International Journal of communication and computer Technologies, ISSN: 2278-9723

Available at http://www.ijccts.org

Security of PHR in Cloud Computing by Using Several Attribute Based Encryption Techniques

[1]Neetha Xavier, [2]V.Chandrasekar**

[1] *PG Student , Department of Computer Science and Engineering,*

[2] *Assistant Professor, Department of Computer Science and Engineering, Vivekanandha College of Technology for Women,*

Received: 14-01-2013, **Revised:** 20-03-2013, **Accepted:** 08-04-2013, **Published online:** 25-05-2013

Abstract— **Personal health record is an emerging trend in the health field for the exchange and use of personal health information. This record is now a day's stored in the third party storage areas like in the cloud providers. To reduce the storage space needed and for the cost reduction, the cloud service applied. There are lots of security issues related with the storage of sensitive personal health information in the clouds. The privacy and confidentiality of personal health information have challenges when cloud storage and applications used. Here the advanced encryption methods like attribute based encryption and its variations are used. Secure sharing of personal health record is assured in this system.**

Keywords—**Attribute Based Encryption (ABE), Break Glass Access, Cloud Computing, Cloud Data Security, Personal Health Record (PHR),**

INTRODUCTION

In recent year, Personal Health Record (PHR) has developed as the emerging trend in the health care technology and by which the patients are efficiently able to create, manage and share their personal health information. This PHR is now a day's stored in the clouds for the cost reduction purpose and for the easy sharing and access mechanism. The main concern about this PHR is that whether the patient is able to control their data or not. It is very essential to have the fine grained access control over the data with the semi-trusted server. But in this the PHR system, the security, privacy and health data confidentiality are making challenges to the users when the PHR stored in the third party storage area like cloud services.

The PHR data should be secured from the external attackers and also it should be protect from the internal attackers such that from the cloud server organization itself. When the PHR owner upload the PHR data to the cloud server, the owner is losing the physical control over the data and thus the cloud server will obtain the access on the plain text data and it will make lots of security challenges to the PHR privacy and confidentiality. The encryption of data before outsourcing it to the third party is consider as the promising approach towards data security and confidentiality towards the third party storage. The normal public key encryption methods and another traditional encryption schemes are making lots key management problem for the sharing of the personal health record and also all those methods provide very less scalability to the system.

In recent days the attribute based encryption scheme and its different variations are chosen as the main encryption primitive for the personal health records which made the storage, retrieval and sharing of the medical information more secure and efficient. But in attribute based encryption, the on demand user revocation is a challenging problem. So the cipher text policy –attribute based encryption and key-policy based attribute based encryption are also applied for the security of the personal health record. For reducing the key-management overhead and distribution problems, the multi-authority attribute based encryptions scheme is used. For the emergency access purpose, the break glass access attribute are also introduced with the personal health record scheme.

I. CLOUD COMPUTING AND PERSONAL HEALTH RECORDS

Cloud computing is an efficient technique by which the user can access any data from anywhere and anytime through internet. Thus it's providing the new world of computing technology to the world. The personal health records are thus also using this cloud computing technology for the efficient storage and retrieval system. But there is still a comparison is going on with the electronic health record and personal health record.

Electronic health record is the electronic version of the medical record of the care and treatment the patient

receives. It is maintained and managed by the health care organizations. But our PHR is the collection of important information that the patient maintain about their health or the health of someone they are caring for. It may be short and simple or very detailed. The traditional PHR was in the form of paper documents, electronic files maintained by their computer, but now the PHR is created by using the tools available in the internet. So which make the facility to use the health information across any distances, and to share with the selective users with special read and write access.

II. ENCRYPTION TECHNIQUES

At the early stages of the cloud computing and personal health record the traditional encryption techniques were applied to the personal health record and now days the advanced encryption techniques such that attribute based encryption and its different variations are used.

1) Public key encryption:

The public key encryption method was the most traditional method applied to the PHR for the security of the data. But it made the high key-management problems and also this method was very less scalable. The user revocation or break glass access and other advanced techniques were not possible with these one-to-one encryption techniques.

2) attribute based encryption:

The attributes can define an object very efficiently just as the identity of an object works. The attribute based encryption provides the security to the database. In this system both the cipher text and secret key will be associated with the attributes. The user who is having a minimum number of attributes only can decrypt the data. So while applying this method the owner doesn't want to know about the entire list of users instead of that they can encrypt the data according to some attributes only. Using ABE, access policies expressed based on the attributes of user data which enable the patient to selectively share the PHR among a set of users by encrypting the file under a set of attributes, and so the owner don't want to know the complete list of users [1].It provides data confidentiality and write access control. But the on-demand user revocation and other techniques were not adaptable with this encryption method.

3) Cipher text policy attribute based encryption

Ciphertext-attribute based encryption is an attribute based encryption technique which allow the data owner to encrypt the data based on an access policy, which will be based on the attributes of the user or the data. So, the decryption is possible when the secret key is matching with the access control policy [2].

The key-idea of the CP-ABE is: the user secret key is associated with a set of attributes and each cipher text will embedded with an access structure. The user can decrypt the message only if the user's attribute satisfied with the access structure of the ciphertext [3].

This method have the benefits such that the third party server won't have the access on the plain data, decryption will be possible only when the secret key matched up with access policy defined on attributes, and every user is needed proper authentication and authorization to access the data. And also it removes the need for knowing the identity of the patient by the patient for providing access grant.

The key challenges regarding this CP-ABE scheme is that the user revocation difficulty. Whenever the owner wants to change the access right of the user, it is not possible to do efficiently with this scheme.

4) key-policy based encryption:

It is an attribute based encryption in which the data are associated with the attributes, for each of which a public key component is defined. In this method, each user will be assigned to an access structure which will specify which type of ciphertexts the key can decrypt [4]. The secret key is defined to reflect the access structure. So the user will be able to decrypt a cipher text if and only if the data attribute satisfy that user's access structure. The key-policy attribute based encryption and ciphertexts-policy attribute based encryptions are almost working in a similar way, but both have some difference in terms of specifying the access policy for the users. The KP-ABE is useful for providing the fine-grained access control to the data system where it can efficiently specify that which part of data system can be accessed by which user and what are the operations they can execute over there.

5) Multi-authority attribute based encryption:

The multi-authority attribute based encryption scheme is an advanced attribute based encryption in which it will have many attribute authority for handling the

different set of users from various domains [5]. In the PHR system the users will be from different domain like the doctors from health care organizations, the friends and family from personal relations and other users from insurance domain too. So each user will be having different access control mechanism based on the relation with the patient or owner. Thus the MA-ABE scheme will highly reduce the key-management issues and overhead and thus it will provide fine-grained access control to the system.

III. THE EXISTING SYSTEM

In the existing system the Cipher-Text attribute based encryption (CP-ABE) is used which is a variation of attribute based encryption scheme. The data owner is uploading the data to the cloud server after encrypting the data according to the access control policy [7] defined with the set of attributes. This encrypted data can be decrypted by the user only if the attributes of that user satisfies the access control policy P.

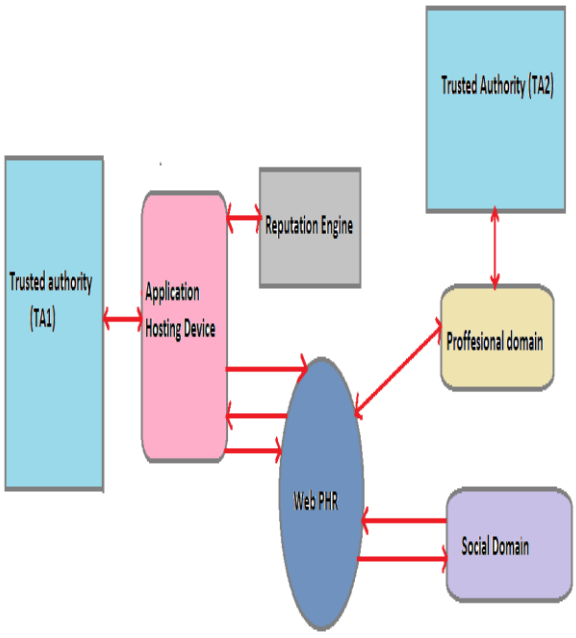

Fig.1 The existing PHR-system

In this system, two trusted authority system is used for the attribute issue purpose, the trusted authority (TA1) for the professional domain and the Trusted Authority (TA2) for the social domain, but the patient can act as this second authority. The reputation of the user is here used for generating the secret key for the users of the social domain [7].

The working principle and algorithm for the existing system is given as follows:

- At first the key-generation algorithm will run by the both the trusted authority by using CP-ABE scheme.
- The professional domain users will obtain their secret keys according to their attributes defined in the system.
- The patient will create the measurement data by the help of devices and tools and which will send to the application hosting devices like personal computer or mobile phones.
- The hosting device will encrypt this data after the categorization according to an access policy P.
- The encrypted data will send to the web PHR repository.
- When the user wants to see this data, they can download the encrypted data from the server and can decrypt them locally by using the secret key.
- When a request get by the patient for the data access grant permission the patient will make a decision by checking the requester's reputation score generated by the reputation engine.
- The patient will generate the secret key for that requester according to his reputation ranking only.

The CP-ABE scheme consists of four algorithms. The following are the four algorithms [8], [9]:

- **Setup Algorithm (MK, PK)**: This algorithm run by the trusted authority or the security administrator. It will take input a security parameter k, and output a master secret key MK and a master public key PK.
- **Key Generation algorithm (SK)**: It also run by the trusted authority and takes input a set of attributes and MK. It has the output a user secret key SK associated with the attribute set.

- **Encryption algorithm (CT)**: It is run by the encryptor of the system. It has the input a message m, a master public key PK, and an access control policy p, the output of the algorithm is a ciphertext CT, under the access policy P.
- **Decryption algorithm (m)**: It is run by the decryptor. The input for the algorithm is the ciphertexts CT to be decrypted and the user secret key SK. The output of the algorithm is the message m, if and only if the secret key of the user satisfies the access policy P, under which the message was encrypted. It shows an error message if the secret key doesn't satisfy the access policy P, under which the message was encrypted.

In this system in removes the single-trusted authority concept and it introduces multiple-authority concept which assure more security to the system. But there are lots of complexities related with the secret key generation for the users since whenever the patient getting new request the patient wants to check the reputation ranking of that requester and according to that ranking patient wants to generate separate secret key which will reduce the scalability and reliability of the system. The system will also suffers from management of large number of users and their key distribution and management problems.

IV. THE PROPOSED SYSTEM

The proposed system is providing the fine-grained access control to the system by using the different attribute based encryption schemes. In this system, the users are classified into two security domains called Personal Security Domain and Public Security Domain.

The users like family members, friends are included in the personal domain and the users from the health care organization and insurance field are considering as the data users from the public domain. For both the two different set of user domain the variations of attribute based encryption is used. For the personal security domain the revocable Key-policy attribute based encryption scheme is used [6]. For the public security domain the Multiple-Authority attribute scheme is proposed. In the PUD the system will define some role-attributes also.

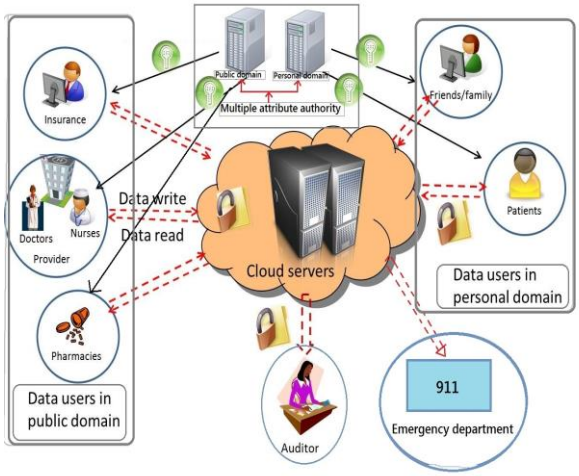

Fig.2 the Proposed System

In this system, the user accesses are controlled in terms of read and write access. The PHR-owner will be providing the different access based on the attribute they defined. The on demand revocation of both the user and attribute are possible through this system. The policy updating is possible by updating the attribute or access policy in the system. The emergency access is provided in the system by defining an emergency attribute in the system which provides break glass access. The write access control is enforced in the system by combining the digital signature techniques with the hash chain techniques.

The system achieves data confidentiality by proving the enhanced MA-ABE scheme. In addition in the security domain, it achieves the forward secrecy and security of write access control. Thus this system have the benefits of fully-patient centric control over the personal health record by the patient it highly reduces the key management overhead and it enhances the privacy guarantee**.**

V. CONCLUSION

The personal health records are now consider as the emerging trend in the personal health information exchange field. So cloud computing storage and sharing service is highly utilized by the users. The data security is the main privacy issue and the attribute based encryptions and its variations are applied for this security purpose. In this paper several variations of attribute based encryptions and its features are discussed. The PHR will

use more secure encryption primitives in the future for reducing the key management problems and complexity and for providing more secure storage and sharing features to the data's stored in the clouds.

REFERENCES

1. M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'lICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

2. L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," technical report, Univ. of Twente, 2009.

3. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.

4. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

5. S. Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure," Proc. ACM Cloud Computing Security Workshop (CCSW'10), pp. 47-52, 2010.

6. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM '10, 2010.

7. M. Chase and S.S. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 121-130, 2009.

8. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.

9. L. Ibraimi, Q. Tang, P. Hartel and W. Jonker, "Efficient and provable secure ciphertext-policy attribute-based encryption schemes," *LectureNotes in Computer Scienc*e. Berlin, Germany: Springer, pp.1-12, vol.5451, 2009.