A Survey on Protected and Well Organized Entree Control for Cloud Storage

Mr. A. Mani
Associate professor, Department of CSE in S.A. Engineering College.
P. Deepa
Students of B.E Computer science and Engineering in S.A. Engineering College
M. Divya dharani
Students of B.E Computer science and Engineering in S.A. Engineering College
E. Karthiga
Students of B.E Computer science and Engineering in S.A. Engineering College

----------**ABSTRACT**----------

Cloud storage is a type of storage used by individuals and organizations to store files and share files on the internet. Some cloud servers can be fully trusted, although access control is challenged. The encryption technique is used in this project to improve the security of cloud storage. Based on the attributes in this paper, we provide safe and efficient data access control for cloud storage. The cloud owner will not communicate directly with the cloud user instead of communicating with the cloud provider for storage. The cloud provider contacts the owner and the user. The cloud provider gives the key to the user. Cloud users will request the download of the encrypted file. The cloud provider provides the secret key to the user. A new secret key will be created for each file. Secret keys and updates to cipher text are carried out in a very public way. By examining it with the related works, we demonstrate the merits of our theme and apply it further to demonstrate its practicality. The random oracle model theme is also tested securely.

Keywords - **Access control, cloud storage, multi-authority cipher text-policy attribute-based encryption (CP-ABE), revocation.**

I. INTRODUCTION

Cloud storage is one of the key for cloud computing services.Data owners can remotely host their data by outsourcing them to cloud servers, making it easy for individuals and companies to share information on the Internet. However, this new approach challenges the approaches of traditional data access control scenarios, where a trusted server is responsible for the implementation of access control mechanisms, since outsourced data (e.g. health records for patients and business development projects) can be sensitive and valuable to data owners and few cloud servers. The attribute-based access control, which uses cipher text-policy attribute-based encryption (CP-ABE), is very promising among the various solutions proposed for the safe sharing of data in cloud storage systems. A set of personal attributes describes each user in this setting and has a secret key according to the attributes of the authority. A data owner defines an access policy for attributes and encrypts the data to be outsourced under this policy. Cloud servers are therefore only outsourced to users whose attributes comply with the access policy and encrypt external data. This effectively prevents unauthorized users from accessing outputs (including cloud servers). CPABE is divided into categories depending on whether one authority or different authorities administer the attributes. In practical terms, this is of course more desirable for cloud storage systems. However, the original multi-authority CP-ABE cannot be deployed directly on cloud storage systems due to the following two problems. First, the public parameter of these schemes depends on the attribute of the universe, which means that the universe attribute is fully fixed when the system is completed. However, the need to add new attributes to the system is very common in practical applications. Second, users of the system would dynamically join or leave a cloud storage system. This requires permission to change these users. This also requires the authorization of these users to be changed. In particular, users should not only be prevented from accessing externalized data previously available (forward security), but also from accessing externalized data (backward security), even if their attributes comply with the relevant access policies. In this study, we will use multi-authority CP-ABE to solve these problems in cloud storage.

II. PRELIMINARIES

This section describes the preliminary approach [2, 3, 5, and 7]. This approach explains about the security in cloud. Next we have explained two models from the literature.

4.1 Bilinear Maps

[2, 3, 5]We are proposing an ABE system. As an ABE authority, a user can simply create a public key and issue private keys to different users. A user can encrypt data from a set of authorities; our greatest hurdle is to make collision resistant. We prove our system secure using the recent dual system encryption methodology. Security proofs work by converting cipher text and private keys to semi-functional shape and then gaining security. Our design is based on some facts about groups with efficiently computable bilinear maps.

Let G0 and G1 be two primary order p multiplicative cyclic groups. Let g be G0's generator.A bilinear map is a function of injection e: G0 × G0 → G1 with the following properties:

- Bilinearity: for all u, v ∈G0 and a, b ∈Zp, we have e (u^a, v^b) = e (u, v) ^{ab}.
- Non-degeneracy: e (g, g) 6= 1.
- Computability: An effective algorithm is available for calculation e (u, v) for ∀u, v ∈G0.

TABLE 1

Average Timing Results of Operations in Prime and Composite order Groups (Unit: Ms)

Operations	Prime order	Composite order	Ratios
Pairing	5.12	421.43	82.3
Exp. in G	4.21	173.08	42.0
Exp. in GT	0.62	31.93	51.5

1.2 Complexity Assumptions

[2, 5, 7]The ABE is a new public encryption that allows users to encrypt and decrypt messages. The ABE is a public encryption. The user can generate cipher text for example, which can only be decrypted by other attributes users. It is currently used for cloud and computer storage.The disadvantage is the size and the time required to decrypt the text. We suggest a new paradigm which eliminates users ' overheads. Bandwidth and decryption are saved by the user. Decisional Bilinear Diffee-Hellman (DBDH) Assumption let a, b, c, z ∈Zp be chosen at random and g be a generator of G0. The DBDH assumption [5] states that no probabilistic polynomial-time algorithm B can distinguish the tuples (A = g^a,B = g^b,C = g^c, e(g, g)^{abc}) from the tuple (A = g^a,B = g^b,C = g^c, e(g, g) ^{z}) with non-negligible advantage.

III. RANDOM ORACLE CONSTRUCTION

[4]Identity-based encryption (IBE) is an exciting alternative to public key encryption because IBE eliminates the need for PKI. PKI is a means of dismissing users from the system. The most practical solution involves the use of time periods by senders. When encrypting and updating all receivers by contacting trusted authority to update private keys regularly. This IBE scheme enhances trusted party key-update. In key generation and encryption algorithms, we drastically reduce computational overhead by replacing T with a hash function used as a random oracle. A simple argument shows that it is possible to "program" the random oracle so that Sahai and Waters ' security proof still holds. For further discussion on the random oracle model, we refer the reader to the literature [4, 8]. The following characteristics are the implementation of T as a random oracle.

First, cipher texts can contain a variable number of attributes, rather than be required to contain n. Second, the n + 1 exponentiations needed to solve T in the Sahai-Waters construction have been replaced with a single cryptographic hash.

However, using model that requires the random oracle heuristic results in a slightly weaker security model; the use of random oracles makes the security of the cryptosystem dependent upon the security of the hash function used to compute T. In Section 6, we experimentally compare implementations of the original Sahai and Waters construction with our variant.

IV. SECURITY

4.1 Backward Security

[10]Our construction guarantees the backward security of the cipher text by providing the functionality of user revocation. In our scheme, we note that only a correct decryption key, which is derived from the original secret key and the current update key in a random manner, can be used to correctly decrypt the corresponding cipher texts. When a user is removed from an attribute domain Uδ, by the KUNodealgorithm, we know that those subsequently published update keys are useless for him/her, since Path (η) _Yδ= ∅. Therefore, without help of the update key, the user can no longer get a correct decryption key, and thus cannot decrypt those subsequently produced cipher texts.

4.2 Forward Security

The forward security of our scheme comesfrom public cipher text update. More precisely, among the cipher textcomponents{Ci, ζ} i∈ [l], ζ∈Tt, we note that the termCi,ζtis mandatorily required for the decryption procedure, and other terms in fact are only used to update Ci, ζttoCi, ζt for a new time period t_ > t. By the construction of Tt, we know that this update procedure is unidirectional, that is, Ci,ζtcannot be conversely derived from Ci,ζt.

Therefore, when the cipher text CTtis updated to CTt_ and then erased, those previously generateddecryption keys naturally expire.

V. COMPARISON FOR PERFORMANCE EVALUATION

TABLE 2

Comparisons of Functionalities with Previous Works

Literature survey	Authority	Revocation level	Forward security	Backward security	Algorithm
[1]	Multiple	Attribute	Yes	Yes	IBE
[2]	Single	Attribute	No	No	KP-ABE & HIBE
[3]	Single	Attribute	No	No	CP-ABE
[4]	Multiple	Attribute	No	No	ABE
[5]	Single	Attribute	No	No	KP-ABE & CP-ABE
[6]	Single	Owner	No	No	CP-ABE
[7]	Single	Attribute	Yes	Yes	CP-ABE
[8]	Single	User and owner as attribute	No	No	DACC
[9]	Multiple	Unauthorized user	No	No	ABE
[10]	Multiple	Attribute	Yes	Yes	Multi-authority CP-ABE
Ours	Multiple	Customer	Yes	Yes	Multi-authority CP-ABE

VI. CONCLUSION

We discussed the various encryption techniques used in cloud storage for security. We are building a secure, secure and effective multi - authority access control system for cloud data sharing information by studying all of these.This scheme supports the revocation of scalable users and the update of public cipher text. The cloud user can download the file safer using the encryption technique.For all these we use a multi-authority cp-abe encryption technique. These predicted results are then used for encrypting the file for multiple users without any key failure.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy encryption based on identity," in Proc. Adv. Cryptol.—EUROCRYPT 2005. New York, NY, USA: Springer, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf.Comput. Commun. Security, 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B.Waters, "Cipher text-policy attribute-based encryption," in Proc. IEEE Security Privacy 2007, 2007, pp. 321–334.

[4] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure systems based on attributes," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 99–112.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute - based sharing of data with revoking attributes," in Proc. 5th ACM Symp. Inf., Comput. Commun.Security 2010, 2010, pp. 261–270.

[6] J. Hur and D. K. Noh, "Attribute - based control of access with efficient data outsourcing revocation," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, Jul. 2011.

[7] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC - MACS: Effective control of data access for cloud storage systems with multi-authorities," IEEE Trans.Inf. Forensics Security, vol. 8, no. 11, pp. 1790–1801, Nov. 2013.

[8] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Control of distributed access in cloud," in Proc. 2011 IEEE 10th Int. Conf. Trust, Security PrivacyComput. Commun, 2011, pp. 91–98.

[9] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records using attribute - based encryption in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[10] J. Hong, K. Xue, and W. Li, "Security analysis of attribute revocation for cloud storage systems in multi - authority data access control," IEEE Trans.Inf. Forens. Security, vol. 10, no. 6, pp. 1315–1317, Jun. 2015.