RESEARCH ARTICLE OPEN ACCESS

An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing

[1]Gummala Brahmani, [2]J Rajasekhar, [3]V Sridhar Reddy

[1]PG Scholar, Dept of CSE, Vignana Bharathi Institute of Technology, Aushapur (v), Ghatkesar (M), Medchal Dist, Telangana, India.

[2]Assistant Professor, Dept of CSE, Vignana Bharathi Institute of Technology, Aushapur (v), Ghatkesar (M), Medchal Dist, Telangana, India.

3Associate Professor, Dept of CSE, Vignana Bharathi Institute of Technology ,Aushapur (v), Ghatkesar (M), Medchal Dist, Telangana, India.

Abstract:

Cipher text-policy attribute-based encryption (CP-ABE) has been a preferred encryption technology to solve the challenging problem of secure data sharing in cloud computing. 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. In this paper, an efficient file hierarchy attribute-based encryption scheme is proposed in cloud computing. The layered access structures are integrated into a single access structure, and then, the hierarchical files are encrypted with the integrated 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 are saved. Moreover, the proposed scheme is proved to be secure under the standard assumption. Experimental simulation shows that the proposed scheme is highly efficient in terms of encryption and decryption. With the number of the files increasing, the advantages of our scheme become more and more conspicuous.

Keywords — **Cloud computing, data sharing, file hierarchy, ciphertext-policy, attribute.**

1. INTRODUCTION

In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. Access control is paramount as it is the first line of defense that prevents unauthorized access to the shared data. With the burgeoning of network technology and mobile terminal, online data sharing has become a new “pet”, such as Facebook, MySpace, and Badoo. Meanwhile, cloud is one of the most promising application platforms to solve the explosive expanding of data sharing. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. Access control is paramount that prevents unauthorized access to the shared data. Recently, attribute-based encryption (ABE) has been attracted much more attentions since it can keep data privacy and realize fine-grained ,one-to-many n,and non interactive access control. Ciphertext-policy attribute based encryption (CPABE) is one of feasible schemes which has much more flexibility and is more suitable for general applications. In cloud computing, authority accepts the user enrollment and creates some parameters. Cloud ser-vice provider (CSP) is the manager of cloud servers and provides multiple services for client. Data owner encrypts and uploads the generated ciphertext to CSP. User downloads and decrypts the interested ciphertext from CSP. The shared files usually have hierarchical structure. That is, a group of files are divided into a number of hierarchy subgroups located at different access levels.

If the files in the same hierarchical structure could-based encrypted by an integrated access structure, the storage cost of ciphertext and time cost of encryption could be saved. cloud computing, a patient divides his PHR information M into two parts: personal information m1 that may contain the patient's name, social security number, telephone number home address, etc. The medical record m2 which does not contain sensitive personal information, such as medical test results, treatment protocols, and operation notes. Then the patient adopts CP-ABE scheme to encrypt the information m1 and m2 by different access policies based on the actual need. For example, an attending physician needs to access both the patient's name and his medical record in order to make a diagnosis, and medical researcher only needs to access some medical test results for academic purpose in the related area, where a doctor must be a medical researcher and the converse is not necessarily true.

2. RELEGATED WORK

2.1 Existing System

Sahai and Waters proposed fuzzy Identity-Based Encryption (IBE) in 2005, which was the prototype of ABE. Latterly, a variant of ABE named CP-ABE was proposed.Since Gentry and Silverberg proposed the first notion of hierarchical encryption scheme, many hierarchical CP-ABE schemes have been proposed. For example, Wang et al. proposed a hierarchical ABE scheme by combining the hierarchical IBE and CP-ABE.Wan et al. proposed hierarchical ABE scheme. Later, Zou gave a hierarchical ABE scheme, while the length of secret key is linear with the order of the attribute set. A ciphertextpolicy hierarchical ABE scheme with short ciphertext is also studied.In these schemes, the parent authorization domain governs its child authorization domains and a top-level authorization domain creates secret key of the next-level domain. The work of key creation is distributed on multiple authorization domains and the burden of key authority center is lightened.

2.2 Proposed System

In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CP-ABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control.The contributions of our scheme are three aspects.Firstly, we propose the layered model of access structure to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure. Secondly, we also formally prove the security of FH-CP-ABE scheme that can successfully resist chosen plaintext attacks (CPA) under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. Thirdly, we conduct and implement comprehensive experiment for FH-CP-ABE scheme, and the simulation results show that FH-CP-ABE has low storage cost and computation complexity in terms of encryption and decryption.

3. IMPLEMENTATION

3.1 Cloud Service Provider (CSP):

It is a semi-trusted entity in cloud system. It can honestly perform the assigned tasks and return correct results. However, it would like to find out as much sensitive contents as possible. In the proposed system, it provides cipher text storage and transmission services.

3.2 Data Owner:

It has large data needed to be stored and shared in cloud system. In our scheme, the entity is in charge of defining access

structure and executing Encrypt operation. And it uploads cipher text to CSP.

3.3 User:
It wants to access a large number of data in cloud system. The entity first downloads the corresponding cipher text. Then it executes Decrypt operation of the proposed scheme.

3.4 Authority:
In this system Authority can generate first Public Key PK and Master Key MK as well The authority executes the algorithm which inputs a set of attributes S(S ⊆ A˜) and creates a Secret Key SK and these keys can be send to authorized User‘s.

Algorithm:
The FH-CP-ABE scheme consists of below operations:
1) (PK, MSK) ← Setup(1κ):
The probabilistic operationtakes a security parameter κ as input and outputs public key PK and master secret key MSK.
2) (SK) ← KeyGen(P K, M SK, S):
The operation inputs PK, MSK and a set of attributes S and creates a secretkey SK.
3) 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.
4) (CT) ← Encrypt (PK, ck, A):
The operation inputs PK, ck = {ck1...ckk} and a hierarchical access tree A. At last, it creates an integratedciphertext of content keys CT.
5) (cki(i ∈ [1, k])) ← Decrypt(P K, CT, SK):
The algorithm inputs PK, CT which includes an integrated access structure A, SK described by a set ofattributes S. If the S matches part of A, some contentkeys cki(i ∈ [1, k]) can be decrypted. If it matches thewhole A, all the content keys can be decrypted. Then,the corresponding files mi(i ∈ [1, k]) will be decryptedwith the content keys by the symmetric decryptionalgorithm.

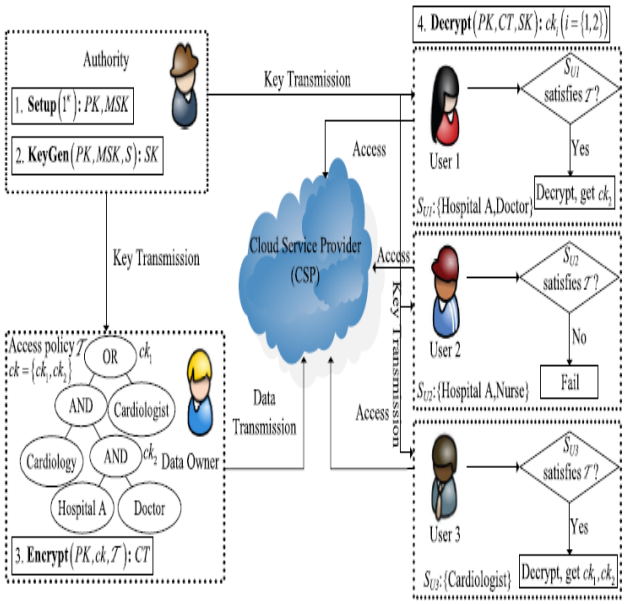

Fig 1 Architecture Diagram

4. EXPERIMENTAL RESULTS

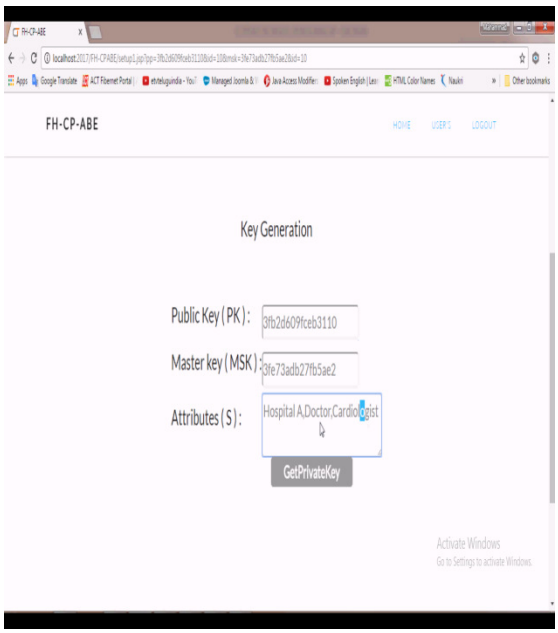

Fig 2 KeyGeneration Page

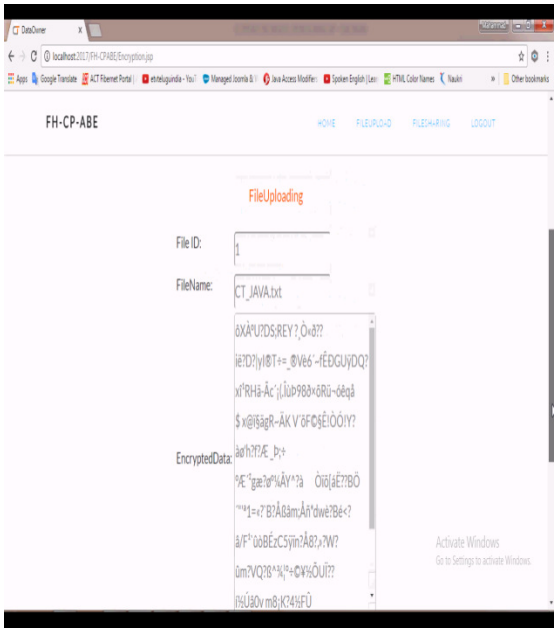

Fig 3 File Uploading Page

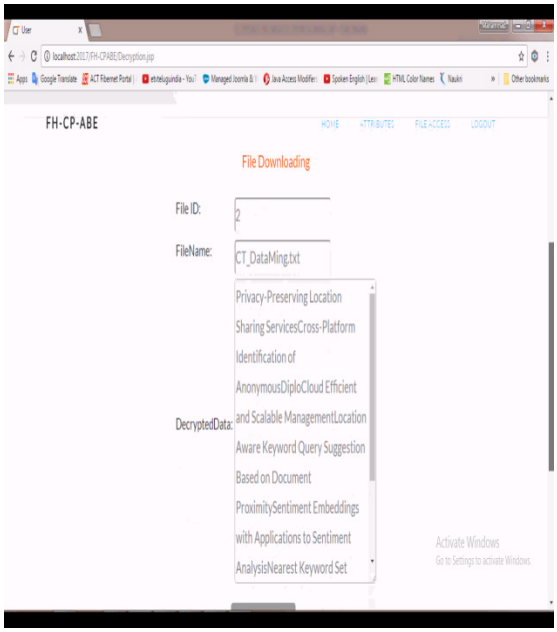

Fig 5 File Download Page

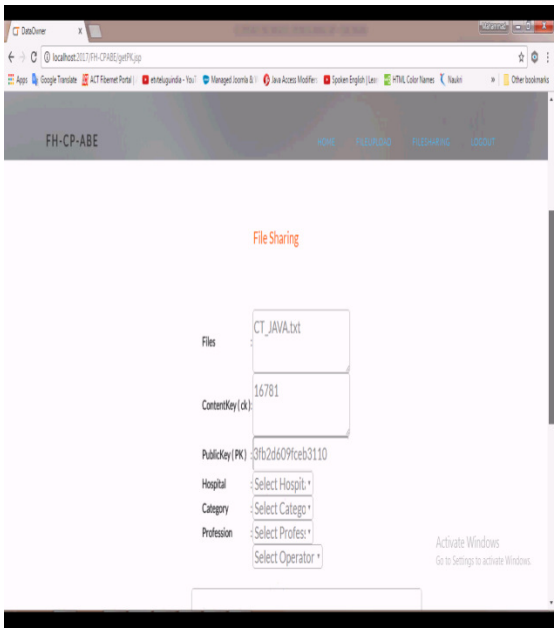

Fig 4 File Sharing Page

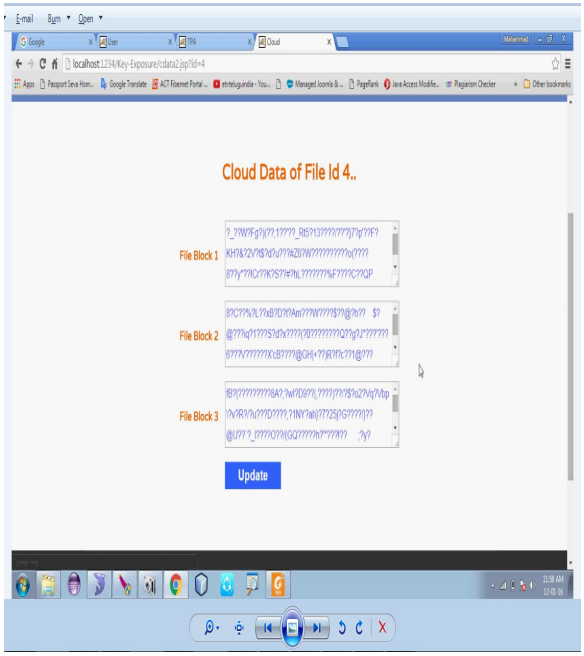

Fig 6 Cloud Data File Updated Page

5. CONCLUSION

In this paper, we proposed a variant of CP-ABE to efficiently share the hierarchical files in cloud computing. The hierarchical files are encrypted with an integrated access structure and the ciphertext components related to attributes could be

shared by the files. Therefore, both ciphertext storage and time cost of encryption are saved. The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files. Moreover, the proposed scheme is proved to be secure under DBDH assumption.

6. REFERENCE

[1] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[2] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Secure and reliable cloud storage against data re-outsourcing," in Proc. 10th Int.Conf. Inf. Secur. Pract. Exper., vol. 8434. May 2014, pp. 346–358.

[3] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. 19th Eur. Symp. Res. Comput. Secur.,vol. 8712. Sep. 2014, pp. 257–272.

[4] T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu, "Identity-based encryption withpost-challenge auxiliary inputs for secure cloud applicationsand sensor networks," in Proc. 19th Eur. Symp. Res. Comput. Secur.,vol. 8712. Sep. 2014, pp. 130–147.

[5] K. Liang et al., "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security ,vol. 9, no. 10, pp. 1667–1680, Oct. 2014.

[6] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo , and J. Zhou, "k-times attribute-based anonymous access control for cloud computing," IEEE Trans. Comput., vol. 64, no. 9, pp. 2595–2608, Sep. 2015.

[7] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two factor access control for Web-based cloud computing services," IEEE Trans. Inf. Forensics Security, vol. 11, no. 3, pp. 484–497, Mar. 2016.

[8] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advancesin Cryptology. Berlin, Germany: Springer, May 2005, pp. 457–473.

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

[10] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attribute-based encryption from R-LWE," Chin. J. Electron., vol. 23, no. 4, pp. 778–782,Oct. 2014.