Adaptive Authorization Access Method for Medical Cloud Data Based on Attribute Encryption

Yu Wu, Nanzhou Lin, Wei Song(✉), Yuan Shen, Xiandi Yang, Juntao Zhang, and Yan Sun

School of Computer Science, Wuhan University, Wuhan 430072, China
songwei@whu.edu.cn

Abstract. The outsourcing storage of medical big data encrypted in the cloud can effectively alleviate the problem of privacy disclosure, but cipher text storage will lead to the inconvenience of data access, which brings new challenges to medical big data shared access. The existing flexible authorization solutions for encrypted data are mainly based on methods such as CP-ABE, which requires the data owner to define the data access strategy, while in reality, the patient is the data owner of the medical data. At the same time, the existing scheme does not support access control authorization in emergency scenarios, and in medical big data applications, when patients can not authorize data users to access cipher text medical data, it will lead to unpredictable consequences. According to the application requirements of encrypted medical big data shared service in cloud environment, an adaptive authorization access method based on attribute encryption is proposed to realize flexible and secure medical data access authorization in normal and emergency situations. Experimental results demonstrate that our scheme is efficient.

Keywords: Attribute encryption · Adaptive access control · Privacy protection · Medical big data

1 Introduction

The development of cloud data enables medical institutions to provide high-quality, convenient and universal medical services. After collecting physiological data from the medical Internet of things, data is transmitted to the Medical big data Center for storage and disease diagnosis. In order to protect the privacy of patients, medical documents need to be encrypted before transmission to prevent eavesdropping on the public domain [1]. In order to realize the authorized sharing service of encrypted medical big data, patients, as the owners of medical data, formulate access policies to protected encrypted medical data and define authorization attributes and relationships. Only users with appropriate attribute keys (health care workers) have the right to decrypt the ciphertext. This encryption method is called attribute-based encryption [2]. There may be an emergency in the medical system, such as a car accident or a sudden collapse of the patient, and the first aid personnel on the scene need to access the electronic medical records of the patient in the process of emergency treatment. However, first aid

W. Ni et al. (Eds.): WISA 2019, LNCS 11817, pp. 361–367, 2019.
https://doi.org/10.1007/978-3-030-30952-7_36

personnel often do not have access to encrypted medical files, hampering emergency care for patients' lives. Therefore, a flexible access authorization method is required in practical medical applications to solve the problem of flexible access authorization for medical data in this emergency.

Aiming at the flexible access authorization problem of encrypted medical data in the cloud environment above, this paper proposes an adaptive access control method based on KP-ABE [3] technology. Under normal circumstances, patients have absolute control over medical data and authorize data users to access personal encrypted medical data in the cloud. In case of emergency, considering that patients are unable to perform data authorization operations, data users contact emergency contacts to negotiate access rights to encrypted medical data, and abnormal authorized access services of medical data in emergency are recorded by the cloud for audit use.

2 Related Work

Aiming at the data access requirements in emergency situations in medical big data applications, Brucker et al. [4] proposed a break-glass access model, which can still access when the system crashes. However, these studies [4, 5] only proposed a framework, but did not implement specific security data access authorization scheme.

Lattice-based cryptography system has the characteristics of simple calculation and high security. Ajtai [6] proposed a scheme to construct ciphers based on lattice problems, which has the advantages of high execution efficiency and strong security.

The research group has carried out research work on the privacy protection of medical big data. Wang et al. [7] proposed a method of Medical data encryption in cloud computing.

3 The Proposed Scheme

Cloud platforms provide an important support for the storage of medical data. But there are security problems, so an adaptive access control method is needed. Under normal circumstances, the data user is authorized to access the data by the patient, but in case of emergency, the patient cannot authorize the data in time, endangering the patient's life safety. For this special situation, this system model allows medical staff to negotiate access to encrypted medical data with emergency contact person after authentication in case of emergency (patients are unable to conduct data authorization due to illness). In order to ensure the accessibility of ciphertext data in emergency scenario, patients also need to set up emergency contact person and share the encryption key to them. In advance, and patients and emergency contact person can negotiate secret parameters together, so that in case of emergency, emergency contact person can reconstruct the key to decrypt patients' medical files through encryption key.

3.1 Scheme Model

The system model includes six entities: Key generation center, Medical institutions, Data owner, Cloud service provider, Data user and Emergency contact. The characteristics and functions of each entity are described as follows.

(1) Key generation center: responsible for generating system public parameters and creating master system key *MSK*. Meanwhile, the key generation center generates key pairs for patients and medical institutions, and generates file encryption parameter matrix *A* for patients, which is sent to patients and medical institutions through secure channels.
(2) Medical institutions: they are composed of various hospitals with medical capacity. A medical institution manages its staff and provides medical services to patients. After the registration of a medical institution, KGC generates public-private key pairs for the medical institution, and securely transmits the private key to the medical structure. A medical institution generates a set of attributes for its medical staff to describe their data access characteristics and generate an attribute key for them.
(3) Data owner: in order to protect the security and privacy of medical data, medical data is considered as a resource that is completely managed by patients (data owners). In the process of providing medical services to patients, medical institutions will send corresponding personal electronic medical documents to patients, who will encrypt the medical documents and store them in the cloud. Patients assign access attribute set to encrypted personal medical data, and only authorized visitors, whose pre-allocated access attributes satisfy the access policy of the corresponding encrypted file, can successfully access the encrypted data.
(4) Cloud service provider: cloud service provider is responsible for storing the ciphertext of medical documents and the set of attributes formulated by patients, and responding to queries according to the access policies of medical institutions.
(5) Data user: data user (such as medical staff of a hospital) registers with medical institutions to obtain attribute keys. Data consumers send data access requests to cloud service providers to obtain encrypted medical files and decrypt them using attribute keys.
(6) Emergency contact: the patient and the emergency contact negotiate the secret parameter y in advance. When patients are in a state of normal authorization, emergency contact use secret parameters restore the encryption key Ψ together with the users of the data.

3.2 Description of Proposed Scheme

Key generation center create system public parameters PP and master key MSK according to the security parameter 1^k. The public parameter *PP* is public in the whole system, and MSK is stored secretly by the key generation center.

GlobalSetup$(1^k) \rightarrow (PP, \text{MSK})$. The key generation center operates the GlobalSetup algorithm. The key generation center randomly sets the hash function H_1: $\{0, 1\}^* \rightarrow Z_p^*$, H_2: $\{0, 1\}^* \rightarrow \mathcal{K}$ and Generate symmetric encryption pair

SEnc/SDec in security key space K. Then the key generation center sets the random number $\eta \in Z_p^*$, g, g_1, g_2, $g_3 \in \mathbb{G}$ and compute bilinear pairs $Y = e(g_1, g_2)^{\eta}$. Finally, the key generation center sets common parameters PP = (g, g_1, g_2, g_3, Y, H_1, H_2, SEnc/SDec) and master key MSK = η.

When a medical organization is registered as the ith medical institution. After the key generation center verifies the identity, it distributes the identity identification MI_i to each medical institution and generates the corresponding PK_i and SK_i.

MiKeyGen $(MI_i, \text{MSK}) \rightarrow (PK_i, SK_i)$. The algorithm is executed in the key generation center, then it randomly sets α_i, β_i, $\gamma_i \in Z_p^*$ and generates public key constituent element $pk_{i,1} = g^{\alpha_i}$, $pk_{i,2} = g^{\beta_i}$. Private key constituent element $sk_{i,1} = g_1^{\alpha_i}$, $sk_{i,2} = \beta_i$, $sk_{i,3} = g_2^{\eta} g_3^{\gamma_i}$, $sk_{i,4} = g_1^{\gamma_i}$, $sk_{i,5} = g_1^{\alpha_i \cdot \gamma_i}$.

When a medical user registers as the jth user in a medical institution. After verifying the user's identity, medical institutions generate an identity identifier $PID_{i,j} \in \mathbb{G}$ for patients, $HID_{i,j} \in \mathbb{G}$ for medical person. According to the role of the medical staff, assign attribute sets $\{attr_k\}_{k \in [\varphi]}$. The key generation center generates attribute keys $SK_{i,j}$ and $PK_{i,j}$ for each user.

UserKeyGen$(MI_i, SK_i, HID_{i,j}, \{attr_k\}_{k \in [\varphi]}) \rightarrow \left(PK_{i,j}, SK_{i,j}\right)$. Medical institutions randomly sets $\gamma_{i,j}^{'}$, t $\in Z_p^*$ and $\gamma_{i,j} = \gamma_i + \gamma_{i,j}^{'}$. When a data owner registers as a patient P_i. Key generation center will generate public-private key pairs for patients according to file encryption parameter matrix and X solution set. The patient will embed the set of attributes in the key.

OwnKeyGen$(PID_i, A, X, \left\{attr_p\right\}_{p \in [\varphi]}) \rightarrow (PPK_i, PSK_i)$. File encryption parameter matrix A and A set of solutions to $AX = 0$, $X = \{\vec{x} | A\ \vec{x} = 0\}$. $PPK_i = g^{H_2(A)}$, $psk_{i,1} = g_1^{H_1\left(\overrightarrow{x_i}\right)}$, $psk_{i,2} = g_2^{H_1(PID_i) \cdot \beta_i}$, $psk_{i,3} = g_2^{\alpha_i} g_3^{H_1\left(attr_p\right)}$, then $PSK_i = \left(psk_{i,1}, psk_{i,2}, psk_{i,3}\right)$.

DepKeyGen$(PID_{i,j}, SK_{i,j}) \rightarrow DK_{i,j}$. When the patient P_i sets up an emergency contact, the corresponding key DK_i is generated for the emergency contact. The patient randomly sets parameter $\lambda \in Z_p^*$, then calculate $DK_{i,1} = \left(psk_{i,1}\right)^{\lambda} = \left(g_1^{x_i}\right)^{\lambda}$, $DK_{i,2} = \left(psk_{i,2}\right)^{\lambda} = \left(g_2^{H_1(PID_i) \cdot \beta_i}\right)^{\lambda}$, $DK_{i,3} = \left(psk_{i,3}\right)^{\lambda} = \left(g_2^{\alpha_i} g_3^{H_1\left(attr_p\right)}\right)^{\lambda}$.

PatientGen$(PID_i, PPK_i, PSK_i, DK_i, \text{file}) \rightarrow (Kf, y)$. Patient calculate bilinear pairs $E = e(PPK_i, PSK_i)$, then $Kf = H_2(E, PID_i, H_1(file))$, and use diffie-hellman key exchange protocol to negotiate the secret parameter $y = H_1 g^{PSK_i \cdot DK_i}$ with the emergency contact for emergency.

Enc$(Kf, \text{file}, A, \overrightarrow{x_i}) \rightarrow (\text{CT}, \Psi)$. When the patient completes the encryption key, symmetric encryption method is adopted to encrypt the file. Encryption key $\Psi = (Kf + \overrightarrow{x_i})A$, $c$iphertext CT = SEnc(Ψ, file$\|0^{\varpi}$).

PropertyMap$(ap, AP_H, \rho) \rightarrow 1/0$. Normally ap maps to AP based on implicit rules. Under normal circumstances, if the attribute judgment result returns 1, then the normal decryption algorithm is carried out.

NorDec$(1/0, HID_{i,j}, \text{CT}, \Psi) \rightarrow \text{file}/\perp$. If the attribute determination result is 1, the patient decrypts the medical file with the encryption key and sends it to the

corresponding medical personnel through the secure channel; Output $\perp$ if the attribute determines that the result is 0.

EcpDec(Kf, $HID_{i,j}$, PSK_i, $SK_{i,j}$, DK_i) $\rightarrow$ file. The patient pre-negotiates the encryption key pair $((Kf + \vec{x} + y + r)A, rA)$ in the event of an emergency with the emergency contact. In case of emergency, the key generation center generates a group password $\overrightarrow{x'}(\overrightarrow{x'} \in X)$ for medical personnel. Send $Kf + \overrightarrow{x'}$ to Emergency contact. Emergency contact generation $(Kf + \overrightarrow{x'} + y)A$ and returned to the medical staff. The medical staff obtains rA from the key generation center to generate the key $(Kf + y+r)A$, and the medical staff decrypts the medical file.

4 Experiments and Verification

In order to verify the efficiency of the adaptive authorized access method of medical cloud data based on attribute encryption, the A^2MAE scheme proposed in this paper is implemented by JAVA parsed method cipher library (jPBC). Four groups of comparative experiments were conducted to compare the efficiency of this scheme with the existing IOT scheme [8], ABEC scheme [9] and IPSD scheme [10] in key generation algorithm, encryption algorithm, normal and emergency decryption algorithm (Fig. 1).

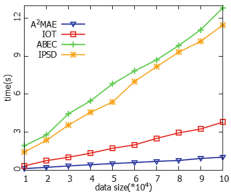

Fig. 1. Key generation

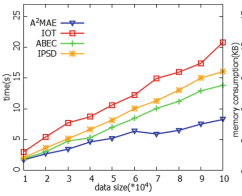

Fig. 2. Encryption

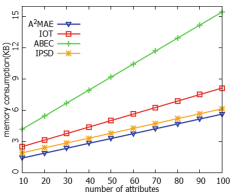

Fig. 3. Nor-decryption

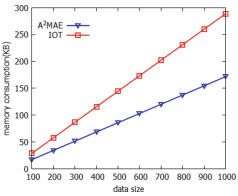

Fig. 4. Em-decryption

The time consumption of key generation and encryption is tested in different data scales. After implementing key generation and encryption phases of IOT scheme, ABEC scheme and IPSD scheme respectively, the experiment conducted a comparative analysis on the time consumption of each phase of the four schemes. In the key generation stage, as shown in Fig. 2, with the continuous increase of data size, IOT scheme uses a large number of bilinear pairwise operations, leading to a greatly increased key generation time. ABEC scheme and IPSD scheme increase the number of keys to enhance security, but at the same time the key generation time significantly increases. When the data volume is large enough, the performance of our scheme will be better.

In the encryption phase, it can be seen from Fig. 3 that our scheme is more stable in terms of time consumption than IOT scheme. ABEC scheme and IPSD scheme show a significant increase in time consumption with the increase of data size. In general, our scheme is more effective under the condition of ensuring certain safety. For the

decryption phase, normal decryption is compared with ABEC scheme, IOT scheme and IPSD scheme for communication consumption. The communication consumption in emergency declassification is compared with IOT scheme.

In the case of normal decryption, as shown in Fig. 3, memory consumption increases linearly as the number of attributes increases. When the number of attributes was 10, our scheme memory consumption was only 1.41 KB. ABEC scheme uses a lot of factorial memory consumption, and our scheme is slightly better than IOT scheme and IPSD scheme. It can be seen that our scheme consumes less decryption memory under normal circumstances. In the case of emergency decryption, due to non-attribute decryption, we only compare the emergency decryption of IOT scheme as shown in Fig. 4. With the increase of data volume, our scheme performs better than the IOT scheme in the case of emergency.

5 Conclusion

For satisfying complex requirements of cloud medical data access control, this paper proposes a medical cloud data based on attribute encryption adaptive grant access method, this method achieved under normal conditions and data access in an emergency. Experimental results show that this method has shorter time and higher performance than other methods on the premise of ensuring safety, but in the scheme attribute matching phase is derived not in-depth study, Therefore, the implicit authorization rules will be further improved in the follow-up research.

Acknowledgements. This work is supported in part by the National Natural Science Foundation of China under grants 61572378, U1811263, and the Natural Science Foundation of Hubei Province under grant 2017CFB420.

References

1. Song, W., Wang, B., Wang, Q., Peng, Z., Lou, W.: Tell me the truth: practically public authentication for outsourced databases with multi-user modification. Inf. Sci. **387**, 221–237 (2017)
2. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_27
3. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of CCS, pp. 89–98 (2006)
4. Brucker, A.D., Petritsch, H.: Extending access control models with break-glass. In: Proceedings of SACMAT, pp. 197–206 (2009)
5. Wang, X., Hu, Q., Zhang, Y., Zhang, G., Juan, W., Xing, C.: A kind of decision model research based on big data and blockchain in eHealth. In: Meng, X., Li, R., Wang, K., Niu, B., Wang, X., Zhao, G. (eds.) WISA 2018. LNCS, vol. 11242, pp. 300–306. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-02934-0_28
6. Ajtai, M.: Generating hard instances of lattice problems. In: Proceedings of ACM Symposium on Theory of Computing, pp. 99–108 (1996)

7. Wang, B., Song, W., Lou, W., Thomas Hou, Y.: Privacy-preserving pattern matching over encrypted genetic data in cloud computing. In: Proceedings of INFOCOM, pp. 1–9 (2017)
8. Yang, Y., Zheng, X., Guo, W., Liu, X., Chang, V.: Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Inf. Sci. **479**, 567–592 (2019)
9. Hui, C., Deng, R.H., Li, Y., Guowei, W.: Attribute-based storage supporting secure deduplication of encrypted data in cloud. IEEE Trans. Big Data **99**, 1 (2017)
10. Han, J., Susilo, W., Yi, M., Zhou, J., Man Ho Allen, A.: Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. IEEE Trans. Inf. Forensics Secur. **10**(3), 665–678 (2015)