Efficient Revocable Data Access Control with Multiple Trusted Authorities and CSP’s in Cloud

GORRY SIVA KRISHNA REDDY[1], DR.C.MD.GULZAR[2]
[1] PG Scholar, Dept of CSE, Dr. K. V. Subba Reddy Institute of Technology, Kurnool, AP, India.
[2]Professor & HOD, Dept of CSE, Dr. K. V. Subba Reddy Institute of Technology, Kurnool, AP, India.

ABSTRACT

Security and access control issues are main obstacles for wide application of cloud computing. To ensure security for data we construct an efficient user revocation CP-ABE scheme through improving the scheme and prove our scheme is secure from chosen plain text attack CPA secure under the selective mod-el. To solve security issue, we embed a certificate into each user’s private key. In this way, each user’s group secret key is different from others and bound to-gether with his private key associated with attributes. To reduce users’ computation burdens, we introduce two cloud service providers named encryption -cloud service provider (E-CSP) and decryption-cloud service provider (D-CSP). The duty of E-CSP is to perform outsourced encryption operation and D-CSP is to perform outsourced decryption operation. We extended the System security by adding One Time Password to the System while downloading the file and to overcome burden of Trusted Authority we Created Multiple Trusted Authorities to handle the requests.

INTRODUCTION

Cloud computing, as a new technology paradigm with promising further, is becoming more and more popular nowadays. It can provide users with seemingly unlimited computing resource.

Enterprises and people can outsource time-consuming computation workloads to cloud without spending the extra capital on deploying and maintaining hardware and software. Flexibly and fine-grained file access control, attribute based encryption (ABE) was proposed and used in cloud storage system. However, user revocation is the primary issue in ABE schemes. In this article, we provide a cipher text policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users’ private keys except for those who have been revoked. Security issues are main obstacles for wide application of cloud computing .To achieve flexible fine grained file access control, attribute based encryption (ABE) was proposed and used. However, user revocation is the primary issue in ABE schemes.

We need efficient user revocation for cloud storage system. At the same time heavy computation cost should not spoil the application performance. The system should with stand collusion attack performed by revoked users cooperating with existing users. The system should be suitable for resource constrained devices also. CPABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys. Notably, our scheme can withstand collusion attack performed by revoked users cooperating with existing users. We prove the security of our scheme under the divisible computation Diffie-Hellman (DCDH) assumption. The result of our experiment shows computation cost for local devices is relatively low and can be constant. Our scheme is suitable for resource constrained devices. A basic CP-ABE scheme concludes the following fundamental algorithms:

Setup: This algorithm takes a security parameter as input. It outputs a public parameter and a master key.

Encrypt: This algorithm takes the public parameter, a message, and an access policy in the attribute universe as input. The algorithm outputs a cipher-text CT such that only the user whose attribute set satisfies the access policy can decrypt

Key Gen: This algorithm takes the master key and an attribute set as input. It outputs a private key with respect to the attribute set.

Decrypt: This algorithm takes the public parameter, a ciphertext CT, and a private key as input. If the user's attribute set satisfies the access structure embedded in the Cipher-Text, then the algorithm decrypts the cipher-text successfully Perform user revocation operation by combining CP-ABE with re-encryption. In their scheme, each user belongs to a group and holds a group secret key issued by the group Manager.

RELATED WORK

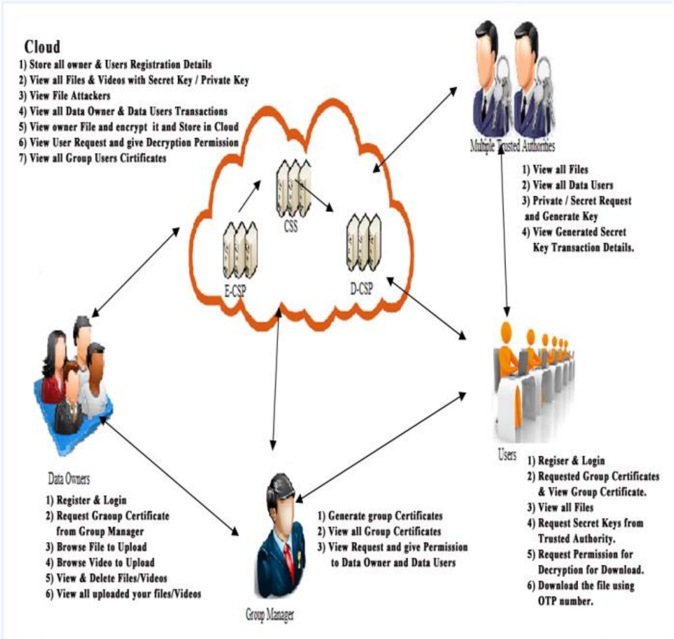
Through applying ABE schemes to cloud storage ser-vices, we can both ensure the security of stored data and achieve fine-grained data access control. Unfortunately, ABE scheme requires high computation overhead during performing encryption and decryption operations. This defect becomes more severe for lightweight devices due to their constrained computing resources. To reduce the com-putation cost for resource-constrained devices, some cryp-tographic operations with high computational load were outsourced to cloud service providers [10-13]. Combined proxy re-encryption with lazy re-encryption technique, Yu et al. [10] designed a KP-ABE scheme with fine-grained data access control. This scheme requires that the root node in the access tree is an AND gate and one child is a leaf node which is associated with the dummy attribute. The dummy attribute is required to be included in every data document's attribute set and will never be updated. In their scheme, cloud service provider stores all the private key components for u ser's private key except for the one corresponding to the dummy attribute. However, cloud service provider does not learn the plaintext for any data document. Green et al. [11] provided an efficient CP-ABE scheme with outsourcing decryption. In their scheme, us-er's private key is blinded through using a random num-ber. Both the private key and the random number are kept secret by the user. The user shares his blinded private key to a proxy to perform outsourced decryption operation. In this paper, we use the similar techniques as [10-11] to ex-tend our scheme with outsourcing ability. However, there is a major limitation to single-authority ABE as in IBE. Namely, each user authenticates him to the authority, proves that he has a certain attribute set, and then receives secret key associated with each of those attributes. Thus, the authority must be trusted to monitor all the attributes. It is unreasonable in practice and cum-bersome for authority. Chase [14] designed a multi-authority ABE scheme with central authority. Their scheme is proved secure in the selective attribute model. Liu et al. [15] proposed a fully secure multi-authority CP-ABE which includes multiple central authorities so that no single authority can decrypt any ciphertext. In order to protect privacy of the user, Han et al. [16] presented a decentralized KP-ABE scheme with privacy-preserving. Similarly, Qian et al. [17] provided a decentralized CP-ABE with fully hidden access structure. Furthermore, they [18] proposed a privacy-preserving personal health record using multi-authority ABE with revocation. Re-cently, some traceable CP-ABE schemes [19-21] were pro-posed in order to find out an efficient solution to identify malicious users who purposely share their decryption keys.

PROBLEM STATEMENT

Security issues are main obstacles for wide application of cloud computing. To achieve flexibly fine-grained file access control, attribute based encryption (ABE) was proposed and used. However, user revocation is the primary issue in ABE schemes. We need efficient user revocation for cloud storage system. At the same time heavy computation cost should not spoil the application performance. The system should with stand collusion attack performed by revoked users cooperating with existing users. The system should be suitable for resource constrained devices also.

IMPLEMENTATION

we construct an efficient user revocation CP-ABE scheme through improving the scheme in and prove our scheme is CPA secure under the selective mod-el. To solve above security issue, we embed a certificate into each user's private key. In this way, each user's group secret key is different from others and bound to-gether with his private key associated with attributes. To reduce users' computation burdens, we introduce two cloud service providers named encryption -cloud service provider (E-CSP) and decryption-cloud service provider (D-CSP). The duty of E-CSP is to perform outsourced en-cryption operation and D-CSP is to perform outsourced decryption operation. Sytem security can be enhanced by adding One Time Password to the System while downloading the file and to over come burden of Trusted Authoriy we Created Multiple Trusted Authorities to handle the request.


Cloud
1) Store all owner & Users Registration Details
2) View all Files & Videos with Secret Key / Private Key
3) View File Attackers
4) View all Data Owner & Data Users Transactions
5) View owner File and encrypt it and Store in Cloud
6) View User Request and give Decryption Permission
7) View all Group Users Cirtificates
CSS
E-CSP
D-CSP
Multiple Trusted Authorities
1) View all Files
2) View all Data Users
3) Private / Secret Request and Generate Key
4) View Generated Secret Key Transaction Details.
Data Owners
1) Register & Login
2) Request Graoup Certificate from Group Manager
3) Browse File to Upload
4) Browse Video to Upload
5) View & Delete Files/Videos
6) View all uploaded your files/Videos
Group Manager
1) Generate group Certificates
2) View all Group Certificates
3) View Request and give Permission to Data Owner and Data Users
Users
1) Regiser & Login
2) Requested Group Certificates & View Group Certificate.
3) View all Files
4) Request Secret Keys from Trusted Authority.
5) Request Permission for Decryption for Download.
6) Download the file using OTP number.

IMPLEMENTATION MODULES:

1. Data Owner(DO)
2. Data User(DU)
3. Group Manager(GM)
4. Multiple Trusted Authorities
5. Cloud Storage Server(CSS)

X. MODULES DESCRIPTION:

1. **Data Owner (DO):**

In this module includes the Data Owner first register his details and login. Next The Owner gives the request to Group Manager for Group Certificate. After receive the certificate DO can Upload a file to the Cloud and the file encrypted by the CP-ABE Algorithm. The Data Owner can also view the Files details and File contents in a Encrypted format. The Data Owner can only View his Group Files.

2. **Data User (DU):**

In this module includes the Data User first register his details and login. Next The User gives the request to Group Manager for Group Certificate. After receive the certificate DU can View a file Details. If Data User wants to download the file means DU send the request to the Auditor for Secret Key of downloading permission. Auditor sends the Secret Key to Data User Mail id. Data User can download the file by using the Secret Key. Data User view and download his Group files only.

3.**Group Manager (GM):**

In this Module Group Manager response Data Owner and Data User Group Certificate requests. Group Manager sends the Group Certificates to the DO and DU. Group Manager done the Users Revocation Process. Once the User is Revoked by GM then the user not able to access the files in the group and the user is unauthorized to login.

4. **Multiple Trusted Authorities:**

In this Module the Trusted Authorities can view the Uploaded file details and response the Data Users Secret Key Requests for Downloading process. Authorities sends the Secret Key to the Data Users Mail id. Without this secret key Data User Cannot able to download the files.

5.**Cloud Storage Server (CSS) :**

The Cloud Storage Server can view the Data Users and Data Owners Details.CSS can also view the File Details .and CSS view the revoked Users Details.

CONCLUSION

We provided a formal definition and security model for CP-ABE with user revocation. We also constructed a concrete CP-ABE scheme which is CPA secure based on DCDH assumption. To resist collusion attack, we embed a certificate into the user's private key. So that malicious users and the revoked users do not have the ability to generate a valid private key through combining their private keys. Additionally, we outsource operations with high computation cost to reduce the user's computation burdens. Through applying the technique of outsource, computation cost for local devices is much lower and relatively fixed. We extended the Sytem security by adding One Time Password to the System while downloading the file and to over come burden of Trusted Authoriy we Created Multiple Trusted Authorities to handle the request.The results of our experiment show that our scheme is efficient for resource constrained devices.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," *EUROCRYPT '05*, LNCS, vol. 3494, pp. 457-473, 2005.

[2] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute- Based Encryption," *Proc. IEEE Symposium on Security and Privacy*pp. 321-334, May 2007, doi: 10.1109/SP.2007.11.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based En-cryption for Fine-Grained Access Control of Encrypted Data," *Proc. 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89-98, 2006, doi:10.1145/1180405.1180418.

[4] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586-615, 2003.

[5] A. Boldyreva, V. Goyal, and V. Kumar , "Identity-Based En-cryption with Efficient Revocation," *Proc. 15th ACM conference on Computer and communications security (CCS ' 08)*, pp. 417-426, 2008.

[6] S. Yu, C. Wang, K. Ren, and W. Lou , "Attribute Based Data Sharing with Attribute Revocation," *Proc. 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS ' 10)*, pp. 261-270, 2010.

[7] M. Yang, F. Liu, J. Han, and Z. Wang, "An Efficient Attribute based Encryption Scheme with Revocation for Outsourced Data Sharing Control," *Proc. 2011 International Conference on Instru-mentation, Measurement, Computer, Communication and Control*, pp. 516-520, 2011.

[8] P.K. Tysowski and M.A. Hasan, "Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applica-tions in Clouds," *IEEE Transactions on Cloud Computing*, pp. 172-186, 2013.

[9] J. Hur and D. K. Noh, “Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,” *IEEE Transactions on Parallel and Distributed Systems*, pp. 1214-1221, 2011.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scal-able, and Fine-Grained Data Access Control in Cloud Comp u-ting,” *Proc. of IEEE INFOCOM ’10*, pp. 1-9, 2010.

[11] M. Green, S. Hohenberger and B. Waters, “Outsourcing the decryp-tion of ABE ciphertexts,” *Proc. 20th USENIX Conference on Security (SEC ’11),* pp. 34, 2011.

[12] J. Li, X.F. Chen, J.W. Li, C.F. Jia, J.F. Ma and W.J. Lou, “Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryp-tion,” *Proc. 18th European Symposium on Research in Computer Security (ESORICS ’13),* LNCS 8134, Berlin: Springer-Verlag, pp. 592-609, 2013.

[13] J.W. Li, C.F. Jia, J. Li and X.F. Chen, “Outsourcing Encryption of At-tribute-Based Encryption with Mapreduce,” *Proc. 14th International Conference on Information and Communications Security (ICICS ’12),* LNCS 7618, Berlin: Springer-Verlag, pp. 191-201, 2012. doi: 10.1007/978-3-642-34129-8_17

[14] M. Chase, “Multi-authority Attribute Based Encryption,” *Proc. 4th Theory of Cryptography Conference (TCC ’07)*, LNCS 4392, Berlin: Springer-Verlag, pp. 515-534, 2007.

[15] Z. Liu, Z. Cao, Q. Huang, D. S. Wong and T. H. Yuen, “Fully Secure Multi-Authority Ciphertext-Policy Attribute-Based Encryption with-out Random Oracles,” *Proc. 16th European Symposium on Research in Computer Security (ESORICS ’11)*, LNCS 6879, Berlin: Springer-Verlag, pp. 278-297, 2011.

[16] J.G. Han, W. Susilo, Y. Mu and J. Yan, “Privacy-Preserving Decentral-ized Key-Policy Attribute-Based Encryption,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no.11, pp. 2150-2162, Nov 2012, doi: 10.1109/TPDS.2012.50.

[17] H.L. Qian, J.G. Li and Y.C. Zhang, “Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption with Fully Hidden Access Structure,” *Proc. 15th International Conference on Information and Communications Security (ICICS ’13)*, LNCS 8233, Berlin: Springer- Verlag, pp. 363-372, 2013.

[18] H.L. Qian, J.G. Li, Y.C. Zhang and J.G. Han, “Privacy Preserv-ing Personal Health Record Using Multi-Authority Attribute- Based Encryption with Revocation,” *International Journal of Information Security*, doi: 10.1007/s10207-014-0270-9.

[19] Z. Liu, Z.F. Cao and Duncan S. Wong, “Black-Box Traceable CP-ABE: How to Catch People Leaking Their Keys by Selling Decryption Devices on eBay,” *Proc. 2013 ACM SIGSAC Conference on Computer and Communications Security (CCS ’13)*, pp. 475-486, 2013, doi: 10.1145/2508859.2516683.

[20] Z. Liu, Z.F. Cao and Duncan S. Wong, “White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 76-88, 2013, doi: 10.1109/TIFS.2012.2223683.

[21] J.T. Ning, Z.F. Cao, X.L. Dong, L.F. Wei and X.D. Lin, “Large Universe Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability,” *Proc. 19th European Symposium on Research in Computer Security (ESORICS ’14)*, LNCS 8713, Berlin: Springer-Verlag, pp. 55-72, 2014.

[22] J.D. Yu, P. Lu, Y.M. Zhu, G.T. Xue and M.L. Li, “Toward Secure Mul-tikeyword Top-k Retrieval over Encrypted Cloud Data,” *IEEE Trans-actions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 239-250, 2013, doi:10.1109/TDSC.2013.9

[23] T. Yang, P.P.C. Lee, J.C.S. Lui, R. Perlman, “Secure Overlay Cloud Storage with Access Control and Assured Deletion,” *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 903-916, 2012, doi: 10.1109/TDSC.2012.49

[24] L. Cheung and C. Newport, “Provably Secure Ciphertext Policy ABE,” *Proc. 14th ACM Conference on Computer and Communications Security (CCS ’07)*, pp. 456-465, 2007, doi:10.1145/1180405.1180418.

[25] D. Boneh and M.K. Franklin, “Identity-Based Encryption from the Weil Pairing,” *CRYPTO ’01*, LNCS, vol. 2139, pp. 213-229, Aug. 2001. [26] A. Beimel, “Secure Schemes for Secret Sharing and Key Distr i-bution” PhD thesis, Israel Institute of Technology, 1996.

[27] M. Blaze, G. Bleumer and M. Strauss, “Divertible Protocols and Atom-ic Proxy Cryptography,” *Proc. International Conference on the Theory and Application of Cryptographic*

Techniques (EUROCRYPT '98), LNCS 1403, Berlin: Springer-Verlag, pp. 127-144, 1998.

[28] A.D. Caro, "Java Pairing-Based Cryptography Library," http://gas.dia.unisa.it/projects/jpbc, 2013.

[29] B. Lynn, "Pairing-Based Cryptography (PBC) Library," http://crypto.stanford.edu/pbc, 2013. [30] H.D Robert, F. Bao, H. Zhu, "Variations of Diffie-Hellman Problem," *Proc. 5th International Conference on Information and Com-munications Security (ICICS '03),* LNCS 2836, Springer-verlag, pp. 301-312, 2003.