International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 1 | Issue – 6

Efficient Access Control and Security for Multi-Authority Cloud Storage Server

Sampath Kumar Tatipally
M.Tech, Department Of CSE, School Of Information Technology (JNTUH), Village Kukatpally, Ranga reddy, Telangana, India

Dr. K. Shahu Chatrapathi
Professor, Department of CSE, JNTUH College of Engineering Manthani, Village Manthnai, Mandal Manthni, Pedhapelli, Telangana, India

ABSTRACT

One of the effective way to ensure data security in cloud computing is data access control. Due to untrusted and outsourcing cloud server, the control of data access became a challenging issue in cloud computing. One of the most suitable technology for data control in cloud is Ciphertext-Policy Attribute-based Encryption (CP-ABE) , because it gives control to the data owners on direct access policies. It is somewhat difficult to apply existing Ciphertext-Policy Attribute-based Encryption (CP-ABE) scheme to cloud data access control because of the attribute revocation problem. In this paper, we design an revocable, expressive and well-organized data access control for multi authority cloud storage, where there are multiple authorities co exist and each authority is able to issue attributes independently. We propose a revocable multi-authority Ciphertext-Policy Attribute-based Encryption scheme, and apply it is the principal techniques to design the data access control scheme. Our revocation attribute method can efficiently achieve both backward security and forward security. The analysis results show that our proposed data access control scheme is secure in the casual oracle model and is more efficient than previous works.

1. INTRODUCTION

One of the significant services in cloud is cloud storage. Through which the data owner can host their data in cloud. The new ideal for data access and data hosting services introduced a new challenge to data access control. Because the cloud owners cannot full fill trust of the data owner, they can no longer cloud server to access control. CP-ABE Is treated as the most appropriate technology for data access control in cloud. Since it gives the data owner more unswerving control on access policies. In Ciphertext-Policy Attribute-based Encryption scheme, there is an right that is liable for attribute management plus key distribution. The authority may principal office in a college, the computer science department in a company, etc. The data owner will only defines the encrypt data and access policies according to the policies. Every user will be given a secret key and a attributes reflecting it. The user can decrypt the data only if attribute satisfies the policies. In general there are two types of Ciphertext-Policy Attribute-based Encryption single and multi authority. All the attributes are managed by multi and single Ciphertext-Policy Attribute-based Encryption where attributes are from different domains and managed by different authorities. Multi authority Ciphertext-Policy Attribute-based Encryption is more suitable for data access control of cloud storage systems, because the user holds the attribute which are issued by multi authorities and data owner may also carve up the data using access policy distinct over attributes from different authorities. For example, in an University, data owners may share the data using the access policy ‘‘Faculty AND Researcher’’, where the attribute ‘‘Faculty’’ is issued by a Principal and the attribute ‘‘Researcher’’ is issued by the Guide. On the other hand, it is tricky to directly apply these multi authority Ciphertext-Policy Attribute-based

Encryption schemes to multi authority cloud systems because of the attribute revocation problem. User attribute changes dynamically in this multi authority Ciphertext-Policy Attribute-based Encryption. A user may be allowed some new attributes or revoke some current attributes. And his authorization of data access must be changed accordingly. On the other hand, existing attribute revocation methods either rely on a lack of efficiency or trusted server, they are not appropriate for commerce with the attribute revocation problem in data access control in multi-authority cloud storage systems. In this paper, we first propose a revocable multi authority Ciphertext-Policy Attribute-based Encryption scheme, where an well-organized and protected revocation method is anticipated to solve the attribute revocation problem in the system. As shown in table our attribute revocation method is well-organized, less computation cost and communication cost, and is secure in the sense that it can achieve both. In the proposed scheme it does not mandatory the server to be a fully trusted, because the key imposed by all attribute not the server. Even if the server is semi trusted our scheme can still assurance the backward security. Here we apply our anticipated revocable multi-authority Ciphertext-Policy Attribute-based Encryption scheme as the essential techniques to assemble the secure and expressive data access control scheme for multi authority cloud storage systems.

Compared to the convention version of this work, we have the subsequent improvements:

1. We change the framework of the scheme and make it more realistic to cloud storage systems, in which data owners are not implicate in the key generation. particularly, a user's secret key is not linked to the owner's key, in a way that each user needs to hold their secret key from each authority instead of several secret keys linked to multiple owners
2. We deeply improve the competence of the attribute revocation method. Particularly, in our new attribute vocation method, only the ciphertexts that linked with the revoked attribute needs to be updated, while in, all the ciphertexts that associated with any attribute from the authority must be updated. in addition in our new attribute revocation method, both the key and the ciphertext can be simplified by using the same update key
3. In the proposed scheme it does not mandatory the server to be a fully trusted, because the key imposed by all attribute not the server. Even if the server is semi trusted our scheme can still assurance the backward security. Here we apply our anticipated revocable multi-authority Ciphertext-Policy Attribute-based Encryption scheme as the essential techniques to assemble the secure and expressive data access control scheme for multi authority cloud storage systems.

Scheme	Authority	Revocation Message	Backward Security	Forward Security	Revocation Enforcer	CT Updater
[11]	Single	$O(n_{non,x} \log \frac{n_u}{n_{non,x}})$	Yes	Yes	Server*	Server*
[13]	Multiple	$O(n_{c,x} \cdot n_{non,x})$	Yes	No	Owner	Owner
[14]	Multiple	$O(n_{c,aid} + n_{non,x})$	Yes	Yes	AA	Server†
Our	Multiple	$O(n_{non,x})$	Yes	Yes	AA	Server†

*: The server is fully trusted; †: The server is semi-trusted.
$|p|$ is the size of element in the groups with the prime order p; n_u denotes the number of users in the system; $n_{non,x}$ denotes the number of non-revoked users who hold the revoked attribute x and $n_{c,x}$ is the number of ciphertexts which contain the revoked attribute x; $n_{c,aid}$ denotes the total number of attributes belongs to the AA_{aid} in all the ciphertexts.

2. System and Security Model

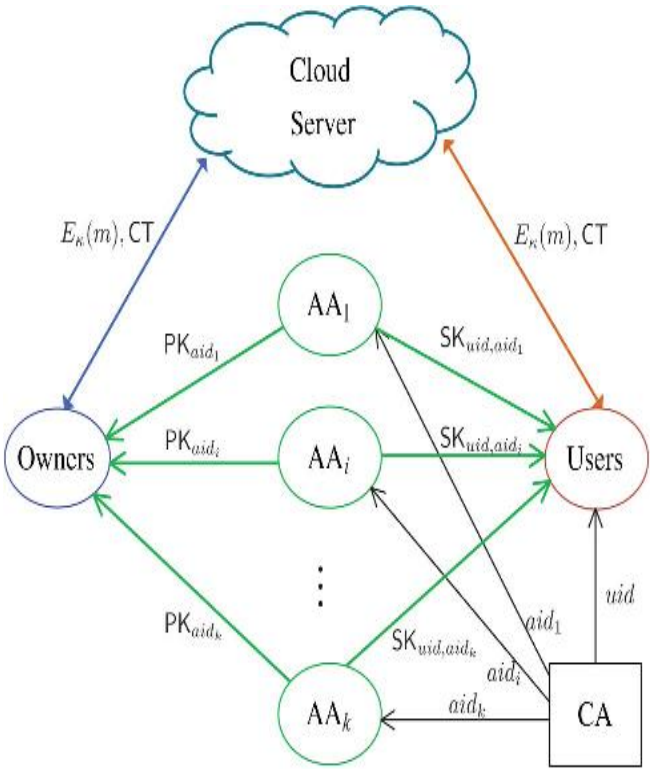
2.1 System Model

We considered the data access control system in multi authority cloud storage as explained in the table 1. There are 5 types of entities in system: data consumers (users), attribute authorities (AAs), a certificate authority (CA), the cloud server (server) and data owners (owners). This algorithm is a global trusted certificate authority in the system and accepts the registration of the user and attribute authority For each and every legal user in the system, the certificate authority assigns a global sole user identity to it and generates global public key for that user.

On the other hand, the certificate authority is no implicated in any creation and attributes management of secret keys that are associated with attributes. For example, the certificate authority can be the Institute, an independent agency of the Departments. Each user will be issued a Social Security Number as its overall identity.

Every attribute authority is an independent attribute authority that is liable for entitling and revoking user's attributes according to their identity or role in its domain. In this scheme, each and every attribute is associated with a single AA, but each attribute authority can manage an arbitrary number of attributes. Every Attribute authority has full control over the semantics and structure 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 their attributes.

Every user has an identity in the system. A user can be entitled a set of attributes which can come from the multiple attribute authority. Ever user will receives the secret key which is associated with its attribute entitled with their corresponding attribute authority.
Every owner divides the data into several components according to the logical granularities and encrypts every data component with an different content keys by using any of the encryption technique. Then, the owner defines the access policies on the attribute from multi attribute authority and encrypt the key under these policies. Then the owner sends the encrypted data to the server along with the ciphertext. They do not relay on the cloud server for the data control. The access control happens in the cryptography. That is only when the user attribute satisfy the access policy defined in the ciphertext.



This fig is the system model of data across control in the multi authority cloud storage

2.2 Security Model

In this system we make the following assumption

- The cipher text policy attribute is completely trusted in the system. It will not scheme with any other user, but it should be prevented from decrypting any txt by itself.
- Every authority attribute is trusted it should be corrupted by the adversary
- The server is curious but integrity. It is curious about the content of the received on encrypted data, but it will correctly execute the task assigned to it
- Every user is deceitful and may try to obtain the unauthorized data.

3. Overview

To design the control representation for the multi authority cloud services system, the chief challenge is to construct the essential revocable multi authority CP ABE protocol. To intend the data access control scheme for multi authority cloud storage systems, the main challenging issue is to construct the primary Revocable Multi authority
CP-ABE protocol. In, follow projected a Multi authority CP-ABE protocol; still, it cannot be unswervingly applied as the underlying techniques because of two main reasons:
1) Revocation Issue
2) Security Issue

We suggested a new revocable multi-authority CP-ABE protocol based on the single-authority CP ABE proposed by Lewko and Waters in. That is we lengthen it to multi authority developed and make it revocable. We relate the techniques in multi-authority CP-ABE protocol to tie jointly the secret keys generated by dissimilar authorities for the same user and avoid the collusion attack. In particular, we separate the functionality of the authority into a global certificate authority and multiple attribute authorities. The CA sets up the system and accepts the registration of users and attributes authority's s in the system. It assigns a global user identity uid to each user and a global authority identity aid to each attribute authority in the system. Because the uid is globally unique in the system, secret keys issued by different AAs for the same uid can be tied together for decryption.

4. RELATED WORK

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is one of the potential techniques which designed for Attribute Revocation contrast of Computation Time. (a) Encryption. (b) Decryption. (c) Encryption. (d) Decryption. (e) Re-encryption.

There are two types of Ciphertext-Policy Attribute-Based Encryption CP-ABE systems: multi and single authority CP ABE where all attributes are managed by a single authority, and multi authority CP-ABE, where attributes are commencing dissimilar domains and Maintained by different authorities. Multi-authority CP-ABE is more apposite for the access control of cloud storage systems, as users may hold attributes issued by multiple authorities and the data owners can share the data using access policy defined on the attributes from different authorities. Conversely, due to the problem in the attribute revocation problem, these multi-authority Ciphertext-Policy Attribute-Based Encryption CP-ABE schemes cannot be directly applied to data access control for such multi-authority cloud storage systems.

To achieve the revocation on attribute level, for this encryption based attribute revocation schemes are proposed by relying on a trusted server. We know that The cloud server cannot be fully trusted by data owners, thus traditional attribute revocation methods are no longer suitable for cloud storage systems.

Ruj, Nayak proposed a DACC scheme, where an attribute revocation method is obtainable for the Lewko and Waters' decentralized ABE scheme. Their attribute revocation method will not require a fully trusted server. But, it incurs a heavy communication cost since it requires the data owner to transmit a new ciphertext component to every non-revoked user.

5. CONCLUSION

In this paper, I proposed an revocable multi authority Ciphertext-Policy Attribute-Based Encryption though which we can support an attribute revocation in an effective way. Then, I designed an effective scheme for data access control In multi authority cloud storage systems. I have also proved that this scheme was unarguably secure in the indiscriminate oracle model. The revocable multi-authority Ciphertext-Policy Attribute-Based Encryption CPABE is a capable technique, which can be applied in any of the remote storage system.

REFERENCES

1) T. Grance and P. Mell , ''The NIST Definition of Cloud Computing,'' 2009.
2) B. Waters, ''Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,'' in Proc. 4th Int'l Conf. Practice and Theory in Public Key Cryptography
3) B. Waters and J. Bethencourt, A. Sahai, ''Ciphertext-Policy Attribute-Based Encryption,'' in Proc. IEEE Symp. Security and privacy (S&P'07), 2007, pp. 321-334.
4) A.B. Lewko, A. Sahai, K. Takashima, and B.Waters, ''Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'10, 2010, pp. 62-91.
5) V. Goyal, A, andA. Sahai, ''Bounded Ciphertext Policy Attribute Based Encryption,'' in Proc. 35th Int'l Colloquium on Automata, Languages, and Programming (ICALP'08), 2008, pp. 579-591.
6) M. Chase, ''Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,'' in Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), 2009, pp. 121-130. [6] M. Chase, ''Multi-Authority Attribute Based Encryption,'' in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC'07), 2007, pp. 515-534.
7) S. Yu, C. Wang, K. Ren, and W. Lou, ''Attribute Based Data Sharing with Attribute Revocation,'' in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS'10), 2010, pp. 261-270
8) A.B. Lewko , ''Decentralizing Attribute-Based Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'11, 2011, pp. 568-588.
9) J. Hur , ''Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,'' IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.
10) M. Li, S. Yu, andW. Lou, ''Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,'' IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013. (ASIACCS'11), 2011, pp. 411-415.