Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 170 – 174

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

Identity and Access Management as Security-as-a-Service from Clouds

Deepak H. Sharma[a] *, Dr. C. A. Dhote[b], Manish M. Potey[c]

[a]K. J. Somaiya College of Engineering, Vidyavihar, Mumbai – 400 077, India
[b]Department of Computer Science & Engineering, P. R. M. I. T & R, Amravati - 444701, India
[c]K. J. Somaiya College of Engineering, Vidyavihar, Mumbai – 400 077, India

Abstract

In Security-as-a-service model the focus is on security delivered as cloud services; i.e. security provided through the cloud instead of on premise security solutions. Identity and Access Management (IAM) focuses on authentication, authorization, administration of Identities and audit. Its primary concern is verification of identity of entity and grating correct level of access for resources which are protected in the cloud environment. The IAM implemented as the cloud service can benefit the user with all the advantages offered by Security-as-a-service (SECaaS). We have implemented a proof-of-concept (POC) of IAM-aaS which is also evaluated. The relevant standards and technologies are also discussed for providing secure access to cloud users.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Cloud Computing; Authentication; Authorization; Audit; Security Issues; Security-as-a-service

1. Introduction

Cloud computing is a nascent and rapidly evolving model, with new aspects and capabilities being added regularly by researchers around the world. Cloud computing has its roots in large-scale distributed computing technology. It is in fact an extension of grid computing, distributed computing, and parallel computing [1]. Nicholas Carr equates the rise of cloud computing in the information age to electrification in the industrial age. Carr argues that in the emerging future organizations will simply plug in to cloud (computing grid) for the computing resources they need [2].

* Corresponding author. Tel.: +91-22-66449191; fax: +91-22-21025272.
E-mail address: deepaksharma@somaiya.edu

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.117

Security-as-a-service model focuses on security delivered as cloud services; i.e. security provided through the cloud instead of on-premise security solutions. The security-as-a-service model enhances the functionality of existing on-premise implementations by working with them as part of hybrid solution. Identity and Access Management (IAM) consists of processes which are used to manage access to resources. This is done by verifying the identity of an entity, after verification of identity the access is granted at the appropriate level based on the policy of protected resource [3].

In this paper we propose the Identity and Access Management as a service (IAMaaS) framework. In particular this IAMaaS is an on-demand portable, and available pay-per-use cost model. The paper addresses various issues regarding security delivered as cloud service. This paper addresses the following issues in separate sections. Section 2 discusses the related work. Section 3 discusses architecture and scope of proof-of-concept (POC) of IAMaaS, in Section 4 the POC is evaluated and Section 5 concludes the paper and discusses future work.

2. Related Work

In Cloud Security Alliance (CSA) SECaaS defined category of service [4], the core functionalities of Identity and Access Management are defined as account provisioning/deprovisioning, authentication, authorization, policy management, role based access and federated single sign on.

In CSA SECaaS Implementation guidance [5], the IAM components include:

- Centralized Directory Services,
- Access Management Services,
- Identity Management Services,
- Identity Federation Services,
- Role-Based Access Control Services,
- User Access Certification Services,
- Privileged User and Access Management,
- Separation of Duties Services, and
- Identity and Access Reporting Services.

In [6] the authors have spelled out specific requirements of IAM, viz. User management, Authentication, Authorization, Monitoring and Auditing. The authors have also proposed Identity management as a service (IDaaS). Here the authentication is delegated to identity management service. The advantages discussed are reduced complexity of different Cloud service providers supporting different federation standards, minimal architectural changes from user’s point of view to support this model.

In [7] the authors have proposed user-centric trust Identity service with an aim to create trust among Cloud Service Providers (CSP). Their model has Authentication, Authorization, and Provisioning and Audit modules along with the Trust agent. The federated environment will allow users to login to various Cloud Service Providers depending on the application access. When the user moves to different CSP the user credentials follow in the federated environment. The Trust Agent in the Identity Management sends the Trust Token along with the user attribute which creates a trust between CSPs.

In [8] the authors have propose an Identity and Access Management architecture in cloud to achieve security requirement like Strong Authentication, Data Loss Prevention, Security as a Service. The various systems components for addressing the above security requirements are Cloud Resource provider, Identity Management, Policy Management, Resource Engine and Access Decision-making. The various advantages of their approach were Comprehensive identity management, standardized architecture, and scalable design.