Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

Access Control in Cloud Computing through Simple, Secure and Efficient Hierarchical Key Assignment

[1]Syed Ashhar Fazal, [2]Sandeep Kumar Sharma, [3]Rakesh Kumar Ranjan, [4]Shridevi Desai

Abstract

Access control is a necessary security component of cloud computing, and hierarchical access control is of particular interest since in practice one is entitled to different access right. This paper presents a hierarchical key assignment scheme based on linear-geometry as the solution of adjustible and fine-grained hierarchical access control in cloud computing. In our scheme, the encryption key of each class in the hierarchy is connected with a private vector and a public vector, and the inner product of the private vector of an ancestor class and the public vector of its descendant class can be used to derive the encryption key of that descendant class without the need of related calculation.

Keywords: Access control, hierarchical key assignment, linear geometry, pseudorandom function

Introduction

We introduced the HASBE scheme for knowing scalable, flexible, and fine-grained power control in cloud computing. The HASBE scheme smoothly incorporates a hierarchical Structure of system users by applying a delegation algorithm to ASBE. HASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user promise because of multiple value tasks of attributes.

CLOUD computing has attracted great attention of both academia and information technology industry. Built on the architecture of parallel and distributed computing, this new computing paradigm possesses numerous advantages including low cost, high-efficiency, flexibility and scalability. From the bottom layer to the top, cloud computing can be divided into three delivery models, namely infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) .

In this paper, we construct a scheme, which has several traits: (1) high performance; (2) fine-grained access control; (3) scalability; (4) full delegation. Our HABE scheme, which is also collusion resistant, can be proven to be semantically secure against adaptive chosen plaintext attacks under the BDH assumption and the random oracle model.

Nowadays, there are many kinds of cloud service systems providing services via the Internet, such as Amazon's EC2, IBM's Blue Cloud, Google App Engine, Microsoft's Azure, etc. With the visualize advances of cloud service systems, enterprise users can access to the resource on the cloud anytime and anywhere, without the need to manage the latent hardware/software systems. Without any doubt, DATA is an extremely important asset for all organizations, especially for enterprise users. But this deserves special attention in the era of cloud computing. Different from the based on local storage, cloud computing stores data on remotely located servers via the Internet.

The data owner needs to upload his/her own data onto the cloud server, and authorized users can retrieve the data from the cloud. In cloud computing, it is the semi trusted Cloud Service Provider (CSP) that manages the cloud and all data on the cloud , and as a result, data confidentiality is at the top of the list of relate cloud computing.

Hierarchical Key Assignment

The hierarchical key assignment scheme (HKAS), first given by Akl and Taylor. It is used to solve the hierarchical multigroup communication problem. From the aspect of access control, HKAS allows authorized users to have different access right in

multi-group communication. According to different access right, users are organized in a hierarchy and divided into different disjoint groups called security classes.

Generally, HKAS is modeled as follows: a central authority (CA) assigns a private information and an encryption key to each class in the hierarchy. The encryption key of each class, which is obtain from the class private information and other public information, is used to protect the data of that class (e.g., the secret key in symmetric-key cryptographic algorithms). Moreover, the private information and encryption key of a class A are sufficient to derive the encryption key of each descendant class of classA.

Motivation

The number of existing HKASs are indirect access methods. Namely, in order to obtain the encryption key of a descendant class, the ancestor needs to repeatedly compute all encryption keys on the path from itself to the descendant class.

We have presented a time-bound key assignment scheme for a partial-order hierarchy. Since our method has the time-bound property, the vendor can offer great flexibility in the user subscription. Each user can only use his key information to calculate the corresponding encrypting key in the duration of his subscription. Therefore our method can easily solve the key update problem without higher costs. In addition, our method applies public values instead of tamper resistant devices, which is more suitable for cloud computing, HKAS based on ECC and polynomial interpolating in requires a large overhead on calculation and storage. Therefore, it is meaningful and important to solve a simple, secure and effective HKAS to meet the requirements of direct data access in cloud computing.

Proposed System

The most important feature of our proposed scheme is that it only needs to calculate the values of pseudorandom function and vector multiplication, which leads to a very light calculation overhead. Additionally, the proposed scheme can achieve powerful key in seperate security with a formal security proof.

We propose a HKAS based on linear geometry. The originality of our scheme is that we use a specially designed matrix to describe the hierarchy of classes. With this method, any ancestor class can directly calculate the encryption keys of its descendant classes. In our proposed scheme, data owner firstly interacts with CA, and obtains system parameters. Then, the data owner generates a finite field Fq and a PRF F.

This paper, present a safe group key management scheme for ranked mobile ad-hoc networks. Our process aims to improve both scalability and survivability of group key management for huge-scale wireless ad-hoc networks.

Chart -1: Time consumed by data owner in key generation.

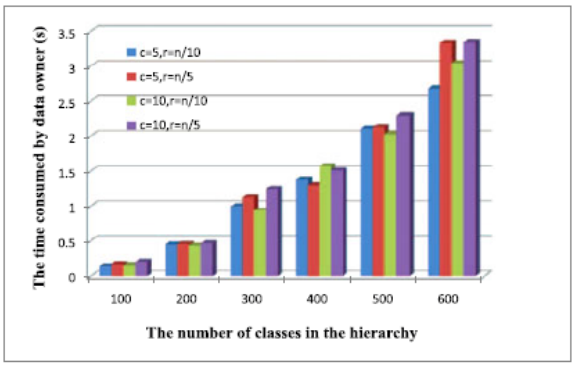


Chart -2: Time consumed by data owner in dynamic management.

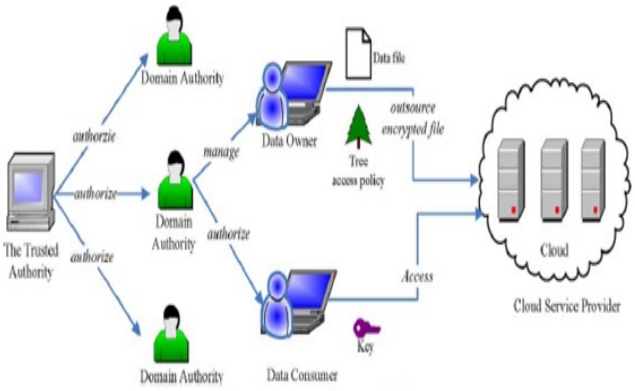


Fig. 1. System model.

System Description

A hierarchical access control system in cloud computing consists of four kinds of entities: CA, data owner, data consumer and CSP. See the access control policy is control by the data owner, not the CSP. It keeps pace with the hierarchical structure of the data consumers. The shared data which is encrypted by the data owner stores in the cloud servers with a hierarchical fabric ID. If a data consumer sends an access request to CSP with a hierarchical fabric ID, CSP finds the corresponding encrypted data for the data consumer.

Security Model

In this paper, we only discuss the KI-security of HKAS, since KI- security implies KR-security the security models with respect to both static and dynamic conflict are polynomially equivalent. Thus, we focus on the security model with respect to a static adversary.

Forward security: the user U cannot access the future communication data of the class Vi when U leaves the class Vi.

Backward security: the user U cannot access the previous communication data of the class Vj when U is added to the class Vj.

Pseudorandom Function

On the construction of HKAS, pseudorandom function is a very heplful tool. Roughly speaking, pseudorandom function is a family of functions, which can be easily calculated given a short and

Random key. Meanwhile, the input/output behavior of the function is computationally different from that of a random function.

Our Contribution

In this paper, we give a HKAS based on linear geometry as a solution to hierarchical access in cloud computing. The important principle of our method is that a private vector and a public vector are connected with the encryption key of each class. Furthermore, we adopt the orthogonality concept of vector space in linear geometry to make sure that two independent classes have nothing to do with each other. The essential ideas are:

- Each class in the system, its private vector is non orthogonal to the corresponding public vector, and the value of their inner product is equal to the encryption key of this class.

- The private vector of an ancestor class is non-orthogonal to the public vector of its descendant classes. The value of their inner product can be taken as an indirect key between the two classes, and the ancestor class can derive the encryption key of the descendant class using this value.

- For each descendant class, its private vector is orthogonal to the public vector of ancestor class.

- If the relationship between two classes is neither descendant nor ancestor, the private vector of one class is orthogonal to the public vector of the other.

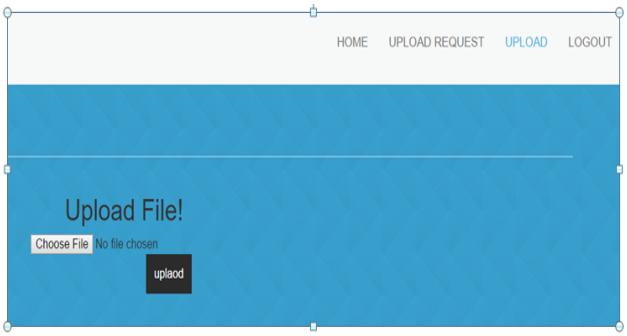
The most important feature of our proposed scheme is that it only needs to calculate the values of pseudorandom function (PRF) and vector multiplication, which result to a very light calculation overhead. Additionally, the proposed scheme can get strong key indistinguishability security (S-KI-security) with a formal security proof.

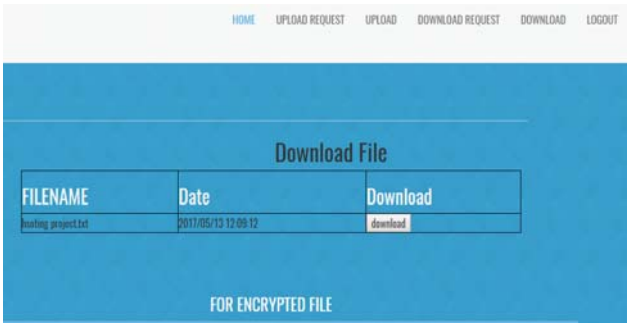
Results and Discussion

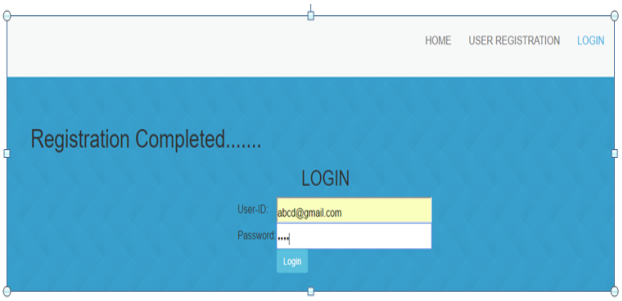
In our design, a private vector and a public vector are connected with the encryption key of each class in the hierarchy. Our scheme provides hierarchical access because class encryption key can be derived from the inner product of the public. Since the computing method is very simple, we believe the proposed. Method can serve as an efficient solution of flexible and fine-grained power control in cloud computing.

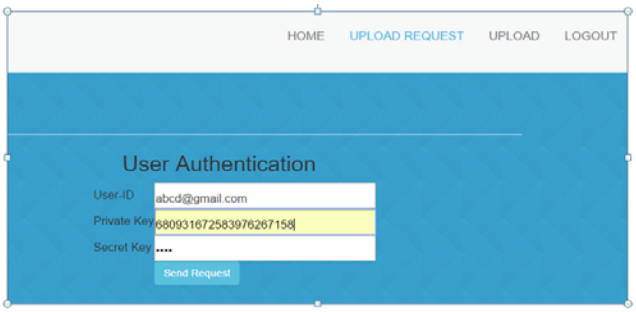
Conclusion

We presented a new design of hierarchical key assignment based on linear geometry. In our design, a private vector and a public vector are connected with the encryption key of each class in the hierarchy. Our method provides hierarchical access because class encryption key can be extracted from the inner product of the public vector of that class and the private vector of its ancestor class. We also give efficient key management solutions to address potential changes in the hierarchy. A formal proof shows that the proposed scheme has the property of strong key indistinguishability under the assumption of pseudorandom functions. Simulations show that our scheme provides an optimized trade-off between computation consumption and storage space, though the size of the public parameter in our scheme is slightly larger than others. Since the computing method is very simple, we believe the proposed scheme can serve as an efficient solution of flexible and finegrained access control in cloud computing.









References

[1]. A Secure Hierarchical Key Management Scheme in Wireless Sensor Network. Authors: - Yiying Zhang, Xiangzhen Li, Jianming Liu, Jucheng Yang and BaojiangCui. Year:- 2012.

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

[3] J.-Y. Huang, C.-K. Chiang and I.-E. Liao, "An efficient attribute-based encryption and access control scheme for cloud storage environment," in Proc. 8th Int. Conf. Grid Pervasive Comput., 2013, pp. 453–463

[4] K. Yang and X. Jia, "Expressive, efficient and revocable data access control for multi-authority cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, Jul. 2014

[5] B.-Z. He, C.-M. Chen, T.-Y. Wu and H.-M. Sun, "An efficient solution for hierarchical access control problem in cloud environment," Math. Problems Eng., vol. 2014, p. 8, 2014.

Author's Details

1 Syed Ashhar Fazal, UG student, CSE, T John Institute of Technology, Karnataka, India, syedashharfazal@gmail.com

2 Sandeep Kumar Sharma, UG student, CSE, T John Institute of Technology, Karnataka, India, sdpsharma93@gmail.com

3 Rakesh Kumar Ranjan, UG student, CSE, T John Institute of Technology, Karnataka, India, rakeshranjantjit@gmail.com

4. Shridevi Desai, Assistant Proffesor, CSE, T John Institute of Technology, Karnataka, India,

shridevi@tjohngroup.com