International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, February 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Role Based and Secure Access Policy for PHR using Homomorphic Cryptosystem

Anuja H. Todkar[1], Imran Y. Inamdar[2], Ashvini A. Todkar[3]

[1,2] *Computer Science & Engineering,Nanasaheb Mahadik College of Engineering, Peth,(India)*

[3] *Computer Science & Engineering, Sanjay Bhokare Group of Institutes, Miraj,(India)*

ABSTRACT

Cloud computing is delivery of computing resources such as processing power, storage and networking as a service to users. Cloud users storing his PHR on the cloud can be targeted and misused by advertising agencies and doctors for in advent actions. For securing user PHR stored on public cloud we have proposed a system which uses homomorphic key encryption. Our proposed system provides protection, integrity, privacy preservation, role based access control, homomorphic key encryption for user PHR stored on public cloud. In role based access control we have divided our system into multiple security domains. Each security domain provides access to authorized users based on roles. In case of emergency break glass access is provided to users from emergency department. Using the solutions quoted above we provide highly secure system for outsourcing and sharing users PHR on public cloud.

***Keywords:* Cloud Computing, Security, Personal Health Record, Role Based Authorization, Homomorphic Cryptosystem.**

I. INTRODUCTION

Cloud Computing provides service to users on demand through Internet. Services such as software, computing, storage, and networking are provided to users on demand basis. Cloud itself is a pool of resources which are rented to users when and where required in cost effective way. Cloud Service Providers provides massive scaling of resources and usage based on per user basis. User Resources on the cloud can be deployed by the vendor and used by the client. Using cloud user is not required to buy resources or go through lengthy procedure of configuring the resources, Instead users can rent these resources and pay only for the usage in hours, days or months.

Cloud services are provided in three categories as follows: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Cloud has three deployment models as public, private or hybrid. Public cloud is hosted, operated by cloud service providers and available publicly. Private cloud is generally deployed in organization's premises and is limited for that organization only. With the advent of cloud computing users are more relied on cloud for storage as well as sharing of data. But this comes with an notion of security as user data resides on third party servers. Cloud service providers are honest but curious and can read

user data out of curiosity which hampers privacy of user. Also there is a possibility where an unauthorized user gains access to the cloud by interrupting an authorized user, there by infecting the entire cloud. This consequently affects many customers who share data via infected cloud.

II. LITERATURE SURVEY

In [1] the author has suggested a suite of mechanism and novel patient-centric framework to control access to user PHR stored on semi trusted cloud servers. To achieve fine-grained access control for PHRs they have used attribute-based encryption (ABE) techniques to encrypt each patient PHR. In this technique authorized users are allowed access to encrypted contents only on possession of certain attributes as specified by data owner during encryption. For additional level of security, in system with multiple data owner they have used multi-authority ABE. These techniques allow dynamic modification of access policies, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Commercially available web-based storage systems do not provide confidentiality for users outsourcing their health data. [2]. Traditional mechanisms for access control have several limitations in providing confidentiality, integrity and enforcing access control policies and the data has to be stored on a central server locked by the access control policies. Also from the moment when data is uploaded to servers, owner loses control on the data. In CP-ABE, user data is encrypted over a set attributes and access control policies. The access policy specifies the set of attributes to be possessed by authorized users in order to decrypt the encrypted data. Once the data is encrypted by using above mentioned scheme, it can now be safely outsourced to public cloud storage, where everyone can download encrypted data but only authorized satisfying access policy and set of attributes can decrypt PHR.

Cloud users outsource their data to the cloud storage servers to reduce the management and maintenance costs. Cloud service providers cannot be fully trusted for storing sensitive personal information. Encryption before storage is a promising way to protect the integrity and confidentiality of the outsourced user health data, but it also introduces much difficulty to performing effective researches over encrypted information. Using online Personal Health Record as a case study, the author first shows the necessity of search capability authorization that reduces the privacy exposure resulting from the search results and establishes a scalable framework for Authorized Private Keyword Search over encrypted cloud data [3]. One of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates [4]. The problem of applying the attribute-based encryption in an outsourced architecture introduces some challenges related to the attribute and user revocation. They have suggested solution to this problem as well. They propose an access control mechanism using cipher text-policy attribute based with efficient attribute and user cancellation capability. By the literature survey, several issues identified in cloud computing environment are security, key complexity and user revocation. Our ultimate objective is to provide solution to the issues identified here. Our proposed system will solve security and key management problem by making use of SDC homomorphic encryption [1]. The key idea is to divide the system into different roles (namely, doctor/family/friend/Individual user) according to the different user's data access requirements. We are focusing on multiple data owner scenario which will supports an efficient on-demand user/attribute revocation and provide emergency access through break glass.

III. NEED OF PRESENT WORK

By the literature survey, following issues are identified in cloud computing:

- Security

Cloud does not differentiate between a sensitive data from a common data thus anyone can access those sensitive data. Thus there is lack of data integrity in cloud computing. It will solve security and key management problem by making use of Homomorphic encryption. In this PHR record is stored in encrypted form. Anyone can download encrypted PHR but the user who provides corresponding decryption key can access the
record.

- Key Complexity

In proposed system we will try to minimize issues regarding privacy exposure, complexity in key management by providing role based access policy for personal health record using homomorphic cryptosystem.

- User Revocation

PHR owner has full control on his /her Personal Health Record. He/she can manage, control and delete record at any time. PHR owner assign access control to PHR users according to their relations with PHR owner. After specific period of time PHR owner can revoke all the access control from the user. We are focusing on multiple data owner scenario and it will support an efficient on-demand user/attribute revocation.

- Role based access policy

Our system divides users into different category like family/friend, doctor, researcher, individual user. Assign role to user according to their relation with PHR owner. First PHR owner checks who is requesting for Personal Health Record. If he/she is one of the family member or close friend then he/she will get full access to record and not as an independent document. Please do not revise any of the current designations.

IV. 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. PHR proprietor has full control on his/her record. He/She can create, manage and control record. To get secure information sharing and access control to PHRs which is put away in cloud server are completely controlled by the patient. A high level of patient security can be guaranteed by utilizing Homomorphic Cryptosystem system and put away this PHR in encoded design. Anybody can download encoded PHR however the client who gives comparing decoding key can get to the record. For secure data storage, the users are divided in the PHR system into multiple security domains that greatly reduces the key management for owners and users. In this we propose mechanism for key distribution and encryption so that PHR owners can specify role-based access policies during file encryption. Each PHR owner access is given to the emergency department i.e ED. If any emergency situation is occur then

emergency staff needs to communicate with ED for accessing PHR record and verify its identity and emergency situation, and obtain temporary read key to access his/her PHR.

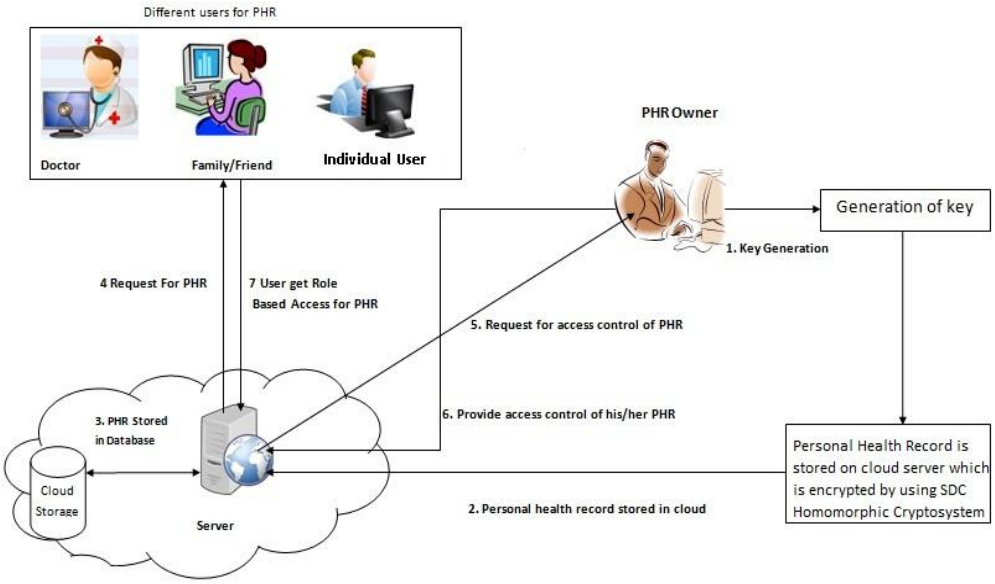

Fig 1. System Architecture

To achieve secure and scalable role based access for personal health record we uses homomorphic cryptosystem. With the use of homomorphic cryptosystem cloud can perform functional computation on encrypted data and send this patient updates and alerts based on the received data.

V. MODULAR DESIGN

Following algorithm is used for key generation, encryption and decryption Proposed Algorithm

1) Key Generation:

Key Generation (Prime number):

The key is a random P-bit odd integer p.

2) Encryption

Figure 2 describes, block diagram for encryption and decryption of PHR using SDC Cryptosystem. Stepwise procedure of encryption is described as follows.

Encrypt (p, msg): To encrypt a bit m {0, 1}, output the cipher text is obtained by c = m + p + r * p * q, where r is a random R bit number and q is a constant Q-bit big integer.

3) Decryption

Decrypt (plain text, cipher): Output (c mod p).

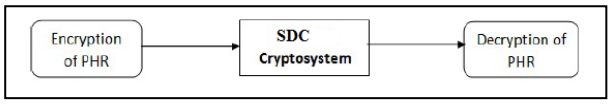

Fig 2. Encryption and Decryption

4) Role Based Access Policy

Figure 3 shows block diagram for role based access policy. In this module users of PHR system are categorized into number of security domains and assign access control for the PHR that greatly minimizes the key management users. PHR is distributed depending on his/her relationship with PHR owner. Users may be in personal sector of public sector, have rights according to their positions with PHR owner. PHR owner is the person who creates medical record and he/she has the all rights on his/her personal health record.PHR owner decides which part of PHR is accessed by which user.

VI. CONCLUSION

During this work, problem of security and key complexity is identified by the literature survey. Our system titled "Secure Role Based Access Policy for PHR using Homomorphic Cryptosystem gives solution to problem identified. This system is applicable for cloud environment. Powerful encryption technique i.e. SDC Cryptosystem is used in this system. SDC gives better security. SDC requires less time for key generation, encryption and decryption as compare to ElGamal and RSA. In future we will extend our work to achieve user revocation. And also we will extend our system to real-time application.

REFERENCES

[1] Ming Li, Member, IEEE, Shucheng Yu, _Scalable and secure sharing of personal health record in cloud computing using attribute based encryption_ IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL.24, NO. 1, JANUARY 2013,vol.25,no. 4, April 2013.

[2] L. Ibraimi, M. Asim, and M. Petkovic,_Secure Management of Personal Health Records by Applying Attribute-Based Encryption,_ technical report, Unit,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, _ EAuthorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing,_ Proc. 31st Intl Conf. Distributed Computing Systems,(ICDCS 11),2011.

[5] A. Boldyreva, V. Goyal, and V. Kumar, _Identity-Based Encryption with E_cient Revocation,_Proc. 15th ACM Conf. Computer and Comm. Security (CCS), ,pp. 417-426,,2008.