A Survey New: Attribute-Based Encryption for Personal Health Records in Cloud Computing

Anitha A[#1], Thamaraiselvi k[*2]

[#] *PG Scholar ,Department of Information Technology, SNS College of Technology Coimbatore-35, Tamilnadu, India*

[1]anitha.it2011@gmail.com

[*]*Assistant professor ,Department of Information Technology, SNS College of Technology Coimbatore-35, Tamilnadu, India*

[2]siva.thamarai@gmail.com

***Abstract*— Personal Health Record (PHR) service is an emerging model for health information exchange. PHR system allows patients to create, control manage, and share their health information with other users as well as healthcare providers like Google eHealth. In reality, a PHR service is likely to be hosted by third-party cloud service providers in order to enhance its interoperability. Meanwhile, there have been serious privacy concerns about outsourcing patients PHR data to the cloud server. Issues such as risks of privacy exposure, scalability in key management, data loss, flexible access efficient user revocation and data theft, have remained the most important challenges toward achieving cryptographically enforced data access control. To achieve fine-grained and scalable data access control for PHR service, Attribute-Based Encryption (ABE) techniques is used to encrypt each patient's PHR file. In Key Policy Attribute-Based Encryption (KP-ABE), a single data owner can encrypt her data and share with multiple authorized users by distributing keys to them. KP-ABE achieves low amortized overhead. Multiple-authority attribute-based encryption (MA-ABE) has multiple trusted authorities, each governs different subset of the system user attributes. Sometimes the credentials from different organization should be treated equally, it is not possible in MA-ABE. So the Distributed Attribute-Based Encryption (DA-ABE) can be used in such cases.**

***Keywords*— Personal health records, cloud computing, data privacy, access control, attribute-based encryption**

I. INTRODUCTION

This The term Personal Health Record (PHR) has undergone substantial changes along with the emergence of cloud computing. A PHR is a set of computer-based tools that allow people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it. Most healthcare information technology vendors and healthcare providers started their PHR services as a simple storage service, and then they moved into a complicated social-network like service for patients to share personal health information with others. However, patients' greatest concern about PHR system, as well as other healthcare system, is security and privacy. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 outlined the legal protections for PHR privacy and security. But, this act does not address all the issues involved. Therefore, by introducing cloud computing into PHR service, there are several important privacy issues. However, by outsourcing PHR into a third party cloud service provider, patients lose physical control to their own healthcare data. PHR file residing on a cloud server are subject to more malicious insider and outsider attacks than paper-based records. Hence, to provide strong privacy assurance other than directly placing those sensitive data under the control of cloud servers [2].

II. ENCRYPTION METHODS

Encryption techniques for personal health records in cloud compuitng literature review as follows..

A. Attribute-Based Encryption

Attribute-Based Encryption (ABE) [3], a generalization of identity-based encryption that incorporates attributes as inputs to its cryptographic primitives. Data is encrypted using a set of attributes so that multiple users who possess proper can decrypt.Attribute-Based Encryption (ABE) not only offers fine-grained access control but also prevents against collusion [2].

One disadvantage of encrypting data is that it severely limits the ability of users to selectively share their encrypted data. Suppose a particular user wants to grant decryption access to a party to all of its Internet track logs for all entries on a particular range of dates that had a source IP address from a particular subnet. The user either needs to act as an intermediary and decrypt all relevant entries for the party or must give the party its decryption key and to have access to all entries. Neither one of these options is not applicable. An important setting where these issues give rise to serious problems is audit logs [4].

Sahai and Waters [5] made some initial steps to solving this problem by introducing the concept of Attributed-Based Encryption (ABE). In an ABE system, a user's keys and ciphertexts are labeled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key.

1)Drawbacks: In [6], Akinyele et al. investigated using ABE to generate self-protecting EMRs, which can either be

stored on cell phones or cloud servers so that EMR could be accessed when health provider is in offline also. However, there exist several common drawbacks the above works discussed. First, assuming the use of a single trusted authority(TA) in the system. Single trusted authority (TA) not only creates a load bottleneck, but also have key escrow problem since the TA can access all the encrypted files. This opens the door for potential privacy exposure [1].

B. Key- Policy Attribute-Based Encryption

Yu et al. (YWRL) applied key-policy ABE to secure outsourced data in the cloud [7], [8], where there will be single data owner who can encrypt his data and share with multiple authorized users by providing decryption keys to them. Key contains the attribute-based access privileges. Yu et al. (YWRL) also propose a method for the data owner to revoke a user efficiently by delegating the updates of affected ciphertexts and user secret keys to the cloud server.

KP-ABE [9] is a public key cryptography primitive for one-to-many encryption. In KP-ABE, data are associated with attributes that will have the public key component. The encryptor/owner associates the set of attributes to the message by encrypting it with the corresponding public key components. Each user/clients is assigned an access structure which is usually defined as an access tree that contains the data attributes in which the interior nodes of the access tree are threshold gates and leaf nodes are associated with attributes. User secret key is defined based on the access structure so that the user is able to decrypt a ciphertext if and only if the data attributes satisfy his access structure.

1) Drawbacks: In KP-ABE, the key update operations can be aggregated over time, YWRL scheme[7] achieves low amortized overhead. Meanwhile in the YWRL scheme [7], the data owner is also a TA at the same time. It would not be efficient to apply in the PHR system with multiple data owners and users. Since each user would receive many keys from multiple owners, even if the cryptographic keys contain the same set of attributes.

C. Ciphertext Policy Attribute-Based Encryption

In the Ciphertext Policy Attribute-based Encryption (CP-ABE), the private key is distributed to users by a trusted central issuer only once. The keys are identified with a set of descriptive attributes, and the encrypter specifies an encryption policy using an access tree so that those with private keys which satisfy it can decrypt the ciphertext.

Ciphertext Policy Attribute-based Encryption (CP-ABE) [10], can be widely applied to realize access control in many applications including medical systems and education systems

X.Liang [10] aimed at developing the CP-ABE scheme with efficient revocation. Designing a revocation mechanism for CP-ABE is not a simple task while considering the following aspects: first, system manager only associates user secret keys with different sets of attributes instead of individual characteristics ; second, users' individuality are taken place by several common attributes, and thus revocation on attributes or attribute sets can not accurately exclude the users with misbehaviors; third, the system must be secure against collusion attack from revoked users even though they share some common attributes with non-revoked users.

1) Drawbacks: CP-ABE systems can support only uncontrolled delegation [12] (the delegator cannot prevent the delegatee to delegate further his authority), or use a system where attributes are valid within a specific time frame [13] (there is no way to revoke an attribute before the expiration date).

D. Multiple-Authority Attribute- Based Encryption

Chase and Chow [14] proposed a multiple-authority ABE (CC MA-ABE) solution in which there will be multiple TAs, each governs a different subset of the system' users' attributes and generate user secret keys collectively. A user needs to obtain one part of his key from each TA. Chase and Chow scheme prevents collusion among at most N-2 TAs.

Lin et al. [15] recently proposed a different approach for building a multi-authority ABE scheme without a central authority. However, their construction requires designers to fix a constant m for the system, which directly determines efficiency. The resulting construction is such that any group of m + 1 colluding users will be able to break security of the encryption.

1) Drawbacks: In CC MA-ABE [15], access policy is embedded in user keys not in the ciphertext and it is non-intuitive approach. Already issued private keys can never be modified until the whole system crashes and cannot able to distinguish the same user in different transaction. Data access right could be given based on user's identities and lack of expressibility in access policy.

E. Distributed Attribute - Based Encryption

Sascha Muller [17], introduced a concept of Distributed Attribute-Based Encryption (DABE). In DABE, there will be an arbitrary number of parties to maintain attributes and their corresponding secret keys. In CP-ABE schemes, where all secret keys are distributed by one central trusted party. There are three different types of entities in a DABE scheme: a master, attribute authorities and users.

The master is responsible for the distribution of secret user keys. However, master is not involved in the creation of secret attribute keys.

Attribute authorities are responsible to verify whether a user is eligible of a specific attribute; in this case they distribute a secret attribute key to the user. An attribute

authority generates a public attribute key for each attribute it maintains; this public key will be available to all the users. Eligible users receive a personalized secret attribute key over an authenticated and trusted channel.

Users can encrypt and decrypt messages. To encrypt a message, user should formulate the access policy in Disjunctive Normal Form (DNF). To decrypt a ciphertext, a user needs at least access to some set of attributes (and their associated secret keys) which satisfies the access policy.

III. CONCLUSIONS

Addressing the security and privacy concerns of cloud-based PHR system by integrating advanced cryptographic techniques, such as ABE, into PHR system. By using appropriate cryptographic techniques, patients can protect their valuable healthcare information against partially trustworthy cloud server. Meanwhile patients gain full control access over their PHR files, by defining fine-grained, attribute-based access privileges to selected data users.

Anonymous attribute-based privilege control scheme AnonyControl can be used to enhance the user privacy problem in cloud. Using Distributed Attribute-Based Encryption (DABE) in the cloud computing system, it achieves anonymous cloud data control and also fine-grained privilege control for cloud computing.

REFERENCES

1. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou, "Scalable and Secure sharing of personal health records in cloud computing using Attribute-based Encryption" in IEEE transaction on parallel and distributed systems,2012.

2. "Privacy-preserving personal health record system using attribute-based encryption," Master's thesis, WORCESTER POLYTECHNIC INSTITUTE, 2011.

3. Sahai and B. Waters, "Fuzzy identity based encryption. In Eurocrypt 2005", 2005.

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. Sahai and B. Waters. "Fuzzy Identity Based Encryption", In *Advances in Cryptology Eurocrypt*, volume 3494 of *LNCS*, pages 457-473. Springer, 2005.

6. J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano, Z. N. J. Peterson, and A. D. Rubin, "Self protecting electronic medical records using attribute based encryption," Cryptology ePrint Archive, Report 2010/565, 2010, http://eprint.iacr.org/.

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. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *ASIACCS'10*, 2010.

9. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute based encryption for fine-grained access control of encrypted data," in *Proc. Of CCS'06*, 2006.

10. X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," *Technical Report, University of Waterloo*, 2010.

11. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext policy attribute-based encryption," in *IEEE S& P '07*, 2007, pp. 321–334.

12. 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.

13. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure attribute-based sys- tems. *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pages 99 112, 2006.

14. M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *CCS '09*, 2009, pp.121–130.

15. Huang Lin, Zhenfu Cao, Xiaohui Liang, and Jun Shao., "Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority. In *INDOCRYPT*, volume 5365 of *LNCS*, pages 426–436. Springer, 2008.

16. Taeho Jung, Xiang-Yang Li and Zhiguo Wan, "Privacy Preserving Cloud Data Access With Multi-Authorities", in http://arxiv.org/abs/1206.2657v5 , 2012.

17. Sascha Muller, Stefan Katzenbeisser, and Claudia Eckert, "Distributed Attribute-Based Encryption", in LNCS 5461, pp. 20 - 36. Springer,2009.