FINE-GRAINED ACCESS OF PERSONAL HEALTH RECORD IN CLOUD COMPUTING

A. V. K Shanthi
Faculty of Computing, Sathyabama University, Chennai, India
E-Mail:avks15@gmail.com

ABSTRACT

Cloud computing is used broadly in various services which maintain Personal Health Record (PHR). It is an emerging Health-centric model of patient health information interchange. Personal Health Record (PHR) information can be stored in a third party server i.e.Cloud server. The most important issues are fine–grained access, cryptographically enforced data access control, scalability in key management and efficient on-demand user revocation. We need to provide the security for the cloud based PHR information. This paper mainly concentrates on the multiple data owner scenario and divides the user into multiple security domains that significantly reduces the key management problems. A high level security of patient privacy is improved simultaneously by developing Multi-Authority Attribute Based Encryption (MA-ABE). We have a tendency to enhance the already existing format of PHR knowledge (template) into a secure format (PDF), GIF, DOC and set access privileges. Before taking a key to decrypt the PHR record in multiple owner scenarios it should raise some security questions on PHR owner.

Keywords: cloud computing,fine-grained access control, public health record system, attribute based encryption, multi-authority attribute based encryption.

1. INTRODUCTION

Personal health record (PHR) is a cloud based Health-centric model of health information exchange. A PHR service allows each patient uniquely to create, edit/update, and set access privileges on our Personal Health Data in cloud, which has made the storage, retrieval, and sharing of PHR information is more secured. Each patient is having the full access privileges of our Personal Health Data and can share our health information with a wide range of users in public and personal domains. A feasible and hopeful approach would be encrypting the PHR file before sharing in cloud. Using ABE, access policies are stated based on the attributes of users or data, which permits a patient to share our own PHR among a set of users by encrypting the file by using AES file encryption under a set of attributes. The complexities per encryption, key generation and decryption are linear with the number of attributes involved. We proposed a new techniques MA ABE-based framework for Patient Health-centric model of secure sharing of PHR information in cloud computing environments, under the multiple-owner scenario. Furthermore, we enhance the already existing format of PHR data (template) into a secure format (PDF), GIF, DOC and set access privileges. Before fetching a key to encrypt the PHR record in multiple owner scenarios it may ask some security questions about PHR owner. We also improve our scheme to several issues in previous ones on demand user revocation, scalability and security.

2. FRAMEWORK FOR SECURE SHARING OF PERSONAL HEALTH RECORD IN CLOUD COMPUTING

In this section, we describe existing approach issues and the novel patient centric model for secure sharing of personal health records in cloud computing we summarized below.

2.1 Issues in existing approach

Due to the high cost of developing and maintaining the data centers in cloud, Many PHR services are outdated to or provided by third-party service providers. There are some privacy risks which are slowing down in cloud system. The main aim is about the patients could not have full control over her sensitive personal health information (PHI), especially when they are stored on a third-party server. The personal health information has been already stored in a template format. These format creates security issues (i.e) the unauthorized users can easily modified the PHR information in cloud. To overcome these issues to enhance the already existing format of PHR data (template) into a secure format (PDF), GIF, DOC and set access privileges. To encrypt the PHR record in multiple owner scenarios it may ask some security questions. If the security questions matched then only get the PHR information in cloud server.

2.2 Overview of framework

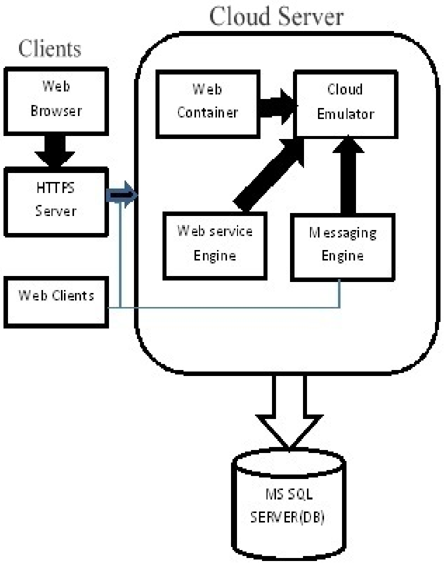


Figure-1. The framework for client machine and cloud server.

3. RELATED WORK

This paper is mostly related to works in analysis of fine-grained access, cryptographically enforced data access control, scalability in key management and efficient user revocation for outsourced data by using the Encryption techniques Attribute Based Encryption(ABE) and Multi Authority-ABE.To improve the scalability of PHR system, ABE encryption techniques can be used. This paper mainly focused on multiple data owner scenario, and divides the user's data in the PHR system into multiple security domains that prominently reduces the key management complexity for owners and users. In Goyal*et al*.'s seminal paper on ABE [11], data are encrypted under a set of attributes so that multiple users who possess proper public keys can decrypt the PHR data. This file encryption scheme and key management more efficient [12].

3.1 Attribute based encryption

Attribute based encryption algorithm equally challenging and also many researches involve to achieving security problems in cloud data. Following Analysis are based work evolved under attribute based encryption (ABE) algorithm.

Attribute Based Encryption is the technique which is used to resolve the security issues. The initial concept of the Attribute Based Encryption is keys of users and the cipher text are combined with the groups of attributes and using particular exact key only to decrypt the uploaded data. So there is the match between the cipher text and private key as well as attributes. In later years the Attribute Based Encryption is based on multiple data approaches, i.e. for specific information for large numbers of users, the encryption schemes are developed.

4. PROPOSED SYSTEM

In this paper, we propose a unique authentication on PHR data and File encryption technique using AES Public key algorithm. The PHR owner should decide how to encrypt the file and to allow which set of users to obtain access to each file.

4.1 Multi-Authority Attribute Based Encryption (MA-ABE)

The multi-authority attribute based encryption scheme is an novel attribute based encryption in which it will have many attribute authority for handling the different set of users from various domains [6]. In the PHR system the users will be from different domain like public and personal domains. So each user will be having different access privileges based on the relation with the PHR owner. Thus the MA-ABE scheme will significantly reduce the key-management issues and overhead and thus it will provide fine-grained access control to the system. The MA-ABE scheme will run the attribute key generation algorithm, and return the public key and private key to the user. In order to decrypt PHR information encrypted with a set of attributes for each attribute authority, a user must have received from each attribute authority policy which allows decryption for that set of encrypted data (attributes) [15]. The main challenge in MA-ABE is to guarantee that two colluding users cannot each obtain keys from a different authority, and then pool their keys to decrypt a message that they are not entitled to.

4.2 The attribute hierarchy

We are using Multi- attribute based encryption for providing security.

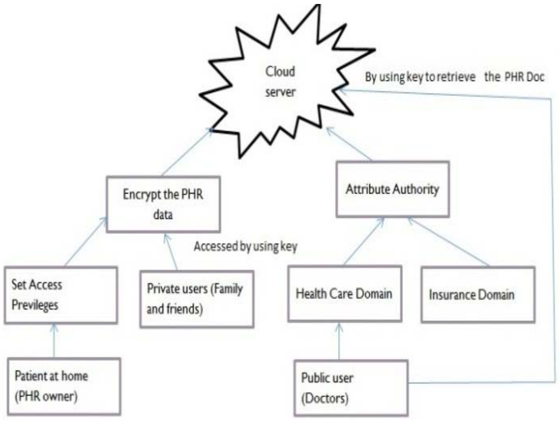


Figure-2. Architecture diagram for encrypting data in cloud server.

4.3 System architecture

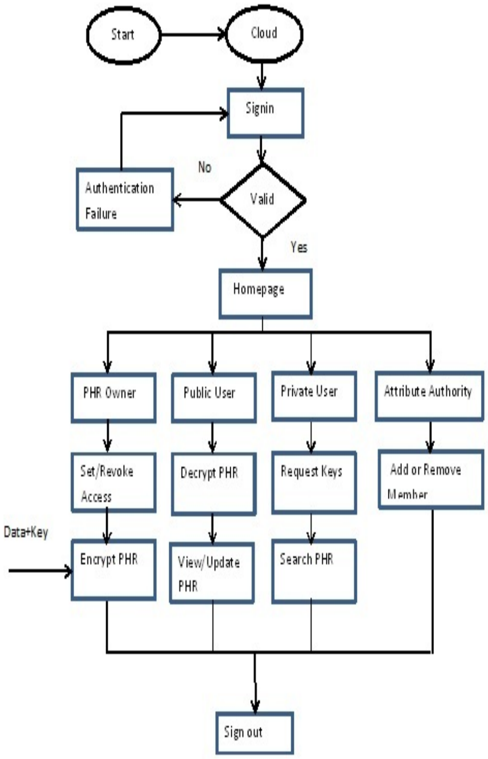
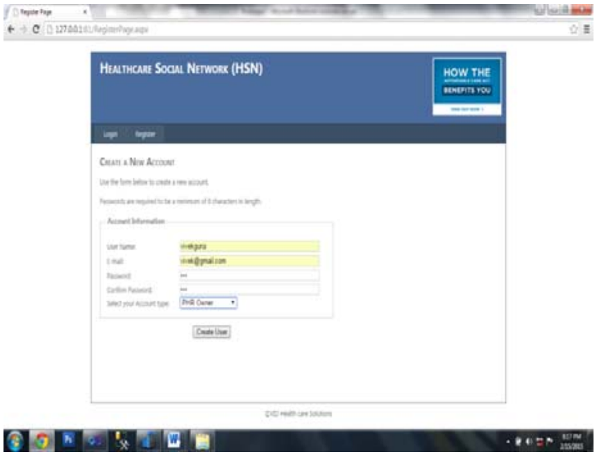


Figure-3. System flow diagram.

5. METHODOLOGIES

5.1 Profile development

The Core Development is responsible for Register PHR owners and PHR users and theirs Login processes. It is also responsible for Profile maintenance of PHR owners and PHR users.


Register Page
127.0.0.1:81/RegisterPage.aspx
Healthcare Social Network (HSN)
HOW THE
BENEFITS YOU
Login
Register

Create a New Account

Use the form below to create a new account.

Passwords are required to be a minimum of 6 characters in length.

Account Information

User Name: vivekguru

E-mail: vivek@gmail.com

Password: ***

Confirm Password: ***

Select your Account type: PHR Owner

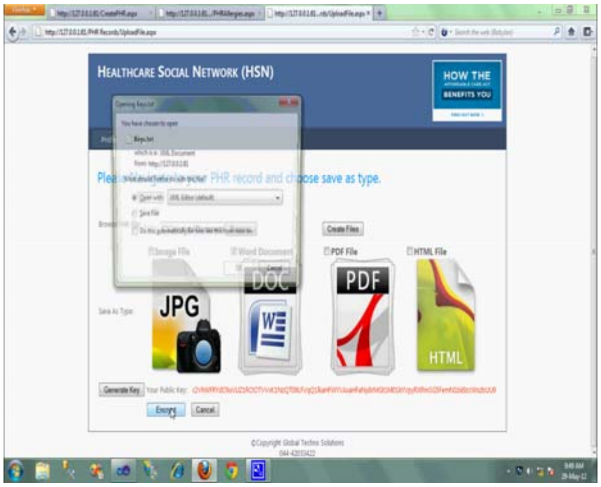
Create User

©XD Health care Solutions

Figure-4. PHRProfile creation.

5.2 PHR Manipulation

In this module the PHR owner should decide how to encrypt her files and to allow which set of users to obtain access to each file.



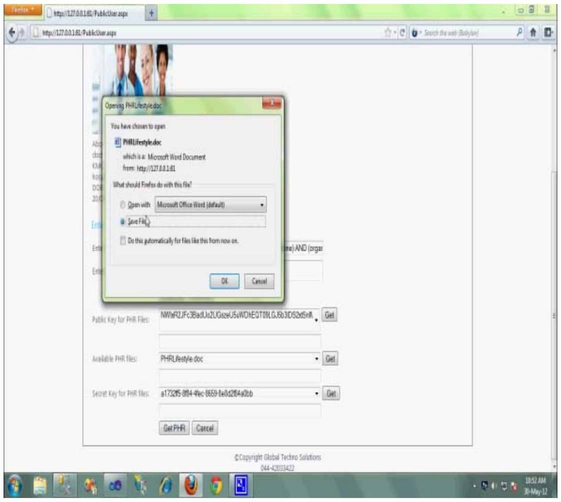
Please ... PHR record and choose save as type.

©Copyright Global Techno Solutions
044-42033422

Figure-5. Creating and encrypting PHR data.

5.3 MA Implementation

In the public domain, we use multi-authority ABE (MA-ABE) to improve the security and avoid key problem.



Opening PHRLifestyle.doc

You have chosen to open

PHRLifestyle.doc

which is a: Microsoft Word Document

from: http://127.0.0.1:81

What should Firefox do with this file?

○ Open with Microsoft Office Word (default)

● Save File

☐ Do this automatically for files like this from now on.

Public Key for PHR Files: NWtxR2JFc3BadUo2UGszeU5uWDhEQT09LGJ6b3lDS2xt5nR

Available PHR files: PHRLifestyle.doc

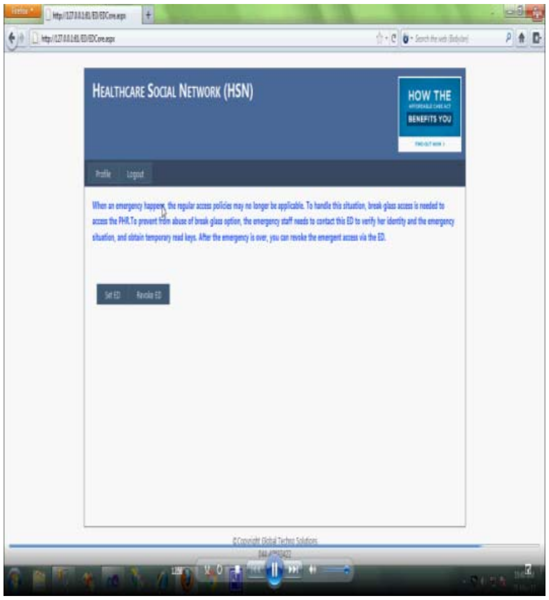
Secret Key for PHR files: a1732ff5-8f84-4fec-8659-8e8d2f84a0bb

©Copyright Global Techno Solutions
044-42033422

Figure-6. Request keys and get PHR information.

5.4 ED Implementation

The Emergency Department(ED) responsible for provide break-glass key, for access PHER file due to the emergency. The emergency key set by the PHR owner while encrypting the PHR file.


Healthcare Social Network (HSN)
HOW THE AFFORDABLE CARE ACT BENEFITS YOU
Profile
Logout
Set ED
Revoke ED

When an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break glass access is needed to access the PHR.To prevent from abuse of break glass option, the emergency staff needs to contact this ED to verify her identity and the emergency situation, and obtain temporary read keys. After the emergency is over, you can revoke the emergent access via the ED.

Figure-7. Creating emergency record.

Access structure revoked successfully

Figure-8. On-Demand user revocation.

6. CONCLUSIONS

The Personal Health Record system needs high level security against unauthorized users. This paper proposed the PHR data with more security function using Multi Authority Attribute Based Encryption which plays an important role because these are unique and not easily hackable. To overcome the issues like key management, on Demand user Revocation problem by using Multi Authority Attribute Based Encryption and also enhance privacy guarantee. A future plan is to design a security model using the ABBE encryption scheme for secure sharing of PHR data in Cloud Computing.

REFERENCES

[1] S. Yu, C. Wang, K. Ren and W. Lou. 2010. Achieving Secure, Scalable and Fine-Grained Data Access Control in Cloud Computing. Proc. IEEE INFOCOM ’10.

[2] M. Li, W. Lou, K. Ren. 2010. Data security and privacy in wireless body area networks. IEEE Wireless Communications Magazine.

[3] M. Li, S. Yu, K. Ren, and W. Lou. 2010. Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings. Proc. Sixth Int’lICST Conf. Security and Privacy in Comm. Networks (SecureComm ’10). pp. 89-106.

[4] V. Goyal, O. Pandey, A. Sahai and B. Waters. 2006. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. Proc. 13thACM Conf. Computer and Comm. Security (CCS ’06). pp. 89-98.

[5] [5] Ming Li,Shucheng Yu, Yao Zheng,KuiRen, and Wenjing Lou.2013. 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.

[6] Chernicoff, David. 2011. HP VDI Moves to Center Stage. ZDNet.

[7] S.Yu,C.Wang,K.Ren and W. Lou. 2010. Attribute Based Data Sharing with Attribute Revocation. Proc. Fifth ACMSymp. Information, Computer and Comm. Security (ASIACCS ’10).

[8] X. Liang, R. Lu, X. Lin and X.S. Shen. 2010. Cipher text Policy Attribute Based Encryption with Efficient Revocation. Technical report, Univ. of Waterloo.

[9] J. Hur and D.K. Noh. 2011. Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems. IEEE Trans. Parallel an distributed Systems. 22(7): 1214-1221.

[10] N. Attrapadung and H. Imai. 2009. Conjunctive Broadcast and Attribute-Based Encryption. Proc. Third Int’l Conf. Palo Alto on Pairing-Based Cryptography-Pairing. pp. 248-265.

[11] Jin Sun, Yupu Hu and LeyouZhang. 2013. A Key-Policy Attribute-Based Broadcast Encryption. The

International Arab Journal of information Technology. 10(5).

[12] D. Boneh, C. Gentry and B. Waters. 2005. Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys.In: Proceedings of the 25th Annual International Cryptology Conference, USA. pp. 258-275.

[13] L. Zhang, Y. Hu and N. Mu. 2009. Identity-Based Broadcast Encryption Protocol for Ad-hoc Networks. In: Proceedings of the 9thInternational Conference for Young Computer Scientists, Hunan. pp. 1619-1623.

[14] P. McDaniel, M. Pirretti, P. Traynorand B. Waters. 2010. Secure Attribute-Based Systems. J. Computer Security. 18(5): 799-837.

[15] Melissa Chase. 2007. Multi-authority Attribute Based Encryption. In TCC, volume 4392 of LNCS, Springer. pp. 515-534.