Chapter 27
Distributed Denial of Service Attacks and Defense in Cloud Computing

Gopal Singh Kushwah
National Institute of Technology Kurukshetra, India

Virender Ranga
https://orcid.org/0000-0002-2046-8642
National Institute of Technology Kurukshetra, India

ABSTRACT

Cloud computing has now become a part of many businesses. It provides on-demand resources to its users based on pay-as-you-use policy, across the globe. The high availability feature of this technology is affected by distributed denial of service (DDoS) attack, which is a major security issue. In this attack, cloud or network resources are exhausted, resulting in a denial of service for legitimate users. In this chapter, a classification of various types of DDoS attacks has been presented, and techniques for defending these attacks in cloud computing have been discussed. A discussion on challenges and open issues in this area is also given. Finally, a conceptual model based on extreme learning machine has been proposed to defend these attacks.

INTRODUCTION

Cloud computing is one of the most promising technologies today. The services provided by cloud computing are grouped into three types, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). SaaS provides various application programs. PaaS provides application development environments. IaaS provides processing power, memory etc. Security is a major concern in this area. The issues related to security in clouds are confidentiality, privacy, access control, integrity, and availability. Confidentiality means only authorized entities should have access to the data stored in the cloud. In the cloud, the data of users are stored away from their site and users do not have direct

DOI: 10.4018/978-1-7998-5348-0.ch027

control over data. Strong data confidentiality techniques are thus needed. The controlled disclosure of personal information of users comes under privacy. Only authorized entities should be provided information about cloud users. Access control ensures that a user should be able to access only those services to which he/she is authorized, not more. Access control should be provided fine-grained. Integrity means only authorized entities should be able to make changes in the data. If there is any change in the stored data, the owner of data should be able to identify the change. Also, if there is any loss or corruption of stored data, there should be a way to retrieve it. Availability means the services should be available all the time to legitimate users. There should be no denial of provided services to its users.

High availability is one of the most important features of cloud computing, it is affected by Distributed denial of service (DDoS) attacks. These attacks have made a huge loss to cloud computing as well as traditional IT infrastructure. In this attack, the attacker uses many compromised hosts to launch the attack. All these hosts work on the instructions provided by the attacker and send traffic to the target, to disrupt the services provided by it. Cloud computing has now become the new target for DDoS attackers as predicted in (Patrick, 2015). This was evidenced by (Seals, 2015) that most of the attacks in the first quarter of 2015 were on cloud-based systems. According to (Global IT security risks survey, 2015), 50% of the surveyed businesses experienced DDoS attacks in the year of 2014. The business' public website is the most affected service. In most of the cases, the website is not accessible. In some cases, a particular area of the website is affected, like login area. The most commonly reported effect of DDoS attack was increased page load time. The loss due to DDoS attacks to small and medium organizations is $52,000 per attack, while for large organizations this loss is $444,000 as depicted in (Global IT security risks survey 2014-Distributed denial of service (DDoS) attacks, 2014). The gaming industry has been the highest target for DDoS attacks in 2017 as shown by (McKeay & Fakhreddine, 2017a; McKeay & Fakhreddine, 2017b; McKeay & Fakhreddine, 2017c; McKeay & Fakhreddine, 2017d). Organization wise DDoS attack target information for the year 2017 is shown in figure 1. Average numbers of attacks per target have been 25, 32, 36 and 29 for Q1 2017, Q2 2017, Q3 2017 and Q4 2017, respectively. In view of these facts, there is a strong need of developing solutions for DDoS attack defense in cloud computing. The solutions for DDoS attacks can be developed using two approaches, proactive and reactive. The first approach is based on avoidance of attack and, the second approach is based on detection and mitigation of attack. In this chapter, some recent works done in DDoS attack defense in cloud computing have been discussed. A prediction based model for attack detection has also been proposed. Specifically, our contributions in this chapter are summarized as follows.

- To give a taxonomy of DDoS attacks.
- To present a literature survey on recent DDoS attack defense solutions in Cloud Computing.
- To discuss challenges and open issues in DDoS attack defense in cloud computing.
- To propose an extreme learning machine based model for defending DDoS attacks.

DDoS ATTACKS AND ITS TYPES

In DDoS attack, the attacker uses many machines to launch the attack. To perform the attack, a botnet of compromised machines is created. These machines are scattered through the Internet and follow instructions of the attacker during the attack. Some other machines called handlers are also used, which are more powerful than the bots. These handlers are directly connected to the attacker and relay the