Chapter 95

Survey on DDoS Attacks and Defense Mechanisms in Cloud and Fog Computing

Deepali Chaudhary
National Institute of Technology Kurukshetra, India

Kriti Bhushan
National Institute of Technology Kurukshetra, India

B.B. Gupta
National Institute of Technology Kurukshetra, India

ABSTRACT

This article describes how cloud computing has emerged as a strong competitor against traditional IT platforms by offering low-cost and "pay-as-you-go" computing potential and on-demand provisioning of services. Governments, as well as organizations, have migrated their entire or most of the IT infrastructure to the cloud. With the emergence of IoT devices and big data, the amount of data forwarded to the cloud has increased to a huge extent. Therefore, the paradigm of cloud computing is no longer sufficient. Furthermore, with the growth of demand for IoT solutions in organizations, it has become essential to process data quickly, substantially and on-site. Hence, Fog computing is introduced to overcome these drawbacks of cloud computing by bringing intelligence to the edge of the network using smart devices. One major security issue related to the cloud is the DDoS attack. This article discusses in detail about the DDoS attack, cloud computing, fog computing, how DDoS affect cloud environment and how fog computing can be used in a cloud environment to solve a variety of problems.

1. INTRODUCTION

The long-held dream of computing as a utility was achieved with Cloud Computing (Gupta & Badve, 2017; Ahuja & Kaja, 2015) that provides the potential of transforming a large part of the IT industry. Organizations which are at the early stage no longer need to invest large capital in buying hardware to deploy their service or large human expense to operate it. There is no need to be concerned about

DOI: 10.4018/978-1-5225-8176-5.ch095

under-utilization of expensive resources for a service which did not meet the expected predictions or exhaustion of the available resources by the service that becomes wildly popular, which may lead to missing potential customers and revenue. Moreover, organizations with large batch-oriented work load can get quick results alongside the scaling of their program, since the cost of accessing 1,000 servers for one hour is almost as much as accessing one server for 1,000 hours. Hence, these features like the elasticity of resources, pay-as-you-go, resource provisioning, on-demand service and much more have made cloud computing very popular (Gupta & Kumar, 2013). However, as all the services in the cloud are hosted over the Internet making cloud prone to many security issues and one such issue is addressed in this paper i.e. the DDoS attack.

DDoS attack or Distributed DoS attack (Gupta et al., 2012; Douligeris & Mitrokosta, 2004) is an attack performed on the victim with the help of a large number of machines which are known as zombie machines or bot that are infected by some malicious code or compromised by an attacker. These machines are centrally controlled and coordinated by an attacker to initiate the attack on the victim machine. The DDoS attack is mainly an attack on availability i.e. victim machine becomes unavailable to the legitimate users trying to establish a connection with it. But when a DDoS attack occurs in a cloud environment (Bhusan & Gupta, 2017; Somani et al., 2016), it exhausts all the resources of the target VM and overburdens it. This situation can be handled by cloud with the allocation of more resources to the victim VM to process all the requests made to it. But the further allocation of additional resources can go on to an extent where either cloud provider runs out of idle resources or the owner of VM cannot pay for the increasing demand of resources anymore.

Fog computing can also be described as an extension to cloud computing which removes several limitations of cloud computing like need of huge amount of data to be forwarded to a cloud server, the high latency for real-time problems, high transportation cost and much more (Lee et al., 2015; Chuck, 2015). Fog computing introduces a new paradigm for cloud computing that includes performing necessary analysis and computation at the edge of the cloud to provide many benefits like less bandwidth consumption and networking strain, decreased costs, reduced latency, faster access, security, and accountability (Stolfo et al., 2012). Fog computing connects machines, sensors, and devices directly to each other enabling real-time decision making without transmitting a vast amount of data through the cloud (Bonomi et al., 2012; Chow et al., 2009). Therefore, fog computing concept can be beneficial for efficient DDoS attack detection and mitigation in future.

Several features of cloud computing including pay-as-you-go pricing model, on-demand services, rapid elasticity, etc. make it more vulnerable to the variety of DDoS attacks. As ensuring availability of cloud services is still a challenge for the service providers, this paper presents various security issues faced by cloud environment, and different DDoS defence mechanisms in the literature are also discussed in this paper. Further, as fog computing overcomes various limitations of cloud computing; therefore, it could be helpful in DDoS attack detection and mitigation. Hence, we have presented the basic concepts of fog computing, its architecture, and its role in DDoS attack defence in cloud computing. We have also discussed various recent approaches in the direction of DDoS attack defence in the cloud using fog computing. Moreover, we have discussed some use cases to help us understand how and where fog computing can be used in order to make our lives easier and safer.

This paper is mainly divided into five sections, section 2 presents the DDoS attack model and statistics. Section 3 elucidates cloud computing environment with its service model and deployment model along with various cloud security challenges. This section also explains how the DDoS attack is carried