INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

N Joint Authorities: Integration of Secured Cloud Data Access Privilege with Attribute based Encryption over Distributed Authorities

G. Saraswathi #1, J. Jayapriya *2

Mailam Engineering College, Mailam #1, *2

sarasgovin@gmail.com #1

Abstract—Cloud computing is a rapid growth field in computer technology, which provides flexible, on-demand, and low-cost usage of computing resources, but the data is deploy to some cloud providers, and variety privacy concerns emerge from it. Variety schemes based on the attribute-based encryption have been implemented to secure the cloud storage. Nevertheless, most work depends on the data contents privacy and the access control, while less interest is paid to the privilege control and the identity privacy. In this, we implement a semi nameless privilege control scheme nameless Control to address not only the data privacy, but also the user identity privacy in existing access control schemes. Nameless Control decentralizes the central authority to limit the identity leakage and thus achieves s. Besides, it also creates the file access control to the privilege control, by which privileges of all operations on the cloud data can be maintained in a fine-grained manner. Frequently, we provide the nameless Control-F, which fully determines the identity leakage and achieve the full anonymity. Finally, this proposed system provides, high performance efficiency and security in cloud Storage.

Keywords: Nameless, Privacy, Semi nameless, Authority, Encryption

1. 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. Various techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir, 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 decrypt's identity has some overlaps with one specified in the cipher text. Soon after, more general tree-based ABE schemes, Key-Policy Attribute-Based Encryption (KP-ABE) and Cipher text-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.

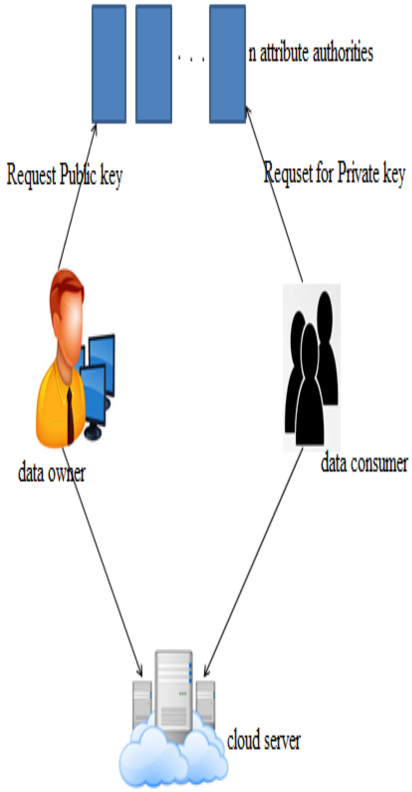
2. Related Work

In a multi-authority system is presented which each user has an ID and they can interact with each regenerator (authority) using different pseudonyms. One user 'different pseudonyms are tied to his private key, but regenerators never know about the private keys, and thus there 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 a user's attributes, which are not enough to figure out the user 'identity considered the basic threshold-based KP-ABE, which lacks generality in the encryption policy expression. Many attributed encryption schemes having multiple authorities have been proposed afterwards, but they either also employ threshold-based ABE, or have a semi-honest central authority, or cannot tolerate arbitrarily many users collusion attack. The work is the most similar ones to ours in that they also tried to decentralize the central authority in the CP-ABE into multiple ones. Use a LSSS matrix as an access structure, but their scheme only converts the AND, OR gates to the LSSS matrix which limits their encryption policy to Boolean formula, while we inherit the flexibility of the access tree having thresholates. Muller et al. also supports only Disjunctive Normal Form (DNF) in their encryption policy. Besides the fact that we can express arbitrarily general encryption policy, our system also tolerates the compromise attack towards attributes authorities, which is not covered in many existing works. Recently, there also appeared traceable multi-authority ABE and, which are on the opposite direction of ours those schemes introduce accountability such that malicious users' keys can be traced. On the other hand, similar direction as ours can be found in, who try to hide encryption policy in the cipher texts, but their solutions do not prevent the attribute disclosure in the key generation phase. To some extent, these three works and ours complement each other the sense that the combination of these two types protection will lead to a completely anonymous ABE. 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 ABE, or have a semi-honest central authority, or cannot tolerate arbitrarily many users' collusion attack are the most similar ones to ours in that they also tried to decentralize the central authority in the CP-ABE into multiple one, Use a LSSS matrix as an access structure, but their scheme only converts the AND, OR gates to the LSSS matrix, which limits their encryption policy to boo lean formula, while we inherit the flexibility of the access tree having threshold gates. Muller et al. also supports only Disjunctive Normal Form (DNF) in their encryption policy. Besides the fact that we can express arbitrarily general encryption policy, our system also tolerates the compromise attack towards attributes authorities, which is not covered in many existing works.

3. Proposed Work

Therefore, we propose Nameless Control and Nameless Control-F (Fig. 1) to allow cloud servers to control users' access privileges without knowing their identity information. Their main merits are: The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in Nameless Control and no information is disclosed in Nameless Control-F. The proposed schemes are tolerant against authority compromise, and compromising of up to (N −2) authorities does not bring the whole system down. We provide detailed analysis on security and performance to show feasibility of the scheme Nameless Control and Nameless Control-F. We firstly implement the real toolkit of a multi authority based encryption scheme Nameless Control and Nameless Control-F.

4. System Design



From this, architecture it consists of the following, data owner, data consumer and the cloud server. First the data owner access for public key to the authorities as well as the data consumer also access private key to the authorities.

5. Methodology

5.1 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 Design Goals

Our goal is to achieve a multi-authority CP-ABE which: achieves the security defined above; guarantees the confidentiality of Data Consumers' identity information; and tolerates compromise attacks on the authorities or the collusion attacks by the authorities. For the visual comfort, we frequently use the following notations hereafter. Ak denotes the k-th attribute authority; Au denotes the attributes set of user u; Auk denotes the subset of Au controlled by Ak; and ATp denotes the attributes set included in tree Tp.

5.2 Nameless control construction

Setup At the system initialization phase, any one of the authorities chooses a bilinear group G0 of prime order p with generator g and publishes it. Then, all authorities independently and randomly picks vk ∈ Zp and send Yk = e(g, g)vk to all ther authorities who individually compute Y := _k∈A Yk = e(g, g)_k∈A vk . Then, every authority Ak randomly picks N − 1 integers skj ∈ Zp(j ∈ {1, . . . , N}\{k}) and computes gskj . Each gskj is shared with each other authority Aj. An authority Ak, after receiving N −1 pieces of gs jk generated by Aj.

We have assumed semi-honest authorities in Nameless Control and we assumed that they will not collude with each there. This is a necessary assumption in Nameless Control because each authority is in charge of a subset of the whole attributes set, and 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, Nameless Control 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 solve this, we leverage the following Oblivious Transfer (OT).

5.3 Fully Anonymous Multi-Authority CP-ABE

In this section, we present how to achieve the full anonymity in Nameless Control to designs the fully anonymous privilege control scheme Nameless Control -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 H(att (i))ri 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 (e.g., IIT, NYU, CMU ...), 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.

6. Conclusion

From this, N joint Authorities Integration of secured cloud data access privilege with attribute based encryption over distributed authorities has been implemented. This paper proposes a semi-anonymous attribute-based privilege control scheme Nameless Control and a fully-anonymous attribute-based privilege control scheme Nameless Control-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. Additionally, we also enhance the system performance and efficiency of the system.

7. 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