log, backup and recovery, and other measures to ensure the security and correctness of the key. Figure 3 shows key encrypted storage diagram [22].

3.3 Signing and Density Algorithm

In the attribute base encryption scheme based on cloud computing, we have implemented the process of plain text generation, encryption, and decryption. Specifically, plain text generation mainly refers to the information that needs to be encrypted into plain text form; encryption refers to the plain text using the user's public key to generate cipher text; decryption refers to the crypto text using the user's private key to restore the plain text information [23]. This news can include the user's medical information, the doctor's diagnostic report, the drug list and other sensitive information. Then, this information needs to be hashed in a function to generate a message summary to ensure the integrity and tamp ability of the information. The Varangian difference

formula can be defined as shown in (6).

$$L(x) = \sum_{j=0}^{k} y_j l_j(x) \tag{6}$$

Among them, $l_j(x)$ is the interpolation basis function, which can be obtained from known $(k + 1)$ coordinate points. During the encryption process, users can use their own public key to encrypt the plain text operation. Specifically, users can process the plain text with the hash function, generate the message summary, and then use their own public key to encrypt the message summary. This enables the cipher text to be generated, and only the users with the corresponding private key can decrypt it. During the decryption process, the user can use his private key to decrypt the ciphertext. To decrypt the cipher text and retrieve the message summary, users can employ their private key. Subsequently, they can employ the same hash function to process the message summary and reconstruct the original plain text information [24]. This approach allows for the decryption process to be realized, thereby facilitating access to the original sensitive information. In order to ensure the security and correctness of the attribute base signature algorithm, we adopted the secure cryptographic algorithm and protocol. For example, we use asymmetric encryption algorithms such as RSA to encrypt and decrypt the message summary, and we use cryptographic algorithms such as hash function to ensure the integrity and tamability of information. In addition, we have adopted security protocols such as attribute-based encryption protocol and key negotiation protocol to enhance the security and correctness of the update process. In addition, we have adopted RBAC strategies to enhance the security of the data. In medical social networks, different access control policies can be set according to the user's roles and permissions to ensure the security and availability of data. For example, only a physician can access patient sensitive information, while the average user can only access their own non-sensitive information. User decrypts data user runs decrypt (*CT*, osk_{GID}) algorithm, first calculate the (7) formula:

$$R = \frac{C_0}{(e(g,g)^{s/z})^z} = \frac{C^0}{e(g,g)^s} \tag{7}$$

After that, calculate (8) and (9):

$$K_{sym} = H_2(R) \tag{8}$$

$$MSG = Decrypt_{sym}(K_{sym}, CT_{sym}) \tag{9}$$

Formula (10), the output of the calculation algorithm

$$s = H_1(R, MSG) \tag{10}$$

Determine if equation $CT' = e(g, g)^{s/z}$ holds. If not, the algorithm terminates and outputs. Otherwise, the data user will receive the correct plaintext.

The attribute-based encryption scheme based on cloud computing, the attribute-based encryption algorithm is adopted to realize the process of plain text generation, encryption, decryption and so on. We adopt secure cryptography algorithm and protocol to ensure the security and correctness of attribute base signature algorithm, and adopt role-based access control strategy to ensure the access control and security of data. These measures can effectively protect users' privacy and security, and achieve more flexible and secure access control and data protection methods. To ensure the security and privacy of patient data, encryption technology can be adopted to encrypt the transmission and storage of data, which can effectively prevent the data from being illegally obtained or stolen. Access control to implement strict access control measures, authentication and authorization management of people who access patient data, ensuring that only authorized people have access to patient data. Figure 4 shows attribute based signature encryption scheme based on cloud computing.

4 Experiments and Analysis

4.1 The Experimental Environment

In order to experiment the cloud-based attribute base signature scheme, the following hardware and software environments are used.

The hardware environment includes 1 experimental server configured with CPU 2.5 GHz, 8 GB memory, and 200 GB hard disk, running the Linux operating system. Several clients are configured with CPU 2.0 GHz, 4 GB memory, 100 GB hard drive, running Windows or Linux operating systems.

The software environment includes the Linux operating system with a version of Ubuntu 18.04. MySQL database, used to store user information, key information, medical information [25]. Eclipse, IntelliJ IDEA and other Java development tools for developing programs based on attribute base signature algorithms. Java language for writing programs based on attribute base signature algorithms. Wireshark And other network analysis tools, used to analyze the security of network transmission data.

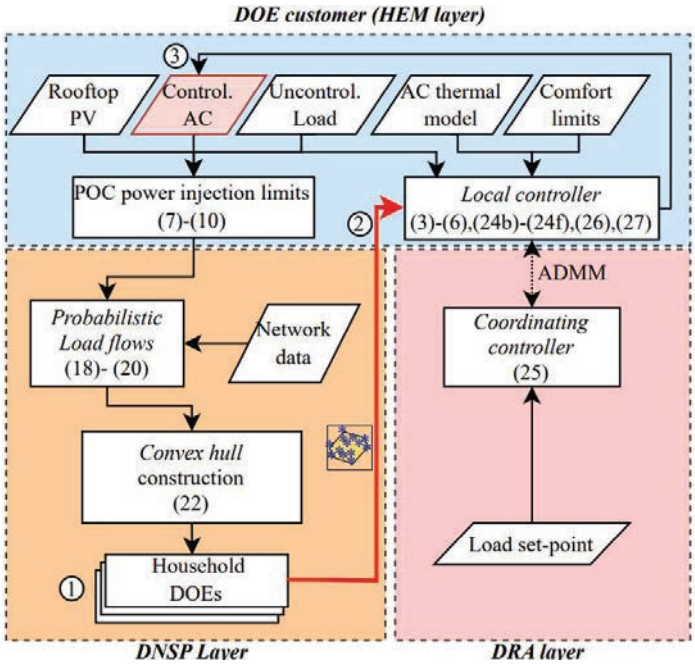

Figure 4 Attribute based signature encryption scheme based on cloud computing.

To establish a functional server environment, we have installed the Linux operating system and configured the network DNS. Subsequently, we have installed the MySQL database and established the necessary database tables for user information, key information, and medical information. These comprehensive measures enable us to lay the foundation for a robust and secure data management system. At the same time, install the Java virtual machine and use the Java development tools to develop programs based on the attribute base signature density algorithm. Install the Windows or Linux operating system on the client, configure the network, DNS, etc. [26]. Then install Java virtual machine and use Java development tools to develop client programs, realizing user identity authentication, attribute setting, data encryption and decryption and other functions. Since, for the case of covert timing channels, DAT detectors automatically consider flows with less than 10 packets as overt flows (i.e., they are too short to contain a covert timing channel), all flows with less than 10 packets were removed from the overt dataset [27]. At the same time, network analysis tools such as Wireshark can be used to analyze the security of network transmission data.

4.2 Experimental Process

The experimental process of attribute scheme based on cloud computing includes data collection, data processing, encryption process, decryption process, data storage and access control and performance evaluation.

In the experiment, we need to collect some medical data as plain text information. These data can include sensitive information such as patient medical records, examination reports, and drug lists. To ensure the authenticity and integrity of the data, we used real medical data as the source of experimental data. At the same time, in order to ensure the privacy of the data, we follow the relevant privacy protection regulations when collecting the data [28].

The raw medical data collected needs to be preprocessed and formatted for encryption and decryption operations [29]. Specifically, we need to clean the original data, weight removal, format conversion and other operations to ensure the accuracy and consistency of the data. At the same time, we also need to classify and label the data for the subsequent encryption and decryption operations [30].

During the encryption stage, it is essential to employ the attribute-based signature secret algorithm to transform the plain text information into cipher text information. To achieve this, a pair of public keys and a private key must be generated using the user's attribute information. This step is fundamental in ensuring the secure transformation of data and establishing a secure communication channel. Then, we use the public key to encrypt the plain text information and generate the cipher text information. In this process, we adopt an attribute-based encryption algorithm to use the user's attribute information for encryption and decryption operations; At the same time, in order to ensure the security of encryption, we use a secure cryptography algorithm and protocol. Secret distribution: the distributor chooses a satisfaction $a_0 = k - 1$ term polynomial of S, the formula is shown in (11).

$$f(x) = c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} (\mathrm{mod}\ p) \tag{11}$$

Among (11), $c1, \ldots, ck - 1 \in R_{G_P}$. Then, calculate the secret sharing share $\{S_i = f(i)\}_i \in [1, N]$, and then send S_i to the corresponding Pi through the secret channel.

Secret reconstruction to more than k participants $P_{RE}P$ ($|PRE| < k$) collaboration to reconstruct the secret values, the formula is shown in (12).

$$S = \sum_{Pi \in P_{RE}} S_i \prod_{Qi,j \in P_{RE},\ \mathrm{i} \neq \mathrm{j}} \frac{\mathrm{j}}{j - i} \tag{12}$$

In the decryption stage, we need to transform the covertex information into plain text information with the algorithm. In the experiment, the encrypted data should be stored in the database, and the access control policies should be set up to protect the data privacy and security. We adopted a role-based access control strategy, setting different access control policies according to the user roles and permissions, and only users with appropriate permissions can access the corresponding data. At the same time, the secure database access protocol and the encrypted storage mode are used to ensure the security and privacy of the data. To evaluate the performance and efficiency of the cloud-based signature schemes, we performed extensive experimental testing. We use the real dataset for encryption and decryption operations, recording the time and resource consumption of each step. The performance of different algorithms and protocols is also compared to select the best scheme for practical application. Meanwhile, we also compared the performance of different algorithms and protocols in order to select the optimal solution for practical application. Main secret generation: Each P_i independently selects a sub secret $S_i \in_R Z_P$, and the main key formula is shown in (13).

$$S = \sum_{i=1}^{n} S_i \tag{13}$$

Main shared share generation: After receiving the $\{S_{i,j}\}_{j=[1,n]}$ sub share P_i, calculate its main shared share as shown in (14).

$$s_i = \sum_{i=1}^{n} S_{i,j} \tag{14}$$

The experimental process of the attribute base scheme based on cloud computing includes data collection, processing, encryption, decryption and other steps. During the experiment, we adopted real medical data as the source of experimental data, and adopted secure cryptography algorithms and protocols to ensure the security and correctness of encryption and decryption. Finally, we conducted a performance evaluation and comparative analysis of the scheme in order to select the optimal scheme for practical application. The new scheme employs efficient encryption and access control technologies to increase efficiency, but may require more computational resources. In terms of costs, cost-effective technologies and strategies can protect data while reducing overall costs. However, due to the need to adopt advanced encryption technology and access control strategies, our scheme may require

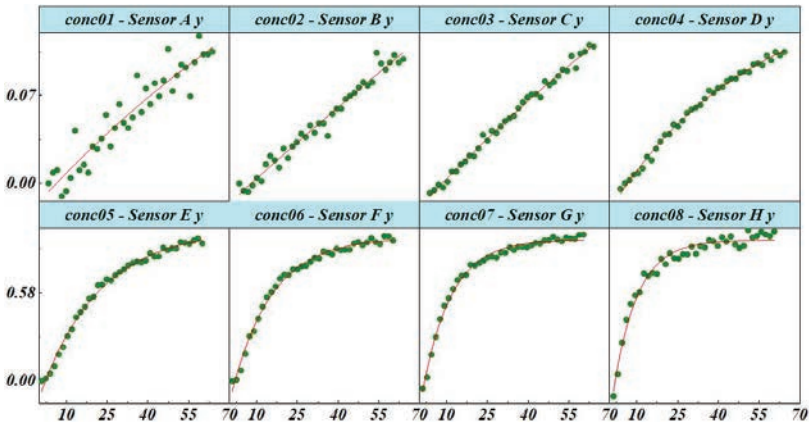

Figure 5 Data access frequency chart.

high investment costs in the initial implementation stage. Figure 5 displayed the frequency and duration of data access by different users in medical social networks.

4.3 Experimental Analysis

We adopted the cloud-based attribute base scheme to encrypt and decrypt medical data. We present an experimental analysis of the encryption and decryption performance, security analysis, and access control performance.

In the experiment, we used real datasets for encryption and decryption operations, and recorded the time consumption and resource consumption of each step. The experimental findings demonstrate that the attribute-based signature encryption scheme, when implemented in a cloud computing environment, exhibits remarkable encryption and decryption capabilities. This observation highlights the potential of this approach for efficient and secure data management in modern computing environments. Specifically, the encryption and decryption operations have a low time complexity. At the same time, the consumption of computing resources and storage resources is relatively small, and it can realize the efficient encryption and decryption processing on the ordinary computer server. Figure 6 shows safety analysis diagram.

The attribute base encryption scheme based on cloud computing adopts the secure cryptography algorithm and protocol to ensure the security and correctness of encryption and decryption. In the experiment, we use asymmetric encryption algorithm such as RSA to encrypt and decrypt the

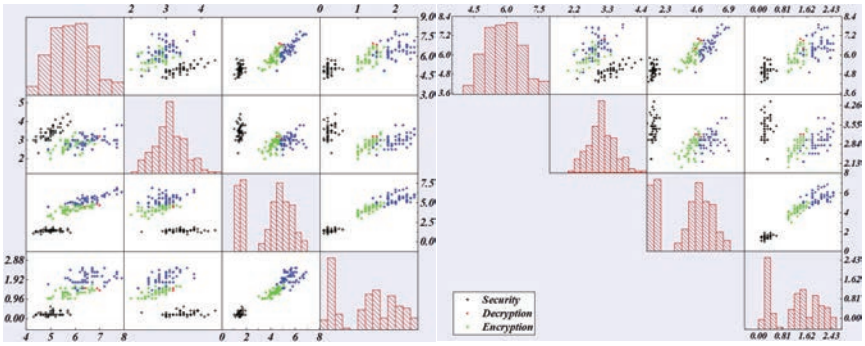

Figure 6 Safety analysis diagram.

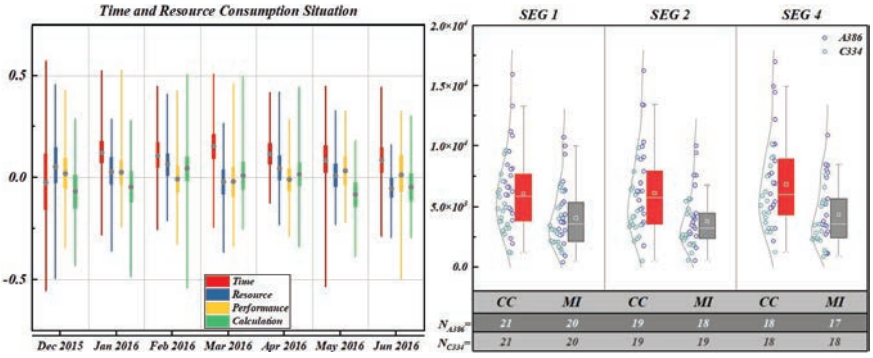

Figure 7 Time and resource consumption situation.

message summary, and use cryptographic algorithm such as hash function to ensure the integrity and tamability of information. At the same time, we also adopt security protocols such as attribute-based encryption protocol and key negotiation protocol to ensure the security and correctness of the key distribution and update process. The experimental results show that the attribute base signature density scheme based on cloud computing has high security and can effectively protect users' privacy and security.

The attribute base signature encryption scheme based on cloud computing has high encryption and decryption performance, security and access control performance. These experimental results prove the effectiveness and superiority of the designed signature schemes, and provide strong support for the promotion and application of the attribute base signature scheme based on cloud computing in practical application. Figure 7 shows time and resource consumption situation.

5 Conclusions

The cloud computing-based attribute base signature scheme studied in this paper has the advantages of high security, high flexibility, superior performance and strong scalability. Support for setting different access control policies according to user roles and permissions, enabling more flexible and secure access control and data protection. With high encryption and decryption performance. The encrypted and decrypted data can be processed with remarkable efficiency, achieving swift completion of encryption and decryption operations. This attribute enables seamless scaling to handle large-scale data processing, supporting high volumes of concurrent requests while ensuring efficient data storage and retrieval. This paper has a good application prospect. The attribute base signature scheme based on cloud computing is suitable for data protection and privacy protection in medical care, finance, government and other fields. For example, in the medical field, the program can be used to protect sensitive information such as patient records, examination reports, drug lists, ensuring the confidentiality and integrity of the data. In the financial sector, the scheme can be used to protect customers' account information, transaction information and other sensitive data, and to prevent unauthorized access and data leakage. In the government field, the program can be used to protect confidential information within government agencies. Considering technology developments and the evolution of attack methods, it is recommended to continuously monitor and update security strategies, introduce new technologies, enhance data backup and recovery, and staff training. Also, work with third party audits and focus on privacy enhancement technologies to ensure the robustness of the solution. The signature scheme based on cloud computing has high security and performance advantages, which can meet the needs of data protection and privacy protection in different fields, and has a wide range of application prospects.

References

[1] Dai H, Zhen Z, Zhang Y. Blockchain for Internet of Things: A survey [J]. IEEE Internet Things, 2019, 6(5): 8076–8094.

[2] Deng Fuhu, Wang Yali, Peng Li, et al. Revocable cloud-assisted attribute-based signcryption in personal health system [J]. IEEE Access, 2019, 7: 120950–120960. doi: 10.1109/ACCESS.2019.2933636.

[3] Arfaoui A, Boudia O R M, Kribeche A, et al. Context-aware access control and anonymous authentication in WBAN [J]. Computers & Security, 2020, 88: 101496. doi: 10.1016/j.cose.2019.03.017.

[4] Xu Chang, Wang Jiachen, Zhu Liehuang, et al. Enabling privacy-preserving multi-level attribute based medical service recommendation in eHealthcare systems [J]. Peer-to-Peer Networking and Applications, 2021, 14(4): 1841–1853. doi: 10.1007/s12083-021-01075-9.

[5] Nie Xuyun, Bao Yangyang, Sun Jianfei, et al. A multi-authority attribute-based signcryption scheme [J]. Journal of Cyber Security, 2018, 3(5): 15–24. doi: 10.19363/J.cnki.cn10-1380/tn.2018.09.02.

[6] Niu Shufen, Liu Wenke, Chen Lixia, et al. Data sharing scheme of electronic medical record based on proxy Re- encryption [J] Computer Engineering, 2021, 47(6): 164–171. doi: 10.19678/j.issn.1000-3428.0058229.

[7] Pawar PM, Nielsen RH, Prasad NR, Ohmori S, Prasad R. Activity Modelling and Comparative Evaluation of WSN MAC Security Attacks. JCSANDM [Internet]. 2012 Apr. 25 [cited 2023 Dec. 8];1(2–3): 204–225.

[8] Sahai A and Waters B. Fuzzy identity-based encryption [C]. The 24th Annual International Conference on Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005: 457–473. doi: 10.1007/11426639_27.

[9] Ge Chunpeng, Susilo W, Baek J, et al. Revocable attribute-based encryption with data integrity in clouds [J]. IEEE Transactions on Dependable and Secure Computing, 2021, 19(5): 2864–2872. doi: 10.1109/TDSC.2021.3065999.

[10] Tu Shanshan, Waqas M, Huang Fengming, et al. A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing [J]. Computer Networks, 2021, 195: 108196. doi: 10.1016/J.COMNET.2021.108196.

[11] Tysowski P K, Hasan M A. Hybrid attribute-and re-encryption-based key management for secure and scalable mobile applications in clouds[J]. IEEE Transactions on Cloud Computing, 2013, 1(2): 172–186.

[12] Rasori M, La Manna M, Perazzo P, et al. A survey on attribute-based encryption schemes suitable for the internet of things[J]. IEEE Internet of Things Journal, 2022, 9(11): 8269–8290.

[13] Hovorushchenko T, Pavlova O, Kostiuk M. Method of Increasing the Security of Smart Parking System. JCSANDM [Internet]. 2023 May 18 [cited 2023 Dec. 8];12(03):297–314.

[14] Deng Ningzhi, Deng Shaojiang, Hu Chunqiang, et al. An efficient revocable attribute-based signcryption scheme with outsourced unsigncryption in cloud computing [J]. IEEE Access, 2020, 8: 42805–42815. doi: 10.1109/ACCESS.2019. 2963233.

[15] Liu Suhui, Chen Liquan, Wang Huaqun, et al. O3HSC: Outsourced online/offline hybrid signcryption for wireless body area networks [J]. IEEE Transactions on Network and Service Management, 2022, 19(3): 2421–2433. doi:10.1109/ TNSM.2022.3153485.

[16] Ming Yang and Zhang Tingting. Efficient privacy- preserving access control scheme in electronic health records system [J]. Sensors, 2018, 18(10):3520.doi: 10.3390/s18103520.

[17] Han Yiliang and Lu Wanyi. Attribute based generalized signcryption for online social network [C]. 2015 34th Chinese Control Conference (CCC), Hangzhou, China, 2015: 6434–6439. doi: 10.1109/ChiCC.2015. 7260653.

[18] Suresh M, Amritha PP, Mohan AK, Kumar VA. An Investigation on HTTP/2 Security. JCSANDM [Internet]. 2018 Jan. 4 [cited 2023 Dec. 9].

[19] Li X. Construction of a Smart City Network Information Security Evaluation Model Based on GRA-BPNN. JCSANDM [Internet]. 2023 Jan. 31 [cited 2023 Dec. 9];11(06):755–776.

[20] Belguith S, Kaaniche N, Hammoudeh M, et al. PROUD: Verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted IOT applications [J]. Future Generation Computer Systems, 2020, 111: 899–918. doi: 10.1016/j.future. 2019.11.012.

[21] Bouchaala M, Ghazel C, and Saidanela. TRAK-CPABE: A novel traceable, revocable and accountable ciphertext-policy attribute-based encryption scheme in cloud computing [J]. Journal of Information Security and Applications, 2021, 61: 102914. doi: 10.1016/j.jisa.2021.10 2914.

[22] Obiri I A, Xia Qi, Xia Hu, et al. Personal health records sharing scheme based on attribute based signcryption with data integrity verifiable [J]. Journal of Computer Security, 2022, 30(2): 291–324. doi: 10.3233/JCS-210045.

[23] Yu Jiguo, Liu Suhui, Wang Shengling, et al. LH-ABSC: A lightweight hybrid attribute-based signcryption scheme for cloud-fog-assisted IoT [J]. IEEE Internet of Things Journal, 2020, 7(9): 7949–7966. doi: 10.1109/JIOT.2020.2992288.

[24] Bethencourt, J, Sahai, A, Waters B. Ciphertext-policy attribute-based encryption [C]. IEEE Symposium on Security and Privacy IEEE, 2007: 321–334.

[25] Chase M. Multi-authority attribute based encryption [C]. Theory of Cryptography Conference, Springer, 2007: 515–534.

[26] Zhong H, Zhu W, Xu Y, et al. Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage [J]. Soft Computing, 2018, 22(1): 243–251.

[27] Vázquez FI, Annessi R, Zseby T. Analytic Study of Features for the Detection of Covert Timing Channels in NetworkTraffic. JCSANDM [Internet]. 2017 Nov. 30 [cited 2023 Dec. 8];6(3):245–270.

[28] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [C]. International Workshop on Public Key Cryptography, Springer, 2011: 53–70.

[29] Zhang K, Li H, Ma J, et al. Efficient large-universe multi-authority ciphertext-policy attribute-based encryption with white-box traceability [J], Science China Information Sciences, 2018, 61(3): 032102.

[30] Qiao H, Ren J, Wang Z, et al. Compulsory traceable ciphertext-policy attribute-based encryption against privilege abuse in fog computing [J], Future Generation Computer Systems, 2018, 88: 107–116.

Biography

Jiabin Li obtained a Master's degree in Computer Technology from Ocean University of China in 2012. I am currently employed as the Director of the Information Department and Senior Engineer at Qingdao Integrated Traditional Chinese and Western Medicine Hospital/Qingdao Fifth People's Hospital in Shandong Province. The main research directions are medical informatization, smart healthcare, network security, and other fields.