A Practical Attribute-Based Document Collection Hierarchical Encryption Scheme In Cloud Computing

Naga Satthibabu Alumolu , Dr.I.R.Krishnam Raju , Sri.V.Bhaskara Murthy
Mca Student, Professor, Associate Professor
Dept Of Mca
B.V.Raju College, Bhimavaram

ABSTRACT

Ciphertext-policy attribute-based encryption can provide _ne-grained access control and secure data sharing to the data users in cloud computing. However, the encryption/decryption efficiency of existing schemes can be further improved when encrypting a large document collection. In this paper, we propose a practical Ciphertext-Policy Attribute-Based Hierarchical document collection Encryption scheme named CP-ABHE. By practical, we mean that CP-ABHE is more efficient in both computation and storage space without sacrificing data security. In CP-ABHE, we first construct a set of integrated access trees based on the documents' attribute sets.We employ the greedy strategy to build the trees incrementally and grow the trees dynamically by combining the small ones. Then, all the documents on an integrated access tree are encrypted together. Different to existing schemes, the leaves in different access trees with the same attribute share the same secret number, which is employed to encrypt the documents. This greatly improves the performance of CP-ABHE. The security of our scheme is theoretically proved based on the decisional bilinear Diffine Hellman assumption. The simulation results illustrate that CP-ABHE performs very well in terms of security, efficiency, and the storage size of the ciphertext.

I.INTRODUCTION

Cloud computing collects and organizes a large amount of information technique resources to provide secure, efficient, flexible and on demand services [29]. Attracted by these advantages, more and more enterprise and individual users trend to outsource the local documents to the cloud. In general, the documents need to be encrypted before being out- sourced to protect them against leaking. If the data owner wants to share these documents with an authorized data user, they can employ any searchable encryption techniques [2], [6], [9], [14], [30], [31] or privacy-preserving multi-keyword document search schemes [3], [5], [8], [37] to achieve this goal.

However, all these schemes cannot provide _ne-grained access control mechanisms to the encrypted documents. Attribute-based encryption (ABE) schemes can provide complicated systems to diversify the data users' access paths. In ABE schemes, each document is encrypted individually and a data user can decrypt a document if her attribute set matches the access structure of the document. Existing ABE schemes can be divided into Key-Policy ABE (KP-ABE) schemes [11], [12], [15], [16], [20], [24], [25], [28] and Cipher text-Policy ABE (CP-ABE) schemes [1], [7], [10], [19], [21]_[23], [27], [34]. Com- pared with KP ABE schemes, CP-ABE schemes are more flexible and suitable for general applications.

In the following, we must analyze the existing ABE schemes in detail and further present the novelty and innovation of the CP-ABHE scheme proposed in this paper. For convenience, we choose the schemes in [1] and [11] as typical examples of KP-ABE scheme and CP-ABE scheme, respectively. LetG0 andG1 be two multiplicative cyclic groups of prime order p. Let g be a generator of G0 and e be a bilinear map, e V G0 _ G0 D G1. Further, let H V f0; 1g_ ! G0 be a hash function which can map an attribute string to a random element in G0. Assume that we need to encrypt a set of documents F D fF1; F2; _ _ _ ; FN g. Attribute set A D fA1; A2; _ _ _ ; AMg is the common attribute dictionary of both documents and data users. We further assume that document Fi is related with a set of attributes, denoted as att(Fi).

We encrypt F in two phases. First, each document Fi is encrypted by a proper symmetric encryption algorithm with a unique content key cki. Second, all the content keys of F are encrypted by ABE schemes. Note that, both the ciph texts of Fi and cki are provided to data users. In decryption process, data users need to _rest decrypt cki based on their attribute- related secret keys and then decrypt document Fi based on cki. In this way, cipher text of Fi can be decrypted only by the data users who have the matched attributes with att(Fi). Considering that the _rest encryption phase does not fall in the scope of this paper, we focus on the second phase which is strongly related to the proposed scheme.

To encrypt all the content keys of F, KP-ABE scheme in [9] is executed as follows. For each content key cki with attribute set att(Fi) and access tree T , the public key is calculated as PK D fe(g; g)_; 8j 2 att(cki); Tj D grj g where _ is a random num- ber in Zp and rj is a number randomly chosen from Zp for attribute j. Then the ciphertext of cki is calculated as CTcki D fT ; cki _ e(g; g)_s; 8j 2 att(Fi); Ej D T s j g where s is a random number in Zp. The above process must be executed for N times to encrypt all the content keys. The total number of elements in the ciphertext can be calculated as Ncip D N C PNi D1 jatt(Fi)j, where jatt(Fi)j denotes the number of attributes in att(Fi). To decrypt the cipher text of cki, a data user needs to store the secret key SK D f8j 2 att(Fi);Dj D g qj(0) rj g, where qj(x) is the polynomial of the leaf node in T corresponding to attribute j. To decrypt all the content keys, N secret keys for the N access trees need to be stored by a data user and the number of total secret values in the keys can be calculated as Nsk D PNi D1 jatt(Fi)j. It can be observed that Nsk increases with the increasing of documents' number and we call this as the secret key expanding problem.

To encrypt all the content keys of F, CP-ABE scheme in [12] is executed as follows. For each content key cki with attribute set att(Fi) and access tree T , the public key is calculated as PK D fh D g_; e(g; g)_g, where _ and _ are random numbers in Zp. Then the scheme calculates the cipher text of cki as CTcki D fT ; cki _ e(g; g)_s;C D hs; 8j 2 att(Fi); Cj D gqj(0);C0 j D H(j)qj(0)g, where qj(x) is the poly-nomial of the leaf node in T corresponding to attributes j. Similar to KP-ABE, the above process is also executed for N times to encrypt all the content keys. The total number of elements in the cipher text can be calculated as Ncip D 2 _ N C 2 _ PNi D1 jatt(Fi)j. Apparently, Ncip greatly expands with the increasing of documents' number. To decrypt the cipher text of cki, the secret key of a data user is calculated as SK D fD D g (_Cr) _ ; 8j 2 att(Fi); Dj D grH(j)rj ;D0 j D grj g where r is a random number in Zp and rj is a random number chosen from Zp for attribute j. Both the KP-ABE and CP-ABE schemes are impractical to encrypt a large document collection because of the following reasons.

First, the encryption process in both the two schemes is executed N times, leading to high computation complexity. Second, there is a tradeoff between the size of the content keys' ciphertext and data users' secret keys. In KP-ABE, the number of secret values in a data user's secret key is extremely large for a document collection, imposing a heavy burden on the data user. In CP-ABE, the size of the cipher text is extremely large. Consequently, CP-ABE scheme increases the data transmission amount between the cloud server and data users, which is a huge challenge for the network.

This is reasonable considering that the access structure of each document must been bedded into the cipher text or the secret keys. Third, decrypting the cipher text is also time-consuming considering that each document is encrypted individually. Recently, Wang et al. [33] attempted to improve the encryption efficiency and propose a _le hierarchy attribute-based encryption scheme named FH-CP-ABE. However, this scheme focused only on how to encrypt a set of documents that share an integrated access tree and hence it also cannot be directly employed to encrypt a document collection.

II.EXISTING SYSYEMS

- Attribute-based encryption schemes have been widely researched in the literatures. The fuzzy identity-based encryption (Fuzzy IBE) scheme proposed by Sahai and Waters [28] is widely treated as the origin of attribute-based encryption (ABE). Sahai and Waters first employ the term ``attribute based encryption (ABE)" in the field of information security. Inspired by Fuzzy IBE, many ABE schemes are designed including KP-ABE schemes and CP-ABE schemes. Goyal et al. extend the Fuzzy IBE scheme and propose the key-policy attribute-based-encryption (KP-ABE) in [11]. Though KP-ABE can provide fine-grained access control, it restricts its attention to the monotone access structure only.

- In [25], Ostrovsky et al. construct a KP-ABE scheme which allows a user's private key can be expressed in terms of any access formula over attributes. Further, they prove the scheme's security based on decisional bilinear Diffie- Hellman assumption. Yang et al. [38] propose a scheme which performs well in terms of both access structure expressivity and security. CP-ABE schemes are more flexible and suitable for general applications and many varieties of CP-ABE schemes have been proposed in the literatures [1], [10], [34]. In CP-ABE schemes, the access structures are embedded in the ciphertext and each data user is assigned with a set of attributes. A data user can decrypt a ciphertext if and only if their be matched with each other.

- Pirretti et al. [26] introduce a novel secure information management architecture based on ABE primitives. A policy system which meets the needs of different data users is designed and used to encrypt distributed file systems. The hierarchical ABE (HABE) scheme [32] is proposed by combining a hierarchical IBE scheme and a CP-ABE scheme. HABE scheme can help the enterprise users to efficiently share confidential data in cloud computing by simultaneously achieving fine-grained access control, high performance, practicability, and scalability. Zhu et al. [39] also propose a file sharing scheme

in cloud computing based on ABE and the security and efficiency of the scheme are evaluated.

- Li et al. [17] provide a CP-ABE scheme with efficient data user revocation for cloud storage. KSF-OABE scheme [18] integrates the keyword search function into the ABE scheme which can improve the search efficiency of ciphertexts. Though all the above proposed schemes can be used in cloud computing, they are designed for encrypting a single document. They cannot be directly employed to encrypt a large document collection, because the encryption/decryption efficiency is low if we encrypt each file singly.

Disadvantages

- In the existing work, the system is less secured due to lack of CP-ABHE, KP-ABE.
- The system's security is very less due to lack of strong cryptography techniques.

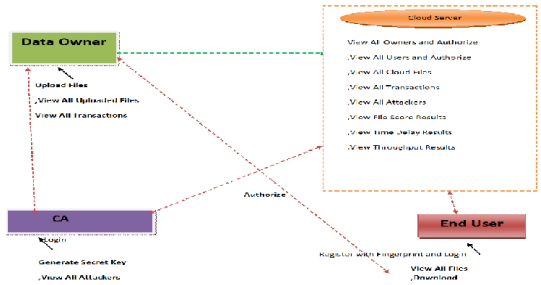
III. PROPOSED SYSYEM

- In the proposed system, the system designs an attribute-based document hierarchical encryption scheme named CP-ABHE which performs well in terms of computation and storage space efficiency. The scheme consists of two modules including integrated access tree construction and tree encryption. We first propose an algorithm to generate the integrated access trees for a document collection. The most important design goal of the algorithm is decreasing the number of integrated access trees which can greatly improve the encryption/decryption efficiency.
- An algorithm to construct the integrated access trees incrementally for the document collection is proposed and it can significantly decrease the number of the access trees.
- A document collection hierarchical encryption scheme is proposed. All the documents that share an integrated access tree are encrypted together which can significantly improve the encryption/decryption efficiency. Moreover, the secret key expanding problem is solved properly.
- The security of CP-ABHE is theoretically proved and the effectiveness of the integrated access tree construction algorithm is analyzed in detail. In addition, a thorough comparison between CP-ABHE, KP-ABE, and CP-ABE in terms of encyption/decryption efficiency and storage space is provided.

Advantages

- The system is implemented based on Attribute Based Encryption scheme which gives more security on data.
- The system is more secured due to CP-ABHE (Attribute Based Hierarchical Encryption).

IV.ARCHITECTURE DIAGRAM



V.IMPLEMENTATION

DATA OWNER:

In this module, initially the data owner has to register to the cloud server and get authorized. After the authorization from cloud data owner will encrypt and add file to the cloud server where in after the addition of file data owner View All Uploaded Files, View All Transactions.

CLOUD SERVER

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with cloud End users and performs the following operations such as View All Owners and Authorize ,View All Users and Authorize ,View All Cloud Files ,View All Transactions,View All Attackers ,View File Score Results ,View Time Delay Results ,View Throughput Results

CA

CA generates the content key and the secret key requested by the end user and also
View All Attackers.

END USER

User has to register and login for accessing the files in the cloud. User is authorized by the cloud to verify the registration. User has to View All Files
,Download.

VI.CONCLUSIONS

In this paper, we design a hierarchical document collection encryption scheme. We must design an incremental algorithm to construct the integrated access trees of the documents and decrease the number of trees. Then, each integrated access tree is encrypted together and the documents in a tree can be decrypted at a time. Different to existing schemes, we construct the secret numbers for the nodes of the trees in a bottom-up manner. In this way, the sizes of cipher text and secret keys significantly decrease. At last, a thorough performance evaluation is provided including security analysis, efficiency analysis, and simulation. Results show that the pro- posed scheme outperforms KP-ABE and CP-ABE schemes in terms of encryption/decryption efficiency and storage space. Our scheme can be further improved in several aspects: First, the access policy discussed in Section III assumes that the access trees are composed of only ``AND" gates. Extending the flexibility and versatility of the access policy is one of the most important research directions. Second, the documents are encrypted before outsourcing and a promising task is how to efficiently search the interested documents over the cipher texts. At last, we focus our attention on the static document collection and how to efficiently encrypt/decrypt a dynamic document collection will be also researched in the future.

REFERENCES

J. Bethencourt, A. Sahai, and B.Waters, ``Ciphertext-policy attribute-based
encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321_334.

[2] D. Boneh and B. Waters, ``Conjunctive, subset, and range queries on
encrypted data," in Proc. TCC, 2007, pp. 535_554.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, ``Privacy-preserving multi-
keyword ranked search over encrypted cloud data," IEEE Trans. Parallel
Distrib. Syst., vol. 25, no. 1, pp. 222_233, Jan. 2014.
[4] A. D. Caro and V. Iovino, ``jPBC: Java pairing based cryptography," in
Proc. IEEE Symp. Comput. Commun. IEEE Comput. Soc., Jun. 2011,
pp. 850_855.
[5] C. Chen et al., ``An ef_cient privacy-preserving ranked keyword search
method," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 4, pp. 951_963,
Apr. 2016.
[6] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, ``Searchable symmet-
ric encryption: Improved de_nitions and ef_cient constructions," in Proc.
ACM CCS, 2006, pp. 79_88.
[7] H. Deng et al., ``Ciphertext-policy hierarchical attribute-based encryption
with short ciphertexts," Inf. Sci., vol. 275, pp. 370_384, Aug. 2014.
[8] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, ``Enabling personalized search
over encrypted outsourced data with ef_ciency improvement," IEEE
Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 2546_2559, Sep. 2016.
[9] P. Golle, J. Staddon, and B. Waters, ``Secure conjunctive keyword search
over encrypted data," in Proc. ACNS, 2004, pp. 31_45.
[10] V. Goyal, A. Jain, O. Pandey, and A. Sahai, ``Bounded ciphertext policy
attribute based encryption," in Automata, Languages and Programming.
Berlin, Germany: Springer, 2008, pp. 579_591.
[11] V. Goyal, O. Pandey, A. Sahai, and B.Waters, ``Attribute-based encryption
for _ne-grained access control of encrypted data," in Proc. 13th ACMConf.
Comput. Commun. Secur., 2006, pp. 89_98.
[12] J. Han, W. Susilo, Y. Mu, and J. Yan, ``Privacy-preserving decentralized
key-policy attribute-based encryption," IEEE Trans. Parallel Distrib. Syst.,
vol. 23, no. 11, pp. 2150_2162, Nov. 2012.
[13] J. Lai, R. H. Deng, C. Guan, and J.Weng, ``Attribute-based encryption with
veri_able outsourced decryption," IEEE Trans. Inf. Forensics Security,
vol. 8, no. 8, pp. 1343_1354, Aug. 2013.
[14] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ``Fully
secure functional encryption: Attribute-based encryption and (hierarchical)
inner product encryption," in Proc. EUROCRYPT, 2010, pp. 62_91.
[15] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, ``Fully
secure functional encryption: Attribute-based encryption and (hierarchical)
inner product encryption," in Proc. Int. Conf. Theory Appl. Cryptograph.
Techn. Berlin, Germany: Springer-Verlag, 2010, pp. 62_91.