Analysis of Detection and Prevention of DDoS Attack in Cloud

[1]Zalak Patel, [2]Prof. Hardik Upadhyay
[1]Computer Engineering, [2]Assistant Professor
[1]IT Systems & Network Security, [2]Computer Engineering
[1]GTU PG SCHOOL, Gandhinagar , Gujarat, India [2] Gujarat Power Engineering and Research Institute, Gujarat, India

***Abstract*—Cloud computing is the most dynamic field used by the IT industry. Most Probably every industry of the public sectors are taking on the cloud computing today, there are many cloud platforms are in demand like, openstack, AWS etc. The cloud has become the most important part of the global infrastructure but there are no borders to safeguard from the critical attacks. In cloud computing, providing the secure and reliable services is the big challenge. DoS and DDoS attacks are the top attacks in the cloud network as it prevents the legitimate users to use the cloud services and sometimes it also can crash the cloud server after having too much requests from unauthorized domains. It causes unavailability of the services to the authorized users. DoS attack is the security breach to make the network resources unavailable to the users by spoofing the IP. This Paper contains the survey about some detection and prevention techniques of DDoS attack in cloud.**

***Index Terms*— Cloud Computing, DoS attack, Distributed Denial of services, Availability**

I. INTRODUCTION

Cloud Computing is the network-based environment which focuses on sharing of network resources, computations, Hardware etc. Clouds are internet-based. It provides the centralized pool of configurable devices, configurable networks. These devices and resources are available through the internet to the users. Advantages of the cloud are scalability, flexibility. Cloud Computing is known for the storage, management, accessing data and information on a particular server.[1] Cloud is becoming the necessary part of the internet , it is necessary for the cloud providers to keep them available. Due to its distributed nature, it has become very easy to attack. The security of the cloud is compromised under the threat of DoS & DDoS attack. [4] DDoS attack is a attack on the availability of the resources or services of a single or multiple systems on cloud.[10] . The biggest problem is to find out the source of the DDoS attack. Due to spoofed packets, the attacker ensures that the hacked computers would remain undetected and further it can be used for the attack. If the origin of the attack remains the stable, it is quite possible to find out and block the particular address and stop the attack. Today, new form of attack which has become distributed. Too many malicious systems synchronically target on targeted server for the attack which makes flood on that server. The attack on the victim by multiple systems will overload networks and systems, so they will deny service to their authorized users.

II. OVERVIEW OF DDoS ATTACK IN CLOUD

DDoS attack is the serious threat [10] in the cloud computing. DDoS attack , which affect on the availability of the resources or services of the single or multiple systems through many compromised victims[9]. The characteristics of the cloud of resource sharing, DDoS is being the serious security threat to such resource pool[9]. This attack is the security breach to make the resources, networks or systems unavailable to its authorized users. DDoS attacks are done by remotely controlled nodes called zombies. Attacker do attack with the help of zombies and targets the victim to make the data unavailable. DDoS attacks are server and cloud infrastructure level attack[10]. DDoS attacks target some kind of resources like, network resources, server resources, application resources.

DDoS Attack Target on Network Resources

Such attacks are attempted to consume the victim's network bandwidth by unwanted traffic which creates flood to prevent the legitimate traffic from reaching the victim's network.

There are some kind of attacks which mostly target the network resources.

Flood Attack : This attack is attempted by sending huge volume of traffic like SYN_FLOOD, UDP_FLOOD to the victim's system with the help of zombies to jam the victim's network with traffic.[8]

DNS Attack : while retrieving server by its name during the translation of a domain name to IP , the victim would be redirected to some cloud server which would be different from name specified.[11]

DDoS Attack Target on Server Resources

This kind of attack is attempted to down the server's capabilities. This attack is launched by taking the advantage of the vulnerabilities of the targeted server.

There are some kind of attacks which target on the servers.

Protocol attack: In this attack , the amount of resources from victim by exploiting the specific feature of the protocol installed on the victim's system. [11]

DDoS Attack Target on Application Resources

This kind of attack is launched by finding the exploit in the application protocol. It is targeted on mostly, HTTP, HTTPS, DNS, SMTP, FTP, etc.

III. CURRENT DETECTION AND PREVENTION MECHANISMS

As per the time, DDoS flooding attack is detected, there should be nothing to be done except to disconnect the victim's cloud server from the network and should be fixed the problem. DDoS attacks mostly waste the resources of the victim's machine, the goal of DDoS detection and prevention techniques to detect the attacks and stop them.[9] Following are some detection and prevention techniques.

Cloud Trace Back Model [1]

The main focus of this module is to give the solution to trace back by Cloud Trace Back to find the source of the DDoS attacks.[1]

Cloud Trace Back.(CTB)

Cloud Trace Back's main objective is to apply SOA technique to trace back method, to identify the source of the DDoS attack.[1] CTB is based on the Deterministic Packet Marking algorithm. All Services requests are sent to the CTB for marking, And there effectively remove the service provider's address which would prevent the direct attack. If attack is successful or discovered at bringing the server down, the victim will be able to recover and reconstruct the CTM tag and the result would be given by revealing the identity of the source.

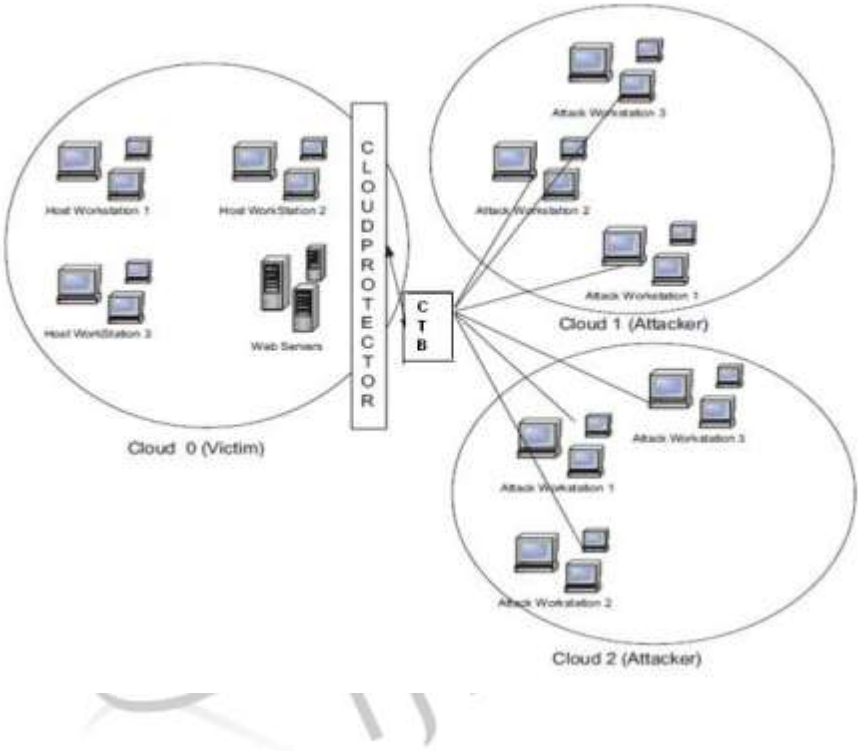


Fig. 1 the Cloud Trace Back Model [1]

SOA Based Trace Back (SBTA) [10]

The main objective of SBTA (SOA based Trace Back)(Service Oriented Architecture) is to trace back and recognize the true source of DDoS in cloud , it is placed within the cloud network by a virtual machine. So, it would be flexible and scalable. All services requests are first sent to the SBTA for marking, then SOAP request message is formulated. If the SOAP requests would be receipt, SBTA will place cloud Trace Back mark tag within the header and it will be sent to the web server. While the message is normal, it will be sent to the to the request handler for the further processing. Web server will prepare a SOAP response which will be sent back to the client by the web server. While the message would be an attack, the victim would recover the cloud Trace back mark and reconstruct from where the attack came on.

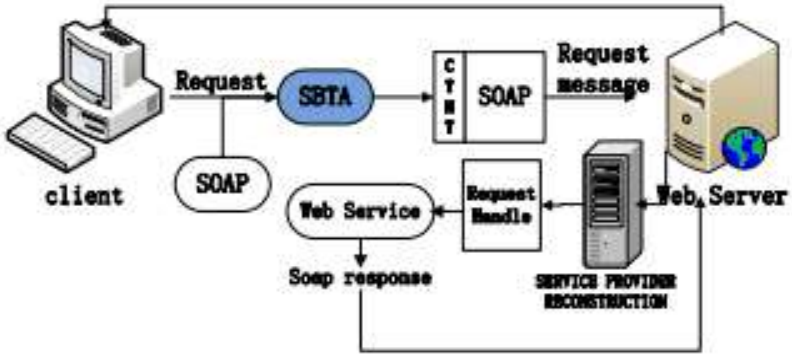


Fig. 2 How SBTA works [10]

VM-Based Intrusion Detection System [14]

VM based IDS are launched, by installation and configuration of snort into each virtual machine. IDS are installed to VM for avoidance of overload and to reduce the attacks. IDS would create the alerts which would be stored in the database which are present in the cloud fusion. Use of single database can reduce the loss of the data. Use of Dempster-Shapher theory in fault tree analysis for VM based IDS will improve the capacity. This technique can reduce the false alerts, can increase detection-rates, by the combination of the information gathered by different sensors.

Hop-Count Filtering Approach(HCF) [6]

Hop Count Filtering is used to recognize the authorized packet and spoofed packet. To calculate the hope count, TTL value is used in the IP Header. TTL is defined for the prevention of the packet from entering in routing loop. If the TTL value is zero, the packet is discarded. So, it can be possible to figure out the Hop-Count with TTL value. Using HCF, a mapping table IP2HC is created. But, it is compulsory to enter the legitimate entries into IP2HC table. [6] HCF works in two phases, learning phase and filtering phase. There is lot of overhead in updating the IP2HC table, as per every incoming packet need to be updated in IP2HC table. This algorithm continues monitor the packets travelling in the network. So it's called packet monitoring technique.

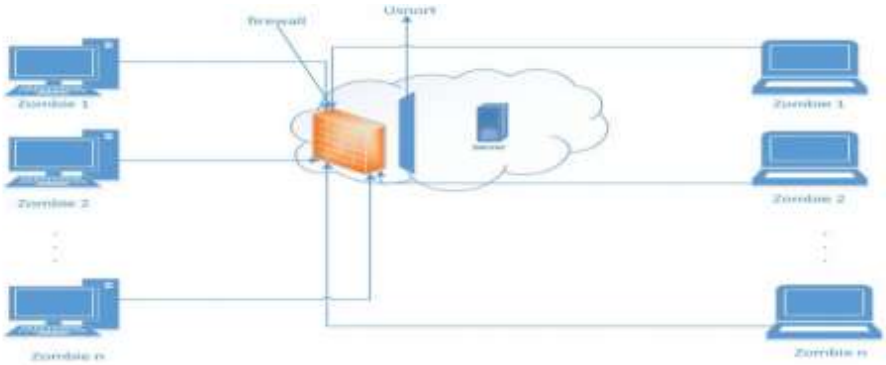
Filter Tree Approach [11]

This approach is used to protect the cloud environment against the application layer attacks.[11] This filter tree approach includes five steps, Sensor filtering, Hop-Count Filtering, IP Frequency Divergence, Double Signature and puzzle Solver.

Distance Estimation Techniques [2]

The mean value of the distance is estimated by using exponential smoothing estimation techniques. The distance Based traffic DDoS detection techniques are based on MMSE (Minimum Mean Square Error) to estimate the traffic rate from the diffident distances.

USnort [12]



Fig, 3 use of Usnort [12]

This tool is an updated version of the Snort. When an attacker attempts the attack on the server, the first thing, the packet will go through the firewall. The firewall is implemented for the protection from malicious attacks. Somehow it bypasses the firewall and tries to get into the server. After that, Usnort comes. Usnort does two things; first, it gives the alert to the admin about the intrusion

with all the relevant data. Second, it drops the connection down with that IP for certain time, so that, the admin can start the recovery plan. So server can be prepared before the attack start infecting it.

IV. CONCLUSION

Cloud is the important part of the fast growing network based on the internet and the availability of the cloud is the most important. To keep the cloud all the time available to the users, it is necessary to have the detection and prevention for the threats which affect on the availability of the cloud. This paper provides the techniques available for detection and prevention for the DDoS attack which are effective. The future work is to find a solution which can successfully detect and prevent DDoS attack in cloud.

REFERENCES

[1] Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi "Securing Cloud Computing Environment Against DDoS Attacks" International conference on computer communication and informatics ,(Jan 10-12),2012.
[2] S.S. Chopade, K.U. Pandey, D.S. Bhade D.M.I.E.T.R, Wardha "Securing Cloud Servers against Flooding Based DDOS Attacks" International conference on communication systems and network technologies , 2013
[3] Shin-Jer Yang and Yu-Zhan Li "Design Issues of Enhanced DDoS Protecting Scheme under the Cloud Computing Environment " International conference on Networking and Network Applications , 2016
[4] Awatef Balobaid, Wedad Alawad and Hanan Aljasim "A Study on the Impacts of DoS and DDoS Attacks on Cloud and Mitigation Techniques " International conference on computing , analytics and security trends (CAST) , 2016
[5] Neeta Sharma, Mayank Singh, Anurajan Mishra, " Prevention against DDos attacks on cloud Systems using Triple filter : An Algorithmic Approach" International conference on computing for Sustainable Global Development ,2016
[6] Waqar Ali , Jun Sang ,Hamad Naeem, "Wireshark window authentication Based Packet capturing scheme to prevent DDos related security issues in cloud network nodes" IEEE Press, 2015
[7] Jeanette Smith-perrone , Jeremy Sims "Securing Cloud, SDN and Large Data Network Environments from Emerging DDoS Attacks " International Conference on Cloud Computing , Data Science & Engineering ,2017
[8] Christos Douligeris and Aikaterini Mitrokotsa "DDOS ATTACKS AND DEFENSE MECHANISMS: A CLASSIFICATION " IEEE Press ,2003
[9] Zhang Chao-yang "DOS attack analysis and study of new measures to prevent ", International Conference on Intelligence Science and Information Engineering ,2011
[10] Lanjuan Yang,Tao Zhang, Jinyu Song, JinShuangWang, Ping Chen , "Defense of DDoS Attack for Cloud Computing " IEEE Press ,2012
[11] B. Prabadevi, PhD Scholar, N.Jeyanthi "Distributed Denial of service Attacks and its effects on Cloud Environment" IEEE Press , 2014
[12] Bikram Khadka1 , Chandana Withana1 , Abeer Alsadoon1 ,Amr Elchouemi2 , "Distributed Denial of Service attack on Cloud: Detection and Prevention " IEEE Press , 2015
[13] Poongothai, M , Sathyakala, M "Simulation and Analysis of DDoS Attacks"International Conference on Emerging Trends in Science, Engineering and Technology ,2012
[14] Mr.K.Narasimha Mallikarjunan, K.Muthupriya , Dr.S.Mercy Shalinie "A survey of Distributed Denial of Service attack" IEEE Press , 2010