Chapter 3
Identity and Access Management in the Cloud Computing Environments

Manoj V. Thomas
National Institute of Technology Karnataka, India

K. Chandrasekaran
National Institute of Technology Karnataka, India

ABSTRACT

Nowadays, the issue of identity and access management (IAM) has become an important research topic in cloud computing. In the distributed computing environments like cloud computing, effective authentication and authorization are essential to make sure that unauthorized users do not access the resources, thereby ensuring the confidentiality, integrity, and availability of information hosted in the cloud environment. In this chapter, the authors discuss the issue of identity and access management in cloud computing, analyzing the work carried out by others in the area. Also, various issues in the current IAM scenario in cloud computing, such as authentication, authorization, access control models, identity life cycle management, cloud identity-as-a-service, federated identity management and also, the identity and access management in the inter-cloud environment are discussed. The authors conclude this chapter discussing a few research issues in the area of identity and access management in the cloud and inter-cloud environments.

INTRODUCTION

Even though cloud computing has become one of the most promising paradigms in the IT domain, many organizations and the enterprises are still reluctant to adopt the cloud for critical workloads or services because of the concern about the security of their personal data (King & Raja, 2012). Hence, managing user identities and their access in the cloud system is a critical problem to be solved effectively so that the cloud computing is safe and secure. Digital identity of a user represents who he is, and it is used to decide his access rights or privileges when he interacts with other users or accesses resources or services.
Identity and Access Management in the Cloud Computing Environments

The identity of a cloud user authorizes him to access data or resources from the cloud environment. When the users make requests to access the cloud resources and services, it is highly important that the identity and the access rights of the users are verified before granting the requested services.

An effective Identity and Access Management (IAM) mechanism is required to make the cloud computing platform trusted, secure, reliable and scalable. Normally, on-premise applications can rely on various on-premise identity infrastructure services such as Active Directory (Microsoft, 2009) and Lightweight Directory Access Protocol (Wahl et al., 1997) for verifying the user identity information. Similarly, an effective identity service in the cloud should solve this issue in the cloud environment. Identity and Access Management deals with the process of identifying entities in a computing system, and also managing access to the available resources in the system based on access rules or policies. In the cloud computing domain, the private data of the cloud customers are stored in the servers or the data centers of the CSPs; rather than keeping it on-premise on the user’s computer. Hence, the CSPs need to address the privacy concerns of the cloud users through proper IAM mechanisms so that the trust level of the cloud users in the Cloud Computing domain is increased. Proper identity management is the first step to be enforced in the cloud environment, in order to avoid unauthorized access of cloud resources.

In this chapter, the authors discuss the issue of identity and access management in the cloud and inter-cloud environments. The analysis of the work done by the researchers in this area shows the merits and demerits of various approaches. The various issues in the identity and access management in cloud computing, such as authentication, authorization, access control models, identity life cycle management are discussed. The authors explain the emerging concepts in identity management, such as the federated identity management, Single Sign-On (SSO) and cloud identity-as-a-service. Also, the various issues in the identity and access management in the inter-cloud (cloud federation) environment are discussed in this chapter. Finally, the authors conclude the chapter discussing a few research issues in the area of identity and access management in the cloud and inter-cloud environments.

BACKGROUND

In the Cloud Computing domain, an efficient IAM is essential for maintaining the confidentiality, integrity and availability of the data stored in the cloud. Generally, in the cloud environment, access control mechanism is required at each of the following layers (Alliance, 2011):

1. **Network Layer**: An access control mechanism at the network layer should not allow a user to see any system or a specified portion of a network (Ping, Route commands) in the cloud unless the access policies allow him to do so.
2. **System Layer**: A user should not be allowed to access any particular host or system in the cloud unless the access policies allow him to do so.
3. **Application Layer**: Access to the cloud applications or any functionality of the applications should be governed by the access control rules, and the access should be permitted after verifying the identities and attributes of a cloud user.
4. **Process Layer**: Access control policies and rules should be effectively used to define the processes or functions that a user is allowed to run within an application.