Secure Sharing of PHR Using Attribute-Based Encryption

[1] Shrikanth N G, [2] Navya Ramesh P P

[1] Assistant professor, Department of CSE, Shree Devi Institute of Technology
Kenjar, Mangalore, Karnataka.

[2] M. Tech Student, Department of CSE, Shree Devi Institute of Technology
Kenjar, Mangalore, Karnataka.

Abstract-Personal health record is web based application that allows people to access and co-ordinate their lifelong health information .The patient centric secure sharing of PHR is achieved by storing them in a third party server, such as cloud server. Cloud server provides a promising platform for storage of data. Each patient is promised the full control of his/her medical records and can share his/her health data with a wide range of users, including healthcare providers, family members or friends. The Patient's only decide which set of users can access which set of files .To achieve fine-grained date access control for personal health records, use attribute based encryption to encrypt the data before outsourcing. This paper focuses on the multiple data owner scenario, and divides the users in the PHR system into multiple security domain that greatly reduces the key management complexity for owners and users. For multiple authority based access control mechanism, use Multi Authority Based Encryption (MA-ABE).

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

1. Introduction

A personal health record (PHR) is a collection of information pertinent to a patient's health. It allows a patient to make, handle, and organize his/her personal health data in one place through the web. Patients can control the health information in PHR and can get it anywhere at any time with Internet access. Each patient has assured the full control of his/her personal health records. It is shared with wide range of users, such as healthcare providers, relatives or friends 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 HealthVault.1 Recently, architectures of storing PHRs in cloud computing have been proposed in [2], [3]. 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. 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. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary [7].

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. The latter has potentially large scale; should each owner herself be directly responsible for managing all the professional users, she will easily be overwhelmed by the key management overhead. In addition, since those users 'access requests are generally unpredicted-able; it is difficult for an owner to determine a list of them.

On the other hand, different from the single data owner scenario considered in most of the existing works [8], [9], in a PHR system, there are multiple owners who may encrypt according to their own ways, possibly using different sets of crypto-graphic keys .To protect personal health data stored on semi-trusted servers, we adopt attribute-based encryption as main encryption primitive. Using ABE, access policies are expressed based on attributes of users or data.

Scalability: 'N' number of users can be added into this application.

Security: We are using Attribute Based Encryption for security purpose. The data is encrypted using RSA.

2. Related Work

2.1 Symmetric Key Cryptography (SKC) based Solutions

Vimercati *et.al*. proposed a solution for securing outsourced data on semi-trusted servers based on symmetric key derivation methods [13], which can achieve fine-grained access control. Unfortunately, the complexities of file creation and user grant/revocation operations are linear to the number of authorized users, which is less scalable. In [4], files in a PHR are organized by hierarchical categories in order to make key distribution more efficient. However, user revocation is not supported.

The SKC-based solutions have several key limitations. First, the key management overhead is high when there are a large number of users and owners, which is the case in a PHR system. The key distribution can be very inconvenient when there are multiple owners, since it requires each owner to always be online. Second, user revocation is inefficient, since upon revocation of one user, all the remaining users will be affected and the data need to be re-encrypted. Furthermore, users' write and read rights are not separable.

2.2 Public Key Cryptography (PKC) Based Solutions

PKC based solutions were proposed due to its ability to separate write and read privileges. Benaloh et. al. [4] 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. In order to deal with the multi-user scenarios in encrypted search, Dong et.al. proposed a solution based on proxy encryption [14]. Access control can be enforced if every write and read operation involves a proxy server. However, it does not support fine-grained access control, and is also not collusion-safe 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 an one-to-one manner, while each PHR may have an unpredictable large number of users. To avoid such inconveniences, novel one-to-many encryption methods such as attribute-based encryption can be used [15]. In the seminal paper on ABE [16], data is encrypted to a group of uses characterized by a set of attributes, which potentially makes the key management more efficient. Since then, several works used ABE to realize fine-grained access control for outsourced data [17, 18, 19, 20]. However, they have not addressed the multiple data owner settings, and there lacks a framework for patient-centric access control in multi-owner PHR systems. Note that, in [21] a single authority for all users and patients is adopted. However, this suffers from the key escrow problem, and patients' privacy still cannot be guaranteed since the authority has keys for all owners. CP-ABE is a policy to acquire complex control on encrypted data. This technique is used to keep encrypted data confidential [10]. However, they still assume a single public authority, while the challenging key-management issues remain largely unsolved.

However, there are several common drawbacks of the above works. First, they usually assume the use of a single trusted authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem since the TA can access all the encrypted files, opening the door for potential privacy exposure. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys.

2.3 Cipher Text Policy Attribute Based Encryption (CP-ABE)

CP-ABE is a policy to acquire complex control on encrypted data. This technique is used to keep encrypted data confidential [10]. However, they still assume a single public authority, while the challenging key-management issues remain largely unsolved. However, there are several common drawbacks of the above works. First, they usually assume the use of a single trusted authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem since the TA can access all the encrypted files, opening the door for potential privacy exposure. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys.

2.4 Key-Policy Attribute-based Encryption (KP-ABE)

KP-ABE is a crypto system for fine grained sharing of encrypted data. The key-policy ABE outsourced data in to the cloud [9], [22], where a single data owner can encrypt her data and share with multiple authorized users, by distributing keys to them that contain attribute-based access privileges. They also propose a method for the data owner to revoke a user efficiently by delegating the updates of affected cipher texts and user secret keys to the cloud server. Since the key update operations can be aggregated over time, their scheme achieves low amortized overhead.

3. Framework for Secure and Scalable PHR Sharing

3.1 Requirements

To achieve patient-centric PHR sharing, a core requirement is that each patient can control who are authorized to access to her own PHR documents. Especially revocation is the core security objectives for any electronic health record system, pointed out by Mandl et al. [7] in as early as 2001. The security and performance requirements are summarized as follows:

3.1.1 Data Confidentiality

Unauthorized users (including the server) 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 sets of documents.

3.1.2 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 [23]. There is also user revocation, where all of a user's access privileges are revoked.

3.1.3 Data Access Policies

The data access policies should be flexible, i.e., dynamic changes to the predefined policies shall be allowed, especially the PHRs should be accessible under emergency scenarios.

3.1.4 Scalability, Efficiency and Usability

The PHR system should support users from both the personal domain and public domains. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. Additionally, the owners' efforts in managing users and keys should be minimized to enjoy usability.

3.2 Architecture

Fig.1 depicts the proposed system architecture for secure sharing of personal health record. In this proposed system, the system is divided into two security domains, such as personal domain (PSDs) and public domain (PUDs). The division is carried out according to the user's data access requirements.

The PUDs includes users who make access based on their professional roles, such as doctors, nurses and insurance agents. Users in the personal domain are personally associated with the patient such as family members or friends. Here, the data owner who possess the PHR and data reader who can access the encrypted PHR.

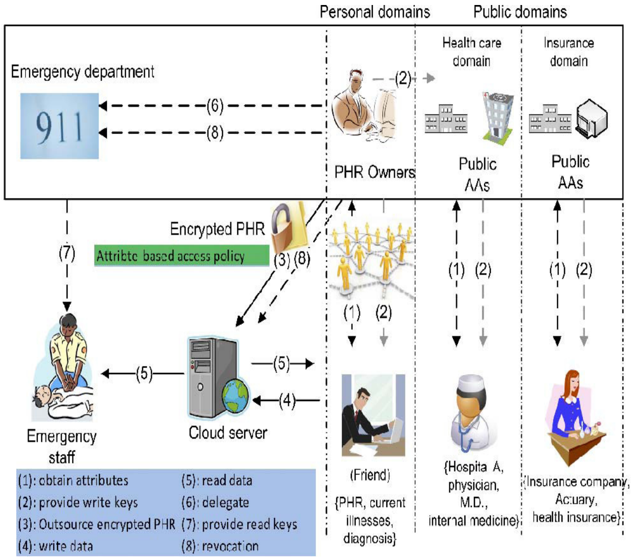

Fig.1. The proposed framework for patient-centric, secure and scalable PHR sharing on semi trusted storage under multiowner settings.

In the PSD, the owner makes use of key-policy attribute based encryption. The owner generates the secret keys for PSD users. The multi-authority attribute based encryption is used in the PUD. Secret keys for PUD users are generated by the attribute authorities depending on their profession.

3.3 Details of the Proposed Framework

In our framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users. In addition, two ABE systems are involved: for each PSD the YWRL's revocable KP-ABE scheme is adopted; for each PUD, our proposed revocable MA-ABE scheme is used.

3.3.1 System Setup and Key Distribution

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).

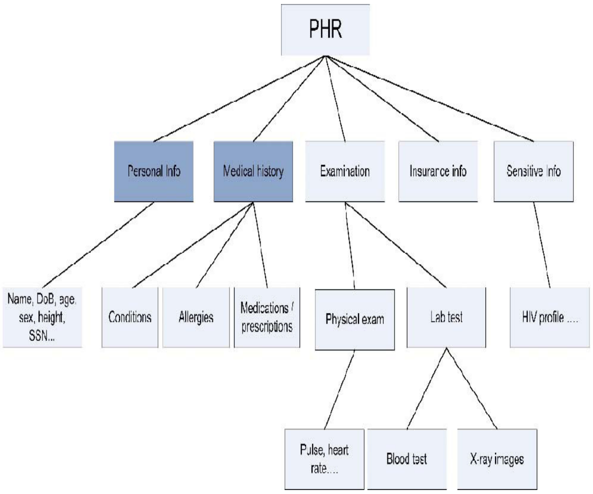

Fig.2. The attribute hierarchy of files—leaf nodes are atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD’s data reader has access to.

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-ABE to generate the user secret key that embeds her access structure. In addition, the data attributes can be organized in a hierarchical manner for efficient policy generation see Fig. 2. When the user is granted all the file types under a category, her access privilege will be represented by that category instead.

3.3.2 PHR Encryption and Access

The owners upload ABE encrypted PHR files to the server [3]. Each owner’s PHR file is encrypted both under a certain fine-grained and role based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the PHR files, excluding the server.

3.3.3 User Revocation

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

I. Revocation of one or more role attributes of a public domain user
II. Revocation of a public domain user which is equivalent to revoking that entire user’s attributes
III. Revocation of a personal domain user’s access privileges
IV. Revocation of a personal domain user.

3.3.4. Policy Updates

A PHR owner can update her sharing policy for an existing PHR document by updating the attributes (or access policy) in the cipher text. The supported operations include add/delete/modify, which can be done by the server on behalf of the user.

3.3.5 Break-glass

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, [24]). 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 [25]. After the emergency is over, the patient can revoke the emergent access via the ED.

4. Advantages and Application of Proposed System

4.1 Advantages

I. Quickly find out information of patient details.

II. In case of emergency doctor and other emergency department quickly get all the details all the informative details and start treatment.
III. If in any condition doctors and medical facilities are not available the PHR owner itself able to take care of his health.
IV. To provide easy and faster access information.
V. To provide user friendly environment.
VI. To provide data confidentiality and write access control.
VII. Reduces the key management complexity for owners and users.

4. 2 Applications

I. Health care website
II. Hospital management
III. Any organization can use this application to store their employees medical information.

5. Conclusion

In this paper, we have designed the proposed framework for the attribute encryption based PHR sharing with authentication. The full control of the personal health record will be always held on the patient and the privacy is assured through the encryption. We use various attribute based encryption techniques to encrypt the PHR files. Thus the patient can allow access to users based on the attributes provided by the patient. The data attributes are defined for personal domain users and role attributes for the users in public domain. The patient can also revoke a user efficiently in this proposed scheme.

Acknowledgments

We would earnestly thank our Supervisor for all his valuable comments and active support.

References

[1] 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

[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] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient controlled encryption: ensuring privacy of electronic medical records,” in CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security, 2009, pp. 103–114.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in IEEE INFOCOM'10, 2010.

[6] 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.

[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. 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.

[9] X. Liang, R. Lu, X. Lin, and X. S. Shen, “Patient self-controllable access policy on phi in ehealthcare systems,” in AHIC 2010, 2010.

[10] J. Bethencourt, A. Sahai, and B. Waters,“Ciphertext-policy attribute-based encryption,” in IEEE S& P ’07, 2007, pp. 321–334.

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

[12] 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. [Online]. Available: http://purl.org/utwente/65471

[13] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, “Overencryption: management of access control evolution on outsourced data,” in VLDB '07, 2007, pp. 123–13

[14] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in CCS '08, 2008, pp. 417–426.

[15] “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.

Shrikanth N G received the BE degree in information Science in 2008 and MTech degree from VTU University in Computer Science and Engineering in 2012.He is an assistant professor in the Department of Computer Science and Engineering at Shree Devi Institute of Technology. His current research interests is on data base and networking.

Navya Ramesh P P received the BE degree in Computer Science and Engineering from Kannur University in 2010. Now she is doing her MTech degree from VTU University in Computer Science and Engineering.