JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-12 E-ISSN: 2347-2693

Encryption Schemes for Securing Cloud-based PHR Systems

Shruthi Suresh

Dept. of CSE, Royal College of Engineering and Technology, Akkikavu, Kerala, India
www.ijcaonline.org

Received: Nov /28 /2014 Revised: Dec/05/2014 Accepted: Dec/18/2014 Published: Dec/31/ 2014

***Abstract*—** Presently, Personal Health Records are widely used by people not only to store their health details, but also to share their health information among doctors, friends, relatives, medical organizations etc. Health records are now stored and shared with the help of cloud services. The sensitive nature of these health records makes it vulnerable to attacks. To ensure privacy of health information, the best method is to encrypt it. In this paper, Attribute Based Encryption and its variants are studied so that they can be used for developing an efficient health record sharing scheme which is more flexible and scalable.

***Keywords*—** Personal Health Record (PHR) ; Cloud Computing ; Attribute Based Encryption (ABE) ; MA-ABE ; Proactive MA-ABE; CA ;Data Privacy ; Fine-grained access control.

I. INTRODUCTION

Personal health information of a person can be effectively managed and shared via Personal Health Records (PHRs). PHRs allow the patients to develop and control their medical record which may be arranged in a single place such as data centers. The high cost of building and maintaining data centers lead to outsourcing of health records to third-party cloud service providers, such as, Google Health. This in turn arise the issue of data privacy. The primary concern is about whether the patients could actually manage the sharing of their sensitive personal health data, especially when they are stored on partially trusted third-party server. "Fig. 1" illustrates a Cloud-based PHR System. To assure privacy control over PHRs, it is crucial to have Fine-grained data access control mechanisms that work with partial-trusted servers. The basic encryption techniques such as public key encryption are found to be inefficient as they lack in providing scalability and also causes a larger key complexity. So, in order to achieve efficiency and reliability, an encryption technique, namely Attribute Based Encryption (ABE) is used in this scheme. ABE enables a patient to selectively share their health record among a set of users by encrypting the file under a set of attributes, without the necessity to know a complete list of users. This is because in Attribute based encryption, it is the attributes of the users or the data that selects the access policies. As a result, the number of attributes involved determines the complexities in encryption, key generation and decryption. One main issue is key management problem. Another issue in secure sharing of health information is on demand user revocation. To solve these problems variants of Attribute Based Encryption can be employed in the system.

This paper discusses about various encryption techniques and their extended versions including their pros and cons. Also, challenges of these encryption schemes at different security levels are studied so that some of these encryption schemes could be used for further enhancing the cloud-based health record system.

Corresponding Author: *Shruthi Suresh, shruthigvr@gmail.com*

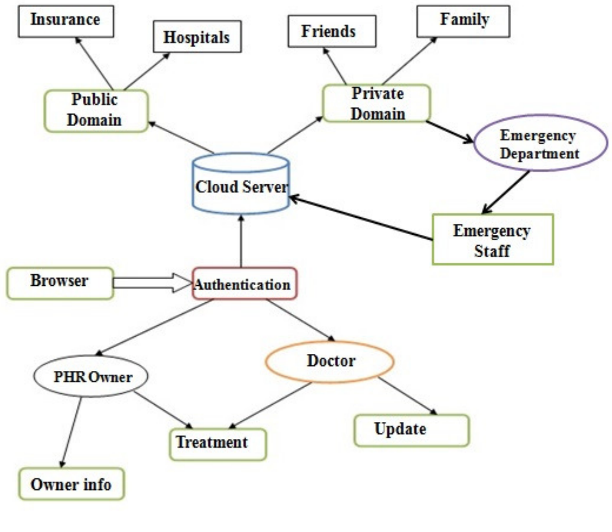

Fig. 1: Block Diagram of Cloud-based PHR System

II. VARIOUS ENCRYPTION SCHEMES

Earlier, Personal health records were encrypted using traditional encryption methods. But nowadays new and improved encryption techniques are applied for secure transfer of Personal health records.

A. *Asymmetric Encryption*

Asymmetric encryption, also known as public key encryption is the most traditional method applied to Personal Health Record for data security [9]. It is one to one encryption method. Traditional public key technique can be adopted in the data encryption procedure, and the owner uses users' public key to encrypt data before uploading to the cloud. If the user sends an access request to the cloud, then the cloud would return the corresponding cipher text to the user. User uses his/her private key to decrypt the data. The disadvantages of this technique are:

- To encrypt data, owner require user's public key.
- Same plain text with different public keys leads to large overhead.
- Less scalable and needs high key management.

To improve these drawbacks, Sahai and Waters proposed an attribute-based encryption (ABE) technique [2].

B. Attribute Based Encryption(ABE)

ABE is a variant of asymmetric encryption in which the secret key of the user and the cipher text depends upon attributes used. In such a system, the decryption of a cipher text is possible only if the set of attribute of the user key matches the attribute of the cipher text. ABE not only offers fine grained access control but also prevents against collusion. It reduced the high key management overhead and requires encrypting multiple copies of a file using different user's keys. Using ABE, access policies expressed based on the attributes of the user data which enable the patient to selectively share the PHR among a set of users by encrypting the file under a set of attributes, and so the owner don't want to know the complete list of users. The main goal for this technique is to provide security, access control and the main aspects are to provide flexibility, scalability, and fine grained access control.

Matthew Pi [1] suggested that attribute based system is an effective solution for securely managing information in huge, distributed systems. But in the traditional model, this system can be achieved only when single trusted authority (TA) is used in the system .This means that the user and server must be in a trusted domain. Since the TA can access all the encrypted files, it results in key escrow problem. Single TA also creates a load chokepoint. This causes a potential threat to the privacy. Also, on demand user annulment was not adoptable with this encryption technique.

C. Key policy Attribute based encryption (KP-ABE)

Key-policy attribute based encryption is modified form of the Attribute Based Encryption. V. Goyal, O. pandey, A. Sahai, and B. Waters [2] proposed key-policy attribute based encryption (KP-ABE) technique to overcome the limitation of traditional model. The new data access control technique i.e. Attribute based encryption (ABE) technique was introduced which consist of key-policy attribute based encryption (KPABE). In this scheme, each user will be ascribed to an access structure that will define which type of cipher text the key can decrypt. The secret key is defined to reflect the access structure. So user will be capable of decrypting a cipher text if and only if the data attribute satisfies that user's access structure. The KP-ABE is useful for ensuring the fine grained access control to data model where it can expeditiously specify which part of data model can be accessed by which user and what are the functions they can execute over there. But this technique has the disadvantage that the data owner is also a trusted authority (TA). If this technique is applied to PHR system with multiple users and data owners, it would be ineffective as each user would receive multiple keys from multiple owners, even if the key contains the same set of attributes.

D. Cipher-text policy Attribute based Encryption (CP-ABE):

Another modified form of ABE called Cipher-text policy Attribute based Encryption (CP-ABE) was introduced by Sahai et al [4]. It allows the data owner to encrypt the data based on an access policy, which will be based on the attributes of the user or data. So, the decryption is possible when the secrete key is the one corresponding to access control policy. The key idea of CP-ABE is that the user secret key is associated with a set of attributes and each cipher text will be embedded with an access structure. The user can decrypt the message only if the users attribute matches with the access structure of the cipher text. This method has gain that the third party sever won't have access on the actual data, decryption will be possible only when the secret key is matched up with access policy defined on attributes, and every user is needed proper authorization to access the data. And also it removes the need for knowing the identity of the patients for providing access grant. CP-ABE improves the disadvantage of KP-ABE that the encrypted data cannot choose who can decrypt it.

The key problems regarding this technique are:

- User delegation is challenging.
- Access right of the user cannot be effectively managed by the owner.
- User attributes are organized logically as a single set, so users can only use all possible combination of attributes in a single set issued in their keys to satisfy policies that are only supported by decryption keys.

E. F. Cipher-text policy Attribute Set based encryption (CPASBE):

A new variation of CP-ABE called Cipher text attribute Set based encryption(CP-ASBE) was introduced by S. Jahid, P. Mittal and N. Borisov et al [10] . Instead of periodical revocation, immediate attribute revocation is applied in this technique. In CP-ASBE user attributes are grouped into a recursive set based structure and user is allowed to impose dynamic constraints on how those attribute may be combined to satisfy a policy. In CP-ABE technique, decryption keys only support user attributes that are arranged logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy a policy. To solve this problem, CP-ASBE is introduced. Grouping of users attributes into sets is done such that those belonging to a single set have no restriction on how they can be combined. CP-ASBE can support compound attributes without sacrificing the flexibility to easily specify policies involving the underlying singleton. While restricting users to use attributes from a single set during decryption can be thought of a regular CPABE technique, the main problem in constructing a CP-ASBE technique is in selectively allowing users to combine attributes from multiple cloud providers.

F. I. Identity based encryption (IBE):

M. Franklin, D. Bonch [3] introduced an identity based encryption technique which allows any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private key Generator (PKG), generates the corresponding private keys. The PKG first publishes a master public key, and holds the corresponding master private key (referred to as *master key*). Any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value as the master public key is already given. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG. The master private key is used by PKG to generate the private key for identity ID. As a result, parties may verify signatures or encrypt messages with no prior distribution of keys between individual participants. This is very useful in cases where pre-distribution of authenticated keys is infeasible due to technical restraints. However, to decrypt or sign messages, the authorized user must obtain the appropriate private key from the PKG. The main concern of this approach is that the PKG must be highly trusted, as it may decrypt messages without authorization as it is capable of generating any user's private key. Also, this system has inherent key escrow problem as any user's private key can be generated through the use of the third party's secret key. A number of variant schemes have been proposed which remove the key escrow problem.

In IBE, data is encrypted using an arbitrary string as the key and a decryption key is mapped to the arbitrary encryption key by a key authority. Though this technique is provably secure, the security proof leans on comparatively new assumptions about the hardness of problems in certain elliptic curve groups. IBE solutions may depend upon cryptographic techniques that are insecure against code breaking quantum computer attacks. Another main disadvantage of this system is key management overhead. Letting each user obtain keys from every owner PHR wants to read would limit the availability. Another version of IBE is Hierarchical identity based encryption (HIBE). It is Hierarchical form of a single IBE [3]. This concept can help to explain the definition of security.

G. M. Multi-Authority Attribute Based Encryption (MA-ABE):

The multi-authority attribute based encryption scheme [7] is an advancement of attribute based encryption in which there are many attribute authorities for handling the different set of users from various domains. In Personal Health Record system the users will be form different domain like physician, friend or family member from personal relations and other users from insurance agency too. So each user will be having different access control mechanism based on the relation with patient or owner. The MA-ABE scheme will highly reduce the key management problems and overhead. Thus MA-ABE provides fine grained access control to the PHR system. The security and privacy concerns of cloud based PHR system can be addressed by integrating advanced cryptographic techniques, such as MA-ABE into PHR system. Meanwhile patient gain full control access over their PHR files and can set access privilege to selected data users. Thus the dynamic policy management model is supported by this technique. With higher security and privacy for PHR, the existing MA-ABE could be inefficient to solve the higher level issues.

The problem of this scheme is that it needs a fully trusted central authority (CA) which can decrypt every ciphertext in the system. This central authority would threaten the whole system if it's corrupt.

H. Extension of MA-ABE:

In order to increase the security level and overcome the limitation of MA-ABE, it is further enhanced. They are-

1. Multi-Authority Fuzzy Identity Based Encryption (MA-FIBE)

This technique present the threshold multi-authority fuzzy identity based encryption (MA-FIBE) scheme without a central authority. This technique consider the stronger adversary model in the sense that the corrupted authorities are allowed to distribute incorrect secrete keys to the users. The security proof lies on the secrecy of the fundamental joint random secret sharing protocol and joint zero secret sharing protocol and the standard decional bilinear Diffe-Hellman assumption. These two techniques focus on removing Central Authority from MA-ABE technique. By enforcing the key distribution scheme and the joint zero secret sharing technique to MA-FIBE, the various difficulties in MA-FIBE could be overcome by the simple modification. The difficulties which overcome are:

- It was difficult to remove the central authority while preventing the collusion attack and keeping the decryption process independent of identifier of each user.

- Another difficulty is that the integration must be accomplished with the last decryption step. The integration aims to emancipate the users from the restriction of individual identifier, which means the integration shouldn't be completed before the final decryption steps.

Thus MA-FIBE technique without a central authority could be constructed which is a more flexible scheme.

2. *Threshold MA-ABE without CA*

This MA-ABE scheme is actually the generalization of the Multi-Authority Fuzzy Identity Based Encryption technique [15]. The major difference between the MA-FIBE and MA-ABE technique lies in the SKD algorithm and the other rest algorithm. The size of their public parameters is the property which differentiates these techniques. The first technique corresponds to the construction for access trees which is denoted as construction for small universe and the other corresponds to the large universe construction.

3. *Proactive Multi authority ABE*

Herzberg etc. [6] introduced Proactive secrete sharing (PSS) in 1995. It supplies useful tool to construct a proactive attribute based model in which the authorities' secret keys could be updated periodically without any modification to the authorities' respective public keys. The advantage resulting from proactive property is that, a large number of GIDs could be adopted in the proactive system, while no more than m GIDs could be used in the basic construction. Since the public keys remain unchanged through different periods, then the secret keys obtained from the old system could still be used for decrypting in the updated system, although the old secret keys couldn't be mixed with the newly-obtained secret keys to decrypt since they correspond to different polynomial evaluations.

Ramasamy.S, Vahidh. J [5] introduced multi authority attribute based encryption for further enhanced to Proactive Multi authority attribute based encryption. A proactive multi authority attribute technique implies that the secret keys hold by the authorities could be updated without altering the public parameters of the whole system. This would result in a more convenient system for the users in the sense that the encryptor needn't renew their ciphertext which was created in the original system before the renewal. This technique also enhances the security level of the system because the adversary has to attack the system successfully during a shortened period of interval compared with the adversary to the underlying multi-authority technique.

III. COMPARISON

"Table 1" shows the comparison of various encryption schemes that can be used in cloud-based PHR systems.

Schemes	Scalability	Flexibility	Access Control	Security
ABE	high	high	high	low
KP-ABE	low	low	high	low
CP-ABE	low	low	high	low
IBE	low	low	low	high
MA-ABE	high	high	high	low

Table 1: Comparison of Encryption schemes

IV. CONCLUSION

Cloud-based PHR systems are widely used by people to store and share their health details securely. The users will be doubtful whether their data is secure in the hands of this third party authority. So, the desired security goals must be achieved. In this paper, the study of different encryption techniques is done with their pros and cons. Also, variations of these techniques are discussed and compared with the existing schemes. This survey paper thus introduced the various accomplishments and limitations that are present or will occur in the cloud based PHR system in future. Therefore for improving the security related issues, various concerns are made. The improvement in multi authority attribute encryption technique is shown on removing the Central Authority. The three various extensions of MA-ABE are found to be proven more secure. Future improvements can be done based on this survey of various encryption techniques.

REFERENCES

[1] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute Based Systems," Journal of Computer Security, vol. 18, no. 5, pp. **799–837**, **2010**.

[2] 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**.

[3] D.Boneh and M. Franklin. "Identity-Based Encryption from the Weil Pairing." Proc. of CRYPTO'01, Santa Barbara, California, USA, **2001**.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy Attribute Based encryption," in IEEE S& P '07, **2007**, pp. **321- 334**.

[5] Ramasamy S, Vahidhunnisha, " Survey on Multi Authority Attribute Based Encryption for Personal Health Record in Cloud Computing", International

Journal of Latest Trends in Engineering and Technology, November **2013,** pp.**223- 229**.

[6] Herzberg etc, "proactive secrete sharing(PSS)," in **1995**

[7] Cheng-chir Lee, Pei-shan C," A survey on ABE scheme of Access control in cloud environment, vol.15, no.4, July **2013**, pp.**231-240**.

[8] Huang Lin, Zhenfu Cao, Xiaohui Liang, Jun Shao,"Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority," INDOCRYPT, **2008,** pp**. 426-436**.

[9] Neetha Xavier, "Security of PHR in cloud computing using ABE technique", International Journal of Communication and Computer Technologies, volume 01-No.72 issue: 07, Nov **2013,** pp. **265-269**.

[10] S.Jahid, P.Mittal, N.Borisov,"Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACMSynp. Information, Computer and Comm.Security, Mar **2011**.