Chapter 3
A Review of Intrusion Detection Systems in Cloud Computing

Chiba Zouhair
Hassan II University of Casablanca, Morocco

Noreddine Abghour
Hassan II University of Casablanca, Morocco

Khalid Moussaid
Hassan II University of Casablanca, Morocco

Amina El Omri
Hassan II University of Casablanca, Morocco

Mohamed Rida
Hassan II University of Casablanca, Morocco

ABSTRACT

Security is a major challenge faced by cloud computing (CC) due to its open and distributed architecture. Hence, it is vulnerable and prone to intrusions that affect confidentiality, availability, and integrity of cloud resources and offered services. Intrusion detection system (IDS) has become the most commonly used component of computer system security and compliance practices that defends cloud environment from various kinds of threats and attacks. This chapter presents the cloud architecture, an overview of different intrusions in the cloud, the challenges and essential characteristics of cloud-based IDS (CIDS), and detection techniques used by CIDS and their types. Then, the authors analyze 24 pertinent CIDS with respect to their various types, positioning, detection time, and data source. The analysis also gives the strength of each system and limitations in order to evaluate whether they carry out the security requirements of CC environment or not.

DOI: 10.4018/978-1-5225-8176-5.ch003

INTRODUCTION

Cloud computing (CC) is rapidly growing computational model in today's IT world. It delivers convenient, on-demand network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, applications, etc.), "as service" on the Internet for satisfying computing demand of users (National Institute of Standards and Technology [NIST], 2011). It has three basic abstraction layers i.e. system layer (which is a virtual machine abstraction of a server), the platform layer (a virtualized operating system of a server) and application layer (that includes web applications). The characteristics of CC include:

- **Virtual:** Physical location and underlying infrastructure details are transparent to users.
- **Scalable:** Able to break complex workloads into pieces to be served across an incrementally expandable infrastructure.
- **Efficient:** Services Oriented Architecture for dynamic provisioning of shared compute resources. (Bakshi & Dujodwala, 2010).
- **Flexible:** Can serve a variety of workload types (consumer and commercial).

Cloud computing has also three service models namely Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models. IaaS model delivers services to users by maintaining large infrastructures like hosting servers, managing networks and other resources for clients. In PaaS, it offers development and deployment tools, languages and APIs used to build, deploy and run applications in the cloud, and in SaaS, systems offer complete online applications that can be directly executed by their users, making them worry free of installing and running software services on its own machines.

Threat Model for Cloud

Due to lack of control over the Cloud software, platform and/or infrastructure, several researchers stated that security is a major challenge in the Cloud (Aljawarneh, 2011). A recent survey performed by Cloud Security Alliance (CSA) and IEEE, indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers (Jouini & Ben Arfa Rabai, 2014). One of major security issues in Cloud is to detect and prevent network intrusions since the network is the backbone of Cloud, and hence vulnerabilities in network directly affect the security of Cloud. Martin from Cyber Security division stated that main concern after data security is an intrusion detection and prevention in the Cloud (Martin, 2010).

There are principally two types of threats; insider (attackers within a Cloud network) and outsider (attackers outside the Cloud network) considered in Cloud Network (Chiba, Abghour, Moussaid, El omri, & Rida, 2016).

- **Insider Attackers:** Authorized Cloud users may attempt to gain (and misuse) unauthorized privileges. Insiders may commit frauds and disclose information to other (or modify information intentionally). This poses a serious trust issue. For example, an internal DoS attack demonstrated against the Amazon Elastic Computer Cloud (EC2) (Macro, 2009).