Enhanced-Adaptive Pattern Attack Recognition Technique (E-APART) Against EDoS Attacks in Cloud Computing

Rohit Thaper, Panjab University, Chandigarh, India

Amandeep Verma, Panjab University, Chandigarh, India

ABSTRACT

Cloud Computing is most widely used in current technology. It provides a higher availability of resources to greater number of end users. In the cloud era, security has develop a reformed source of worries. Distributed Denial of Service (DDoS) and Economical Denial of Sustainability (EDoS) are attacks that can affect the 'pay-per-use' model. This model automatically scales the resources according to the demand of consumers. The functionality of this model is to mitigate the EDoS attack by some tactical attacker/s, group of attackers or zombie machine network (BOTNET) to minimize the availability of the target resources, which directly or indirectly reduces the profits and increase the cost for the cloud operators. This paper presents a model called Enhanced-APART which is step further of the authors' previous model (APART) that can be used to mitigate the EDoS attack from the cloud platform and shows the nature of the attack. Enhanced-APART model offers pre-shared security mechanism to ensure the access of legitimate users on the cloud services. It also performs pattern analysis in order to detect the EDoS caused by BOTNET mechanism and includes time-based and key-sharing post-setup authentication scheme to prevent the replication or replay attacks and thus results in mitigation of EDoS attack.

Keywords: APART, Cloud Computing, DDoS, DoS, E-APART, EDoS, EDoS-Shield, Security, SLA

1. INTRODUCTION

These days society's reliance on information technology has increased by large extent and cloud computing is an environment which fulfill this huge demand of resources in a cost efficient way. In Cloud Computing resources are provided as services to the users on pay-per-use model (http://csrc.nist.gov/groups/SNS/cloud-computing). Resources can be dynamically scaled up without much interaction between users and service providers. Different resource provided by cloud Computing are data storage, computing resources and network platforms. These resources are provided over the internet to the users.

DOI: 10.4018/JCIT.2015070105

Cloud security is one of the main issue in Cloud Computing which resist the organizations too fully shift their business to cloud. Cloud Computing is prone to number of attacks (Tsai & Lin, 2010). One of the main attack is Denial-of-service (DoS) in which a legitimate user is denied of computing services due to malicious actions of attacker (Jamdagni, Tan, He, Nanda & Liu, 2013).

DoS attacks results in unavailability of a resource which can be router, host or a whole network to the authenticated users. Attackers send a huge amount of useless packets to force the resource to be out of services for a few minutes or even few days by burdening the system (Tan, 2013; 2012; 2011). Due severity of this attack some detection methods of DoS attack are compulsory to protect the online services (Stolfo, Fan, Lee, Prodromidis & Chan, 2000).

When DoS attacks are generated from multiple distributed machines it become another very difficult attack known Disturbed-denial-of-services (DDoS) (Liu, 2009). In DDoS attack a huge amount of traffic is generated at the victim server by sending large amount of invalid packets as a result the legitimate users are denied of services by the victim server due to congestion created by attackers. DDoS attack is even harder to detect than DoS due its multiple origins and use of IP spoofing by attackers (www.arbornetworks.com) (Bhandari, 2013).

When DDoS attack is implemented in Cloud Computing environment it leads to another attack known as Economical-Denial-Of-Sustainability (EDoS). This attack exploits the dynamic scalability property of cloud (Metz, 2009). In EDoS, attacker uses the provisioned resources of the user and dynamically scale it by using the resources for invalid request generated by zombie machines. This results in raising the cost for the user and decrementing the profit and trust of the service provider thus affecting the sustainability of CSP as shown in Figure 1.

In EDoS the users are charged for resources which they don't even use (Robinson, 2005). The firms chosen for cloud will experience an overstated bills for using auto scaling feature to address an overflow of malicious traffic in order to meet the necessity to clear SLA.

A service level agreement (SLA) is an article which describes the connection among two parties: the provider and the receiver (Kandukuri, Reddy, Ramakrishna & Rakshit, 2009).

This is undoubtedly a very significant element of certification for both parties. If used correctly it must:

Figure 1. Effect of an EDoS Attack against the cloud