Special Issue - 2015
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
NCACI-2015 Conference Proceedings

Significant, Capable Information Retrieve Control for Multi Ability Cloud Storage Space

P. Nirupama
Professor,
Sidharth Institute of Engineering & Technology

V. Balaji
Assistant Professor
Sidharth Institute of Engineering & Technology

***Abstract* - Information retrieve control is an effectual way to guarantee the information protection in the cloud. Due to information outsourcing and un trusted cloud servers, the information retrieve control becomes a demanding issue in cloud storage systems. Coded text-Policy Attribute-based Encryption (CP-ABE) is regard as one of the most appropriate technologies for information retrieve control in cloud storage, because it gives information owner more straight control on entrance strategy. However, it is complicated to straight apply obtainable CP-ABE methods to information retrieve control for cloud storage systems because of the attribute revocation problem. In this paper, we aim an expressive, capable and revocable information retrieve manage method for multi-ability cloud storage scheme, where there are multiple authorities co-exist and every ability is able to issue attributes independently. Particularly, we suggest a revocable multi-ability CP-ABE method, and pertain it as the underlying method to design the information retrieve control method. Our quality revocation method can capability achieves both forward protection and backward protection. The analysis and model results show that our projected information retrieve control method is protected in the random oracle model and is more capable than previous works.**

I. INTRODUCTION

CLOUD storage is a key service of cloud computing [1], which suggest services for information owners to host their information in the cloud. This new paradigm of information hosting and information retrieve services introduces a great challenge to information retrieve control. Because the cloud server cannot be fully trusted by information owners, they can no longer rely on servers to do retrieve control.

Coded text-Policy Attribute-based Encryption(CP-ABE) [2], [3] is regarded as one of the most suitable Technologies for information retrieve control in cloud storage systems, because it gives the information owner more direct control on retrieve strategy. In CP-ABE method, there is an ability that is responsible for attribute management and key distribution. The ability can be the registration office in a university, the human resource department in a company, etc. The information owner defines the retrieve strategy and encrypts information according to the strategy. Every client will be issued a clandestine key reflecting its attributes. A client can decrypt the information only when its attributes satisfy the retrieve strategy. There are two types of CP-ABE systems: single-ability CP-ABE [2], [3], [4], [5] where all attributes are managed by a single ability, and multi-ability CP-ABE [6], [7],[8] where attributes are from dissimilar domains and managed by dissimilar authorities. Multi-ability CP-ABE is more appropriate for information retrieve control of cloud storage systems, as clients may hold attributes issued by multiple authorities and information owners may also share the information using retrieve policy defined over attributes from dissimilar authorities. For example, in an E-health system, information owners may share the information using the retrieve policy ‘‘Doctor AND Researcher’’, where the attribute ‘‘Doctor’’ is issued by a medical organization and the attribute ‘‘Researcher’’ is issued by the administrators of a clinical trial. However, it is difficult to directly apply these multi-ability CP-ABE methods to multi-ability cloud storage systems because of the attribute revocation problem.

II.SYSTEM MODEL AND PROTECTION MODEL

2.1 System Model

We consider an information retrieve control system in multi-ability cloud storage, as described in Fig. 1. There are five types of entities in the system: permit ability (CA), attribute authorities (AAs), information owners (owners), the cloud server (server) and information consumers (clients). The CA is global trusted certificate ability in the system. It sets up the system and accepts the registration of all the clients and AAs in the system. For every authorized client in the system, the CA assigns a global unique client identity to it and also generates a global public key for this client. However, the CA is not involved in any attribute management and the creation of clandestine keys that are associated with attributes. For example, the CA can be the Social Protection Administration, an independent agency of the United States government. Every client will be issued a Social Protection Number (SSN) as its global identity. Every AA is an independent attribute ability that is responsible for entitling and revoking client’s attributes according to their role or identity in its domain. In our method, every attribute is associated with a single AA, but every AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Every AA is responsible for generating a public attribute key for every attribute it manages and a clandestine key for every client reflecting his/her attributes.

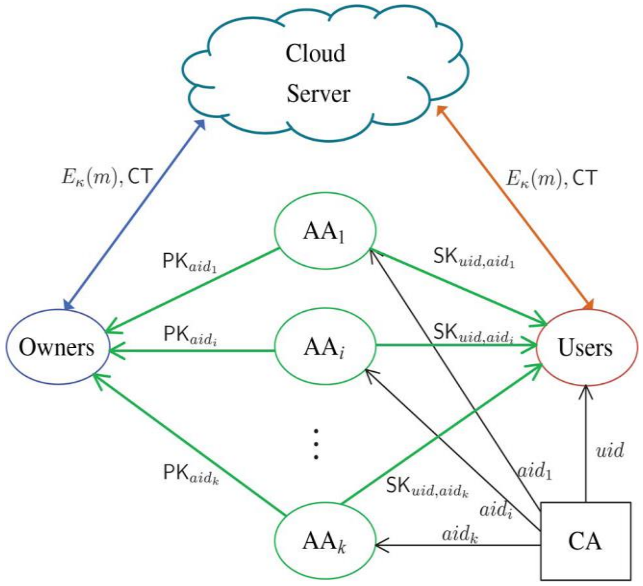

Fig. 1. System model of information retrieve control in multi-ability cloud storage.

III.OUR INFORMATION RETRIEVE CONTROL METHOD

3.1 Overview

To design the information retrieve control method for multi ability cloud storage systems, the main challenging issue is to construct the underlying Revocable Multi ability CP-ABE protocol. In [6], Chase recommend d a multi-ability CP-ABE protocol, however, it cannot be directly applied as the underlying techniques because of two main reasons: 1) Protection Issue: Chase's multi-ability CP-ABE protocol allows the central ability to decrypt all the coded texts, since it holds the master key of the system;2) Revocation Issue: Chase's protocol does not support attribute revocation. We recommend a new revocable multi-ability CP-ABE protocol based on the single-ability CP-ABE recommend d by Lewko and Waters in [16]. That is we expand it to multi ability circumstances and make it revocable. We apply the techniques in Chase's multi-ability CP-ABE protocol [6]to tie together the clandestine keys generated by dissimilar authorities for the same client and prevent the collusion attack. Specifically, we separate the functionality of the ability into global certificate ability (CA) and multiple attribute authorities (AAs). The CA sets up the system and accepts the registration of clients and AAs in the system.7 It assigns a global client identity uid to every client and a global ability identity aid to every attribute ability in the system. Because the uid is globally unique in the system, clandestine keys issued by dissimilar AAs for the same uid can be tied together for decryption. Also, because every AA is associated with an aid, every attribute is discernible even though some AAs may issue the same attribute.

To deal with the protection issue in [6], instead of using the system unique public key (generated by the unique master key) to encrypt information, our method requires all attribute authorities to generate their own public keys and uses them to encrypt information together with the global public parameters. This prevents the certificate ability in our method from decrypting the coded texts. To resolve the attribute revocation problem, we assign a version number for every attribute. When an attribute revocation happens, only those components associated with the revoked attribute in clandestine keys and coded texts need to be updated. When an attribute of a client 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 clients, except the revoked client, who hold the revoked attributes can update its clandestine, key (Backward Protection). By using the update key, the components associated with the revoked attribute in the coded text can also be updated to the current version. To improve the efficiency, we delegate the workload of coded text update to the server by using the proxy re encryption method, such that the newly joined client is also able to decrypt the previously published information, which are encrypted with the previous public keys, if they have sufficient attributes (Forward Protection). Moreover, by updating the coded texts, all the clients need to hold only the latest clandestine key, rather than to keep records on all the previous clandestine keys.

3.5 Information Decryption

All the authorized clients in the system can freely query any interested encrypted information. Upon receiving the information from the server, the client runs the decryption algorithm Decrypt to decrypt the coded text by using its clandestine keys from dissimilar AAs. Only the attributes the client possesses satisfy the retrieve structure defined in the coded text CT, the client can get the content key.

IV. PROTECTION ANALYSES

Backward Protection:

During the clandestine key update phase, the corresponding AA generates an update key for every non-revoked client. Because the update key is associated with the client's global identity uid, the revoked client cannot use update keys of other non-revoked clients to update its own clandestine key, even if it can compromise some non-revoked clients. Moreover, suppose the revoked client can corrupt some other AAs (not the AA corresponding to the revoked attributes),

2) Storage Overhead on Every Owner: The public parameters contribute the main storage overhead on the owner. Besides the public parameters, in [13], owners are required to re-encrypt the coded texts and in [14] owners are required to generate the update information during the revocation, where the owner should also hold the encryption clandestine for every coded text in the system. This incurs a heavy storage overhead on the owner, especially when the number of

Coded text is large in cloud storage systems.

3) Storage Overhead on Every Client: The storage overhead on every client in our method comes from the clandestine keys issued by all the AAs. However, in [13], the storage overhead on every client consists of both the clandestine keys issued by all the AAs and the coded text

components that associated with the revoked attribute x, because when the coded text is re-encrypted, some of its components related to the revoked attributes should be sent to every non-revoked client who holds the revoked attributes. In [14], the client needs to hold multiple clandestine keys for multiple information owners, which means that the storage overhead on every client is also linear to the number of owners nO in the system.

4) Storage Overhead on Server: The coded texts contribute the main storage overhead on the server (here we do not consider the encrypted information which are encrypted by the symmetric content keys).

V. MESSAGE COST

The message cost of the normal retrieve control is almost the same. Here, we only compare the message cost of attribute revocation, as shown in Table 3. The message cost of attribute revocation in [13] is linear to the number of coded texts which contain the revoked attribute. In [14], the message overhead is linear to the total number of attributes NC; aid belongs to the Said in all the coded texts. It is not difficult to find that our method incurs
much less message cost during the attribute revocation.

VI. CONCLUSION

In this paper, we projected a revocable multi-ability CPABE method that can support capable quality revocation. Then, we construct an effective information retrieve control method for multi-ability cloud storage space systems. We also proved that our method was provable protected in the arbitrary oracle model. The revocable multi-ability CPABE is a promising technique, which can be applied in any remote storage space systems and online social networks etc.

REFERENCES

[1] P. Mell and T. Grance, ‘‘The NIST Definition of Cloud Computing,’’ National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[2] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Codedtext-Policy Attribute-Based Encryption,’’ in Proc. IEEE Symp. Protection and privacy (S&P’07), 2007, pp. 321-334.[3] B. Waters, ‘‘Codedtext-Policy Attribute-Based Encryption: An Expressive, Capable , and Provably Protected Realization,’’ in Proc. 4th Int’l Conf. Practice and Theory in Public Key Cryptography (PKC’11), 2011, pp. 53-70.

[4] V. Goyal, A. Jain,O. Pandey, andA. Sahai, ‘‘Bounded Codedtext Policy Attribute Based Encryption,’’ in Proc. 35th Int’l Colloquium on Automata, Languages, and Programming (ICALP’08), 2008,pp. 579-591.

[5] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ‘‘Fully Protected Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,’’ in Proc. Advances in CryptologyEUROCRYPT’10, 2010, pp. 62-91.

[6] M. Chase, ‘‘Multi-Ability Attribute Based Encryption,’’ in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC’07), 2007, pp. 515-534.

[7] M. Chase and S.S.M. Chow, ‘‘Improving Privacy and Protection in Multi-Ability Attribute-Based Encryption,’’ in Proc. 16th ACM Conf. Computer and Comm. Protection (CCS’09), 2009, pp. 121-130.

[8] A.B. Lewko and B. Waters, ‘‘Decentralizing Attribute-Based Encryption,’’ in Proc. Advances in Cryptology-EUROCRYPT’11, 2011, pp. 568-588.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Attribute Based Information Sharing with Attribute Revocation,’’ in Proc. 5th ACM Symp. Information, Computer and Comm. Protection (ASIACCS’10), 2010, pp. 261-270.

[10] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, ‘‘Scalable and Protected 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.