Chapter 26
Denial of Service (DoS) Attacks Over Cloud Environment: A Literature Survey

Thangavel M.
https://orcid.org/0000-0002-2510-8857
Thiagarajar College of Engineering, India

Nithya S
Thiagarajar College of Engineering, India

Sindhuja R
Thiagarajar College of Engineering, India

ABSTRACT

Cloud computing is the fastest growing technology in today's world. Cloud services provide pay as go models on capacity or usage. For providing better cloud services, capacity planning is very important. Proper capacity planning will maximize efficiency and on the other side proper control over the resources will help to overcome from attacks. As the technology develops in one side, threats and vulnerabilities to security also increases on the other side. A complete analysis of Denial of Service (DOS) attacks in cloud computing and how are they done in the cloud environment and the impact of reduced capacity in cloud causes greater significance. Among all the cloud computing attacks, DOS is a major threat to the cloud environment. In this book chapter, we are going to discuss DOS attack in the cloud and its types, what are the tools used to perform DOS attack and how they are detected and prevented. Finally it deals with the measures to protect the cloud services from DOS attack and also penetration testing for DOS attack.

DOI: 10.4018/978-1-7998-5348-0.ch026

INTRODUCTION

Cloud computing is an emerging trend in the field of Information Technology. Cloud computing provides scalable and flexible resources for the end users on demand. The cloud offers three levels of services. They are Infrastructure as a service (Iaas), Platform as a service (Paas), and Software as a service (Saas). In Infrastructure as a service, the consumer (customer) have the capability of processing, storage and other computing resources. The consumer can deploy and run the software, like operating systems and applications (E.g. Host firewall). In platform as a service, the consumer can create the applications using libraries, tools and programming languages offered by cloud service providers (cloud middleware's –E.g. Open nebula). The consumer cannot control the cloud infrastructure like operating systems, networks, and servers. In Software as a service, the consumer can make use of the applications that were created by the cloud service provider (E.g. Web based applications). Cloud characteristics include multi tenancy, device independence, resource pooling, measured services, resource allocation, scalability, use of third party services and energy efficiency.

Cloud computing provides the capabilities to store and process the data of the users and organizations in a third party (Cloud Service Provider) storage center. Cloud computing is one of the most innovative technologies in the present decade. In cloud computing, there are three types of cloud, namely, public cloud, private cloud and hybrid cloud. The advantages of cloud computing are cost saving, manageability and reliability. On the other side, there is a controversy in security and vendor lock in issue. In cloud computing, still some organizations cannot switch from one services to other services and it has not been completely evolved. This is called as vendor lock in. One of the major advantage of cloud computing is elasticity of the resources. The proper capacity planning is very necessary to manage the resources. Capacity planning means to plan the resources needed for the application in future. Pay as you go services is good as it needs to be paid only for the utilized resources. Capacity planning of resources will make us to handle multiple resources simultaneously.

In security aspect, there are so many attacks happening everyday like data theft, DOS attack and side channel attack, etc. Even though the cloud service providers provide the security standards, providing security in all aspects is quite difficult. In public cloud the vulnerable server or system and exploitation could happen easily. Other disadvantages are limited controls, technical difficulties, and downtime. Downtime is one of the disadvantages of the cloud service that affects the services when the internet connection goes down. In future, the security exploitation in cloud computing has to be managed effectively from the perspective of both providers and users.

COMMON ATTACKS ON CLOUD

Authentication Attack

Authentication is one of the vulnerable points in the cloud services. Generally authentication is provided for the users using username and password. Some of the developed organizations used site keys, virtual keyboards, and biometrics and shared secret questions. Most possible authentication attacks are i) brute force attack ii) shoulder surfing iii) Replay attack iv) Dictionary attack v) key loggers. We see in detail about all the above attacks. In a brute force attack, in order to break the username or password, we have to try all the possibilities (all possible combinations). In cloud, brute force attack is used to break the