Cryptanalysis of A Hierarchical Data Access and Key Management in Cloud Computing

Cheng-Ying Yang¹, Cheng-Chi Lee², Tsuei-Hung Sun³ and Min-Shiang Hwang⁴,⁵*
¹Department of Computer Science, University of Taipei, Taipei, Taiwan (Email: cyang@utaipei.edu.tw)
²Department of Library and Information Science, Fu Jen Catholic University, New Taipei City, Taiwan 24205
³Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan 402
⁴*Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan 41354
⁵Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan 40402
*Email: mshwang@asia.edu.tw

Abstract. One of major applications in cloud computing is cloud storage service. It’s an important research issue to protect the stored data from illegal access by the system manager in the Cloud. To encrypt entire file by using data owner’s secret keys is the simple solution. However it will raise a key management problem. To solve this problem, Hwang and Sun proposed a hierarchical key management scheme. In their scheme, the data owner could change the encryption key more easily, and not to affect other users in Cloud Storage Service system. However, we find that some weaknesses of their scheme. In this article, we will show some weaknesses of their scheme.

1. Introduction

There are many advantages for individuals and enterprises to have services in cloud environment. These services include storage, computing ability, and network connection quality [1-2]. One of major applications in cloud computing is cloud storage service [3-4]. However, there services and resources are in the cloud but not in the user’s devices. It raised a new problem of data protection and verification [5-10].

One of the protecting data schemes is Attribute-Based Encryption schemes (ABE), which could delegate the re-encryption capability to the proxy and re-encrypt the encrypted data by using the re-encryption key [11-14]. In ABE scheme, the attributes were applied to generate the public key for encrypting data. The attributes were also used as an access policy to control users’ access [15-17].

In 2013, Hsu et al. proposed a Public Key Encryption with Keyword Search scheme (PEKS) in cloud environment [18]. PEKS is able to search an encrypted data with a keyword without revealing any information. In 2013, Lee et al. studied some conjunctive keyword searchable schemes [19]. The conjunctive keyword searchable scheme is able to search some encrypted documents by using more than one keyword.

In 2015, Yang et al. proposed a practical outsourcing scheme for data access control in cloud server [20]. However, Liu, Cao, and Mao pointed that their scheme was flawed to protect the session keys with more memory overhead [21]. In 2017, Patel proposed accountability in cloud by means of chain...
of trust [22]. In 2018, Al-Shaikhly, El-Bakry, and Saleh proposed a genetic algorithm using Markov chain to enhance the cloud security [23]. In 2018, Ma et al. proposed a secure and efficient cloud data deduplication scheme. Their scheme support the dynamic data public auditing [24]. In 2018, AbdElminaam proposed a new hybrid cryptography algorithm to improve the security of cloud computing [25]. In 2018, Vaanchig et al. proposed a collaborative cloud data storage scheme by key-escrow-free multi-authority CP-ABE with dual-revocation [26].

It's an important research issue to protect the stored data from illegal access by the system manager in the Cloud [27-31]. To encrypt entire file by using data owner's secret keys is the simple solution. However it will raise a key management problem. To solve this problem, Hwang and Sun proposed a hierarchical key management scheme. In their scheme [32], the data owner could change the encryption key more easily, and not to affect other users in Cloud Storage Service system. However, we find that some weaknesses of their scheme. In this article, we will show that their scheme is vulnerable to 1. It need many times symmetric encryption/decryption to use renew file encryption key message so that it will bring higher computing overhead to mobile device users. 2. The data owner still needs to keep all keys in hierarchical tree to generate renewed key message so to increase data owner's storage cost.

The organization of the article is as follows. In Section 2, we briefly review Hwang and Sun’s hierarchical data access and key management scheme in cloud computing. In Section 3, the vulnerabilities of their scheme are analysed. Finally, we make a conclusion of the paper in Section 4.

2. Review of Hwang and Sun's Scheme

In this section, we will introduce the Hwang and Sun's scheme using hierarchical shared key tree and point out that their scheme is vulnerable to two security weaknesses.

Hwang and Sun’s scheme uses access right group to cluster users into different access right trees. Although there are many users in the same tree, their own secret keys are different so that it can achieve user revocation efficiently [32].

Hwang and Sun's scheme has three kinds of roles: Data owner, Cloud, and User. Data owner is an individual content provider or a renter of enterprise who has many files stored in Cloud, and he/she only wants to share these files with specific users who have paid to use files or enterprise internal employee. This scenario needs not only to consider the efficient access control and key management for the data owner, but also to think about the resource of mobile devices is limited. Thus, Hwang and Sun present the efficient scheme to solve these problems, and their scheme includes three phases: The brief description is as follows.

- Setup Phase. See Figure 1(a). Data owner chooses his/her own secret key KO, generates an encryption key of each file Fi by KFi=h(KO || FIDi || cFi), and encrypts all files before uploading and storing in Cloud. The key KF can let data owner not needed to store the key of each file he/she has since it can be re-generated by file id FID and a renew time counter cF. After that, data owner will create an access right list ARL which records the access right of user id with authorized encrypted files and sends all encrypted files with ARL using over-encryption to be stored in Cloud.

- Registration Phase. See Figure 1(b). In the first time, the new user will send request message to data owner to ask for access right of specific files. After data owner checks if the user has paid the bill, he/she will add this user into ARL, selects a secret key KU for the user, and appends the secret key into shared key tree as a leaf node. Then, data owner sends renewed key message to cloud and authorized information to the user, respectively.

- Download Data Phase. See Figure 1(c). The user sends a download request message to Cloud with his/her id UID and the file id FID he/she desired. Then, Cloud will check the user's access right, and sends back the encrypted file and related renewed key messages. In the end, the user can use KU decrypt renewed key message sequent and obtain KF to decrypt the file.
3. Weaknesses of Hwang and Sun’s Scheme

Although Hwang and Sun’s scheme achieves that each user only needs to store one key for all authorized files, and data owner can use KO to re-generate each encryption key KF of file, and the renewed key message to reduce overhead of user revocation. However, their scheme still has some problems:

- Data owner needs to store all keys in the hierarchical tree. It need many times symmetric encryption/decryption to use renew file encryption key message so that it will bring higher computing overhead to mobile device users.

- The computing cost of renewed key message is a little high for data owner and users because it uses symmetric encryption; when the deeper the tree has, the times of symmetric decryption will increase linearly. The data owner still needs to keep all keys in hierarchical tree to generate renewed key message so to increase data owner's storage cost.

![Diagram of Hwang and Sun's scheme]

Figure 1. Hwang and Sun's scheme.
4. Conclusion
In this article, we have pointed out the weaknesses of Hwang and Sun’s hierarchical key management scheme. Their scheme needs many times symmetric encryption/decryption to use renewed file encryption key message so that it will bring higher computing overhead to mobile device users. Furthermore, the data owner still needs to keep all keys in hierarchical tree to generate renewed key message so to increase data owner's storage cost.

5. Acknowledgments
This work was partially supported by the Ministry of Science and Technology, Taiwan, under grant MOST 106-3114-E-005-001, MOST 107-2221-E-845-002-MY3, and MOST 107-2221-E-845-001-MY3.

6. References
[1] Mosa A, El-Bakry H M, Abd El-Razek S M, Hasan S Q. A proposed E-government framework based on cloud service architecture [J]. International Journal of Electronics and Information Engineering, 2016, 5(2): 93-104.
[2] Kibiwott K P, Zhang F, Anyembe Q A, Adu-Gyamfi D. Secure Cloudlet-based eHealth Big Data System with Fine-Grained Access Control and Outsourcing Decryption from ABE [J]. International Journal of Network Security, 2018, 20(6): 1149-1162.
[3] Brindha K, Jeyanthi N. Securing portable document format file using extended visual cryptography to protect cloud data storage [J]. International Journal of Network Security, 2017, 19(5): 684-693.
[4] Cao Z, Liu L, Markowitch O. Analysis of One Scheme for Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates [J]. International Journal of Network Security, 2017, 19(6): 950-954.
[5] Elgazzar S E, Saleh A A, El-Bakry H M. Overview of Using Private Cloud Model with GIS [J]. International Journal of Electronics and Information Engineering, 2017, 7(2): 68-78.
[6] Liu L, Kong W, Cao Z, Wang J. Analysis of one certificateless encryption for secure data sharing in public clouds [J]. International Journal of Electronics and Information Engineering, 2017, 6(2): 110-115.
[7] Cao Z, Mao C, Liu L. Analysis of one secure anti-collusion data sharing scheme for dynamic groups in the cloud [J]. International Journal of Electronics and Information Engineering, 2016, 5(2): 68-72.
[8] Zhang J, Li P, Xu M. On the Security of an Mutual Verifiable Provable Data Auditing in Public Cloud Storage [J]. International Journal of Network Security, 2017, 19(4): 605-612.
[9] Singh D, Patel D, Borisantiya B, Modi C. Collaborative IDS framework for cloud [J]. International Journal of Network Security, 2016, 18(4): 699-709.
[10] Tai W L, Chang Y F. Comments on a secure authentication scheme for IoT and cloud servers [J]. International Journal of Network Security, 2017, 19(4): 648-651.
[11] Chung P S, Liu C W, Hwang M S. A study of attribute-based proxy re-encryption scheme in cloud environments [J]. International Journal of Network Security, 2014, 16(1): 1-13.
[12] Lee C C, Chung P S, Hwang M S. A survey on attribute-based encryption schemes of access control in cloud environments [J]. International Journal of Network Security, 2013, 15(4): 231-240.
[13] Liu C W, Hsien W F, Yang C C, Hwang M S. A survey of attribute-based access control with user revocation in cloud data storage [J]. International Journal of Network Security, 2016, 18(5): 900-916.
[14] Zhao Y, Fan P, Cai H, Qin Z, Xiong H. Attribute-based encryption with non-monotonic access structures supporting fine-grained attribute revocation in M-healthcare [J]. International Journal of Network Security, 2017, 19(6): 1044-1052.
[15] Ma H, Peng T, Liu Z. Directly revocable and verifiable key-policy attribute-based encryption for large universe [J]. International Journal of Network Security, 2017, 19(2): 272-284.
[16] Balusamy B, Krishna P V, Arasi G S T, Chang V. A secured access control technique for cloud computing environment using attribute based hierarchical structure and token granting system [J]. International Journal of Network Security, 2017, 19(4): 559-572.

[17] Tian Y, Peng Y, Gao G, Peng X. Role-based access control for body area networks using attribute-based encryption in cloud storage [J]. International Journal of Network Security, 2017, 19(5): 720-726.

[18] Hsu S T, Yang C C, Hwang M S. A study of public key encryption with keyword search [J]. International Journal of Network Security, 2013, 15(2): 71-79.

[19] Lee C C, Hsu S T, Hwang M S. A study of conjunctive keyword searchable schemes [J]. International Journal of Network Security, 2013, 15(5): 321-330.

[20] Yang K, Jia X H, Ren K. Secure and verifiable policy update outsourcing for big data access control in the cloud [J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(12): 3461-3470.

[21] Liu L, Cao Z, Mao C. A note on one outsourcing scheme for big data access control in cloud [J]. International Journal of Electronics and Information Engineering, 2018, 9(1): 29-35.

[22] Contractor D, Patel D. Accountability in cloud computing by means of chain of trust [J]. International Journal of Network Security, 2017, 19(2): 251-259.

[23] Al-Shaikhly M H R, El-Bakry H M, Saleh A A. Cloud security using Markov chain and genetic algorithm [J]. International Journal of Electronics and Information Engineering, 2018, 8(2): 96-106.

[24] Ma H, Han X, Peng T, Zhang L. Secure and Efficient Cloud Data Deduplication Supporting Dynamic Data Public Auditing [J]. International Journal of Network Security, 2018, 20(6): 1074-1084.

[25] AbdElminaam D S. Improving the security of cloud computing by building new hybrid cryptography algorithms [J]. International Journal of Electronics and Information Engineering, 2018, 8(1): 40-48.

[26] Vaanchig N, Xiong H, Chen W, Qin Z. Achieving collaborative cloud data storage by key-escrow-free multi-authority CP-ABE scheme with dual-revocation [J]. International Journal of Network Security, 2018, 20(1): 95-109.

[27] Hwang M S, Sun T H, Lee C C. Achieving dynamic data guarantee and data confidentiality of public auditing in cloud storage service [J]. Journal of Circuits, Systems, and Computers, 2017, 26(5).

[28] Liu C W, Hsien W F, Yang C C, Hwang M S. A survey of public auditing for shared data storage with user revocation in cloud computing [J]. International Journal of Network Security, 2016, 18(4): 650-666.

[29] Hsien W, Yang C C, Hwang M S. A survey of public auditing for secure data storage in cloud computing [J]. International Journal of Network Security, 2016, 18(1): 133-142.

[30] Hwang M S, Lee C C, Sun T H. Data error locations reported by public auditing in cloud storage service [J]. Automated Software Engineering, 2014, 21(3): 373-390.

[31] Chen M Y, Liu C W, Hwang M S. SecureDropbox: A file encryption system suitable for cloud storage services [C]. Proceedings of the 2013 ACM Cloud and Autonomic Computing Conference, ACM, 2013: 21-22.

[32] Sun T H, Hwang M S. A hierarchical data access and key management in cloud computing [J]. ICIC Express Letters, 2012, 6(2): 569-574.