IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Achieving Secure Personal Health Records Using Multiple-Authority Attribute Based Encryption

S.Dharanya[1] ,D.Indira priyadharshini[2] and S.Blessy[3]

[1,2,3]Information Technology, Anand Institute of Higher Technology, Kazhipattur, Chennai

Abstract

The revolution of medical field is sharing secure Personal Health Record(PHR) via the internet. Personal Health Record(PHR) is a health record where health data and information related to the care of a patient is maintained by the patient. The PHR owner outsource the PHR to the third party servers for the wide database management and for the security. 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. In this paper we proposed Attribute Based Encryption(ABE) technique for the personal health records stored in the semi-trusted servers. ABE is used to enable fine-grained and scalable 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. In this way, each patient has full control over her own privacy, and the key management complexity is reduced dramatically.

Keywords: *Personal health record, multiple authority, Attribute authorities, cloud computing, Key management, fine-grained data access control.*

1. Introduction

Personal health record is the record of a patient who can share her medical information with a large number of users. PHR provide the service for the patients to create and manage their records via web. The PHR service outsourced the records to the cloud servers due to the difficulties in cost of building and maintaining the data. The cloud server is an semi-trusted server and hence the PHR owner encrypt the data before outsourcing. The storing of PHR record is proposed in [2], [3]. There is a risk in security and privacy for the PHR services for everyone who uses this service. The sensitive personal health information has the high value and hence the various malicious behaviours also target the third-party storage servers. The people who use the PHR service may not fully trust the third party server. It is important to note that usually cloud providers are not covered entities [4]. To overcome these drawbacks, we proposed an approach to encrypt the data before outsource to the third-party server. The PHR owner can decide about the key distribution. As our main goal is to encrypt the attribute, the PHR owner can set the attributes for the large number of users and the PHR owner can provide the decryption keys for those users. In our work, we use the divide and rule technique for divide the users into personal and professional users. Examples of the personal users can be close friends, family members and the latter can be doctor, insurance company, researchers, etc. In the existing works [5], [6], in a PHR system, there are single data owners and it is difficult to encrypt the data. For the efficient key management, we propose the multiple owners who can encrypt their data according to their own way, using the different sets of cryptographic keys. The user can obtain the keys from the individual PHR owner and they can access the data. But the PHR owners are not always in online, hence there is a limit in the accessibility by the user. Due to the complexities in the key management, central authority is proposed in the existing system but it shows too much trust on a single authority. This may leads to the key escrow problems. For the scalable and secure sharing of PHR stored on semi-trusted servers such as cloud server, we proposed the Attribute Based Encryption (ABE) in this paper. Using this ABE technique we can allocate the attributes for users and under a set of attributes we can encrypt the data. ABE is used to limit the issues in key management, dynamic policy updates, user revocation. We make the following contributions for solve the issues.

1.1 Our contributions in this paper:

We propose the attribute based encryption for secure sharing of PHR in cloud computing. For the key management complexity, we divide the users into personal and professional users. Hence the owner needs to manage the keys for small number of users in his/her personal domain and the majority professional users are managed by attribute authorities (AA). The owner and the user both require the minimal key management only.

We use the multi-authority ABE (MA-ABE) in the public domain to avoid the key escrow problem in the central authority. For the personal users, based on their request the owner distributes the decryption keys. We propose MA-ABE also for the on-demand user revocation scheme.

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].

2.1 Single trusted authority

For the secured sharing of personal health record, the data is stored in cloud server and the key management is provided by the single trusted authority [2], [3]. It not only leads to load bottleneck, but also creates the key escrow problem. As it is a single trusted authority there may be user collision due to the confusion in key distribution. It is not secured to delegate the key management for all attributes to the single trusted authority. There is a need to divide the users into public and professional users based on the divide and rule, for the secure sharing of PHR. Both the user and owner can manage the minimal keys under a set of attributes. For the key management under the set of attributes we propose the Multiple Authority-ABE (MA-ABE).

2.2 Data access control

For outsourcing the data in the cloud server there exist a work to realize data access control for the outsource data [6], [9], [10], [11]. They use the cipher text-ABE (CP-ABE) [12] for the direct revocation and the cipher text length increases with the number of unrevoked users. In the existing system for the secure sharing of PHR they apply CP-ABE technique [13]. But there exists drawbacks such as the use of single trusted authority and lack of on-demand user revocation. In the existing system they provide the time limit for the decryption keys. So it is difficult to access the data for long time with that key and there is a need for re-encryption by providing dummy attributes additionally. To overcome this problem we propose on-demand user revocation by the break-glass access system. For accessing on demand user revocation MA-ABE scheme is used where the user's secret key can be revoked by re-encrypting the cipher text and can be updated efficiently to the server immediately. The AA updates and governs the unrevoked users. The updates can be of this kind 1) the affected attributes of the public key components, 2) the secret key of each unrevoked user corresponding to that attribute, 3) all the cipher texts can be updated by the servers. To reduce the delegation of 2 and 3 operations a proxy encryption can be used and lazy revocation is used to reduce the burden. The unrevoked user's secret key can be updated along with a re-key. The updates of the server must be delegated by using a dummy attributes additionally in the AA. For revoking MA-ABE a minimal subset of attributes is required, without it the user's secret key access structure will not be satisfied.

3. The proposed framework for attribute based encryption in public health records (PHR)

3.1 Patient centric framework

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. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its 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. Which there are multiple "attribute authorities" (AAs), each governing a disjoint subset of attributes. Role attributes are defined for PUDs, representing the professional role or obligations of a PUD user. Users in PUDs obtain their attribute-based secret keys from the AAs, without directly interacting with the owners. To control access from PUD users, owners are free to specify role-based fine-grained access policies for her PHR files, while do not need to know the list of authorized users when doing encryption. Since the PUDs contain the majority of users, it greatly reduces the key management overhead for both the owners and users

3.2 Key distribution- PHR Encryption and 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) (which could be part of the PHR service. 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, Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access), 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, when the user is granted all the file types under a category, her access privilege will be represented by that category instead. The owners upload ABE-encrypted PHR files to the server. 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. For improving efficiency, the

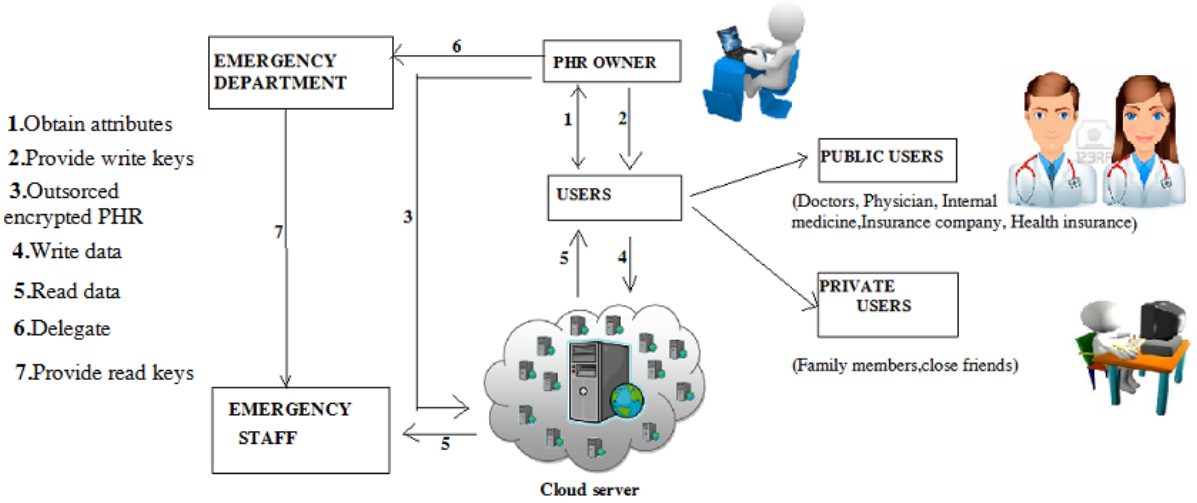

Fig.1.Architecture diagram for personal health record using attribute based encryption

data attributes will include all the intermediate file types from a leaf node to the root. The data readers download PHR files from the server, and they can decrypt the files only if they have suitable attribute based keys. The data contributors will be granted write access to someone's PHR, if they present proper write keys.

3.3 ABE for Fine-grained Data Access Control

In this module ABE to realize fine-grained access control for outsourced data. Especially, there has been an increasing interest in applying ABE 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-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of unrevoked users. In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs applied cipher text policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains investigated using ABE 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.

3.4 Break-glass module

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. Main design issues

This paper is mainly proposed for recover the following issues. The key distribution is obtains by the following key policies.

4.1 Security concern

Data access control is the main challenging issues in cloud computing. We can provide the secure data access control by allowing only authorized users to access the data. For the secure data access control we use the fine-grained data access control which means different types of data can accessible to different types of users. The fine-grained access control also faces the challenges such as user collusion and key abuse. We propose the ABE (one to many encryption) design tool to avoid the collusion resistance and user accountability.

4.2 Key Policy

To prevent users from sharing the illegal key we use two key policies such as cipher text policy ABE (CP-ABE) and key policy ABE (KP-ABE). These two policies are powerful tools for fine-grained access control. The key distribution is based on the hierarchy access structure associated with a set of attributes. The decryption of data requires satisfy the user access structure. In the existing system, the message is encrypted with the CP-W. The sender computes with W||*,
If the key is in following form the sender can decrypt the data.

$$K(A,W) = 1$$

Here A is the attribute key of the user. It is not secure for set the key based on the attribute so we include the id with the attribute this id is based on the category of the users.

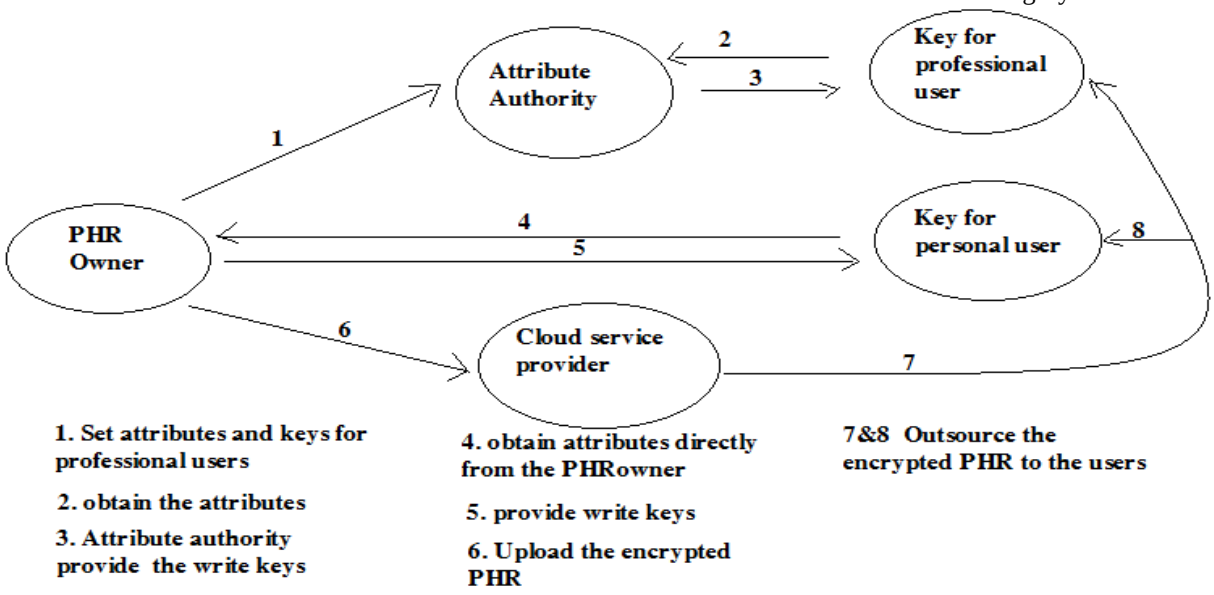

Fig.2.Providing Keys using attribute authority

Table.1.Key encryption

User ID	*Attribute list*	*Key structure*
Personal user PEK	*A=(A1,A2,A3,A4)*	*A||PEK*
Public user PUK	*B=(B1,B2,B3,B4)*	*B||PUK*

The sender computes a ciphertext with policy W‖*, such that any user with attribute list K (A,W)=1 can decrypt, regardless of the identity ID.Assume the personal user's secret key is for A‖PEK, where K (A, W)= 1.The user can only decrypt the ciphertext with attribute private key of A and the secret key of PEK. We propose the key structure using CP-ABE under the set of attribute and id in the following form.

K (A||PEK,W) = 1.

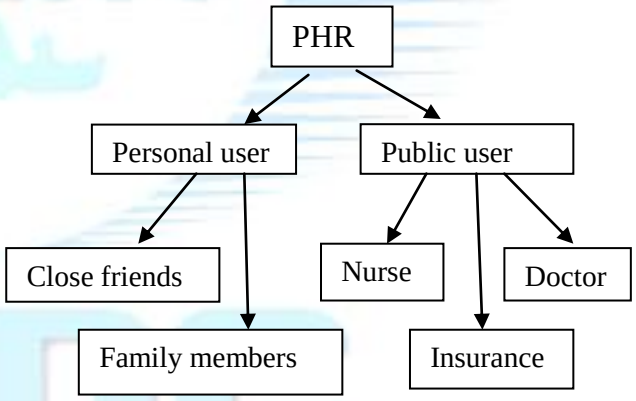

Fig.3.Hierarchy for attribute structure

We can also increase the cipher text length of our secret key by using the leaf node to the root scheme from the hierarchy structure of the attributes in the PHR.

We can provide the CP-ABE keys based on the leaf node to root scheme. For example the insurance company has the attribute structure as {PHR, Public user, Insurance company}. If the decrypted key has the same structure the owner can allow them for accessing the data.

5. Multi-Authority ABE

The users in the system are divided into two types of domains namely public and personal domains for addressing the key management. Multi- authority ABE (MA-ABE) is used in the public domain for improving the security and to

avoid key escrow problem .The whole system cannot be governed by the attribute authority(AA), so it is governed by the disjoint subset of role attributes. In the personal domain the personal users can get access from the users directly and the attributes are encrypted in the PHR before the personal users access it.For further security we use MA-ABE on demand of the users in a revocation scheme.Now the users have privacy over their PHR records.Our usage of MA-ABE is extended in public domain than personal domain.Using this revocable scheme we can provide a security proof for the PHR record.

6. Advantages

6.1 Security

Without the user providing secret key no one can access the user's profile. Only the members of the personal and public domain can access the record, even the members cannot get the whole access of writing or reading.It is up-to the owner's wish of providing read or write access to the users.The data's are highly secured by using ABE, as the information is encrypted before outsourcing it to others. To decrypt the information we need a secret key.

6.2 Storage

The whole information is stored in the server. The requested attributes are encrypted and are then stored in the cloud server. For the purpose of memory allocation the records are divided into attributes which saves memory space. The encrypted data is stored in the cloud server for the purpose of better output.

6.3 Portability

The users or the members of the PUD or PSD can access the information from anywhere and anytime as the encrypted data's are stored in the cloud server. It reduces the cost for accessing the information as it can be accessed from anywhere and anytime.

7. Conclusion

In this paper, our main goal is to provide a secure service in the medical field. For this secure service, we proposed the separation of users as personal and public users which makes the key management and security an easier task. We provide this service to a third party server to reduce the management risk of the PHR owner. We use multi authority-ABE (MA-ABE) for providing encryption of each attributes for the purpose of secured data access control. As the users are large in number we use fine grained data access control which means different types of users can access with different types of attributes.

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.Lohr, 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.2011.

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

[5] 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.

[6] S.Yu,C.Wang,K.Ren,and W.Lou,"Achievingsecure,scalable,and fine-grained data access control in cloud computing," in IEEE INFOCOM'10,2010.

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

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

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

[10] 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.

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

[12] S.Narayanan,M.Gagne,andR.Safavi-Naini,"Privacy preserving EHR System using attribute-based infrastructure," ser.CCSW '10,2010,pp.47-52.