Control Cloud Data Access with Attribute Based Encryption in Cloud Computing

Ms.R.Samatharani, Mrs.P.Priyanka

ABSTRACT:

Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, we present a semi anonymous privilege control scheme *AnonyControl* to address not only the data privacy, but also the user identity privacy in existing access control schemes. *AnonyControl* decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity.Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the *AnonyControl-F*, which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both *AnonyControl* and *AnonyControl-F* are secure under the decisional bilinear Diffie–Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes.

I. INTRODUCTION

CLOUD computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a 'cloud'. It greatly attracts attention and interest from both academia and industry due to the profitability, but it also has at least three challenges that must be handled before coming to our real life to the best of our knowledge. First of all, data confidentiality should be guaranteed. The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control. More likely, users want to control the privileges of data manipulation over other users or cloud servers. This is because when sensitive information or computation is outsourced to the cloud servers or another user, which is out of users' control in most cases, privacy risks would rise dramatically because the servers might illegally inspect users' data and access sensitive information, or other users might be able to infer sensitive information from the outsourced computation. Therefore, not only the access but also the operation should be controlled.

Secondly, personal information (defined by each user's attributes set) is at risk because one's identity is authenticated based on his information for the purpose of access control (or privilege control in this paper). As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client's personal information. Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers.

II. RELATED WORK

In [5] and [6], a multi-authority system is presented in which each user has an ID and they can interact with each key generator (authority) using different pseudonyms. One user's different pseudonyms are tied to his private key, but key generators never know about the private keys, and thus they are not able to link multiple pseudonyms belonging to the same user. Also, the whole attributes set is divided into *N* disjoint sets and managed by *N* attributes authorities.

In this setting, each authority knows only a part of any user's attributes, which are not enough to figure out the user's identity. However, the scheme proposed by Chase *et al.* [6] considered the basic threshold-based KP-ABE, which lacks generality in the encryption policy expression. Many attribute based encryption schemes having multiple authorities have been proposed afterwards [7]–[10], but they either also employ a threshold-based ABE [7], or have a semi-honest central authority [8]–[10], or cannot tolerate arbitrarily many users' collusion attack [7].

III. PROBLEM FORMULATION

A. System Model

In our system, there are four types of entities: *N Attribute Authorities* (denoted as A), *Cloud Server*, *Data Owners* and *Data*

Consumers. A user can be a Data Owner and a Data Consumer simultaneously.

Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into *N* disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes. A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them.

Newly joined Data Consumers request private keys from all of the authorities, and they do not know which attributes are controlled by which authorities. When the Data Consumers request their private keys from the authorities, authorities jointly create corresponding private key and send it to them. All Data Consumers are able to download any of the encrypted data files, but only those whose private keys satisfy the privilege tree *Tp* can execute the operation associated with privilege *p*. The server is delegated to execute an operation *p* if and only if the user's credentials are verified through the privilege tree *Tp*.

B. Threats Model

We assume the Cloud Servers are semi-honest, who behave properly in most of time but may collude with malicious Data Consumers or Data Owners to harvest others' file contents to gain illegal profits. But they are also assumed to gain legal benefit when users' requests are correctly processed, which means they will follow the protocol in general. *N* authorities are assumed to be untrusted. That is, they will follow our proposed protocol in general, but try to find out as much information as possible individually. More specifically, we assume they are interested in users' ttributes to achieve the identities, but they will not collude with users or other authorities.

IV CONCLUSION AND POSSIBLE EXTENSIONS

This paper proposes a semi-anonymous attribute-based privilege control scheme *AnonyControl* and a fully-anonymous attribute-based privilege control scheme *AnonyControl-F* to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information. More importantly, our system can tolerate up to $N - 2$ authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis which shows that *Anony-Control* both secure and efficient for cloud storage system. The *AnonyControl-F* directly inherits the security of the *AnonyControl* and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-*n* oblivious transfer. One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes [39]–[41] who support efficient user revocation is one of our future works.

REFERENCES

[1] A. Shamir, “Identity-based cryptosystems and signature schemes,” in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[2] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in *Proc. 13th CCS*, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in *Proc. IEEE SP*, May 2007, pp. 321–334.

[5] M. Chase, “Multi-authority attribute based encryption,” in *Theory of Cryptography*. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.

[6] M. Chase and S. S. M. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in *Proc. 16th CCS*, 2009, pp. 121–130.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, “Secure threshold multi authority attribute based encryption without a central authority,” *Inf. Sci.*, vol. 180, no. 13, pp. 2618–2632, 2010.

[8] V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, “Multi-authority

attribute-based encryption with honest-but-curious central authority," *Int. J. Comput. Math.*, vol. 89, no. 3, pp. 268–283, 2012.

[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in *Proc. IEEE 7th SOSE*, Mar. 2013, pp. 573–577.

[10] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2895–2903.

JUNG *et al.*: CONTROL CLOUD DATA ACCESS PRIVILEGE AND ANONYMITY 199

[11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.

[12] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," *Bull. Korean Math. Soc.*, vol. 46, no. 4, pp. 803–819, 2009.

[13] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, "Multiauthority ciphertext-policy attribute-based encryption with accountability," in *Proc. 6th ASIACCS*, 2011, pp. 386–390.

[14] H. Ma, G. Zeng, Z. Wang, and J. Xu, "Fully secure multi-authority attribute-based traitor tracing," *J. Comput. Inf. Syst.*, vol. 9, no. 7, pp. 2793–2800, 2013.

[15] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public-Key Cryptography*. Berlin, Germany: Springer-Verlag, 2013, pp. 162–179.

[16] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 11, pp. 2171–2180, Nov. 2013.

[17] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, "Anonymous attributebased encryption supporting efficient decryption test," in *Proc. 8th ASIACCS*, 2013, pp. 511–516.

[18] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2001, pp. 213–229.

[19] A. Sahai and B. Waters, "Fuzzy identity-based encryption," *Advances*

in Cryptology. Berlin, Germany: Springer-Verlag, 2005.

[20] J. Liu, Z. Wan, and M. Gu, "Hierarchical attribute-set based encryption for scalable, flexible and fine-grained access control in cloud computing," in *Information Security Practice and Experience*. Berlin, Germany: Springer-Verlag, 2011, pp. 98–107.

Author's Profile

Ms. R.Samatha rani received M.Tech degree from AuroraTechnological & Research Institute & Engineering , Warangal affiliated to JNTUH, Hydearabad. She is currently working as Assistant professor, Department of CSE, in Vinuthna Institute of Technology & Science ,Hasanparthy, Warangal, Telangana, India. Her interest includes Data Base Management Systems.

Mrs. P.Priyanka received B.Tech Degree from chaithnya Institute of Engineering and Technology , Rajahmandry affiliated to JNTUK, Kakinada. She is currently pursuing M.Tech Degree in Software Engineering specialization in Vinuthna Institute of Technology & Science Hasanparthy, Warangal, Telangana, India.