A Framework of Scalable and Secure Sharing of Personal Health Record in Cloud using Enhanced Multi Authority Attribute Based Encryption

Ms. G. Ida Rani
M.E.Computer and Communication Engg
Einstein college of Engineering, Tirunelveli,India.

Mr. M. Suresh Thangakrishnan
Associate Professor(CSE dept)
Einstein college of Engineering, Tirunelveli,India.

***Abstract*-Personal Health Record is a recently growing technology in cloud which allow users to store and access their health record in one centralized place. To provide high security for user data, encrypt each record before stored it to the cloud server. For encryption use RSA algorithm because there is no attacker is hack the data from the RSA encrypted data. To reduce the key management complexity Attribute Based Encryption method is recently used. ABE is used to generate access policy or procedures to access PHR. To handle the remote user in an efficient manner divide the users in the system into public domain and personal domain based on user roles. For personal domain PHR owner provide access policies and distribute the key. In public domain an enhanced MA-ABE scheme is used. The key and access policy for public domain is distributed by TPA. In this way the PHR service is work well in cloud environment and reduce the task of owner and user and also provide secure and efficient access of PHR.**

***Keywords*---Cloud Computing, Attribute Based Encryption, PHR, Scalable, EMA-ABE.**

I. INTRODUCTION

cloud computing allow user to store data and access resources from the centralized virtual network. The best way to handle user data in cloud provide certain rules and access procedures. But the difficult task is to provide security for cloud storage data. In recent years cryptographic techniques[12] has been proposed for cloud security. These method require public/private key pair generation, data encryption, & data decryption. It is difficult for a single user could manage all these task, for that an Attribute Based Encryption[7] technique has been proposed in recent years. Personal Health Record(PHR) is one of the cloud service which allow patients can store and access their health record from the cloud server in an efficient and secure manner. To provide security for user data it is possible to encrypt the record before stored into the cloud server. The encryption procedures should be decide by the user itself because he/she know which user is wants to read or write record and which user is not. The data encryption is needed only at the server level for high security. It is not possible for a single user to handle all user request. The efficient way to handle user request divide the system of user into two domains public domain and personal domain. The personal domain users are family members, relatives and close friends. The patient itself handle all personal domain user request. The public domain users are doctor, nurse, insurance ,physician. The user request in public domain to be handled by the trusted Third Party Authority(TPA).In public domain multiple user is present for a single patient ,to handle all user in efficient manner use an enhanced MultiAuthority –Attribute Based Encryption (MA-ABE) which define multiple Attribute Authorities(AA) to handle different set of users. These method shows that, this system is a scalable system and provide efficient access and also reduce the workload of both data owner and users .

II. RELATED WORK

Several encryption technique has been proposed for cloud usage data. Traditional cryptographic techniques are public key encryption[12], symmetric key encryption[3]. In all these methods it is required to maintain the secret keys each time, and also the user should decrypt and access the file. Due to this complexity an Attribute Based Encryption[7] method has been recently taken place in cloud environment. With the usage of ABE the data should be encrypted at the server level only not at client level. The user can access the cipher text from cloud and request the secret key from the authorized data owners and get the original data. In a CP-ABE encryption method[4], each user is associated with a set of attributes, based on that the user's private key is to be generated. The data contents should be encrypted based on access policy. In a Key Policy –Attribute Based Encryption (KP-ABE) scheme[9] the data owner can encrypt the file and distribute to authorized users. The key for the data to be associated with certain access policies. Identity based Encryption (IBE) [11] allow ciphertext is not necessary to encrypted for particular users.In Hierarchical ABE[7]users are arranged in hierarchical manner and share the data based on their roles, policy to be provided in an efficient way and it reducing searching time of user roles.

III. PROBLEM DEFINITION

PHR service is used by multiple owners and multiple users at the same time. It allow data owner can create, manage and access their health record in a secure manner. For efficient access owner define access policy to his health record. To handle simultaneous users request divide the users into multiple domains and reduce the owner management task. The data owner design access policies and share the secret key to private users. For handling public users request define multiple attribute authorities and handle multiple users request by different set of AAs.

IV. PROPOSED SYSTEM MODEL

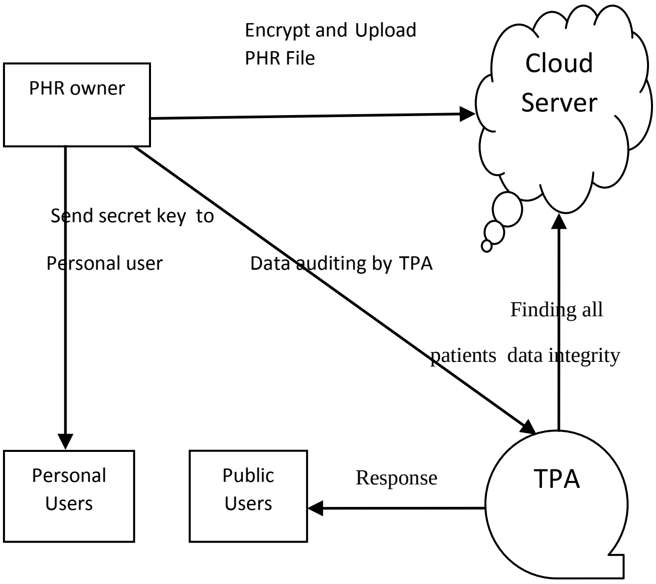
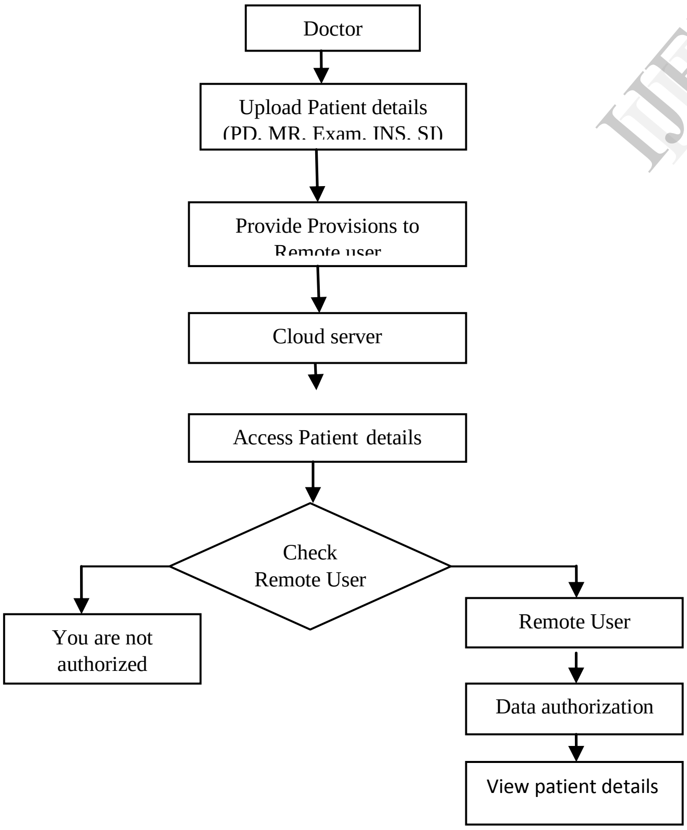


Fig. 1. Secure Sharing of PHR

System Flow Model



V. IMPLEMENTATION DETAILS

A. *System Setup and PHR File Upload*

The PHR system divides the health record into five set of files such as “basic profile”, “medical history”, “examination”, “insurance” and “sensitive information”. Then the PHR owner define the data attribute as “PD”, ”MR”, ”EX”, ”INS”, ”SI” which is shared by every user, and upload PHR file into cloud server. For efficient access, PHR file is arranged in a hierarchy of tree structure leaf nodes denotes the file attributes and the internal nodes are file categories. Dark boxes shows the access categories of a PSD users.

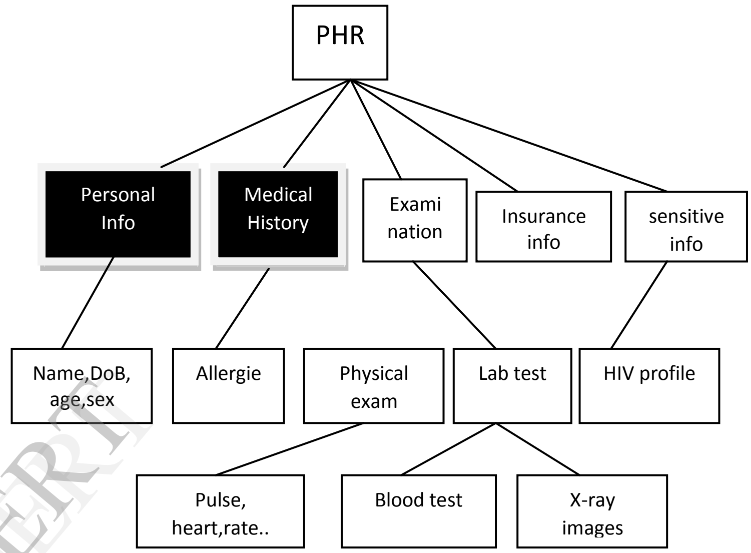


Fig. 2. Attribute Hierarchy of Files

B. *Secret Key Generation and Distribution*

To concentrate on key management issues, the system users are divided into two categories namely public users and personal users. Once the PHR files are uploaded the public and secret key for the PHR file is to be generated by the client application by which is shared by owners and users. The public key for the data owner is published via user’s profile in an online healthcare social-network (HSN). There are two ways to distribute the secret keys for personal users. First, a PHR owner can specify the access privilege for the PSD users and send their private key through mail. Second, a data reader in PSD can obtain the secret key by sending a request to the PHR owner via HSN, and the owner will give a subset of requested data types, then the user send the type of attribute he want to access and the owner provide the requested attribute key. RSA algorithm is used for both key generation and PHR file encryption.

a) Steps for PHR Key Generation

RSA contain both public and private key pairs. The public key to be publicly announced by every user profile and it is used for encrypting messages. The keys for PHR encryption are generated in the following way:

1) Select two different prime numbers p,q.

2) Calculate $n = pq$. (1)

3) Compute $\varphi(n) = (p - 1)(q - 1)$ (2)

4) Select the value e such that $1 < e < \varphi(n)$

and $\gcd(e, \varphi(n)) = 1$ (3)

5) Find d from $d^{-1} \equiv e \pmod{\varphi(n)}$ (4)

C. *PHR Encryption and Access*

Once the public key and private key are generated then the PHR owner encrypt the PHR file using these generated keys. The encryption use the public key and the prime factor n.

b) Steps for PHR Encryption

PHR owner transmits his public key (n, e) to HSN and keeps the private key secret. Then computes the ciphertext c corresponding to

$$c \equiv m^e \pmod{n}. \qquad (5)$$

PHR owner then send the encrypted message to the cloud server. The user from the any domain can see the message from the cloud server in an encrypted way until having the correct secret key.

D. *Data Auditing by TPA*

The encrypted PHR file is also send to trusted TPA. This is for handling public user request. For that the system define multiple AAs by using enhanced MA-ABE. Whenever the user requesting the secret key for the particular patient, it check the role of the user in HSN, and if the user attribute match with all the attribute corresponding to system data/role attributes, then send the secret key to the requested user. TPA handles these work on behalf of owner because the PHR owner is not always in online and also it reduces the key management task of owner. TPA maintains the data integrity and public auditing, and provide service for the remote user to access the patient details and also provide the write access control.

E. *Policy provision to Public User*

The Doctor or User has to upload the patient details to the Cloud server. The access policy are generated by TPA. The policy structure is conjunction normal form(CNF).Let **p1** be the CNF, the policy structure is of the form in eqn.(6)

p1$:=((A_1=a_{1,1})\wedge\ldots\wedge(A_1=a_{1,d1}))\wedge\ldots\wedge(A_m=a_{m,1}))\wedge\ldots\wedge(A_m=a_{m,dm}))$ (6)

where $a_{i,j}$=role attributes, m=total no.of attributes.

Example of key policy in eqn.(7)

p1:="(profession=doctor)^(specialty=HIV)
(organization=hospital A)". (7)

i.e. The doctor in hospital A want to access the PHR file for user1 and he is specialist in HIV domain then the doctor send the request(7) to TPA ,it verify access structure from its own if the attributes are matched then send the corresponding key to doctor.

F. *Policy Updates*

A PHR owner often updating the sharing policy for existing PHR file and also updating the attributes/access policy. The update operations include add/delete/modify and also set the write access control. For that it define the structure for which user has to read and which user should write on PHR. Fig 3 shows the update and access policy of PHR.

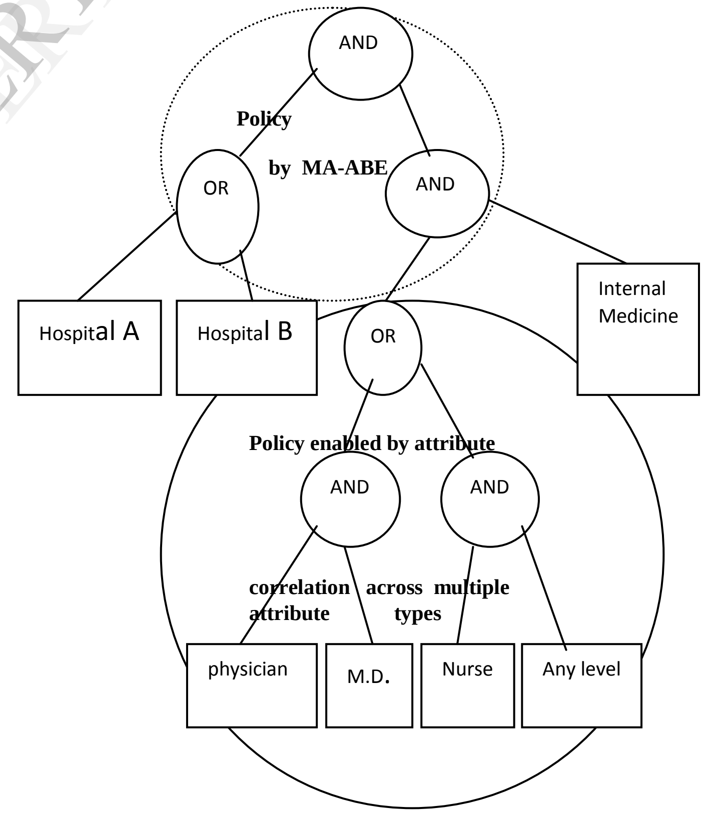


Fig. 3. Enhanced MA-ABE key generation and encryption rule

VI. CONCLUSION

The implementation results of this paper shows that it will work well in secure sharing of patients health records and other files in cloud computing. It allow any user can access and utilize the PHR service from the cloud server with high security. Patients can have full control of their own health data by encrypting their Personal Health Record (PHR) and also it allow selective users to access selective record only and not for all. It also solve the key management challenges by setting multiple PHR owners and users. Key management complexities are greatly reduced by using Attribute Based Encryption method. EMA-ABE scheme work well in public domain to add more number of AAs to handle multiple users simultaneously and efficiently access PHR by defining access policies and data attributes. The proposed solution is more scalable, secure and highly efficient than previous work.

In future, to reduce the encryption key size and improve the security level in cloud server, use elliptic curve cryptography algorithm to encrypt data before stored the PHR into the cloud server.

REFERENCES

[1] C. Dong, G. Russello, and N. Dulay,“Shared and Searchable Encrypted Data for Untrusted Servers,” Computer Security, vol. 19, pp. 367-397, 2010.

[2] 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.

[3] Q.Wang,”Enabiling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,” Proc. ESORICS ’09, pp.213-222 , Sep. 2009.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption”, *IEEE S& P ’07*, 2007, pp. 321–334.

[5] H. Lohr, A.R. Sadeghi, and M. Winandy, “Securing the e-health cloud,” in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI ’10, 2010, pp. 220–229.

[6] L. Ibraimi, M. Asim, and M. Petkovic, “Data Sharing on Untrusted Storage with Attribute-Based Encryption”, Technical Report, University of Twente, 2009.

[7] M. Guojun Wang, Qin Liu, Jie Wub, Minyi Guo,” Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers”, Inform. Forensics and Security, IEEE Transactions on Vol.7, 2011 pp.132-142,

[8] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption” in IEEE 2013 Transactions on Parallel and Distributed Systems, Volume: PP , Issue:99

[9] M. Li, S. Yu, N. Cao, and W. Lou, “Authorized private keyword search over encrypted personal health records in cloud computing,”in ICDCS ’11,Jun. 2011.

[10] 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.

[11] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-Based Encryption with Efficient Revocation”, ACM CCS, ser. CCS ’08, 2008, pp.417–426.

[12] R.C.Merkle, “The Protocols for Public Key Cryptosystems,” Proc.IEEE Symp.Security Privacy,1980.