ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

An Effective DPM Method to Detect DDOS Attacks and to Prevent it in Cloud

Sanket P Patil, Yogesh S Patil

M.E. [CSE] Student, Shri Santh Gadgebaba COET, Bhusawal, Maharastra, India

Assistant Professor, Dept. of CSE, Shri Santh Gadgebaba COET, Bhusawal, Maharastra, India

ABSTRACT: Cloud computing has become popular and a huge platform for computing where large number of data are available online. Nature of cloud computing is distributed; due to this kind of nature they have become easy target for attackers to exploits the security vulnerability. Availability of data is most important part of cloud computing and even for economic growth of the society.

Cybercrime attacks can occur in various form. One major type of attack is a denial-of-service (DDoS) or distributed denial-of-service (DDoS). This attack attempts to make a machine or network resource unavailable to its intended users like bandwidth of network, data structures, operating system and computing power. Distributed Denial of Service (DDoS) attacks continue to plague the Internet. Distributed Denial-of-Service (DDoS) attacks are a significant problem because they are very hard to detect, there is no comprehensive solution and it can shut an organization off from the Internet.

So objective of this review paper is identify DDOS Attack Types and Understand Their Effects, Recognize Attack Tools and Protecting Organization Against DDoS Attacks. In next paper we are targeting use of very few surveillance points, our proposed method would be able to monitor the effect of DDoS flooding attacks.

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.

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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

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 conducts 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.

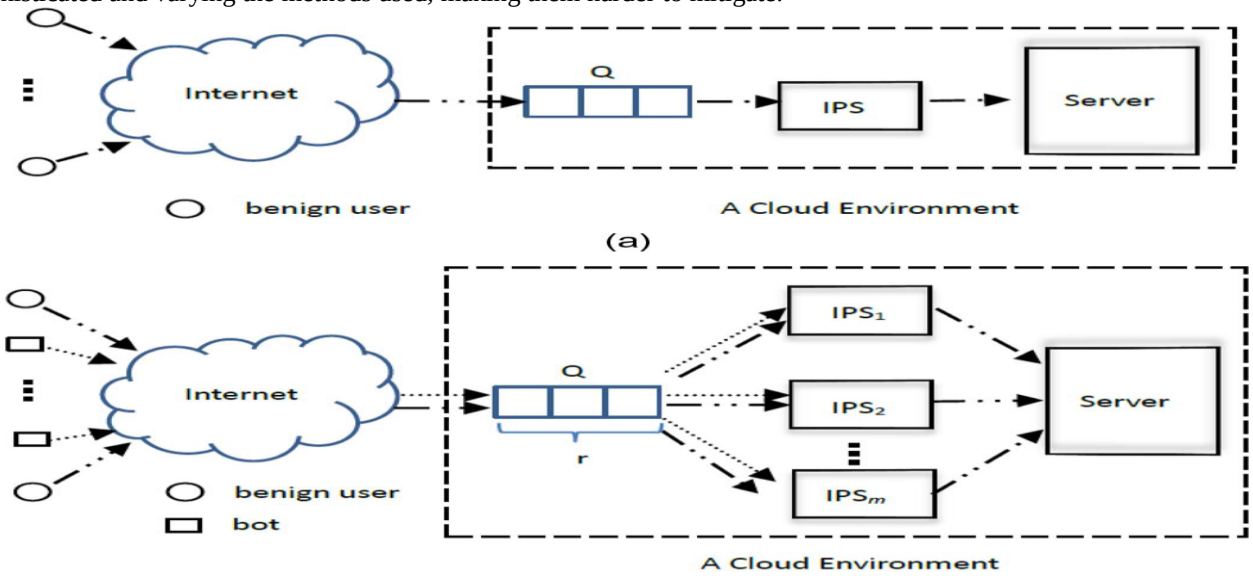

Fig1: DDoS attack scenario in Cloud.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

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 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 Attack Taxonomy

In order to devise 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 effects 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];

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.

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.

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].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

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.

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.

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. 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.

1. Developed DDOS Prevention Mechanisms:

DDOS Prevention Mechanisms (DPM) 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].

A. Developed Preventive Mechanism against DDOS Attack

One of the complicacy to have effective defense against DDoS is identify the attacked traffic separately than genuine (Original) traffics. Attackers normally use many spoofed IP addresses to attack the system, therefore it become resource consuming to check each of the data packets. In case of DDoS attack, large volume of data will be coming from certain hosts. If the source IP has been forged, the type of data will be identical for most of the cases. Using TTL or hop counts, data packets can be grouped as trusted or untrusted.

Following DDOS Prevention Architecture diagram gives flow of developed system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

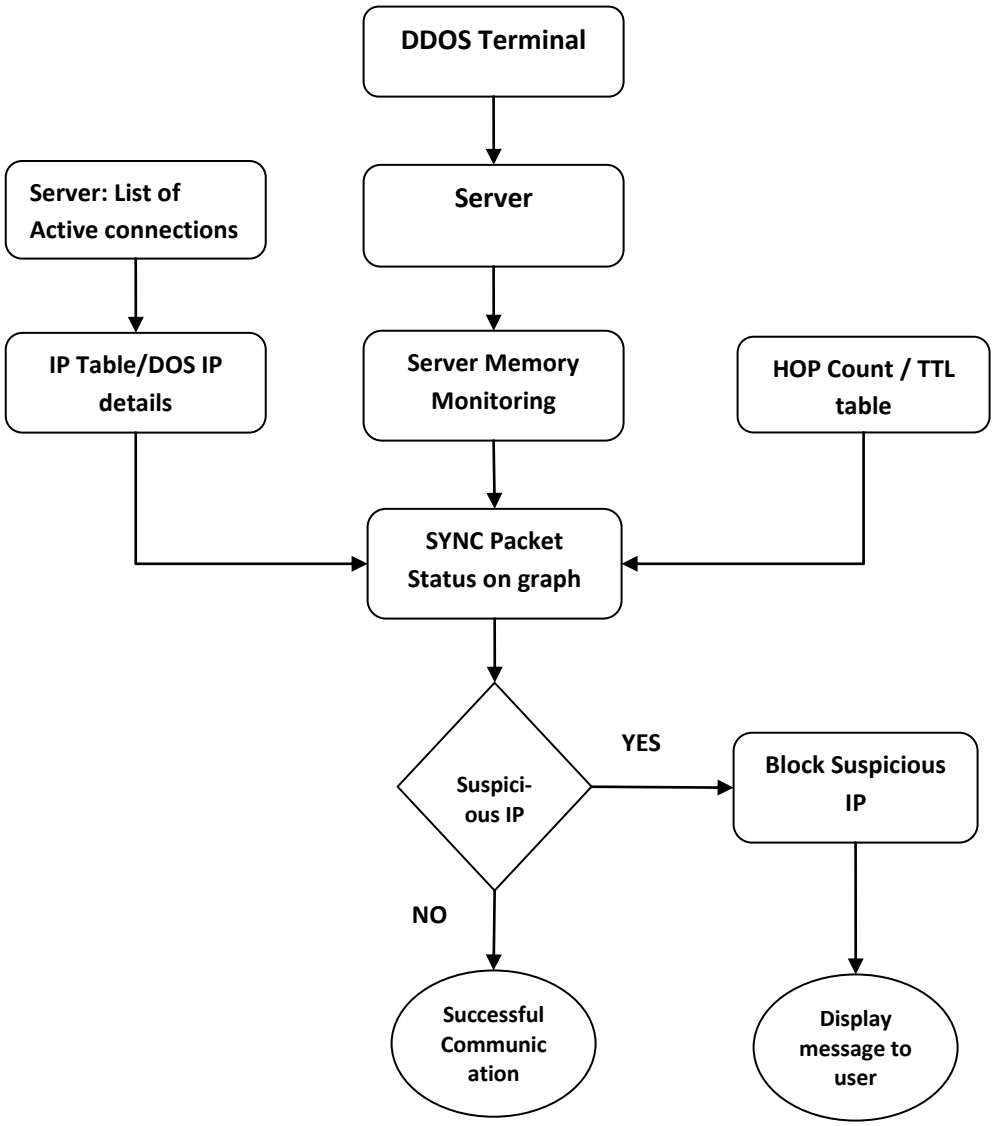

Fig 2: Architecture diagram of prevention DDOS attacks in Cloud.

To perform this operation, DDOS Prevention Mechanisms (DPM) can be used. DPM uses trace back mechanism by using hop count i.e. path between source (user) and destination (server) as well as it uses Time to Live (TTL) to test the authenticity of source of data, irregularity of the type of data and classify the source/data as trusted or untrusted.

DPM also maintains a table of incoming data IP, which can use certain cache timing, so that traffic from certain host is not blocked permanently. After certain time, DPM will check the incoming data packets from specific host or IP again as that might be a genuine host machine which will be allowed to be live, at the same time will also find out non-genuine/unwanted IP which should be blocked and that DPM blocks the attacks.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

It also provide memory consumption graph which indicates traffic on network if untrusted DOS attckes takes place on server it suddenly shows hype or jump in graph in the form of wave. DPM continuously monitor the activity of DDOS attacks. It also monitor used and free space memory graph.

It list of all SYN count on server. It finds out how many active SYNC-REC are accruing on server. In normal function, that count is very less. Here we are considering pretty count i.e. 5 in normal situation. Due to the nature cloud computing, when DDOS attcks takes place in cloud, that pretty count drastically increase for making unavailable server to its intended user.

Sometimes due to attacker's worm, Unwanted/DOS attacks can be compromised. This updated table of trusted and untrusted hosts will be checked again after stipulated time and DPM checks the functioning of IPs. If it found DOS motive, it blocks that compromised IP also and DMP send the traffic to the right destination. So our developed DPM is able to protect system from TCP SYN attack also.

Specific DPM should be assigned traceback operation to verify the source of information. DPM works as follows;

1. Once packet will reach to the network, source of the packet will be identified.
2. Hop Counts and TTL Traceback mechanism used to check the authenticity of source address.
3. DPM maintain incoming data IP table for certain stipulated time and it updates frequently.
4. If IP table source cannot be verified, packet will be marked as falsehood/untrusted and will be blocked.
5. So DPM maintain IP table as well as untrusted IP source for blocking in future also base on frequent souse IP authenticity mechanism.
6. It also provide memory consumption graph which indicates traffic on network if untrusted DOS attckes takes place on server it suddenly shows hype or jump in graph in the form of wave. DPM continuously monitor the activity of DDOS attacks. It also monitor used and free space memory graph.
7. It list of all SYN count on server. It finds out how many active SYNC-REC is accruing on server. In normal function, that count is very less. Here we are considering pretty count i.e. 5 in normal situation. Due to the nature cloud computing, when DDOS attcks takes place in cloud, that pretty count drastically increase for making unavailable server to its intended user.
8. Developed system DDOS terminal (DPM) provides complete solution for detecting suspicious DOS attacks in cloud and destroy it.
9. Since it optimize the performance of the system by blocking untrusted IP on network which reduce the memory consumption of destination (server) and speedup the system.
10. It list of all IP's count are connected to the server using TCP or UDP protocol in cloud and check on ESTABLISHED connection instead of all connection and display the connection count for each IP.
11. Since DPM is able to send right traffic on right direction.

IV. PERFORMANCE EVALUATION

We have evaluated our DPM system on cloud where we have used Amazon Cloud. Following are steps of execution and evaluation of our system.

1. When we start DPM utility at server side, it shows all DOS IP details. It display all active internet connection with server and only established connections are included and also include active internet connection to the server at port number 80. It is useful to detecting single flood by allowing you to recognize many connections coming from one IP.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

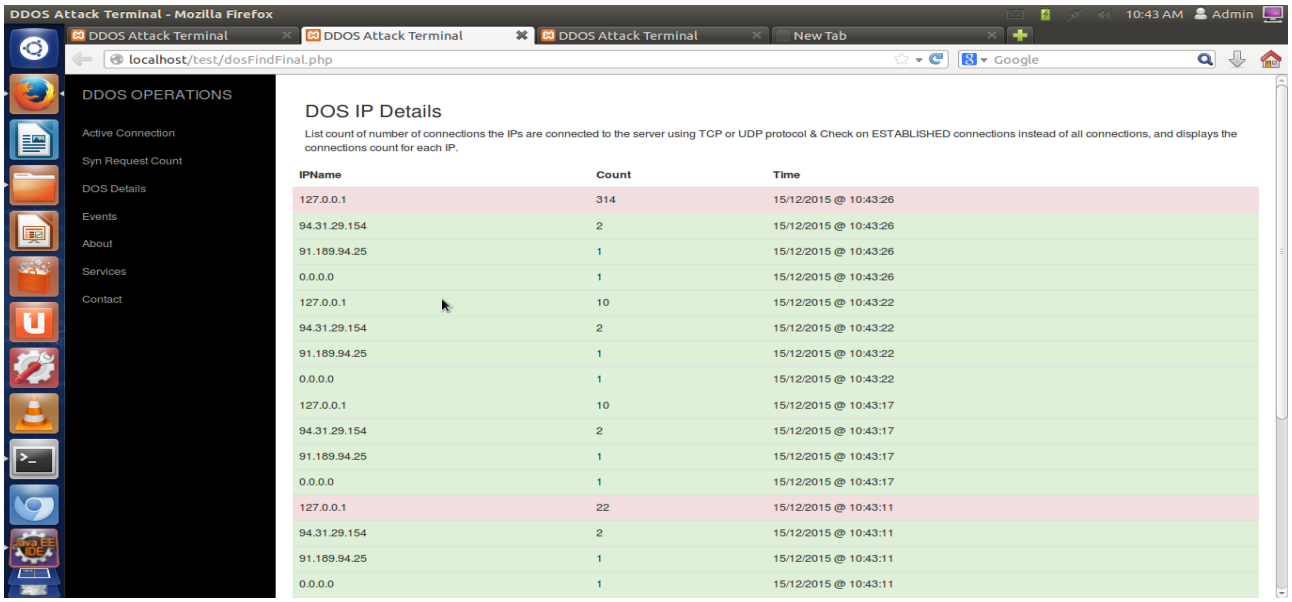

Fig 3: DOS IP Details.

2. DDOS Terminal monitors the IP table which is maintained by our system to recognize suspicious IP. Terminal indicates to the user about server memory status. If there is hike in graph means something suspicious activity happening. Following figure shows details as well as we can observe the difference between following 2 figures 4 & 5.

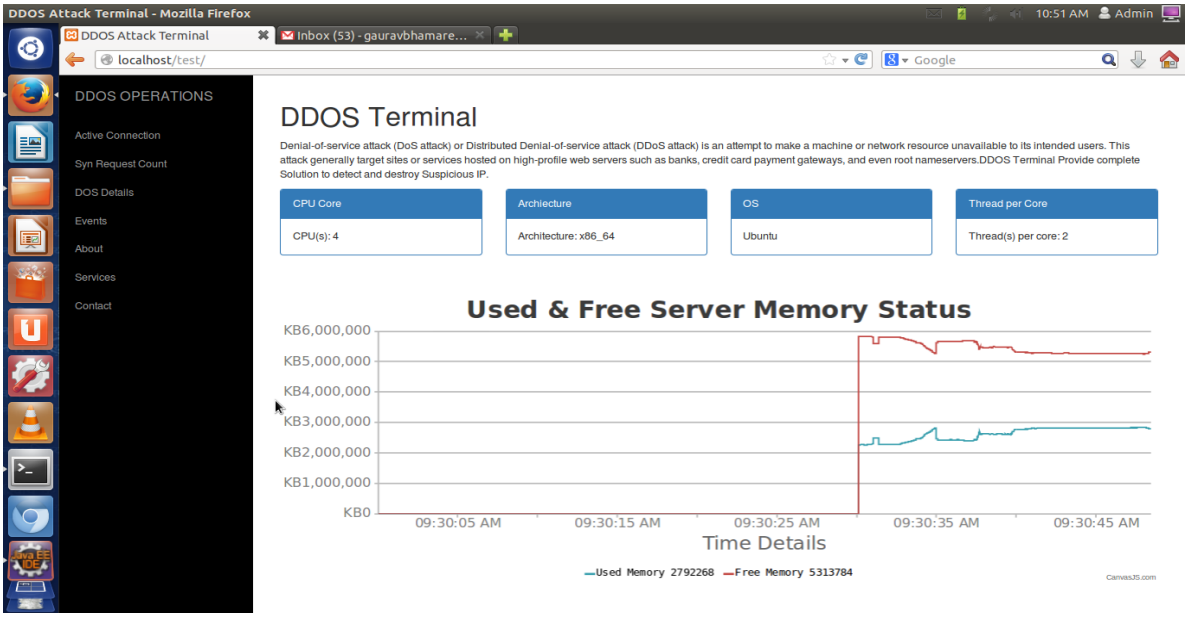

Fig 4: DDOS Terminal.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

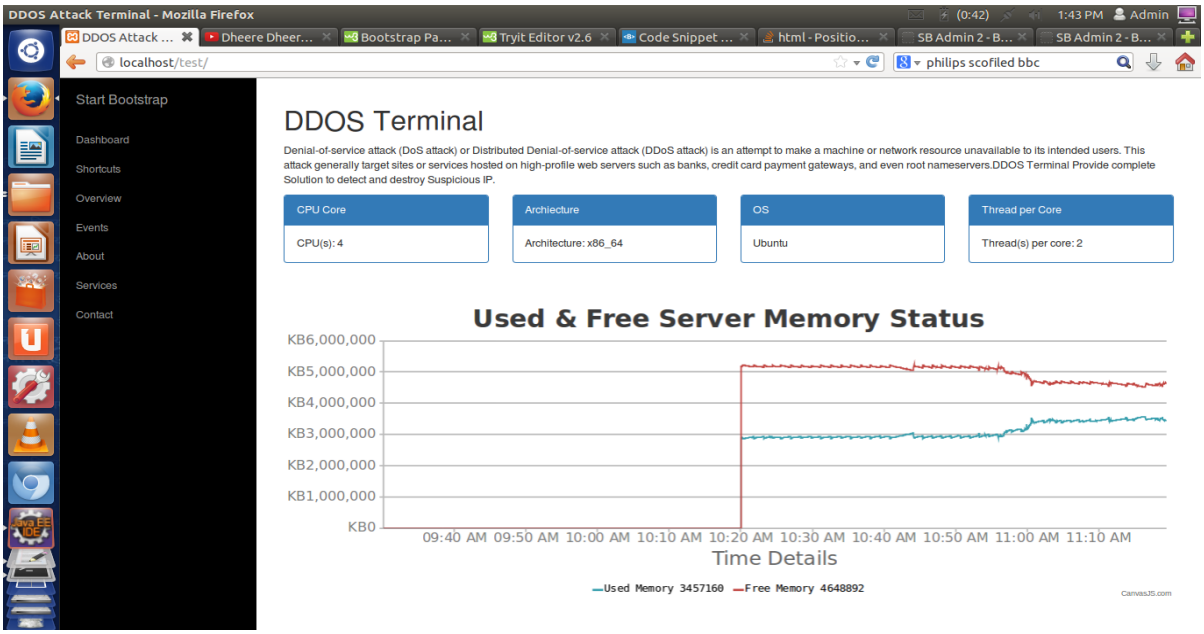

Fig 5: DDOS Terminal.

3. It gives all SYN Count on server. It finds out how many active SYNC-REC is accruing on server. In normal function, that count is very less. Here we are considering pretty count i.e. 5 in normal situation. Due to the nature cloud computing, when DDOS attacks takes place in cloud, that pretty count drastically increase for making unavailable server to its intended user.

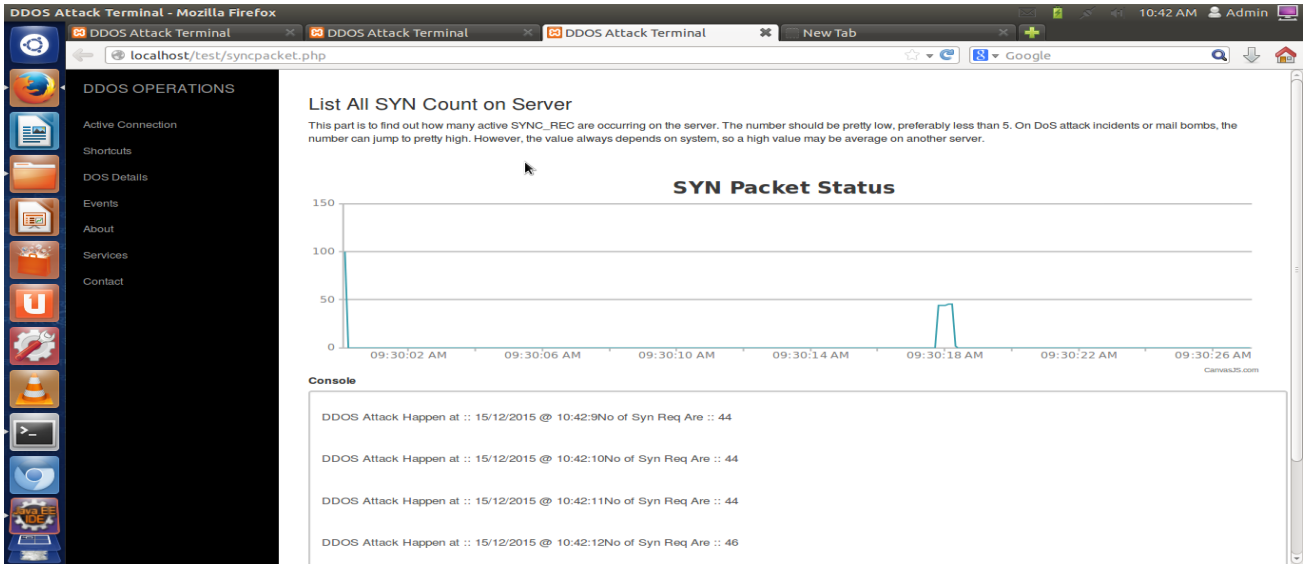

Fig 6: List of all SYN Count on Server.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

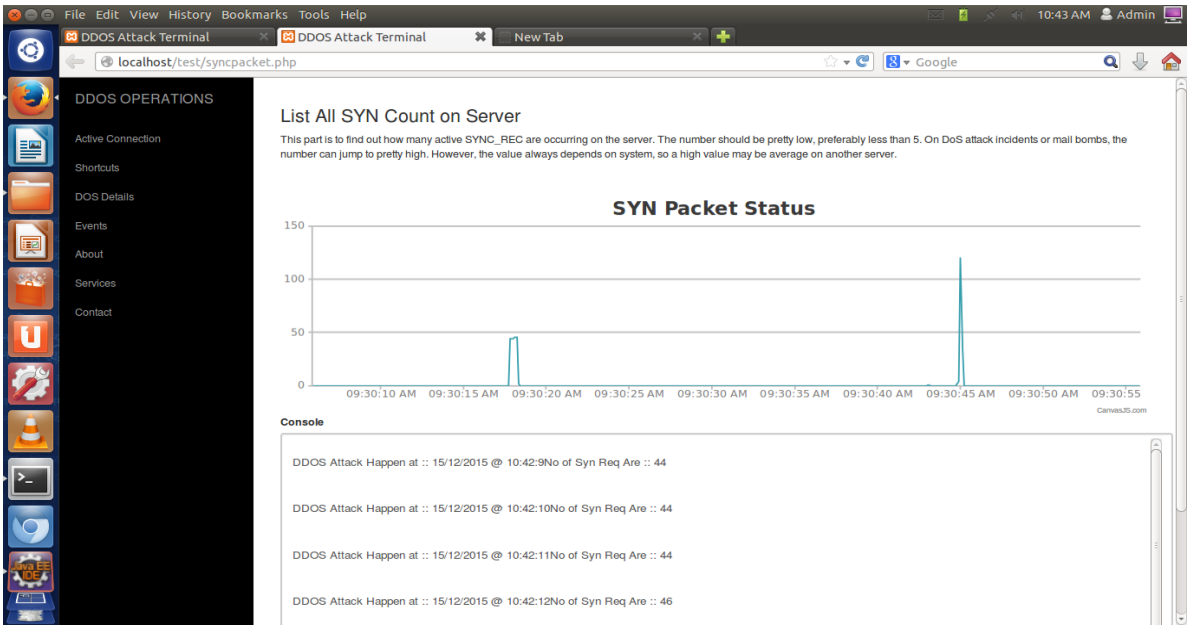

Fig 7: SYN Packet Status and respective wave generation in graph while suspicious IP.

4. It list of all IP's count are connected to the server using TCP or UDP protocol in cloud and check on ESTABLISHED connection instead of all connection and display the connection count for each IP. Since it optimize the performance of the system by blocking untrusted IP on network which reduce the memory consumption of destination (server) and speedup the system.

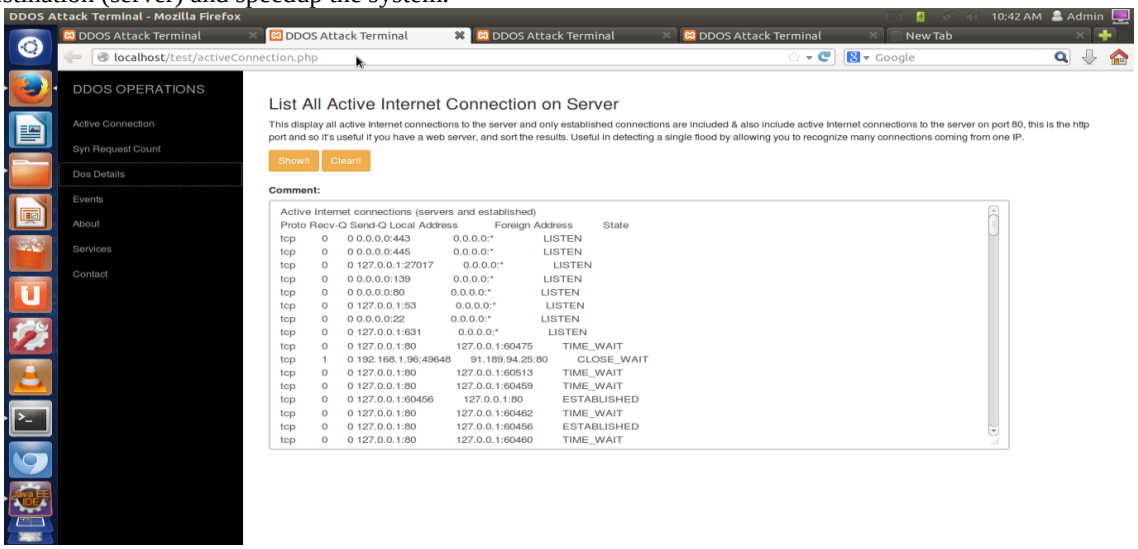

Fig 8: List of all active connection using TCP, UDP.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

V.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.

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. From system evolutions is cleared that DPM is effective in blocking DDoS attacks in cloud environment.

It list of all IP's count are connected to the server using TCP or UDP protocol in cloud and check on ESTABLISHED connection instead of all connection and display the connection count for each IP. Since DPM is able to send right traffic on right direction.

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. Information 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 31, 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 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. Available 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

[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.