Representative, efficacious, and revocable data access control for multi-authority cloud storage

Shruti A. Upari¹, Prof. Vivekanand Reddy²

¹Department of Computer Science and Engineering, Visvesvaraya Technological University, Belagavi, Karnataka, India
²Faculty in Department of Computer Science and Engineering, Visvesvaraya Technological University, Belagavi, Karnataka, India

Abstract: Cloud Computing is one of the most prominent technology. It offers a service known as cloud storage which provides data outsourcing. Data access control is a way that ensures security in the cloud. However the cloud servers are untrusted which affects data access control. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design a Representative, Efficacious, and Revocable Data Access Control for Multi-Authority Cloud Storage, where there are multiple authorities co-exists and each authority is able to issue attributes independently. Ciphertext Policy Attribute-based Encryption (CP-ABE) scheme is used to propose revocable multi-authority method for access control. The attribute revocation method in this proposed work achieves both backward and forward security.

Keywords— Cloud Computing, Cp-abe, Cloud Storage, Multi-authority, data access control

I. INTRODUCTION

Cloud Computing is a model for access of data. As indicated by NIST (National Institute of Standards and Technology, US), Cloud Computing gives a helpful, on-interest system access to a common pool of figuring assets [1]. Most important service of this is Cloud Storage which provides services for data owners. As the cloud servers are sometimes un-trusted these owners do not depend on them for access control. Hence CP-ABE [2], [3] scheme is used for data access control which allows the owner on access policies to have direct control. In this scheme, there exists an authority that is responsible for attribute management and key distribution. The owner defines some policies and encodes data based on these policies. Each consumer/user will be issued a secret key reflecting its attributes. The user can then decode the data only if he/she has the attributes that satisfies the policies defined by owner.

Cloud Storage is a Cloud Computing model which is used to preserve the data on remote servers which can be later accessed using Internet or Cloud. Cloud storage is usually maintained, operated and managed by different cloud storage service provider. Earlier there were many ways where we could save the data such as Floppy Disk, CDs, and Pen drives but there was always the problem of storage capacity if the data to be stored was of a very huge amount. For this purpose, Cloud Computing was brought forth which provided the business people, consumers a way to store the data which we popularly now know as Cloud Storage.

In this paper, a revocable multi-authority CP-ABE scheme is proposed where there are several authorities co-existing that solve the problem of attribute revocation. This proposed scheme is very efficient meaning that it incurs less communication and computation cost when compare to the earlier works. The scheme here makes use of semi trustable cloud server because the updating of keys is done by the attribute authority not the server.
II. RELATED WORK

S. Yu et al. [5] proposed Attribute Based Data Sharing with Attribute Revocation. Authors mainly used semi-trustable on-line proxy servers. This server enables the authority to revoke user attributes with minimal effort. This scheme was uniquely integrating the technique of proxy re-encryption with CP-ABE, and also enables the authority to delegate most of laborious tasks to proxy servers. The advantages of this scheme is More Secure against chosen cipher text attacks. Provide importance to attribute revocation which is difficult for CP-ABE schemes. The one of the drawback is the storage overhead could be high if proxy-servers keep all the proxy re-key.

S J. Hur and D.K. Noh, [6] worked on Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems. They presented an access control mechanism based on cipher text-policy attribute-based encryption to implement access control policies with efficient attribute and user revocation method. The fine-grained access control can be achieved by dual encryption scheme. The dual encryption mechanism gets advantage of the attribute-based encryption and selective group key distribution in each attribute group. This method is securely managing the outsourced data and achieved efficient and secure in the data outsourcing systems.

M. Li, S. Yu, Y. Zheng, K. Ren, and W.Lou, [7] presented Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. They considered the use of dual system encryption methodology. The encryption techniques from Multi-authority ABE and Key-Policy ABE are combined into a single module. The proposed MA-ABE technique proves useful for key management and flexible access handled by KP-ABE. The proposed framework has attempted to achieve data security by MA-ABE and data privacy by KP-ABE scheme. The overall security of the system has been improved. Existing attribute revocation methods rely on a trusted server or lack of efficiency also they are not suitable for dealing with the attribute revocation problem in data access control in multi-authority cloud storage systems.

III. SYSTEM OVERVIEW

3.1. DATA ACCESS CONTROL SYSTEM IN MULTI AUTHORITY CLOUD STORAGE:
There are five types of entities in the system as in Fig 1: a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server) and data consumers (users). The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. For each legal user in the system, the CA assigns a global unique user identity to it and also generates a global public key for this user. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. For example, the CA can be the Social Security Administration, an independent agency of the United States government. Each user will be issued a Social Security Number (SSN) as its global identity. Every AA is an independent attribute authority that is responsible for entitling and revoking user’s attributes according to their role or identity in its domain.

![Figure 3.1 System Model](image-url)
In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key. For each user reflecting his/her attributes.

IV. PROPOSED WORK

In this proposed system main focus is given on the revocation problem that occurred in the existing system. This revocation problem is being solved and hence it obtains a very less amount of loss in the computation and communication and also achieves security that is both forward and backward security. Specifically, we separate the functionality of the authority into a global certificate authority (CA) and multiple attribute authorities (AAs). The CA sets up the system and accepts the registration of users and AAs in the system. It assigns a global user identity to each user and a global authority identity to each attribute authority in the system. Because the user id is globally unique in the system, secret keys issued by different AAs for the same them can be tied together for decryption. Also, because each AA is associated with an authority id, every attribute is distinguishable even though some AAs may issue the same attribute. To deal with the security issue in [6], instead of using the system unique public key (generated by the unique master key) to encrypt data, our scheme requires all attribute authorities to generate their own public keys and uses them to encrypt data together with the global public parameters. This prevents the certificate authority in our scheme from decrypting the ciphertexts.

To solve the attribute revocation problem, we assign a version number for each attribute. When an attribute revocation happens, only those components associated with the revoked attribute in secret keys and ciphertexts need to be updated. When an attribute of a user is revoked from its corresponding AA, the AA generates a new version key for this revoked attribute and generates an update key. With the update key, all the users, except the revoked user, who hold the revoked attributes can update its secret, key (Backward Security). By using the update key, the components associated with the revoked attribute in the ciphertext can also be updated to the current version. To improve the efficiency, we delegate the workload of ciphertext update to the server by using the proxy re-encryption method, such that the newly joined user is also able to decrypt the previously published data, which are encrypted with the previous public keys, if they have sufficient attributes (Forward Security). Moreover, by updating the ciphertexts, all the users need to hold only the latest secret key, rather than to keep records on all the previous secret keys.

Advantages of the Proposed System:

- The framework of the scheme has been modified in such a way that owner is not involved in the generation of keys.
- The efficiency of attribute revocation is increased.
- There is improvement in the expressivity of data access control scheme.
V RESULT ANALYSIS

Fig 1: Start Page

Fig 2: Login Page of the Owner

Fig 3: Registration Page of the Owner

Fig 4: Owner Login with credentials

Fig 5: Home Page of the Owner

Fig 6: Owner uploads the file

Fig 7: Select File to upload

Fig 8: Consumer List
Fig 9: Authority set by the Owner

Fig10: Cipher text Policy-Attribute Based Encryption

Fig11: Encrypted file after applying CP-ABE

Fig12: Uploaded files

Fig13: Consumer Login Form

Fig 14: Consumer requests for key

Fig 15: Key sent to Consumer

Fig 16: Consumer enters the key
VI CONCLUSION

This paper proposes an efficient and secure data access control scheme for multi-authority cloud storage systems. This proposed scheme guarantees that the cloud storage systems properly launches and authenticates legal users as well as attribute authorities if and only if every CA successfully verifies the message sent by another CA using the latter CA’s public commitment. In this, we have proposed a revocable multi-authority CPABE scheme that can support efficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. The revocable multi-authority CPABE is a promising technique, which can be applied in any remote storage systems and online social networks etc.

REFERENCES


