International Journal of Computer Applications Technology and Research
Volume 4– Issue 1, 58 - 62, 2015, ISSN:- 2319–8656

Secure Sharing of Personal Health Records in Cloud Computing using Encryption

Sabna A B
Department of Computer Science and Engineering
Jyothi Engineering College
Cheruthuruthy, Thrissur, India

Harsha T D
Department of Computer Science and Engineering
Jyothi Engineering College
Cheruthuruthy, Thrissur, India

Abstract: The PHR is a tool that you can use to collect, track and share past and current information about your health or the health of someone in your care. Personal health record (PHR) is considered as an emerging patient-centric model of health information exchange, where people can share their health information to other people. Since there are wide privacy concerns about the health records and due to high operational cost, users stored at a third party server called as Cloud Server. The issues such as risks of privacy exposure, scalability in key management, access problem, user revocation, have remained the most important challenges towards achieving fine-grained, cryptographically enforced data access control. In order to get rid off from this ,in this paper we introduce attribute-based encryption (ABE) techniques to encrypt each patient's PHR file so that an unauthorised people won't be able to view our PHR file.

Keywords: Personal Health Records, Cloud computing, Attribute Based Encryption.

1. INTRODUCTION

Personal Health Record (PHR) is emerged as a patient- centric model of health information exchange. Nowadays most of the users store their health related data in a third parties on the Internet. It allows the patient to create and control his/her medical related data which may be placed in a single place such as information center. Due to the high cost of building of the sensitive personal health information, especially when they are stored at a third-party server which people may not fully trust example, personal email, data, and personal preferences are stored on web portal sites such as Google and Yahoo. So in this paper we use an encryption called Attribute based Encryption so that people will be able encrypt their PHR file from wherever they want to. The main concern is about the privacy of patients, personal health data and to find which user could gain access to the medical records stored in a cloud server.

In ABE [1], the attributes of users or data that selects the access policies enables a patient to share their PHR selectively among a set of users after encrypting the file on the basis of a set of attributes. As a result, the number of attributes involved determines the complexities in encryption, generation of key and decryption. The Multi Authority Attribute Based Encryption (MA ABE) scheme provides multiple authority based access control mechanism in . The PHR owner should decide how to encrypt their files and how to allow the users to obtain access for each file. A PHR file should only be available to the users who are given the corresponding decryption key, which will be confidential to the rest of users.

By using ABE, to address key management challenges, we divide the users into two types of domains; they are public and personal domain. For personal domain, KP-ABE scheme is used. For public domain, MA-ABE scheme is used and the PHR is under control of outsource agent. Here we propose a novel idea which is an enhance MA-ABE so that, the user will have full control on their own PHR.

Furthermore, the patient will always have the right to not only grant, but also revoke access privileges when the patient feel it is necessary. The main goal of patient-centric privacy is conflict with scalability in PHR system. The authorized users may either want to access PHR file for personal use or professional purposes. Implementation of standards for health-care data, accurate patient identification and matching of records, and definition of incentives for accelerated deployment of health information technology.

2. PROBLEM DEFINITION

In Multi Authority –Attribute Based Encryption the existing key is created by outsourced again the data is endangered so that the key control is visited with the outsource agent and it became difficult to manage. Thus the future enhancement to propose a novel idea which is an enhance MA-ABE so that, key will be given by the user.

3. RELATED WORK

In this paper, most of the related works in cryptographic enforced accessing control for the outsourced data and ABE. To realize fine-grained access control, the traditional public key encryption (PKE)-based schemes [10],[8] either need high key management or require encrypting the multiple copies of a file using different users keys. To improve upon the scalability of the above solutions, one-to-many encryption methods such as ABE can be used. In Goyal et al.'s paper on ABE [11], data's are encrypted based on a set of attributes so that multiple users who possess proper keys can decrypt. This will potentially makes encryption and key management more efficient [12].

Fine grained access control systems facilitate granting differential access rights to a set of users and specify the access rights of individual users. Several techniques are known for implementing the grained access control.

They also note how their techniques for resisting collusion attacks are useful in attribute-based encryption. However, the cost of their scheme in terms of computation, private key size, and cipher text size increases exponentially with the number of attributes. We also note that there has been other work that applied IBE techniques to access control.

4. FRAMEWORK

In this paper, the purpose of our framework is to provide security for patient-centric Personal Health Record access and key management in an efficient manner at the same time[14]. If the users attribute is not valid, then the user will be unable to access the future Personal Health Record files using the attributes. The PHR data should support the users from personal domain as well as public domain. The public domain may have more number of users who may be in huge number and unable to predict, so that the system should be highly scalable in terms of the complexity in key management system communication, computation and storage. The owner in managing users and keys should be minimized to enjoy usability Fig-1 By using the ABE, encryption of personal health records self-protective, that is they can access only authorized users on a semi trusted server.

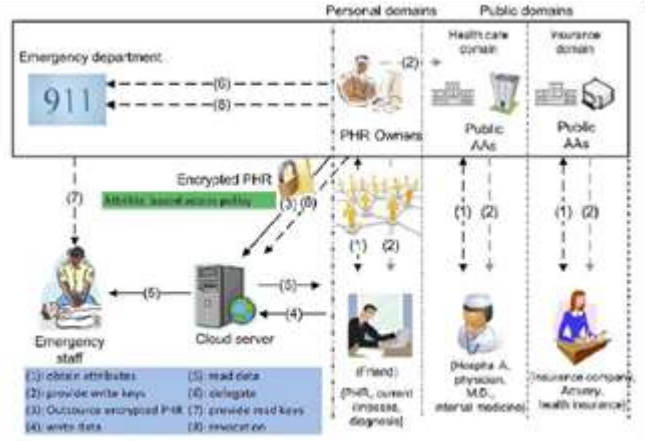

Fig -1: Framework of PHR

5. DESIGN GOALS

In this paper, our main goal is to provide the security for the data files present in the cloud server. Especially we allow each and every data owner to provide the access policy for each data. The users are given with a set of attributes and their corresponding keys. The individual users can only decrypt the files if and only if the corresponding set of attributes matches with the access policy. In addition to that, we handle the users who are revoked. That is users who are unauthorized but once upon a time authorized must not be able to access the data.

In the case of Maintaining Confidentiality, it allows the unauthorized users are not allowed to read data file or modify the data file and thus maintaining the confidentiality of each data file in the cloud server. In Data Access,the data access can be described in two ways[3]. First of all ,any member of the group can access the data present in the cloud. Second, unauthorized and revoked users cannot gain the access to the files of the cloud resources

6. PROPOSED SCHEME

The Personal Health Records are maintained in the data server under the cloud environment. A novel framework for secure and sharing of the personal health records has been proposed in this paper. The Public access and Personal access models are designed with the security and the privacy enabled mechanism Fig-2. The framework addresses the unique challenges brought by the multiple PHR owners and the users, so that the complexity of key management is greatly got reduced. The attribute-based encryption model is enhanced to support the operations with the Multi Authority Attribute Based Encryption. The System will improve its dynamic policy management model. Thus, Personal Health Records are maintained with the security and privacy.

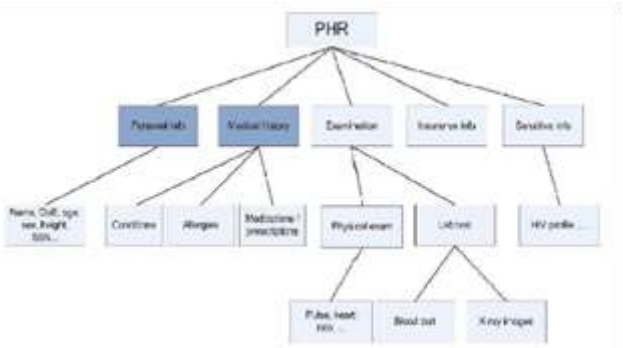

Fig -2: Attribute Hierarchy of files

The solution we propose is based on the following assumptions:

- There is a trusted authority (TA) who generates the keys for the users of the system. There is also a public directory that is used by the TA to publish the system public values (such as public keys) and the parameters that are needed for cryptographic operations.

- A user is associated with a unique identifier (ID), and (ii) a set of attributes (ω). Each user has a public key and a private key. The Private Key is generated and issued by the TA after verification of the user's attributes.

- The health record database is hosted on the cloud storage. The cloud server is trusted for performing the requested operation but will not be able to do other unspecified operations such as reading patients' data. Therefore the health information on the storage must be kept in secured form.

PHR encryption and access. The owners upload ABEencrypted PHR files to the server (3). Each owner's PHR file is encrypted both under a certain fine-grained and rolebased 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 data attributes will include all the intermediate file types from a leaf node to the root. For example, in Fig. 2, an "allergy" file'sattributes are fPHR; medical history; allergyg. The data readers download PHR files from the server, and they can decrypt the files only if they have suitable attribute-based keys (5). The data contributors will be granted write access to someone's PHR, if they present proper write keys.

User revocation. Here, we consider revocation of a data reader or her attributes/access privileges[15]. There are several possible cases:

1. revocation of one or more role attributes of a public domain user;

2. revocation of a public domain user which is equivalent to revoking all of that user's attributes. These operations are done by the AA that the user belongs to, where the actual computations can be delegated to the server to improve efficiency (8).

3. Revocation of a personal domain user's access privileges;

4. revocation of a personal domain user. These can be initiated through the PHR owner's client application in a similar way.

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

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, (6)). To prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity .

Remarks. The separation of PSD/PUD and data/role attributes reflects the real-world situation. First, in the PSD, a patient usually only gives personal access of his/her sensitive PHR to selected users, such as family members and close friends, rather than all the friends in the social network. Different PSD users can be assigned different access privileges based on their relationships with the owner. In this way, patients can exert fine-control over the access for each user in their PSDs. Second, by our multidomain and multiauthority framework, each public user only needs to contact AAs in its own PUD who collaboratively generates a secret key for the user, which reduces the workload per AA (since each AA handles fewer number of attributes per key issuing). In addition, the multiauthority ABE is resilient to compromise of up to N 1 2 AAs in a PUD,which solves the key-escrow problem. Furthermore, in ourframework user's role verification is much easier. Differentorganizations can form their own (sub)domains and becomeAAs to manage and certify different sets of attributes, whichis similar to divide and rule.

Using MA-ABE in the Public Domain

For the PUDs, our framework delegates the key management functions to multiple attribute authorities. In order to achieve stronger privacy guarantee for data owners, the Chase-Chow (CC) MA-ABE scheme [21] is used, where each authority governs a disjoint set of attributes distributively. It is natural to associate the ciphertext of a PHR document with an owner-specified access policy for users from PUD.

However, one technical challenge is that CC MA-ABE is essentially a KP-ABE scheme, where the access policies areenforced in users' secret keys, and those key-policies do notdirectly translate to document access policies from the owners' points of view. By our design, we show that by agreeing upon the formats of the key-policies and the rules of specifying which attributes are required in the ciphertext, the CC MA-ABE can actually support owner-specified document access policies with some degree of flexibility

Setup. In particular, the AAs first generate the MKs and PK using setup as in CC MA-ABE. The kth AA defines a disjoint set of role attributes UUk, Table-1,which are relatively static properties of the public users. These attributes are classified by their types, such as profession and license status, medical specialty, and affiliation where each type has multiple possible values. Basically, each AA monitors a disjoint subset of attribute types. For example, in the healthcare domain, the AMA may issue medical professional licenses like "physician,""M.D.," "nurse," "entry-level license," etc., the ABMS could certify specialties like "internal medicine," "surgery,"etc; and AHA may define user affiliations such as "hospitalA" and "pharmacy D." In order to represent the "do not care" option for the owners, we add one wildcard attribute in each type of the attributes.

TABLE 1
Frequently Used Notations

$\mathcal{U}_D, \mathcal{U}_R$	The attribute universes for data and roles
$\mathcal{T}, L(\mathcal{T})$	A user access tree and its leaf node set
A_k^C	Attributes in the ciphertext (from the kth AA)
A_k^u	User u's attributes given by the kth AA
A, a	An attribute type, a specific attribute value of that type
$\mathcal{P}$	Access policy for a PHR document
P	A key-policy assigned to a user
MK, PK	Master key and public key in ABE
SK	A user's secret key in ABE
$rk_j^{(k)}$	Proxy re-key for attribute j and version k

This primary-type based attribute association is illustratedin Fig. 2. Note that there is a "horizontal association"between two attributes belonging to different types assigned to each user. For example, in the first AA (AMA) "license status" is associated with "profession," and "profession" is a primary type. That means, a physician's possible set of license status do not intersect with that of a nurse's, or a pharmacist's. An "M.D." license is always associated with "physician," while "elderly's nursing licence" is always associated with "nurse." Thus, if thesecond level key policy within the AMA is "1 out of n1 ^ 1 out of n2," a physician would receive a key like "(physician OR *) AND (M.D. OR *)" (recall the assumption that each user can only hold at most one role attribute in each type),nurse's will be like "(nurse OR *) AND (elderly's nursing licence OR *)." Meanwhile, the encryptor can be made aware of this correlation, so she may include the attribute set: {physician, M.D., nurse, elderly's nursing licence} during encryption.

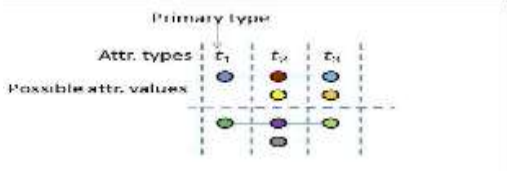

Fig 3: Enhanced Key policy generation rule

Due to the attribute correlation, the set of users that can have access to this file can only possess one out of two sets of possible roles, which means the following policy is enforced: "(physician AND M.D.) OR (nurse AND elderly's nursing licence)." The direct consequence is it enables a disjunctive normal form (DNF) encryptor access policy to appear at the second level. If the encryptor wants to enforce such a DNF policy under an AA, she can simply include all the attributes in that policy in the ciphertext. Furthermore, if one wants to encrypt with wildcard attributes in the policy, say: "(physician AND M.D.) OR (nurse ANDany nursing license)" the same idea can be used,i.e., we can simply correlate each "profession" attribute with its proprietary "*" attribute.

In this above, we present a method to enforce owner's access policy during encryption, which utilizes the MAABE scheme in a way like CP-ABE. The essential idea is todefine a set of key-generation rules and encryption rules.There are two layers in the encryptor's access policy, the first one is across different attribute authorities while thesecond is across different attributes governed by the same AA. For the first layer, conjunctive policy is enabled; for the second, either k-out-of-n or DNF policy are supported. We exploit the correlations among attribute types under an AA to enable the extended second-level DNF policy.

7.SECURITY ANALYSIS

The results are shown in Table 3. It can be seen that, our scheme achieves high privacy guarantee and on-demand revocation. The conjunctive policy restriction only applies forPUD, while in PSD a user's access structure can still bearbitrary monotonic formula. In comparison with the RNSscheme, in RNS the AAs are independent with each other,while in our scheme the AAs issue user secret keyscollectively and interactively. Also, theRNSscheme supportsarbitrary monotonic Boolean formula as file access policy.However, our user revocation method is more efficient interms of communication overhead. In RNS, upon eachrevocation event, the data owner needs to recompute andsend new ciphertext components corresponding to revokedattributes to all the remaining users. In our scheme, such interaction is not needed. In addition, our proposed framework specifically addresses the access requirements in cloudbased health record management systems by logically dividing the system into PUD and PSDs, which considersboth personal and professional PHR users. Our revocation methods for ABE in both types of domains a

8. CONCLUSION

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 whileenhance the privacy guarantees compared with previousworks. 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. Furthermore, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we showthat our solution is both scalable and efficient.

9. REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grainedn Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10),pp. 89-106, Sept. 2010.

[2]H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-HealthCloud," 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 KeywordSearch over Encrypted Personal Health Records in CloudComputing," Proc. 31st Int'l Conf. Distributed Computing Systems(ICDCS '11), June 2011.

[4] "The Health Insurance Portability and Accountability Act,"http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp,2012.

[5] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply toThem," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6] "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.

[7] K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards andPatients' Control: How to Keep Electronic Medical RecordsAccessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287,Feb. 2001.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "PatientControlled Encryption: Ensuring Privacy of Electronic

MedicalRecords," Proc. ACM Workshop Cloud Computing Security(CCSW '09), pp. 103-114, 2009.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,"Proc. IEEE INFOCOM '10, 2010.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and SearchableEncrypted Data for Untrusted Servers," J. Computer Security,vol. 19, pp. 367-397, 2010.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06),pp. 89-98, 2006.

[12] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in WirelessBody Area Networks," IEEE Wireless Comm. Magazine, vol. 17,no. 1, pp. 51-58, Feb. 2010.

[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryptionwith Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

[14] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker,"Ciphertext-Policy Attribute-Based Threshold Decryption withFlexible Delegation and Revocation of User Attributes," 2009.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based DataSharing with Attribute Revocation," Proc. Fifth ACM Symp.