ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption

Ambadas Wairagar[1], Sandip Pawar[1], Rahul Kanthale[1], Prof.Shrikant Markad[2]

Students, Dept. of Computer Engineering, SCCOE, Rahuri Factory Ahmednagar, Maharashtra, India[1]

Assistant Professor, Dept. of Computer Engineering, SCCOE,Rahuri Factory Ahmednagar, Maharashtra, India[2]

ABSTRACT: Personal health record (PHR) is patient centric model in that patient's health information can share with anyone it will be store in third part, it will be work as cloud. Hence there is main concern of security of private health information as it was stored at third party server and to unauthorized parties. In these proposed method before outsourcing the data give the assurance to patients they having the authority to access own PHR. Till issue such as risk of Health information exposure, easily accessibility, Key Management, efficiency user revocation. In this paper, we define patient-centric architecture and access control for achieve the information of PHR which is stored in cloud server. We can encrypt patient's PHR File by using Attribute based Encryption and easy to access control on PHR File. As compare to previous work we secure data outsourcing. In these studies we focus on multiple data owner scenario for the avoid complexity for the user and owner and divided users in different security domain. We can focus also access policies dynamic modification, support to on demand user or attribute revocation, access speedily in emergency situation. In our proposed method scalability, efficiency and securities.

KEYWORDS: Personal health records, cloud computing, data privacy, fine-grained access control, attribute-based encryption.

I. INTRODUCTION

Now a days, personal health record (PHR) is patient centric model which is store the health information for exchange from third party server. These system help for the stored data in one place where we can retrieve data easily, PHR work effectively for the create, manage and Update own Data through the Web and sharing of the medical information more efficient .the important thing is each patient can access the full control on her/his medical information and can share the own health data with different doctors, friends and family members. PHR service outsource to and provide by third party. For example, Microsoft HealthVault.1 Recently, architectures of storing PHRs in cloud computing have been proposed in [2], [3].

It was efficient PHR Service thus the access on large amount so privacy security and risk is also high which could obstruct it's widely adoption. The sharing personal health information is sensitive part so the main concern is can patient access information easily, especially when the data store in third party server and which may not secure. In [4] Author define the already exist healthcare regulations like HIPAA now a days amended to incorporate business associates, entities not covered by Cloud providers [5]. On opposite site the due to sensitive personal health information third party storage server can target of various malicious behaviour it will be caused destroy the personal health information. To encrypt data before outsourcing is promising and scalable approach. Who is given associated decryption keys these users only have to access PHR, while remain confidential to the rest of users. Further when patient feel it's necessary then they always retain the information not only grant but also accessing privilege. Thus the goal of the system is keep privacy of patient disease history. PHR system. The authorized users need PHR either personal use or professional use, means for inform personal doctor, family members or friends while the latter can be pharmacist or researcher etc. We refer to the two categories of users as personal and professional users, respectively. When some user's access request is unpredictable then it was difficult to list out. An opposite way in [8], [9] existing system define single data owner scenario. In a PHR system, by using crypto graphic key among the users can encrypt own personal health information on own way. There is limitation to access owner's history as owner if not online, the

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

each user can access the data by requesting for the key. Another option is Central Authority CA who can manage the information on behalf of PHR owner. In this studies, we focus on patient centric model, security of PHRs sharing which is stored in third party server or semi trusted server and focus on complicated management issues. In order to protect the personal health data stored on a semi trusted server, we adopt attribute- based encryption (ABE) as the main encryption primitive. On the based on attribute of users or data access policies can be define as using ABE patient able to share one of the particular part with the user by the encrypted these specific part, without the need to know a complete list of users. Hence to intergrade ABE into high scale data issue are dynamic policy update, on demand revocation, management scalability and remain up to date information. To this end, we make the following main contributions:

1. In cloud computing environment to securing the patient-centric sharing PHR we develop ABE based framework under multi owner setting. To resolve the management challenges we divided users in two type of domain public domain and personal domain. On our framework we can handle multiple PHR sharing applications requirement while incurring owner and user in the system.

2. We define key encryption and description mechanism so PHR users can personalized well grained access policies during file encryption. In personal domain owner can assign access privilege to personal users with using data attributes encrypt PHR file.

3. In terms of multiple metrics in computation, communication, storage, and key management we provide an analysis of the complexity and scalability of our proposed secure PHR sharing solution. We compare our studies to previous one in security, scalability, complexity. The efficiency of our scheme of is implementing on modern workstation.

We clarify Multi authority Application Based Encryption in public domain and explain which type of access policies.

II. LITERATURE SURVEY

User In these studies cryptographically enforced to access control on data and encrypted data of PHR. We define scalability and complexity of the proposed system PHR sharing solution.

2.1 ABE for Fine-Grained Data Access Control

Most of the users work on ABE to realized access control on outsourced data [13], [14], [9], [15].To secure personal health information used ABE. In [16] define attribute based infrastructure in EHRs system, where each patient's EHRs file can encrypted for broadcast ABE which allows direct revocation. In [20], investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cellphones so that EMR could be accessed when the health provider is offline. Hence the some issue of these method .In the system define use of single trusted Key. Trusted Key can access encrypted file and given opportunity for potential privacy exposure.

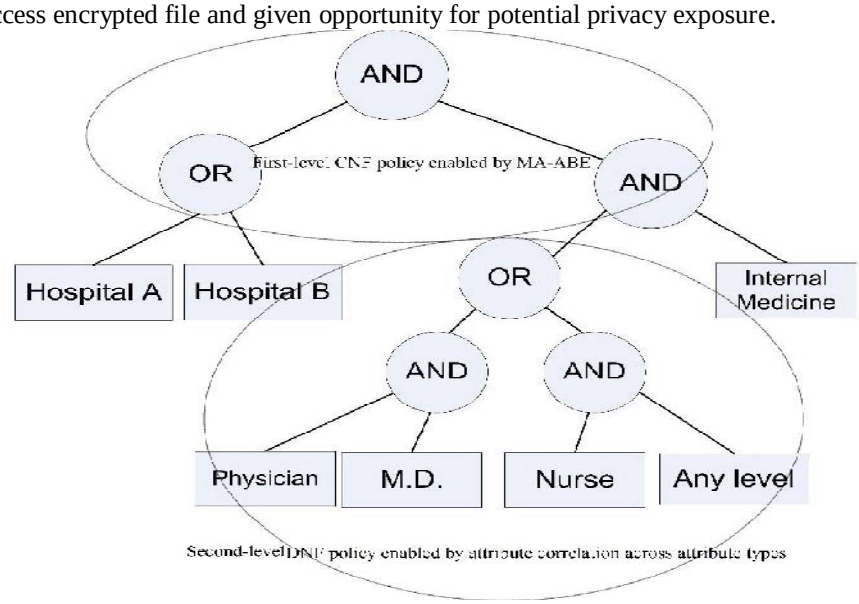

Fig. 1 **ABE Based Access Control**

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

2.2 Revocable ABE

Traditionally, by using broadcasting periodic key update information and re invoke user's [13], it is challenging problem to revoke users/ attributes efficiently and on-demand in ABE. Which is not achieve both side's security and it was not efficient.

III. PROPOSED SYSTEM

In our studies, there are multiple SDs, multiple AAs, multiple owners, and multiple users. In addition, two ABE systems are involved: We term the users having read and write access as data readers and contributors, respectively.

A. ***System setup and key distribution***

The system define similar and common attributes which include in PSD like Patient Profile, Previous medical history, disease history, patients allergies, medicines, prescription. An emergency attribute is also defined for break-glass access.

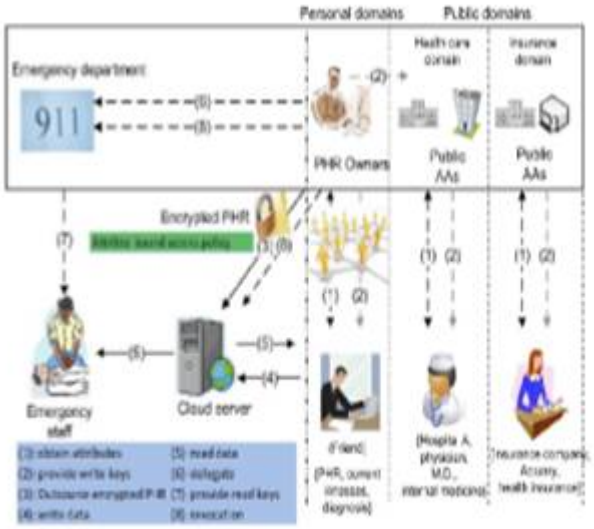

Fig. 2 System Architecture

There are two ways for distributing secret keys. When user can used PHR service first time user can stored some access privileges in his own PSD. After his application generated and the user can distributed corresponds key, in a way resembling invitation on GoogleDoc. Secondly by sending request user can obtain secret key in PSD. The owner will grant her a subset of requested data types. In addition, the AAs distribute write keys that permit contributors in their PUD to write to some patients' PHR (2).

B.PHR encryption and access

The owners upload ABE- encrypted PHR files to the server (3). Each owner can encrypted his own data and stored in PHR under role based access policy to access each user from the PSD. As using secret key user can access encrypted data. This secret key will be send on users email id. Only authorized users can decrypt the PHR files, excluding the server. For improving efficiency, the data attributes will include all the intermediate file types from a leaf node to the root. For

C.User revocation

Here, we consider revocation of a data reader or her attributes/access privileges. There are several possible cases:

1. Revocation of one or more role attributes of a public domain user; 2. Revocation of a public domain user which is aquiver- lent to revoking all of that user's attributes. These can be initiated through the PHR owner's client application in a similar way.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

IV. EXPERIMENTAL RESULTS

Fig.3 PHR Registration

Owner can register his details in PHR.

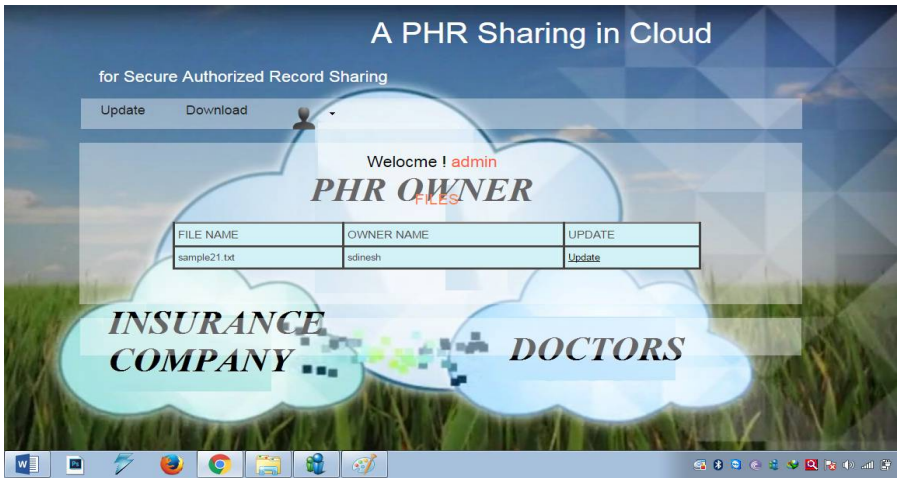

Fig.4 PHR File Update

Owner login in to PHR for upload the data.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Fig.5 Upload Data

To share the data in PHR owner can upload history.

Fig.6 File Upload By PHR owner

Owner can upload file to the cloud.

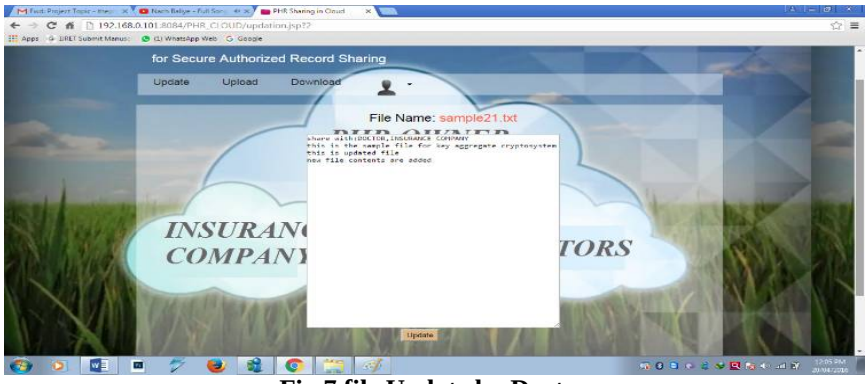

Fig.7 file Update by Doctor

Doctor or PHR owner can update the file present on the cloud.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

V. CONCLUSION

In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing. 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. Through implementation and simulation, 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. H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10),pp. 220-229, 2010.
3. M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.
4. "The Health Insurance Portability and Accountability Act,"http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp, 2012.
5. "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.
6. "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded," http://articles.latimes.com/2006/jun/26/health/ he-privacy26, 2006.
7. K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287, Feb. 2001.
8. 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.
9. 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.
10. C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.
11. 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.
12. M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 1, pp. 51-58, Feb. 2010.
13. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.
14. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes," 2009.
15. 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