ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Improved Privacy of Cloud Storage Data with Multi-Authority Cloud Storage Using CPABE

Vidyavati Bannatti
PG Scholar,
Computer Science and Engineering,
Bheema institute of Technology and Science.

K.Arjun
Assistant Professor,
Computer Science and Engineering,
Bheema institute of Technology and Science.

ABSTRACT:

Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it givesdata owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to dataaccess control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

Index Terms:

Access control, multi-authority, CP-ABE, attribute revocation, cloud storage .

1.INTRODUCTION:

Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works. One important service provided by cloud computing to the data owners to outsource their data in cloud is cloud storage.

The method of data outsourcing and data access counters a major challenge in data access control. The reason is that the data owners cannot fully trust the cloud servers. Ciphertext-Policy Attribute-Based Encryption(CP-ABE) is considered as acceptable technology in cloud storage systems for data access control. In this scheme, there is an authority which is responsible for attribute management and key distribution. For multi-authority system, cipher text policy based encryption is deployed. It handles the attributes from different authorities. The encrypted plain text is integrated with attributes. By using he symmetric key encryption algorithm the data will be encrypted under the access control scheme came from the attribute authority. The CP-ABE system is classified into two types:single-authority CP-ABE, where single authority manages all the attributes, and multi-authority CP-ABE, where different authorities manages attributes from different domains. Multi- authority CP-ABE is most suitable for data access control in cloud storage systems, as multiple authorities issues attributes that user holds and the data owners can share their datas In this paper we propose Privacy enhanced Data Access Control Scheme. Before storing the datas in the cloud the owner will encrypt the message with the different ids which are created randomly. After encryption, the aggregated key for the receiver in order to decrypt the message will be generated with the help of owner private key. The receiver can retrieve the content that he needed by decrypting the cipher text with the help of aggregated key and corresponding access permission id. In this work the data anonymity level is increased by wrapping the data values before data transmission.

That is user request is achieved by wrapping around the user access permission details with the data before transmitting/ storing it in the server. Hence only the user who satisfies the corresponding access permission details like verification information only will gain access to it. Based on the access permission given to the users, the new encryption key will be generated for individual users. By using the encryption that is generated for the unique user, each user can down load the datas which is only accessible to them.In our scheme, the key update is done by each attribute authority and not by the servers. The semi trusted natures of authorized user are eliminated where the datas are hidden from the authorized users also and it achieves more privacy and security over datas

2 SYSTEM MODEL AND SECURITY MODEL:
2.1 System Model:

The remaining paper is structured as follows. Section II describes the background. Section III describes the structure and the system model. The construction of the data access control scheme is given in section IV. The security analysis is described in section V . Theconclusion is givesection VI

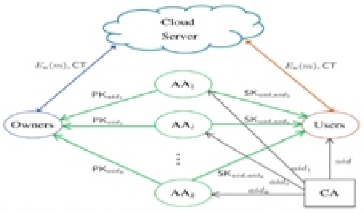

Fig. 1. System model of data access control in multi-authority cloud storage.

In this paper, we first propose a revocable multiauthority CP-ABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system. As described in Table 1, our attribute revocation method is efficient in the sense thatit incurs less communication cost and computation cost, ,mand is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new ciphertext that requires the revoked attribute to decrypt) and forward security (The newly joined user can also decrypt the previously published ciphertexts1, if it has sufficientattributes). Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi-trusted in some scenarios, our scheme can still guarantee the backward security. Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

TABLE 1
Comprehensive Comparison of Attribute Revocation Methods for CP-ABE Systems

Scheme	Authority	Revocation Message	Backward Security	Forward Security	Revocation Enforcer	CT Updater
[11]	Single	$O(n_{non,x} \log \frac{n_u}{n_{non,x}})$	Yes	Yes	Server*	Server*
[13]	Multiple	$O(n_{c,x} \cdot n_{non,x})$	Yes	No	Owner	Owner
[14]	Multiple	$O(n_{c,aid} + n_{non,x})$	Yes	Yes	AA	Server†
Our	Multiple	$O(n_{non,x})$	Yes	Yes	AA	Server†

*: The server is fully trusted; †: The server is semi-trusted.
$|p|$ is the size of element in the groups with the prime order p; n_u denotes the number of users in the system; $n_{non,x}$ denotes the number of non-revoked users who hold the revoked attribute x and $n_{c,x}$ is the number of ciphertexts which contain the revoked attribute x; $n_{c,aid}$ denotes the total number of attributes belongs to the AA_{aid} in all the ciphertexts.

DATA ENCRYPTION BY OWNERS:

Before outsourcing the datas to cloud, the data owner first partitions the data into several components according to logical granularities as m={m1,....mn}. Forexample, data can be partitioned into {name, address, employee, salary, contact number}, next the data components is encrypted with different content keys{k1,.....,kn } using symmetric encryption method, last the access structure mechanism Mi is defined for each content key ki(i=1,...,n). the encryption algorithm takes GPP as input, a collection of publis keys fpr all AAs and outputs CT= GPP,{PKaidk} aidk=k(∏aidЄAAsPK aidk=PKaid1..DATA DECRYPTION BY USERS Inexisting scenario, user login in to the CSPs and the data's can be downloaded with the normal registration, but in existing system the CA will check the user authentication entity. The user can obtain the content key only when it satisfies the access structure defined in thecipher-text CT.

The Decrypt(CT,GPKuid,GSKuid{SKuid,aid}K= (∏aid ЄAAsK'aidkuidk}=(∏aidЄAAsguid,ruid..n\)=CT,GPK uid,GSK

7 CONCLUSION:

In this paper, we proposed a revocable multi-authority CPABE scheme that can support efficient attribute revocation. Then, we constructed an effective data access controlscheme formultiauthority cloud storage systems. We also proved that our scheme was provable secure in therandom oracle model. The revocable multi-authority CPABE\is a promising technique, which can be applied in anyremote storage systems and online social networks etc.

ACKNOWLEDGMENT:

This work was supported by the Research Grants Council of Hong Kong under Project CityU .

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in Proc. IEEE Symp. Security and privacy (S&P'07), 2007, pp. 321-334.

[3] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: AnExpressive, Efficient, and Provably Secure Realization," in Proc.4th Int'l Conf. Practice and Theory in Public KeyCryptography(PKC'11), 2011, pp. 53-70.

[4] V. Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded Ciphertext Policy Attribute Based Encryption," in Proc. 35th Int'l Colloquiumon Automata, Languages, and Programming (ICALP'08), 2008, pp. 579-591.

[5] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters,'Fully Secure Functional Encryption: Attribute-Based Encryptionand (Hierarchical) Inner Product Encryption," in Proc.Advances in Cryptology-EUROCRYPT'10, 2010, pp. 62-91

[6] M. Chase, "Multi-Authority Attribute Based Encryption," inProc. 4th Theory of Cryptography Conf. Theory of Cryptography(TCC'07), 2007, pp. 515-534.

[7] M. Chase and S.S.M. Chow, "Improving Privacy and Securityin Multi-Authority Attribute-Based Encryption," in Proc. 16thACM Conf. Computer and Comm. Security (CCS'09), 2009,pp. 121-130.

[8] A.B. Lewko and B.Waters, "Decentralizing Attribute-BasedEncryption," in Proc. Advances in Cryptology-EUROCRYPT'11,2011, pp. 568-588.

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

[10] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[11] J. Hur and D.K. Noh, "Attribute-Based Access Control withEfficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[12] S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation," inProc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), 2011, pp. 411-415.

[13] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed AccessControl in Clouds," in Proc. 10th IEEE Int'l Conf. TrustCom, 2011,pp. 91-98.

[14] K. Yang and X. Jia, "Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage," in Proc. 32th IEEEInt'l Conf. Distributed Computing Systems (ICDCS'12), 2012,pp. 1-10.

[15] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proc. 21st Ann. Int'l Cryptology Conf.: Advances in Cryptology - CRYPTO'01, 2001, pp. 213-229.

[16] A.B. Lewko and B. Waters, "New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques," in Proc. 32st Ann. Int'l Cryptology Conf.: Advances in Cryptology - CRYPTO'12, 2012, pp. 180-198.

Kan Yang received the BEng degree from University of Science and Technology of China,in 2008 and the PhD degree from City University of Hong Kong, Hong Kong, in August 2013. Hewas a visiting scholar in State University of New York at Buffalo, in 2012. His research interestsinclude cloud security, big data security, cloud data mining, cryptography, social networks,wireless communication and networks, and distributed systems. He is a Student Member ofthe IEEE. Xiaohua Jia received the BSc and MEng degrees from University of Science and Technology of China, in 1984 and 1987, respectively, and the DSc degree in information science from University of Tokyo, Japan, in 1991. He is currently Chair Professor at the Department of Computer Science at City University of Hong Kong. His research interests include cloud computing and distributed systems, computer networks, wireless sensor networks and mobile wireless networks. Prof. Jia is an editor of IEEE TRANSACTIONS ON PARALLEL ANDDISTRIBUTED SYSTEMS (2006-2009), Wireless Networks, Journal of World Wide Web, Journal of Combinatorial Optimization, etc. He is the General Chair of ACM MobiHoc 2008, TPC Co-Chair of IEEE MASS 2009, Area- ,Chair of IEEE INFOCOM 2010, TPC Co-Chair of IEEE GlobeCom 2010, Ad Hoc and Sensor Networking Symp, and Panel Co-Chair of IEEE