Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 10, October -2017, pp. 383-387 www.ijcert.org

An Encryption Scheme Based on Peculiarity For an Ordered File Hierarchy in Cloud Computing

[1]Ms.Faiqa Mateen, [2]Mr. Mohammed Khaleel Ahmed,[3] Dr. G.S.S Rao
[1]Pursuing M.Tech(CSE),[2]Associate Professor,[3]Professor & HOD
[1,2,3]Nawab Shah Alam Khan College of Engineering and Technology, Hyd
Email :habeebunissabegum27@gmail.com
,ahmedkhaleelmohammed@gmail.com,profgssrao@gmail.com

Abstract: There are several issues that always occur throughout the sharing of knowledge within the cloud. To unravel this,we use a technology of encoding known as the ciphertext attribute-based encoding which is employed in cloud computing. The files that are being shared on the cloud have the structure hierarchy feature. During this project, we propose the encoding policy supported peculiarity for associate ordered file hierarchy in cloud computing. The files that are present in an exceedingly graded format are encoded in an integrated access structure. The files that are in a serial layer format are combined into one structure that is accessible. This method saves plenty of time and price for the encoding. Below the quality assumption, this projected policy is verified to be secure and safe. Within the encoding and decipherment processes, the expected theme is established to be extremely economical. With the number of files increasing within the cloud because the users keep uploading them, the benefits of the projected theme become additional evident.

Keywords: Cloud computing, data sharing, file hierarchy, cipher text-policy, attribute-based.

---

1. Introduction

With the burgeoning of network technology and mobile terminal, online knowledge sharing has become a replacement "pet," like Facebook, MySpace, and Badoo. Meanwhile, cloud computing [1–5] is one up-and-coming application platforms to unravel the explosive increase of knowledge sharing. In cloud computing, to guard knowledge against leaking, users ought to encipher their knowledge before it is shared.

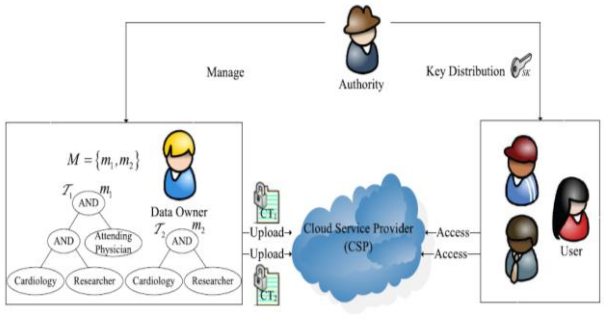

Fig. 1. An example of secure data sharing in cloud computing.

Access management [6], [7] is very important because it is the initial line of defense that stops unauthorized access to the shared knowledge. Recently, attribute-based encoding (ABE) [8–10] has been attracting rather more attention since it will keep the knowledge privacy and understand fine-grained, one-to-many, and noninteractive access management. Ciphertext-policy attribute-based encoding (CP-ABE) [11–21] is one in every of the possible schemes that have way more flexibility and is more appropriate for general applications [22], [23]. In cloud computing, as illustrated in Fig. 1, the authority accepts the user enrollment and creates some parameters. Cloud service supplier is that the manager of cloud servers and provides multiple services for the consumer. Knowledge owner encrypts and uploads the generated ciphertext to cloud service supplier. User downloads and decrypts the interested ciphertext from cloud service supplier. The shared files sometimes have a hierarchical data structure. That is, a bunch of files is split into a variety of hierarchy subgroups set at entirely different access levels. If associate integrated access structure can encrypt the files within the same hierarchical data structure, the storage price of ciphertext and time price of encoding can be saved. It allows us to take the non-public health record (PHR) as an example [24]. To firmly share the PHR information in cloud computing, a patient divides his PHR information M into 2 parts: 'm1'- personal information that contains the patient's name, social insurance range, number, home address, etc. and 'm2' - it doesn't contain sensitive personal info, like medical check results, treatment protocols, and operation notes. Then the patient adopts a CP-ABE policy to encipher the data using different access policies. As an example, associate attending Dr. has to access each the patient's name and his case history to form an identity, and medical scientist solely has to access some medical check results for tutorial purpose.

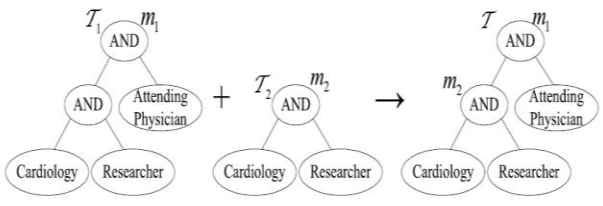

Fig. 2. The integrated access structure. $\mathcal{T}_1$ and $\mathcal{T}_2$ are access structures of m_1 and m_2, respectively. $\mathcal{T}$ is the integrated access structure of m_1 and m_2.

Suppose that the patient sets the access structure of m1as:T1. Similarly, m2 is termed as T2. The instance is deployed in cloud system as shown in Fig. 1. Apparently, the data has to be encrypted double if m1 and m2is encoded with access structures T1 and T2. Two ciphertexts CT1 = Y1 (that has cardiology, researcher, and attending physician) and CT2 = Y2 (that has researcher and cardiology) are made [11]. In the Fig. 1, we will notice that the 2 access structures have graded relationships where the access structure T1 is the expansion of T2 [25]. The 2 structures can be integrated into one structure T as shown in Fig. 2. If the 2 files can be encoded with the integrated access structure and manufacture ciphertext CT then CT=Y (that has a researcher, attending physician, and cardiology). Here, the elements of ciphertext are associated with the policy. Meanwhile, access structure can be shared by the 2 files. Therefore, the computation quality of encoding and storage overhead of ciphertext are often reduced greatly. Moreover, since transport node is added to the access structure, users will decipher all authorization files with the computation of secret key once. The computation price of decipherment also can be reduced if users ought to decipher multiple files at an equivalent time.

2. Existing System

Sahai and Waters projected fuzzy Identity-Based encoding (IBE) in 2005 that was the epitome of ABE. Later, a variant of ABE named CP-ABE was expected.

Since Gentry and Silverberg projected the original notion of graded encoding scheme, several graded CP-ABE schemes are projected. As an example, Wang et al. proposed a graded ABE theme by combining the graded IBE and CP-ABE.

Wan et al. projected ABE policy. Later, Zou gave a better ABE theme, whereas the length of the key secret is linear with the order of the attribute set. A ciphertext-policy graded ABE policy with short ciphertext is additionally studied.

In these schemes, the parent authorization domain governs its child authorization domains, and a top-ranking authorization domain creates a secret key of the next-level field.

The work of key creation is distributed on multiple authorization domains, and therefore the burden of key authority center is lightened.

Drawbacks

- In Existing System time and price for encoding is high.
- Special multiple graded files are not used.
- Decryption system time and computation price are considerably high.

3. Proposed System

In this study, an associate economical encoding theme supported the stratified model of the access structure is projected in cloud computing, that is called file hierarchy CP-ABE theme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CP-ABE with a hierarchical data structure of access policy, therefore on reach easy, versatile and fine-grained access management.

The contribution of this scheme is a combination of the following 3 aspects.

Firstly, we to propose the stratified model of access structure to unravel the matter of multiple graded files sharing. The files are encoded with one integrated access structure.

Secondly, we additionally formally prove the safety of FH-CP-ABE scheme which with success resist chosen plaintext attacks (CPA) below the Decisional additive Diffie-Hellman (DBDH) assumption.

Thirdly, we conduct and implement whole experiment for the FH-CP-ABE policy, and therefore the simulation results show that FH-CP-ABE has low storage price and computation quality regarding encoding and decipherment.

Advantages

- CP-ABE schemes have much additional flexibility and are more appropriate for general applications.
- Multiple graded files are shared. They are also encoded and decoded. Therefore the proposed policy saves a lot of time for both encoding and decipherment.
- In the projected system, each ciphertext storage and time price of encoding are very much saved.
- The projected theme has users that decipher all authorization files by computing secret key once. Thus, the time price of decipherment is additionally saved if the user has to read multiple files.
- The computation price of decipherment also can be reduced if users ought to decipher multiple files at an equivalent time.

4. Implementation

4.1 Modules:

- Data owner Module
- User and Physician Module
- Cloud Service Provider (CSP)
- Authority Module
- Researcher Module

4.2 Modules Description:

1. Data owner Module:

We develop the information owner module which is the very 1st module. The owner can Sign up and look forward to the approval Key of admin. After obtaining the key, the Owner will login exploiting the key to transfer any records associated with user's medical info on the cloud.

In this module, knowledge owner can check the progress of the file transfer by him/her. Its knowledge is required to be held on and shared within the cloud system. In this scheme, the entity is responsible for shaping access structure and encoding operation. And it uploads ciphertext to CSP. When the work is completed, owner sign off the session.

2. User and Physician Module:

The second module we develop is the User Module. The user can register and log in on the user's page. We extend this module in such a way that the User can look out for his/her case history by given user medical record id on the page. The user can get search results of the medical records associated with the id and he/she can request admin to access the document that is encrypted by the admin him selves.

After obtaining decipher key from the admin, he/she can access the medical records. The User logs out of the session. It desires to access a wide range of knowledge within the cloud system. The entity first downloads the corresponding ciphertext. Then it executes decipher operation of the projected theme.

3. Cloud Service Provider (CSP)

This is the third module. It is a semi-trusted entity within the cloud. It will honestly perform the assigned tasks and provide correct results. However, it might prefer to determine as several sensitive contents as possible. Within the projected system, it includes ciphertext storage and transmission services. In this module, we develop admin module method. Admin can log in on the admin page. He/she can check the unfinished requests. To carry out the encoding, a master key is generated by the admin. For deciphering a secret key is used by the user to whom admin provides the key only after accepting the request which was sent by him.

4. Authority Module

The fourth module is the Authority Module that agrees with the enrollment of the users within the cloud and executes Setup and therefore the KeyGen operations.This is a trusted entity in the proposed policy. Setup and KeyGen operations are used in the projected theme.

5. Researcher Module

The final module is the researcher module which can also be called as the scientist module. In this module, the scientist needs a decoding key from the admin to decipher the file. Thus the requests for it. Once he gets the key, he will look out for his required case history by any category e.g.Diabetes, Thyroid, etc.

5. Conclusion

In this paper, we suggest a variant of CP-ABE to share the graded files in the cloud. The graded files are encoded with associate integrated access structure, and therefore the ciphertext elements associated with attributes can be shared by the files. Accordingly, each ciphertext storage and time price of encoding is saved. The projected theme allows the users to decipher all required files by computing secret key once. Thus, the time price of decipherment is additionally saved if the user has to decipher multiple data. Moreover, the projected theme is verified to be secure beneath the DBDH assumption. In the future scope, besides this authorities and options, we will add another new party known as the Trust Party authority. This module helps to extend the safety in future for the modules. This new module will manage the different modules like the scientist, owner, etc. this module also can be used because of the interface to the company network. Recently the primary target of the service suppliers is to the safety and protection of the information of the patient that is held on within the cloud.

References

[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. Secure. 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 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 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 Advances in 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. 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, "Cipher text-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.
[16] A. Balu and K. Kuppusamy, "An expressive and provably secure ciphertext-policy attribute-based encryption," Inf. Sci., vol. 276, pp. 354–362, Aug. 2014.
[17] X. Liu, J. Ma, J. Xiong, and G. Liu, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data," Int. J. Netw.Secur., vol. 16, no. 6, pp. 437–443, Nov. 2014.
[18] Y. Chen, Z. L. Jiang, S. M. Yiu, J. K. Liu, M. H. Au, and X. Wang, "Fully secure ciphertext-policy attribute based encryption with security mediator," in Proc. 16th Int. Conf. Inf. Commun. Secur., vol. 8958. Dec. 2014, pp. 274–289.
[19] Y. Yang, J. K. Liu, K. Liang, K.-K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in Proc. 20th Eur. Symp. Res. Comput. Secur.(ESORICS), vol. 9327. Sep. 2015, pp. 146–166.
[20] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption," Future Generat. Comput. Syst., vol. 52, pp. 67–76, Nov. 2015.
[21] K. Liang et al., "A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing," Future Generat. Comput. Syst., vol. 52, pp. 95–108, Nov. 2015.
[22] C.-I. Fan, V. S.-M.Huang, and H.-M. Ruan, "Arbitrary-state attributebased encryption with dynamic membership," IEEE Trans. Comput., vol. 63, no. 8, pp. 1951–1961, Aug. 2014.
[23] H. Zheng, Q. Yuan, and J. Chen, "A framework for protecting personal information and privacy," Secur.Commun.Netw., vol. 8, no. 16, pp. 2867–2874, Nov. 2015.
[24] F. Xhafa, J. Wang, X. Chen, J. K. Liu, J. Li, and P. Krause, "An efficient PHR service system supporting fuzzy keyword search and fine-grained access control," Soft Comput., vol. 18, no. 9, pp. 1795–1802, Sep. 2014.
[25] S. Wang, J. Yu, P. Zhang, and P. Wang, "A novel file hierarchy access control scheme using attribute-based encryption," Appl. Mech. Mater., vols. 701–702, pp. 911–918, Jan. 2015.
[26] A.Shekinah Prema Sunaina," Study on Competent and Revocable Data Access Control Scheme for Multi-Authority Cloud Storage Systems." International Journal of Computer Engineering in Research Trends., vol.2, no.5, pp. 365-368, 2015.
[27] R.Srinivas and Ajay Kumar," Attribute-Based Encryption for Reliable and Secure Sharing of PHR in Cloud Computing." International Journal of Computer Engineering in Research Trends., vol.2, no.10, pp. 679-682, 2015.
[28] NUTAKKI PRASAD and K.KIRAN KUMAR," A Dynamic Secure Multi Owner Data Sharing Scheme Over Cloud Computing." International Journal of Computer Engineering in Research Trends., vol.2, no.10, pp. 889-895, 2015.
[29] S.L.SOWJANYA, D.RAVIKIRAN," Secure Data Sharing for Dynamic Groups in the Public Cloud." International Journal of Computer Engineering in Research Trends., vol.1, no.6, pp. 428-435, 2014.
[30] Allam Jyothi,G.Somasekhar and Dr S.Prem Kumar," A Secure Multi-Owner Data Sharing Scheme for Dynamic Group in Public Cloud." International Journal of Computer Engineering in Research Trends., vol.2, no.8, pp. 475-480, 2015.

