Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORD IN DISTRIBUTED SYSTEM: ABE AND KEY MANAGEMENT

MayuriPawar[1], JayaMali[2], JayashriPawar[3], AnkitaPatil[4]
[1,2,3,4] *Computer Department, KKWIEER Nashik*

Abstract- The security of personal health records is a major problem when patients use commercial Web-based systems to store their health records. Previous access control techniques have many limitations with respect to enforcing access control policies and ensuring data security. In particular, the data has to be stored on a distributed server protected by the access control mechanism and the data owners or patients loses control on their health data from the moment when the data is stored on the server. Therefore, these mechanisms do not fulfill the requirements of data outsourcing scenarios where the unauthorized party storing the data should not have access to the unencrypted data and it is not trusted to enforce access policies. In this paper, we present a new type of attribute-based encryption that is multi-authority attribute-based encryption (MA-ABE) scheme which is used to enforce patient/organizational access control policies. In MA-ABE [8] [9], the data is encrypted according to an access policy over a set of attributes. The various access policy specifies which attributes a user needs to have in order to decrypt the encrypted data. Once the data is encrypted, it can be safely stored in an untrusted distributed server such that every user can download the encrypted data but only authorized users who satisfy the access policy can decrypt. The originality of our construction is that attributes can be from two security domains: personal domain (e.g. family, friends) and private domain (e.g. hospital staff, insurance company).

Keywords- Personal Health Record, Data privacy, Attribute-Based Encryption, Fine-Grained Access Control, MA-ABE.

I. INTRODUCTION

Now a days, the healthcare delivery has exponentially extended from acute institutional care to outpatient care and home healthcare. Healthcare services can now be availed at a distance due to the advances in communication and information technology. Besides these, there are a number of initiatives for adoption of electronic health records (EHRs) from different governments around the world as well as from the private sector for adoption of personal health records (PHR). While EHR systems function to serve the information needs of health care professionals, PHR systems capture health data entered by individuals and provide information related to the care of those individuals. There are number of web services that an individual can use to store her PHRs including the prominent examples of Microsoft HealthVault, Google Health or WebMD. They allow individuals to enter, store and share their own health data, upload health measurements from their devices, but also to import their health records from hospital EHR systems [5] [6].Despite numerous initiatives by industry and a number of standards under development to provide the interoperability across different PHR and EHR services, confidentiality of patient's health information remains a major obstacle with respect to the adoption of the PHRs by the individuals.

Access-control mechanisms are very important to protect the confidentiality of electronic health records [5] [6]. They comprise a very large set of technologies, which include mechanisms to authenticate and authorize individuals or systems to access resources. Many consumers hesitate to upload their health data to commercial PHR systems since they do not trust access control mechanisms provided by these companies. Next to that, in modern healthcare, where a lot of IT

functionality gets outsourced, patients are worried if their health data will be treated as confidential by companies running data centers. The problem addressed in this paper is the confidentiality of PHRs. Patients records contains sensitive information such as details of a patient's disease, drug usage, sexual preferences, etc. Inappropriate disclosure of a record can change patient's life, and there may be no way to repair such harm financially or technically.

Therefore, it is crucial to protect patient's health records when they are uploaded and stored in commercial Web-based systems [2].Our scheme allows a patient to store her PHRs in an encrypted form on a commercial PHR system and share them securely with other users who belong to two different security domains personal domain (e.g. family, friends) and private domain (e.g. doctors, nurses, insurance company).

II.LITERATURE SURVEY

Role-Based Access Control(R-BAC) - Role-based access control [10] prevents unauthorized access and provides secure accessing of information. A person is restricted from accessing the data other than he has the right for. Also he can access the data according to the role assigned.

Cipher-text Policy Attribute-Based Encryption (CP-ABE): Using this algorithm [11], encrypted data can be kept confidential and secure even if the server is untrusted also this prevents collusion attack.

Key Policy Attribute-Based Encryption (KP-ABE):In this algorithm[12],the primitive enables the senders to encrypt messages under a set of attributes and private keys are associated with access policies that is access structure in this context that specify the cipher text the key holder will be allowed to decrypt.

Adaptively Secure	Std. Model	Prevent Decryption by Individual Authorities	Support Large Attribute Universe	Expressiveness
Yes	Yes	Yes	Yes	Expressive
No	Yes	Yes	Yes	Limited
No	Yes	No	Yes	Limited
Yes	No	Partially	No	Limited

Table 1. Comparison of ABE Systems

III. ABE FOR PERSONAL HEALTH RECORD

This paper recount the scalable and secure sharing of patient centric health record on semi-trusted server.

3.1. Problem Definition

In PHR system where there are multiple PHR owners (patients) and users .The owners refer to patients who have full control over their own PHI (Personal Health Information).They can create, manage and delete records. The distributed server belonging to the PHR service provider that stores all the owners PHR data. Users can access the PHR documents through the server in order to access someone's PHI data, and a user can simultaneously have access to multiple owners data according to the rights assigned to them [6].The users may come from various categories like a friend, hospital staff. The PHR records can be handled by multiple users. This guides need of MA-ABE [8] [9].

3.2. Attribute Revocation

The PHR system should support users from both the domains: Personal domain and Public domain. Since set of users in public domain may be enormous and incalculable, the system should be highly scalable in terms of entanglement in key management, storage, computation and communication [1] .The PHR owner's effort in managing users and keys should be minimized to enhance usability.

3.3. Fine-grained Access Control

Fine-grained access control [7] should be compulsory. This states that various PHR users are approved to access or read different PHI records [1].PHR is accessed with systematic key management. If the attributes which are assigned to PHR users are no longer valid then that PHR user will not be able to access the PHR records in future.

3.4. Data Confidentiality

The crucial requirement of PHR system is sharing. PHR owner or patient have control to his own PHR. Patient on its own decide that which users are allowed to access the PHR.

IV. ALGORITHM

Multi-Authority Attribute-Based Encryption (MA-ABE) [8] [9] is a type of attribute-based encryption scheme which can be used to enforce access policies cryptographically. In MA-ABE, the data owner encrypts the data according to an access control policy P defined over a set of attributes, and the receiving end can decrypt the encrypted data only if his secret key associated with a set of attributes satisfies P. For example, suppose Alice encrypts her data according to an access policy P= (al AND a2) OR a3. Bob can decrypt the encrypted data only if his secret key is associated with a set of attributes that satisfy the access policy. To satisfy P, Bob must have a secret key associated with at least one from the following attribute sets: (ab a2), (a3) or (al, a2, a3)' In general, MA-ABE scheme consists of four algorithms:

4.1. Setup algorithm (MK, PK)

Setup (1 k): is run by the trusted authority or the security administrator. The setup algorithm takes as input a security parameter k and outputs a master secret key MK and a master public key PK.

4.2. Key Generation algorithm (SK)

Key Gen (MK, ffi): is run by the trusted authority, and takes as input a set of attributes wand MK. The algorithm outputs a user secret key SK associated with the attribute set w.

4.3. Encrypt algorithm (CT)

Encrypt (m, PK, P): is run by the encryptor. The input of the algorithm is a message m, a master public key PK and an access control policy P, the output of the algorithm is a cipher-text CT encrypted under the access control policy P.

4.4. Decrypt algorithm (m)

Decrypt (CT, SK): is run by the decryptor. The input of the algorithm is a cipher-text CT to be decrypted and a user secret key SK. The message m is a output of an algorithm, if the attribute set of the secret key satisfies the access policy P under which the message as encrypted, or an error message if the attribute set of the secret key does not satisfies he access policy P under which the message was encrypted.

V. RESULT

File Size (KB)	Encryption Time (msec)	Decryption Time (msec)
800	12827	3516
500	9089	2869
150	3803	1639
100	2563	982

Table 2. Result data

VI. CONCLUSION

As suggested in paper, secure management of personal health records which are stored and shared from an un-trusted web server is managed. The MA-ABE scheme has shown to be a useful tool in a healthcare setting since the access policy is enforced by virtually associating the access control policy to the protected data. This removes the need for involving a trusted entity which has to enforce access policies. A possible future work is to provide a formal security proof for the proposed scheme.

REFERENCES

[1] 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 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-Health Cloud," 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 Keyword Search over Encrypted Personal Health Records in Cloud Computing," 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] K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287, Feb. 2001.

[6] 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.

[7] 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.

[8] 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.

[9] Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption," master's thesis, Worcester Polytechnic Inst., 2011.

[10] M.Yamaguchi,M.Imazato,S.Moromugi and T.Ishimatsu ," A Robot Chair for Mobility at Steep and Narrow stairways," International Conference on Control,Automation and Systems 2007.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.

[12] Jin Sun,Yupu Hu and Leyou Zhang," A Key-Policy Attribute-Based Broadcast Encryption," The International Arab Journal of Information Technology, Vol. 10, No. 5, September 2013.

