Applied Computing and Informatics (2017) 13, 57–65

Saudi Computer Society, King Saud University

Applied Computing and Informatics

(http://computer.org.sa)
www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

Multilevel classification of security concerns in cloud computing

Syed Asad Hussain [a,*], Mehwish Fatima [a], Atif Saeed [b], Imran Raza [a], Raja Khurram Shahzad [c]

[a] Department of Computer Science, COMSATS Institute of Information Technology Lahore, Pakistan
[b] School of Computing and Communications, Lancaster University, Lancaster, United Kingdom
[c] School of Computing, Blekinge Institute of Technology, Sweden

Received 11 May 2015; revised 11 March 2016; accepted 20 March 2016
Available online 8 April 2016

KEYWORDS

Cloud computing;
Security;
Virtualization;
SaaS;
PaaS;
IaaS

Abstract Threats jeopardize some basic security requirements in a cloud. These threats generally constitute privacy breach, data leakage and unauthorized data access at different cloud layers. This paper presents a novel multilevel classification model of different security attacks across different cloud services at each layer. It also identifies attack types and risk levels associated with different cloud services at these layers. The risks are ranked as low, medium and high. The intensity of these risk levels depends upon the position of cloud layers. The attacks get more severe for lower layers where infrastructure and platform are involved. The intensity of these risk levels is also associated with security requirements of data encryption, multi-tenancy, data privacy, authentication and authorization for different cloud services. The multilevel classification model leads to the provision of dynamic security contract for each cloud layer that dynamically decides about security requirements for cloud consumer and provider.

1. Introduction

Cloud computing is a broad paradigm based on models for providing services of storage and platform software. Cloud computing concept has emerged from distributed and grid computing domains that are already in use for mail servers, web storage and hosting services. Cloud computing, as defined by NIST, is referred to as: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].

* Corresponding author.
E-mail addresses: asadhussain@ciitlahore.edu.pk (S.A. Hussain), mehwish.fatima@ciitlahore.edu.pk (M. Fatima), a.saeed2@lancs.ac.uk (A. Saeed), iraza@ciitlahore.edu.pk (I. Raza), khurram.shahzad@bth.se (R.K. Shahzad).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.aci.2016.03.001

In cloud computing, clouds can be described at different layers, i.e., SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). Although applications for clouds are in development phase, however security requirements for the data and services on the clouds are getting attention of researchers and it has become necessary to consider each layer of a cloud for possible attacks. It is worth noting that cloud computing systems have many advantages; however, large organizations are still hesitant to shift their setups on the cloud mainly due to security issues and risks. Thus, it is important to address the security issues and problems in cloud systems, and to find a solution for the widespread acceptance of these solutions. However, being a new domain, the research on the requirements and issues regarding security of clouds is still in its early stages.

In the literature, there are different classifications of cloud security attacks [2–7] targeting a specific cloud service or a particular kind of the cloud system. Thus there is a need for a more comprehensive classification of security attacks across versatile cloud services at each layer. This paper proposes a multilevel classification of security attacks for different cloud services and their associated risks at cloud layers. It also discusses provision of dynamic security contract for each cloud layer that dynamically decides about security requirements for cloud consumer and provider.

The rest of paper is structured as follows: Section 2 consists of related work. Section 3 presents the proposed multilevel classification of security concerns in cloud computing. Section 4 is based on the dynamic security contract concept. Section 5 concludes the paper.

2. Related work

The application softwares at SaaS are provided with a specific license based subscription, pay-as-go [8]. Platform as a Service (PaaS) caters services for operating system, network capacity, storage and multi-tenancy via the Internet. Infrastructure as a service (IaaS) provides utility computing, automation of administrative tasks, dynamic scaling, desktop virtualization, policy-based services, and Internet connectivity. IaaS provides virtual servers with unique IP address and storage pool as required by customers. The concept of infrastructure and hardware layer is mentioned by different researchers. Some authors have suggested that the infrastructure layer offers system software services and hardware layer provides hardware-based services. Infrastructure and hardware layers may be combined due to intrinsic relationship between hardware and software.

In [9], security aspects of one of the popular cloud Amazon Elastic Compute Cloud (EC2) have been discussed. It consists of systematic analysis of various crucial vulnerabilities in publicly available Amazon Machine Images (AMIs) and mechanisms to eliminate them. The proposed tool referred to as Amazon Image Attacks (AmazonIA) uses only publicly available interfaces regardless of the underlying cloud infrastructure. As a result of exploiting vulnerabilities and successful attacks, authors are able to extract sensitive information including passwords, and credentials from AMIs. The extracted information can be used to initiate botnets, or create back doors to launch impersonate attacks or access source code of a web service available on AMI. The authors have discussed effects of successful attacks and also the methods to mitigate those attacks. Some research groups have worked on the interfaces of both public and private clouds [10]. The public cloud under their consideration is Amazon, while the private cloud is Eucalyptus.

Authors in [11] consider security as a service for cloud-based applications. The architecture considers the existing services at different levels. It considers user-centric security i.e., users have control over their security permitting them to use security solutions across different clouds. They can subscribe to any security solution provided by any cloud provider and use that particular security solution for their cloud and may also have multiple security solutions for a particular service depending upon its criticality. The multiple security solutions can also be used at different levels.

Authors in [9] address the security and privacy aspects of real-life cloud deployments, while ignoring the malicious cloud providers or customers. Here authors' focus is Amazon Elastic Compute Cloud (EC2). They have analyzed the crucial vulnerabilities of Amazon Machine Images (AMIs) through an automated tool and as a result of attack information regarding API Keys, private keys and credentials of publishers were extracted [9]. Vulnerabilities were discovered in Secure Shell. The extracted information can be further used to create multiple security threats resulting in botnet instances, access of backend services or code of the Web sites through back-doors content.

In [12] authors suggest that security should be provided as a service and propose a model for security as service. Security as a service implies that the security applications and services can be provided by a cloud vendor, or cloud consumer or even by a third trust-worthy party. The security service can be in the form of a cloud-based infrastructure or software. The authors have proposed a component based software model in which authorization components can be developed by any party regardless of being a service provider. An eXtensible access control markup language (XACML) decision engine that is composed of a context handler, a policy decision point and a policy administration point, can be furnished by reusable components to augment the security service. By XACML standard attributes of subjects, resources and environments and authorization rules can be defined as Boolean expressions. Thus, these types of security services, which can be managed and altered by cloud customers, are helpful to build trust of cloud customers on cloud systems.

In [3] Cloud Computing Open Architecture (CCOA) concept is discussed for clouds in virtual environments. The role and functions of the architecture are discussed according to different infrastructures for IT and business systems. Different types of architectures complicate security management for cloud systems. This architecture provides a solution for different security aspects regarding virtual environments. The authors suggest physical and logical isolation of data instances for each customer to enhance the data privacy and expeditious replication and recovery system. Authorized users based on the role-based access control can access the sensitive data on platforms. To prevent intrusion attacks, cloud service provider blocks the malicious and un-trusted codes enabling digital forensic applications.

Research in [14] suggests a trusted computing and attestation system for virtual environments. In virtual environments systems are more prone to threats due to the poor computer communication architectures and hidden network channels. These hidden channels can be a risk since many virtualized network channels can be easily observed and hacked.