RSA-ABE: A Hybrid Encryption Approach for Medical Privacy Data with Cloud Storage

Yiheng Sun and Chenxu Li

Abstract Increasing sensitive medical data raises medical privacy concerns. Unauthorized access endangers patients. We propose an approach using ciphertext-policy attribute-based encryption (CP-ABE) and RSA to enable secure and controlled access to medical data based on user-defined access policies. Our approach enables: (1) Patient-defined fine-grained access control policies; (2) Secure "one-to-many" sharing with authorized users; and (3) Encrypted policy and data transmission. We generate CP-ABE keys and use socket programming to enable patient-user communication. The patient defines an attribute-based access policy. CP-ABE encrypts medical data under this policy. RSA encrypts the public key for transmission to users. Users submit attributes; If users' attributes satisfy the policy, the ciphertext can be decrypted, authenticating the users. Results show the hybrid scheme achieves secure, controlled medical data sharing through patient-defined access policies. Patients need not know accessing users in advance. Only authorized users related to a patient's condition access data.

Keywords Access control · CP-ABE · Hybrid encryption · Medical privacy

1 Introduction

First of all, we give a brief introduction to this paper from three aspects: background and related work, our solution and solution and contributions.

1.1 Background and Related Work

Cloud storage, as the further development of distributed computing, are widely used through the advantages of fine-grained price and high scalability. It provides users

Y. Sun (✉) · C. Li
Zhengzhou University, Zhengzhou, China
e-mail: yh_xsyx@163.com

W. Wang et al. (eds.), *Communications, Signal Processing, and Systems*, Lecture Notes in Electrical Engineering 1032, https://doi.org/10.1007/978-981-99-7505-1_2

with online storage services available anytime and anywhere, so that users can store local data into the cloud server. Thus, it facilitates people's life to a large extent. At the same time, it also has problems with information leaks, illegal access and so on. If medical privacy data is obtained by some illegal elements for illegal activities, it may cause great trouble to patients' life and even endanger the life of the owner. Therefore, the security of medical privacy data must be inseparable from access control.

Attribute-based Encryption assigns certain attributes to each legitimate participant. According to the Attribute set of the participant, the data owner formulates an access policy and encrypts the data. Only the data visitor whose attributes meet the access policy can decrypt the data. So, It can effectively protect medical privacy data.

Attribute encryption is derived from identity encryption (IBE), which was first proposed by Shamir in 1984 [1]. In 2020, Zheng et al. [2] proposed an attribute-based data sharing scheme that supports efficient revocation of users, allowing users to join, revoke and re-join efficiently. In 2021, Gao et al. [3] combined blockchain, CP-ABE and IPFS to propose a blockchain-based personal data secure sharing and privacy protection solution. In 2021, Hijawi et al. [4] proposed a lightweight KP-ABE scheme. In 2022, Li et al. [5] introduced a white-box traceable CP-ABE scheme that can solve the problems of user and authorization center key abuse.

These Attribute-based Encryption schemes use ABE encryption and decryption locally. However, data security is not guaranteed in the process of two-terminal communication transmission. These hybrid encryption schemes do not implement access control. Therefore, in order to remedy this defect, we propose a hybrid encryption approach: RSA-ABE. In this scheme, we not only uses ABE to implement access control of medical privacy data, but also uses RSA to encrypt ABE keys. Because this way can enhance the security of two-terminal communication. And in two-terminal communication, the mpk used for encryption needs to be transmitted through the two-terminal communication, which ensures the security of the mpk during transmission. This is different from the local use of ABE encryption and decryption.

1.2 Our Solution

The purpose of this paper is to design an access control approach, which not only satisfies the requirement that a person can specify his own access policy, namely fine-grained access, but also satisfies the requirement that users with legal permissions can access the resources they have the right to access, while illegal users or malicious users cannot access the protected resources. Medical privacy data access control based on attribute encryption, patients do not need to know in advance which medical staff can view their medical data, and in order to enhance the security of patients' health privacy, only medical staff related to the patient's condition can access the patient's medical data, that is, in addition to protecting the security of patients' medical data, One-to-many data sharing and flexible access control are also required. The data owner can precisely control the data user who decrypts the Ciphertext by

embedding the developed access policy in the ciphertext. With fine-grained access control. The patient only needs to formulate access policies for encrypted medical data according to the attributes of the authorizer. If the attributes of the user meet the access policies defined by the patient, the corresponding medical data can be obtained by decrypting the ciphertext.

1.3 Contributions

- CP-ABE is used to control access to medical privacy data, meet the "one-to-many" data sharing and flexible access control, and protect data security.
- Implement user-driven authorized access, where users can define their own access control policies and follow their own privacy preferences.
- Compared with traditional medical data access control, attribute-based access control is fine-grained, flexible, adaptable to the cloud environment, and does not require users to manage keys online.

2 Hybrid Encryption System

This paper uses hybrid encryption system (CP-ABE and RSA) to realize access control and protect data security. The process of hybrid encryption as Fig. 1.

Example: As shown in Fig. 1, Alice generates ABE keys (public parameters mpk and master key msk), then uses RSA to encrypt mpk to s_mpk. This ensures the security of mpk during transmission. Then, when Alice and Bob establish a

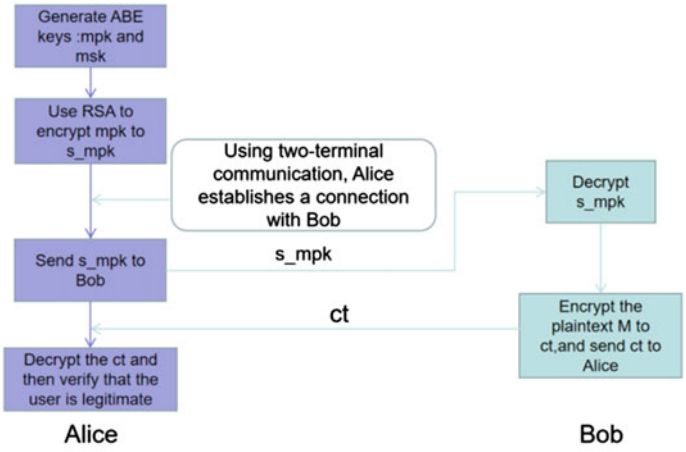

Fig. 1 The process of hybrid encryption

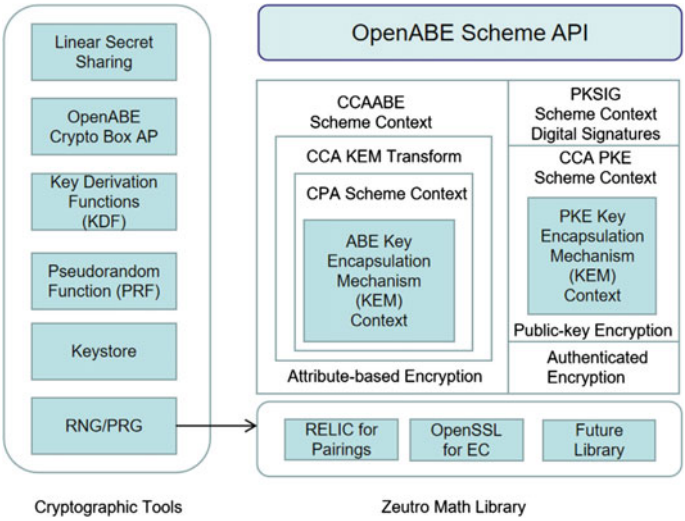

Fig. 2 OpenABE architecture diagram

connection using two-terminal communication, Alice sends s_mpk to Bob. After receiving s_mpk, Bob decrypt it. Moreover, Bob encrypts the plaintext M to CT, and send CT to Alice. After Alice receives the CT, she decrypts it. And then, Alice can verify the legitimacy of the user.

2.1 OpenABE

This article uses the attribute encryption and decryption library OpenABE. The architecture diagram is as Fig. 2.

In this paper, CP-ABE in OpenABE is used. The encryption and decryption process is as Fig. 3. After initializing the OpenABE library by constructing the Crypto Box context and generating domain parameters, you can perform key generation by specifying attributes, attribute lists, and access policies, then encrypt messages under a chosen access policy with the public key, and authorized users can decrypt the ciphertexts and recover the original messages using their private keys.

2.2 Two-Terminal Communication

As illustrated in Fig. 4, to achieve two-terminal communication between the Server and Client, two dedicated and non-interfering threads, one handling input and the other output, need to be implemented on both sides.

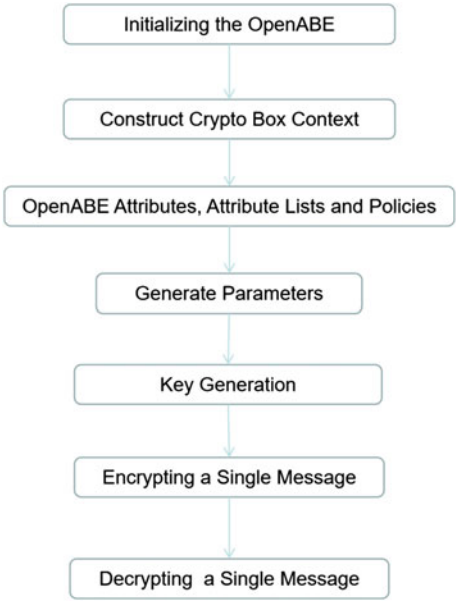

Fig. 3 The encryption and decryption process

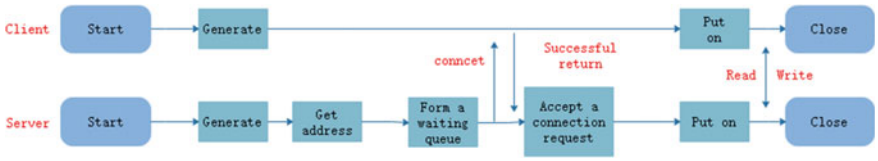

Fig. 4 The two-terminal communication process

3 Experiment and Results

This article adopts RSA-ABE: A Hybrid encryption Approach for Medical Privacy Data with Cloud Storage. This article not only uses ABE to implement access control of medical privacy data, but also uses RSA to encrypt ABE keys. Because this way can enhance the security of two-terminal communication. And in two-terminal communication, the mpk used for encryption needs to be transmitted through the two-terminal communication, which ensures the security of the mpk during transmission.

We use CP-ABE to realize access control, allowing patients to define the access control structure by themselves, and specifying people to access their medical privacy data, so that the control is fine-grained and flexible. In the process of public key transmission, the asymmetric key RSA is used for encryption to realize data confidentiality. One end defines the access control structure, and the other end uses attributes to decrypt access, which satisfies the characteristics of cloud storage.

```
CP-ABE key
mpk = AAAAFqpvyT/mYIB25dlWrNRvbe9L23ltcGsAAAHToQFBsgEEtLIBAANBC9Ko6QWZZ5qUvUbUvQ
tlFW+aBvVfOi9xdFe04gpIAd0x+o65uTTatNk4mIt5DN7EvYX6WeZ27Sp7v92e7EgdikyGk+CXK7j4Un
guaKk96xu+mLbT/LSSWnnSrcVvuQBKH7+3fhCab3wSDd4m66jy84KtgeN2F2jO0UwLfIp+ByfoRs7xBA
mpXhKZPqv/vfGrshCFT3UeSNeWUaskR2UMz3Z+iqvMjggdSmcy6I6+YJ9m4mjGtHbI4KDRfEEhMCGV+J
+2bJi/F9m0KT0rCj+GmY7A3u9pTDJ0PXywn6psBMKJiKoMY4lUs6x984sCfalijtW7LXxaWqRheIoRmP
KhAmcxoSSyoSEDCJ8DuANsYA0BVendQ+YOPs2fvu26oEIeNnGlprmaWiKhA2cxYaEksqEhAwiHbbpgVp
iOakaKS6gUiGhEqastgmDiHFiIDFte87GRoQJnMqFEs6FBAhKDU6W4dLXcmzu4KnEmHT/sExppqd5w7W
9Sh7igO1wiG5v6WMQJliRehnyKj+0PmBkp0wVyztkc32Rjxo8GWz6hAWuhJR0AAAAgywTxRr1gTii7Rx
e10Ytd2avi7DkMUaPdIQNbGffzk78=
```

Fig. 5 Mpk

1. First, generate mpk and msk at the A terminal. As shown in Fig. 5.
2. Then, use RSA to encrypt mpk on end A.
3. The connection between A terminal and B terminal is established. As shown in Fig. 6.
4. The encrypted data is sent to B terminal. As shown in Fig. 7.
5. After receiving the encrypted mpk, B terminal decrypts the mpk using RSA. Then, use CP-ABE to encrypt data. As shown in Fig. 8.
6. The encrypted data is sent to A terminal. As shown in Fig. 9.
7. A terminal decrypts and verifies whether the user is legitimate. The result is shown in Fig. 10.

In this experiment, first, the public and private keys of CP-ABE are randomly generated, and then stocket is used to establish the two-ended communication. After

```
server_fd = 3
lo ipv4 address = 127.0.0.1
ens33 ipv4 address = 192.168.22.136
ens34 ipv4 address = 192.168.22.138
ens35 ipv4 address = 192.168.22.137
lo ipv6 address ::1
ens33 ipv6 address fe80::20c:29ff:fe61:4e09
ens34 ipv6 address fe80::9f1e:a3:d4a8:78d5
ens35 ipv6 address fe80::8aa6:8166:d961:10f5
Bind success!
Server port number = 34316
Server ipv4 addr: 192.168.22.137
Listening ...
Client accepted: IP addr = 192.168.22.137, port = 41794
```

```
Input server's hostname/ipv4:  192.168.22.137
Input server's port number: 34316
server's official name = 192.168.22.137
        server address = 192.168.22.137
local socket ip addr = 192.168.22.137, port = 41794
```

Fig. 6 Establish a two-terminal connection

```
                                        server 192.168.22.137 >>>> nb7Jq3nehmXRa
gkhKg2ybiAxDgX4v19XQxZsAwj+ft8cdIDH66D51mjOf+kSrrbXSapNJ/ENp18Gb0wrQ1p0Z0WIUsWND
jhpCJSEEH8jCIpV1sXbbCWb6it8+4DaNAweNWdM1vCtmqfrTfXlI/K70z2EbvBa0uS0ViWm8HLJxQ3Wl
GeB3pso4EknfuZyHkngRq8IIFMUIkeqzvUtT8Tln/USlVEe7dKXhILlQqo0jvY/v9je13gz0DonL08Jj
ONmCmrAGrf4S4Gz2exIAUIcl2O6PjrB+/HzMjoM0/MPuWIKgjeRA8I5wflIXi2pmJ7Vlo7OYbg7WuGpp
N34RDOOeJW0tfXcC/DnuLOstS0N7Uk7MvXWWWm8LdYP9zLP3qKDqE8pGgcdNsA7ngQ6kT8jRDgh3BVme
6jzQhKtqRH+JWq8/vltmlZ389FgF3ghMyk4AwqdADFdSQgRqqvFIvJshED/HSw6buhXamDnBoDF7Wjv6
m//pFB/1AieR5l84ajzchHVmFsX/zVqQWSHM+2FZmH9fPU9N2jNE1C5iSyP9FcqWInf9gtkdstgd3B/l
uwpyv4WS/zlAiBHkjhYl5sjoExhCfBgPFz1N+vx5HzoWiioP7kQSX0js3rEthHg5Uv9UvFe4E1b1AByI
WSJXT7g+6h3Lg/IPOxG6Js3Y2rIqsh6pcTDP5FCb+gw4G2bAobyyX+1z7K8gnDWgmrX/cgQL6jQN1Beb
vSv6lpVJFsa3R0ViXBaV8JeaqVXd2xIdYgF6bPHbRR533s70wgqDOefGkSYG7iM3nnoPzuGf/gwXReeA
zGUUdyKY623/Mbwo71d2wLWFopo5JAALsxfUg1kGGGLDd2WNpmvFTqbAYeimyM9wV7IumaS+689hYyO/
XDNZIbLG9nADkMrM0XwJk3AG3fr96KDifbvqKDi7O3JAJRkFMZKz0lhnPODjk/BYkN5vYigbBwya44QW
zoucNOUJstm621I/JAihHjIO0vaQAgG4MQXR4gcHFbVbWifN1q
```

Fig. 7 Send to B terminal

Fig. 8 Encrypt data at the B terminal

Fig. 9 Send to A terminal

Fig. 10 Verify identity

encrypting the public key using RSA, it is sent to the patient using two-ended communication. The patient himself define access structure (id4254111988342 and man and age30 and day444 and chronicrespiratoryinfections).Obviously, it must have all the above properties to meet the access structure. Then, the patient encrypts the data using the access structure and the transmitted key. Encrypted data is transmitted to the end that Users need access to patients' medical data. When a user access to the patient's medical data, submit his own properties (| id4254111988342 | man | age30 | day444 | chronicrespiratoryinfections).Obviously, the set of properties meet the

patients themselves defined access structure, and the ciphertext can be decrypted, so the authentication passed (User qualification!).

Our hybrid encryption scheme can achieve the following goals:

First of all, patients can define their own access structure, and only the person designated by the patient can access the patient's medical data, enhancing the security of the patient's medical privacy.

Secondly, a patient's medical data can be accessed by multiple users, satisfying the "one-to-many" data sharing and flexible access control.

Finally: RSA is used to encrypt data during transmission to protect data security.

4 Conclusion

In this paper, to protect the privacy of medical data, we propose the RSA-ABE: a hybrid encryption approach for medical privacy data with cloud storage. In our construction we employ two-terminal communication and CP-ABE. The user can customize the access structure on one end. At the other end, Identity authentication can be performed through the transmitted data and attribute entered by a user for an access request. And RSA encryption is used during data transmission to protect data security. In the cloud storage environment, one end defines the access control structure, and the other end uses attributes to decrypt access, meeting the cloud storage characteristics. Therefore, this solution is feasible. In the future, this scheme can be applied to various industries, such as transportation, education, power, etc., and CP-ABE can also be improved to realize hierarchical control and encrypt transmitted data with other encryption algorithms.

References

1. Shamir A (1984) Identity-based cryptosystems and signature schemes. Adv Cryptol 21(2):47–53
2. Zheng D, Qin BD, Li YN et al (2020) Cloud-assisted attribute-based data sharing with efficient user revocation in the internet of things. IEEE Wirel Commun 27(3):18–23
3. Gao H, Ma Z, Luo S et al (2021) BSSPD: a blockchain-based security sharing scheme for personal data with fine-grained access control. Wireless Commun Mob Comput 1–20.
4. Hijawi U, Unal D, Hamila R et al (2021) Lightweight KPABEarchitecture enabled in mesh networked resource—constrained IoT devices. IEEE Access 9:5640–5650
5. Li JG, Zhang YC, Ning JT et al (2022) Attribute based encryption with privacy protection and accountability for CloudIoT. IEEE Trans Cloud Comput 10(2):762–773