A Healthcare Data Encryption for Scalable and Secure Sharing of Personal Health Records in Cloud Computing

1 R.Arivoli , 2 Dr.S.THIRUNIRAI SENTHIL 3 T.SILAMBARASAN

1&3 PG Scholars of Computer Engineering Department

2 PROF OF CSE, PRIST UNIVERSITY

Prist University, Pondicherry Campus

ABSTRACT

This paper presents the design and implementation of Personal Health Records and providing security to patients using Healthcare Data Encryption while they are stored at third party such as cloud. Personal Health Record is web based application that allows people to access and coordinates their lifelong health information. The patient has control over access to their own PHR. To achieve security of personal health records we use the healthcare data encryption to encrypt the data before outsourcing it. Here we focus on multiple types of PHR owner scenario and division of personal health records users into multiple security domains which reduce key management complexity for owners and users. A high degree of patient's privacy is guaranteed. Our scheme gives personal health record owner full control of his/her data. Extensive security and performance analysis shows that the proposed scheme is highly efficient.

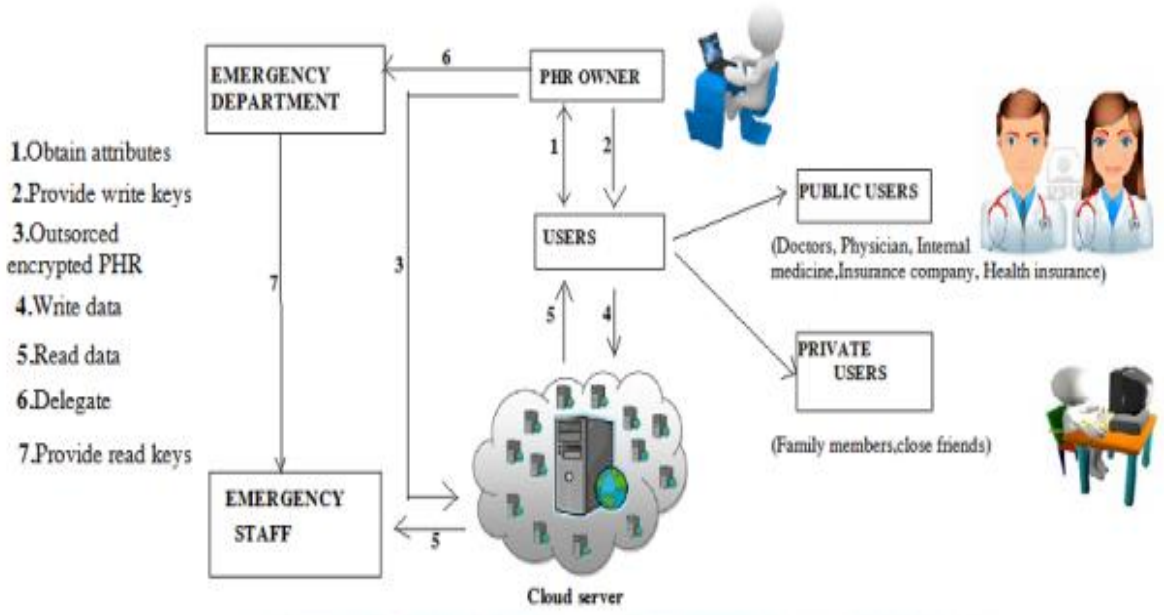
I. INTRODUCTION

Personal Health Record (PHR) concept has emerged in recent years. We can say that it is a patient centric model as overall control of patients data is with patient. He/she can create, delete, modify and share his PHR through the web. Due to the high cost of building and maintaining data centers, third-party service providers provide PHR service.

But while using third party service providers there are many security and privacy risks for PHR. The main concern is whether the PHR owner actually gets full control of his data or not, especially when it is stored at third party servers which is not fully trusted. To ensure patient-

centric privacy control over their own PHRs, it is essential to provide data access control mechanisms. On the onehand, although there exist healthcare regulations suchas HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. On the other hand, due to the highvalue of the sensitive personal health information (PHI),the third-party storage servers are often the targets ofvarious malicious behaviors which may lead to exposureof the PHI.

Our approach is to encrypt the data before outsourcing. PHR owner will decide which users will get access to which data in his PHR record. A PHR file should available to only those users who are given corresponding decryption key. And the patient shall retain the right to revoke the access privileges whenever they feel it is necessary. The authorized users may either need to access the PHR for personal use or professional purposes. We divide types of users into two domains, personal domain and public domain. To protect personal health data stored on semi-trusted servers, we adopt attribute-based encryption as main encryption primitive. Using Healthcare Data Encryption, access policies are expressed based on attributes of users or data.
Our scheme gives personal health record owner full control of his/her data. Extensive security and performance analysis shows that the proposed scheme is highly efficient.



2. RELATED WORKS

We begin our work with an over view of data access control for outsource data and attribute based encryption for the high key management we refer the public key encryption (PKE) in the existing systems [5], [8]. For the encryption of a set of attributes we have reference in Goyalet.al's seminal paper [7].

J. Benaloh, [8] has proposed a scheme in which a file can be uploaded without key distribution and it is highly efficient. This is a single data owner scenario and thus it is not easy to add categories. C. Dong, [10] has explored that the data encryption scheme does not require a trusted data server. The server can perform encrypted searches and updates on encrypted data without knowing the plaintext or the decryption keys. But in this scheme the server knows the access pattern of the users which allows it to infer some information about the queries. To realize fine grained access control, the traditional public key encryption based schemes [8], [10] either incur high key management overhead, or require encrypting multiple copies of a file using different users' keys. To improve upon the scalability of the said solutions, one-to-many encryption methods such as attribute based encryption (HDE) can be used. In Goyal et. al's paper [11] , data is encrypted under a set of attributes so that multiple users who possess proper key can decrypt.

2.2 Disadvantages in Existing System

(1) There is no policy management for file access, so that unauthorized users can also able to access the sensitive data.

(2) There is no encryption and decryption concept, the files stored in the semi-trusted cloud can able to leak the information to others.

(3) There is no structured way to access the file for personal & professional purpose.

3. THE PROPOSED FRAMEWORK FOR ATTRIBUTE BASED ENCRYPTION IN PUBLIC HEALTH RECORDS (PHR)

HDE for Fine-grained Data Access Control

In this HDE to realize fine-grained access control for outsourced data especially, there has been an increasing interest in applying HD to secure electronic healthcare records (EHRs). An attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-HDE that allows direct revocation. However, the cipher text

length grows linearly with the number of unrevoked users. In a variant of HDE that allows delegation of access rights is proposed for encrypted EHRs applied cipher text policy HDE (CP-HDE) to manage the sharing of PHRs, and introduced the concept of social/professional domains investigated using HDE to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline.

3.2 Setup and Key Distribution

In this the system first defines a common universe of data attributes shared by every PSD, such as “basic profile”, “medical history”, “allergies”, and “prescriptions”. An emergency attribute is also defined for break-glass access.

Each PHR owner’s client application generates its corresponding public/master keys. The public keys can be published via user’s profile in an online healthcare social-network (HSN) .There are two ways for distributing secret keys.

First, when first using the PHR service, a PHR owner can specify the access privilege of a data reader in her PSD, and let her application generate and distribute corresponding key to the latter, in a way resembling invitations in GoogleDoc.

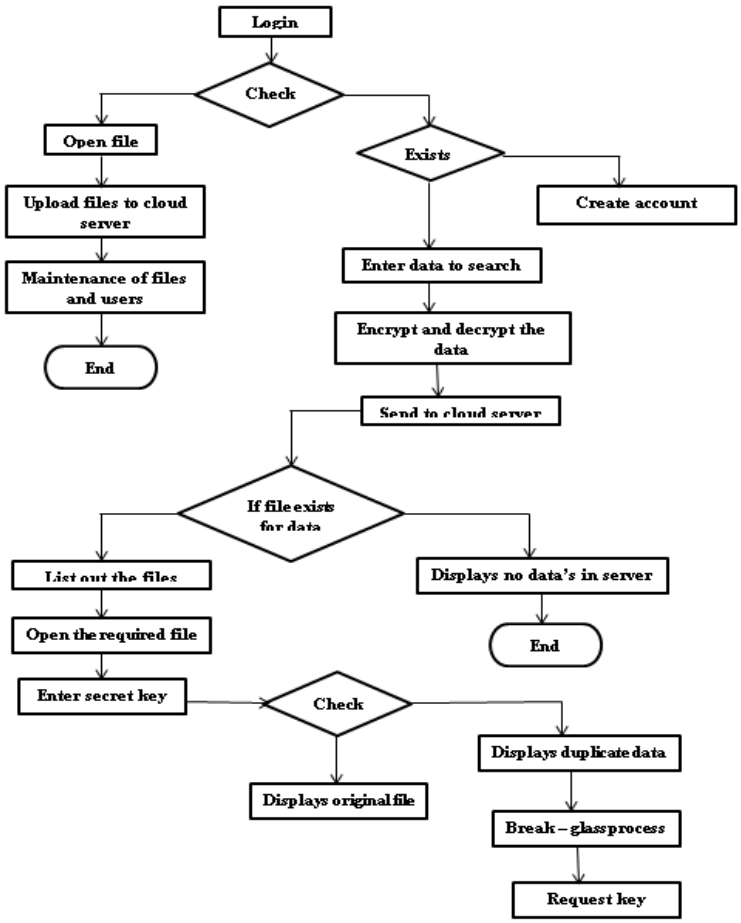
Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access) to the PHR owner via HSN, and the owner will grant her a subset of requested data types. Based on that, the policy engine of the application automatically derives an access structure, and runs keygen of KP-HDE to generate the user secret key that embeds her access structure.

3.3Break-glass

In this module 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 victim’s PHR. In our framework, each owner’s PHR’s access right is also delegated to an emergency department ED to prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED.

4. ENCRYPTION AND DECRYPTION

Encryption is the process in which, a message in its original form (plaintext) is converted (encrypted) into an unintelligible form (cipher text) by a set of procedures known as an encryption algorithm (cipher) and a variable, called a key. The cipher text is transformed (decrypted) back into plaintext using the encryption algorithm and a key. In this scheme, using Data Encryption Standard (DES) algorithm data is encrypted and decrypted. DES is the block cipher, an



System Implementation

Algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string.

In DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is always quoted as such. DES uses the two basic techniques of cryptography - confusion and diffusion. At the simplest level, diffusion is achieved through numerous permutations and confusion is achieved through the XOR operation.

Fig (3) gives the general description of DES encryption algorithm.

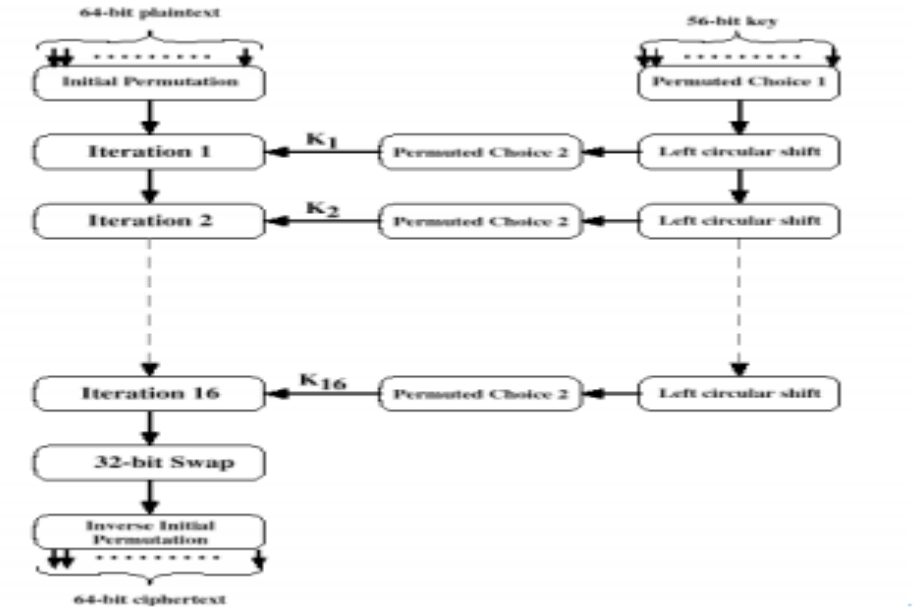


Fig3. General description of DES algorithm

The basic process in enciphering a 64-bit data block and a 56-bit key using the DES consists of:

- An initial permutation (IP)
- 16 rounds of a complex key dependent calculation
- A final permutation, being the inverse of IP.

5. CONCLUSIONS

In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing. 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 HDE 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. Furthermore, we enhance an existing MA-HDE scheme to handle efficient and on-demand user revocation, and prove its security. 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," in *SecureComm'10*, Sept. 2010, pp. 89–106.

[2] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in *Proceedings of the 1st ACM International Health InformaticsSymposium*, ser. IHI '10, 2010, pp. 220–229.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing,"in *ICDCS '11*, Jun. 2011.

[4] "The health insurance portability and accountability act." [Online]. Available: http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp

[5] "Google, microsoft say hipaa stimulus rule doesn't apply to them," http://www.ihealthbeat.org/Articles/2009/4/8/.

[6] "At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded," 2006. [Online]. Available: http://articles.latimes.com/2006/jun/26/health/he-privacy26

[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, p. 283, Feb. 2001.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in *CCSW '09*, 2009, pp. 103–114.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *IEEEINFOCOM'10*, 2010.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in *Journal of ComputerSecurity*, 2010.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *CCS '06*, 2006, pp. 89–98.

[12] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEEWireless Communications Magazine*, Feb. 2010.

[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *ACM CCS*, ser. CCS '08, 2008, pp.
417–426.

[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.