ISSN:0975-9646

Sharing Health Records in Personal and Public Domains in a Secure Environment with ABE

M Thulasi[1], D Shobha Rani[2]

[1] *M.Tech Student, Department of Computer Science & Engineering,*
SV Engineering College for Women,Tirupati, A.P, India.
[2]*Assistant Professor,Department of Computer Science & Engineering,*
SV Engineering College for Women,Tirupati, A.P, India.

Abstract-Now a days, cloud is one of the main source to share information online from anywhere at any time. And, here the cloud is also used to share one of the most sensitive information that is health information. A personal health record, or PHR, is a health record that contains health information related to the patient. The PHR is a patient centric model of health information exchange and it is outsourced to a third party such as a cloud provider which is a semi trusted server. The patient is considered as the owner for their PHRs. To assure patient's control over their own PHRs, it is a proficient method to encrypt the PHRs before outsourcing. So here we are proposing an ABE method to encrypt each patient's health record. We can utilize two ABE techniques namely KP-ABE in personal domain and MA-ABE in public domain respectively.

Keywords-PersonalHealthRecord, Encryption, Decryption, Attribute based Encryption.

I. Introduction

Today, Cloud is one of the most important sources to share any information even sensitive information at anywhere and anytime. This can be achieved by the on-demand facility of the cloud. Here, in this paper we are considering one of the most sensitive information i.e., health information that is going to be shared at online through cloud.. A PHR is a record that contains highly sensitive information of the patient. So here the patient will act as the owner for each health record. A PHR service allows a patient to create, manage, and control her personal health data in once place through the web, which has made storage, retrieval and sharing of the medical information more efficient. [1] Since the patient is the owner for their health record, he/she have to concern about her health records and can share the health information with a miscellaneous users including healthcare providers, family members or friends. Due to the high cost of construction and maintenance for specialized data centers, most of the PHR services are outsourced to third-party service providers, for example Microsoft Health Vault.[2].

While sharing such type of health information, we need to consider issues related to security and privacy to provide convenient PHR services for everyone in a secure environment. So here each owner personally take care regarding their health records in such a way that they are in a position to determine the access rights to various users based on the relationship with them.

II. Related Work

To access the sensitive information in the cloud environment, it is necessary to ensure the security and privacy risks in the data transmission. The traditional works include the Cryptographic techniques.

A. *Symmetric-Key Encryption (SKE)*

This is also termed as Single Key Encryption, only a single can be used for both encryption and decryption processes. The algorithms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) are well known algorithms that works based on Symmetric Key Encryption (SKE).

B. *Public Key Encryption (PKE)*

This is also named as Asymmetric Key Encryption; it uses two keys namely Private key and Public key. The private key is personally associated with each user, while the public key can be shared among the various users who involved in the data transmission. The algorithms such as Rivest Shamir Adleman (RSA) and Deffie Hellman Key Exchange are the examples for Public Key Encryption.[3]

C. Attribute Based Encryption (ABE)

Attribute Based Encryption (ABE) is a well known technique used today to secure the outsourced data in cloud. Here it uses a set of valid attributes to get access to the data.

Based on the attributes the data owner will generate some access policies. The users who satisfy the policy with valid attributes can get the key to access the data.

There are two well-known techniques that are used in ABE are KP-ABE and MA-ABE.

III. Proposed Frame work

Here, in this paper we consider the overall scenario by dividing the various users into two security domains broadly i.e., personal domain and public domain. Mainly the users who are directly associated with patient/PHR owner belongs to Personal domain. The users in public domain are the public user's namely health care providers, medical agencies, insurance authorities, pharmacists. With the help of ABE, access policies are generates based on the users or data attributes, which enables a patient to selectively share the PHR data among a set of users by encrypting the file under a set of attributes, without considering a complete list of the users.[4].

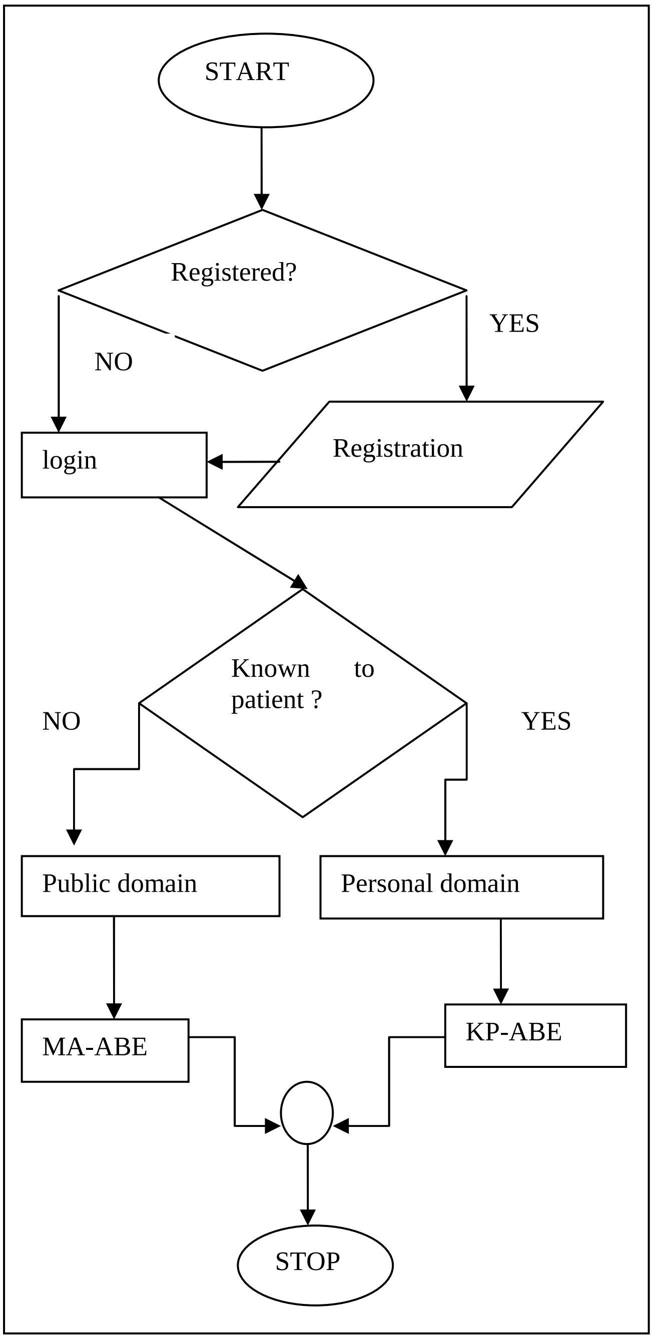


Fig 1: Overall Scenario for PHR Accessing.

IV. Securing PHRs in Personal Domain using KP-ABE

Here, in this domain the users like friends, family members are personally associated with PHR owner. In this paper, we are proposing one of the techniques of ABE such as KP-ABE for this personal domain. The owner of the PHR say patient is the ultimate trusted authority for the personal domain. With the use of KP-ABE system, the owner can manage the secret keys and access rights of users in the personal domain.

In the Personal Domain (PSD), the owner can provide access to users i.e., personal users by considering data attributes such as name, relation with owner etc., Based on the personal information and the medical the owner will provide access privileges to various users in the personal domain.

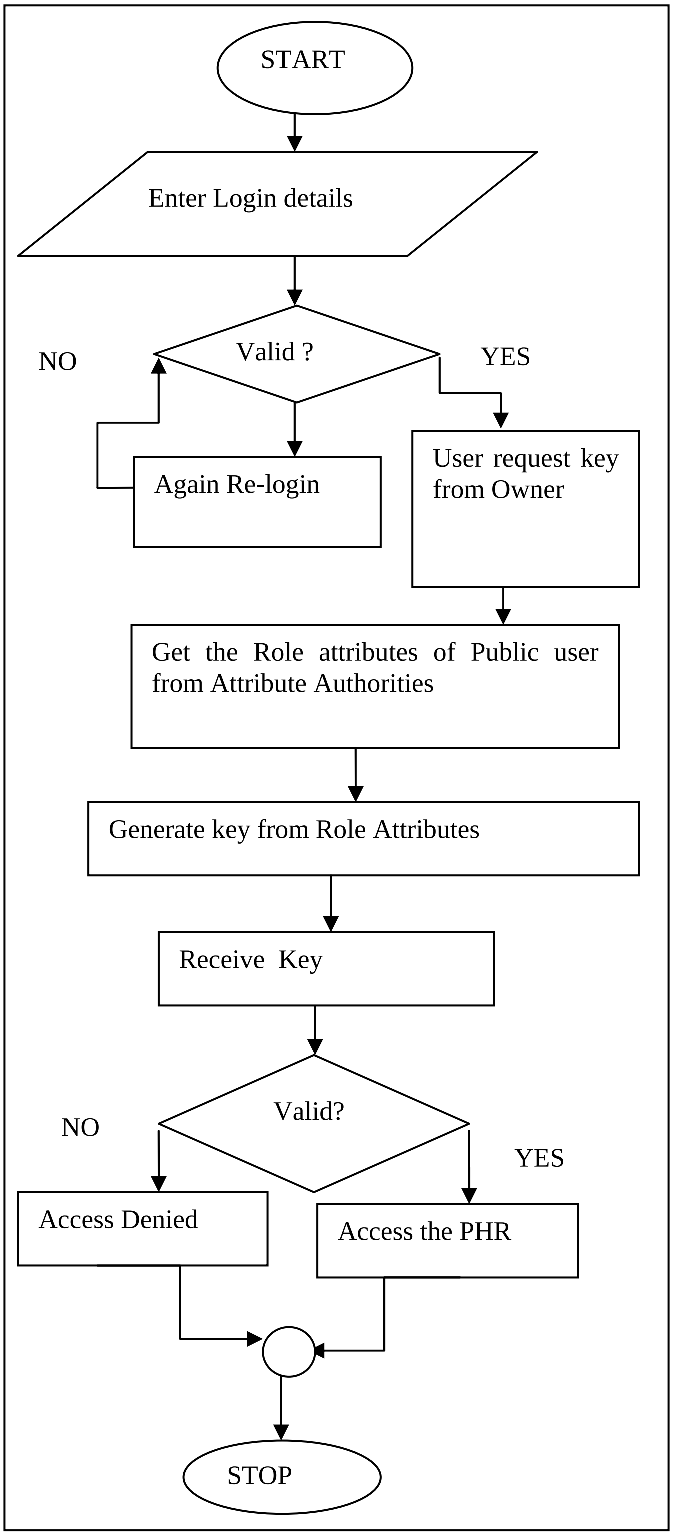

START
Enter Login details
Valid ?
NO
YES
Again Re-login
User request key from Owner
Get the Role attributes of Public user from Attribute Authorities
Generate key from Role Attributes
Receive Key
Valid?
NO
YES
Access Denied
Access the PHR
STOP

Fig: 2 Securing PHRs in personal domain using KP-ABE.

V. Securing PHRs in Public Domain using MA-ABE

For the public domain, this system define a set of role attributes to each user and a reader in PUD obtains secret key from different security authorities such as attribute authorities (AA) that binds the user to her claimed attributes/roles. For example a user in a public domain can have the role attributes such as profession, specialty, organization etc.,

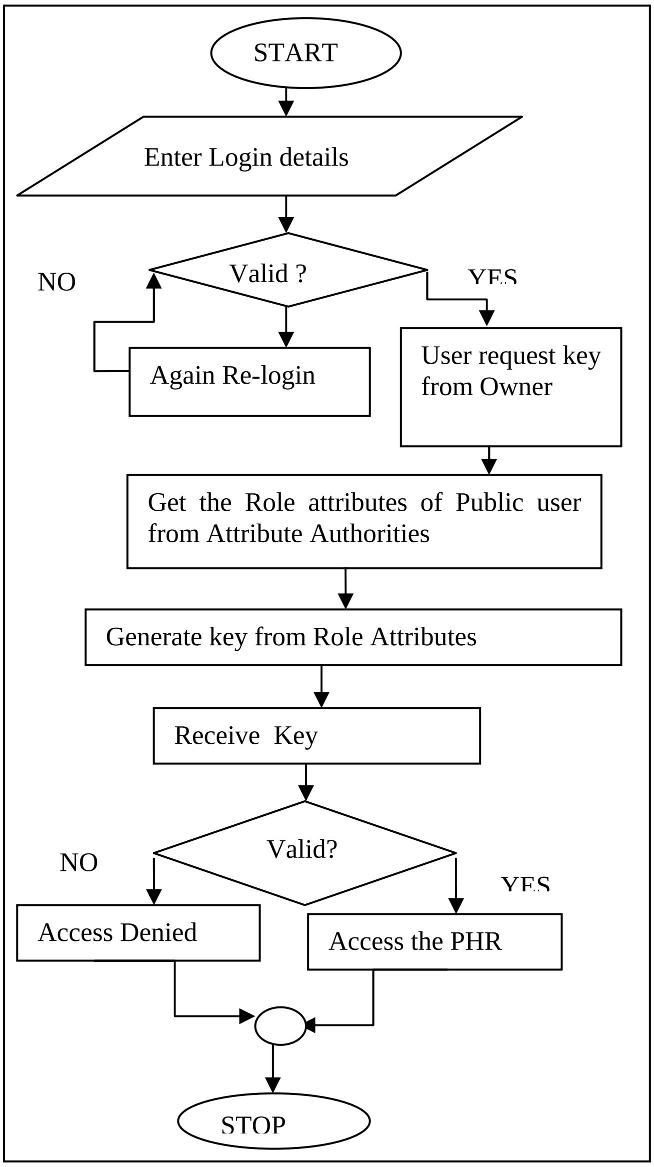
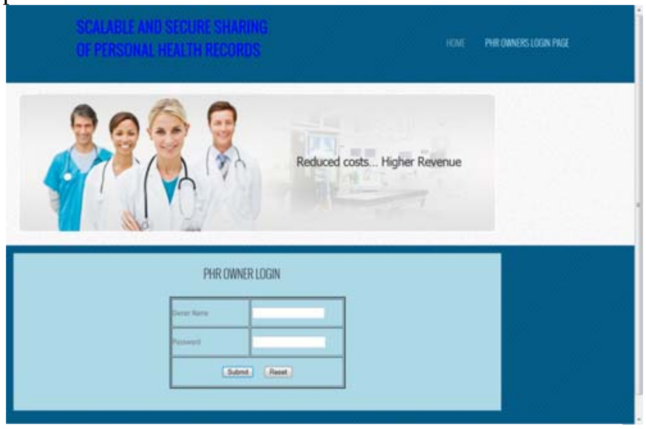

START
Enter Login details
Valid ?
NO
YES
Again Re-login
User request key from Owner
Get the Role attributes of Public user from Attribute Authorities
Generate key from Role Attributes
Receive Key
Valid?
NO
YES
Access Denied
Access the PHR
STOP

Fig: 3 Securing PHRs in public Domain

VI. Experimental results

We consider twenty patients health records for experimental verification for secured data transmission. The experimental results show the efficiency of the proposed framework. The below figures show some experimental results.



SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS

HOME | PHR OWNERS LOGIN PAGE

Reduced costs... Higher Revenue

PHR OWNER LOGIN

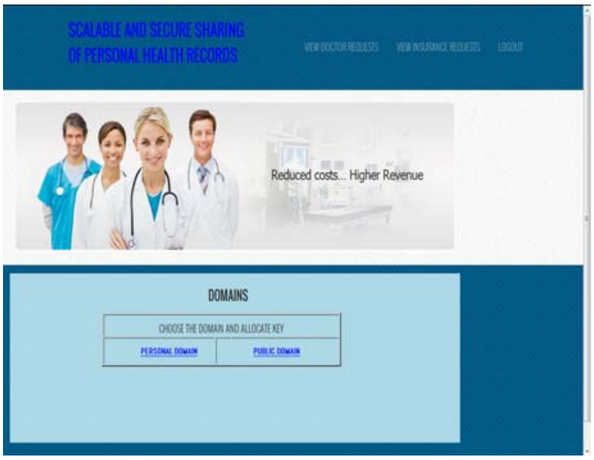
Owner Name:
Password:

Submit | Reset

Fig: 4 PHR Owner Login Page

The figure 4 shows the PHR Owner Login Webpage having owner name and the password. If the owner provides valid information, then he can have successful login.

The below figure, fig 4 contains the domains such as personal and public domains respectively. Based on the category of the users they fall into the particular domain. The Users who are personally associated belongs to Personal Domain hence required to use KP-ABE technique for sharing health records. Here, the data attributes of the various users are considered to provide access privileges to different users in the system.



SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS

VIEW DOCTOR REQUESTS | VIEW INSURANCE REQUESTS | LOGOUT

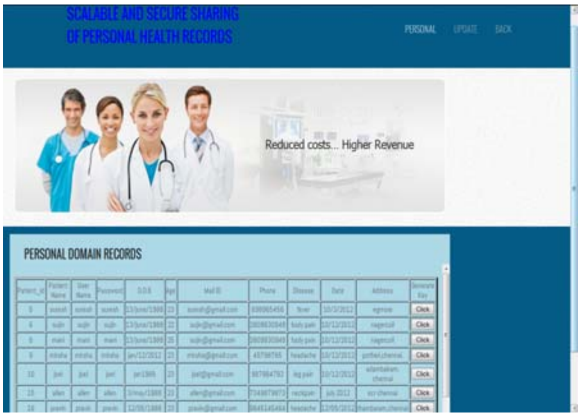
Reduced costs... Higher Revenue

DOMAINS

CHOOSE THE DOMAIN AND ALLOCATE KEY

PERSONAL DOMAIN | PUBLIC DOMAIN

Fig: 5 Multiple Domains in the System



SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS

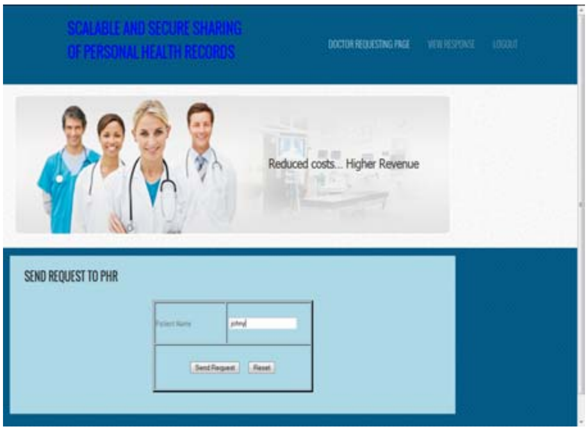
PERSONAL | UPDATE | BACK

Reduced costs... Higher Revenue

PERSONAL DOMAIN RECORDS

Patient_id	Patient Name	User Name	Password	D.O.B	Age	Mail ID	Phone	Disease	Date	Address	Generate Key
5	suresh	suresh	suresh	13/june/1988	23	suresh@gmail.com	8989965456	fever	10/3/2012	egmore	Click
6	sujin	sujin	sujin	13/june/1988	22	sujin@gmail.com	09898930848	body pain	10/12/2012	nagercoil	Click
8	mani	mani	mani	13/june/1988	25	sujin@gmail.com	09898930848	body pain	10/12/2012	nagercoil	Click
9	nitisha	nitisha	nitisha	jan/12/2012	23	nitisha@gmail.com	45798785	headache	10/12/2012	porthet,chennai	Click
10	joel	joel	joel	jan1988	23	joel@gmail.com	987984792	leg pain	10/12/2012	adambakkam chennai	Click
13	allen	allen	allen	3/may/1988	23	allen@gmail.com	7348879873	neckpain	july 2012	ecr chennai	Click
14	pravin	pravin	pravin	12/05/1988	23	pravin@gmail.com	9845145464	headache	12/05/2012	thambaram,chennai	Click

Fig:6 Health Records in Personal Domain



SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS

DOCTOR REQUESTING PAGE | VIEW RESPONSE | LOGOUT

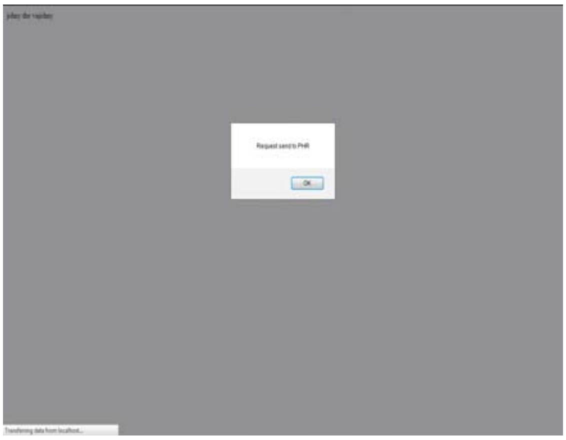
Reduced costs... Higher Revenue

SEND REQUEST TO PHR

Patient Name: johny

Send Request | Reset

Fig: 7 Requests for PHR



Request sent to PHR

Transferring data from localhost...

Fig: 8 Issuing key for PHR Access

The above figures show the PHR accessing by requesting key from the owner and sending key to the user.

VII. Conclusion

In this paper, we proposed a novel framework to share health records across personal and public domains. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. By considering nearly twenty patients records we show that our solution is both scalable and efficient

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

[2] http://microsofthealthvault.com

[3] “Cryptography and Network Security “ ,fourth edition by William Stallings.

[4] Attribute-Based Encryption with Fast Decryption by Susan Hohenberger and Brent Waters.

First Author Ms. M.Thulasi, is a student of SV Engineering college for women (affiliated to JNTU Anantapur) pursuing M.Tech in the Department of Computer Science Engineering, Tirupati, A.P, India.

Second Author Mrs. D.Shobha Rani M.Tech., working as an Assistant Professor in the Department of Computer Science & Engineering at SV Engineering College for Women (affiliated to JNTU Anantapur) Tirupati, A.P, India.