# Chapter 10
# A Deep Learning Approach for Detection of Application Layer Attacks in Internet

**V. Punitha**
*National Institute of Technology, Tiruchirappalli, India*

**C. Mala**
*National Institute of Technology, Tiruchirappalli, India*

## ABSTRACT

*The recent technological transformation in application deployment, with the enriched availability of applications, induces the attackers to shift the target of the attack to the services provided by the application layer. Application layer DoS or DDoS attacks are launched only after establishing the connection to the server. They are stealthier than network or transport layer attacks. The existing defence mechanisms are unproductive in detecting application layer DoS or DDoS attacks. Hence, this chapter proposes a novel deep learning classification model using an autoencoder to detect application layer DDoS attacks by measuring the deviations in the incoming network traffic. The experimental results show that the proposed deep autoencoder model detects application layer attacks in HTTP traffic more proficiently than existing machine learning models.*

## INTRODUCTION

The technological advancements bring out new dimensions in application development. The availability of the applications and services are intentionally blocked by Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks. DoS attack is the one of the powerful threats in internet. In this attack, the malicious user makes the server and other network resources unavailable to legitimate users by interrupting the server's regular activities. Malicious user launches this attack by sending overwhelming requests to targeted server continuously, until legitimate access are unable to be processed by the server, and thereby blocking the availability of the server to legitimate users. Malicious user uses single com-

DOI: 10.4018/978-1-7998-2491-6.ch010

puter system to launch this attack over the internet (Douligeris and Mitrokotsa 2004; Peng et al., 2007). DDoS attack is the one of the most vulnerable threats in the internet. Similar to DoS attack, it is also created by sending overwhelming requests to targeted server to block the availability of the server. But, DDoS attacks are launched using multiple compromised computers on the internet (Prasad et al., 2014).

UDP and ICMP flood attacks & TCP SYN flood attack are network and transport layer DDoS attacks. Here, the attacker transmits large number of UDP/ICMP packets to the targeted server. The packets are either transmitted to targeted port or to random ports. In both cases, the sender's identities are spoofed. In TCP SYN attack, the attacker overwhelms the targeted server with huge number of connection requests. This activity forces the server to send connection acknowledgement to each malicious request, and subsequently waiting for connection response indefinitely. Thus, the availability of the server is blocked to legitimate users. These attacks are volumetric attacks. They are detected using arrival statistics and traffic size (Basicevic et al, 2015; Elejla et al., 2018; Perakovic et al., 2017). The recent technological advancements induce the attackers to shift the target of the attack to the application services, and thereby increasing application layer DDoS attacks in internet traffic. The application layer attacks are created to impair specific application or web server. They are not volumetric attacks like network/transport layer attacks. It requires only low or mid bandwidth as it is launched after receiving protocol confirmation, i.e., application layer attacks are launched only after protocol handshakes or connection establishment phase. Therefore, these attacks appear as normal requests. Thus, they are stealthier than network/transport layer attacks. As the botnet apparently transmits legitimate requests to the server, the application layer DDoS attacks are difficult to discriminate (Zhou et al., 2014).

The application layer attacks are low and slow attacks. The attackers use diverse intelligent clients to launch various types of attacks such as HTTP-GET/POST flood, slow rate attack, BGP Hijacking. Unlike the network/transport layer attacks such as SYN flood, ICMP flood & NTP amplification attacks, the application layer attacks cannot be discriminated using traffic rate. It requires deep investigation on requesting behavior of the client and the network packet parameters. Hence, the existing defense mechanisms which are applied to detect network/transport layer attacks are ineffective in detecting application layer DDoS attacks (Mantas et al., 2015).

Hypertext Transfer Protocol (HTTP) is one of the most widely used application layer protocols. Request flooding attack is the most powerful threat in application layer, especially while using HTTP protocol. Here, enormous amount of HTTP requests are generated by botnet and transmitted to intended application server. Initially, the attacker establishes a valid connection to the server, then it transmits huge number of HTTP GET or POST requests through the valid connection. These requests are intentionally transmitted to consume server resources, and thereby blocking their usage to legitimate users (Zhou et al., 2014). In most cases, HTTP-GET or POST flood attacks are launched to crash Apache and OpenBSD servers. Another powerful threat in HTTP traffic is a slow rate attack. Here, the attacker transmits the requests or data very slowly, so that, the server resources are consumed for long time and thereby preventing the legitimate access. Slow read attack is another kind of slow rate attack, where the attacker transmits the valid HTTP request to the server and reading the responses very slow just to continue the session for long duration meaninglessly (Mantas et al., 2015). BGP hijacking is another application layer attack. It impersonates a network and diverts the network traffic to the attacker's destination. Diverse DDoS attacks and avalanche of such threats demand automatic detection techniques to enhance internet security.