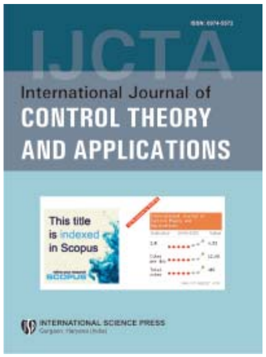

International Journal of Control Theory and Applications

ISSN : 0974–5572

© International Science Press

Volume 9 • Number 40 • 2016

A Secure Data Sharing Scheme for Preserving Privacy in a Cloud Environment

Prabha V.S.N. Vinay Kumar[a] and K. Venkatesh[a]

[a]Department of Information Technology, S.R.M University Chennai, Tamil Nadu-603203

E-mail: pvsnvinay@yahoo.com, Venkatesh.k@ktr.srmuniv.ac.in

Abstract: With the popularity of data sharing in public cloud environments, the security and integrity of shared data have become one of the major issues. The cloud service provider is a third party service provider and cannot be trusted completely of its semi-trusted nature, and hence the common security models cannot be directly integrated into cloud based data sharing frameworks. The aim of this paper is to propose a novel secure way in which the data owner need not share any key information with the cloud service provider who is the third party, by implementing a token system using with the help of proxy re-encryption server and attribute based encryption mechanism is used to provide access to the users based on their groups hence privacy, security and an fine grained access to data is provided to the users in the cloud environment.

Keywords: *Proxy re-encryption, Token, Attribute based encryption, Fine grained access, Privacy.*

1. INTRODUCTION

Cloud Computing provides the chance to convert information technology from cost based scenario to a strategy based driven scenario. The services provided by the cloud can be divided into three types: Software-as-a-service (SaaS), Platform-as-a-service (PaaS) and Infrastructure-as-a service (IaaS). Among these three services, Infrastructure-as-a-service (IaaS) is the most popular and it provides cloud storage service which is widely used everywhere. In the present scenario Cloud storage has become a constant solution to provide flexible, on-demand and easy access to huge amounts of information which is shared on the Internet. However, while utilizing the leverage of sharing information with the help of cloud storage, users are also more worried about the possible leaks of data in the cloud. [1] Such leaks of data can be from a misbehaving or a malicious cloud operator, can lead to many serious breaches of personal privacy or secrets of the business (*e.g* ,The Photos of high profile celebrities being leaked through iCloud).But still many of the individuals and Companies would prefer to store their information in the cloud environment as it is very cost effective and provides huge data storage service. To avoid these threats the data needs to be encrypted before sending the data to cloud storage and the access to the data should be given to legit users. A fine-grained access [2] should be provided for the users to access the data. The access control should be more flexible, a user performing different roles in the organization should be granted access to all the data that is required to perform those roles in the organization.

For instance, a dean in a hospital should be access the cases related to all the departments in the hospital. Hence access control should be flexible in designing the user's privileges to perform operations on the data, which helps the user to perform all his roles successfully.

An important feature of data storage should be is to ensure the confidentiality is provided to the data that is stored. There are some existing cryptographic encryption mechanisms [3], which can be used to encrypt the data multiple number of times before storing the data in the cloud. This leads to the challenge of storage and distribution of the keys among the users.

Even though encrypting the data is a foremost solution for providing confidentiality to the data but it reduces efficiency while utilizing the data. [2] Data owner shares data related to multiple users, even though the receiver is interested in data which is related to him. For instance, the hospital stores the data related to its patents on cloud storage, but a doctor who is an ENT specialist is interested to view the data related to the ENT patents. The easiest way is to download the files and decrypt them locally to find the required information. But this so is not a practical solution as huge bandwidth cost is involved in downloading all the files and lot of computations should be made to decrypt [4] the entire data related to the user which will be an overhead. To utilize the data more efficiently, user must be given access to send a request by performing "Query" on cloud service provider for getting the data required. Cloud service provider should perform a search on entire encrypted data for user's query and give the required response. This leads to privacy issues like the CSP or the user might be able to get any sensitive information related to data- consumer or data-owner from the query.

Consider a scenario in which a hospital stores the medical records and information related to patients in the cloud storage environment and the data is encrypted multiple number of times to secure the privacy of the data, but a lot of time and storage is being wasted to distribute and store these key details.

aim of the research is to solve the above problems. To preserve privacy and confidentiality of the information related to the users by implementing a token mechanism.

2. BACKGROUND

This section reviews the attribute based encryption, proxy re-encryption and the existing scenario in cloud environment based on the background analysis.

2.1. Attribute Based Encryption

To provide fine grained access to the attribute based encryption (ABE) was introduced and one to many encryption. In ABE, the attribute is related to the user's information like the users ID, Role etc. These attributes are mainly used to create two major elements in ABE, *i.e*. access policies and group of attributes. [5]The access policy is used to avoid unauthorized users from accessing the information. There are mainly two types of ABE, *i.e*. KP-ABE and CP-ABE. In KP-ABE the encryption of the message is done based on the attributes by the data owner and the key is granted by the key generation authority based on the access policy [6]. In Attribute Based Encryption, the information is stored on storage in the encrypted form, the users can decrypt different parts of the data as per the attributes or the requirements of the users. This helps in eliminating unauthorized access to the data and provides more efficient data access to the users. In this paper the encryption and decryption of data is done based on attributes using KP-ABE.

2.2. Proxy Re-Encryption (PRE)

Proxy Re-Encryption (PRE) is a cryptographic method, using which the proxy server will be converting cipher text encrypted under one user into a token using which the other user can decrypt the information [7]. It is a semi-trusted server so it should not have original plain text in proxy server. The user should update the secret key component to the server. Proxy re-encryption is similar to symmetric and asymmetric encryption, it has an additional 2 extra function:

1. **Delegation:** It allows the key owner to create a re-encryption key, using his own private key and the public key of the other user. The function is re-encrypted by the proxy using this new key. It can be used both in uni-directional and bi-directional way. A uni-directional is a one-way method, it is composed in such a way that the key holder need not give away his secret key. A bi-directional way is reversible, the secret keys of the key holders must be shared using which a new re-encryption key is generated.
2. **Transitivity:** Transitive proxy re-encryption gives the option for a ciphertext to be re-encrypted as many number of times as we need. For example, a ciphertext can be re-encrypted from mary to alen and then from alen to Charles and so on. Non- Transitive methods can be used to perform re-encryption on the cipher text only limited number of times. [7] Transitive proxy re-encryption can only be used only in the bi-directional way.

2.3. Present scenario of cloud computing

In the present one of the major issues faced by the cloud is to provide privacy to its user, to save the privacy of the clients, data is being encrypted multiple number of times by the cloud service providers and clients in order to secure the privacy of the data, in this process they are making it very complicated process to manage the encryption and the decryption keys, related to the data.[8] Hence lot of time is wasted to encrypt and decrypt this data and memory is wasted to store these keys. Created by Mambo and Okamoto [9] and further expanded as Proxy Re-Encryption (PRE), which is proposed as an effort to solve the problem of data sharing. The proxy Re-Encryption (PRE) allows a semi-trusted party, called proxy, to maintain and distribute the keys by generating a token without leaking the knowledge of message. Now the overhead of the Data Owner will be transferred to the Proxy Re-Encryption server. In order to solve this problem proxy based re-encryption along with attribute based encryption will be implemented using which no keys will be shared between the data owner and the cloud service provider. [10]

3. PROPOSED WORK

To Deploy an novel system in which the Data owner need not share any key information to the third party cloud service provider and to implement attribute based encryption due to which only specific people will be able to access specific kind of data and try to send the tokens to the user to access the encrypted data, these tokens will be generated using proxy based re-encryption with RSA token mechanism and stored using Amazon Simple Storage Service, provided by the Amazon Web services. The proxy based re-encryption server will share this key information with user, using Token mechanism and reduces the overload from the data owner and only the public key information is shared with the cloud service provider (CSP), Secret keys are stored in the Proxy server, using which the proxy server generates a token using RSA token mechanism whenever a request is generated by the user for the data and is sent to the user using which the user can decrypt the data, Hence the privacy of the user information is preserved without sharing any secret key information with the third party cloud service provider.

4. SYSTEM DESIGN

4.1. Data Owner

Data owner will be encrypting the data using attribute based encryption mechanism, in which the details related to each user will be considered as a separate attribute and a key will be generated using which the information related to the user can be Decrypted, which helps in maintaining the integrity of the information related to the users and provide security. The Encrypted information will be stored in the amazon simple storage service (S3) storage and the Private Key will be sent to the Proxy Based Encryption Server.

4.2. Proxy Based Encryption Server

The Proxy Based Encryption server will be used to generate a token using RSA Token mechanism [11] using the private key of the encrypted data, whenever a user requests for the information. This token will be sent to the user to decrypt the information and can only be used to decrypt the data only once. Whenever a user requests to access the data, a new token will be generated and is sent to the user using which he can decrypt the data. This helps in preserving privacy of the users.

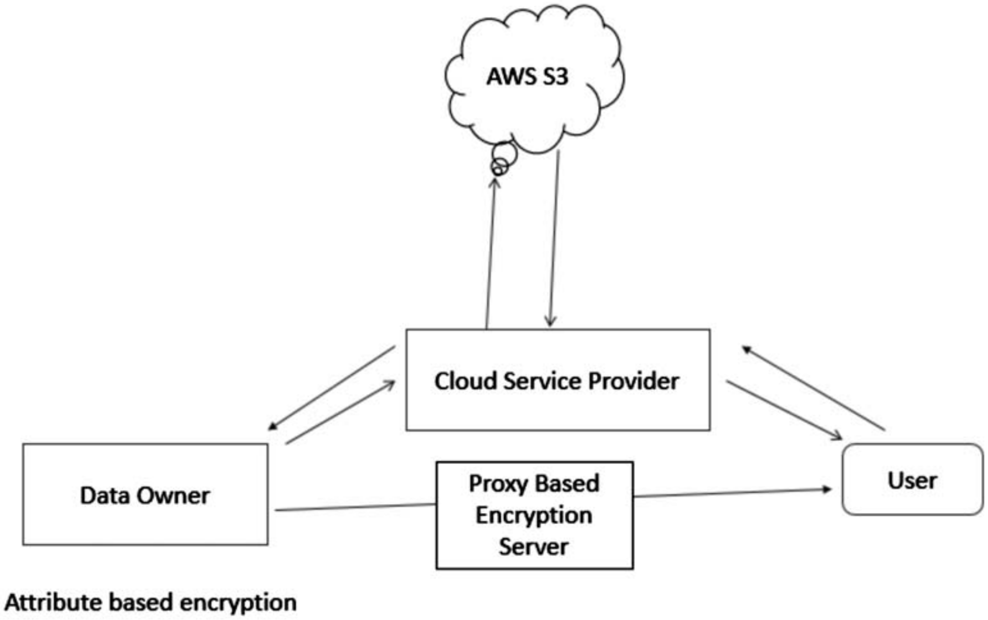

Figure 1: System Design

4.3. Amazon cloud

The Amazon cloud environment provides request authentication, servicing the requests, backup operation execution, bucket and object management, implementing the related simple storage service (S3) bucket policies. It also provides the choice of selecting a region in which the data can be stored, which is near to the geographical location of the Data owner. [12]

4.4. System Description

The system mainly consists of four groups (proxy server, data owner, cloud service provider (CSP), user). The following is the description of the system.

1. **System Setup:** The public key, master key, system attribute set T is generated by the Data owner
   a) Public key PK = $(Z, A_1, A_2 \ldots, A_n)$
   b) Master key MK = $(z, a_1, a_2, a_n T)$
   c) Attribute set T = $(t_1, t_2, \ldots, t_n)$
2. **New File Creation:** Data owner will generate the header $(I, F_1, \{F_i\}_{ieI})$ and body $(H.g^{H(r\|t)})$ and sends the header to the proxy server and the body to CSP.
3. **New User Creation:** The Data owner can assign the access to the new user if he wants to join the system.

4. **File Access:** A token will be generated using RSA token mechanism and sent by the proxy server to the user, which is used to decrypt the data.

5. **User Revocation:** The user is revoked by updating the master key of the system and the public key of the component if the user enters wrong token details.

6. **File Deletion:** It is performed when the user requests the Data owner to delete the file.

5. IMPLEMENTATION

5.1. Construction of scenario

The scenario is as follows, a patient registers with the medical issues that he is having, all the information is encrypted with respect to the type of health issue that the user is having, and is stored in the Amazon Simple Storage Service (S3). The doctor can access the medical report related to the patient on a regular basis to keep track of patient's medical conditions. A token will be generated by the proxy server whenever the doctor requests to access the medical records using RSA token mechanism. This token is sent to the doctor and is used to download the medical records related to the patient.

5.2. Construction of the System Model

1. The Data Owner generates two keys, using Attribute Based Encryption (k), which are Public Key PK and the Master Key MK. The data owner describes the type of data D and passes on ($\mathrm{H.g}^{\mathrm{H}(r\|t)}$), which is an encrypted file H as DEK(= $g^{\mathrm{H}(r\|t)}$)through Attribute EncryptC(H, DEK) algorithm, and (I, F_1, $\{\mathrm{F}_i\}_{i\,\varepsilon\,\mathrm{I}}$), which is encrypted DEK with Attribute Encrypt(I, DEK, PK), the encrypted file H is sent to cloud service provider and the keys are stored in the Proxy server.

2. The user group sends a request, to access the information related to the patient.

3. The authentication details will be checked, once the user is verified a request will be sent to the proxy server to generate the proxy re-encryption key P and $\{sk_i\}_{i\,\varepsilon\,\mathrm{I}}$) to CSP.

4. A private key $s\acute{k}_i$ will be generated for the user group using AUpdateSK(I, sk_i, AHL_i) algorithm and is sent by attaching to ($\mathrm{H}.g^{\mathrm{H}(r\|t)}$). Proxy server generates (i, Ẽ, $\{\mathrm{E}_i\}_{i\,\in\,\mathrm{I}}$) which corresponds $s\acute{k}_i$ using AUpdate(i, E_i, AHL_i) sends it.

5. The user group gets the DEK (Token) using ADecryptH(p, SK,E) Algorithm with private key $s\acute{k}_i$ and proxy re-encryption key P.

6. Using the Decrypt (m.DEK, DEK), ($\mathrm{H}.g^{\mathrm{H}(r\|t)}$) is decrypted with DEK to get the required information requested by the user.

5.3. Security Analysis

The previous models were open to attacks like collision of revoked user and CSP, fine grained access control was an issue. It is because the encrypting and decrypting authority was given to the CSP. The proposed system maintains the keys by setting up a proxy encryption server which carries out the encryption and decryption process, and the cloud storage has the encrypted data, it doesn't have any private key information with it, thus the proposed scheme is able to maintain privacy of the users by not providing any private key information with the cloud service provider. Along with it attribute based encryption is used in this system, which gives a controlled access to the information and eliminates unauthorized access to the information, thus proving more security to the data. Thus the proposed scheme prevents collision attacks, guarantees data confidentiality and provides a fine grained access to the data.

6. CONCLUSION

In this paper a secure scheme for data sharing was designed to preserve the privacy of the user by implementing attribute based encryption (ABE) and proxy based re-encryption mechanism (PRE), any secret key information related to the data is not shared with the Cloud Service Provider(CSP). Moreover the encryption computation and storage overhead from the Data Owner is reduced, but still some amount of computational overhead still exists. The future work might be able to deduct the computational overhead more effectively.

REFERENCES

[1] G. Ateniese, K. Benson, and S. Hohenberger, "Key-private proxy re-encryption," in Topics in Cryptology–CT-RSA (Lecture Notes in Computer Science), vol. 5473. Berlin, Germany: Springer-Verlag.

[2] Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage Baojiang Cui, Zheli Liu and Lingyu Wang IEEE TRANSACTIONS ON COMPUTERS, VOL. 6, NO. 1, JANUARY 2016.

[3] Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage Kaitai Liang, Willy Susilo, Senior Member, IEEE, and Joseph K. Liu IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 8, AUGUST 2015.

[4] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity basedencryption with constant size ciphertext," in Advances in Cryptology–EUROCRYPT (Lecture Notes in Computer Science), vol. 3494. Berlin,Germany: Springer-Verlag, 2015, pp. 440–456.

[5] Y. S. Rao and R. Dutta, "Recipient anonymous ciphertext-policy attributeBased encryption," in Information Systems Security (Lecture Notes inComputer Science), vol. 8303. Berlin, Germany: Springer-Verlag, 2013,pp. 329–344.

[6] "Building Foundations for ehealth: Report of the WHO Global Observatory for ehealth," Accessed: 17.02.2016. [Online]. Available: http://www.who.int/goe/publications/bf FINAL.pdf.

[7] G. Ateniese, K. Benson, and S.Hohenberger, "Key-private proxy re encryption," in Topics in Cryptology–CT-RSA (Lecture Notes inComputer Science), vol. 5473. Berlin, Germany: Springer-Verlag, 2009, pp. 279–294.

[8] K. Liang, C.-K. Chu, X. Tan, D. S. Wong, C. Tang, and J. Zhou, "Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts," Theoretical Comput. Sci., vol. 539, pp. 87–105, Jun. 2014.

[9] S.C. Yu, C. Wang, K.I. Ren, and W.J. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,"INFOCOM, 2010 Proceedings IEEE, pp.321-334, 2010

[10] S. Chatterjee and P. Sarkar, Identity-based encryption. Springer Science & Business Media, 2011.

[11] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,"Proc. IEEE INFOCOM, pp. 525-533, 2010.

[12] Amazon S3. http://aws.amazon.com/s3/.