International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Secure Role Based Access Policy for PHR Patient-Centric Model of Health Information Exchange Using Homomorphic Encryption

Rasal Swati A.[1], Pawar B. V.[2]

[1] M. E. (Computer Engg.) II Student, Padmabhushan Vasantdada Patil College of Engineering, Pune University, Pune

[2] Associate Professor, Padmabhushan Vasantdada Patil College of Engineering, Pune University, Pune

Abstract: ***Cloud computing has being defined as a pool of virtualized computing resources. Due to this virtualization, there is an immense growth in applications of cloud computing. One of the important fields is Personal Health Records. In recent years, personal health records (PHR) has transpired as a patient-centric model for exchanging health information. The health information is outsourced to a third party like cloud service providers. But what if the service providers are compromised, this may create a huge threat to the patient's information. Personal Health Records enables patients to manage their own medical records in a centralized way. But by storing PHRs in the cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt their PHR data before uploading to the cloud servers. In our proposed framework we securely share PHR files with fine-grained access. The framework efficiently handles the prime challenge of key management brought by introduction of multiple PHR users and owners. The framework addresses the unique challenges brought by multiple PHR owners and users, in that it will also reduce the key management complexity while enhance the privacy guarantees compared with previous works. The solution for securely storing PHR on cloud can be proved as both scalable and efficient though implementation and simulation.***

Keywords: PHR, cloud computing, fine-grained access control, attribute-based encryption

1. Introduction

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in a centralized place through the web, from anywhere and at any time (as long as they have a web browser and Internet connection), which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient has the full control of her medical records and can effectively share her health data with a wide range of users, including staffs from healthcare providers, and their family members or friends. In this way, the accuracy and quality of care are improved, while the healthcare cost is lowered.

The PHR providers are more and more willing to shift their PHR storage and application services into the cloud instead of building specialized data centers, in order to lower their operational cost. For example, two major cloud platform providers, Google and Microsoft are both providing their PHR services, Google Health1 and Microsoft HealthVault2.

While it is exciting to have PHR services in the cloud for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about the privacy of patients' personal health data and who could gain access to the PHRs when they are stored in a cloud server. Since patients lose physical control to their own personal health data, directly placing those sensitive data under the control of the servers cannot provide strong privacy assurance at all.

The PHR data could be leaked if an insider in the cloud provider's organization misbehaves, due to the high value of the sensitive personal health information (PHI). Since cloud computing is an open platform, the servers are subjected to malicious outside attacks. To deal with the potential risks of privacy exposure, the proposed methodology is developed to secure the personal health record.

2. System Architecture

As shown in figure 1, any user can create personal health record and store it on cloud server. Such user is known as PHR owner. Patient having PHR for storing health related information on cloud has all access control of creating, managing and controlling his/her record. Records are fully controlled by the patient for maintaining security of data sharing and access control of the records. Homomorphic Encryption is used for ensuring the high degree of patient privacy PHR is stored in an encrypted format. Only authorized users have rights to access the PHR.

To maintain the security of data storage and reducing the key management for the owners and users, users are categorized into multiple security domains. Personalized fine-grained role based access policies are specified for file encryption in the proposed mechanism for key distribution and encryption of records. In case of emergency of any type emergency department i.e. ED has a control on the PHR of the patient. In the case of any emergency, emergency staff communicates with the ED. ED provides access to the PHR record by verifying the emergency situation and its identity and also provides the temporary read key for accessing the record [1]. Homomorphic encryption technique is used for maintain the security and scalability of personal health records and also provides role based access policies to the user. With this

mechanism cloud can perform operations on encrypted data and send this patient updates, alerts based on the received data.

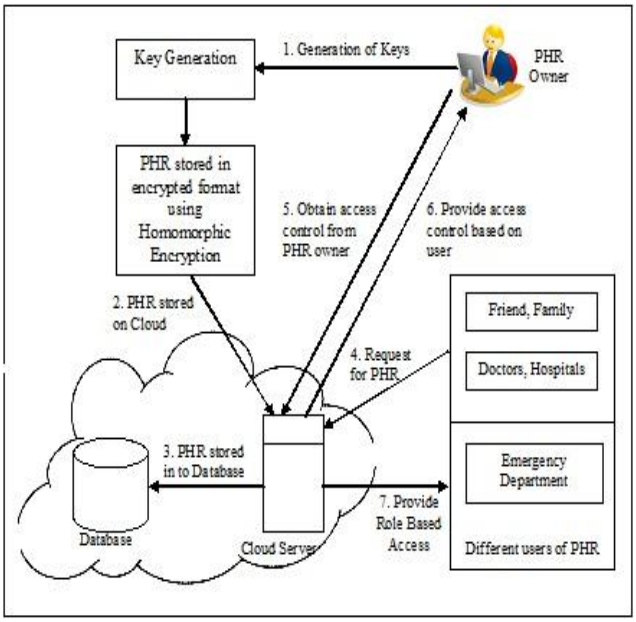

Figure 1: System Architecture

3. Description of Modules

The framework is divided into following modules:

3.1 Key Generation Module

By using Elgamal homomorphic encryption algorithm we will generate two keys i.e. private key 'privk' and public key 'pubk'.

3.2 Encryption & Decryption Module

A key is used to encrypt and decrypt whatever data is being encrypted /decrypted. In proposed system data is stored in encrypted format. Anyone can download encrypted PHR but only those users can read data that provides corresponding decryption key. The algorithms used for Encryption and Decryption are described in the next subsection.

3.3 Role Based Access Policy

In this module users of PHR system are divided into multiple security domains and assign access control for the PHR that greatly reduces the key management for owners and users. Users like PHR owner, doctor, family members, friends, researchers, emergency staff access, and access by cloud provider.

4. Software & Hardware Requirement

The system will require minimum two machines with following configuration:

4.1 Hardware Requirements

Processor: core2duo (& onwards)
RAM - 2 GB (min)
Hard Disk - 80 GB

4.2 Software Requirements

Operating System- Linux or Windows
Application Libraries: Java Vaadin framework, Maven plugin, core java and MySQL Connector
Language: J2EE and Java
Front End - Java vaadin UI
Database: MySQL Server

5. System Detailed Design Diagram

5.1 Data Flow Diagram

The Data Flow Diagram (DFD) is a graphical representation of the flow of data through a system. It enables, to represent the processes in the system from the viewpoint of data. The DFD of the proposed system is shown below. The input and output are the source node and destination node respectively. The data flow in the system is shown with different level of DFDs. Figure 2, 3 and 4 shows the different levels of DFDs.

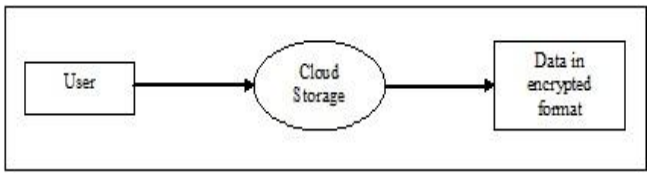

Figure 2: DFD Level-0

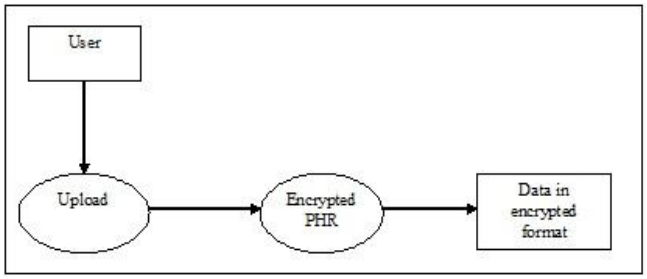

Figure 3: DFD Level-1

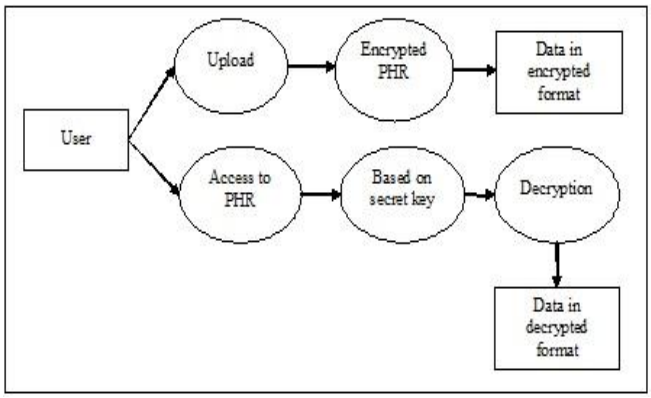

Figure 4: DFD Level-2

5.2 System Activity Diagram

Activity diagrams are graphical representations of workflows of stepwise activities and actions. In the Unified Modeling Language, activity diagrams show the overall flow of control. The figure 5 illustrates the complete flow of system.

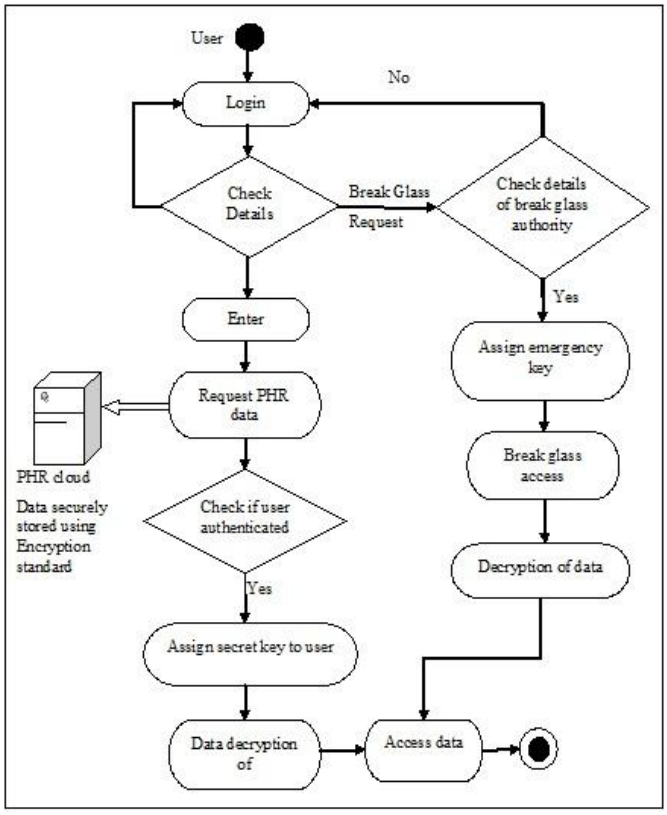

Figure 5: System Activity Diagram

5.3 System Sequence Diagram

Sequence diagrams describe interactions among classes in terms of an exchange of messages over time. Interaction among the components of a system is very important from implementation and execution perspective. The interaction of various components of proposed system is depicted in the following figure 6.

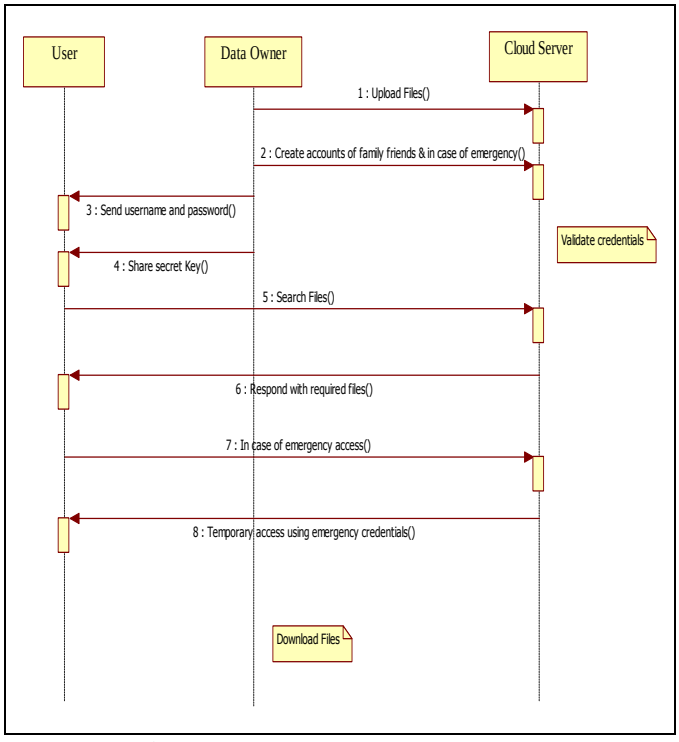

Figure 6: System Sequence Diagram

6. Result Analysis

Figure 7, shows the first window used for signing on the PHR system for PHR owner and doctor. This form provides the authentication for the input values. All the fields provided should be filled by user.

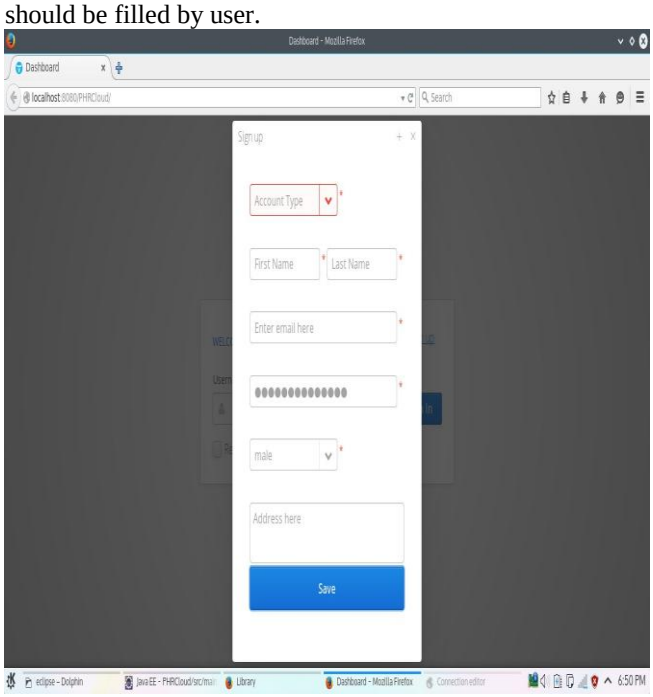

Figure 7: Sign up form

Figure 8, shows the login window for all the users (PHR owner, doctor, friend, family) on PHR system.

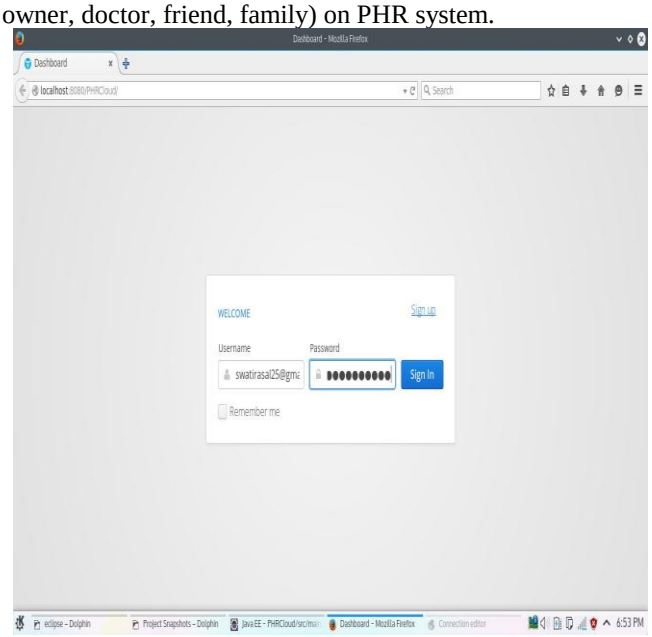

Figure 8: Login window for all users

Figure 9, 10 shows the dashboard of the PHR owner. Owner has the menus of uploading records, updating his personal information, managing the accounts of friends and family members.

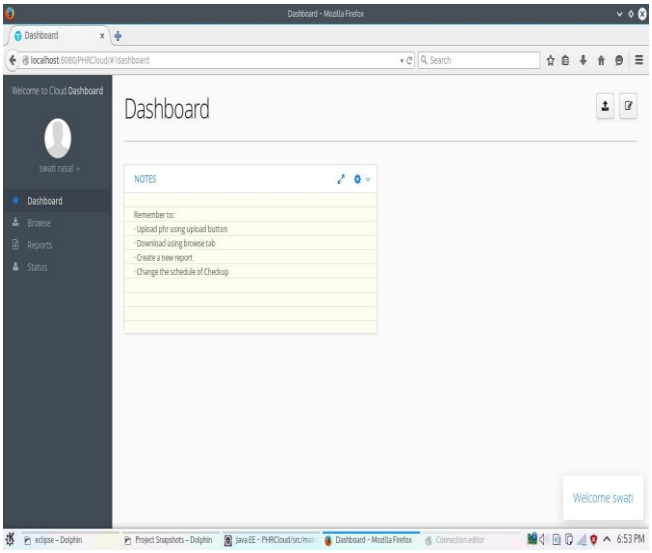

Figure 9: Dashboard of PHR owner

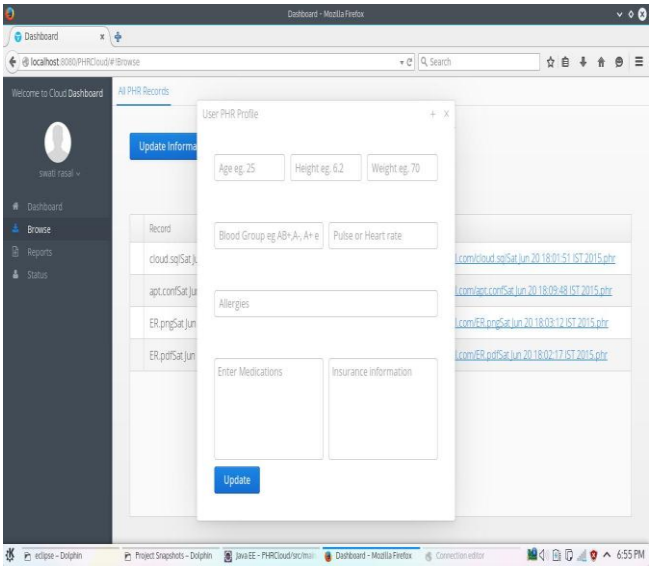

Figure 10: PHR owner profile

Figure 11, illustrates PHR Owner Add friend and family members to access his records and secret key is sent to the mail at the time of account creation.

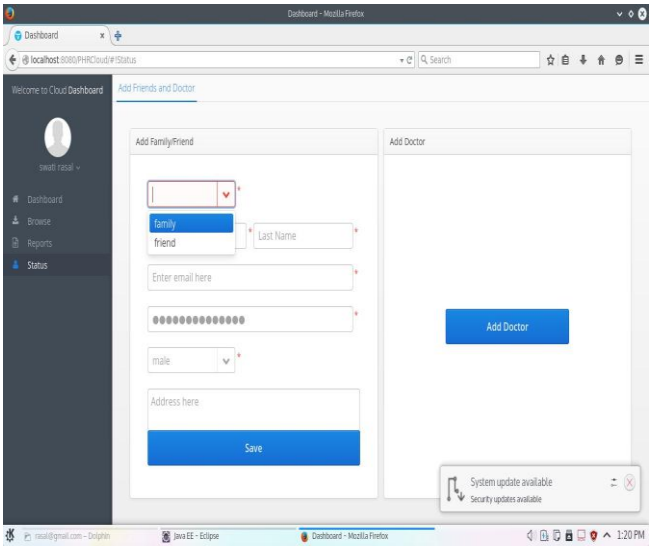

Figure 11: PHR owner manages other accounts

Figure 12, illustrates show the uploaded files of PHR owner. Owner requires the private keys those were sent to his mail at the time of uploading, for accessing those files. Only users having the keys have rights to download the files. This provides the security for managing the record on cloud. The uploaded files are stored on cloud in an encrypted format.

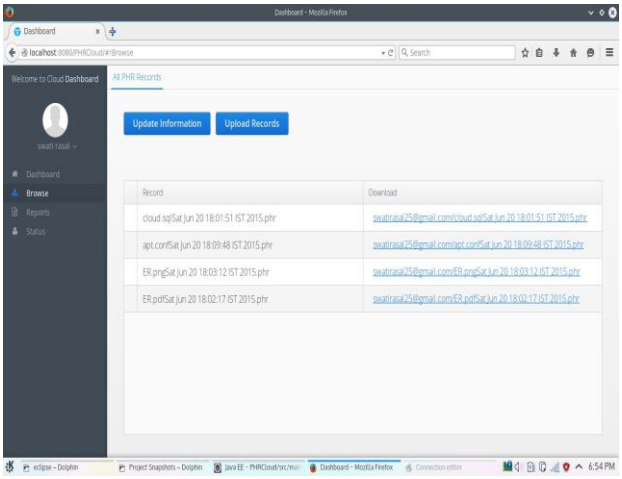

Figure 12: PHR owner files

Figure 13, 14, illustrates the dashboard of doctor. Doctor has the facility of viewing the profile of patient. He can also view the files of patient. For accessing the uploaded files of patient the doctor requires the private keys those were sent to his mail account. This maintains the security of patient's health record. Only authorized user has the rights to access the records.

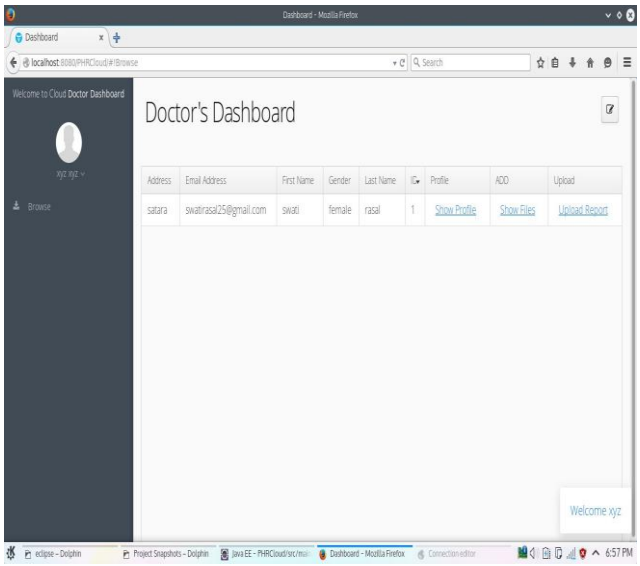

Figure 13: Doctor's Dashboard

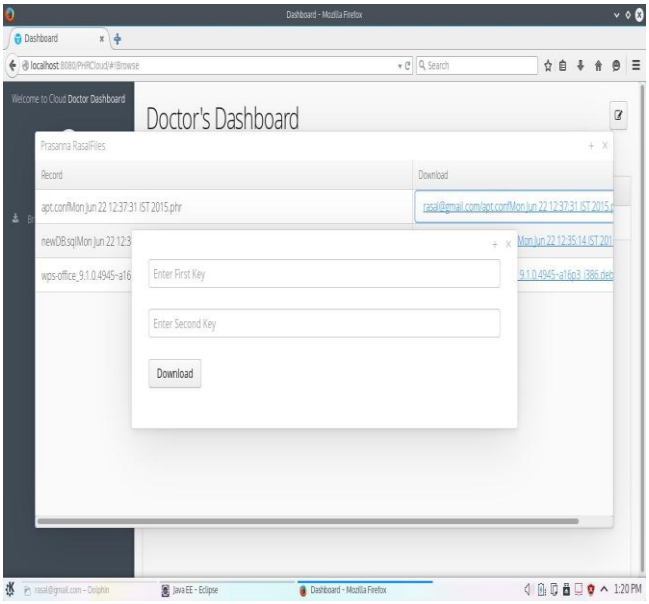

Figure 14: Doctor accessing patient's record

7. Comparison Of Developed System And Existing System

There have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. The existing systems usually assume the use of a single trusted authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem since the TA can access all the encrypted files, opening the door for potential privacy exposure. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys[1].

The developed system assures the patients' control over access to their own PHRs; and it provides promising method to encrypt the PHRs before outsourcing. The system ensures patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. In order to protect the personal health data stored on a semi-trusted server, system enabled a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users

The system focuses on the multiple data owner scenario, and divides the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. It bridges the above gaps by proposing a unified security framework for patient-centric sharing of PHRs in a multi-domain, multi-authority PHR system with many users. The framework captures application level requirements of both public and personal use of a patient's PHRs, and distributes users' trust to multiple authorities that better reflects reality.

8. Conclusion

1) The project discusses platform for sharing of personal health records in the secure and scalable manner by using Cloud computing. To enhance the fully patient centric concept and its privacy each PHR file is encrypted which also allows fine grained data access.
2) The user doesn't need to locally store their data. So there is burden of managing data at local site. User can rely on cloud service provider for the storage of their data.
3) The framework efficiently handles the prime challenge of key management brought by introduction of multiple PHR users and owners.
4) Homomorphic Encryption is used for security purpose and for key management.
5) The key idea is to divide the system into multiple security domains (namely public domains and personal domains) according to the different user's data access requirements.

References

[1] Ming Li, Member, IEEE, Shucheng Yu, Scalable and secure sharing of personal health record in cloud computing using attribute based encryption [1], IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013
[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] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Intl Conf. Distributed Computing Systems (ICDCS 11), June 2011.
[5] A. Boldyreva, V. Goyal, and V. Kumar, Identity-Based Encryption with Efficient Revocation[5], Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.