Journal of Engineering Sciences
Vol 11, Issue 7, July /2020
ISSN NO:0377-9254

SECURE AND EFFICIENT ATTRIBUTE-BASED SHARING SCHEME FOR PERSONAL HEALTH RECORDS

[1]MURALIKRISHNA B, [2]TELANAKULAVENKATAALEKHYA, [3]PENDAYALA HARINI SRI TEJA, [4]MUNAGALA SEETHA, [5]DAMARAMYA

[1]Asst. Professor, Dept. of CSE, PBR VITS, Kavali, A.P, India.
[2, 3, 4,5B.Tech], Dept. of CSE, VEC, Kavali, A.P, India.

Abstract – Since cloud computing has been playing an increasingly important role in real life, the privacy protection in many fields has been paid more and more attention, especially, in the field of personal health record (PHR). The traditional ciphertext-policy attribute-based encryption (CP-ABE) provides the fine-grained access control policy for encrypted PHR data, but the access policy is also sent along with ciphertext explicitly. However, the access policy will reveal the user's privacy, because it contains too much sensitive information of the legitimate data users. Hence, it is important to protect user's privacy by hiding access policies. In most of the previous schemes, although the access policy is hidden, they face two practical problems: 1) these schemes do not support large attribute universe, so their practicality in PHR is greatly limited and 2) the cost of decryption is especially high since the access policy is embedded in the ciphertext. To address these problems, we construct a CP-ABE scheme with efficient decryption, where both the size of public parameters and the cost of decryption are constant. Moreover, we also show that the proposed scheme achieves full security in the standard model under static assumptions by using the dual system encryption method.

Index terms – Cloud Computing, CP-ABE, Personal Health Record.

I. INTRODUCTION

As an emerging technology in recent years, cloud computing provides a fast and efcient way to share data resources, and a mountain number of people access data through the network. For example, in the personal system health record system, a patient does not have to carry various paper versions of the test forms to make a diagnosis according to the traditional way, but he/she can store, retrieve and share the health record only by uploading

his own personal health record to the PHR system. A patient has the full control to his/her own PHR document and authorizes who can access these health data, such as friends, family or healthcare providers. In order to achieve accurate access control of PHR, data owners urgently need a kind of encryption scheme that can realize ne-grained access control.

Hidden ciphertext policy attribute-based encryption scheme provides a good way to solve the problem, where it achieves privacy protection by hiding access control policy. However, In the previous mechanisms, the access control policy is often sent along with ciphertext explicitly, which makes it easy reveal the users' privacy, since some attributes in access structure carry crucial identity information of the legitimate users. In PHR, an access policy dened by a patient may contain some sensitive attributes such as cardiologist, central hospital and so on. Therefore, for an unauthorized user, even if he cannot decrypt successfully, he can also infer from the access policy in cleartext form which the encryptor suffers from some disease.

The first hidden ciphertext-policy attribute-based encryption (HCP-ABE) was introduced, where the access structure was embedded in the ciphertext and not sent directly. Subsequently, some other hidden CP-ABE schemes were also successively proposed. However, access structures in these schemes only support AND gates or AND gates on positive, negative and wildcard. These lead to two drawbacks. First, the size of public parameters increases linearly with the number of attributes, and secondly, the cost of the decryption is greatly increased. Due to the above drawbacks, some low-overhead schemes are introduced and the common method adopted by these schemes is to introduce a decryption test by adding some redundant components to a ciphertext before the decryption stage. Although the above schemes improve the efficiency of decryption, the length of ciphertext is also significantly increased and this will become a bottleneck restricting higher performance. Additionally, these schemes are extremely vulnerable to decisional Dife-Hellman test (DDH-test) attack.

Since Attribute-Based Encryption was first proposed by Sahai and Waters, it has been seen as the most promising approach for ne-grained access control in the field of cloud computing. With the continuous improvements of ABE, currently, there are mainly two basic types of ABE schemes, Key Policy ABE (KP-ABE) and Ciphertext Policy ABE (CP-ABE). In KP-ABE scheme, keys

Vol 11, Issue 7, July /2020
ISSN NO:0377-9254

are associated with access structure and ciphertexts are associated with a set of attributes.The first CP-ABE scheme was introduced, where ciphertexts were associated with access structure defined by data owners and the key are associated with sets of attributes about users. Some other works were proposed to make further improvements on anonymous CP-ABE scheme.

In PHR, the specific attribute values in a access policy carry much more sensitive information, such as the patient's pulse frequency, his family history of hereditary diseases, the result of the patient's laboratory test report and so on. Hidden ciphertext policy attribute-based encryption scheme provides a good way to solve the problem, where it achieves privacy protection by hiding access control policy. Our contributions mainly include the following three parts.

- Access structure
- Fast decryption
- Data verifiability

II. BACKGROUND WORK

Since Attribute-Based Encryption was first proposed by Sahai and Waters, it has been seen as the most promising approach for ne-grained access control in the field of cloud computing. With the continuous improvements of ABE, currently, there are mainly two basic types of ABE schemes, Key Policy ABE (KP-ABE) and Ciphertext Policy ABE (CP-ABE). In KP-ABE scheme, keys are associated with access structure and ciphertexts are associated with a set of attributes. The first KP-ABE scheme was proposed by Wang and He. But in this scheme, the trusted authority fully determines the combination of attributes associated with the ciphertext, because the access control associated with the key are generated by the center for each legitimate decryption user. Then Sahai et al. proposed another KP-ABE scheme, in which the decryption keys of users' could express any access formulas over attributes, including non-monotone ones.

Thefirst CP-ABE scheme was introduced, where ciphertexts were associated with access structure defined by data owners and the key are associated with sets of attributes about users. Subsequently, there are a lot of CP-ABE schemes were also successively proposed, but these schemes only support AND gates. To realize the access structure more expressive, Waters proposed an access structure based a linear secret sharing scheme (LSSS), and it is also a provably secure scheme under the standard model. In order to further protect users' privacy, the rst the CP-ABE scheme with hidden access structure was proposed by Nishide et al. In their work,

access control policy isn't sent along with ciphertext explicitly, in other words, no unauthorized user can obtain useful information about the access structure. Some other schemes with the same performance have been proposed by other researchers, which are called Anonymous Attribute-Based Encryption. In these schemes, only sets of the user satisfying the access policy was embedded in the ciphertext, then the user can successfully decrypt the ciphertext. Later, authors in introduced another highly effective anonymous CP-ABE scheme, and its security proof was given under the Decisional Modied Bilinear Dife-Hellman assumption (MBDH). However, their work only gives a general analysis and lacks detailed security proof. Some other works were proposed, and to make further improvements on anonymous CP-ABE scheme. Unfortunately, all of them have to face high-overhead of decryption, which may make them lose their practicability.

III. PROPOSED WORK

Our main construction will be given where it will be provably secure under a concrete, non-interactive assumption. Moreover the scheme not only realizes expressive functionality but also gives an efficient decryption algorithm. The encryption algorithm in the proposed scheme will take a LSSS access matrix A as input and choose a set of random exponents from the distinct subgroups of G. Therefore, private keys and ciphertexts in this scheme are randomized to protect the sensitive information of the access structure. The overview of the our proposed system is shown in figure 1.

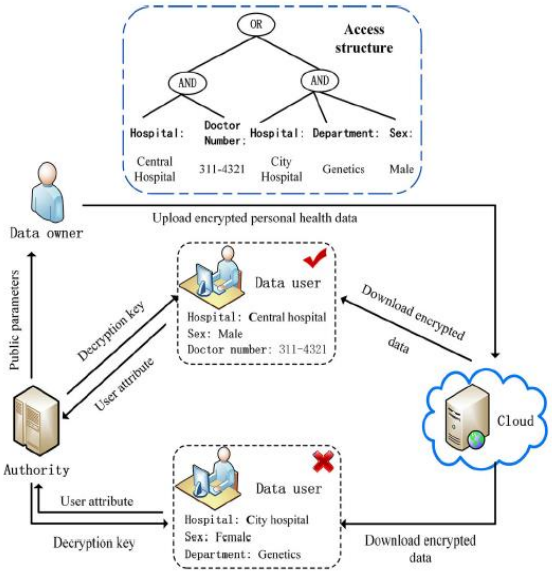

Fig. 1: System Architecture.

A hidden CP-ABE scheme consists of the following four algorithms.

Setup : It is a randomized algorithm that takes a security parameter as input and outputs the public parameters PK and master key MSK.

KeyGen: The key generation algorithm takes the public parameters PK, the master key MSK and the user's attributes set S as input. It

Vol 11, Issue 7, July /2020
ISSN NO:0377-9254

outputs the user's private key SK associated with S.

Encrypt: The encryption algorithm takes the public parameters PK, a plaintext message M, and an access structure as input, and outputs a ciphertext CT, where T is a set of attribute values in the access structure and not sent along with the ciphertext CT.

Decrypt: It takes the public parameters PK, a secret key SK associated with the attributes set S, and a ciphertext CT encrypted under access structure as input, and outputs the message M or a special symbol denotes that a user failed to decrypt the ciphertext CT.

Implementation Modules

Data Owner:

- In this module, Data owner can register and login to the system and he upload the file into untrusted cloud server.
- Here, he can view the uploaded file details and checks whether file data is safe or not.

Data User:

- In this module, data user/end user can register and login to the system and he search the file if he has search permission.
- If he is not having search permission, he/she can request the search permission to authority.
- Once the authority provides permission then he search file and send request to cloud server for decrypt and download file.
- After getting permission from cloud server he/she can decrypt and download files.

Authority:

- In this module, Authority is login to the system.
- He can view the user request and generate the search permission based on user search request.
- He can also view the files uploaded in the cloud.

Cloud Server:

- In this module, Cloud Server login to the system and view all users details, authorize them.
- Cloud Server can view the files uploaded to the system and he check the file decrypt and download requests and accept/reject the request.
- He can also generate the various reports.

IV. RESULT ANALYSIS

In this section, we show the implementation of our proposed system in the following figures.

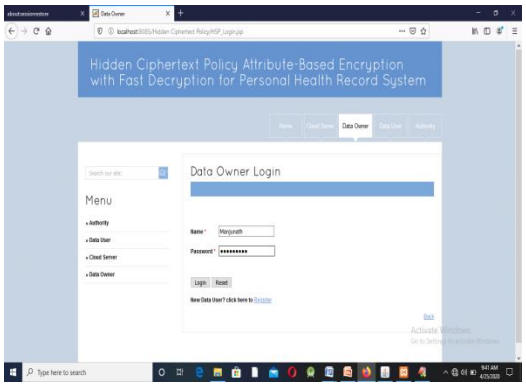

Fig. 2: Data Owner Login

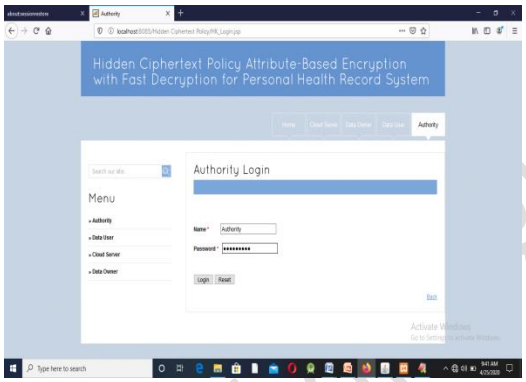

Fig. 3: Authority Login

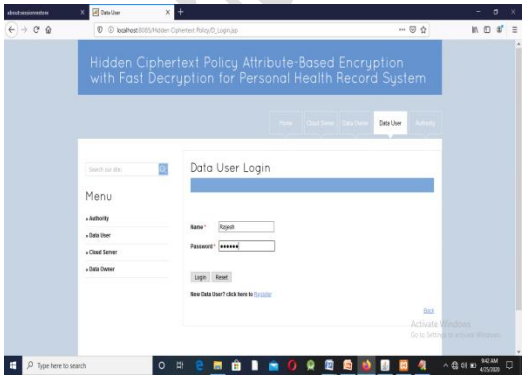

Fig. 4: Data User Login

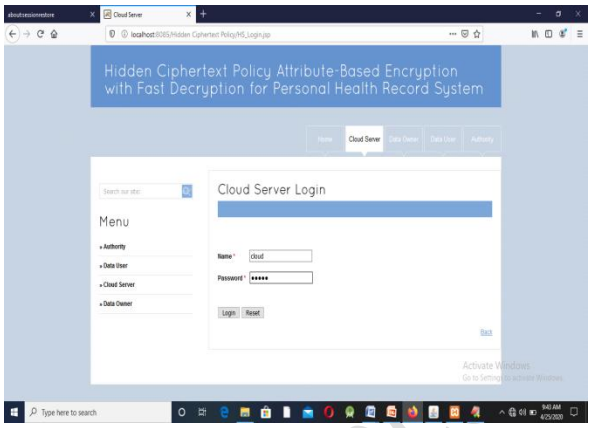

Fig. 5: Cloud Server Login

V. CONCLUSION

In this project, we introduced a new method called linear secret sharing with multiple values, which can greatly improve the expression of access policy. Moreover, each attribute is divided into two parts, namely the attribute name and its value. Therefore, the most obvious advantage of the proposed scheme is that sensitive attribute values can be hidden. And it can protect users' privacy well in PHR. In the proposed scheme, the size of public parameters is constant and the cost of the decryption is only two pairing operations, which also make it more practical. The proposed scheme only achieves partly hiding policy. It is an interesting problem that achieves fully hiding policy with fast encryption, which is left as a future work.

Vol 11, Issue 7, July /2020
ISSN NO:0377-9254

REFERENCES

[1] B.Waters, ``Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, Aug. 2009, pp. 619636.

[2] M. Qutaibah, S. Abdullatif, and C. T. Viet, ``A ciphertext-policy attribute- based encryption scheme with optimized ciphertext size and fast decryption," in Proc. ACM Asia Conf. Compute. Commun.Secure., Apr. 2017,pp. 230240.

[3] B. Waters, ``Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Workshop Public Key Cryptogr. Berlin, Germany: Springer, Mar. 2011, pp. 5370.

[4] V. Goyal, O. Pandey, A. Sahai, and B.Waters, ``Attribute-based encryption for ne-grained access control of encrypted data," in Proc. 13th ACMConf.Comput, Commun. Secur., Nov. 2006, pp. 8998.

[5] J. Lai, R. H. Deng, and Y. Li, ``Expressive CP-ABE with partially hidden access structures," in Proc. 7th ACM Symp.Inf., Comput.Commun.Secur., May. 2012, pp. 1819.

[6] A. Sahai and B.Waters, Fuzzy Identity-Based Encryption, R. Cramer, Eds. Berlin, Germany: Springer, 2005, pp. 457473.

[7] J. Bethencourt, A. Sahai, and B.Waters, ``Ciphertext-policy attributebased encryption," in Proc. IEEE Symp.Secur.Privacy, May.2007, pp. 321334.

[8] Y. Zhang, D. Zheng, and R. H. Deng, ``Security and privacy in smart health: Efficient policy-hiding attribute-based access control," IEEE Inter- net Things J., vol. 5, no. 3, pp. 21302145, Jun. 2018.

[9] H. Cui, R. H. Deng, G. Wu, and J. Lai, ``An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures," in Provable SecurityPROVSEC (Lecture Notes in Computer Science), vol. 10005, L. Chen, Eds. Berlin, Germany: Springer, 2016, pp. 1938.

AUTHORS

MURALIKRISHNA B has received his B.Tech in Computer Science and Engineering and M.Tech degree in Computer Science and Engineering from JNTU, Hyderabad in 2006 and JNTU, Anantapur in 2014

respectively. He is dedicated to teaching field from the last 12 years. He has guided 20 P.G and 20(batch) U.G students. His research areas included AI,Data Mining and Computer Architecture,Cloud Computing. At present he is working as Assistant Professor in PBR Visvodaya Institute Of Technology And Science,Kavali, Andhra Pradesh, India.

TELANAKULA VENKATA ALEKHYA, pursuing B.Tech in Computer Science and Engineering (CSE) from Visvodaya Engineering College, Kavali,Nellore (dt),Andhra Pradesh.

PENDAYALA HARINI SRI TEJA,pursuing B.Tech in Computer Science and Engineering (CSE) from Visvodaya Engineering College, Kavali, Nellore (dt), Andhra Pradesh.

MUNAGALA SEETHA, pursuing B.Tech in Computer Science and Engineering (CSE) from Visvodaya Engineering College, Kavali, Nellore (dt), AndhraPradesh.

DAMA RAMYA,pursuing B.Tech in Computer Science and Engineering (CSE) from VisvodayaEngineeringCollege,Kavali, Nellore (dt),AndhraPradesh.