Chapter 24
The HTTP Flooding Attack Detection to Secure and Safeguard Online Applications in the Cloud

Dhanapal A
VIT University, Chennai, India

Nithyanandam P
VIT University, Chennai, India

ABSTRACT

Cloud computing is the cutting edge and has become inevitable in all forms of computing. This is due to its nature of elasticity, cost-effectiveness, availability, etc. The online applications like e-commerce, and e-healthcare applications are moving to the cloud to reduce their operational cost. These applications have the vulnerability of a HTTP flooding Distributed Denial of Service attack in the cloud. This flooding attack aims to overload the application, making it unable to process genuine requests and bring it down. So, these applications need to be secured and safeguarded against such attacks. This HTTP flooding attack is one of the key challenging issues as it shows normal behaviour with regard to all lower networking layers like TCP 3-way handshaking by mimicking genuine requests and it is even harder in the cloud due to the cloud properties. This article offers a solution for detecting a HTTP flooding attack in the cloud by using the novel TriZonal Linear Prediction (TLP) model. The solution was implemented using OpenStack and the FIFA Worldcup '98 data set for experimentation.

INTRODUCTION

Cloud computing aids start-ups, small and medium level organization to reduce their capital investment (Salesforce, 2015) on the infrastructure front and use those investments towards their core business accomplishments. National Institute of Standards and Technology (NIST) defines the cloud computing

DOI: 10.4018/978-1-7998-5348-0.ch024

(NIST, 2017) is a model for enabling convenient on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes the availability and it exhibits the following five characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

Cloud Computing Classifications, Threats and Types

The cloud computing is classified based on the cloud services offered and cloud deployment scenario as follows:

- The cloud service delivery-based classifications are (WhatIsCloud, 2016a) Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS);
- The cloud deployment service models categories are (WhatIsCloud, 2016b) Private cloud, Public cloud, Hybrid cloud and Community Cloud.

Cloud Computing Threats

The cloud computing itself is evolving day by day. So, all the potential threats that are faced by computing technologies such as data breach, distributed denial of service, insider threat, malware injection, data loss, etc., are also applicable to the cloud computing (Ma, 2015) as well. It has become a question of how secure and safe the cloud computing for the business or business critical applications such as E-commerce, E-healthcare, financial services, online services like reservation system etc. Due to these security concerns, cloud computing adoption for business is very slow. The Distributed Denial of Service (DDoS) is one of the major threat to the cloud computing environment. There are multiple types of DDoS exists and they are explained in the next section.

Types of DDoS Attacks

The DDoS attacks are generally classified (Arbor Networks, 2019) (Radware, 2016) (Wikipedia, n.d.) into the following types:

- **Volumetric Attacks:** The attack is targeted to the network bandwidth. Examples are ICMP flooding, UDP flooding, etc.;
- **Protocol Attacks:** The server resources targeted in this type attack. Example is Ping of death;
- **Application Layer Attacks:** This aims to bring down the application services. The example is HTTP flooding attack.

The motivation behind DDoS attacks may be anything like bring down the competition, revenge, political reasons, etc. (Spacey, 2011) (Penta Security, 2016).