Chapter 24

Attack Detection in Cloud Networks Based on Artificial Intelligence Approaches

Zuleyha Yiner
Siirt University, Turkey

Nurefsan Sertbas
Istanbul University – Cerrahpaşa, Turkey

Safak Durukan-Odabasi
Istanbul University – Cerrahpaşa, Turkey

Derya Yiltas-Kaplan
Istanbul University – Cerrahpaşa, Turkey

ABSTRACT

Cloud computing that aims to provide convenient, on-demand, network access to shared software and hardware resources has security as the greatest challenge. Data security is the main security concern followed by intrusion detection and prevention in cloud infrastructure. In this chapter, general information about cloud computing and its security issues are discussed. In order to prevent or avoid many attacks, a number of machine learning algorithms approaches are proposed. However, these approaches do not provide efficient results for identifying unknown types of attacks. Deep learning enables to learning features that are more complex, and thanks to the collection of big data as a training data, deep learning achieves more successful results. Many deep learning algorithms are proposed for attack detection. Deep networks architecture is divided into two categories, and descriptions for each architecture and its related attack detection studies are discussed in the following section of chapter.

DOI: 10.4018/978-1-7998-2466-4.ch024

INTRODUCTION

Cloud networks include virtual data centers that handles the physical or traditional data centers to give the opportunity of storing data or benefiting from the hardware devices to the end users (Bhamare et al., 2016). Several computer application areas such as image processing need very large amount of storage size and processing time (Marwan et al., 2018). This leads to the requirement of spread usage of cloud networks that achieve a gain on operational and physical costs.

Cloud computing covers several branches of computer engineering discipline. These are distributed computing, grid computing, networking, software, and virtualization. The cloud also involves many advantages related with the sides of computer hardware or software, namely data storage solutions, scalability, rapid configuration, security options, lower costs, flexibility in the network access, and so on. Actually cloud computing can be defined with different explanations such as virtualization of on-demand resources and abstraction of services. However, cloud computing can be explained in two general definitions. The first definition says that it is an infrastructure that gives the opportunity to the end-user applications with a payment in return for the software/hardware usage rate. The second definition means that it is a model in which the end-users access the network area involving hardware or software elements such as servers, storage devices, and applications by the help of the service providers. If the stored data is about healthcare and obtained as several images from the patients, the service provider brings profit to the healthcare organizations especially on data management, access, and processing from several different user points (Said et al., 2016, Chonka et al., 2011, Marwan et al., 2018).

The largest technology companies in the world, namely Google, Amazon, and Ebay, make investments for cloud computing. Technology vendors enable the customers to use any hardware or software parts in their computers against payment of a fee. By the time going on, the attacks over the cloud systems gain an increase on their amounts and a robustness in their structures. Because that the cloud infrastructure is a sharing environment, the security becomes vital and vulnerable. The two endpoints of the cloud, namely service provider and the user should be confident that the security problems are solved in the cloud network. Some private data such as patient files should be encrypted before sending to the remote servers (Chonka et al., 2011, Said et al., 2016).

CLOUD ARCHITECTURE AND CLOUD SECURITY ISSUES

There are three different layers in a cloud structure. These are Deployment Models, Service Models, and Essential Characteristics respectively from the bottom to the top. The classes in the Deployment Models are public, private, hybrid, and community. For any class of the deployment models, there are delivery models called Service Models, which involve Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These models are the core of the cloud network and get several characteristics from the top level of the structure. The characteristics can be exemplified as measured service, on-demand self-service, and rapid elasticity (Said et al., 2016).

The large amounts of data and customers in a cloud environment cause the performance degradation and inaccessibility to the network. To solve any problem and also any security issue, the cloud computing requires specific methods. Because the system and its properties like sharing of the resources are different from the other networking types.

Related Content