Chapter 1
An Abstract Model for Integrated Intrusion Detection and Severity Analysis for Clouds

Junaid Arshad
University of Leeds, UK

Paul Townend
University of Leeds, UK

Jie Xu
University of Leeds, UK

ABSTRACT

Cloud computing is an emerging computing paradigm which introduces novel opportunities to establish large scale, flexible computing infrastructures. However, security underpins extensive adoption of Cloud computing. This paper presents efforts to address one of the significant issues with respect to security of Clouds i.e. intrusion detection and severity analysis. An abstract model for integrated intrusion detection and severity analysis for Clouds is proposed to facilitate minimal intrusion response time while preserving the overall security of the Cloud infrastructures. In order to assess the effectiveness of the proposed model, detailed architectural evaluation using Architectural Trade-off Analysis Model (ATAM) is used. A set of recommendations which can be used as a set of best practice guidelines while implementing the proposed architecture is discussed.

1. INTRODUCTION

The advent of internet technologies has significantly changed the methods used in e-Science along with the emergence of new computing paradigms to facilitate e-Science research. Cloud computing is one of such emerging paradigms which makes use of the contemporary virtual machine technology. The collaboration between internet and virtual machine technologies enable Cloud computing to emerge as a paradigm with promising prospects to facilitate the development of large scale, flexible computing infrastructures, available on-demand to meet the computational

DOI: 10.4018/978-1-4666-1879-4.ch001

requirements of e-Science applications. Cloud computing has witnessed widespread acceptance mainly due to compelling characteristics such as; Live Migration, Isolation, Customization and Portability, thereby increasing the value attached with such infrastructures. The virtual machine technology has profound role in it. Amazon, Google and GoGrid (2010) represent some of commercial Cloud computing initiatives whereas Nimbus and OpenNebula represent academic efforts to establish a Cloud.

Cloud computing has been defined in different ways by different sources however, for the purpose of research described in this paper, we define Clouds as a high performance computing infrastructure based on system virtual machines to provide on-demand resource provision according to the service level agreements established between a consumer and a resource provider.

A Cloud computing system representing the above definition has been presented in Figure 1. A system virtual machine, as described in this definition, serves as the fundamental unit for the realization of a Cloud infrastructure and emulates a complete and independent operating environment. Within the scope of this paper, we define the cloud platforms focused at satisfying computation requirements of compute intensive workloads as *Compute Clouds* whereas those facilitating large scale data storage as *Storage or Data Clouds.* For the rest of this paper, we use terms *Cloud computing* and *Clouds* interchangeably to refer to our definition of compute clouds. As described in the above definition, Cloud computing involves on-demand provision of virtualized resources based on Service Level Agreements (SLA) thereby facilitating the user to acquire resources at runtime by defining the specifications of the resource required (Burchard, Hovestadt, Kao, Keller, & Linnert, 2004). The user and the resource provider are expected to negotiate the terms and conditions of the resource usage through SLAs so as to protect the quality of service being committed at resource acquisition stage.

As with any other technology, different models of Cloud computing have been proposed to

Figure 1. A Cloud computing system