Chapter 96
Multi-Aspect DDOS Detection System for Securing Cloud Network

Pourya Shamsolmoali
Advanced Scientific Computing, CMCC, Italy

Masoumeh Zareapoor
Shanghai Jiao Tong University, China

M.Afshar Alam
Jamia Hamdard University, India

ABSTRACT

Distributed Denial of Service (DDoS) attacks have become a serious attack for internet security and Cloud Computing environment. This kind of attacks is the most complex form of DoS (Denial of Service) attacks. This type of attack can simply duplicate its source address, such as spoofing attack, which defending methods do not able to disguises the real location of the attack. Therefore, DDoS attack is the most significant challenge for network. In this chapter we present different aspect of security in Cloud Computing, mostly we concentrated on DDOS Attacks. The Authors illustrated all types of Dos Attacks and discussed the most effective detection methods.

INTRODUCTION

Cloud computing according to National Institute of Standards and Technology (NIST) is “a service that is provided in two forms. Computing power and data storage, remotely over the internet with negligible efforts for resource allocation, management, and release” (Mell and Grance, 2011). The US National Institute of Standards and Technology (NIST) have captured five essential cloud characteristics which are (Mell & Grance, 2011). “Ubiquitous network access, Rapid elasticity, Resource pooling, on-demand self-service, measured service”.

DOI: 10.4018/978-1-5225-8176-5.ch096

With Cloud Computing, users use a range of devices, including PCs, laptops, smartphones and PDAs to access programs, storage, and application development platforms over the Internet, via services offered by cloud computing providers Cloud computing provides three major services to its users at various layers of computing. These include as follow: "software as a service, platform as a service and infrastructure as a service". Advantages of the cloud computing technology consist of cost savings, high availability and easy scalability (Man & Huh, 2011). Cloud computing 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)" (Shelke et al., 2012).

While switching from traditional local computing paradigm to the cloud computing paradigm, new security and privacy challenges come out because of the distributed nature of cloud computing. A number of these security vulnerabilities leave open doors, which stem from the existing computing models; and some of them, inherent from cloud-based models. Therefore, Attacker force these doors to attack the system, and they attack end-users' private data; processing power, bandwidth or storage capacity of the cloud network.

Armbrust et al. (2010), noted, the cloud has the ability to change a large part of the IT industry. Currently, it is rising as a computing key platform for distributing infrastructure resources, software resources and application resources (Doua et al., 2013). "DDOS attacks prevents the legitimate access the server, exhaust their resources and accrues large financial loss and have become one of the most important security threats to the Net". It is simple to start an attack with few tools but at the victim side, it is not easy to stop it (Du and Nakao, 2010; Doua et al., 2013). Therefore, these critical services need some advanced protection system. "Network Performance degradation, revenue loss, and service unavailability is an issue that motivated us to offer protection for these collaborative applications.

Since Cloud infrastructure has massive network traffic, the traditional Intrusion Detection Systems are not competent enough to handle such a large data flow. Most known Intrusion Detection Systems are single threaded and due to prosperous dataset flow, there is a need of multi-threaded Intrusion Detection Systems in Cloud computing environment.

In this chapter, it is aimed to offer definitions and properties of several attack types in cloud network and to introduce DDOS detection and prevention models to resist these types of attacks. The Proposed model has a high accuracy, very simple to set up and requires very small storage.

BACKGROUND

The increased incidences of security threats and increased harm by DDoS attacks have motivated the development of multiple types of attack detection mechanisms. These approaches differ depending on the purpose of detection and set of rules required for operation. Most of these methods are based on identifying anomalies in network traffic.

Specht and Lee (2004), Shamsolmoali et al. (2014) mentioned "DDOS attack is generally classified into bandwidth depletion and resource depletion attack. In bandwidth depletion attack, attackers flood the target with huge packet traffic that avoids the legitimate traffic and intensifies the attack by sending messages to broadcast IP address." In resources reduction attack, attackers aim to tie up the significant resources (processor and memory) then trying to enable the victim to process the services.

Karimazad and Faraahi (2011) introduced an anomaly based DDoS detection system based on features of attack packets. For evaluation, the author used Radial Basis Function (RBF) neural networks. Vectors