An Efficient file Hierarchy Attribute Based Encryption Scheme in cloud Computing

Mr. Tanveer K. Patel[1], Prof. Hemant B. Jadhav[2]

[1]*Research Scholar, Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, Savitribai Phule University of Pune, Maharashtra, India*

[2]*Guide, Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, Savitribai Phule University of Pune, Maharashtra, 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 is 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-based encryption.*

1.INTRODUCTION

In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. Access control [6], [7] 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 . Defense is access control 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, and non interactive access control.

Ciphertext-policy attribute based encryption (CP-ABE) is one of feasible schemes which has much more flexibility and is more suitable for general applications.

In cloud computing, as illustrated in Fig. 1, 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

be encrypted by an integrated access structure, the storage cost of ciphertext and time cost of encryption could be saved.

.

2.IMPLEMENTATION

In this paper we present an access control scheme for scalable media. The scheme has several benefits which make it especially suitable for content delivery. For example, it is extremely scalable by allowing a data owner to grant data access privileges based on the data consumers' attributes (e.g., age, nationality, gender) rather than an explicit list of user names; and it ensures data privacy and exclusiveness of access of scalable media by employing attribute-based encryption. For this purpose, we introduce a File Hierarchy Ciphertext Policy Attribute Based Encryption (FH-CP-ABE) technique. FH-CP-ABE encrypts multilevel access structure within integrated cipher text, so as to enforce flexible attribute-based access control on scalable media. Specifically, the scheme constructs a content key which is used to FH-CP-ABE encryption, encrypts media units with the corresponding keys, and then creates Content Key Ciphertext (CT). User can decrypt the Content Key Ciphertext by using FH-CP-ABE decryption into decrypted content key. Then content keys can be decrypted using symmetric decryption algorithm (DES, AES). The scheme offloads computational intensive operations to cloud servers while without compromising user data privacy.

J. Bethencourt, Amit Sahai, Brent Waters [11], a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements. The system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. The system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. In the future, it would be interesting to consider attribute-based encryption systems with different types of expressibility.

Lightweight devices, such as radio frequency identification tags, have a limited storage capacity, which has become a bottleneck form any applications, especially for security applications. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic tool, where the encryptor can decide the access structure that will be used to protect the sensitive data. However, current CP-ABE schemes suffer from the issue of having long decryption keys, in which the size is linear to and dependent on the number of attributes. This drawback prevents the use of lightweight devices in practice as storage of the decryption keys of the CP-ABE for us ers. In this paper, we provide an affirmative answer to the above long standing issue, which will make the CP-ABE very practical. We propose a novel CP-ABE scheme with constant-size decryption keys independent of the number of attributes.[15]

System Framework of FH-CP-ABE:

As illustrated in Fig. 1, the system model in cloud comput-ing is given, which consists of four different entities: authority,CSP, data owner and user. In this work, we assume that data owner has k files with k access levels and M ={m1,..., mk }is shared in cloud computing. Here, m1 is the highest hierarchy and mk is the lowest hierarchy. If a user can decrypt m1,the user can also decrypt m2,..., mk .

1.Authority: It is a completely trusted entity and accepts the user enrollment in cloud computing. And it can also execute Setup and KeyGen operations of the proposed scheme.

2.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 ciphertext storage and transmission services. 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 ciphertext to CSP.

3.User: It wants to access a large number of data in cloud system. The entity first downloads the corresponding

ciphertext. Then it executes Decrypt operation of the proposed scheme.

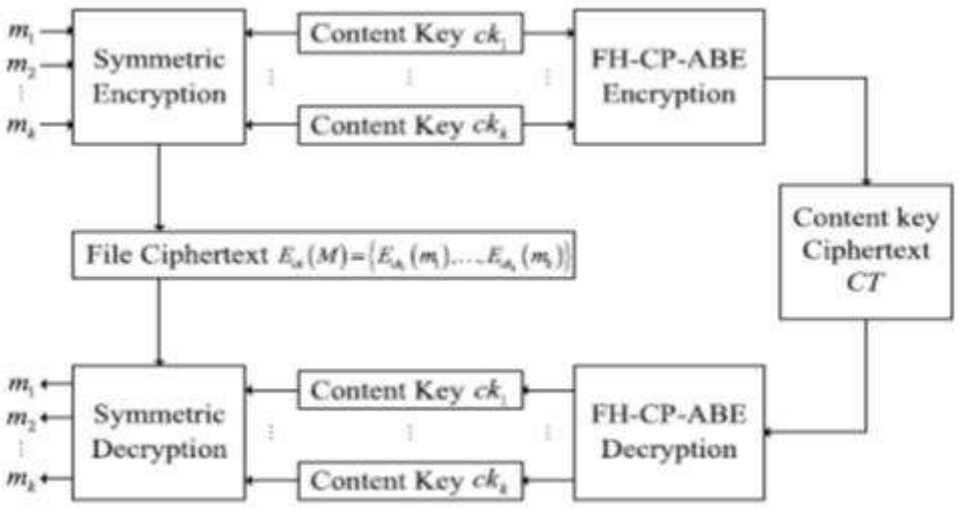

Fig.1.The system framework of FH-CP-ABE scheme.

3.CONLUSION

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

REFERENCES

[1] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Securityoncerns 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 encryp-tion with post-challenge auxiliary inputs for secure cloud applications and 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 comput-ing," IEEE Trans. Comput., vol. 64, no. 9, pp. 2595–2608, Sep. 2015.

[7] J.K.Liu,M.H.Au,X.Huang,R.Lu,andJ.Li,"Fine-grainedtwo-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 Advances in Cryptology. Berlin, Germany: Springer, May 2005, pp. 457–473.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp-tion for fine-grained access control of encrypted data," in Proc. 13th ACM 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.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.

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

[13] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in Proc. 10th Int. Workshop Inf. Secur. Appl., Aug. 2009, pp. 309–323.

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

[15] 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.

BIOGRAPHY

Patel Tanveer is a Research Scolar, Department of Computer Engineering, Vishwabharati Academy's College of Engineering, A'Nagar, Savitribai Phule University of Pune, Maharashtra, India. The research was supported by the senior faculty and Scholars of Vishwabharati Academy's College of Engineering, A'Nagar Department of Computer Engineering.