Preserving Privacy of Public Clouds through Access Control Mechanisms: A Review

S Aparna[1], Devi Dath[2]

[1]*PG scholar, Department of Computer Science, College of Engineering Perumon, Kerala, India*

[2]*Assistant Professor, Department Of Computer Science, College Of Engineering Perumon, Kerala, India*

Abstract— **Enforcing privacy on public clouds through access control mechanisms are currently based on Single Layer Encryption. Under Single Layer Encryption, data owners should upload data on the cloud after encrypting them and have to re-encrypt the data whenever access policies or user profiles are changed. This could increase the communication and computational costs at data owners. A better approach is to delegate the responsibility of re-encryption to the cloud, while at the same time preserving the privacy of data stored in the cloud. An approach based on two layer encryption, were the data owner performs an encryption based on a primary access control policy and cloud performs a second layer encryption over the owner encrypted data based on the remaining access control policies. It is important to distinguish between the access control policies so that owner level encryption can be performed using a primary condition and the cloud level encryption can be performed using the remaining set of access control policies.**

Keywords— **Access Control Policies, Single Layer Encryption, Two Layer Encryption.**

I. INTRODUCTION

In order to preserve security and privacy of data items stored in the cloud, access control policies must be enforced to users that define which user can access which data. These access control policies are derived from the identity attributes of the users. But providing identity attributes to owners or clouds could reveal their identity. This may contain personal information about users which can be a threat to the privacy of users therefore must be protected from the cloud. As a solution to this issue users can register at a key management module to retrieve tokens. These tokens further be used to derive security keys using which the users re-encrypt the data. Data owners encrypt the data using ACP's, so that only users who satisfy the policies will be given the key to decrypt them. This approach can have several limitations as follows:

• Data Owners does not keep the copy of data, therefore when the user profile or the policies are updated, the data owner needs to download the data again from the cloud to re-encrypt them with new keys.

•New keys are to be communicated with the users.

According to Single layer encryption, whenever the user credential changes, data owners have to re-encrypt the data item with new keys which may incur high communication and computational costs. In order to overcome these limitations, two layer encryption (TLE) is introduced, the data owner. Under this approach, the data owner performs an encryption based on a primary access control policy and cloud performs a second layer encryption over the owner encrypted data based on the remaining access control policies. To summarize there are two main types of encryptions [1] to enforce security and privacy in clouds:

1. Single Layer Encryptions
2. Two Layer Encryptions

II. COMPARISON BETWEEN SINGLE LAYER ENCRYPTION AND TWO LAYER ENCRYPTION

The SLE scheme consists of the four entities, Owner, user, key management and Cloud.

Owner- Owner encrypts the data based on access control policies and uploads them to cloud.

User- Users registers at key management module to retrieve tokens, which are in turn used to register at owner to retrieve secret keys.

Key management- Users registers at key management module providing any identity attributes to retrieve tokens.

Cloud – Cloud receives encrypted data from the owner and re-encrypts it using access control policies.

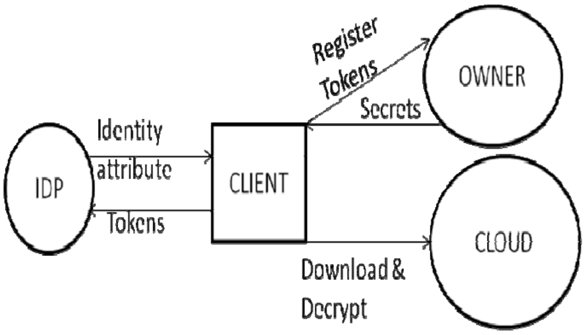


Fig 1: Single Layer Encryption

In Single Layer Encryption [4], user registers at owner using the tokens it received from key management module. But when the user credential or policies changes, owner has to re-encrypt the data with new keys. To resolve these issues two layer encryption was introduced.

In Two layer encryption, access control policies will be decomposed into two (policy1 and policy2), such that decomposition will be consistent. Policy1 will be a primary condition i.e., if policy1 is violated, policy2 will not be considered.

Two layer encryption also consist of four phases but with modifications that resolve the drawbacks of single layer encryption.

Key management- Users registers at key management module by providing their identity attributes to retrieve tokens.

As shown in Figure2, user provides identity attribute to an identity service provider [2]. It then issues an identity token for each such identity attribute.

Format for token = (pnym, id, val, sig)

Where,

- pnym is a pseudonym for identifying a User.
- Id is for identifying the identity attribute.
- Val is the value for identity attribute.
- sig is the IdP's digital signature for pnym, id and val.

For example, an identity token that a User, identified by "12121", receives for the identity attribute tag "age", looks like IT = (12121, age, 25, 4322348998254219).

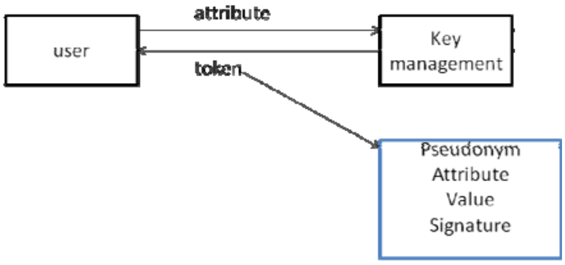
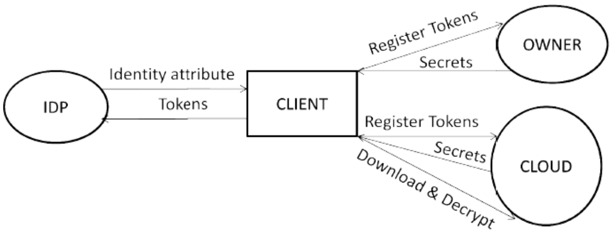
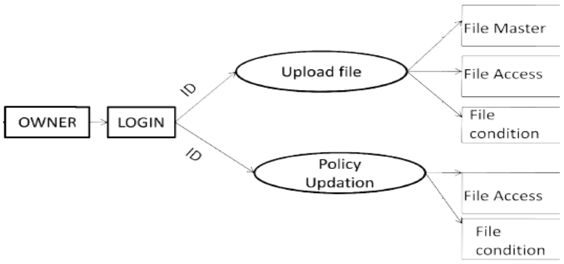


Fig2: Key Management

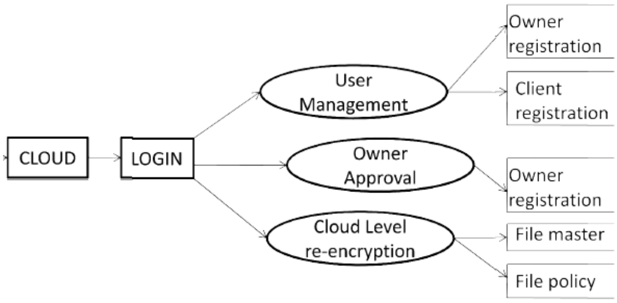
User-After collecting tokens from key management or identity service provider, user registers at owner and cloud with those tokens.



Owner- Owner encrypts the data using policy1 and uploads it to cloud. It provides secret keys to valid users using which they decrypt 1rst layer of encryption. Owners can upload files and can update the policies whenever required.



Cloud Service Provider- Cloud performs second layer encryption over the owner encrypted data and performs re-encryption whenever user dynamics changes. It could also manage the users as well as owners [3].



To summarize, the main difference between SLE and TLE is that, whenever the user dynamics changes, only cloud level re-encryption are required in case of TLE rather than owner level re-encryptions in SLE. Thus it reduces the computational and communication cost at data owner.

III. CONCLUSIONS

In the SLE approach, the Owner performs the attribute based encryption based on ACPs. The attribute based encryption assures that Users who satisfy the ACPs can get the encryption keys. The TLE approach enforces the access policies through two encryptions. Each ACP is decomposed into two sub ACPs such that the decomposition is consistent. The Owner performs the first layer encryption using one part of the decomposed ACPs through attribute based encryption [5]. The Cloud performs the second layer encryption using the remaining ACPs through another attribute based encryption. User can access the data item after decrypting both the layers of encryption made by owner and cloud.

However, the future work of this topic was concluded from the fact that clients no longer have physical possession of data indicates that they are facing a risk for missing or corrupted data. To avoid the security risks, audit services can be delegated to ensure the integrity and availability of outsourced data. For this a cryptographic technique called Provable data possession (PDP) for verifying the integrity of data without retrieving it at an untrusted server, can be used.

REFERENCES

[1] M. Nabeel and E. Bertino, “Privacy preserving delegated access control in the storage as a service model,” in EEE International Conference on Information Reuse and Integration (IRI), 2012.

[2] M. Nabeel and E. Bertino, “Towards attribute based group key management,” in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011

[3] Balakrishnan S, Saranya G, et al. (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(2), 397–400.

[4] Yu, S., Wang, C., Ren, K., Lou, W.: Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. In: Proc. IEEE INFOCOM. pp. 534–542 (2010).

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute based encryption for fine-grained access control of encrypted data,” in ACM Conference on Computer and Communications Security, 2006, pp. 89–98