IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 6, August 2014.
www.ijiset.com
ISSN 2348 – 7968

# Reliable Sharing Of Personal Health Records In Cloud Using Attribute Based Encryption

**Pinisetty Chandra sarika**[1] **P.venkateswar rao**[2]

[1]PG Student, M.Tech, Computer Science and Engineering,
Audisankara College of Engineering & Technology, Gudur.A.P, India

[2]Associate Professor, Department of CSE,
Audisankara College of Engineering & Technology, Gudur.A.P, India

## Abstract

This project is to design and implement personal health record (PHR) and provide security and stored in cloud provider. This application allows user to access their lifetime health information, it maintained in centralized server to maintain the patients personal and diagnosis information. The person health records should maintain with high privacy and security. The patient data is protected from the public access through these security techniques. To convince the patients' access over to their own PHRs, before outsourcing we have to encrypt the PHRs. To protect the personal health data stored in a partly-trusted server, we have to adopt attribute-based encryption (ABE) as a main encryption primitive. To obtain fine-grained and scalable information access control for PHRs and to encrypt each patient's PHR file we purchase attribute based encryption (ABE) techniques. The same data values can be accessed by multiple data owners. The proposed scheme can be extended to multi authority attribute based encryption (MA-ABE) for multiple authority based access control mechanism.

**Keywords:** *Personal Health Records, Cloud Computing, Data Privacy, Fine-grained access control, Multi Authority Attribute Based Encryption.*

## 1. Introduction

In Recent years, personal health record is maintained as a patient centric design of health message exchange. It allows a patient to create and control their medical data and it can be maintained in a single place such as data centres. High cost of building and managing stream of data centres and many of PHR services are outsourced to third party service providers, for example Google Health, Microsoft Health Vault. The PHR which is stored in cloud computing have been proposed in [1], [2]. When it is exciting to have convenient PHR data passing for each one, there are number of privacy and security risks it's a wide adoption. In the third party service provider there is no security and privacy risk for PHR. The maximum values of sensitive Personal Health Information (PHI) the unauthorized person storage service are often to target the various malicious behaviours which lead to exposure to the PHI.

The main concern is about privacy of patients, personal health data and to find which user could gain access to the medical records stored in a cloud server. The famous incident, department of Veterans Affairs containing sensitive database PHI of 26.5 million military veterans, including their health problems and social security numbers was theft by an employee who take the data home without authorization [13]. We ensure the privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi trusted servers. Then we can skip to a new encryption pattern namely Attribute Based Encryption (ABE). In this ABE it attributes the users' data to selects the access policies. It allows a patient to share their own PHR among a group of users by encrypting the file under a set of attributes, need to know complete information of users. The scope of result the number of attributes is to determine the complexities in the encryption technique, security key generation, and decryption.

By using ABE to address the 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.

## 2. Problem Definition:

In MA-ABE in the existing since key is created by outsourced again the data is endangered because the key control is visited with outsource agent it become difficult to manage. Thus future enhancement we propose a novel idea which is an enhance MA-ABE so that, key will be given by the user.

## 3. Methodology

### 3.1 Requirements:

The most important task is to achieve patient-centric PHR sharing. That means, the patient should contain the fundamental control over their own health record. It

ISSN 2348 – 7968

also determines which users should have access to their medical data. The user control write/read access and revocation are two main security purposes for any type of electronic health record system. The write access control is controlled by the person to prevent in PHR context entitles by the unauthorized users to get access on the record and to modifying it.

### 3.2 Framework:

The purpose of our framework is to provide security of patient-centric PHR access and efficient key management at the same time. If users attribute is not valid, then the user is unable to access future PHR files using that attribute. The PHR data should support users from the personal domain as well as public domain. The public domain may have more number of users who may be in huge amount and unpredictable, system should be highly scalable in terms of complexity in key management system communication, computation and storage. The owner's endeavour in managing users and keys should be minimized to enjoy usability. By using attribute based encryption we can encrypt personal health records self-protective that is they can access only authorized users even on a semi trusted server.

By using ABE to address the 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.

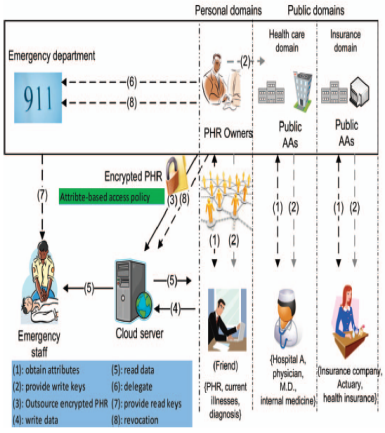


Fig.1: Framework for PHR sharing

### 3.3 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 [8] is used, where each authority governs a disjoint set of attributes distributive. It is natural to associate the cipher text 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 are enforced in users' secret keys, and those key-policies do not directly 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 cipher text, the CC MA-ABE can actually support owner-specified document access policies with some degree of flexibility (such as the one in Fig. 3), i.e., it functions similar to CP-ABE2.

In order to allow the owners to specify an access policy for each PHR document, we exploit the fact that the basic CC MA-ABE works in a way similar to fuzzy-IBE, where the threshold policies (e.g., $k$ out of $n$) are supported. Since the threshold gate has an intrinsic symmetry from both the encryptor and the user's point of views, we can pre-define the formats of the allowed document policies as well as those of the key-policies, so that an owner can enforce a file access policy through choosing which set of attributes to be included in the cipher text.

By enhancing the key-policy generation rule, we can enable more expressive encryptor's access policies. We exploit an observation that in practice, a user's attributes/roles belonging to different types assigned by the same AA are often correlated with respect to a primary attribute type. In the following, an attribute tuple refers to the set of attribute values governed by one AA (each of a different type) that are correlated with each other.

**Enhanced Key-Policy Generation Rule*:*** In addition to the basic key-policy generation rule, the attribute tuples assigned by the same AA for different users do not intersect with each other, as long as their primary attribute types are distinct.

**Enhanced Encryption Rule*:*** In addition to the basic encryption rule, as long as there are multiple attributes of the same primary type, corresponding no intersected Attribute tuples are included in the cipher text's attribute set.

This primary-type based attribute association is illustrated in Fig. 2. Note that there is a "horizontal association" between two attributes belonging to different types assigned to each user. 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 the second level key policy

ISSN 2348 – 7968

within the AMA is "1 out of $n1 \wedge 1$ 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. 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)".

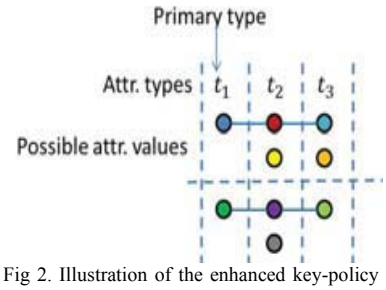


Fig 2. Illustration of the enhanced key-policy generation rule. Solid horizontal lines represent possible attribute associations for two users.

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 cipher text.

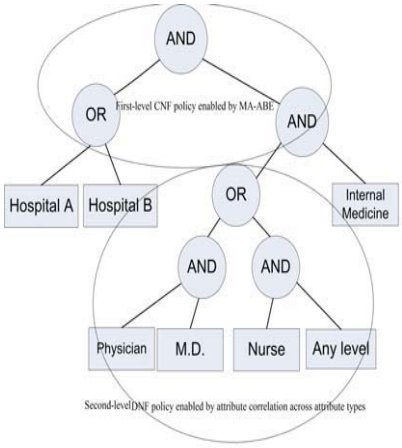


Fig 3. An example policy realizable under our framework using MA-ABE, following the enhanced key generation and encryption rules.

Furthermore, if one wants to encrypt with wildcard attributes in the policy, say: "(physician AND M.D.) OR (nurse AND any nursing license)" the same idea can be used, i.e., we can simply correlate each "profession" attribute with its proprietary "*" attribute. So we will have "*nursing license, *physician license" etc. in the users' keys. The above discussion is summarized in Fig. 3 by an example encryptor's policy. If there are multiple PUDs, then $P = \cup PUDj\{PPUDj\}$, and multiple sets of cipher text components needs to be included. Since in reality, the number of PUDs is usually small, this method is more efficient and secure than a straight forward application of CP-ABE in which each
Organization acts as an authority that governs all types of attributes [7], and the length of cipher text grows linearly with the number of organizations. For efficiency, each file is encrypted with a randomly generated file encryption key (*FEK*), which is then encrypted by ABE.

## 4. Techniques

### 4.1 Attribute Based Encryption

The database security is provided by using Attribute Based Encryption techniques. In this the sensitive information is shared and stored in the cloud provider; it is needed to encrypt cipher text which is classified by set of attributes. The private key is associated with access make to control with cipher text a user is able to decrypt. Here we are using Attribute Based Encryption (ABE) as the principal encryption primitive. By using ABE access policies are declared based on the attributes of user data, which make possible to selectively share her/his PHR among a set of users to encrypting the file under a set of attributes, without a need of complete users. The complexity per encryption, security key generation, and decryption are only linear with multi number of attributes are included. When we integrate ABE into a large scale of PHR system, the important dispute such as dynamic policy updates, key management and scalability, and an efficient on demand revocation are non-retrieval to solve.

### 4.2 Cipher Text Policy Attribute Based Encryption

Cipher text-attribute based encryption is one of the encryption techniques in an attribute based encryption which is used to encrypt the data based on an access policy, which is based on the data or the user attributes. If the secret key is matching with the access control policy [3] then the decryption is possible.

The key-plan of the CP-ABE is: The secret key of the user is related with a set of attributes and each cipher text is surrounded with an access structure. The message can be decrypted by the user only if the attributes of the user's fulfilled with an access structure of the cipher text [5].

This technique have the profit such as the plain text can't be accessed by the third party server,

ISSN 2348 – 7968

when the secret key matched with access policy on the user attributes then the decryption is possible, and every user is required proper authorization and authentication to access the information.

The user revocation is difficult by this CP-ABE scheme. Whenever the user access right wants to change by the owner, it is not feasible to do changes efficiently with this scheme.

### 4.3 Key-Policy Based Encryption:

Key-policy based encryption is one of the attribute based encryption technique in which the data is related with the attributes, a public key component is defined for each of this. In this method, each user will be assigned to an access structure is assigned by each user which used identify which type of cipher texts is used for decryption [6]. The access structure is revealed by this secret key. If the data attribute suit to the user's access structure then only the user will be able to decrypt a cipher text. Cipher texts-policy attribute based encryptions and the key-policy attribute based encryption is nearly functioning in a similar way, but they have some variation in terms of identifying the access policy for the users.

### 4.4 Multi-Authority ABE

A Multi-Authority ABE system is included with k attribute authorities and one central control. The value dk is assigned to every attribute authority. In this proposed system we can use the following algorithms:

The random algorithm is run by the central authority or some other trusted security. It takes input as a security parameter and outputs as a public key and secret key pair for each of the attribute authorities and also outputs as a system public key and master secret key, which is used for central authority.

**Attribute Key Generation:** A random algorithm is run by an attribute authority. The secret key is to take as an input for security authority and the authority's value dk, a user's GID, and a set of attributes in the authority's domain and output secret key for the user.

**Central Key Generation:** A central authority can be used be run by a random algorithm. It takes the master key as an input and a user's GID and outputs secret key for user.

**Encryption:** This technique can be run by a sender. Take a set of attributes as an input for each authority, and the system public key. The outputs are in the form of cipher text.

**Decryption:** This mechanism can be done by a receiver. Takes input as a cipher text, which was encrypted under a set of decryption keys for attribute set.

By using this ABE and MA-ABE it will increase the system scalability, there are some restriction in building PHR system. The ABE does not handle it efficiently. In that scenario one may regard with the help of attributes based broadcast encryption.

## 5. Security Model Of The Implementation System

### 5.1 Data confidentiality:

This research plan reveals the data about each user to access on the PHR among one another. The different sets of documents are authorized by the users to read the document.

### 5.2 User Access Privilege Confidentiality:

The system does not disclose the rights from one person to another. This ensures the user to access strong confidentiality. And also it maintains both public domain and private domain. Secure Sharing of Personal Health Records System designer maintain Personal Health Records with various user access points. These data values are managed under a third party cloud provider system. The cloud provider will provide security for the data. Multiple modules can be provided by this system.

 Data owner is designed to manage the patient details. With multiple attribute collections the PHR is maintained. Access permission to different authorities can be assigned by data header.

 Cloud provider module is used to store the PHR values. The encrypted PHR is uploaded by the data header to the cloud provider. Patients can access data and also maintained under the cloud provider.

 Key management is one of the main tasks to plan and control key values for various authorities. The owner of the data will update the key values. This dynamic policy is based on key management scheme.

Patients are accessed by the client module. This system uses the personal and professional access pattern. Access classification is used to provide multiple attributes. Client's access to log maintains to the user request information to process auditing.

## 6. Conclusion

A framework of secure sharing of personal health records has been proposed in this paper. We can provide good security to our data using encryption technique in cloud. Public and Personal access models

ISSN 2348 – 7968

are designed with security and privacy enabled mechanism. The framework addresses the unique challenges brought by multiple PHR owners and users, in that the complexity of key management is greatly reduced. The attribute-based encryption model is enhanced to support operations with MAABE. The system is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy.

## 7. References

[1] 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.

[2] 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.

[3] M. Li, S. Yu,Y. Zheng, ,K. Ren, &W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption", IEEE Transactions on Parallel and Distributed Systems, vol. 24(1), pp. 131-143, 2013

[4] 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," Proc. Sixth Int'l ICSTConf.SecurityandPrivacyinComm.Networks (SecureComm'10), pp. 89-106, Sept. 2010.

[5] 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.

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

[7] 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.

[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] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.

[10] 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.

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

[12] 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.

[13] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safe- guarded," http://articles.latimes.com/2006/jun/26/health/ he-privacy26, 2006.

[14] S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar. 2011.

[15] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Comm. (TrustCom), 2011.