Creating Time-Limited Attributes for Time-Limited Services in Cloud Computing

Azin Moradbeikie, International University of Imamreza, Mashhad, Iran
Saied Abrishami, Ferdowsi University of Mashhad, Mashhad, Iran
Hasan Abbasi, International University of Imamreza, Mashhad, Iran

ABSTRACT

Nowadays, Cloud Computing is considered one of the important fields in both research and industry. Users enjoy membership of cloud providing effective services called time-limited services. This paper addresses time-limited services offering an attribute-based access control method and time-limited attributes providing users’ time-limited membership in cloud service. The proposed method authenticates users for specific time limit after which they are considered invalid. This method is decentralized resistible against backward and forward attacks. Moreover, this approach compared to other approaches reduces calculation and communication overhead.

KEYWORDS

Access Control, Attribute-based Encryption, Cloud Computing, Secret Sharing Scheme, Time-limited Services

1. INTRODUCTION

Cloud computing is a system whose resources as data center are shared through technology virtualization. This system consists of some basic attributes including virtualization, elastic properties based on demand and instant service provision. Therefore, cloud reduces the expenses and provides user with increased speed (Tanzim Khorshed Md., 2012). Cloud services are basically categorized as infrastructure as service, applications as service, and platform as service (Xiao AZhifeng, 2013).

Despite all of the attributes and facilities, users are skeptical to join the cloud since they distrust cloud security. Cloud has unique attributes leading to new security problems and issues including users’ distrust toward cloud providers. Privacy is one of the important issues demanded by users to be provided by the cloud. Cloud privacy means that users’ data and personal information should be kept secret and confidential for both cloud providers and other users. Besides, the cloud is supposed to ensure user information privacy meaning that information outsourced by one user should not be accessible to other non-authenticated users. Thus, before outsourcing to the cloud, the cloud should encrypt the data and prevent the probable problems through running an appropriate access control method.

Cloud facing with many users demonstrates attributes like dynamic nature, lack of harmony and variation in services, and different and even antithetical access control policies (Younis Y A., 2014). These attributes make the existing access control methods inefficient. On the other hand, offering a new access control method is not a good option since presenting a new method requires time and effort for testing and solving the relevant problems. Therefore, the best option is to modify and adapt the existing models so that they could well meet all the existing cloud requirements.

There are generally four models of access control. Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC), andAttributed-Based
Access Control (ABAC). In mandatory access control, a central authority is responsible for making decisions about who can access to resources. In this approach, each user and source is given an access class. This class is a security level used for securing information flow between users and resources. Despite the provision of security during information flow, this model lacks enough required flexibility. In the discretionary access control model, every user is given the permission to access resources based on their identity or membership in a particular group. This method is more flexible than the previous one though showing less security because it does not have the ability to control the flow of information. This makes this model inefficient for cloud computation. Role-based access control model is commonly used for controlling access to resources of organizations. In this method, a person might have several roles or might be a member of different groups, and information is accessible based on different roles without any sensitivity imposed on information (Ferraiolo D.F., 1992). Attribute-based access control is the expanded version of role-based access control aiming at solving some of the problems of the former models and getting more adaptable to cloud attributes. In this model, every single user is given some attributes, and an access policy is given to every data outsourced in the cloud according to which data are encrypted. Users whose attributes can meet the access policy can decrypt the text. This method makes use of attribute-based encryption that is the combination of identity-based encryption and secret sharing scheme explained more in 1-3 section. Different works and projects have enjoyed the application of this access control method (For example (Li M., 2010; Wang G., 2010; Zhao F., 2011; Ruj S. N. A., 2011)).

Users can use cloud applications according to some predetermined principles (for instance the expenses to be paid) for specific time limits beyond which they are considered non-authorized. In this method, people are only authorized to use information for the determined period after which they have no access to the protected resources. Playing online games and watching online videos are some examples of these applications. To implement these Apps in cloud through current attribute-base access control, we need to create a new key attribute for preventing outdated users from data access and share it with in-service ones. This increases the cost of computations and the volume of key exchanges between the cloud and users. To reduce some of these cost, the present study proposes a method called “time-limited (or time trial) attributes” usable only for a time-limited period after which attributes are considered expired and invalid. For implementation of this idea, we have used the combination of two keys for attributes, one for management of time intervals and the other for attribute privacy. The proposed method provides backward and forward security.

1.1. Main Objectives
The main objectives of this study are as follows

- Providing an effective approach for removing or adding members in cloud services
- Reducing the traffic between the cloud server and the user
- Reducing the overhead/burden computations when the membership of a user is expired in a service
- The method must be resistant against collusion attack i.e. different users combining their attributes should not be able to access to any data to which they have not access individually
- This method should provide forward security i.e. the members whose membership time is expired should not be able to decrypt the data after their expiration
- The method should provide backward security i.e. the members recently joined to the service should not be able to decrypt data before their subscription

This paper is organized as follows
Related Content

Critical Analysis of the Role of the Reserve Bank of India in Managing Liquidity in the Interbank Market amidst Financial Stress

Applying Enterprise Risk Management on a Fiber Board Manufacturing Industrial Case
[www.igi-global.com/article/applying-enterprise-risk-management-on-a-fiber-board-manufacturing-industrial-case/120557?camid=4v1a](www.igi-global.com/article/applying-enterprise-risk-management-on-a-fiber-board-manufacturing-industrial-case/120557?camid=4v1a)

Identifying Vulnerabilities of Advanced Persistent Threats: An Organizational Perspective
[www.igi-global.com/article/identifying-vulnerabilities-of-advanced-persistent-threats/111283?camid=4v1a](www.igi-global.com/article/identifying-vulnerabilities-of-advanced-persistent-threats/111283?camid=4v1a)

Microsoft Project as a Risk Management Tool
[www.igi-global.com/article/microsoft-project-risk-management-tool/67375?camid=4v1a](www.igi-global.com/article/microsoft-project-risk-management-tool/67375?camid=4v1a)