Security in Cloud computing Using Attribute Based Encryption: Proxy Re-encryption

Ms. Dipali L.Patil

Computer Engineering, Jspm's ,RSCOE, Tathwade,

Savitribai Phule Pune University

Pune, India

ABSTRACT

In today's world securing personal health record (PHR) is an up-coming model in sharing the information about health. PHR system offers different features to view health data, secure communication with the providers, new entry of data, securely transfer health data. Patients have whole control over their health record and share that with the system providers and users. Patients have control over their own health care record can effectively share their health data with the other users. A PHR service is operated by the semi-trusted cloud service providers. More privacy required for health record stored on cloud servers, because of increasing number circumstances happened in recent years with the cloud data. In present system, Encrypted PHRs are stored on semi-trusted servers such that sensitive PHR's does not accessed by the server. Patients can have rights to use their PHR by assigning attribute-based access, fine grained access constitutional rights to selected data users.

Index Terms - Attribute based encryption, Cloud computing, Fine grained access control, KP-ABE, Proxy re-encryption,

1. INTRODUCTION

Today in computer technology more peoples were attracted over to store their secret data on third-party server called cloud provider. So it need to be stored securely on third party server. The sensitive data stored on public cloud and is also operated by un-trusted cloud service provider. By emerging PHR service into the cloud, several issues related to the privacy and security about PHR gets better resolved. This method is better than traditional paper record to keep security in PHR. But when PHR resides on cloud there can be possibility of malicious attacks. Need to apply cryptography techniques on sensitive data before outsourcing PHR. Applying the cryptographic scheme over PHR gives more security to access and share PHR. Key management is the main problem to achieve fine-grained access control when PHRs are encrypted with symmetric key or asymmetric key cryptography scheme.

PHR owners should make a decision how to encrypt data and how many users can access data. The users whom allowed for accessing PHRs can only access data; however the users whom having the decryption key can decrypt encrypted data. Only authorized users allowed to access PHR for the personal use or professional use. There are two types of users one is personal user and other is professional user. Attribute-based encryption (ABE) as a encryption technique. Users are classified depending upon their attributes, like professional roles (pharmacist, doctor). Owner (patient) can encrypt own PHR data by using some attributes, and user who satisfy attributes set are permitted to read those data. Lot of efforts required to manage professional users. So there is key management in cloud. It is unpredictable for owner to list out professional users.

There are multiple owners who encrypt their data with different set of keys. The user who wants PHR, they required to obtain key from the owner because patients are not always online. One alternative is to maintain central authority who is responsible for key management. But disadvantage is that central authority is semi-trusted. PHR may be stored on a different location, such as an Internet database, a provider's PHR, the owner's personal computer, transportable devices such as a smart card or a privately maintained database. While patients can access their own data, but always they do not look for anyone else may access it. In professional domain more no of users are their because of that security problem arises as well as key management is also very complex task. To solve this problem multi-authority attribute based encryption (MA-ABE) is used. Because of that there may be no. of attribute authority .only single authority is not responsible for controlling whole system, this technique is achieved by role based encryption technique.

2. METHODOLOGY

2.1. Attribute Based Encryption

The one of the encryption technique used to store data on semi-trusted server is attribute based encryption (ABE). There are two schemes for ABE (1) KP-ABE and (2)CP-ABE such that key policy attribute based encryption and cipher-text policy attribute based encryption respectively. The difference between two schemes is the system use attributes to depict the user's private key or encrypted data. Normally CP-ABE is correlated to RBAC; while KP-ABE is more related to ABAC [1].ABE allows fine grained access control and data protection. It is not possible for the owner to find each and every user who operates the file. So it is required to find attributes universe which can distinctly define each user. If there is no proper attribute universe then it becomes problematic. There requires trusted authority must be responsible for protecting master key and generating private key for user.

Present PHR system provides the functionalities as follows:

Add User-access: Patient have rights to add attributes of health care provider to provide access to the patient's health data.

ISSN: 2278 – 1323

Revoke User-access: Health care provider's access can be revoked by system to the patient's health information without re-encrypting the data.

Delegation: Health care providers have the ability to delegate access generating the private key for any set of attributes they hold.

Keyword Search: Cloud server does not alert about the keyword but the providers have rights to search a patient's record. The result returned by the server which matches to the query.

Security: The must provide data confidentiality. Files required in encrypted form and authorized users by the owner can decrypt the PHR data.

Privacy: The system must be confident about, they does not read anything from files stored on cloud server as well as which search is provided by the user.

ABE based on access controls and policies which include mechanisms to authenticate and authorize users of system [7]. The access-control mechanisms provide data confidentiality. RBAC is mechanism in which some person have specific role e.g. doctor, nurse, pharmacist. Attribute-based access control is a mechanism where the access is based on set of attributes.

2.1. Requirements of PHRs service

1. **Data confidentiality:** Unauthorized users who do not have attributes fulfilling the access rights should be prohibited from decrypting a PHR file, as well as checked for user collusion. Fine-grained access control is achieved means unusual users are authorized to examine different sets of files.

2. **On-demand revocation:** Each time the attributes of the user is no longer valid, then user should not able to access PHR files in future by using previous attribute called as revocation of attribute. User revocation is also one of revocation where the user access privileges are revoked.

3. **Write access control:** Prevent an unauthorized user from write access control.

4. **Policies :** Policies should be easy to change, PHRs should be accessible under emergency scenarios as well as to users who need it.

5. **Scalability, efficiency, and usability:** There are two types of domain in PHR system personal domain and professional domains. Since the large no. of users are in professional domain, the system should be capable for the managing as well as for storage . For usability the hard work required for users and keys management should be minimized.

2.2. Key Policy Attribute Based Encryption

KP-ABE is a public key cryptography primitive for one-to-many communications. In KP-ABE, data are associated with attributes for each of which a public key component is defined. The owner associates the set of attributes to the message by encrypting it with the corresponding public key components. Each user is assigned an access structure which is usually defined as an access tree over data attributes. User secret key is defined to reflect the access structure so that the user is able to decrypt a cipher text if and only if the data attributes satisfy his access structure. A KP-ABE scheme is composed of four algorithms which can be defined as follows:

Setup This algorithm takes as input a security parameter κ and the attribute universe $U = \{1, 2, \ldots, N\}$ of cardinality N. It defines a bilinear group G1 of prime order p with a generator g, a bilinear map $e : G1 \times G1 \rightarrow G2$ which has the properties of *bilinearity*, *computability*, and *non-degeneracy*. It returns the public key *PK* as well as a system master key while *PK* is publicly known to all the parties in the system; *MK* is kept as a secret by the authority party.

Encryption This algorithm takes a message *M*, the public key *PK*, and a set of attribute *I* as input. It outputs the cipher text *E*.

Key Generation This algorithm takes as input an access tree *T*, the master key *MK*, and the public key *PK* .It outputs a user secret key *SK* .

Decryption This algorithm takes as input the cipher text *E* Encrypted under the attribute set *I*, the user's secret key *SK* for access tree *T*, and the public key *PK*.

2.3. Proxy Re-encryption technique

Proxy re-encryption scheme is cryptographic system which allows third parties to revise a cipher-text encrypted for one of the party. Basically the proxy re-encryption is used when sender, wants to disclose message contents sent to him and that is encrypted with his public key to the third party, without enlightening his secret key to third party. Receiver expects that the proxy must not read his messages. Sender could delegate to a proxy to re-encrypt single of his messages that is to be sent to third party. This process creates a fresh key that third party can use to decrypt the message. Now if sender sends a message to the third party that was encrypted under receiver's key, then proxy will alter the content of the message, allow third party to decrypt. This method is used in a many applications such as email, content sharing etc.

ISSN: 2278 – 1323

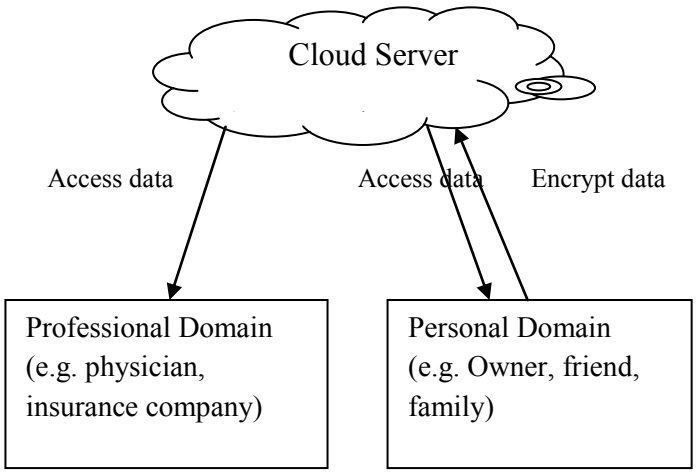

Figure 1: Architecture of PHR System

3. CONCLUSION

Here we studied the secure cloud-based PHR system by emerging advanced cryptographic mechanisms, such as ABE, PHR system. With the help of suitable cryptographic techniques, patients keep their sensitive health information secure against third party un-trusted cloud server. Patients achieve full control over access to their PHR files, by assigning fine-grained, attribute-based access rights to selected data users. Here users divided into two domains and sharing PHRs from different domains.

REFERENCES

[1] S. Yu, W. Lou, M. Li and K. Ren, "Securing Personal Health records in Cloud Computing," 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] S. Yu, K.Ren, C. Wang, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM '10, 2010.
[5] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security,vol. 19, pp. 367-397, 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] S. Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure," Proc. ACM Cloud Computing Security Workshop (CCSW '10), pp. 47-52, 2010.
[8] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," technical report, Univ. of Twente, 2009.

ISSN: 2278 – 1323