

Secure Personal Health Records Using Encryption

D. Devikanniga
Dept. of Information Technology
Sri Ramakrishna Engineering College
Coimbatore, India

S.N. Gomathi Balan
Dept. of Information Technology
Sri Ramakrishna Engineering college
Coimbatore, India

Abstract-In the dispersed world, health information is exchanged based on the patients Personal Health Records (PHRs). Due to this reason, the construction and maintenance are focused by data centers, which are used for persons to gain high cost. The cloud providers are used in most of the PHR services to outsource the PHRs, which are stored by third party. The privacy is main anxiety because the PHRs information is shared to third party servers and illegal parties. To avoid this problem and to provide the guarantee security for PHRs, the encryption is applied for all PHRs before it is outsourcing. After encryption is applied still few major issues are present such as, flexible access, scalability in key organizations and well organized user revocation. These are the residual important challenges. In this proposed system, a patient-centric model has been generated with appropriate mechanisms for accessing PHR which are stored in semi confidential servers. Here the Attribute Based Encryption technique is used to encrypt every patients PHR's. To support on demand, user revocations are also enabled dynamically based on the variations of access policies or file attributes to improve the process.

Keywords-cloud computing, personal health records.

1. INTRODUCTION

Personal Health Record (PHR) is an upcoming concept. Network Security can be preventing an unauthorized access. The network is controlled by Network administrator. Through access control policies authorized data can be handled by network security. The authorized people, who are accessing the authorized information, can be identified by their ID and password. Network security having different computer networks, such as public and private that

are used in everyday's transaction and communication of business. Networks can be private but it is used by public to access the information.

Our approach is to encrypt the data before outsourcing. Our approach consist of two modules the doctor and the lab technician. The doctor can give certain information of the patient to the lab technician and he may send the report to the doctor after test.

In our approach we used ABE encryption and Advanced Encryption Standard to encrypt the files of the patient

2.RELATED WORKS

The traditional encryption techniques were applied to the personal health record at the early stages of the cloud computing and personal health record. Which is not secure nowadays and so attribute based encryption[1][3] with various variations is used

2.1 Symmetric Key Cryptography (SKC) based Solutions

Symmetric key algorithms in cryptography use the same cryptographic keys for both encryption and decryption of text. Based on the symmetric key derivation methods, various solution for securing outsourced data on semi-trusted servers has been proposed,

2.2 Public Key Cryptography (PKC) based Solutions

The most traditional method applied to the PHR for the security of data was public key encryption method. It is very less scalable in high key management. In one-to-one encryption techniques, in which break glass access is not possible during emergencies.

2.3 Attribute Based Encryption based Solutions

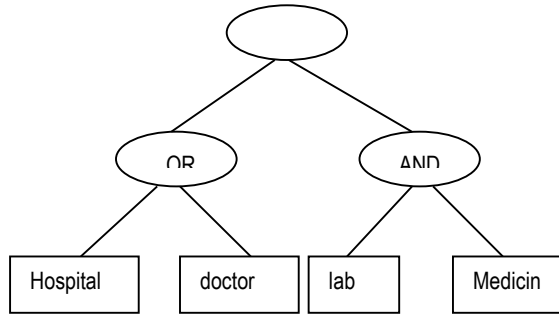


Fig.1. Attribute Based Encryption

The attributes can define an object very efficiently just as the identity of an object works. In ABE system both the cipher text and secret key will be depended on the attributes. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. 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 attribute only.

3. PROBLEM DEFINITION

The problem is being extended to a wide range of PHR system, where there are multiple PHR owners and users. The patients whose health data are being controlled. There exist semi trusted servers where patients store their health details and the users have access to those data. The access rights various according to the users such as some can have read access alone and some can have both read and write access. These access rights are provided by the owner of the corresponding PHR. The PHR document can be handled by multiple owners and so Multi-Authority Attribute Based Encryption (MA-ABE) is .

4. PROPOSED SOLUTION

4.1 Architecture

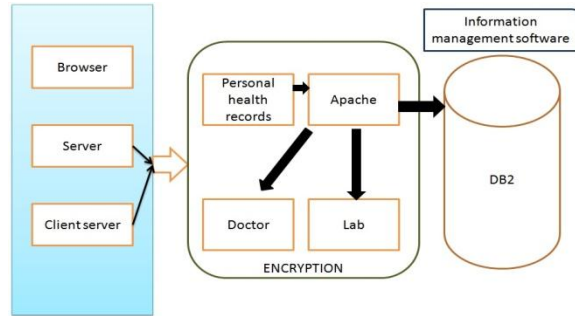


Fig.2. System Architecture

PHRs are stored and shared on semi trusted server. The patient health report is based on ABE algorithm. The owner allows multiple users to access patient health report with multiple authorities. Access rights are given based on authority. For this purpose MA-ABE techniques are proposed. An attribute wise encryption is done on health records.

Patient medical record is stored on server in encrypted format. Attribute wise encryption is done using ABE. PHR owners only knew who can access the health record. The owners distribute the secret keys for read and write data to authorized persons. The owner previously provides the temporary key to the emergency department. Breaking the normal procedure in an emergency period to access the whole data is called "Break-glass". This is clearly explained in Figure 2.

4.2 Design of Modules

This detailed insight of the design and working model of the proposed attribute based encryption for fine-grained access control is described below. The operations of proposed medical record sharing system combine KP-ABE traditional cryptography, allowing patients to share their medical records. These operations can be classified into following modules: In this section we discuss main module design concept for sharing of medical records using attribute based encryption.

Modules of the system are:

1. System Setup and Secret Key Generation
2. Encryption of Medical Records

3. View Medical Records (Decryption)

4.2.1 System Set-Up and Key-Generation

The KP-ABE algorithm takes security parameter as input. Using this input it provides public key and master secret key as output. Public key is specified as Pk and master secret key is specifies as Mk. Pk is used for encryption purpose by message senders. Mk is used for generating secret keys which is known by the authority.

user obtains secret key from the data owner through secure email by sending a request for the keys or data owner send the secret key to personal domain user via secure email.

4.2.2 Encryption

In attribute encryption the Sender runs randomized algorithm. It takes a given attribute for each user, the generated public key and a message as input. It provides cipher text as outputs.

The files can be requested by the user or the authority and can be viewed.

4.2.3 View Medical Record File /Decryption

The decryption uses deterministic algorithm which is run by patient or the doctor. It takes cipher text as input, which was encrypted and decrypted under the given set of attributes. The output is the patient health records.

User access structure is able to describe sophisticated logics over attributes. Each patients secret key has a unique secret sharing scheme which don't "match" each other[2][5]. Different types of users need access to different types of data in different phases by giving read and write permission to the public domain shown as fig.3.a and fig.3.b

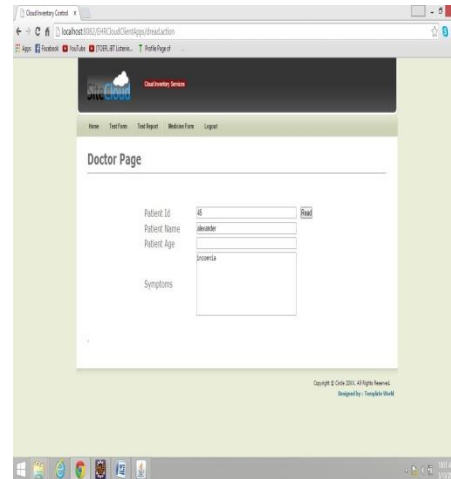


Fig.3.a. Fine-Grained Access Control Doctor page

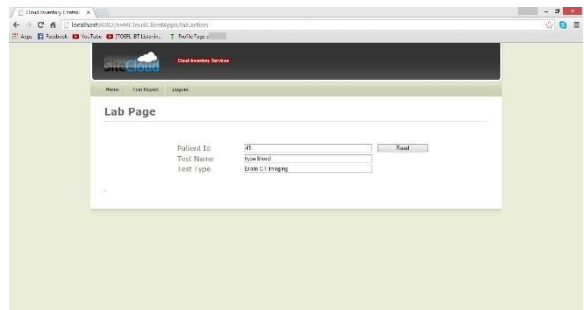


Fig.3.b: Fine-Grained Access Control lab page

5. IMPLEMENTATION

5.1 Algorithm for Attribute Key Setup

Step 1: KP-ABE Setup: Outputs public key and Master key for A as Set of attributes.

Step 2: Associate for each attribute in A with attribute universe as $U = \{1, 2, 3, \dots, n\}$.

Step 3: Associate each attributes $i \in U$ with a number t_i and also chose y uniformly at random in public parameter (Z_p^*) and y .

Step 4: The public key is: $PK = (T1 = gt^1, \dots, T1 = gt^{|U|}, Y = e(g, g)^y)$.

Step 5: The master key is: $MK = (t1, \dots, t | U | y)$.

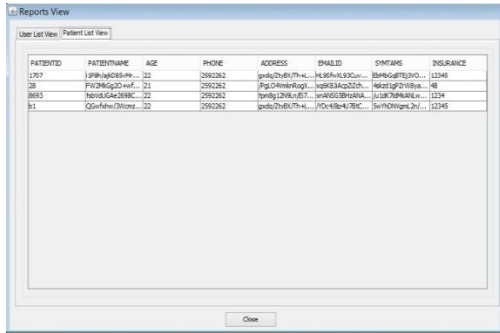
6. RESULT ANALYSIS

6.1 Analysis of Fine-Grained Access Control

In this access control method, the users access is limited. Based on the attribute the users defined access will be provided.. The policy updating is possible by updating the attribute or access policy in the system[4]. In emergency break glass access is provided.

6.2 ABE over Analysis of Fine-Grained Access Control

In the PHR system the users will be from different domain like the doctors, lab technician, and patient. Each user will be having different access control mechanism over the record.



PATIENTID	PATIENTNAME	AGE	PHONE	ADDRESS	EMAIL	SYMPTOM	INSURANCE
1707	SPH-ajC85-4M...	22	2592262	gndc7h8r7h-n...	H-96Fh-K-950v...	B8hGagfTEj3hD...	12245
8843	h2hG-G42-598C...	22	2592262	gng-2h8h8h8g...	h29633h2222h...	H2h2g7h7h7h...	12234
851	Q2h8h8h78h2m...	22	2592262	gndc7h8r7h-n...	JYD-48h-478C...	h2hDh7h7h2h...	12245

Fig.4. View of Health Records

The MA-ABE scheme will highly reduce the key-management issues. Users selects the attributes and the medical file wants to encrypt , Uploaded medical record can view by the other user as shown in fig.4. The users can view the record by providing the secret key matching the encrypted file.

7. APPLICATION

Medical centre ,organizations which try to secure their/employee health records can use this application

8. CONCLUSION

The personal health record system needs to be secure our application provides basic securities to protect the information from unauthorized access and loss. Our approach provides more security than traditional security which is easily hackable.

9. REFERENCES

[1] Ming Li and Shucheng Yu, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, January 2013

[2] 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'l ICST Conf. Security and Privacy

in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010

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

[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] 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'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89- 106, Sept. 2010