Securing Data Storage By Extending Role-Based Access Control

Mamoon Rashid, Department of Computer Science Engineering, Ramgharia Institute of Engineering and Technology, Phagwara, Punjab, India
Er. Rishma Chawla, Department of Computer Science Engineering, Ramgharia Institute of Engineering and Technology, Phagwara, Punjab, India

ABSTRACT

Role-based access control (RBAC) models have generated a great interest in the security community as a powerful and generalized approach to security management and ability to model organizational structure and their capability to reduce administrative expenses. In this paper, the authors highlight the drawbacks of RBAC models in terms of access control and authorization and later provide a more viable extended-RBAC model, which enhances and extends its powers to make any Cloud Server more secure by adding valuable constraints. Later the Blobs are stored on cloud server which is then accessed by the end users via this Extended RBAC model. The authors describe a practical implementation of the proposed extended RBAC based architecture and discuss the performance results with its base models. The authors later show how the users with different premiums can access this architecture in a better way and also how the unknown users for this architecture can be denied the usage of services by adding valuable constraints.

Keywords: Architecture, Authorization, Blobs, Role-Based Access Control (RBAC), Server

1. INTRODUCTION

Cloud computing has begun to emerge as a hotspot in both industry and academia; It represents a new business model and computing paradigm, which enables on demand provisioning of computational and storage resources. Economic benefits consist of the main drive for cloud computing due to the fact that cloud computing offers an effective way to reduce capital expenditure and operational expenditure. The definition of cloud computing as per the literature in I. Foster (2009) is "A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet.”

DOI: 10.4018/ijcac.2013100103
The Cloud Security Alliance has summarized five essential characteristics (CSA, 2009) that illustrate the relation to, and differences from, traditional computing paradigm:

- **On-demand self-service:** A cloud customer may unilaterally obtain computing capabilities, like the usage of various servers and network storage, as on demand, without interacting with the cloud provider;

- **Broad network access:** Services are delivered across the Internet via a standard mechanism that allows customers to access the services through heterogeneous thin or thick client tools (e.g., PCs, mobile phones, and PDAs);

- **Resource pooling:** The cloud provider employs a multitenant model to serve multiple customers by pooling computing resources, which are different physical and virtual resources dynamically assigned or reassigned according to customer demand. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- **Rapid elasticity:** Capabilities may be rapidly and elastically provisioned in order to quickly scale out or rapidly released to quickly scale in. From customers’ point of view, the available capabilities should appear to be unlimited and have the ability to be purchased in any quantity at any time;

- **Measured service:** The service purchased by customers can be quantified and measured. For both the provider and customers, resource usage will be monitored, controlled, metered, and reported.

However authorization and access control has always been a fundamental security technique in systems like cloud computing in which multiple users share access to common resources. Authorization is the process of expressing security policies that determine whether a subject (e.g., process, computer, human user, etc.) is allowed to perform an operation (e.g., read, write, execute, delete, search, etc.) on an object (e.g., a tuple in a database, a table, a file, a service, and, more generally, any resource of the system). These policies define the subject’s permissions (rights to carry out an operation on an object) in a computer system. Access control is the process of enforcing these policies in order to achieve the desired level of security. Managing and administering the users’ privileges is one of the most challenging tasks in access control. Several access control models have been proposed, such as, discretionary and mandatory access control models (DAC and MAC), Clark-Wilson model, Lipner’s Integrity model, Chinese wall model, Task based models, and Role Based Access Control models and RBAC has further been extended up to some level. Among these models Role-based access control (RBAC) models have been receiving attention as they provide systematic access control security through a proven and increasingly predominant technology for commercial organizations. One of the main advantages of the RBAC over other access control models is the ease of its security administrations. RBAC models are policy neutral (R. Sandhu, 1996); they can support different authorization policies including mandatory and discretionary through the appropriate role configuration. In spite of the success of the RBAC, researchers have determined that there are still many application security requirements that are not addressed by the existing RBAC models (E. Bertino, 2001). In the past few years, several RBAC extensions have been proposed to address such security requirements (K. Devdatta, 2008; Z. Xinwen, 2003; S. Chakraborty, 2006; H. Shen, 2005; I. Ray, 2007; I. Ray, 2006). Although, these extensions geared and enhanced basic RBAC model, however we find some applications where individually these extended models fall short. We will uncover the loop-hole in existing extended RBAC model and later will add a mechanism to resolve such an issue.
Related Content

Analysis of State Dependent Vacation Queues with Threshold Gated Service Policy
www.igi-global.com/chapter/analysis-state-dependent-vacation-queues/64164?camid=4v1a

Environmental Turbulence and Complexity and the Optimal Degree of Internal Open Innovation for MNCs
www.igi-global.com/article/environmental-turbulence-and-complexity-and-the-optimal-degree-of-internal-open-innovation-for-mncs/100393?camid=4v1a
Managing Intellectual Capital in Non-Profit Elderly Care Organizations
www.igi-global.com/article/managing-intellectual-capital-non-profit/73030?camid=4v1a

Homomorphic Encryption as a Service for Outsourced Images in Mobile Cloud Computing Environment
www.igi-global.com/article/homomorphic-encryption-as-a-service-for-outsourced-images-in-mobile-cloud-computing-environment/179536?camid=4v1a