ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

A Survey and Taxonomy of Dos Attacks in Cloud Computing

Priyanka Gupta, Prof. Pradeep Tripathi

M. Tech Research Scholar, Department of Computer Science & Engineering, Vindhya Institute of Technology and Science - [VITS, SATNA], Madhya Pradesh, India

Professor & Head of the Department, Department of Computer Science & Engineering, Vindhya Institute of Technology and Science - [VITS, SATNA], Madhya Pradesh, India

ABSTRACT: Cloud computing has become popular and a huge computing platform where large amounts of data are available online. The nature of cloud computing is distributed; they have become easy targets for attackers to exploit the vulnerability of security because of this kind of nature. Data availability is the most important part of cloud computing, and even for the society's economic growth.

Cybercrime attacks can take place in different forms. One big form of attack is a denial of service (DDoS) or a Denial of Service (DDoS) distributed. This attack seeks to make a computer or network resource inaccessible to its intended users, such as network bandwidth, data structures, operating system and computing power. Attacks by Distributed Denial of Service (DDoS) continue to plague the Internet. Distributed Denial-of-Service (DDoS) attacks are a major problem because they are very difficult to detect, there is no comprehensive solution, and an organization can be shut off from the Internet.

Identify DDOS Attack Types and Understand Their Impact, Recognize Attack Methods and Secure Organization Against DDoS Attacks is the purpose of this review document. Our proposed method would be able to monitor the effect of DDoS flooding attacks in the next paper we are targeting the use of very few surveillance points.

I.INTRODUCTION

The last few years we have seen that cybercrime is increasing drastically across all regions and sectors. Nature of cybercrime is constantly evolving and attackers having different arsenal for stealing credential of victims. With over 1 billion users today, the Internet has become a conduit for people and businesses to regularly access useful information perform tasks such as banking, and shop at many different retailers. The rise of social media has also rendered the Internet an invaluable place for businesses and other organizations to use for critical branding and other core customer interactions – often generating significant revenue in the process. The downside of all this convenience is vulnerability to disruption. Malicious users are often able to steal information or halt normal computer operation, with motives ranging from industrial espionage and revenge to financial gain and political aims.

DoS and DDoS attacks make news headlines around the world daily, with stories recounting how a malicious individual or group was able to cause significant downtime for a website or use the disruption to breach security, causing financial and reputational damage. Since DDoS (Distributed Denial of Service) attack is one of the techniques mostly often used by cybercriminals. It is estimated that over 7,000 such attacks occur daily and it is intended to reduce an information system, typically a website, to a state where it cannot be accessed by legitimate users. One popular DDoS scenario is a botnet-assisted attack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

II.GENERAL IDEA AND IMPRESSION OF DDOS

Distributed denial-of-service (DDoS) attacks, as the name implies, attempt to deny a service to legitimate users by overwhelming the target with activity. The most common method is a network traffic flood DDoS attack against Web servers, where distributed means that multiple sources attack the same target at the same time. These attacks are often conducted through botnets.

According to a survey by Neustar, 60 percent of companies were impacted by a DDoS attack in 2013 and 87 percent were hit more than once. The most common affected sectors are the gaming, media, and software industries. The purpose of most attacks is to disrupt, not to destroy. In contrast to targeted attacks, DDoS attacks will not lead to data breaches, but on the other hand, they are a lot easier to conduct. Attackers can rent DDoS attack services for as little as $5, letting them conduct a few minutes-worth of DDoS attacks against any chosen target.

Hacktivist groups often use flooding attacks as a political protest and generate media attention. One example of a hacktivist group is the al-Qassam Cyber Fighters, which attacked US financial institutions. DDoS attacks are also used by cybercriminals to extort money from online services, by gamers to settle disputes, or as diversions during targeted attacks. For the first half of 2014, most DDoS attack traffic originated in India, followed by the United States. One reason for this might be the large number of badly configured servers that can be misused for amplification attacks and the high number of bots [1].

DDoS attacks often cause collateral damage to companies close to the real target. Once the bandwidth fills up, any site hosted by the same provider may not be accessible through the Internet. As a result, these sites might face downtime even if they were not directly targeted.

DDoS attacks are not a new concept, but they have been proven to work and can be devastating for companies. There is no way to prevent a DDoS attack, but there are some ways to mitigate its impact to the business. The most important step is to be prepared and have an action plan ready. Such DDoS attacks have grown larger year over year.

In 2014-15, the largest attack volume peaked at 300 Gbps. So far in 2015, we have already seen one attack with up to 400 Gbps in attack volume. In recent times, DDoS attacks have become shorter in duration, often lasting only a few hours or even just minutes. According to Akamai, the average attack lasts 17 hours.

These burst attacks can be devastating nonetheless, as most companies are affected by even a few hours of downtime and many business are not prepared. In addition to the reduced duration, the attacks are getting more sophisticated and varying the methods used, making them harder to mitigate.

III.BACKGROUND

Cloud computing is becoming a more and more accepted solution for hosting the information resources of organizations across the globe, with no physical deployments needed at the client's side. Instead every needed service can be made available as a subscription-based service [2][3].

The Internet community has been facing the DoS problem for over two decades. One of the earliest known DoS attacks occurred in 1974 at the Computer-based Education Research Laboratory (CERL).

A few years ago, DDoS attacks were mostly conducted using large botnets to directly flood the target with traffic. Now, we often see the use of amplification attacks through open third-party services or botnets of hijacked servers, which have more bandwidth than compromised computers. But common botnets still play an important role in DDoS attacks.

In the past, many DDoS bots were controlled through Internet Relay Chat (IRC) channels. In recent years, most attackers have moved to using HTTP-controlled command servers or have even started using peer-to-peer (P2P) networks to make their attack infrastructure more resilient against takedowns.

3.1 DoS attack and defense mechanisms:

A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent the legitimate users

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

of a service from using the service provided by a network or server. It can be launched in several ways, but this project is focused in two of them. The first aims at crashing the system by sending crafted packets that exploit software vulnerability in the target system. The other way is by sending massive volumes of useless traffic to overwhelm and occupy the resources that could service legitimate traffic [4].

3.1.1 DoS and DDoS Attacks

The volume of traffic for the attack must be large enough to consume the target's resources. In order to deny services and accomplish more complicated attack detection, the attack is carried out through multiple sources. This variant of DoS attack is known as DDoS (Distributed Denial of Service) attack. A typical DDoS attack contains three mai n elements as shown in Figure 2.1. First of all, the attacker selects a set of vulnerable systems (zombies) and sets up attack systems in them. Once the attack mechanisms are installed, the attacker can launch attack commands to the zombies through a secure channel to carry out the DoS attack on the victim.

The complexity of the attack increases due to the zombies modifying the packets, commonly spoofing the source. As a consequence, it becomes even more difficult to trace the origin of the attack. Zombie systems, also known as bots and the structure of elements the attacker can launch to attack systems over them, and carry out joint attacks is commonly known as botnet. An important feature of botnets is the ability to update software from the attacker through the security channel between the attacker and the bots.

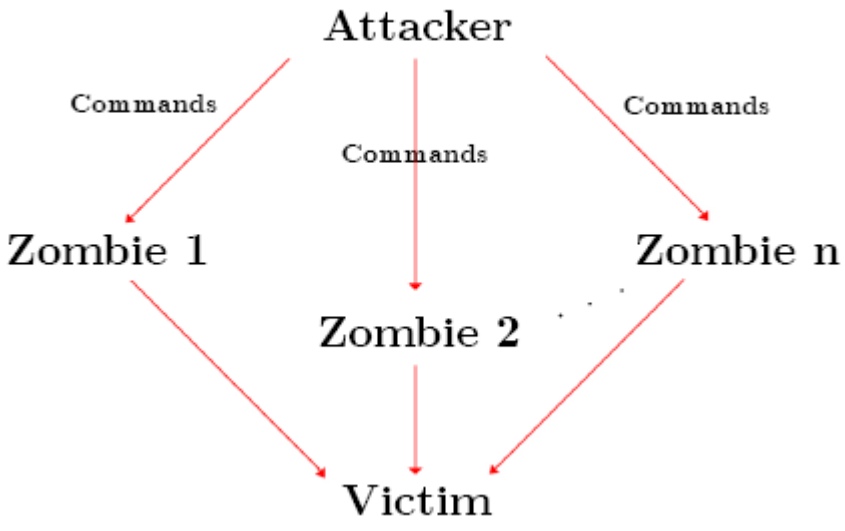

Figure 3.1: DDoS Attack Structure

3.1.2 Attack Taxonomy

In order to devise a taxonomy of DDoS attacks, we have to take into account some features of the attacks, as well as the means used to prepare and perform the attack, the characteristics of the attack itself and the selection and the effec ts upon the victim. In this survey, we will focus on selected attacks depending on the victim type, classifying them as Protocol Attacks, Bandwidth Attacks or Logic Attacks.

There are already some other taxonomies to explain all aspects in greater detail [5];

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

a. Protocol Attacks

The attacker continuously sends packets to the server at a particular rate to take advantage of the inherent design of common network protocols. In other words, these attacks try to exploit the weaknesses of the system, considering the expected behavior of protocols such as TCP, UDP, and ICMP. SYN Flooding Attacks flood the server, by sending SYN packets that consume its resources and fill up the backlog.

A UDP Flood attack is another protocol attack which aims at bringing down the server by sending UDP packets to a random port in the target. For a large number of UDP packets, the target will be forced to send back ICMP packets, but to a unreachable destination [6]. Other examples are Smurf Attacks [7] and ICMP Attacks.

b. Bandwidth Attacks

High-data-volume attacks can consume all available bandwidth between an ISP and a target. The ISP networks need to have a high capacity due to the heavy traffic that they have to route from many resources to many destinations. The connections between the ISP and the victim usually have less capacity than the ones inside the ISP, so when high volumes of traffic coming from the ISP go through these connections, the links fill up and legitimate traffic slows down.

An attacker can consume bandwidth by transmitting any traffic to all the network connection. For example, high volumes of simple ICMP packets to consume the bandwidth [8].

c. Logic Attacks

In Logic or software attacks, a small number of malformed packets exploit known specific software bugs in the operating system or in an application of the target system. This can potentially disable the victim's machine with one or multiples packets. These attacks are relatively easy to avoid either through the installation of software that eliminates vulnerabilities or by adding specialized filter rules to filter out malformed packets [9].

In ping of death attack, the attacker sends a ping message with the packet size over the limit (656536 octets) so that it is allowed to be retransmitted over the Internet. Other examples are land attacks, Teardrop Attack [6].

3.2 Defense Classification:

a. Attack Prevention:

Its objective is to stop attacks before they actually cause damage. This type of category tries to deny traffic that can be recognized as malicious, based on known patterns. The best place to allocate these mechanisms is in the edge routers and hosts, which implies fixing all the vulnerabilities of all Internet hosts that can be misused for an attack. Like;

- Filtering: This measure implies installing ingress and egress packet filters on all the routers.
- Firewall: Before an attack is carried out, a firewall might be useful to filter out traffic according to the protocol, ports or incoming IP addresses.
  But, the problem is that firewalls cannot distinguish between an attack and legitimate traffic, and denying all traffic for a specific port or protocol is not suitable.

b. Attack Detection:

Once the attack is in process, an attack detection mechanism must recognize if it is actually an attack or just legitimate traffic.

i. **Pattern Detection:**

An attack can constantly be detected by comparing incoming traffic with known attacks signatures stored in a database.

Problems arise when there are new attacks or slight variants that can dodge the defense.

SNORT [11] and Bro [10] are two commonly used pattern detection approaches.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

ii. **Anomaly Based Detection**:
It identifies malicious activity in a network by detecting anomalous network traffic patterns such as size of the packet, since those being too short violate specific application layers protocols.

c. Attack Source Identification:

Once an attack is detected, the best response is to block the attack traffic at its source. But problem arias when IP source addresses can be forged easily by attackers. The second is the stateless nature of IP routing, where routers normally know only the next step for forwarding a packet [12].

d. Attack Reaction: Attack reaction tries to eliminate the effects of an attack and filter the attack traffic without disturbing legitimate traffic.

i. Filtering dropping the traffic considered as unwanted or malicious is an effective way to prevent a DDoS attack. The problem is that some attacks use well-formed packets and legitimate requests to servers, making them non filterable.
Dropping spoofed incoming packets by ingress filtering, identifying and dropping packets based on the change of the time-window-size, saving proved previously legitimate IPs [13], are some of the attack reaction mechanisms based on filtering.

ii. Rate limiting The rate of malicious traffic packets is reduced with this technique when there is a high number of false positives.

IV.DDOS ATTACKS TOOLS

One of the major reason that make the DDoS attacks wide spread and easy in the Internet is the availability of attacking tools and the powerfulness of these tools to generate attacking traffic. There are a variety of different DDoS attack tools on the Internet that allow attackers to execute attacks on the target system [14].

DDoS attack tool	Commands used	Types of Attacks Generated	Communication Methods
Trinoo [15,16]	Not encrypted	UDP flooding	Attacker to master-unencrypted TCP Master to slave- unencrypted UDP Slave to master - unencrypted UDP
TFN[17]	Numeric code and not encrypted	ICMP flooding TCP flooding UDP flooding Smurf	Attacker to master -required third-party program Master to slave- unencrypted ICMP Slave to master - none
TFN2K[18]	Encrypted	ICMP flooding TCP flooding UDP flooding Smurf Mix flood	Master to slave- can be mixture of encrypted TCP, UDP and ICMP Slave to master - none

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

Stacheldraht [19]	Encrypted	ICMP flooding TCP flooding UDP flooding Smurf	Attacker to master -encrypted TCP Master to slave- TCP and ICMP Slave to master - none
Shaft[20]	Not encrypted	ICMP flooding TCP flooding UDP flooding Mix flood	Attacker to master -unencrypted TCP Master to slave- unencrypted UDP
Mstream[21]	Not encrypted	TCP flooding	Attacker to master -unencrypted TCP Master to slave- unencrypted UDP Slave to master - unencrypted UDP
Trinity [22,23]	Not encrypted	TCP flooding UDP flooding	Uses IRC as it's communication method

V.DDOS PREVENTION MECHANISMS

Attack prevention methods try to stop all well known signature based and broadcast based DDoS attacks. Attack prevention schemes are not enough to stop DDoS attacks because there are always vulnerable to novel and mixed attack types for which signatures and patches are not exist in the database. To defend against DDoS attack in cloud computing there are several mechanisms that discussed in following section [24].

5.1 CTB Model to defend against DDoS attacks:

One method is using of Cloud Trace Back (CTB) and Cloud protector. CTB would be utilized in both LAN and Grid network structure. The purpose of having CTB in our cloud network is to have ability to trace back the source of these attacks and also make use of a neutral network named cloud protector is to detect and filter such attack traffic.

CTB and Cloud Protector are located between the each cloud web service to defense against XML based DDOS attack. This method gave ability to cloud networks for detecting and filtering most of the attack's bases on DDoS. Fig. 1 shows the CTB place in the cloud environment [25].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

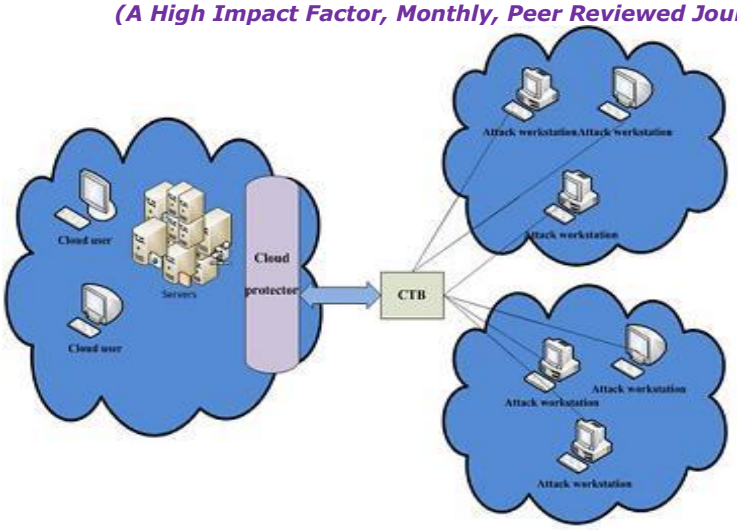

Fig. 5.1 CTB and Cloud Protector

5.2 Distributed Cloud Intrusion Detection Model:

Using Intrusion Detection System in Virtual Machine for securing cloud networks against DDoS attacks is another method for solving this problem. IDS located on the virtual switch and gave ability to system to log the network traffic inbound and out bound through the database for auditing. Intrusion detection system examined all packets to find a type of attack base on predefined rules. Virtual server by getting the help of IDS could be able to recognize the security risks involved in such attacks.

Using this method to defend against DDoS attack in the cloud could be fed away most of the problem. To have an effective IDS with ability of working in the cloud the proposed model is based on a Distributed cloud IDS which uses of multi-multi-threading method for enhancing IDS performance over the cloud infrastructure.

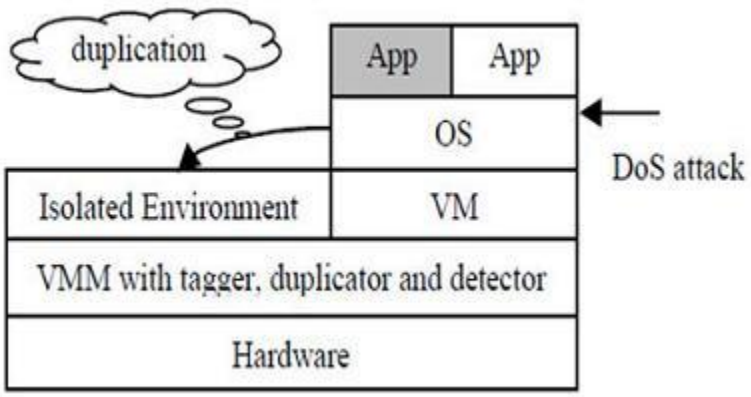

Fig. 5.2 Proposed model by using VMM

5.3 A Filter Tree Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS Attack:

A Filter Tree approach was proposed to protect cloud against HTTP-DDoS and XML attacks. They present a cloud defender with three steps between client and service provider and tried to stop attacking before catch the cloud. This method use IP addressed to recognize and trace back the illegitimate VMs.

Cloud defender is included five steps such as sensor filtering, Hop counts filtering, IP Frequency Divergence Filter, Confirm legitimate user IP Filter, and Double Signature

Filter. Fig. 5 showed the proposed model.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

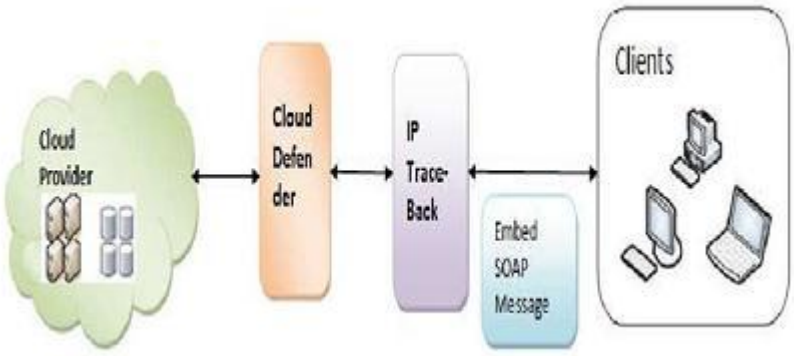

Fig.5.3 Filter Tree approach

5.4 Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing and SAVE (Source address validity enforcement) protocol

It comes under Source-based mechanisms which are deployed near the sources of the attack to prevent network customers from generating DDoS flooding attacks. Some examples of source-based mechanisms include ingress/egress filtering, which filters packets with spoofed IP addresses at the source's edge routers based on the valid IP address range internal to the network, and Source Address Validity Enforcement (SAVE) Protocol. SAVE protocol enables routers to update the information of expected source IP addresses on each link and block any IP packet with an unexpected source IP address [26].

5.5 Hop Count Filtering:

Hop-Count Filtering is use to weed out spoofed IP packets at the very beginning of network processing, thus effectively protecting victim servers' resources from abuse. The rationale behind hop-count filtering (HCF) is that most randomly spoofed packets, when arriving at victims, do not carry hop-count values that are consistent with the IP addresses being spoofed. The hop-count information is indirectly reflected in the Time-to-Live (TTL) field of the IP header, since each intermediate router decrements the TTL value by one before forwarding a packet to the next hop but there is a possible hop-count instability. Otherwise it is one of good mechanism against DDOS attacks [27].

5.6 The TCP-Based DDoS Attack:

Most DDoS attacks exploit TCP control packets by spoofing the three-way handshake between the source and the destination server [28]. In this section we analyze the behavior of TCP control packets first in a normal three-way handshake and then in a spoofed three-way handshake. If a source host spoofs its IP address, it will be unable to finish a three-way handshake.

This solution works well to prevent source spoofing at end systems, but attackers are free to spoof the source address of the first packet of a three-way handshake, and they can launch DoS flooding attacks with these packets.It is major drawback of given solution.

5.7 Cloud Computing Security Model to Detect and Prevent DoS and DDoS Attack based on based watermarking technology [29]

It detects and prevents DoS attack will work on following principles:

1) Once packet will reach to the network, source of the packet will be identified.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

2) Traceback mechanism should be used to check the authenticity of source address by using Hop Counts and TTL.
3) If the source cannot be verified, packet will be marked as untrusted and will be dropped without sending it to internal network.
4) Each packet coming from same untrusted source will be grouped together based on source authenticity.
5) If the source is verified, anomaly of the data packets and connection mechanism should be checked against "knowledge based database". Any suspicious data packets should be sending to Firewall or IPS for in depth investigation to reduce the rate of false positive or false negative response.
6) Based on known attack type, packet and source should be marked as untrusted and drop the packet on edge of the network.
7) Only "trusted" packets should be marked and passed to the internal network.

VI.CONCLUSIONS

Efficiency and scalability are the key requirements in design of defense against DDoS Attacks. In this paper illustrate study of various DDOS attack techniques and prevention techniques. The survey of the all relevance detection and defense techniques against DDoS, we can conclude that methods are differ in their region of action, the amount of legitimate traffic they drop and the type of attack they are effective against. Each method has certain features and drawbacks.

Cloud computing is a fast growing network and becoming the dominant part of today's internet and along with data security, availability is also the important part of it. Therefore it is very necessary to provide effective way of Detection and Prevention mechanism for the attack which targets the availability of cloud.

REFERENCES

[1] Candid Wueest, "The continued rise of DDoS attacks" Security Response by Semantec, Version 1.0 – October 21, 2014.
[2] J. Li and Y. Yang, "Design and Realization of a Large-scale Distributed Intrusion Management," in IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008, pp. 537-540.
[3] R. Maggiani, "Cloud Computing is Changing How We Communicate," in IEEE International Professional Communication Conference, Waikiki, HI, 2009, pp. 1-4.
[4] Peng, T., Leckie, C., and Ramamohanarao, K. Survey of network-based defense mechanisms countering the dos and ddos problems. ACM Computing Surveys (CSUR) 39, 1 (2007), 3.
[5] Specht, S. M., and Lee, R. B. Distributed denial of service: Taxonomies of attacks, tools, and countermeasures. In ISCA PDCS (2004), pp. 543-550.
[6] Gupta, B., Joshi, R. C., and Misra, M. Defending against distributed denial of service attacks: issues and challenges. In formation Security Journal: A Global Perspective 18, 5 (2009), 224-247.
[7] Advisory CA-1998-01., C. Smurf IP Denial-of-Service attacks. http: //www.cert.org/historical/advisories/CA-1998-01.cfm? [Online; accessed 01-Dec-2013].
[8] Bellovin, S. M., Leech, M., and Taylor, T. ICMP trace back messages. Internet Engineering Task Force, Marina del Rey, Calif (2003). [9] Molsa, J. Mitigating denial of service attacks: A tutorial. Journal of computer security 13, 6 (2005), 807-837.
[10] Paxson, V. Bro: a system for detecting network intruders in real-time. Computer networks 1, 23 (1999), 2435-2463. [11] Roesch, M., et al. Snort: Lightweight intrusion detection for networks. In LISA (1999), vol. 99, pp. 229-238.
[12] Peng, T., Leckie, C., and Ramamohanarao, K. Survey of network-based defense mechanisms countering the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 1, January 2020

dos and ddos problems. ACM Computing Surveys (CSUR) 39, 1 (2007), 3.
[13] Peng, T., Leckie, C., and Ramamohanarao, K. Protection from distributed denial of service attacks using history-based ip ltering. In Communications,
2003. ICC'03. IEEE International Conference on (2003), vol. 1, IEEE, pp. 482-486.
[14] B. B. Gupta, Student Member, IEEE, R. C. Joshi and Manoj Misra, Member, IEEE "Distributed Denial of Service Prevention Techniques"
International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010.
[15] J. Mirkovic, P. Reiher, "A Taxonomy of DDoS Attack and DDoS defense Mechanisms," ACM SIGCOMM Computer Communications Review,
Volume 34, Issue 2, pp. 39-53, April 2004.
[16] D. Dittrich, "The DoS Project's Trinoo Distributed Denial of Service attack tool," University of Washington, October 21, 1999. Available at:
http://staff.washington.edu/dittrich/misc/ trinoo.analysis.txt.
[17] D. Dittrich, "The Tribe Flood Network Distributed Denial of Service attack tool," University of Washington, October 21, 1999.
[18] J. Barlow, W. Thrower, "TFN2K- An Analysis," Axent Security Team. February 10, 2000. Available at:
http://security.royans.net/info/posts/bugtraq_ddos2.shtml.
[19] D. Dittrich, "The Stacheldraht Distributed Denial of Service attack tool," University of Washington, December 1999. Avai lable at:
http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt.
[20] S. Dietrich, N. Long, D. Dittrich, "Analyzing Distributed Denial of Service tools: The Shaft Case," in Proceedings of the 14th Systems
Administration Conference (LISA 2000), New Orleans, LA, USA, pp. 329-339, December 3–8, 2000.
[21] D. Dittrich, G. Weaver, S. Dietrich, and N. Long, "The "Mstream" distributed denial of service attack too," May 2000. Available at:
http://staff.washington.edu/dittrich/misc/mstream.analysis.txt.
[22] B. Hancock, "Trinity v3, a DDoS tool," hits the streets, Computers Security 19(7), pp. 574, 2000.
[23] M. Marchesseau, „Trinity-Distributed Denial of Service Attack Tool," 11 Sept, 2000. Available at: http://www.giac.org/ certified_professionals/practicals/gsec/0123.php.
[24] Sarah Farahmandian "A Survey on Methods to Defend against DDoS Attack in Cloud Computing"
ISBN: 978-1-61804-162-3 [25] Chonka, A. and Y. Xiang, Protecting Cloud Web Services from HX-DoS
attacks using Decision Theory. 2012.
[26] J. Li, M. J., M. Wang, R. P., and L. Zhang, "SAVE: Source address validity enforcement protocol," in Proc. IEEE INFOCOM'02, vol. 3, 2002, pp.1557–1566.
[27] W. Haining, et al., "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," Networking, IEEE/ACM Transactions on, vol. 15, pp. 40-53, 2007
[28] Bin Xiao, Wei Chen, Yanxiang He, "A Novel approach to detecting DDoS attacks at an early Stage". In Springer Science + Business Media LLC 2006.
[29] Masudur Rahman, Wah Man Cheung "A Novel Cloud Computing Security Model to Detect and Prevent DoS and DDoS Attack" IJACSA, Vol. 5,No. 6, 2014.