IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

Completely Anonymous Encryption Attribute-Based Access Control With The Right Data To The Cloud And Anonymity

Ms. M.Lakshmi Thulasi Mr.P.VIJAY

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.

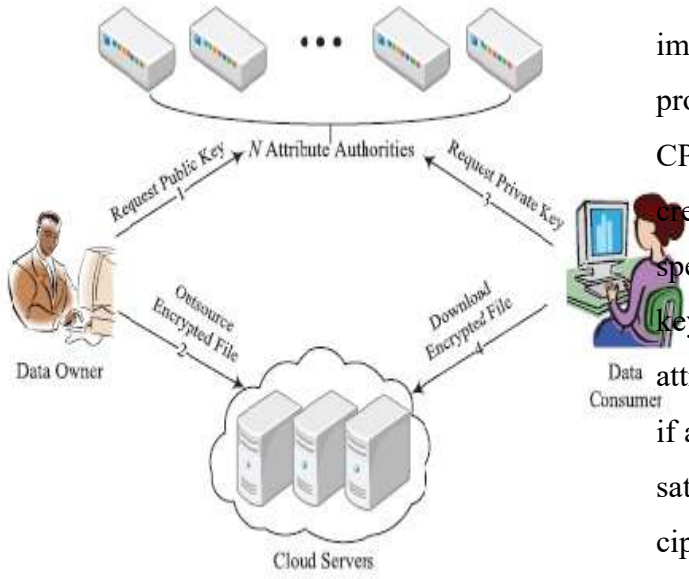
1INTRODUCTION

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’. 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

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

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. Various techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by], in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it. Few years later, Fuzzy Identity-Based Encryption is proposed, which is also known as Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a descriptor's identity has some overlaps with the one specified in the cipher text. Soon after, more general tree-based ABE schemes, Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute- Based Encryption (CP-ABE) are presented to express more general condition than simple 'overlap'. They are counterparts to each other in the sense that the decision of encryption policy (who can or cannot decrypt the message) is made by different parties.

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363



In the KP- a ciphertext is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes this user's identity (e.g. IIT AND (Ph.D OR Master)). A user can decrypt the ciphertext if and only if the access tree in his private key is satisfied by the attributes in the ciphertext. However, the encryption policy is described in the keys, so the encrypter does not have entire control over the encryption policy. He has to trust that the key generators issue keys with correct structures to correct users. Furthermore, when a re-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation. On the other hand, those problems and overhead are all solved in the CP-ABE. In the CP-ABE, cipher texts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users' attributes. A user can decrypt the ciphertext if and only if his attributes in the private key satisfy the access tree specified in the ciphertext. By doing so, the encrypter holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots. Unlike the data confidentiality, less effort is paid to protect users' identity privacy during those interactive protocols.

Users' identities which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes. But it seems natural that users are willing to keep their identities secret while they still get their private keys. Therefore, we propose AnonyControl and AnonyControl-F to allow cloud servers to control users' access

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

privileges without knowing their identity information.

Their main merits are: 1) the proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. 2) The proposed schemes are tolerant against authority compromise, and compromising of up to (N −2) authorities does not bring the whole system down. 3) We provide detailed analysis on security and performance to show feasibility of the scheme AnonyControl and AnonyControl-F.

2 PROBLEM FORMULATIONS

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.

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

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' attributes to achieve the identities, but they will not collude with users or other authorities. This assumption is similar to many previous researches on security issue in cloud computing and it is also reasonable since these authorities will be audited by government offices. However, we will further relax this assumption and allow the collusion between the authorities

3. ACHIEVING FULL ANONYMITY

We have assumed semi-honest authorities in AnonyControl nd we assumed that they will not collude with each other. This is a necessary assumption in AnonyControl because each authority is in charge of a subset of the whole attributes set, nd for the attributes that it is in charge of, it knows the exact information of the key requester. If the information from all authorities is gathered altogether, the complete attribute set of the key requester is recovered and thus his identity is disclosed to the authorities. In this sense, AnonyControl is semi anonymous since partial identity information (represented as some attributes) is disclosed to each authority, but we can achieve a full-anonymity and also allow the collusion of the authorities.

The key point of the identity information leakage we had in our previous scheme as well as every existing attribute based encryption schemes is that key generator (or attribute authorities in our scheme) issues attribute key based on the reported attribute, and the generator has to know the user's attribute to do so. We need to introduce a new technique to let key generators issue the correct attribute key without knowing what attributes the users have. A naive solution is to give all the attribute keys of all the attributes to the key requester and let him pick whatever he wants. In this way, the key generator does not know which attribute keys the key requester picked, but we have to fully trust the key requester that he will not pick any attribute key not allowed to him. To solv B. Fully Anonymous Multi-

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

Authority CP-ABE In this section, we present how to achieve the full anonymity in AnonyControl to designs the fully anonymous privilege control scheme AnonyControl-F.

The Key Generate algorithm is the only part which leaks identity information to each attribute authority. Upon receiving the attribute key request with the attribute value, the attribute authority will generate and sends it to the requester where att (i) is the attribute value and ri is a random number for that attribute. The attribute value is disclosed to the authority in this step. We can introduce the above 1-out-of-n OT to prevent this leakage. We let each authority be in charge of all attributes belonging to the same category. For each attribute category c (e.g., University), suppose there are k possible attribute values, then one requester has at most one attribute value in one category. Upon the key request, the attribute authority can pick a random number ru for the requester and generates H(att (i))ru for all i ∈ {1, . . . , k}. After the attribute keys are ready, the attribute authority and the key requester are engaged in a 1-out-of-k OT where the key requester wants to receive one attribute key among k. **By introducing the 1-out-of-k OT** in our Key Generate algorithm, the key requester achieves the correct attribute key that he wants, but the attribute authority does not have any useful information about what attribute is achieved by the requester. Then, the key requester achieves the full anonymity in our scheme and no matter how many attribute authorities collude; his identity information is kept secret.

4. SECURITY ANALYSIS

A. Tolerance Against Authorities' Collusion or Compromise Attack In the proposed scheme, an authority generates a set of random secret parameters and shares it with other authorities via secure channel, and is computed based on this parameters. It is believed that DDH problem is intractable in the group G0 of prime order p, therefore does not leak any statistical information about This implies even if an adversary is able to compromise up to (N − 2) authorities, there are still two parameters kept unknown to the adversary. So, the adversary is not able to guess the valid g_vk,

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

and he fails to construct a valid secret key. Hence, the scheme achieves compromise tolerance to up to (N − 2) authorities compromise. But, if we reduce the time complexity of the setup phase by dividing authorities into several clusters having C authorities in each, attackers can compromise C − 1 authorities in a cluster to create valid master keys of that cluster. Therefore, there is a tradeoff between tolerance and complexity. However, since the number of authorities is typically not very huge, and the setup is one-time operation at the very beginning of the system setup, we recommend using the original setup algorithm whose complexity is O(N2).

Note that the compromised authorities are able to issue valid attribute keys for which they are in charge of, so the cipher texts whose privilege trees have only those attributes might be illegally decrypted if the attacker issue all possible attribute keys to himself. But, since the authorities are well protected servers, it is hard to compromise even one authority, and the probability of compromising enough authorities to illegally decrypt some cipher text is very low. B. Tolerance Against Users' Collusion Attack In order to access a plaintext, attackers must recover Y s0 = e(g, g)s0_vk , which can be recovered only if the attackers have enough attributes to satisfy the tree T0.

When two different keys' components are combined, the combined key cannot go through the polynomial interpolation in the decryption algorithm due to the different randomizers in each key. Therefore, at least one key should be valid to satisfy a privilege tree. C

5. PERFORMANCE EVALUATION

In this section, we present the performance evaluation based on our measurement on the implemented prototype system of AnonyControl-F. To the best of our knowledge, this is the first implementation of a multi-authority attribute based encryption scheme. Our prototype system provides five command line tools.

AnonyControl-setup: Jointly generates public key and N master keys.

Anonycontrol-keygen: Generates a part of private key for the attribute set it is responsible for.

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

Anonycontrol-enc: Encrypts a file under r privilege trees.

Anonycontrol-enc: Decrypts a file if possible.

AnonyControl-rec: Decrypts a file and re-encrypts it under different privilege trees.

6 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 loud computing environment. We also conducted detailed security and performance analysis which shows that Annoy- 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 that support efficient user revocation is one of our future works.

7. RELATED WORK

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. 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 but they either also employ a threshold-based or have a semi-honest central authority or cannot tolerate arbitrarily many users' collusion attack.

8. ACKNOWLEDGEMENTS

The authors offer their gratitude to their colleague Jingshan Yin, who implemented the 1-out-of-n protocol, and Shih-ming Huang from NCTU, who proofread their paper to correct minor errors.

9. 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.

[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,

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

Germany: Springer-Verlag, 2011, pp. 98–107.

[21] A. Kapadia, P. P. Tsang, and S. W. Smith, "Attribute-based publishing with hidden credentials and hidden policies," in Proc. NDSS, 2007, pp. 179–192.

[22] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in Proc. 4th Workshop Secure Netw. Protocols, Oct. 2008, pp. 39–44.

[23] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.

[24] T. Jung, X. Mao, X.-Y. Li, S.-J. Tang, W. Gong, and L. Zhang, "Privacypreserving data aggregation without secure channel: Multivariate polynomial evaluation," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2634–2642.

[25] T. Jung and X.-Y. Li, "Collusion-tolerable privacy-preserving sum and product calculation without secure channel," IEEE Trans. Dependable Secure Comput., to be published.

[26] X.-Y. Li and T. Jung, "Search me if you can: Privacy-preserving location query service," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2760–2768.

[27] L. Zhang, X.-Y. Li, Y. Liu, and T. Jung, "Verifiable private multipartycomputation: Ranging and ranking," in Proc. IEEE INFOCOM, Apr. 2013, pp. 605–609.

[28] L. Zhang, X.-Y. Li, and Y. Liu, "Message in a sealed bottle: Privacy preserving friending in social networks," in Proc. IEEE 33rd ICDCS, Jul. 2013, pp. 327–336.

[29] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.

[30] C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in Proc. IEEE INFOCOM, Apr. 2011, pp. 820–828.

[31] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE 30th ICDCS, Jun. 2010, pp. 253–262.

[32] Y. Liu, J. Han, and J. Wang, "Rumor riding: Anonymizing unstructured peer-to-

peer systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 3, pp. 464–475, Mar. 2011.

[33] Tor: Anonymized Network. [Online]. Available: https://www.torproject.org/, accessed 2014.

[34] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[35] M. Naor and B. Pinkas, "Oblivious transfer and polynomial evaluation," in Proc. 31st STOC, 1999, pp. 245–254.

[36] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," Commun. ACM, vol. 28, no. 6, pp. 637–647, 1985.

[37] W.-G. Tzeng, "Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," IEEE Trans. Comput., vol. 53, no. 2, pp. 232–240, Feb. 2004.

[38] Ciphertext-Policy Attribute-Based Encryption Toolkit. [Online]. Available: http://acsc.csl.sri.com/cpabe/, accessed 2014.

[39] W. Ren, K. Ren, W. Lou, and Y. Zhang, "Efficient user revocation for privacy-aware PKI," in Proc. ICST, 2008, Art. ID 11.

[40] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[41] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. 5th ASIACCS, 2010, pp. 261–270.

AUTHOR'S DETAILS

.P.VIJAYA RAGHAVULU received M.Tech(CSE) Degree from School of Information Technology, Autonomous, and Affiliated to JNTUA,Anathapur. He is currently working as Assistant Professor in the Department of Computer Science and Engineering in Modugula Kalavathamma Institute of Technology for Women, Rajampet, Kadapa,AP India. His interests includes Object Oriented Programming, Operating System, Database Management System, Computer Networking, Cloud Computing and Software Quality Assurance.

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

Ms. M.Lakshmi Thulasi. She is currently pursuing M.tech Degree in Computer Science and Engineering specialization in Modugula Kalavathamma Institute of Technology for Women, Rajampet, Kadapa,AP .