MULTI AUTHORITY CLOUD STORAGE HAVING REVOCABLE DATA ACCESS CONTROL

Durairajan, M. S, Dhanapal, M and S. Elavarkuzhali

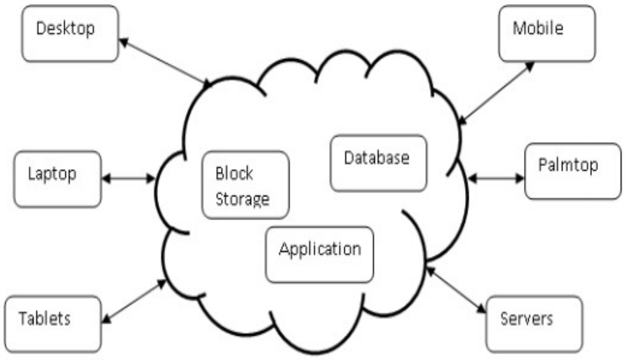
Department of Computer Science and Engineering, Madha Engineering College,
Kundrathur, Chennai-600069.

ABSTRACT

Cloud computing multi-tenancy feature, which provides privacy, security and access control challenges, because of sharing of physical resources among untrusted tenants. Thus to have data security among them its effective way to have access control. Cipher text policy based encryption considered the most suited technique for data access control as it has direct control on access policies. Though it faces attribute revocation problem. Thus there exists a need to have revocable data access control. This attribute revocation method resolves both forward and backward security.

INTRODUCTION:

Data Hosting and Data accessing are an important services of cloud storage in cloud computing. This actually introduces greater challenge to access control. CP-ABE regarded as most suitable technique as it gives data owner direct control in cloud storage systems. There exist two types of CP-ABE systems: single authority where all attributes are managed by single authority and multi authority CP-ABE is more appropriate for data access control of cloud storage as users may hold attributes issued by multiple authorities and data owners may also share data using access policy defined over attributes [1]. Here multi authority is more appropriate to have good access control. The data access policy can be defined as “Doctor and Researcher” here attributes are doctor and researcher which are issued by medical organization and administrators separately. But these attributes are not static as their positions can be upgraded or else degraded. Since the attributes are dynamic attribute revocation problem occurs.



DATA SHARING OF CLOUD STORAGE

Existing system: Cloud servers prone to Byzantine failure, where a storage server can fail in arbitrary ways. The cloud is also prone to data modification and server colluding attacks. In server colluding attack, the adversary can compromise storage servers, so that it can modify data files as long as they are internally consistent. To provide secure data storage, the data needs to be encrypted. The clouds should not know the query but should be able to return the records that satisfy the query. This is achieved by means of searchable encryption. The keywords are sent to the cloud encrypted, and the cloud returns the result without knowing the actual keyword for the search. The problem here is that the data records should have keywords associated with them to enable the search. The correct records are returned only when searched with the exact keywords. These are achieved by having multiple key distribution centres meaning that decentralized access control. This greatly avoids single point of failure and reduces the complexity in providing the key to consumers if having only single key distribution centre. The keys are generated based on attributes they have. The attributes are given based on the role they possess and provided by cloud server [2].

Proposed System: There exists a challenge on attribute dynamicity and question what happens when the attribute got terminated. There comes attribute revocation problem. The proposed dealt with efficient and effective revocable data access control as with changes on attributes. A candidate who possesses certain role can be upgraded or degraded on further period. Thus all attributes are dynamic in nature. The access control need to be modified accordingly as the attributes get changed. Thus the revocable data access control does the job and another drawback of untrusted cloud server gets addressed. Since the cloud server though honest they are curious about the data get stored. So the access control gets shifted to data owner itself. Instead of several key distribution centres we have several such attribute authorities and a single certificate authority. The CA only provides basic identities and the AA provides the attributes independently. A user can get attributes from single authority whereas the attribute authority can provide any number of attributes to many users as need [3].

PHASES:

System Initialization: The CA and AA get setup with their algorithms as follows. CA having no input but taking security parameter it provides global master key GMK and global public parameters GPP and users with global public keys and global secret keys. AA setup takes attribute universe as input and output secret and public key pair, it also generates set of version keys.

Secret Key Generation: It actually runs by each AA. It takes input as GPP, global public keys and one secret key of user id and set of attributes and also its corresponding version keys. It outputs a secret key for the user which is used for decryption.

Data Encryption by Owners: Owners first divide the data into several components according to the logic granularities and encrypt each data component with different content keys by using symmetric encryption techniques. Then the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies. Then the owner sends the encrypted data to the cloud server together with the cipher text. The cipher text denote the encrypted content keys with CP-ABE.

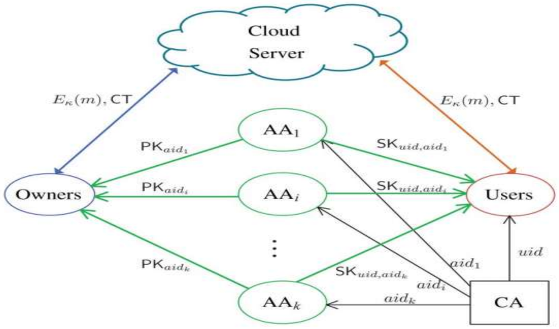
Data Decryption by the Users: Users first run the decryption algorithm to get the content keys and use them to further decrypt the data. It takes as input the cipher text and global public key, global secret key. The user will be able to decrypt the cipher text only when he is able to satisfy the access policy.

Attribute Revocation:

User Key Generation: Here the revoked attribute got managed by AA; it takes input as secret key, the revoked attribute and its current version. It outputs the new version and the update key.

Secret key update: They take input as current secret key of non revoked user and the update key. The non revoked users are users who possess the revoked attribute but have not been revoked. It outputs new secret key for each non revoked user.

Cipher text update: They take input as cipher texts which contain the revoked attribute and update key. It outputs the latest version of the revoked attribute. Moreover at last we shall say that all users need to hold only the latest secret key, rather than to keep records on all previous keys.



.

Analysis: During the secret key update phase, the corresponding AA generates an update key for each non revoked user. The revoked user cannot use update keys of other non revoked user to update its own secret key even if it can compromise some non revoked users. This guarantees backward security. After each attribute revocation operation the version of the revoked attribute will be updated. When new users join the systems, their secret keys associated with attributes with the latest version. The newly joined users can still decrypt previously published cipher texts, if their attributes can satisfy access policies associated with cipher texts. This guarantees forward security.

CONCLUSION:

Thus proposed a revocable multiauthority CP-ABE scheme that supports efficient attribute revocation. The access control gets modified as with change in attributes. The access policy fully maintained by owner rather cloud server. Thus no user with revoked attribute can decrypt the data or replace data with stale information. This revocable CP-ABE is a promising technique, which can be applied in any remote storage systems and online social networks.

REFERENCES

1. Waters, 2010.“Ciphertext policy Attribute based Encryption: An expressive efficient and provably secure Realization,” in Pro, 4th Intl conf. Practise and Theory in public key cryptography (PKC’11)
2. Yang and X.Jia, 2012. “Attribute based Access control for multi authority systems in cloud storage” in proc, 32th IEE Intl conf (ICDCS’12) 2012
3. Benthencourt., A. Sahai and B. Waters 2007.“Cipher text policy Attribute based encryption”, in proc IEEE symp security and privacy, Grace.
4. Lewko and B. waters, 2012.“New proof methods for Attribute based encryption; achieving full security through selective techniques” in proc 32st Intl cryptography conf: CRYPYTO’12, 2012.