INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Detection Mechanism of DDoS Attack in Cloud Computing

Shalini Verma
M. Tech. Student, Gyan Ganga College of Technology, Jabalpur, M.P., India
Saurabh Sharma
Faculty, Gyan Ganga College of Technology, Jabalpur, M.P., India

Abstract:
The Cloud Computing is a distributed computing model that was built to meet increasing demand for memory, storage and power due to industrialization and scientific research. In cloud environment, entire data resides over set of resources, which enables data to be accessed from Virtual Machines (VM). Availability of the cloud services is key security issues. Recently Distributed Denial of Service (DDoS) attacks are among one of the top threats to cloud environment and its being distributed in nature makes it simpler to launch. During DDoS, a program mostly occupies lots of computing resources, which prevents legitimate users from using services. This can be serious penalty for companies relying on cloud for their business. Thus, it becomes very important to reduce the impact of DDoS. This paper explains DDoS attack, & its effect in cloud computing and the important things which are to be needed while selecting defense mechanism for DDoS.

Keywords: *Cloud computing, Cloud security, DDoS.*

1. Introduction

Cloud computing is defined as a type of computing that relies on *sharing computing resources* rather than having local servers or personal computers to handle applications. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers or devices in a network are connected to solve problems too intensive for any stand-alone machine. Most popular definition is defined by National Institute of Standards and Technology (NIST) which describe as: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or client and service provider interaction 1. Virtualization is the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources where the framework divides the resource into one or more execution environments. Virtualization is a technique to allow your operating system and your software to believe they're running on standard, ordinary hardware while in reality they're running on top of another kind of software known as the hypervisor, which simulates a real computer. You create a hypervisor on your server and then create a number of so-called virtual machines inside of it. Each virtual machine can be seen as a completely new and independent server, and a completely insulated environment without any possibility of contamination among the virtual machines. A provision with virtual network interfaces to communicate with each other, and the internet.

DDoS attack is become a trouble to the availability. In cloud computing, a denial-of-service (DoS) attack is an attempt is to make a machine or network resource and services unavailable to the legitimate users, such as to temporarily or indefinitely interrupt or suspend services of a user connected to the Internet. A distributed denial-of-service (DDoS) is where the attack source is more than one and moreover thousands of unique IP addresses. The main intention of a DDoS attack is to make the victim service unavailable to the resources. In most of the scenarios, the target could be web servers, CPU, Storage, and the other Network resources 6.

A Denial of Service, or DoS as it is often abbreviated, is a malicious attack on a network. This type of attack is essentially designed to bring a network to its knees by flooding it with useless traffic. Many DoS attacks are working by exploiting limitations in the TCP/IP protocols.

The flood of incoming messages to the targeted system essentially forces it to sleep down, therefore by denying service to the system of targeted users. In a typical DDoS attack, the assailant begins by exploitation of a vulnerability from one computer system and making it the DDoS master. The attack master, which is also known as the botmaster, identifies and identifies first and then infects other vulnerable systems with malware. Eventually, the assailant instructs the controlled machines to launch an attack against a specified targeted system.

2. Cloud Overview

2.1. Definition

Cloud computing is a computing paradigm, where a large pool of systems are connected to the private or public networks, for providing dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly.

The idea of cloud computing is based on a very fundamental principal of „reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries.

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

This definition includes cloud architectures, security, and deployment strategies. In particular, five essential elements of cloud computing are clearly articulated:

- On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops and workstations). Broad network access includes private clouds that operate within a company's firewall, public clouds, or a hybrid deployment.
- Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacenter). Examples of resources include storage, processing, memory and network bandwidth.
- Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured Service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer.

2.2. Service Model

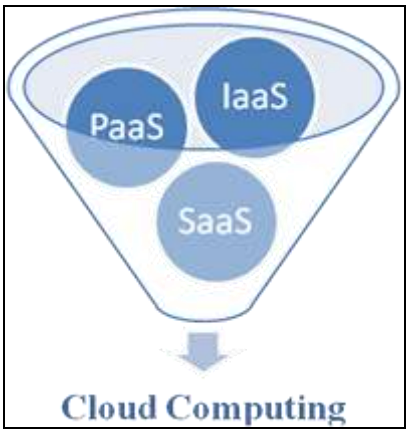

Figure 1

In addition to these five essential characteristics, the cloud community has extensively used the following three service models to categories the cloud services:

- Software as a Service (SaaS): In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers‟ side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

- Platform as a Service (PaaS): Here, a layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySQL and PHP), restricted J2EE, Ruby etc. Google's App Engine, Force.com, etc are some of the popular PaaS examples.

- Infrastructure as a Service (IaaS): Cloud IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, 3 Tera, etc.

- Data storage as a Service (DaaS): The delivery of virtualized storage on demand becomes a separate Cloud service - data storage service. DaaS providers collect and make available data on a wide range of topics, from economics and finance to social media to climate science. Some DaaS providers offer application programming interfaces (APIs) can provide on demand access to data when bulk downloads are not sufficient.

2.3. Deployment Model

More recently, four cloud deployment models have been defined in the Cloud community:

- Private cloud: The cloud infrastructure has been deployed, and is maintained and operated for a specific and particular organization. The operation may be in-house or with a third party vendor on the premises. There are two variations :
  - → On-premise Private Cloud: On-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security.
  - → Externally hosted Private Cloud: This type of private cloud is hosted externally with a cloud provider, where the provider facilitates an exclusive cloud environment with full guarantee of privacy. This is best suited for enterprises that don't prefer a public cloud due to sharing of physical resources.
- Public cloud: The cloud infrastructure is widely available to the public or customer on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared to the expenditure requirements normally in association with other deployment options. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.
- Hybrid cloud: Hybrid Clouds combine both public and private cloud models. The cloud infrastructure consists of a number of clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.
- Community cloud: The cloud infrastructure is to be shared among a number of organizations with similar requirements. This would help to limit the capital expenditure costs for its establishment as the costs are shared among the organizations.

The cloud community forms into a degree of economic scalability and democratic equilibrium.

2.3.1. Understanding the Attack

DDoS attacks are launched by affecting the victim in following forms:

- Attacker can find some bug or weakness in the software implementation to disrupt the service.
- Some attacks deplete all the bandwidth or resources of the victims system.

DDoS attacks are an attempt by a malicious party to overload systems and networks with malicious requests so that they can no longer serve content. For a website, this means that the site will not load and customers are unable to make purchases, view content, or log into accounts. For networks, DDoS attacks can cause bandwidth saturation or even inundate network infrastructure, causing widespread outages to customers on the entire network.

Hackers uses the DoS attacks to prevent targeted user of computer network resources and their services. DoS attacks are classified as attempts to flood a network, attempts to disrupt network connections between two computers, attempts to prevent an individual from accessing a service or attempts to disrupt service to a specific system or network. Those who are on the receiving end of a DoS attack might lose valuable resources, such as their e-mail services, Internet access or their Web server. Some of the DoS attacks may eat up all your system bandwidth or even use up all of a system resource, such as server memory, for example. Some of the worst-case scenarios we have seen over the past couple years is a Web site, used by millions of people being forced to cease operation because of a successful DoS attack.

2.3.2. DDoS Attacks in Past

A DoS attack may be very well appeared to the legitimate traffic on the system or network, but differs in that the volume and frequency of the traffic will increase to unmanageable levels. An attack on a Web server, for example, would not be normal spurts of visitors, but it would be a large barrage of hits in close proximity so the server that cannot keep up with the sheer volume of page requests. On a mail server, thousands of messages can be sent to the server site in a short period of time where the server would normally only handle under a thousand messages in that same period of a time. The legitimate server would most likely to be brought to a halt from a DoS attack because it runs out of swap space, process space or network connections.

While DoS attacks do not usually result in information theft or any security loss for a company, they can cost an organization both time and money while their network services are down. For the hacker (or the script kiddies who often use DoS attacks), a DoS attack is usually committed for "ego boosting" purposes.

In an around early 2001 a new type of DoS attack became rampant, called a Distributed Denial of Service attack, or DDoS. In this case multiple comprised systems are used to attack a single target. The flood of incoming traffic to the target will usually force it to shut down. Like a DoS attack, In a DDoS attack the legitimate requests to the affected system are denied. Since a DDoS attack it launched from multiple sources, it is often more difficult to detect and block than a DoS attack.

Thus, the network that has been burdened by the attack load can be considered as one more victim of the DDoS attack.

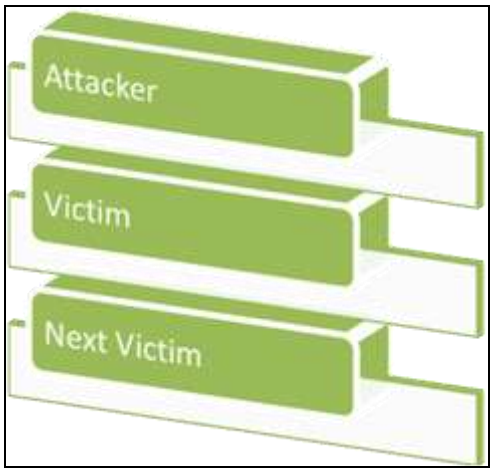

Figure 2: Constituents of DDoS

2.3.3. DDoS Constituents

Recently, Botnets are been used widely to perform DDoS attacks. In a typical DDoS attack, the army of the attacker consists of *master zombies* and *slave zombies*. The hosts of both categories are compromised machines that have arisen during the scanning process and are infected by malicious code. The attacker coordinates and orders master zombies and they, in turn, coordinate and trigger slave zombies. More specifically, the attacker sends an attack command to master zombies and activates all attack processes on those machines, which are in hibernation, waiting for the appropriate command to wake up and start attacking. Then, master zombies, through those processes, send attack commands to slave zombies, ordering them to mount a DDoS attack against the victim. In that way, the agent machines (slave zombies) begin to send a large volume of packets to the victim, flooding its system with useless load and exhausting its resources.

2.3.4. Classification

The variety of DDoS attacks are sprouting in the computing world. The major types include Bandwidth based and resource based attacks. Both types consume the entire bandwidth and resources of the network that's been exploited.

Bandwidth Depletion Attacks: This type of attack consumes the bandwidth of the flooded user or target system by flooding the unwanted traffic signal to prevent the intended traffic from reaching the victim network system. There are tools like Trinoo are usually used to perform these attacks.

Resource Depletion Attacks: An attacker depletes a resource to the point that the target's functionality is affected. Virtually any resource necessary for the target's operation can be targeted in this attack. The result of a successful resource depletion attack is usually the degrading or denial of one or more services offered by the target. The DDoS Resource depletion attack is targeted to exhaust the victim system's resources, so that the legitimate users are not serviced.

2.3.5. Defense Mechanism

Various countermeasures had been adopted and still emerging for mitigating against the DDoS attacks. Mostly DDoS attacks are influenced by an intruder attempting to make an unauthorized access in the victim system/network.

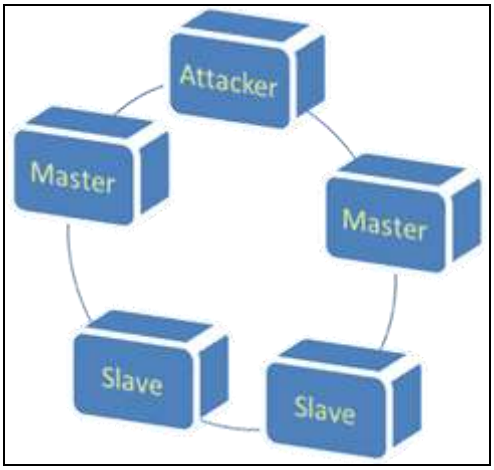

Figure 3

3. Prevention Techniques

The preventive techniques are used to eliminate the possibility of DDoS attacks altogether or to enable legitimate victims to endure the attack without denying the services to targeted clients. With regard to attack prevention, countermeasures can be taken on zombies. This simply means the modification of the system configuration to eliminate the possibility of accepting a Dodos attack or participating unwillingly in a DDoS attack. Hosts should guard against illegitimate traffic from or toward the machine. By keeping protocols and software up-to-date, we can reduce the weaknesses of a computer. A regular scanning of the machine is also necessary in order to detect any "anomalous" behavior. Examples of system security mechanisms include monitoring access to the computer and applications, and installing security patches, firewall systems, virus scanners, and intrusion detection systems automatically. The modern trend is toward security companies that guard a client's network and inform the client in case of attack detection to take defending measures.

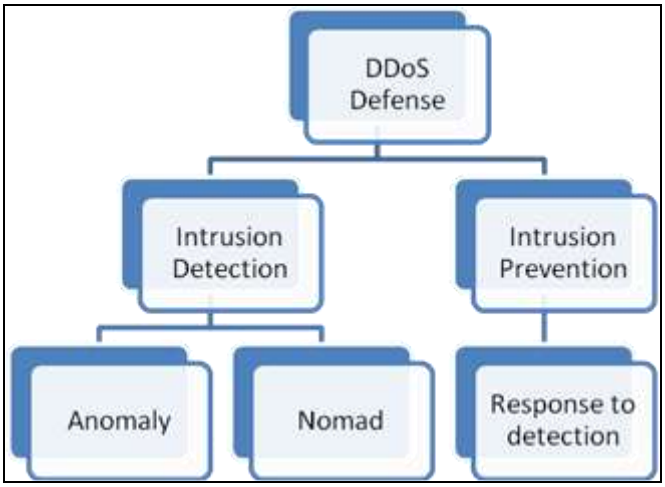

Figure 4

4. Detection Techniques

The intrusion detection system helps the victim system to avoid the propagation of DDoS attacks and prevents it from crashing. From the beginning, all legitimate users have tried to respond against these threats. University communities and software corporations have proposed several methods against the DDoS threat. Despite the efforts, the solution remains a dream. The attackers manage to discover other weaknesses of the protocols and—what is worse—they exploit the defense mechanisms in order to develop attacks. They discover methods to overcome these mechanisms or they exploit them to generate false alarms and to cause catastrophic consequences. The various methods in intrusion detection include:

Anomaly detection: This method is used to detect the attacks by recognizing the abnormal behaviors or anomalies of the system. This detection is done by comparing the current values with previously detected system's performance. This method identify the negativities in the systems behavior. Some of the Anomaly detection techniques are following:

Nomad: A Nomad is a scalable network system that monitors the system and detects the network anomalies and behavior of a system by analyzing the IP packet header information.

5. Response to detection

In case when DDoS attack is detected, the next step to do is the attack should be blocked so that attacker should be traced out for finding out attacker's identity. This can be done within two days, firstly manually using ACL and other is automatically.

5.1. DDOS Attack in Cloud Environment

As discussed in our paper 1, recently the cloud computing has been increased in both academic research and industrial technology. DDoS are one of the security threats that can be challenged to the availability. In Accordance with the Cloud Security Alliance, DDoS attack is one of the top nine threats in cloud computing 4. Out of many attacks in clod environment there are 14% are DDoS attacks. Many of the popular websites like yahoo were affected by DDoS in early 2000. The company was dependent on internet for their production work and business was greatly impacted. Forrester Consulting was contracted by VeriSign in March 2009.The survey was performed among the 400 respondents from the US and Europe 8. 74% that had experienced one or more DDoS attacks in their organizations.

Cloud service consists of other services like that has been provided on the same hardware servers, which may be suffered by workload and can caused by flooding. Thus, if a service try to be run on the same server with different flooded service, this will affect its own availability. Another effect of a flooding in cloud is raising of the bills for Cloud usage drastically. The problem with this is that there is no "upper limit" for the usage 5. As one of the potential attacks to cloud computing is neighbor attacks i.e. Virtual Machine can attack its neighbor in same physical manner or infrastructures and thus prevent it by providing its services. These attacks can easily affect the cloud performance and can cause the financial losses and harmful effect to other servers in the same cloud infrastructure.

5.2. Factors for Selecting Defense Solution

While selecting DDoS solution many things need to be considered:

- Functional: The solution for the attack should be functional enough, which means it should be able to reduce impact of the attack.
- Transpicuous: The solution for the attack must be easy to implement i.e. it should not require the modification of the existing network and its infrastructure as well.
- Lightweight: Most importantly the solution to the attack should not overhead the system's performance.
- Precise: The solution selected for the attack should not give lots of negativity. Many of the methods need the traffic to be discarded and the solution must not drop genuine traffic.

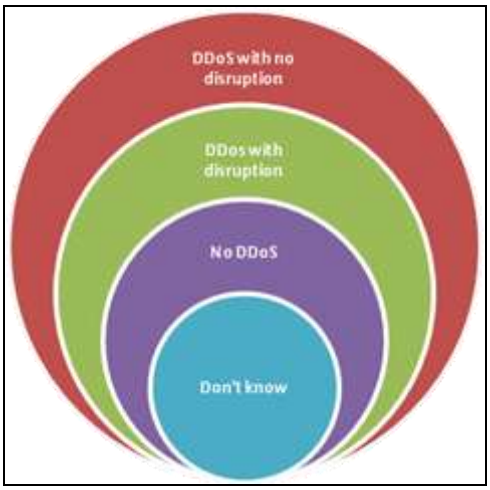

Figure 5

5.3. Proposed Work

Soft computing methods

We can use soft computing techniques and learning paradigms, such as neural networks, radial basis functions and genetic algorithms are increasingly used in DDoS attack detection because of their ability to classify intelligently and automatically. Soft computing is a general term for describing a set of optimization and processing techniques that are tolerant of imprecision and uncertainty.

The detection of DDoS attacks needs adaptive and incremental learning classifier, less computational complexity, and accurate decision making from uncertain information. Hence, the DDoS attacks could be detected using existing soft computing techniques such as fuzzy logic, neural networks, and genetic algorithms. Genetic algorithm provides optimal solutions.

6. Conclusion

As DDoS attacks are the rising attack in cloud computing. This paper provides a brief survey on DDoS attacks, then the taxonomy of attacks, its types and the various counter measures for mitigation of the DDoS attacks. DDoS attacks make a service unavailable to

targeted users. These attacks can be seriously damage a system if a critical system is the used as a primary victim. The proposed method tries to mitigate DDoS attack to reduce its impact on the user system. This survey mainly confers the DDoS detection, prevention and tolerance techniques. The paper concludes by providing some points to be considered while selecting DDoS defense solution.

7. References

i. Rashmi D. and Kailas D. mitigating ddos attack in cloud environment with packet filtering using iptables in International Journal of Computer Engineering and Applications, Volume VII, Issue II, August 14.
ii. T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," in 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), 2010, pp. 2733.
iii. N.Weiler, Honeypots for Distributed Denial of Service, in Proceedings of the Eleventh IEEE International Workshops Enabling Technologies: Infrastructure for Collaborative Enterprises 2002, Pitsburgh, PA, USA, June 2002, pp. 109114.
iv. The Notorious Nine, Cloud Computing Top Threats in 2013, https://downloads.cloudsecurityalliance.org/initiatives/topthreats/TheNotoriousNine CloudComputingTopThreatsin2013.pdf
v. Meiko Jensen, Jorg Schwenk, Nil Gruschka "On technical issues in cloud computing", IEEE International Conference on cloud computing, 2009.
vi. Denial of Service Attack, http://en.wikipedia.org/wiki/Denial-of-service_attack.
vii. B. Grobauer, T.Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," Security Privacy, IEEE, vol. 9, no. 2, pp. 5057,Mar. 2011.
viii. CERT Advisory CA-1998-01, Smurf IP Denial-of-Service Attacks, January 5, 1998, Available: http://www.cert.org/advisories/CA-1998-01.html.
ix. R.R. Talpade, G. Kim, S. Khurana, NOMAD: Traffic based network monitoring framework for anomaly detection, in: Proceedings of the Fourth IEEE Symposium on Computers and Communications, 1998.
x. P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST special publication, vol. 800, no. 145, p. 7, 2011.

.