

# 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.*

*Keywords:* Architectural Evaluation, Cloud Computing, Intrusion Detection, Intrusion Severity Analysis, Virtual Machines

---

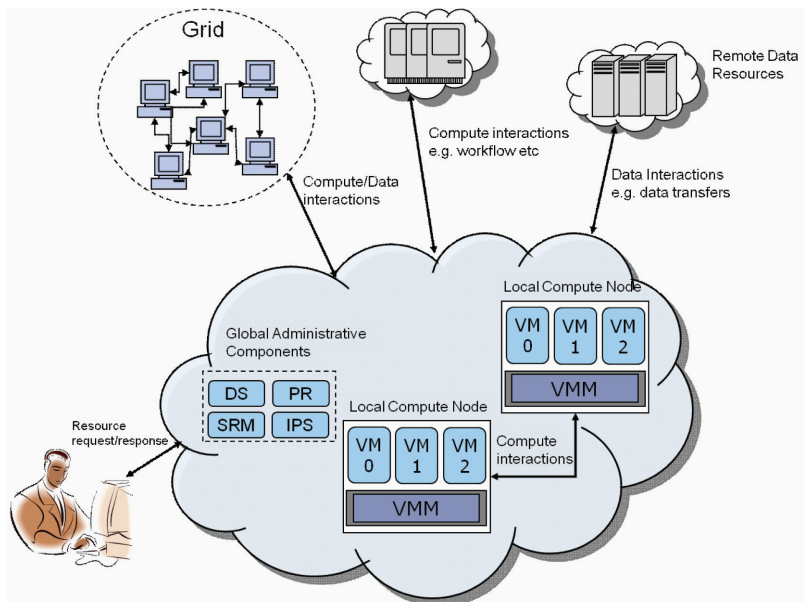
## 1. INTRODUCTION

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 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.

DOI: 10.4018/ijcac.2011010101

Figure 1. A Cloud computing system



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 harvest its benefits. These are *Infrastructure as a Service (IaaS)*, *Software as a Service (SaaS)* and *Platform as a Service (PaaS)*. Each of these models is focused at achieving specific objectives by introducing novel mechanisms at respective layers of the modern software architecture (Arshad, Townend, Xu, & Wei, 2010). With regards to these models, the Cloud computing system presented in Figure 1 resembles IaaS and therefore, inherits the characteristics of this model of Clouds. In the remaining sec-

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/article/abstract-model-integrated-intrusion-detection/53139](http://www.igi-global.com/article/abstract-model-integrated-intrusion-detection/53139)

## Related Content

---

### Fault Tolerant and Optimal Task Clustering for Scientific Workflow in Cloud

Nagaraj V. Dharwadkar, Shivananda R. Poojaraand Priyanka M. Kadam (2018).

*International Journal of Cloud Applications and Computing* (pp. 1-19).

[www.irma-international.org/article/fault-tolerant-and-optimal-task-clustering-for-scientific-workflow-in-cloud/207838](http://www.irma-international.org/article/fault-tolerant-and-optimal-task-clustering-for-scientific-workflow-in-cloud/207838)

### Automating Corporate Strategy: How Cloud AI Transforms Managerial Intelligence

Himanshi Rajora, Dilshad Jefferyand Azadeh Amoozegar (2026). *Automating Intelligence With Cloud-Native AI Tools* (pp. 183-196).

*Automating Intelligence With Cloud-Native AI Tools* (pp. 183-196).

[www.irma-international.org/chapter/automating-corporate-strategy/402679](http://www.irma-international.org/chapter/automating-corporate-strategy/402679)

### A Bounded Health Information Technology System Design Approach to Support Community-Based Care Delivery

Liam Peyton, Jaspreet Bindra, Aladdin Baarah, Austin Chamneyand Craig Kuziemsky (2015). *International Journal of Cloud Applications and Computing* (pp. 32-45).

[www.irma-international.org/article/a-bounded-health-information-technology-system-design-approach-to-support-community-based-care-delivery/124841](http://www.irma-international.org/article/a-bounded-health-information-technology-system-design-approach-to-support-community-based-care-delivery/124841)

### Towards the Development of Vehicular Ad-Hoc Networks (VANETs): Challenges and Applications

Mekelleche Fatihaand Haffaf Hafid (2020). *IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks* (pp. 21-47).

[www.irma-international.org/chapter/towards-the-development-of-vehicular-ad-hoc-networks-vanets/252285](http://www.irma-international.org/chapter/towards-the-development-of-vehicular-ad-hoc-networks-vanets/252285)

### An Analytical Study of Cloud Computing Fundamentals and Applications

Pallab Banerjee, Ahmad Faraz, Mohit Kumarand Dipra Mitra (2026). *Digital Watermarking in Cloud Environments For Copyright Protection* (pp. 327-354).

[www.irma-international.org/chapter/an-analytical-study-of-cloud-computing-fundamentals-and-applications/388668](http://www.irma-international.org/chapter/an-analytical-study-of-cloud-computing-fundamentals-and-applications/388668)