A Novel Revocable Personal Health Record Scheme Using outsourced CP-ABE

Nana Huang[a], Liang Shen[b]

The Third Research Institute of the Ministry of Public Security, Shanghai, China

[a]1058219406@qq.com, [b]huangnn@mctc.org.cn

Keywords: Personal health record, outsourced, revocable

Abstract: With the rapid development of the cloud computing, personal health record (PHR) has become a hot topic recently. However, the most important issue is how to implement secure and efficient data sharing scheme since PHR is often outsourced to be stored at a third party. Therefore, the research on a secure and efficient Personal Health Record scheme to protect patients' privacy in PHR files is of great significance. In this paper, we present a revocable outsourced CP-ABE based personal health record scheme. In the scheme, we divide the users into personal domain (PSD) and public domain (PUD) logically. In the PSD, we adopt the Improved Key-Aggregate Encryption (IKAE) to achieve read access permission. For the PHR users of PUD, we use revocable outsource-able MA-ABE to largely eliminate the overhead for both the PHR owner and users, which can also support efficient attribute revocation without updating the PHR user's private key. At the same time, the import of multi-authority reduces the complexity of the key management and avoids the single point of failure. Function and performance testing results show the security and efficiency of the proposed scheme.

1. Introduction

With the rapid development of computer technology, big data and public cloud services has been widely used. Meanwhile, the concept of medical cloud with the same data demand put forward. As a result, Personal health record (PHR) is proposed, as an emerging patient-centric model to exchange health information. In medical cloud systems, each PHR owner store their medical records on third-party cloud server, where they can share their health information with many users. The PHR service allows patients to create, modify and control their personal health data in a local network, which makes the storage and sharing of medical information more efficient. In PHR system, in order to protect patient data privacy, the patient should encrypt their medical data before uploading to the cloud server.

Medical cloud brings many benefits, however, there is also a key problem to be solved. Due to the high cost construction and complex maintenance management, many medical services are outsourced or provided by a third party service. To protect privacy of patients, we need to develop an effective and secure access control solution in medical system. In this paper, we mainly adopt outsourced attribute based encryption (ABE) as the primitive encryption in the public domain, which enables the patient to set an access policy to encrypt his PHR, and only the users whose own attributes satisfied the access policy can decrypt it. However, to integrate ABE into a large-scale PHR system, important issues such as huge amount computation, efficient on-demand revocation and key management are urgently to be solved. In this paper, we propose a novel revocable outsourced CP-ABE based scheme in medical cloud system under the multi-user settings, which can flexibly implement management of users, permissions and attributes in the respective domains, largely eliminate the overhead for both the PHR owner and users, and support efficient attribute revocation.

2. Related Work

In this paper, encryption and decryption technology are mainly burdened by the third party, in which case patients can trust on the storage servers. At the very beginning, the traditional public key encryption (PKE)-based schemes [1] are used to realize fine-grained access control, which will cause the complexity of key management and not suitable for practical application. Recently, Wang et al. [2] put forward a novel user revocation scheme, which do not apply to the system with vast numbers of users and brings system bottleneck problem. Aiming at this problem, Xie et al. [3] proposed a new CP-ABE scheme which support users and attribute revocation and Green et al.[4] put forward a kind of outsourcing decryption ABE scheme for the first time. In their scheme, the traditional private key is broken up into the user key and transform keys. However, the scheme also does not apply to the system with more authorization centers. Based on this idea, Yang et al. [5,6] proposed two CP-ABE schemes which support outsourcing decryption and have multiple authorized centers. However, it did not consider whether outsourcing calculation results are correct. In general, the existing CP-ABE scheme for cloud storage has the following disadvantages: In cloud storage system, the multi-authority scene more satisfy the real demand. But the corresponding CP-ABE access control scheme is not mature enough, and most of the existing schemes are based on one authorization center which easily bring such problems as single point of failure and system bottleneck, unable to meet the needs of the practical application. Existing scheme still does not support highly efficient and flexible user and the attribute revocation. Recently ABE has been gradually applied to electronic healthcare records (PHR). Mohan et al. [7] implemented a subsystem of the PHR sharing system and this system used the ABE-based scheme which implemented the user privacy protection. Ibraimi et al. [8] first used ciphertext policy ABE (CP-ABE) in the PHR. However, the previous schemes adopted in the PHR system have many efficiency and the attribute revocation problems.

In order to overcome all of above insufficient, we proposed improved CP-ABE schemes based on many authorized center and applied it in the PHR system. In this scheme, most of the encryption and decryption calculation can be outsourced to the cloud service providers, and users only need to complete a small amount of calculation, which greatly reduce the computing burden of the PHR owners and users. At the same time, the corresponding verification scheme of outsourcing result is designed according to the proposed calculation outsourcing scheme. In addition, the corresponding users and attribute revocation scheme is designed. When revocation occurs, just to remove the agent key of the revoked user stored in the cloud without complex update operations; In the attribute revocation phase, most of the update and re-encrypt calculations are outsourced to the cloud service provider, which requires only a small amount of computation for users.

3. Design of Our Scheme

In our framework, the idea of domain partition is adopted. In the PSD domain, the paper used improved Aggregate key encryption algorithm (IKAE) to realize read access permission. In general, the PHR owner only want the PHR users to access parts of data files, and different users can access different parts of the PHR files. In the PUD domain, there are a large number of unknown PHR users, so this paper uses revocable outsourced MA-ABE scheme to realize secure and efficient data sharing. This scheme is based on the outsourcing encryption and decryption combined with multi-authority and attribute revocation mechanism. The import of multi-authority can not only simplify the complexity of the key management but avoid single point of failure problem. The outsourced encryption and decryption technique greatly reduces the computation overhead both for PHR owner and PHR users. Meanwhile, the scheme in the public domain can achieve efficient attribute revocation. The system framework is shown in Fig.1.

For the PSD, we adopt improved Key-Aggregate Encryption [9]. The original aggregate key encryption scheme only involves the encryption and decryption for direct communication and refers to a large computation. In order to realize the efficient access control and reduce the computational burden of the PHR users and the PHR owner, the trusted third party which is responsible for key generation and management is adopted. In the improved aggregation key encryption scheme, the system parameters are generated by the trusted CA and shared by all PHR users, which reduces the computing burden of PHR users. In addition, this scenario become indirect communication after we add a third party, thus, the PHR owner only need to set the PHR file access permissions, encrypt them, and upload to the server. When the PHR users access to the PHR files, the third party firstly judge the PHR users' access, then aggregate the private key corresponding to the authorized PHR file into a constant size aggregate key, and send it to the PHR users. Thus, the IKAE scheme greatly reduce the computing burden of the PHR owner and realize efficient read access permission. The specific algorithm implementation framework is shown in Fig.2: Assume that the PHR user has the permission to access files 1, 4, 6. Own to the limited space we will omit the specific description of algorithm of the improved aggregate key encryption.

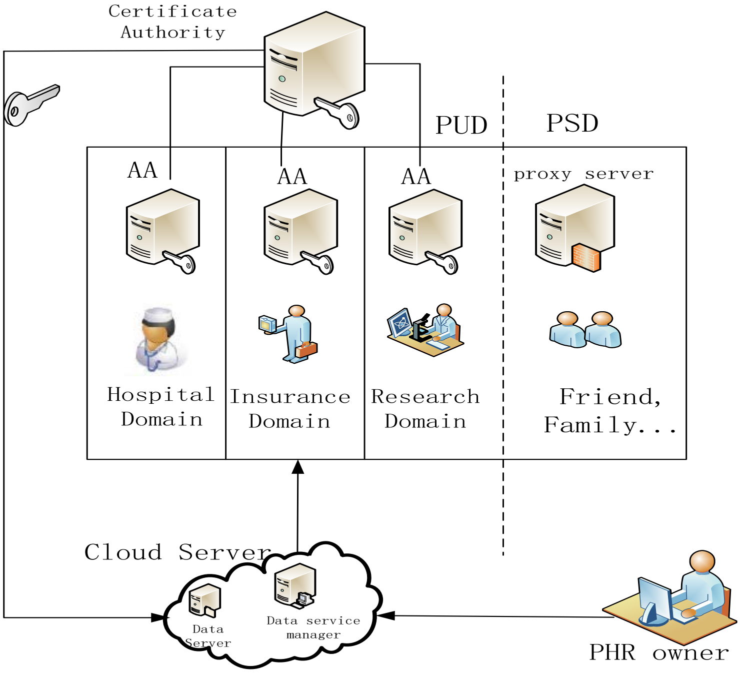

Fig.1. System Framework

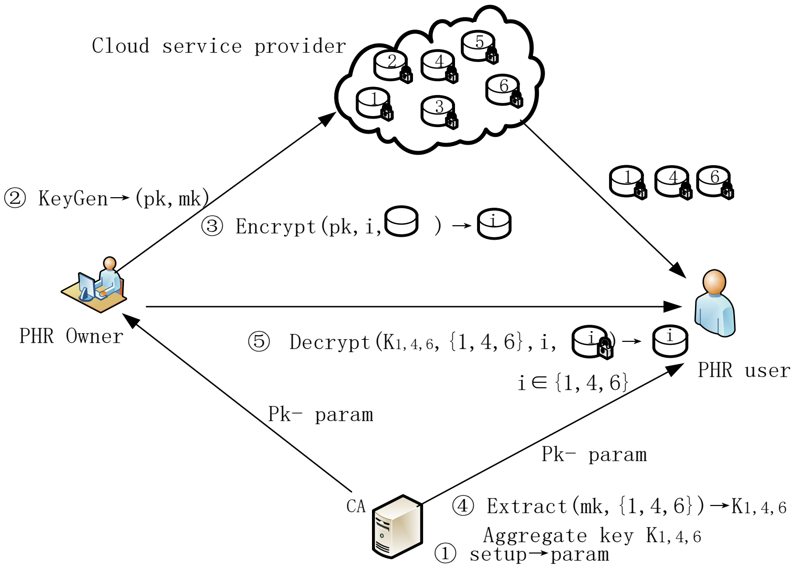

Fig.2. IKAE algorithm implementation framework

For the PUD, ABE is adopted in the previous schemes which is suitable for the public domain. However, one of the main efficiency drawbacks of ABE is a large computation burden on both the owners and users. In order to eliminate the overhead for users, Green’s outsourcing decryption of ABE scheme is used. But there is only one authority in the system which can easily lead to system bottlenecks and the owner’s encryption computation is large. In the outsource-able MA-ABE scheme put forward by Huang [10], there are many CA which can solve the single point failure problem, but it does not resolve the large computation of owners. In order to reduce the calculation burden of both users and owner, most complicated calculation in the process of encryption and decryption are outsourced to the cloud service providers. Based on this outsourcing thought, our scheme will further optimize the calculation efficiency by outsourcing encryption calculation to cloud services to reduce the calculation burden on the PHR owners.

However, the difficulty of outsourcing encryption scheme is that the encryption process itself is confidential and once some of the encryption elements leaked, the data privacy of PHR owner would suffer danger. In order to outsource the calculation as much as possible and guarantee PHR owner’s data privacy, the paper adopts the idea of confusion before correction. The confusion process is that the cloud services randomly select parameters to encrypt the PHR file. After receiving outsourced encrypted PHR files, PHR owner then select the new parameters to correct the parameters selected by cloud service provider, so that even if the parameters are selected out by the cloud service provider, illegal users cannot construct correct PHR files. This construction method greatly reduces the computation of the PHR owner who only need to encrypt the public key of the PHR files and correct the parameter. Although outsourcing calculating has obvious benefits, the cloud service provider is not completely reliable, it may only return an intermediate calculation value, or collude with the illegal users deliberately and return an error result. Once this situation happens, the subsequent calculation of encryption and decryption will be affected. Thus, the verification of the outsourcing calculation results is also a problem need to solve. And the difficulty to design validation scheme of the outsourcing calculation results is that if the corresponding calculation are only completed by the PHR owner and user itself, it will gives PHR owner and user additional computational burden. Therefore, the verification scheme should use proper skills to reduce the computing cost of PHR owners and users as much as possible. For outsourcing encryption, the scheme adopts the batch validation. The cipher texts are multiplied together and the result can be verified one-time without computing the cipher text one by one. Once the calculation result is not correct, there is an error in the cipher at least, then the result of outsourcing calculation is wrong. The method in this scheme is to compute a verification cipher text by hash function. After receiving outsourcing decryption result, the PHR user only need to use the private key to complete a small amount of calculation, then comparing with the validation of cipher text. If the result is different, the outsourcing calculation result is wrong.

Based on the above analysis, the basic framework of public domain is shown in Figure 3 and the specific steps of revocable outsource-able MA-ABE framework are as follows.

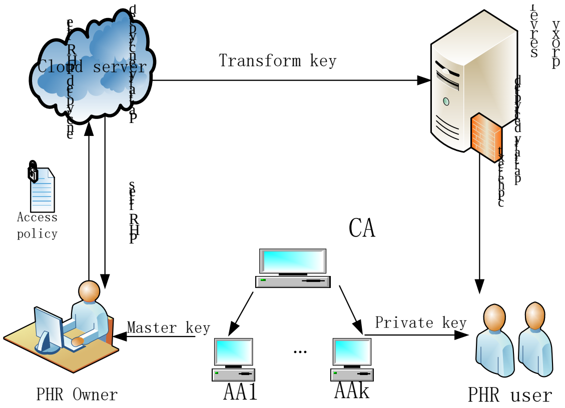

Fig.3. revocable outsource-able MA-ABE framework

Global Setup (*l, U*) $\rightarrow$ {*GP* , *uid* , *aid*} ）:CA inputs a system security parameter λ and U, and outputs global public parameter *GP*, user identity *uid* and CA *aid.*

Authority *Setup* (*aid*) $\rightarrow$ { PK_{aid} , SK_{aid} ,{ PK_{xk} }$_{aid\ I\ A}$ }）:Each AA inputs CA *aid* , outputs a pair of CA public key PK_{aid} and private key SK_{aid}, and generate an attribute public key { PK_{xk} }$_{aid\ I}$

$_{A}$ for each attribute managed by CA.

$Encrypt\_out\ (GP, \{PK_{xk}\}_{aid\ I\ A}) \rightarrow CT_{out}$:The CSP inputs global public parameter GP and attribute public key $\{PK_{xk}\}_{aid\ I\ A}$ and outputs partially encrypted ciphertext CT_{out} .

$Verify\_enc\ (GP, CT_{out}) \rightarrow b$:PHR owner inputs global public parameter GP partially encrypted ciphertext CT_{out} and outputs verification results. If $b = 1$, then the result is correct, if $b = 0$, then the result is wrong.

$Encrypt\_do\ (GP, PK_{aid}, \{PK_{xk}\}_{aid\ I\ A}, CT_{out}, M, (A, r)) \rightarrow CT$:PHR owner inputs global public parameter GP, the relevant CA public key PK_{aid}, attribute public key$\{PK_{xk}\}_{aid\ I\ A}$, partially encrypted ciphertext CT_{out},plaintext M and access structures A and outputs the encrypted full ciphertext CT.

$KeyGen\ (\mathrm{GP}, uid, S_{uid\ ,\ aid}, SK_{aid}, \{PK_{xk}\}_{aid\ I\ A}) \rightarrow \{PxK_{uid\ ,aid}, SK_{uid}\}$:CA inputs global public parameter GP, user identity uid, a set of user attributes $S_{uid\ ,aid}$, CA private key SK_{aid} ,attribute public key$\{PK_{xk}\}_{aid\ I\ A}$, outputs proxy key $PxK_{uid\ ,aid}$ and user private key SK_{uid} .

$Decrypt\_out\ (GP, CT, PxK_{uid\ ,aid}, \{PK_{xk}\}_{aid\ I\ A}) \rightarrow CT'$:The CSP inputs global public parameter GP, ciphertext CT, *user* proxy key $PxK_{uid\ ,aid}$, attribute public key$\{PK_{xk}\}_{aid\ I\ A}$, and outputs partially decrypted ciphertext CT'.

$Verify\_dec\ (GP, CT, CT') \rightarrow b$:The PHR user inputs public parameter GP, ciphertext CT, partially decrypted ciphertext CT', and outputs outputs verification results. If $b = 1$, then the result is correct,if $b = 0$, then the result is wrong.

$Decrypt\_user\ (CT, CT', SK_{uid}) \rightarrow M$:The PHR user inputs ciphertext CT, partially decrypted ciphertext CT', user private key SK_{uid}, and outputs plaintext M.

This paper mainly includes two kinds of revocation, one is user revocation and another is attribute revocation. User revocation means that the PHR user is no longer a legal user for the PHR owner and his all attributes are invalid. Attribute revocation includes system attribute revocation and the revocation of a PHR user’s one attribute. The system attribute revocation is simply to delete the revoked attribute in the system attribute set. The revocation of one attribute of a user will bring high communication overhead, as it requires a data owner to re-encrypt the ciphertext containing this attribute and update private key to every non revoked user. In order to realize on-demand and efficient revocation, we present a new scheme which combines the outsourcing decryption technique with encryption version number. We adopt proxy encryption to delegate operations b and c to the server, when revocation occured, only the key stored in CSP need to be updated, and PHR users don't need to update their keys. Own to the limited space we will omit the specific step of attribute revocation.

4. Performance Analysis

In this section, we will analyze the security and efficiency of the proposed PHR scheme.

In PSD, we adopt the IKAE scheme to realize the read access control, as the PHR owner have the control of the access permissions of the files, the PHR user can only access to part of the PHR files. For cloud server, the PHR files are all encrypted with different random number t, so the cloud server is in complete ignorance of the PHR files, thus to protect the secrecy of PHR data.

Table 1 Comparison of security

Scheme	Security	User domains	Access structure	Revocation
NGS[3]	Single CA	PUD	Attribute policy	ACL-level
RNS[6]	Against N-1 AA collusion	PUD	Access tree	Attribute-level
Our scheme	Against N-1 AA collusion and user collusion	PUD and PSD	LSSS matrix	Attribute-level

In the PUD, we compare the security of our scheme with several existing works, in terms of confidentiality guarantee, access control structure, and revocation method, etc. It can be seen from Table 1, our scheme achieves high privacy guarantee and immediate revocation. In comparison with the other schemes, we adopt revocable outsourcing MA-ABE scheme, in which the transform key is stored on the CSP, the collusion between the PHR users or the PHR user and agency need to be considered. In this paper, to prevent the collusion attack, the TK of each PHR user is independently associated with the PHR user, and the TK contains a parameter Z which binds with the PHR users. Each user's Z is different, so different TK can't be combined together to make collusion attack. So that, our scheme can against users' collusion compared with the other schemes. Furthermore, although the CSP transforms the ABE ciphertext on message m into an El Gamal-style ciphertext on the same m, he learns nothing about m. Thus, our scheme supports server attack. In conclusion, the scheme in PUD can ensure the PHR user's privacy.

In the PSD, the size of the keys is the same as the element G and the size of the ciphertext is $(2G+G_T)$, which means the size of aggregate key and the ciphertext are constant. Therefore, we adopt the IKAE scheme to implement the read access permission, which can improve the access efficiency.

Table 2 Notations for efficiency comparison

Notation	Meaning
T_p	Time for one pairing operation
T_m	Time for one exponentiation operation
TK	Transform key
Z	Random parameter in TK
m	Partially decrypted ciphertext
G_T	The size of C
G	The size of C'

In the PUD, we adopt revocable outsourcing MA-ABE scheme. Firstly, in our scheme, most complicated operations of the encryption process have been outsourced to the cloud service. The PHR owner only need to complete a common public key encryption, a exponential operations and some parameter correction operations. As these calculations have nothing to do with attributes, so the encryption time spent is a constant value, which greatly reduces the computational overhead on PHR owner compared with the SE-PHR scheme [10]. Secondly, this technique supports efficient attribute revocation without updating the user's private key. In the previous schemes, upon each revocation event, the PHR owner needs to recompute and send new ciphertext components corresponding to revoked attributes to all the remaining users. While in our scheme, when revocation occures, only the key stored in CSP need to be updated, PHR users don't need to update their keys.

5. Conclusion

In this paper, we proposed a revocable outsourcing MA-ABE scheme in PHR system, which can enhance the privacy guarantees as patient-center under the scenario of multiple PHR owners and users, and greatly reduce the complexity of key management. In the PSD, the improved Key-Aggregate Encryption is exploited to implement the read access permission which improves the access efficiency. In the PUD, we use revocable outsource-able MA-ABE to largely eliminate the overhead both for PHR owners and users, so that our scheme can flexibly implement management of PHR users and reduce the key management complexity.

Acknowledgement

This work was supported by National Key R&D Program of China (2016YFB0800901).

References

[1] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,” Proc. ACM Workshop Cloud Computing Security (CCSW ’09), pp. 103-114, 2009.

[2] Wang H, Zheng Z, Wu L, et al. New directly revocable attribute-based encryption scheme and its application in cloud storage environment [J]. Cluster Computing, 2017, 20(3): 2385-2392.

[3] Xie X, Ma H, Li J, et al. New ciphertext-policy attribute-based access control with efficient revocation[C]//Information and Communication Technology-EurAsia Conference. Springer, Berlin, Heidelberg, 2013: 373-382.

[4] Green M, Hohenberger S, Waters B. Outsourcing the decryption of abe ciphertexts[C]//USENIX Security Symposium. 2011, 2011(3).

[5] Yang K, Jia X. Attributed-based access control for multi-authority systems in cloud storage [C]//Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on. IEEE, 2012: 536-545.

[6] Yang K, Jia X. Expressive, efficient, and revocable data access control for multi-authority cloud storage [J]. IEEE transactions on parallel and distributed systems, 2014, 25(7): 1735-1744.Mohan A, Bauer D,

[7] Blough D M, et al. A patient-centric, attribute-based, source-verifiable framework for health record sharing [J]. 2009.

[8] L. Ibraimi, M. Asim, and M. Petkovic, “Secure Management of Personal Health Records by Applying Attribute-Based Encryption,” technical report, Univ. of Twente, 2009.

[9] A. Lewko and B. Waters, “Decentralizing Attribute-Based Encryption,” EUROCRYPT: Proc. 30th Ann. Int’l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology, pp. 568-588, 2011.

[10] Fan K, Nana H, Wang X, et al. Secure and Efficient Personal Health Record Scheme Using Attribute-Based Encryption [J]. Networking and Applications, 2017(2):1-12.