Chapter 25
Controlled Intelligent Agents' Security Model for Multi-Tenant Cloud Computing Infrastructures

Howard Hamilton
Florida Atlantic University, USA

Hadi Alasti
Indiana University-Purdue University, USA

ABSTRACT

Data security in the cloud continues to be a huge concern. The adoption of cloud services continues to increase with more businesses transitioning from on premise technology infrastructures to outsourcing cloud-based infrastructures. As the cloud becomes more popular, users are increasingly demanding control over critical security elements of the data and technology assets that are in the cloud. In addition, there are still cries for greater data and security in the cloud. The goal of this paper is to provide cloud service users with greater control over data security in the cloud while at the same time optimizing overall security in the multi-tenant cloud computing environment. This paper introduces cloud-based intelligent agents that are configurable by the users and are expected to give greater compliance for data security in any of the cloud service models.

INTRODUCTION

The importance of cloud computing as a salient way to provide service and data storage over the Internet is ever increasing (Varadharajan & Tupakula, 2014). Yet, security is a challenging issue in cloud computing against different types of malicious access and attacks. These security issues continue to present huge concerns as more users seek to utilize cloud computing initiatives.

Cloud computing continues to be a revolutionary disruptive technological innovation (Huang, 2012). As more businesses seek to adopt the cloud computing paradigm, the security of the cloud continues

DOI: 10.4018/978-1-5225-5634-3.ch025

to surface as a major challenge. The ever-growing demand to host and process data in the cloud has changed cloud computing to a vital technology. As the number of clients increase and the operating systems become more complex, the vulnerability also increases exponentially and security becomes more critical (Varadharajan & Tupakula, 2014). Although many organizations rate security as a critical issue in moving to the cloud, few know what to do about it (Peterson, 2010).

Companies are still contending with the lack of control over security activities and services in the cloud. Some users require greater controls so that they can defend their compliance status in regulatory matters. Government, healthcare, and finance organizations that need to conform to regulatory and strict security policies are challenged with the lack of hands-on control over major parts of the security administration in the cloud. To overcome this problem, cloud intelligent agents (CIA) were proposed by Hamilton and Alasti (2016). These agents are expected to operate differently from traditional software agents and are able to obtain and communicate intelligence, in a better way. The model that was proposed by Hamilton and Alasti has agents that are able to gather allowed security intelligence from its environment, share with other agents, communicate with agents in the user environment, replenish or retire agents when necessary, and even retire themselves to protect the environment that they are safeguarding.

In this paper, the CIA monitors the data processing and tracks, records and manages the access to data and other resources in the cloud. The CIA monitors the flow of incoming and outgoing data from and to the software, platform or infrastructure to improve integrity and availability. It may also dynamically cipher the data as an additional protection step for improvement of confidentiality.

MOTIVATION AND PROBLEM STATEMENT

One of the concerns of cloud computing by many information systems and network administrators is that they lose control over security in the cloud. It seems that more business users would be willing to adopt cloud computing for regular non-critical and essential applications, if they had more control over the security of the applications, infrastructure and data that will be pushed to the cloud.

Current security measures for cloud computing include encryption, physical security, and other general network and information security. These measures are usually solely implemented in the cloud and do not necessarily give the cloud user any control over how they are implemented and executed. Users seem to be demanding cloud service security that offer them some control over how the security is implemented and executed. This could further improve the adoption of cloud computing services and reduce the uncertainties of business users willing to run critical applications in the cloud.

CLOUD INTELLIGENT AGENTS

The CIAs are software agents that are deployed in the cloud and on users or hosts computers and networks. The difference with the agents presented in this paper is that they will have the ability to learn, reproduce, retire and provide intelligence to other agents. The CIAs will work in groups and can be controlled by cloud service users (CSUs). The CSUs can provide the parameters required to initiate the agents and determine when and how they are retired during the service.

Agent-based cloud computing involves the coordination, negotiation, and cooperation of cloud computing systems that automate the activities that are being executed within the cloud (Sim, 2012).