Chapter 65
Defensive Mechanism Against DDoS Attack to Preserve Resource Availability for IoT Applications

Manimaran Aridoss
Madanapalle Institute of Technology and Science, India

ABSTRACT

The major challenge of Internet of Things (IoT) generated data is its hypervisor level vulnerabilities. Malicious VM deployment and termination are so simple due to its multitenant shared nature and distributed elastic cloud features. These features enable the attackers to launch Distributed Denial of Service attacks to degrade cloud server performance. Attack detection techniques are applied to the VMs that are used by malicious tenants to hold the cloud resources by launching DDoS attacks at data center subnets. Traditional dataflow-based attack detection methods rely on the similarities of incoming requests which consist of IP and TCP header information flows. The proposed approach classifies the status patterns of malicious VMs and ideal VMs to identify the attackers. In this article, information theory is used to calculate the entropy value of the malicious virtual machines for detecting attack behaviors. Experimental results prove that the proposed system works well against DDoS attacks in IoT applications.

INTRODUCTION

Internet of Things connects all kind of physical devices across the world in order to make all the devices communicate each other without human intervention. To establish IoT environment, Sensors act as input devices and Actuators works as output devices. Across the globe there are millions of sensors are fixed and generated data can be stored in the cloud server for data processing. IoT data are time sensitive for most of the applications like Health care management, mining industries, Industrial IoT and so on. Hence the significant of processing IoT data is highly Time sensitive, so delay of millisecond may cause very

DOI: 10.4018/978-1-5225-9866-4.ch065

serious problem. In order to protect the IoT data from attackers, suitable attack detection mechanism is required to maintain the IoT services (Samalia et al., 2017).

Mantra of cloud computing is its resource abstraction nature, for example, cloud users need not install any particular hardware or software for difficult operations. Security issues are major hurdles for adopting cloud computing. Cloud Data Center has to maintain some security standards to protect resource from attackers to sustain resource availability (Jegadeeswari et al., 2016; Iyengar et al., 2015). Cloud Computing achieves greater benefits by incorporating various distributed networking technologies like distributed computing, grid computing, and virtualization (Reddy et al., 2016). Challenging security threat for availability of the Datacenter resource is Distributed Denial of Service (DDoS) attack (Durairaj & Manimaran, 2015). DDoS attacker intention is to collapse the entire cloud network or memory resources of Data Center (Figure 1) either by exhausting of victim bandwidth or by stealing the sensitive information from the victim end (Girma et al., 2015; Chandrika & Bharadwaj, 2016). Security issue like resource availability heavily affects the IoT environment because of resource requirement at the right time is the core features of IoT services. In order to provide the IoT data to its legitimate end users, need to propose the mechanism to detect DDoS attacks to protect the IoT sensor generated data from attackers (Jing et al., 2014).

The existing attack detection mechanisms are not effective when incoming traffic rate is high. Hence, suitable attack detection mechanism needs to be devised for protecting DC resources from DDoS attack to provide service to the legitimate users. Attackers are mainly using IP Spoofing technique to denial resource availability for the legal users by generating DDoS attack (TCP SYN flood, UDP flood, and ICMP flood) and control over virtual machines (Nandwani et al., 2016). Objective of this paper is to improve resource availability of Data Center and to provide effective mechanism to protect resources

Figure 1. Cloud network