Efficient PHR Sharing using ABE with USB Token

[1]Fathima Jaleel, [2] Meenu RS ,[3] Rithumol R S, [4] Silpha Ann Thomas

Mrs. Lekshmy P.L(Professor)

[1234]B.Tech,Department of Computer Science and Engineering

[1234]LBS Institute of Technology For Women,Trivandrum,Kerala,India

Jubinafathima3@gmail.com,meenurs9428@gmail.com,rithumol394@gmail.com,silphaann@gmail.com

Abstract—Online PHR system enables the user's to share the personal health records via the internet. PHRs grant patients access to a wide range of health information sources. In this system PHR owner is responsible for create, manage and control the personal health data in a centralized place using the web. Due to the high cost of building and maintaining a specialized data centers the PHRs are outsourced to store at a third party such as cloud servers. Cloud computing servers provides the platform for storage of data. The confidentiality of the PHR is the major problem when patients use commercial cloud servers to store their records because it can be view by everyone. The third party servers are semi-trusted servers and hence it is important to provide encryption before outsource the PHR to the third party servers, which ensures the patient's full control over their PHR. The Attribute Based Encryption (ABE) technique is used to encrypt patient's health records and also provides break glass access under emergency scenarios. The security problems of break glass access can be resolved by using hardware token security.

Keywords—Personal health records, attribute based encryption, attribute authority

I. INTRODUCTION

The personal health record (PHR) system is a database of medical data objects and health related data managed by a patient. In this patients can store their health information on certain web servers. A PHR system allows a patient to create, manage and control their personal health data in centralized place through the web [1]. Each patient has full control over their medical records and they can share the health data with a wide range of users including healthcare providers, family members, friends etc. In the past the health care providers (such as family doctor) have stored medical records of their patients on paper locally. For reducing complexity it was replaced with modern technologies by using personal computers. This also reduces the effort and provides more privacy of individual medical records. The cloud computing servers provides platform for storage of data. 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. The confidentiality of the medical records is major problem when patients use commercial cloud servers to store their medical records because it can be view by everyone, to assure the patient's control over access to their own medical records; it is a promising method to encrypt the files before outsourcing. The PHR owner will decide how to encrypt the files and allow which set of users to obtain the access to each file. So that only the authorized users can have access to the PHR. The authorized users may access the PHR for personal use or professional purposes. So here the system is divided into public domain and personal domain. The public domain consists of the users who make access to the PHR according to their roles, such as doctors, nurses and medical researchers. The personal domain consists of the users, they are personally associated with the data owner such as family members, friends etc. In order to protect the personal health data stored on a semi-trusted server Attribute Based Encryption (ABE) is used.

II. RELATED WORK

Traditionally, research on access control in electronic health records (EHRs) often places full trust on the health care providers where the EHR data are often resided in, and the access policies are implemented and enforced by the health providers. However, for personal health records (PHRs) in cloud computing environments, the PHR service providers may not be in the same trust domains with the patients'. Thus patient-centric privacy is hard to guarantee when full trust is placed on the cloud servers, since the patients lose physical control to their sensitive data. For access control of outsourced data, partially trusted servers are often assumed. With cryptographic techniques, the goal is trying to enforce that who has (read) access to which parts of a patient's PHR documents in a fine-grained way.

A. Symmetric key cryptography (SKC) based solutions.

In [6], files in a PHR are organized by hierarchical categories in order to make key distribution more efficient. However, user revocation is not supported. In [9], an owner's data is encrypted block-by-block, and a binary key tree is constructed over the block keys to reduce the number of keys given to each user. The SKC-based solutions have several key limitations. Here the key management overhead is high when there are a large number of users and owners, which is the case in a PHR system.

B. Public key cryptography (PKC) based solutions.

PKC based solutions were proposed due to its ability to separate write and read privileges. Benaloh *et. al.* [6] proposed a scheme based on hierarchical identity based encryption

(HIBE), where each category label is regarded as an identity. However, it still has potentially high key management overhead.

C. Attribute-based encryption (ABE).

The SKC and traditional PKC based solutions all suffer from low scalability in a large PHR system, since file encryption is done in a one-to-one manner, while each PHR may have an unpredictable large number of users. In [10], KP-ABE is used for the encryption. Here cipher texts are labeled with set of attributes and keys are associated with the access structures. In [7], CP-ABE is used. Here each user is associated with a set of attributes and data are encrypted with access structures on attributes. It will resist the collusion attacks. In a multi authority ABE system [8] have many attribute authorities, and many users. So it reduces the key management complexity. In [1] [2], both KP-ABE and MAABE is used for reducing the key management complexity

III. PROBLEM DEFINITION

This paper is mostly related to work in cryptographically enforced access control for outsourced data and attribute based encryption. To improve upon the scalability of the above solutions, one-to-many encryption methods such as ABE can be used. A fundamental property of ABE is preventing against user collusion. However the security of break glass access is very low. Because all the patients emergency key can be stored in a common database controlled by the agent of emergency department. If the emergency key of a patient losses all the data can be accessed. This can be prevented by using a secondary security to the website. Now a day's hacking techniques are improved a lot, so picking image and textual security is not a secure one. So a hardware token security is introduced to increase the security of break glass access module.

IV. ATTRIBUTE BASED ENCRYPTION

The standard encryption/decryption techniques (symmetric and Asymmetric) used for EHR increase the access control and performance overhead. The traditional method of encrypting data has another drawback that data can be selectively shared only at a coarse-grained level [6]. This means that we provide third party with private key and keep public key with authority. Hence, Sanai and Waters in 2005 proposed a system in which data is encrypted at the fine grained level and named it as Attribute Based Encryption (ABE).In ABE a sender can encrypt a message specifying an attribute set and a number ***d***, such that only a recipient with at least ***d*** of the given attributes can decrypt the message [10]. 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. ABE enables a patient to share the encrypted records among the selected users. To handle the key management challenge the users in the system are conceptually divided into two types of domains labeled as public and personal domains [2].Professional users are managed by attribute authority (AA) while personal domain having less numbers of users is governed by owner. This arrangement handles the different types of PHR sharing applications requirement while minimizing the key management overhead for both owners and users in the system. The framework also supports write access control, dynamic policy updates and for emergency scenario a scheme called Break glass access. Further for public domain a multi-authority ABE i.e., (MA-ABE) scheme is used to improve security and to avoid key escrow problem [2]. In MA-ABE a disjoint subset of user role attributes is governed of user role attributes is governed by attribute authority (AA) but none of them alone is able to control the security of the whole system.

In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes. Various attribute encryption techniques are used for fine grained encryption of data and are discussed below.

A. Multi Authority ABE

In a multi-authority ABE system [8] have many attribute authorities, and many users. There are also a set of system wide public parameters available to everyone (either created by a distributed protocol between the authorities). A user can choose to go to an attribute authority, prove that it is entitled to some of the attributes handled by that authority, and request the corresponding decryption keys.

V. RSA ALGORITHM

- Choose two prime numbers p and q.
- Compute $n = p\,q$.
- Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$
- Choose an integer e such that $1 < e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$,e is public key exponent.
- Determine d as $d_{-1} \equiv e \pmod{\varphi(n)}$
- $d\text{-}e \equiv 1 \pmod{\varphi(n)}$
- d is kept as the private key exponent.

• Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice.

$$\mathrm{C} \equiv \mathrm{m}_{\mathrm{e}} \pmod{\mathrm{n}}$$

• Decryption

Alice can recover m from c by using her private key exponent d via computing

$$\mathrm{m} \equiv \mathrm{c}_{\mathrm{d}} \pmod{\mathrm{n}}$$

VI. PROPOSED FRAMEWORK

A Architecture

The Fig.1 shows the proposed system architecture and various modules. In the proposed framework a hardware token security is introduced for handling the emergency department. There are lots of hardware token devices such as RFID, Fingerprint, CD/DVD, USB etc. From this, USB is picked as hardware token because of its simplicity and it is easy to carry. USB token is first introduced at the time of emergency department registration where the USB is plugged, to detect the PNP Device ID using the class code. This ID is submitted along with secret key while submitting the registration form. All Plug and Play devices must contain a Plug and Play device ID in order to allow the operating system to uniquely recognize the device so that it can load the appropriate driver software. USB storage devices, offer many advantages for us. There is some secured data in our software/site which do not want other users to use, without our permission. Therefore, there is a need to secure our application/site with the help of a device like USB.

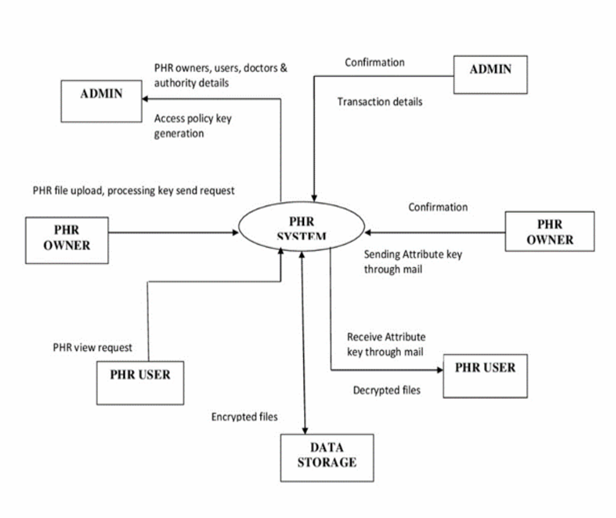
PHR owners, users, doctors & authority details
Confirmation
ADMIN
ADMIN
Transaction details
Access policy key generation
PHR file upload, processing key send request
Confirmation
PHR OWNER
PHR SYSTEM
PHR OWNER
Sending Attribute key through mail
Receive Attribute key through mail
PHR view request
PHR USER
PHR USER
Decrypted files
Encrypted files
DATA STORAGE

Fig .1: System Architecture

B. *Design of modules*

The operations of proposed medical record sharing system combine KP-ABE and Multi-Authority ABE and traditional cryptography, allowing patients to share their medical records. These operations can be classified into following modules:

- System setup
- PHR owner
- Admin
- Search user
- Authority
- Emergency / Break glass Access

VII. FUTURE WORK

In future, to provide high security and privacy for Personal Health Record (PHR), the existing Multi authority attribute based encryption could be further enhanced to proactive Multi authority attribute based encryption. Also when the case of an emergency situation arises, it is possible to implement an identification mechanism to recognize the identity of the victim. A recognition method using fingerprint identification will serve the purpose. For that the fingerprint of individual user has to be recorded at registration and this will help the emergency department handler to access the victim's information quickly.it also discusses how new health information technologies can support richer future health record data and how these records can provide a foundation for current and future applications of computational science approaches, supporting what might be called Computational Health.

VIII. CONCLUSION

The personal health record system allows a patient to create, manage and store the health records in a centralized place through the web. The cloud servers are used to store the large amount of records. The security of the PHR is the major problem while outsourcing the records into the cloud. So the attribute based encryption technique is used for encrypting the records before outsourcing. However the security of the emergency department is much low. It can be resolved by means of a hardware token security such as USB. A number of hardware token devices are available now, from this USB is picked due to the ease of use. So the emergency department is highly secured by means of the USB key.

REFERENCES

[1] M. Li, S. Yu, K. Ren, Y. Zheng and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Us ing Attribute-Based Encryption", *IEEE Trans. Parallel and Distributed Systems*, vol. 24,no.7, January 2013

[2] Ming Li., Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou" Securing personal health records in cl oud computing: Patient-Centric and Fine-Grained Access Control in Multi-Owner Settings" IEEE Trans. Parallel and Distributed Systems,vol.xx,No.xx,2012

[3] J. Hur and D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[4] 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.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010

[6] 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.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker,"Ciphertext-policy attribute-based threshold decryption with delegation and revocation of user attributes," 2009.

[8] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in CCS '09, 2009, pp.121–130.

[9] Wang,W., Li, Z., Owens, R., Bhargava, B.: Secure and efficient access to outsourced data. In: CCSW 2009, pp. 55–66 (2009)

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *CCS '06*, 20