Chapter 42
A Comprehensive Review of Access Control Mechanism Based on Attribute Based Encryption Scheme for Cloud Computing

Lokesh B. Bhajantri
https://orcid.org/0000-0002-3947-4292
Department of Information Science and Engineering, Basaveshwar Engineering College, Bagalkot, India

Tabassum N. Mujawar
Ramrao Adik Institute of Technology, Navi Mumbai, India

ABSTRACT

Cloud computing is the most prevailing paradigm, which provides computing resources and services over the Internet. Due to immense development in services provided by cloud computing, the trend to share large-scale and confidential data on cloud has been increased. Though cloud computing provides many benefits, ensuring security of the data stored in cloud is the biggest challenge. The security concern about the data becomes main barrier for adoption of cloud. One of the important security aspects is fine grained access control mechanism. The most widely used and efficient access control scheme for cloud computing is Attribute Based Encryption (ABE). The Attribute Based Encryption (ABE) scheme provides a new technique for embedding access policies cryptographically into encryption process. The article presents an overview of various existing attribute-based encryption schemes and traditional access control models. Also, the comparison of existing ABE schemes for cloud computing, on basis of various criteria is presented in the article.

DOI: 10.4018/978-1-7998-7705-9.ch042

INTRODUCTION

In today's era, cloud computing has become an attracting technology, which has brought extreme changes to IT industry. Cloud Computing enables network access to various computing resources such as servers, storage, networks, applications and services. It is basically a paradigm that provides access to shared pool of resources online on demand (Armbrust et al., 2010). It is computing over internet. The users can store any amount of data on cloud and then can access it at any time, from anywhere. The most fascinating benefit of cloud computing is that it provides cost saving as the users will pay only for their usage. Cloud computing is also termed as distributed computing over a network. The term cloud can be defined as collection of servers delivering computing resources as a service on demand. Generally, the cloud comprises various interfaces, networks, hardware, storage devices etc. (Majumder et al., 2014).

Security is the biggest barrier for adoption of cloud computing. The data is present in shared environment, where other users can also access it. The users do not have complete control over the transit of data stored in cloud as both users and data are present in different domain. Hence the privacy concern arises for user's data and many users cannot completely trust the cloud environment. (KPMG, 2010; Hashizume et al., 2013, Tabassum et al., 2017). The security challenges can be faced at different levels such as architectural level, communication level and contractual and legal level (Ali et al., 2015). After adoption of cloud computing the organization cannot apply traditional security mechanism such as authentication, authorization in similar way as they exist. The reason is that the security requirements of organization with cloud environment are very much different than the traditional organization (Li and Ping, 2009).

Generally, in cloud environment users share their sensitive data with other users. In order to access the data, user must possess necessary permissions or credentials. Access control is a mechanism, which decides who can use a specific system, resource or application. It defines a way to allow, deny or restrict user access to system or its resources (Khan, 2012). Access control mechanism ensures that data must be accessed by authorized users only. In cloud environment, the owner of data and the data are present in different administrative domains. Thus, it is extremely important to ensure authorized access to data and manage user's identity. Due to the distributive and dynamic nature of cloud computing access control becomes very complex task. In traditional method the data is stored on some third-party server and access control mechanism is employed statically. However, this method does not guarantee the confidentiality of data because the server storing the data can be un-trusted entity. Therefore, providing better access control mechanism is a very important component of cloud security (Majumder et al., 2014). The main goal of access control is to restrict user to access what he/she should be able to do and prevent unauthorized access. The access control is defined as a mechanism to determine correct access to data by legitimate user depending on access privileges and permissions that are already defined in security policies (Younis et al., 2014). The major endeavor of this paper is to present brief overview of access control mechanisms used for cloud computing. Here, the classification of access control models applied for cloud computing that includes some traditional models and various Attribute Based Encryption schemes is elaborated.

The classification of access control models for cloud computing includes two categories as traditional models and the models based on cryptographic approaches. The taxonomy of access control models applied for cloud computing is depicted in Figure 1. The Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role based Access Control (RBAC) model come under traditional access control models.