Chapter 85
Access Control in Cloud Computing

Qianqian Zhao
Xidian University, China

Maode Ma
Nanyang Technological University, Singapore

Yuqing Zhang
Xidian University, China

Bingsheng He
Nanyang Technological University, Singapore

ABSTRACT

Data sharing as one of the most popular service applications in cloud computing has received wide attention, which makes the consumers achieve the shared contents whenever and wherever possible. However, the new paradigm of data sharing will also introduce some security issues while it provides much convenience. The data confidentiality, the privacy security, the user key accountability, and the efficiency are hindering its rapid expansion. An effective and secure access control mechanism is becoming one way to deal with this dilemma. In this chapter, the authors focus on presenting a detailed review on the existing access control mechanisms. Then, they explore some potential research issues for the further development of more comprehensive and secure access control schemes. Finally, the authors expect that the topic of access control in cloud computing will attract much more attention from academia and industry.

1. INTRODUCTION

Cloud Computing has emerged as a promising computing paradigm that has drawn extensive attention from both academia and industry recently. By combining a set of existing and new techniques from the research areas including Service-Oriented Architectures (SOA) and virtualization, cloud computing is regarded as a computing paradigm in which resources in the computing infrastructure are provided as a service over the Internet. The cloud computing provides a platform to cut costs and help the users to focus on their core business instead of being impeded by information technology (IT) obstacles.

Along with this new paradigm, many researchers are engaged in the design of the valuable service applications in cloud computing. Especially, the data storage service based cloud computing has reached an unprecedented development. Cloud storage allows data owners to host the data from their local computing systems to the cloud. First,
the cloud storage is a model of networked online storage where the data is stored in the virtualized pools of storage which are generally hosted by the third parties such as the storage service providers. Then, the service providers operate some large data centers for the data owners to purchase or lease storage capacity from them in a pay-as-you-go business model. The service providers, in the background, virtualize the resources according to the requirements of the customers and expose them as storage pools, which the customers themselves can use to store files or data objects. Physically, the resource may span across multiple servers. Finally, the cloud storage can provide a comparably low-cost, scalable, location independent platform for managing the users’ data, thus more and more data owners start to store their data in the cloud. By hosting their data in the cloud, data owners can avoid the initial investment of expensive infrastructure setup, large equipment, and daily maintenance costs. The data owners only need to pay for the space they actually use described by the cost-per-gigabyte-stored model. Another reason is that data owners can rely on the cloud to provide more reliable services, so that they can access data from anywhere in the world at any time. Individuals or small-sized companies usually do not have the resource to keep their servers as reliable as the cloud does. In a word, the significance of cloud storage is to provide the cloud users with the ample storage resources anywhere anytime at the cost of little investment on their own local servers.

However, this new paradigm of data storage service will introduce some security challenges. It is obvious that the data owners would worry their data be misused or accessed by the unauthorized users in the cloud storage system. Since the cloud storage service separates the roles of the data owners from the data service provider, the data owners cannot interact with the users directly to provide data access services. Therefore, the access control scheme will be an effective way to ensure the data security in the cloud storage. Traditional access control architectures usually assume that the data owners and the servers storing the data are in the same trusted domain, where the servers are fully entrusted as an omniscient reference monitor responsible for defining and enforcing the access control policies. Those existing methods usually delegate the data access control to a trusted server and let it be in charge of defining and enforcing access policies. However, the cloud servers cannot be fully trusted by the data owners because the cloud servers could be allowed to unauthorized users for the data access to make profits. Thus, the traditional server-based data access control mode is no longer suitable for the cloud storage systems. The design of the secure and effective access control mechanisms with the semi-trusted cloud servers will become demanding in the cloud storage systems.

In this book chapter, we mainly investigate the security issues of access control in cloud storage system and introduce some solutions to these security issues in detail. We hope that the topic of access control in cloud computing can attract much more attentions from the academia and industry. We first make a brief description about the definition or the background involved in this topic, which includes the following several aspects, cloud computing, cloud storage, the access control, the security issues and so on. Then, as the main contribution of this chapter, we explore the solutions to these security issues and make a detailed comparison among the existing schemes. In the end, we explore potential future research direction for the design of more secure and effective access control scheme for the cloud storage systems.

2. BACKGROUND

Cloud Computing

Cloud Computing is the result of evolution and adoption of existing computing technologies
Related Content

Ontology Mapping Validation: Dealing with an NP-Complete Problem
[www.igi-global.com/chapter/ontology-mapping-validation/72959?camid=4v1a](www.igi-global.com/chapter/ontology-mapping-validation/72959?camid=4v1a)

Class Level Test Case Generation in Object Oriented Software Testing
[www.igi-global.com/article/class-level-test-case-generation/2644?camid=4v1a](www.igi-global.com/article/class-level-test-case-generation/2644?camid=4v1a)

Semantic Web Adaptation
[www.igi-global.com/chapter/semantic-web-adaptation/37626?camid=4v1a](www.igi-global.com/chapter/semantic-web-adaptation/37626?camid=4v1a)

Adoption of Web Services in Digital Libraries: An Exploratory Study
[www.igi-global.com/chapter/adoption-web-services-digital-libraries/37680?camid=4v1a](www.igi-global.com/chapter/adoption-web-services-digital-libraries/37680?camid=4v1a)