A Proficient Hierarchical ABE Access Control for Securing Cloud Data and Its Performance Analysis

[1]SADIA SYED,[2]M.USSENAIAH
[1]Research Scholar, Dept. of Computer Science, Vikrama Simhapuri University, Nellore, A.P
[2]Assistant Professor Dept. of Computer Science,Vikrama Simhapuri University, Nellore, A.P

Abstract

Proficient Hierarchical Attribute Based Encryption by extend cipher text-policy attribute based encryption with a hierarchical structure of users. The proposed schemes not only achieve scalability due to its hierarchical structure, but also inherit elasticity and fine-grained access control in supporting complex attributes. The layered access structures are integrated into a single access structure, and then, the hierarchical files are encrypted with the incorporated access structure. The cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage and time cost of encryption is saved. The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of academics, healthcare and the military. However, the hierarchy structure of shared files has not been explored in CP-ABE. While in our system attributes are used to describe a user's credentials, and Encrypting data determines a policy for who can decrypt. However, when organization users outsource top secret data for sharing on cloud servers, the adopted encryption system should not only support fine-grained access control, but also supply high performance, practicability, and scalability to best serve the needs of accessing data anytime and anywhere.

Keywords: HABE, Fine-grained access control, Cloud Storage

1. INTRODUCTION

Proficient HABE not only maintains compound attributes due to flexible attribute set combinations, but also attains efficient user revocation because of multiple value assignments of attributes. We properly proved the security of Proficient HABE based on the security of existing ABE schemes. To end with, we realized the suggested proposal, and accomplished complete performance analysis and evaluation, which demonstrated its effectiveness and benefits over obtainable schemes. The scope of the work is to build up a new computing technology necessitates users to hand over their precious data to cloud providers, thereby raising safety and confidentiality concerns on outsourced data.

2. RELATED WORKS

Since Gentry and Silverberg [1] proposed the firstnotion of hierarchical encryption scheme, many hierarchicalCP-ABE schemes have been proposed. For example,Wang et al. [2] proposed a hierarchical ABE scheme by combining the hierarchical IBE [1] and CP-ABE. Wan et al.

[3]proposed hierarchical ABE scheme. Later, Zou [4] gave ahierarchical ABE scheme, while the length of secret keyis linear with the order of the attribute set. A ciphertextpolicy hierarchical ABE scheme with short ciphertext is alsostudied in [5]. In these schemes, the parent authorizationdomain governs its child authorization domains and a top-levelauthorization domain creates secret key of the next-leveldomain. The work of key creation is distributed on multipleauthorization domains and the burden of key authority centeris lightened.

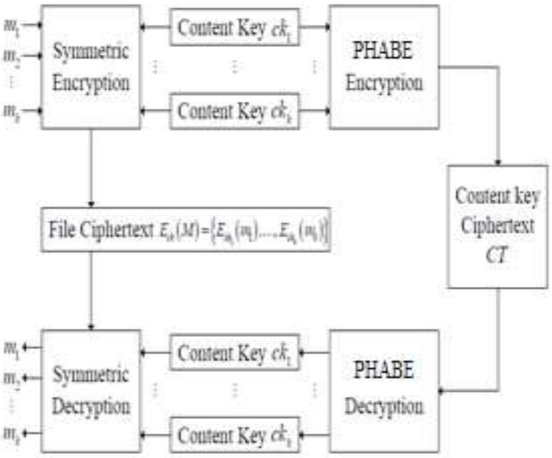
At present, there are three types of access structuresAND gate, access tree, and linear secret sharingscheme (LSSS) used in existing CP-ABE schemes.Cheung and Newport [6] first used AND gate accessstructure to achieve CP-ABE scheme. Later, some improvedschemes [7], [8], [9] are proposed. Meanwhile, there areCP-ABE schemes based on access tree [10], [11], [12]–[13]that support AND, OR, and threshold, and based onLSSS [14], [15], [16], where [10] and [15] are the typicalschemes of access tree and LSSS.

3. PROFICIENT HIERARCHICAL ATTRIBUTE BASED ENCRYPTION

“Proficient Hierarchical ABE Access Control for Securing Cloud Data and Its Performance Analysis” is to create a fully fledged web application which would communicate with the remote server to send and retrieve data as per requirement. The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of healthcare and the military. However, the hierarchy structure of shared files has not been explored in CP-ABE. Even though Cloud allows data users to outsource/share their data while enjoying affordable Price and high scalability. Proficient hierarchical attribute-based encryption can be the right cryptographic tool solving these concerns. Data owners can specify access control policy on outsourced data while encrypting it, and users can decrypt cipher texts only if their attributes satisfy the access control policy. However, ABE is not sufficient for data sharing applications since users’ access rights are not static: a user’s access right might be revoked if he/she leaves the organization.

This proposed model is to improve the cloud data security by incorporating various

The main reason for making this algorithm client side is to have the self-satisfaction and to ensure security for the clients of the cloud. Even though cloud is not trustworthy using this proposed method data can be stored in the cloud environment by implementing



Request Access for file and data’s From Data Owner, Secret Word for Security (attribute), the attribute must need for downloading file, Logical position for attribute,we improve the efficiency of the algorithm by Introducing Content keys,we introduces data segmentation and de-segmentation process,Triple Content keys,Encrypting keys rather data to reduce heavy computation.

4. SECURITY ANALYSIS OF PROFICIENT HIERARCHICAL ATTRIBUTE BASED ENCRYPTION

We have developed web application by considering the structure of university which consists of different departments. All departments are monitored by highest centralized authority known as “Admin”. Each department has a head of department called as “HOD” who controls all the employees working at a lower level. This is hierarchical implementation.

Step-I: (PK, MSK) ← Setup (1κ):

The probabilistic operation takes a security parameter κ as input and outputs public key PK and master secret key MSK.

Step-II: (SK) ← KeyGen(P K, M SK, S):

The operation inputs PK, MSK and a set of attributes S and creates a secretkey SK.

Step-III: File Encrypted Data ← FileEncrypt(FileData m, ContentKeyck):

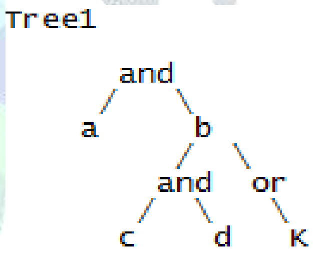
The operation inputs File Data m and Content Key ck and using of content key ck we can encrypt the file data and store in cloud.

A data owner processes the files as follows:

Firstly, the data owner chooses *k* content keys {*ck*1, . . . ,*ckk*},and encrypts files {*m*1, . . . ,*mk*} with the content keys by using symmetric encryption algorithm

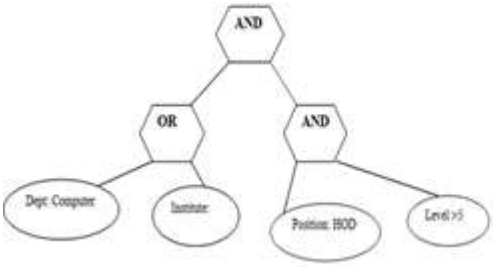
Step-IV:(cki (i ∈ [1, k])) ← **Decrypt**(PK,CT, SK). The algorithm inputs PK, CT which includes an integrated access structure A, SK described by a set of attributes S. If the S matches part of A, some content keys cki (i ∈ [1, k]) can be decrypted. If it matches the whole A, all the content keys can be decrypted. Then, the corresponding files mi (i ∈ [1, k]) will be decrypted with the content keys by the symmetric decryption algorithm.

Proficient HABE a node in access policy tree is either a terminal or non terminal node, each non terminal node can be described in terms of a Boolean function. Each terminal node is labeled with a constant from {0, 1} and has no child node. Each policy is represented as a Boolean function. We use simplification of Boolean expressions to reduce a lengthy expression in the tree to simple form this reduces the computation time while using access structure as a key. The major focus is minimizing access structure without loss of generality.



PHABE Performs scan in the tree from root, level by level if the condition is not satisfied at one level then no need to scan the remaining portion and decryption is not possible.

In Proficient HABE where each element is either a set or an element related to attribute. Depth of the key structure decides the level of recursive set. Member set at depth 1 can either sets or Attribute elements but members at depth 2 may only attributes elements. Consider the example where {Dept: Computer, Institute: VSU, Position: Lecturer, Level: 3}, {Position: HOD, Level: 6} is key structure of depth 2. It represents attributes related to one person who is tester at level 3 and manager at level 6 as shown in figure.



Proficient HABE introduces tree access structure in which nonleaf nodes are threshold gates and leaf nodes are attributes. In the following figure, AND" and „OR" gates are used tree only demands HOD in computer department or VSU of level value larger than 5. Access structure and attribute sets are compared if attribute set satisfy

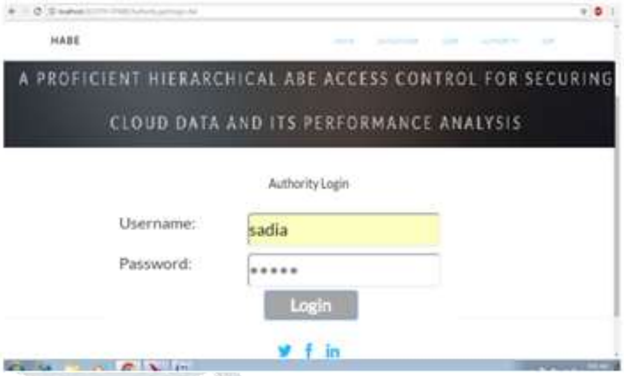
```
The same may also constructed like(a^b^c^d) or (a^b v k)

   and
  /|\\
 a b c d
   |
   or
    \k
```

tree access structure then access is provided to user belongs to that access tree structure.

Fine-grained access control is achieved as data owner can define expressive policy for file access. This resulted in an efficient system response time as well as increased performance of the system. For security purpose, it keys are provided private key, public key content key and master key. Scalability is achieved by distributing the workload within hierarchical structure. Another feature provided is User Revocation that allows expiration of user's key to be updated after the duration of key is near to expiration. System model consists of 5 types of components as data owner, data consumer, cloud service provider, domain authorities, and a trusted authority.

5. EXPERIMENT RESULTS

Authority Login:



A PROFICIENT HIERARCHICAL ABE ACCESS CONTROL FOR SECURING CLOUD DATA AND ITS PERFORMANCE ANALYSIS

Authority Login

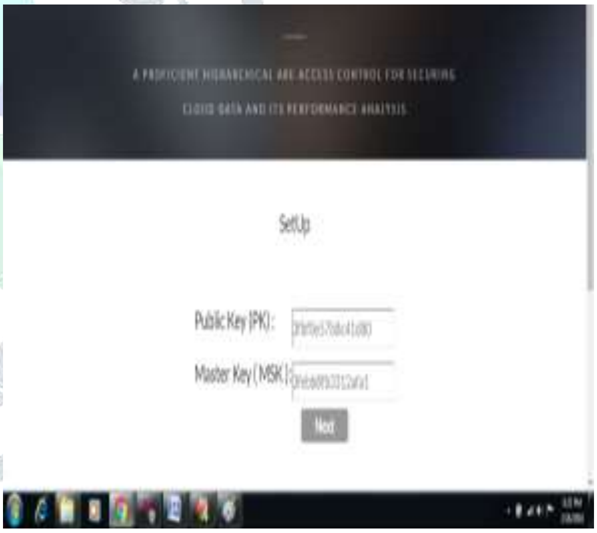
Username: sadia

Password: •••••

Step-I: (PK, MSK) ← Setup(1κ):

The probabilistic operationtakes a security parameter κ as input and outputs public key PK and master secret key MSK.

Generating Keys:



A PROFICIENT HIERARCHICAL ABE ACCESS CONTROL FOR SECURING CLOUD DATA AND ITS PERFORMANCE ANALYSIS

SetUp

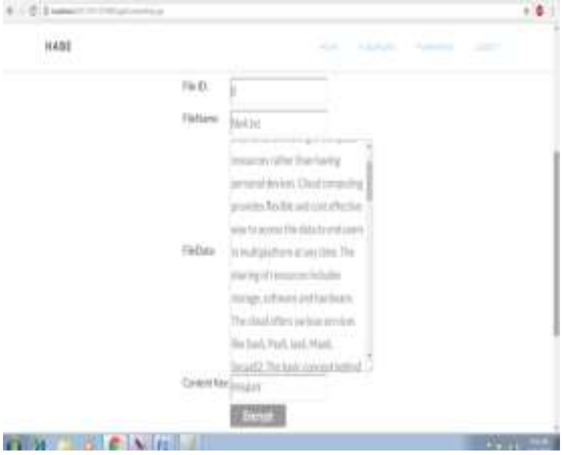
Public Key (PK): [illegible]

Master Key (MSK): [illegible]

Step-II: (SK) ← KeyGen(P K, M SK, S):

The operation inputs PK, MSK and a set of attributes S and creates a secretkey SK.

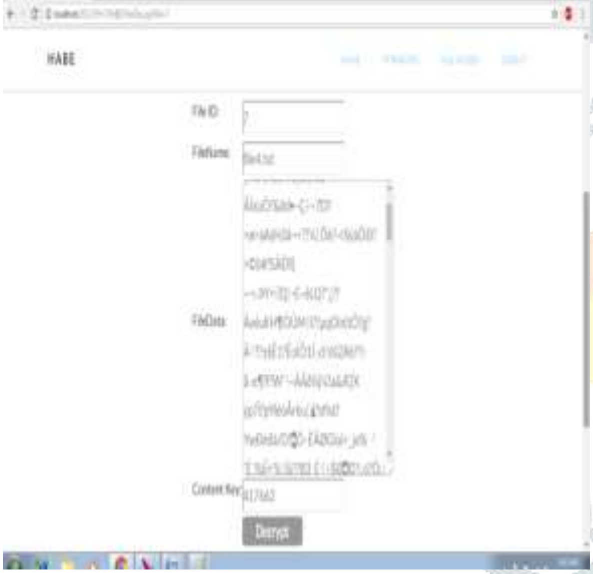
DataOwner-Generating FileId, ContentKey:

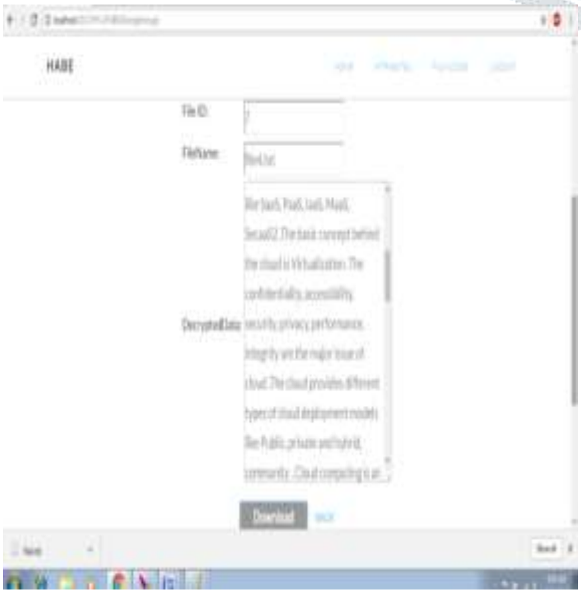


Encrypting Data to Upload File:

Step-III: File Encrypted Data ← FileEncrypt(FileData m, ContentKeyck):

Downloading File:





Step-IV:(cki (i ∈ [1, k])) ← **Decrypt**(PK,CT, SK). The algorithm inputs PK, CT which includes an integrated access structure A, SK described by a set of attributes S. If the S matches part of A, some content keys cki (i ∈ [1, k]) can be decrypted. If it matches the whole A, all the content keys can be decrypted. Then, the corresponding files mi (i ∈ [1, k]) will be decrypted with the content keys by the symmetric decryption algorithm.

6. CONCLUSION

We proposed a variant of ABE to efficiently share the files in cloud computing. The files are encrypted with an integrated access structure and the ciphertext components related to attributes could be shared by the files. Therefore ciphertext storage, time and cost of encryption are saved. The proposed scheme has an advantage that users can decrypt all authorized files by getting secret key once. Thus, the time of decryption is also saved if the user wants to decrypt multiple files.Proficient HABE access control scheme which is implemented to full fill the efficiency and security requirements in cloud. We formally proved the security of PHABE based on the security of CP-ABE. Finally, we implemented the proposed scheme, and conducted comprehensive performance analysis, which showed its efficiency and advantages over existing schemes.

7. REFERENCES

[1] C. Gentry and A. Silverberg, “Hierarchical ID-based cryptography,”in Advances in Cryptology. Berlin, Germany: Springer, Dec. 2002,pp. 548–566.

[2] G. Wang, Q. Liu, and J. Wu, “Hierarchical attribute-based encryptionfor fine-grained access control in cloud storage services,” in Proc. 17thACM Conf. Comput.Commun.Secur., Oct. 2010, pp. 735–737.

[3] Z. Wan, J. Liu, and R. H. Deng, “HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754Apr. 2012.

[4] X. Zou, “A hierarchical attribute-based encryption scheme,” Wuhan UnivJ. Natural Sci., vol. 18, no. 3, pp. 259–264, Jun. 2013.

[5] H. Deng et al., “Ciphertext-policy hierarchical attribute-based encryptionwith short ciphertexts,” Inf. Sci., vol. 275, pp. 370–384, Aug. 2014.

[6] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,”in Proc. 14th ACM Conf. Comput. Commun.Secur., Oct. 2007,pp. 456–465.

[7] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan,“CP-ABE with constant-size keys for lightweight devices,” IEEE Trans.Inf. Forensics Security, vol. 9, no. 5, pp. 763–771, May 2014.

[8] T. Nishide, K. Yoneyama, and K. Ohta, “Attribute-based encryption with partially hidden encryptor-specified access structures,” in Proc. 6th Int.Conf. Appl. Cryptogr. Netw.Secur., vol. 5037. Jun. 2008, pp. 111–129.

[9] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi,“A ciphertext-policy attribute-based encryption scheme with constantciphertext length,” in Proc. 5th Int. Conf. Inf. Secur. Pract.Exper.,vol. 5451. Apr. 2009, pp. 13–23.

[10] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in Proc. IEEE Symp.Secur. Privacy, May 2007,pp. 321–334.

[11] X. Xie, H. Ma, J. Li, and X. Chen, “An efficient ciphertext-policyattribute-based access control towards revocation in cloud computing,”J. Universal Comput. Sci., vol. 19, no. 16, pp. 2349–2367, Oct. 2013.

[12] V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded ciphertext policyattribute based encryption,” in Proc. 35th Int. Colloq. Automata, Lang.Program., vol. 5126. Jul. 2008, pp. 579-591.

[13] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, “Efficient and provablesecure ciphertext-policy attribute-based encryption schemes,” in Proc.5th Int. Conf. Inf. Secur.Pract.Exper., vol. 5451. Apr. 2009, pp. 1–12.

[14] A. Balu and K. Kuppusamy, “An expressive and provably secureciphertext-policy attribute-based encryption,” Inf. Sci., vol. 276,pp. 354–362, Aug. 2014.

[15] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive,efficient, and provably secure realization,” in Proc. 14th Int. Conf. Pract.Theory Public Key Cryptogr.(PKC), vol. 6571. Mar. 2011, pp. 53–70.

[16] 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. 29th Annu. Int. Conf.Theory Appl. Cryptogr.Techn., vol. 6110. May 2010, pp. 62–91.