Engineering Science and Technology, an International Journal xxx (2018) xxx–xxx

HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

journal homepage: www.elsevier.com/locate/jestch

Review

Identity and access management in cloud environment: Mechanisms and challenges

I. Indu [a], P.M. Rubesh Anand [a,*], Vidhyacharan Bhaskar [b]

[a] Department of Electronics and Communication Engineering, Hindustan University, Chennai 603103, India
[b] Department of Electrical and Computer Engineering, San Francisco State University, 1600 Holloway Avenue, San Francisco, CA 94132, USA

ARTICLE INFO

Article history:
Received 1 December 2017
Revised 22 March 2018
Accepted 14 May 2018
Available online xxxx

Keywords:
Access management
Authentication
Authorization
Cloud computing
Security
Web services

ABSTRACT

Cloud computing is a complex system with combination of diverse networked devices that supports demanded services. The architecture of cloud computing consists of different kinds of configurable distributed systems with a wide variety of connectivity and usage. The organizations are adapting to cloud networks at a rapid pace due to the benefits like cost-effectiveness, scalability, reliability and flexibility. Though the primary merits of cloud computing are promising facts, cloud networks are vulnerable to various kinds of network attacks and privacy issues. The features like multi tenancy and the third party managed infrastructure in cloud environment necessitates the requirement of identity and access management mechanism. The problems involved in secure access to cloud resources have been addressed by many academicians and industry personnel. In this paper, the issues related to authentication, access management, security and services in cloud environment are surveyed along with the techniques proposed to overcome the same. A detailed comparative study of the existing techniques in the perspective of cloud service providers and cloud users that include identity and access management, security issues and services in the cloud environment are highlighted.

Contents

1. Introduction . . . 00
2. Authentication mechanisms . . . 00
  2.1. Physical security mechanisms . . . 00
  2.2. Digital security mechanisms . . . 00
    2.2.1. Credentials and secure Shell keys . . . 00
    2.2.2. Multifactor authentication . . . 00
    2.2.3. Chip & PIN . . . 00
  2.3. SSO & federation . . . 00
    2.3.1. Enterprise SSO . . . 00
    2.3.2. OpenID . . . 00
    2.3.3. OAuth . . . 00
    2.3.4. SAML . . . 00
3. Authorization mechanisms . . . 00
  3.1. Access control mechanisms . . . 00
    3.1.1. Mandatory access control . . . 00
    3.1.2. Discretionary access control . . . 00
    3.1.3. Entitlement/Task based access control . . . 00
    3.1.4. Role based access control . . . 00
    3.1.5. Attribute based access control . . . 00

* Corresponding author.
E-mail address: rubesh.anand@gmail.com (P.M.R. Anand).
Peer review under responsibility of Karabuk University.

https://doi.org/10.1016/j.jestch.2018.05.010
2215-0986/

Please cite this article in press as: I. Indu et al., Identity and access management in cloud environment: Mechanisms and challenges, Eng. Sci. Tech., Int. J. (2018), https://doi.org/10.1016/j.jestch.2018.05.010

3.2. Access control governance . . . 00
3.2.1. Certification & risk score . . . 00
3.2.2. Life cycle management . . . 00
3.2.3. Segregation of duties . . . 00
4. Identity & access management systems . . . 00
5. Security threats in cloud environment . . . 00
5.1. Threats in cloud infrastructure . . . 00
5.1.1. Data security . . . 00
5.1.2. Virus or malware . . . 00
5.1.3. Availability of resources . . . 00
5.1.4. Virtual Machine & Multitenancy . . . 00
5.1.5. Apts and malicious outsiders . . . 00
5.2. Threats in cloud services . . . 00
5.2.1. Protocols and standards . . . 00
5.2.2. Cloud web services . . . 00
5.2.3. Web technologies . . . 00
5.2.4. Availability of services . . . 00
6. Security analysis in cloud environment . . . 00
6.1. Man-in-the-Middle (MITM) attacks . . . 00
6.2. Insider attacks . . . 00
6.3. Password/Key compromise . . . 00
6.4. Replay attacks . . . 00
6.5. Session/Cookie hijacking . . . 00
6.6. Guessing attacks . . . 00
6.7. Denial-of-Service attacks (DoS/DDoS) . . . 00
7. Recommendations and best practices . . . 00
8. Conclusions . . . 00
Acknowledgements . . . 00
References . . . 00

1. Introduction

Cloud computing is a combination of different configurable computing resources like networks, servers, storages, services, applications that help in providing convenient and on-demand access to the cloud users [1]. Cloud computing is largely mentioned by people and is currently used in many commercial fields. Cloud service providers (CSPs) are responsible for identity and other kinds of management in cloud environment. However, a large number of data leakage incidents are caused due to the vulnerabilities in identity management systems [2]. Identity and access management (IAM) in cloud environment is a crucial concern for the acceptance of cloud-based services. Presently, the mechanism of identity management is mainly CSP-centered, which hardly meets the requirement of users' flexible and fine-grained access control policy.

The cloud environment is generally classified as Private Cloud, Public Cloud and Hybrid/Federated Clouds. A private cloud is designed and dedicated to the needs of a specific organization. In a public cloud environment, infrastructure support to multiple organizations is facilitated and managed by third party provider. Public cloud model is also known as multi-tenant environment which shares the resources among the organizations to bring down the overall service cost. Hybrid or Federated cloud infrastructure is a mix of on-premises, private and public cloud services. Another concept in cloud infrastructure is multi-provider clouds which is an environment that relies on multiple clouds providers and divides the work load among the cloud environment. There are also different cloud environments which is specifically designed to support the service like Internet of Things (IoT) cloud services which are specifically designed to handle and analyse the data from IoT devices and mobile cloud services which uses cloud computing to deliver applications to mobile devices.

Cloud computing is commonly divided into three primary cloud service models, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Cloud is based on service-oriented architecture which has the capability of providing Database-as-a-service (DbaaS), Identity-as-a-service (IDaaS) and Anything-as-a-Service (XaaS) [3]. Cloud computing provides a better way of handling resources in both industry and academia. Cloud system is vibrant in nature by considering numerous users, devices, networks, organizations, and resources that are frequently connected and disconnected to the system. The best option for the cloud service model that has to be implemented is determined through a number of factors. The important factors that are to be considered are flexibility, scalability, interoperability, and control of service [4]. Cloud computing requires extensive authentication and authorization mechanism to secure its data and resources due to the complexity of usage. Lack of efficient mechanism creates multiple challenges in cloud environment which include identity management, risk management, trust management, compliance, data security, privacy, transparency, and data leakage [5]. Another facet of cloud systems is complexity and their associated security challenges. The loss of control and transparency issues are also created while storing and processing user information by Cloud Service Providers (CSPs), or outside the organizational boundaries. Due to these distinctive security challenges, the cloud environment adoption is slow regardless of the assured and attractive features of the cloud. In spite of the aforesaid problems, the organization has a tendency of reluctance in contributing their critical identity information to the cloud [6].

In a cloud system, the storage and processing of data is performed by organizations or with the help of third party vendors. The service provider has to ensure that data and applications stored in cloud are protected as well as the infrastructure is in secure environment. Further, users need to verify that their credentials for authentication is secure [7]. There are many security issues that compromise data in the process of data access and storage in the cloud environment, especially in the case of data storage with the help of third party vendors who themselves may be a malicious attacker. Though standards and best practices are available for overcoming such security problems, cloud service

Please cite this article in press as: I. Indu et al., Identity and access management in cloud environment: Mechanisms and challenges, Eng. Sci. Tech., Int. J. (2018), https://doi.org/10.1016/j.jestch.2018.05.010