A Framework for Intrusion Tolerance in Cloud Computing

Vishal M. Karande and Alwyn R. Pais

Information Security Lab, Dept. of Computer Science and Engineering,
National Institute of Technology Karnataka, Surathkal, India - 575025
{vishalmkarande,alwyn.pais}@gmail.com

Abstract. Cloud Computing has been envisioned as the next generation architecture and one of the fastest growing segments of the IT enterprises. No matter how much investment is made in cloud intrusion detection and prevention, cloud infrastructure remains vulnerable to attacks. Intrusion Tolerance in Cloud Computing is a fault tolerant design approach to defend cloud infrastructure against malicious attacks. Thus to ensure dependability we present a framework by mapping available Malicious and Accidental Fault Tolerance for Internet Applications (MAFTIA) intrusion tolerance framework for dependencies such as availability, authenticity, reliability, integrity, maintainability and safety against new Cloud Computing environment. The proposed framework has been validated by integrating Intrusion Tolerance via Threshold Cryptography (ITTC) mechanism in the simulated cloud environment. Performance analysis of the proposed framework is also done.

Keywords: Cloud Computing, Framework,Intrusion Tolerance, Security, and Threshold Cryptography.

1 Introduction

Experience shows that attacks may never be completely prevented or detected accurately and on time. Thus Intrusion Tolerance combining the aspects of protection, detection and reaction is currently considered to be the optimal way to address information security challenges [1]. However, the architecture of intrusion-tolerant systems, integrating multiple layers of defenses, redundancy and diversity is often considered to be costly and heavy weight to provision it dynamically. At the same time, the information technology landscape has been evolving continuously with the introduction of new software technology Cloud Computing.

Cloud computing provides simple, on-demand access to pools of highly elastic computing resources. Cloud Computing delivers software, platform and infrastructure as subscription-based services to its user in a pay-as-you-go model. These services are referred to as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) wherein resources are provided as a service over a network. Corporations and individuals are concerned about

A. Abraham et al. (Eds.): ACC 2011, Part IV, CCIS 193, pp. 386–395, 2011.

how security and compliance integrity can be maintained in this new rapidly evolving cloud computing environment. Even more concerning, though, is the corporations that are jumping to cloud computing while being oblivious to the implications of putting critical applications and data in the cloud. So cloud computing environment should be secure enough in maintaining cloud users trust level as small intrusion can cause a huge loss to both cloud users as well as cloud service executives [10]. Cloud computing being new and evolving rapidly, intrusions causing damage to its functional and operational units should be taken care of in their early stages of development.

In this paper we present a framework for intrusion tolerance in cloud computing environment which summarizes how a number of defenses and security techniques, especially those providing availability, integrity and confidentiality can possibly be integrated in the cloud or within its services. We have studied the MAFTIA intrusion tolerance framework. This existing framework for intrusion tolerance does not account for essential characteristics of cloud computing, such as scalability, elasticity, ubiquitous access, computer virtualization, relative consistency, commodity, reliability. The new framework is obtained by mapping available intrusion tolerance framework for dependencies such as availability, authenticity, reliability, integrity, maintainability and safety against new cloud computing environment wherein for each component we provide requirement, design description (architecture, specification), reasoning and evidence (why description meets the requirement under assumptions). The framework serves as an excellent platform for making cloud services intrusion tolerant. To test the feasibility of the proposed framework a Cloud Computing environment is simulated using CloudSim [12] toolkit, and using Intrusion Tolerance via Threshold Cryptography (ITTC) [7] mechanism cloud's Infrastructure as a service (IaaS) is made intrusion tolerant. Performance of the new simulated service model is measured using various performance metrics such as total execution time, intrusion detection time, recovery time, number of cloudlets etc.

The rest of the paper includes following structure, Section 2 provides a brief summary of the related work in this area. In section 3, we propose our framework. Section 4 gives the validation of our proposed framework and the paper concludes in Section 5.

2 Related Work

A dependable system is defined as one that is able to deliver a service that can justifiably be trusted [1]. Attributes of dependability include availability (readiness for correct service), reliability (continuity of correct service), confidentiality (prevention of unauthorized disclosure of information), and integrity (the absence of improper system state alterations). An intrusion-tolerant system is a system that is capable of self diagnosis, repair, and reconfiguration while continuing to provide a correct service to legitimate users in the presence of intrusions.