"Patient Centric Frame Work For Data Access Control Using Key Management In Cloud Server"

Gowri. N. Dixit
M.Tech Student, VTU
Computer Networking, EWIT
Bangalore.

Dr. Suresh M B
Head Of The Department,
Department Of ISE, EWIT
Bangalore.

Abstract - Cloud server is an emerging computing paradigm where patient's health information can be stored. Online personal health record (PHR) enables patients to manage their own medical records in a centralized way, which greatly facilitates the storage, access and sharing of personal health data. As more sensitive data is shared and stored on third-party server, so there is wide concern of data security and access control. It is a promising method to encrypt the PHRs before outsourcing, so that patient has control over access to their own PHRs. In this paper, we present a patient-centric model and a set of methodology for data access control to PHRs stored in semi-trusted servers. Attribute based encryption (ABE) techniques to encrypt each patient's PHR file was used to achieve fine-grained and scalable data access control for PHRs. To reduce the key distribution complexity, we divide the system into multiple security domains , where each domain manages only a subset of the users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our proposed scheme is also flexible, in that it supports efficient and on-demand revocation of user access rights, and break-glass access under emergency scenarios.

***Key terms*– Cloud computing, personal health records, fine-grained access control, attribute-based encryption.I. Introduction**

I. Introduction

The demand for outsourcing data storage and management has increased dramatically in the last decade. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. In this model each patient is allowed to control access rights as her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Instead of building and maintaining specialized data centers which cost more, third party servers can be used. Successful examples are Amazon's EC2and S3 [2], Google App Engine [3], and Microsoft Azure [4] which provide users with scalable resources in the pay-as-you use fashion at relatively low prices. One of the biggest challenges raised by data outsourcing is confidentiality. Data confidentiality is not only a privacy issue, but also of juristic concerns. In healthcare application scenarios use and disclosure of protected health information (PHI) should meet the requirements of Health Insurance Portability and Accountability Act (HIPAA) [5], and keeping user data confidential against the storage servers is not just an option, but a requirement. Due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI. To ensure 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.

To deal with the potential risks of privacy exposure, instead of letting the PHR service providers encrypt patients' data, PHR services should give patients (PHR owners) full control over the selective sharing of their own PHR data. To this end, the PHR data should be encrypted in addition to traditional access control mechanisms provided by the server [4]. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing PHRs in cloud computing have been proposed. While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption.

The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the one hand, although there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates. Cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI. A feasible and promising approach would be to encrypt the data before outsourcing. Basically, the PHR Owner herself should decide how to encrypt her files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary.

Disadvantage in Existing System

- There is no policy management for file access, so that unauthorized users can also able to access the sensitive data.
- There is no encryption decryption concept the files stored in the semi-trusted cloud can able to leak the information to others.
- There is no structured way to access the file for personal & professional purpose.

II. Related Work

This paper is mostly related to works in cryptograph ically enforced access control for outsourced data and attribute based encryption. In this paper, we endeavor to study the patient centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key 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. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date. To this end, we make the following main contributions:

- We propose a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains. In particular, the majority professional users are managed distributive by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain.
- In the public domain, we use multi-authority ABE (MA-ABE) to improve the security and avoid key escrow problem. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system. We propose mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes.

A. Objective

The goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either need to access the PHR for personal use or professional purposes. Examples of the former are family member and friends, while the latter can be medical doctors, pharmacists, and researchers, etc. We refer to the two categories of users as personal and professional users, respectively.

B. Advantage in Proposed System

- There is policy management for file access, data access member can able to access the files which they have rights set by the policy.
- Files stored in the semi-trusted cloud are in encrypted form and there is no chance of others to view the file content.
- There is a structured way to access the file for personal & professional purpose through attribute policies and attribute based encryption and decryption.

III. PROPOSED ALGORITHM

A. Problem statement

Our main design goal is to help the data owner achieve fine-grained access control on files stored by Cloud Servers. Specifically, we want to enable the data owner to enforce a unique access structure on each user, which precisely designates the set of files that the user is allowed to access. We also want to prevent Cloud Servers from being able to learn both the data file contents and user access privilege information.

B. Architecture of the Proposed System

The proposed framework for patient-centric, secure and scalable PHR sharing on semi-trusted storage under multi-owner settings. Proposed system's working is based on the below architecture. Here it consists of cloud server for storage, application server where actually the PHR system resides and user access the system through internet. Here data access members may be from public domain or from personal domain, so both domain data access members can access related data from cloud server through internet

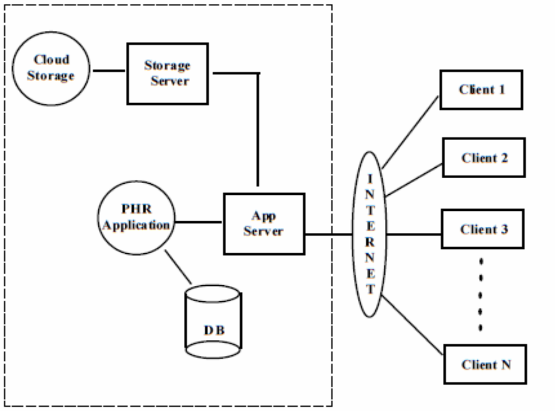

Fig 1 Architecture of patient centric framework

C. Proposed framework

Below figure shows the PHR framework, there are multiple sub domains, multiple owners, multiple attribute authority, and multiple users. The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains (PUDs) and personal domains (PSDs)) according to the different users' data access requirements. Users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner

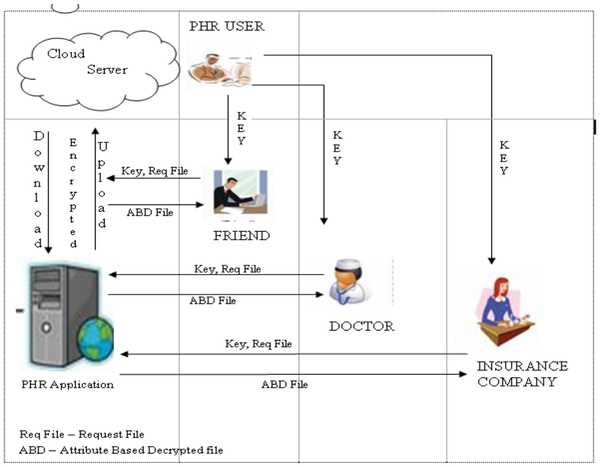

Fig 2 Framework of patient centric model

In cloud Environment PHR Owners need upload data on cloud in such a manner that confidentiality of data and access rights of the data in highest point. Before uploading the file to cloud it should be encrypted and while downloading also it has to decrypted in the application where PHR application is running. This system has three types of users Admin, PHR Owner & Data Access Member. Sample files, attributes types and access policy table of the system are shown below.

Sample Files used in this system

- Personal File
- Medical History
- Current Medical Examination
- Insurance Details
- Sensitive Details

Attribute Types in this System

- Friends
- Hospitals
- Insurance
- Emergency

Table 1
Access Policy Table

Files / Attribute	Friends	Hospitals	Insurance	Emergency
Personal	Yes	No	No	Yes
Medical_History	Yes	Yes	No	Yes
Current_Exams	No	Yes	Yes	Yes
Insurance	No	Yes	Yes	Yes
Sensitive	No	No	No	Yes

Admin sets up policy management by creating access policy table, where he categories different user and also files of the PHR owners. Based on access rights various user can access various files according to there rights.

D. *Key Generation*

Here admin generates key using various attribute and PHR owner distributes the key to the data access members, using this key they access the data. Key is generated using above attributes and the password of the user profiles, by XORing above attributes the admin generates secret key and the PHR owner forwards the key to various data access members.

Key Generation

1. Generate two large prime numbers, p and q
2. Let $n = pq$
3. Let $m = (p-1)(q-1)$
4. Choose a small number e, coprime to m
5. Find d, such that $de \% m = 1$

Publish e and n as the public key. Keep d and n as the secret key.

Encryption

$C = P^e \% n$

Decryption

$P = C^d \% n$

$x \% y$ means the remainder of x divided by y

This secret key is distributed to the data access members through email address. The email address of the data access members will be known to PHR owners in advance only. Using this secret key data access member can access the files required.

E. *Security issues*

- Data confidentiality. Unauthorized users who do not possess enough attributes satisfying the access policy or do not have proper key access privileges should be prevented from decrypting a PHR document, even under user collusion. Fine-grained access control should be enforced, meaning different users are authorized to read different set of documents.

- Write access control. We shall prevent the unauthorized contributors to gain write-access to owners PHRs, while the legitimate contributors should access the server with accountability.
- The data access policies should be flexible, dynamic changes to the predefined policies shall be allowed, especially the PHRs should be accessible under emergency scenario.
- On-demand revocation. Whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute. This is usually called attribute revocation, and the corresponding security property is forward secrecy. There is also user revocation, where all of a user's access privileges are revoked.

F. Sample Input and Sample Output

When the PHR Owner is uploading a file from his local machine to web server, it has to be redirected to Attribute based Encryption Service which is running in cloud server 1 and Cloud server 1 will encrypt the file and the encrypted file has to send to cloud server 2 using web service concept which will store in cloud server 2.When the Data Access Member is downloading a file from the Cloud server through policy management control, the corresponding file has to fetch from cloud server 2 and it will send to Attribute based decryption service which is running in cloud server 1. Once the file is decrypted it will be downloaded to the user machine.

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 ABE 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.

REFERENCES

[1] Scalable and secure sharing of Personal Health Records in Cloud Computing using Attributebased encryption- Ming Li Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE

[2]H. L öhr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, 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. 201

[4] "The health insurance portability and accountability act."

[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, "Achiev secure, scalable,and fine-grained data access control in cloud computing," in IEEE INFOCOM'10, 2010.

[10]C. Dong, G. Russello, and N. Dulay, "Shared and Searcha encrypted data for untrusted servers," in Journal of Computer Security, 2010.

[11]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," IEEE Wireless communications Magazine, Fe

[13]A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser.CCS'08, 2008b.2010.,