Review on State of Art Intrusion Detection Systems Designed for the Cloud Computing Paradigm

Nalaka Arjuna Premathilaka, Achala Chathuranga Aponso, Naomi Krishnarajah
Department of Computing
Informatics Institute of Technology
University of Westminster
Colombo, Sri Lanka

Abstract– **Cloud Computing is an emerging technology that enhances capability, usability and scalability of computer systems. On account of some exclusive features, cloud computing system always differs from the traditional computer system; not only the capabilities but also the vulnerabilities and threats.**

Intrusion Detection System (IDS) is a significant component of computer system security and compliance practices that protects computer systems from various types of malicious activities and attacks. Intrusion Detection Systems have been evolved over decades and various types of systems are currently available to identify and eradicate attacks based on different system conditions and different aptitudes.

The main purpose of this paper is to review the state-of-art Intrusion Detection Systems available for cloud computing paradigm, which adhere to features of cloud computing architecture. Scalability, elasticity, reliability, performance, security and distributed nature of the Intrusion Detection Systems will be reviewed in order to identify suitable approaches for cloud computing.

Keywords- Intrusion Detection System; Computer System Security; Cloud Security; Network based IDS; Host based IDS; Intrusion detection system for cloud computing;

I. INTRODUCTION

The Cloud Computing paradigm is an emerging technology in the IT sector. Most of the organizations are moving their IT systems into the cloud computing paradigm because of its encouraging characteristics, such as easy usage, availability, reliability and cost efficiency. Cloud computing is a different form of computer system and it has some special characteristics such as (a) virtualization, (b) distribution, (c) On-demand self-service, (d) Broad network access, (e) Resource-pooling(Multi-Tenancy), (f) Rapid elasticity, (g) Measured service and (h) dynamically extendibility [3] [4].

The Intrusion Detection System (IDS) is one of the rapidly expanding advance security solutions which protect computer systems from the various types of malicious activities and attacks. Since cloud computing environment is different from the general computer systems, Intrusion Detection System should be specially designed to be compatible with most of the properties of a cloud computing environment. Plenty of studies are being carried out to propose the suitable security mechanism for cloud computing architecture using Intrusion Detection Systems.

This review was mainly carried out in the area of Intrusion Detection Systems used in the cloud computing infrastructure; Advantages and disadvantages of Intrusion Detection Systems when adopting with the cloud computing were discussed based on the types, methodologies and their suitability for cloud environments. Accordingly, the best process and the best features of the Intrusion Detection Systems in cloud computing were identified.

II. INTRUSION DETECTION SYSTEM

The concept of the Intrusion Detection System (IDS) was born with the idea of James Anderson's paper on "Computer Security Threat Monitoring and Surveillance" [5] and since then IDS has evolved over three decades. IDS is a proactive monitoring technology and defensive mechanism in protecting critical IT infrastructures from malicious behaviours, which may compromise sensitive data and critical applications through cyber-attacks [6]. Because of the high volume and the complexity of computer system attacks, a dramatic rise of the usage in IDSs is noted recently.

Characteristics of an ideal IDS are described by the Cramer, Cannady and Harrell [7] as (1) Timeliness (2) High probability of detection (3) Low false-alarm rate (4) Specificity (5) Scalability and (6) Low a priori information required. Further, six compelling reasons to acquire and use an Intrusion Detection System within any organization were identified byBace and Mell [8]. Based on those criteria, many enterprise-level IDSs have been developed and released to the market. Snort [9], Bro [10], StealthWatch [11], AirDefense [12] and Proventia [13] are some of the famous products.

Since the cloud computing is a special type of network, traditional decentralized IDS approach is not adhering to cloud computing requirements [6]. Further, the special requirements of IDS to use with the grid/cloud computing environment were discussed by Kumar, Hanumanthappa and Kumar [14] and the main point they emphasize is "IDS must be distributed to work in a grid computing environment. It must monitor each node and, when an attack occurs, it must alert other nodes in the environment".

Considering both traditional and cloud-based IDSs, the approaches can be categorized based on three factors [8]; They are an information source of the IDS, analysis approach of the IDS and response type of the IDS. Further based on the data sources, the existing Intrusion Detection Systems can be categorized into three groups [8], [15], [16].