IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p-ISSN: 2278-8735
PP 62-67
www.iosrjournals.org

Secure Sharing of Personal Health Records in Cloud Storage using HASBE

Rojitha Abdulla
Department of Computer Science & Engineering,Muslim Association College of Engineering, Kerala, India

Abstract: *Personal Health Records or PHR is the medical information of an individual, stored and managed by the patient himself, in third party servers like clouds, so as to make it available for global data sharing. As the usage of such servers for storage purposes become more complex, they give rise to various security issues. Privacy, scalability and flexibility are some common issues concerning third party servers. Attribute Based Encryption (ABE), one of the earliest methods used for outsourced data encryption, has been utilized in several schemes as a solution, but such designs suffer from inflexibility, when the access control policies used are complex. This work focuses on the multi-data owner/patient scenario, where the PHR system users are divided into two security domains- the private domain and public domain, each of which is encrypted using its own set of mechanisms. We present the advantages of using the Hierarchical Attribute Set Based Encryption (HASBE) technique rather than the Multi-Attribute ABE, an extension of Ciphertext ABE, for situations where complex access control policies are required. Hierarchical ASBE uses dynamic constraints while combining attributes and thereby provides greater flexibility. This scheme also supports efficient on-demand user revocation. We have proven its efficiency by implementation.*

Keywords: *Flexibility, Access Policy, Scalability;*

I. Introduction

A PHR is information about the health of a patient, compiled and maintained by the patient himself. This can be used to track and share an individual's past and current health information. PHR is also a tool for global medical data sharing. Thus an authorized medical care provider can have access to a patient's health related information and thereby gains more insight into the health history of the patient under his care. To overcome the obstacles arising as a result of scalability problems, many PHR services are outsourced to third party servers like the clouds.

Cloud Computing, one of the most powerful paradigms in the IT sector, is a way to increase capacity on the fly without investing in new infrastructure, training new personnel, or licensing new software. However cloud computing means storage of data on the internet. The outsourcing of PHR data on to clouds has led to concerns of the insecurity of the medical information. The medical information of an individual is highly sensitive and must be accessed only by the patient or by those who has been given authorization by the patient. The data must remain confidential to all else.

A solution to this dilemma is to encrypt the information before uploading for storage in clouds. There has been various techniques proposed for the encryption of data outsourced to clouds. One method is the usage of passwords provided by the owner/patient whenever access to a PHR file is needed. Another mechanism is the presence of a Central Trusted Authority. But all these techniques have limitations. The usage of passwords requires a PHR owner/patient to be continuously online, which is not feasible. Central Authority can lead to a single point of failure. A better suggestion, which has also been effectively implemented, is the Attribute Based Encryption (ABE) scheme. Users of the PHR service are given access to a PHR file only if they have been authorized by the PHR owner/patient, i.e., the patient. A patient's PHR file can be accessed by his relatives, friends, doctors, nurses etc. If the owner/patient is responsible for managing all details of each user key, then, keeping in mind the large and unlimited number of possible professional users, there could be heavy key management overhead.

To solve the key management issues and also taking into account the multi-owner/patient scenario, Ming Li proposed a scheme, in [1], where, a patient PHR user profile can be divided into two categories or domains, one being the private domain, which consists of his friends and relatives, and the other being the public domain, which consists of the medical professionals who are authorized to view his medical files, and, managing both domains by different means. He propounded the usage of Multi-Authority ABE (MA-ABE), (an extension of the Ciphertext Policy ABE (CP-ABE)) in the public domain and Key-policy ABE (KP-ABE) in the private domain. However CP-ABE fails when complex access control policies are used.

We have already put forth the suggestion of utilizing the Hierarchical Attribute Set-Based Encryption (HASBE) in place of MA-ABE in the public domain in our paper, [2]. In this paper, we implement the HASBE technique to prove its effectiveness, when compound key structures and complex access policies are incorporated.

II. Related Work

Public Key Encryption or PKE schemes were the primary techniques used for enforcing access control for data stored in third party servers. However these led to high key management overhead. Scalability has also become a major issue. As an improvement, 1 to N encryption schemes were introduced. In ABE, the stored data is encrypted with a set of attributes and only those users who have the proper key structure as specified by the PHR file owner/patient are authorized to decrypt the data. Different variants of ABE schemes have been suggested in [3], [4]. Ibraimi et. al. in [5] suggested CP-ABE and also introduced the idea of private-public domains. Another variant of ABE was used by Akinyele et. al. in [6] to create self-protecting EMRs. Despite successful implementation of the ABE scheme, they were proven to be not much efficient. The presence of a single trusted central authority led to many complications like the key escrow problem, in case of a corrupt central authority. They can cause bottlenecks and key management problems. The user revocation process was also not given due importance.

The KP-ABE was put forth by Yu et. al. in [4]. The owner/patient encrypts the data and distributes the keys to those who need access to information. Key Management is kept to a minimum because of the limited amount of users. User revocation is also present. It is, however, inefficient in a multi-owner/patient scenario. Lewko and Waters's ABE [7] is a revocable ABE but has high key update communication overhead. MA-ABE, a variant of the CP-ABE scheme, proposed by Chase and Chow in [8] lacks efficient user revocation. Basic CP-ABE schemes are not much effective, when complex access policies are involved. CP-ABE supports the involvement of user attributes that can only be grouped as a single set. Bobba et.al. set forth the suggestion of Ciphertext Policy Attribute Set-Based Encryption (CP-ASBE or simply ASBE) in [9], where user attributes can be grouped into a recursive set structure form, which leads to much greater flexibility in expressing complex access policies, thereby providing more efficiency in barring unauthorized personals from gaining illegal access to information.

ASBE can be used to put into effect restrictions on uniting attributes to satisfy an access policy set by an owner. When recursive structures are used, attributes from the same set can only be grouped to realize a policy while those from different sets cannot be joined. This provides more feasibility in many complex situations. ASBE is also capable of allotting multiple values to the same attribute which helps in solving user revocation. However, ASBE does not support a hierarchy structure of attribute or domain authorities. The HASBE described in [2] is the solution for this scenario. It is an extended version of ASBE and is capable of handling multiple levels of authorities.

III. System Model And Assumptions

In this section, we present the framework used in our scheme. Also, certain assumptions upon which the entire system rests is also discussed here.

1.1. Private Domain System Model & Assumptions

The Private Domain system model consists of a PHR cloud service provider, data owner/patients and consumers. The cloud service provider provides the medical file storage facility and is assumed to be untrusted. Data owner/patients and consumers are members of a health social network. Whenever consumer requires access of a data owner/patient PHR file, an access request message is send to the owner/patient. The owner/patient decides which files the consumer can access and generates the appropriate key, which is send to the consumer. The consumer can then access the required files.

1.2. Public Domain System Model & Assumptions

The Public Domain system model basically consists of a PHR cloud service provider, a trusted authority, one or more domain authorities, zero or more subordinate domain authorities, data owner/patients and consumers. The whole system is organized in a hierarchical manner, as shown in figure 1.

The trusted authority (TA) is the core authority, in this respect, the Ministry of Health. The TA is responsible for the domain authorities, which, in this case, has been selected as the National Medical Association. A domain authority can be trusted by all parties under its control but not by others. Data owner/patients and consumers come under the control of the domain authority. The data owner/patients are the patients and the data consumers are all those who requires access to the patient health record like friends and relatives of the patient along with the doctors, nurses, emergency department staff etc. The latter are considered

malicious. The clouds provide the health record storage facility. Similar to the private domain, they are assumed to be untrusted. The data owner/patients encrypt their medical records and upload it on to the clouds for storage. Data consumers can only read the uploaded files.

The PHR file is encrypted by the data owner/patient and uploaded on to the clouds for storage. Each data consumer has a key structure provided by their domain authority. The key structure is validated with the access policy set by the owner/patient for each file. The consumer is authorized for data access only if validation is successful. Thus the downloaded file can be decrypted by an authorized data consumer.

IV. Implementation

This section deals with the methodology involved in the entire PHR system. The working of both private domain and public domain are detailed below.

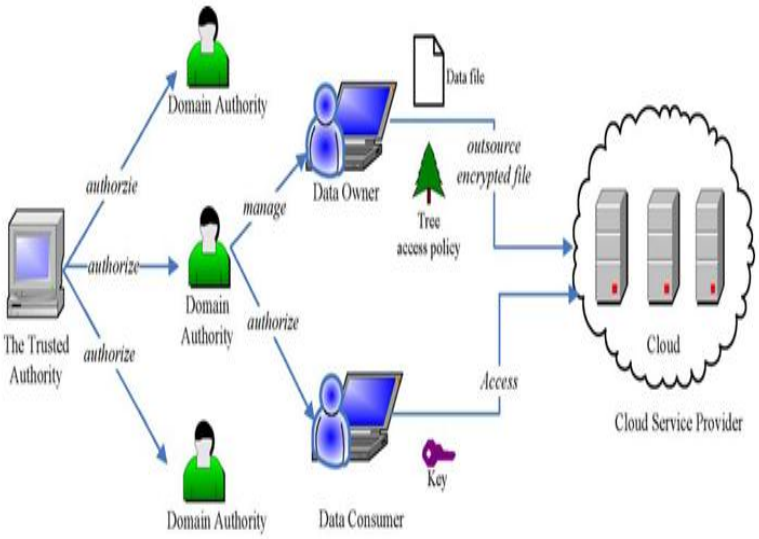

Fig. 1. Public Domain System Model

1.3. Implementation of the Private Domain

The private domain implementation follows the KP-ABE scheme followed by Ming Li et. al. in [1]. The owner/patient is the trusted authority here, who grants the decryption keys to the data consumer, viz, friends and relatives, on access request. The owner/patient determines which data types can be viewed by the requester, thereby generating the access policy followed by the decryption key. Thus the consumer is granted a subset of data types applied for. Data attributes, based on the inherent properties of a PHR file, are used for the personal health record encryption by the owner/patient.

1.4. Implementation of the Public Domain

In this section, the inner details of HASBE scheme are discussed. HASBE is in effect, an extended version of ASBE, in conjunction with a delegation algorithm for the inclusion of the hierarchical user structure as described in [10]. The data owner/patient, viz, the patient creates his PHR and uploads the encrypted file on to the clouds. An access policy is set by the owner/patient prior to file creation. Only data consumers, in this respect, the doctors, nurses and medical department personnel, who have the required key structure as provided by their organization, to satisfy the set access policy, can decrypt the downloaded PHR.

1.5 Key structure: The key structure used is recursive and set based. It's depth refers to the level of recursions in the recursive set. The depth, in this instance, is taken as two. It can be varied according to necessity. The components of a set at depth 1 may either be attribute elements or sets but components of a set at depth 2 will only be attribute elements. {Department: Cardiology, {Hospital: KIMS, Designation: Physician}, {Hospital: PRS, Designation: MD}} is an example for a depth 2 key structure.

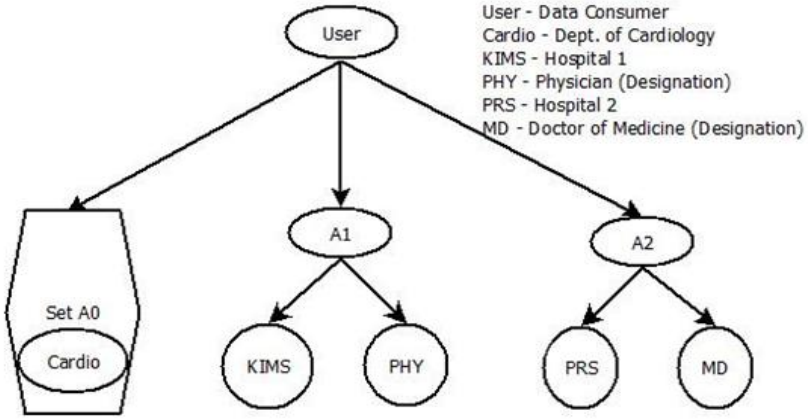

Fig. 2. Key Structure of a Data Consumer

Distinct labels can be given for each of these sets. Since depth is of 2, indices can be used for labeling. The set at depth 1 can be alluded as set 0. The entire key structure can be represented as Â= {A0,A1,A2}, where A0 represents the set at depth 1 and A1 and A2 represents sets at depth 2. In our example, A0 represents {Department: Cardiology}, A1 represents {Hospital: KIMS, Designation: Physician} and A2 {Hospital: PRS, Designation: MD}. The example key structure has been depicted in fig. 2.

1.4.1Access Structure: Tree access structure is used here. The leaf nodes are attribute elements and non leaf nodes are threshold gates. According to example fig. 3, the owner/patient has set the access policy such that only an MD in the department of Cardiology of hospital KIMS may decrypt his medical files. Using CP-ABE schemes lead the attributes of the doctor to be taken as {Department: Cardiology}, {Hospital: KIMS, PRS} and {Designation: Physician, MD}. This, in turn, allows the illegal combination of attributes across multiple sets, thereby leading to unauthorized access of sensitive medical information. Such a combination of attribute elements over multiple sets can be prevented using HASBE, which provides distinction to each set.

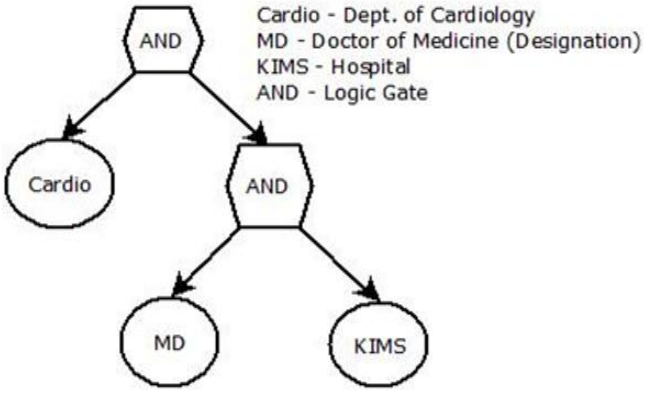

Fig. 3. Access Policy set by the patient, viz, the data owner/patient

1.4.1. HASBE scheme: We utilize the HASBE scheme described in [10] by Wan et. al. The Ministry of Health is the trusted Authority and is responsible for the creation and allocation of the system parameters and the master key of the domain authority, viz, the National Medical Association. The domain authority is, in turn, accountable for the data owner/patient-consumer key generation and distribution. HASBE consists of seven major operations:

1.4.1.1. System Setup: The Ministry of Health creates the public key, which is made public, and the master secret key.

1.4.1.2. Top-Level Domain Authority Grant: In this part, a domain authority is given its public-private key, i.e., the ID and the recursive attribute set Â. When a new domain authority aspires to join the system, it is first verified by the trusted authority. If it is found to be valid, an ID is generated for the domain authority. The domain authority may now validate new users in its domain. Thus this section handles the authorization of the National Medical Association by the Ministry of Health. They are given IDs and attribute sets.

1.4.1.3. New User Grant: User, in this instance, refers to the data owner/patient or consumer. The case for a new user grant is similar to the preceding section. The only difference is that, in this case, the domain authority, viz, the National Medical Association authorizes the new user. After it is found to be valid, a key structure corresponding to its role and a new ID is provided to the new user and a secret key is then made available to the user.

1.4.1.4. New File Creation: The patient encrypts his PHR and stores it on the clouds. The following procedures are involved in a new file creation.

1.4.1.4.1. An ID is created for the PHR file.

1.4.1.4.2. A symmetric data encryption key, DEK, is randomly chosen and the file is encrypted using the same.

1.4.1.4.3. An access structure is constructed for the file and the DEK is encrypted with the access tree using the HASBE encryption algorithm. This is the Ciphertext PHR.

1.4.1.5. User Revocation: In this instance, user refers only to the consumer. A revoked data consumer must not be able to view the patient files any longer. For this purpose, extra parameters are introduced. An access policy date is set for each PHR file which is the time at which it was created by the patient. An expiration time is specified for the consumer key which is a maximum of one day. The expiration time of the consumer, say X, must always be greater than the policy date, say Y, i.e., $X \geq Y$, and the access policy must also be a perfect match with the attributes present in the consumer key structure, for him to access the relevant PHR. By updating the expiration time parameter of the consumer key, a domain authority can perform user revocation.

1.4.1.6. File Access: When a data consumer requests for a patient PHR, the clouds sends the encrypted files to the consumer. If the consumer is authorized, then he will be able to view the PHR, else, the files remain encrypted. For authorization, the consumer key structure is compared with the access policy and if the attributes in the former matches with the specified requirement, then he is provided the decryption key to decrypt the Ciphertext PHR to get the data encryption key or DEK. DEK is further used to decrypt the actual PHR Ciphertext.

1.4.1.7. File Deletion: A data owner/patient may also delete his encrypted file.

II. Result Analysis And Discussion

2.1. Analysis

We evaluated the performance of our scheme by implementation. The following procedures were followed and results procured.

5.1.1. Initialization - The patient becomes a member of a Health Social Network (HSN) and uploads PHR file on to the clouds. The patient PHR file access policy is set as {Hospital: KIMS, Department: Cardiology, Designation: MD}. The data consumers are registered in the respective domain authorities, i.e., the National Medical Association, in this case. Their individual attributes are as shown in Table 1.

5.1.2. Phase 1 (Private Domain Phase) - The patient friends and relatives are also members of this HSN. They form connections with one another and make key request for file access. A patient record can be accessed only if permission to access that record has been set, which will be apparent from the access policy reflected in the secret key.

5.1.3. Phase 2 (Public Domain Phase) – The users here are Doctor 1 and Doctor 2 whose respective attributes are given in Table 1. Doctor 1 tries to access patient records illegally by combining the attributes of his two roles. {KIMS, Cardiology, Physician} and {PRS, Cardiology, MD} are his two attribute sets. On using CP-ABE, the attributes which satisfy the required access policy, i.e., {KIMS, Cardiology, MD} can be selected from the two sets and combined, thereby gaining illegal access to patient records. However, such combining of attributes from multiple sets are not possible with HASBE. Thus Doctor 1 gets rejected because both of his attribute sets do not match with the required access policy. But Doctor 2 is given access because one of his attribute sets is the required policy, as is evident from Table 1.

5.1.4. Phase 3 (User Revocation) – In the public domain, the secret key date of the doctor must always be greater than the policy date, but less than the secret key expiration time, which is set for a single day, else the doctor will be blocked from access. In the private domain, a key can be used to access only a single record. Subsequent accesses using the same key are blocked.

III. Discussion

This segment makes a comparison between our scheme and that proposed by Ming Li et. al. in [1]. Since private domain utilizes the KP-ABE in both schemes, there is no difference in its performance. The relative advantages in employing HASBE instead of CP-ABE security-wise are as discussed below.

3.1Scalability- HASBE is extended from ASBE with the help of a key delegation algorithm. It paves way for the existence of a hierarchy of multiple levels of domain authorities. Thus the workload of the trusted

authority is halved and shifted to lower level domain authorities. Also workload of each domain authority at each level is also reduced and divided among its subordinate domain authorities. Thus the hierarchical structure gives way to greater scalability.

3.2Flexibility- HASBE can put into effect restrictions on uniting attributes to satisfy an access policy set by an owner/patient. When recursive structures are used, attributes from the same set can be grouped to realize a policy while those from different sets cannot be joined. This makes for more feasibility in many complex situations. More complex access policies can be created.

3.4Fine-grained access control- Since more complex access policies are possible using this scheme, it allows for more fine grained access of data.

3.5User Revocation- The consumer key contains the expiration date component which can be updated as and when necessary by the domain authority responsible for the consumer. This possible because of HASBE's capability of assigning multiple values for a single attribute.

Table 1. Attribute Set Table 1

Profession	Role Status	Attributes		
		Hospital	Department	Designation
Doctor 1	2	KIMS	Cardiology	Physician
Doctor 1	2	PRS	Cardiology	MD
Doctor 2	2	KIMS	Cardiology	MD
Doctor 2	2	MCH	General Medicine	MD

IV. Conclusion

In this paper, we have put forth HASBE as a viable option in the public domain, to increase the security of the medical information stored in the clouds. This work is an extended version of ASBE with the inclusion of a delegation algorithm to incorporate the hierarchical system of users. More complex access policies can be realized as a result of this scheme. Finally, we have proven its efficiency through implementation and the advantages discussed. The private domain implemented follows the scheme proposed by Ming et. al. in [1].

References

[1]. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, "Scalable and secure sharing of Personal Health Records in Cloud Computing using Attribute Based Encryption." in IEEE transactions on parallel and distributed systems Vol 24, pages 131-143, Jan 2013.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2]. Rojitha Abdulla, Anupriya Vysala, "Secure Personal Health Records in Clouds: A Hierarchical Attribute Based Solution." in International Journal of Computer Science and Mobile Computing, ICMIC13, December- 2013, pg. 44-49.Y.

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

[4]. 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.

[5]. Melissa Chase "Multi-authority Attribute based Encryption," Computer Science Department Brown University Providence, RI 02912

[6]. J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute based encryption," in IEEE S&P ″07, 2007, pp 321-324

[7]. 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.

[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]. A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Advances in Cryptology–EUROCRYPT, pp. 568–588, 2011

[10]. Zhiguo Wan, Jun″e Liu, Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for flexible and scalable access control in cloud computing" in IEEE transactions on Information forensics and security, Vol. 7, no. 2, April 2012.K. Elissa, "Title of paper if known," unpublished.

[11]. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

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

[13]. J. A. Akinyele et al., "Self-protecting electronic medical records using attribute based encryption," Cryptography ePrint Archive, Report 2010/565, 2010.

[14]. R. Bobba, H. Khurana and M. Prabhakaran, "Attribute-sets: a practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.

[15]. R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009