An Attribute Based Encryption Middleware with Rank Revocation for Mobile Cloud Storage

Qinghe Dong[1], Qian He[1,2(✉)], Mengfei Cai[1], and Peng Liu[2,3]

[1] Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education, Guilin University of Electronic Technology, Guilin 541004, China
treeqian@gmail.com
[2] Key Lab of Cloud Computing and Complex System, Guilin University of Electronic Technology, Guilin 541004, Guangxi, China
[3] Guangxi Key Lab of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, Guangxi, China

Abstract. The Attribute Based Encryption (ABE) algorithm can be used to realize fine grained access control for the mobile cloud storage. In ABE, the decryption algorithm has high complexity and the rank revocation is difficult to be implemented. An ABE middleware with rank revocation is given in this paper. The ABE middleware delegate the ABE decryption operation for the resource constrained mobile device. The attribute authority can revoke the user's rank through this middleware instantly with fine-grained control and the revocation process may not affect any other users. The ABE middleware is implemented and experiment results show that the ABE middleware improves ABE decryption performance about 30 times.

Keywords: Attribute based encryption · Mobile cloud storage
Middleware · Rank revocation

1 Introduction

The mobile users increased explosively in recent years. In 2014, the mobile users reach 5.27 billion, which is beyond the personal computer (PC) users [1]. Compared with the traditional PC, the mobile device is resource constrained in the computing, storage, and battery power capacity. Therefore, the mobile device should work with the cloud to enhance its power and the mobile cloud computing becomes a new important stream.

Cloud computing is a new computing model which becomes a hot technology in recent years. Cloud computing builds a large number of computational and storage resources into a shared pool with configuration, so difference applications can be obtained different resources according to the demands [2]. In the cloud storage system, the numerous users and data storage are dispersed. Compared with the traditional software, all the data in the cloud computing are maintained by the third party, which may bring more security issues [3, 4].

M. Huang et al. (Eds.): WICON 2016, LNICST 214, pp. 61–69, 2018.
https://doi.org/10.1007/978-3-319-72998-5_7

The Attribute Based Encryption (ABE) algorithm is viewed as one solution to realize fine-grained access control in the cloud environment [5–7]. ABE has two categories: the Key Policy Attribute Based Encryption (KP-ABE) and Ciphertext Policy Attribute Based Encryption (CP-ABE). Since the pairing and exponent operation of big numbers exist in ABE, the ABE computation cost is large, which is not suitable for the resource constrained mobile device. The decryption operation should be invoked every time when the data are consumed, so it is invoked more frequently than the encryption. The attribute revocation is still a difficult problem in the ABE mechanism [8]. Pirretti etc. [9] proposed to complete attribute revocation through updating the user private key periodically, but this revocation scheme cannot be performed in real time and will produce large overhead because the users need to save the private key at each time. In the literature [10], Asim etc. realized the user name revocation by adding the revocation user name into ciphertext, but the complexity of the decryption algorithm increases with the number of users. Reference [11] constructs CP-ABE scheme supported fine-grained cancellation based on double system encryption. All above solutions require the data to be re-encrypted when the ranks are revoked, so the efficient is low.

In this paper, an ABE middleware with rank revocation is proposed. The main contributions are as follows:

1. A special ABE algorithm is proposed for the ABE middleware. The ABE middleware delegates the decryption partly, and provides the middle result for the mobile to complete the whole ABE decryption. The ABE decryption cost of the mobile device is decrease and the decryption process becomes fasten.
2. The rank revocation is provided based on the ABE middleware. If a user' rank is revoked, the process become simple and the re-encryption of data is avoided.
3. The ABE middleware based mobile storage application system is realized. The performance of the decryption and attribute revocation is verified by the experiment.

The remainder of this paper is organized as follows: Sect. 2 introduces our system architecture; Sect. 3 presents our ABE algorithms with revocation; Sect. 4 analyzes the experiment; finally, and Sect. 5 concludes this paper.

2 System Design of the ABE Middleware

2.1 System Architecture

The mobile cloud storage system based on the ABE middleware consists of five parts: Data Owner (DO), Attribute Authority (AA), ABE Middleware (ABE-M), Cloud Storage (CS) and Mobile User (MU). DO is the data owner which define the access control policy, encrypt the sensitive data with the help of ABE-M, and then upload them to the CSP; AA is responsible for the system initialization, key generation and revocation operation; ABE-M do the ABE decryption task and attribute revocation. MU is the data requestor from CS. In the whole system, the cloud host always is semi-trusted, that is to say, the cloud host will perform correctly system commands, but

at the same time it may try to steel data for his profits. The system architecture of ABE middleware application is given in Fig. 1.

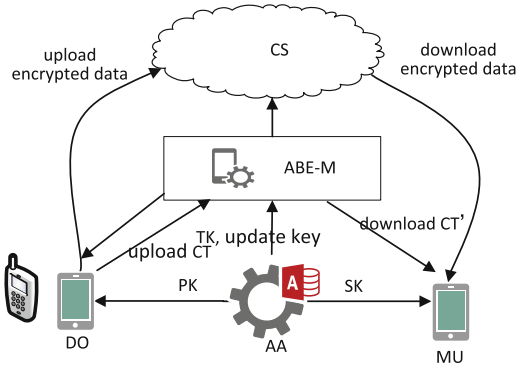

Fig. 1. System architecture of the ABE middleware application

In this application system architecture, two encryption algorithms including ABE and the symmetric encryption algorithm are used. ABE is used to encrypt the symmetric key and generate ciphertext *CT*, and the symmetric encryption algorithm utilizes this symmetric key to encrypt the file. The users cannot decrypt the encrypted file until the symmetric key is obtained which is decrypt with the satisfied attribute user.

2.2 Structure Model

The structure model of the ABE middleware is shown in Fig. 2. There exist five modules as follows.

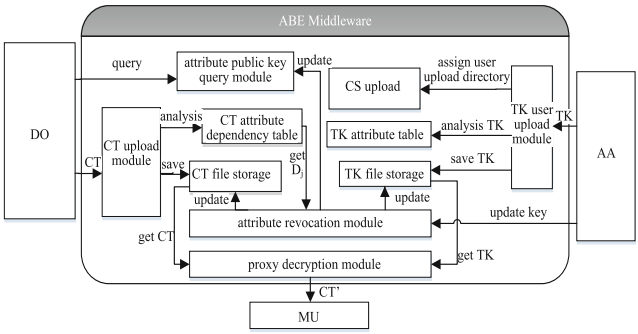

Fig. 2. Structure model of the ABE middleware

TK upload module: when *AA* releases one user's *TK* to service middleware, this module will save *TK* and assign independent upload directory to separated user.

CS upload module: manage directory access permission in the cloud through the access control policy. Only the satisfied user can add, delete, modify the files in the directory.

CT upload module: after the data sharing user uploads *CT*, the module will save *CT* and its attribute dependency according to the *CT*'s attribute dependency table. In the process of attribute revocation, *CT* needed to be uploaded can be quickly positioned through *CT* attribute dependency table.

Attribute revocation module: The module is responsible for upgrading *CT* and user conversion key generated by *AA*. If the attribute revocation user does not get the upgraded key, the key component corresponding to this attribute in *TK* become invalid.

Attribute public key query module: query whether the attribute public key changes before the data are encrypted by DO. If changed, the module upgrades the attribute public key.

Decryption delegation module: delegate and decrypt *CT* and get a middle result *CT'*, and then send to the MU who wants to access the encrypted data in the cloud storage.

3 ABE Algorithms

3.1 Construction

The reference [6] provides a basic CP-ABE, and reference [7] proposes an ABE with revocation. We combined them together and propose the ABE algorithms as follows.

Initializing algorithm. $Setup(\lambda, U) = \{PK, MSK, PKx\}$: is executed by attribute authority, input security parameters λ and attribute sets U. Choose a group G with the order p, and g becomes the generator. The mapping function ρ will map each attribute in U into the element in G. Chooses three parameters: α, β, a from Zp randomly, chooses the parameter $V_x \in Z_p$ for each attribute x in U, and then outputs the public key $PK = \{g, e(g,g)^{\alpha}, g^a, \rho\}$, master key $MSK = \{\alpha, \beta, \{Vx\}_{x \in U}\}$, attribute public key $PK_x = \{g^{V_x}\} x \in U$.

Encrypt algorithm. $Encrypt(\psi, PK, PKx, A) = CT$: encrypts the input message by using *PK*, *PKx*, and access control policy *A*. According to access control policy A, the algorithm generate one LSSS matrix $M_{n,k}$, and then choose $V = [s, y_1, y_2 \ldots y_{k-1}]^{\perp}$ at random and compute $\lambda = MV$. In addition, randomly selects $r_1, r_2 \ldots r_n \in Z_p$, the ciphertext $CT = \{C = \psi \cdot e(g,g)^{\alpha s}, C' = g^s, \{C_i = g^{a\lambda_i} \cdot [g^{V_{x_i}} \cdot \rho(x_i)]^{-r_i}, \quad D_i = g^{r_i}\}_{1 \le i \le n}\}$ is gotten, where x_i is attribute corresponding to the row i of the matrix M.

Key generation algorithm. $Keygen(MSK, PK, PKx, S) = \{TK, SK\}$: is executed by *AA* by using *MSK*, *PK*, *PKx*, user's attribute set S, and output the private key SK and the conversion private key *TK*. After selecting $z \in Z_p$ randomly, $TK = \{K = g^{\alpha/z} \cdot g^{a\beta/z}, L = g^{\beta/z}, \{K_x = [g^{V_x} \cdot \rho(x)]^{\beta/z}\}_{x \in S}\}$, $SK = \{z\}$ is gotten, where *TK* is held by the service middleware, SK is held by users.

Decryption delegation algorithm. $Transform(CT, TK) = CT'$: is executed by the ABE middleware. First, chooses vector $W = \{w_1, w_2 \ldots w_n\}$ to make $W \cdot M = \{1, 0, 0 \ldots 0\}$. Then calculates for each line of CT: $e(C_i^{w_i}, L) \cdot e(D_i^{w_i}, K_i)$, where K_i is the key share corresponding to the attribute. The computation result of each line is multiplied: $A = \prod_{i \in I} e(C_i^{w_i}, L) \cdot e(D_i^{w_i}, K_i) = e(g, g)^{sa\beta/z}$. Computing $R = e(C', K)/A = e(g, g)^{\alpha s/z}$, The middle result $CT' = \{C, R\}$ is send to the mobile finally.

Decryption algorithm. $Decrypt(CT', SK) = \psi$: is executed in the mobile. Receiving CT', the mobile can decrypt and obtain the original data: $\psi = C/R^z$.

Since our ABE algorithm is based on the basic CP-ABE and the ABE given in reference [7], it has the same security properties for the decisional BDH assumption.

3.2 Attribute Revocation

Assuming AA hopes to revoke the attribute *attr* of one user, the procedure of attribute revocation works as follows:

1. AA chooses a new attribute parameter V'_{attr} for *attr*, computes $PK_{attr} = g^{V'_{attr}}$, and sents *attr* and PK_{attr} to the ABE middleware.
2. The service middleware updates attribute public key as PK_{attr} of *attr* in the attribute public key query module.
3. The ABE middleware queries attribute dependency table CT, gets FID of CT using the attribute and corresponding row index. $D_{attr} = g^{r_i}$ is loaded according to FID and the row index.
4. The ABE-middleware returns D_{attr} to AA.
5. AA generates the upgrade key of CT based on D_{attr}, that is $CUK = D_{attr}^{-(V'_{attr} - V_{attr})} = g^{-r_i(V'_{attr} - V_{attr})}$, and then sends it to the service middleware.
6. The middleware upgrades CT by using CUK: $C_{attr} = C_{attr,old} \cdot CUK$, and then get $C_{attr} = g^{a\lambda_i} \cdot [g^{V'_{attr}} \cdot \rho(attr)]^{-r_i}$.
7. AA generates the upgrading key for the mobile who has not been revoked attribute *attr*: $UUK = g^{(V'_{attr} - V_{attr}) \cdot \beta/z}$, and sends it to the ABE middleware.
8. The ABE middleware uses UUK to upgrade TK: $K_{attr} = K_{attr,old} \cdot UUK$, and then we can obtain $K_{attr} = [g^{V'_{attr}} \rho(attr)]^{\beta/z}$.

After completing the above process, the attribute parameters of *attr* in CT are upgraded from V_{attr} to V'_{attr}. For the user who is not revoked the attribution attr, AA generates UUK and upgrades the attribute attr parameter in K_{attr} to V'_{attr}. The user who has been revoked *attr* cannot be upgraded because they don't get UUK. So K_{attr} of the revoked users become invalid, and then the user's rank is revoked.

4 Experiments

4.1 Experiment Environment

We realize the ABE middleware and the ABE middleware based mobile client application in Java which is shown in Fig. 3, and deployed in an experiment lab. The experiment environment includes a Dawn server w5801-G10 (CPU: 2 *Intel Xeon E5-2630, Memory: 64G) and a Huawei smart phone Y635-CL00 (CPU: Snapdragon 410, Memory: 1G). The attribute authority and ABE middleware are deployed in the Dawn server as a virtual machine, and the decryption and revocation performances are evaluated.

Fig. 3. The ABE middleware based mobile client

4.2 Decryption Performance

The experiment are carried out to respectively test the server middleware and mobile equipment decryption consumed time for attribute index from 10 to 100 in the *CT*, the time consuming comparison is shown in Fig. 4.

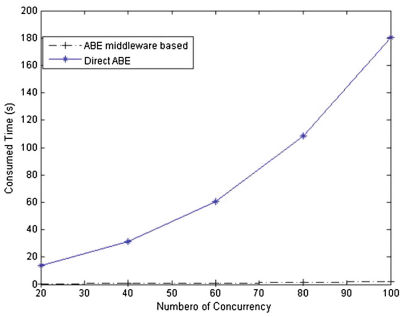

Fig. 4. Decryption time of the mobile

It can be seen from the experiment result that the attribute based decryption time is greatly reduced by using the middleware. When *CT* contains 10 attributes, the decryption time has been cut by 19.5 times, and with the increase of number of attributes, the advantage is more obvious. When the number of attributes is increased to 100, the decryption time is dropped by 30.7. This method using middleware proxy decryption reduce the requirement for terminal, fully reflect the advantage of cloud computing.

4.3 Concurrency Performance

The concurrency processing capability for server middleware is tested using the LoadRunner 9 (http://environment.yale.edu/loadrunner/). For a CT with 10 attributes, we can simulate the request decryption for 0 to 100 concurrent users. The concurrent performance is shown in Fig. 5.

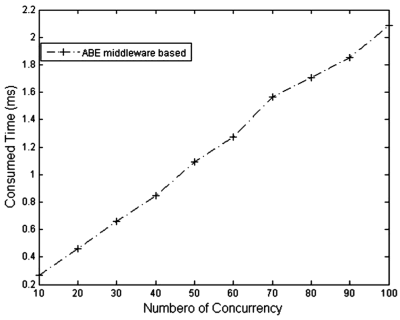

Fig. 5. Concurrency performance of ABE middleware

The result shows that when the system has 100 concurrent requests, the response time is 2.087 s which is shorter than directly decryption of mobile devices. With the increasing of concurrency, proxy decryption time may exceed the directly decryption time of mobile devices. But we should notice the service middleware is deployed in the cloud, cloud computing has the following features such as massive computing resources, easy expansion and easy deployment, so we can solve the high concurrency problem by extending the computing resources of service middleware.

4.4 Rank Revocation

The user's rank is revoked means that one or more of its attributes are changed. When revoking one attribute of users, it is needed to upgrade CT component corresponding with this attribute and other key component of no-revocation users.

Compared with the attribute revocation schemes in [9–11] require user to encrypt data again, the method in this paper has great advantage. The result shows that the attribute revocation time approximately linear increases with the increase of the number of users and CT associated with this attribute. In the experiments, when the number has

100 and the users have 400 associated with the revocation attribution, the total consumption time on attribute revocation is 17.68 s, which is 5 times of that of 1 CT and 2 users. The attribute revocation process can further improve the performance by increasing the number of middleware.

5 Conclusion

It is difficult to achieve the attribute based decryption because of its high complexity in the resource limited mobile device, so this paper proposes a ABE based method for the mobile to use cloud storage securely. The mobile equipment can outsource large number of computation in the ABE decryption process through the ABE middleware. The attribute authority can complete the fine grained revocation for user attribute without affecting any other users. All services in the middleware provided by the Restful interface are suitable for the mobile device to invoke. The proposed ABE middleware performance is tested in the real mobile cloud storage application. The result shows that the ABE middleware can improve the decryption performance of mobile device obviously, and the performance of concurrency and attribute revocation can satisfy the practice. In the future, we will further study the distribution integration method about the multiple ABE middle wares.

Acknowledgment. This work was partly supported by the National Natural Science Foundation of China (61661015), Ministry of Education Key Lab of Cognitive Radio and Information Processing Found (CRKL160101), Guangxi Collaborative Innovation Center of Cloud Computing and Big Data Found (YD16801), Guangxi Scientific and technological plan (1598008-28), High Level of Innovation Team of Colleges and Universities in Guangxi Outstanding Scholars Program Funding, and GUET Cloud Security and Cloud Service Innovation Group Project.

References

1. The 34th accounting reports of the development situation of China Internet. China Internet, vol. 7 (2014)
2. Armbrust, M., Fox, A., Griffith, R., et al.: A view of cloud computing. Commun. ACM **53** (4), 50–58 (2010)
3. Feng, D.G., Zhang, M., Zhang, Y., Xu, Z.: Study on cloud computing security. J. Softw. **22** (1), 71–83 (2011)
4. Horváth, M.: Attribute-based encryption optimized for cloud computing. In: Italiano, G.F., Margaria-Steffen, T., Pokorný, J., Quisquater, J.-J., Wattenhofer, R. (eds.) SOFSEM 2015. LNCS, vol. 8939, pp. 566–577. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46078-8_47
5. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption, pp. 321–334 (2007)
6. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_4

7. Wang, Y.D., Yang, J.H., Xu, C., Ling, X., Yang, Y.: Survey on access control technologies for cloud computing. Ruan Jian Xue Bao/J. Softw. **26**(5), 1129–1150 (2015)
8. Su, J.S., Cao, D., Wang, X.F., Sun, Y.P., Hu, Q.L.: Attribute-based encryption schemes. J. Softw. **22**(6), 1299–1315 (2011)
9. Pirretti, M., Traynor, P., Mcdaniel, P., et al.: Secure attribute-based systems, pp. 99–112 (2006)
10. Asim, M., Ibraimi, L., Petković, M.: Ciphertext-policy attribute-based broadcast encryption scheme. In: De Decker, B., Lapon, J., Naessens, V., Uhl, A. (eds.) CMS 2011. LNCS, vol. 7025, pp. 244–246. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24712-5_25
11. Wang, P.P., Feng, D.G., Zhang, L.W.: CP-ABE scheme supporting fully fine-grained attribute revocation. J. Softw. **23**(10), 2805–2816 (2012)
12. Belqasmi, F., Glitho, R., Fu, C.: RESTful web services for service provisioning in next-generation networks: a survey. IEEE Commun. Mag. **49**(12), 66–73 (2011)
13. Belqasmi, F., Singh, J., Bani Melhem, S.Y., et al.: SOAP-based vs. RESTful web services: a case study for multimedia conferencing. IEEE Int. Comput. **16**(4), 54–63 (2012)
14. Li, Y., Zeng, Z.Y., Zhang, X.F.: Outsourced decryption scheme supporting attribute revocation. J. Tsinghua Univ. (Sci. Technol.) **12**, 1664–1669 (2013)