IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 7, July 2015.
www.ijiset.com
ISSN 2348 – 7968

DDoS Attacks in Cloud and Mitigation Techniques

Isha Chawla
Researcher, SBS State Technical Campus Ferozepur, India

Pawan Luthra
Assistant Professor, SBS State Technical Campus Ferozepur, India

Daljeet Kaur
Associate Professor, SBS State Technical Campus Ferozepur, India

Abstract – The cloud computing is one of the developing segmenting of IT industry as well as a promising concept to the end users.Cloud computing is an internet based pay as use service which provides three layered services (Software as a Service, Platform as a Service and Infrastructure as a Service) to its consumers on demand. These on demand service facilities provide to its consumers in multitenant environment but as facility increases complexity and security problems also increase. As Cloud computing is a shared facility and is accessed remotely, it is vulnerable to various attacks, including host and network based attacks hence requires immediate attention. In recent years, the major attacks in the cloud are a Distributed denial of service (DDoS) attacks on the catalog of cloud attacks. This paper focus on the various types of DDoS attacks at the different layers of OSI model in cloud and the various mitigation techniques available to overcome with the issue.

Keywords – Cloud Computing,DDoS Attacks,Mitigation techniques.

I. INTRODUCTION

Clouds provide a powerful computing platform that enables individuals and organizations to perform variety levels of tasks such as: use of online storage space, adoption of business applications, development of customized computer software, and creation of a "realistic" network environment.Cloud computing virtually and dynamically distributes the computing and data resources to a variety of users, based on their needs, with the use of virtualization technologies and uses public and private APIs (Application Programming Interface) to provide services to its consumers.It provides better utilization of resources and hence results in reduced service access cost. Cloud computing has gained great attention from industry but there are still many issues which are hampering the growth of Cloud. Security is as much of an issue in the cloud as it is anywhere else.

According to the two surveys done by an International data Corporation in 2008 and 2009 respectively, security is top most issue in a Cloud environment. Although Cloud service provider provides some traditional security mechanisms still there are more non-identifiable attacks have been launched against the Cloud environment. One such attack is Distributed Denial of Service (DDoS) attack. In recent years there is significant increase in number of DDoS attacks launched against a Cloud environment, so it is necessary to take steps against these attack. The purpose Denial of Service attack is to make the network resources such as internet, web services and applications unavailable to the genuine users for a certain period of time. According to Akamai's "State of the Internet" report for the fourth quarter of 2012, the number of DDOS attacks increased by 200% compared to 2011[4]. So, it is very important to counter act these kind of attacks over cloud environment to ensure its security.

.

II. Distributed Denial of Services Attacks

DOS attacks are among the most common threats to Internet operations. These attacks occupy network bandwidth to make the network unavailable to its intended users. They involve blasting a site with decent traffic to flood the connections between the Internet and the end users[4]. Often multiple nodes are used to send traffic to a site in a distributed denial of service (DDoS). Distributed denial-of-service (DDoS) attacks are a real—and growing—threat to businesses worldwide. DDoS attacks reduce the amount of traffic that any one attacking system needs to send while increasing the impact on the target. DDoS attacks are weapons of mass disruption. Unlike access attacks that penetrate security perimeters to steal information, DDoS attacks paralyze Internet systems by overwhelming servers, network links, and network devices (routers, firewalls, etc.) with bogus traffic or zombies[3].
The figure shows that attacker uses zombies/slaves to generate large amount of malicious traffic to flood the victim over the cloud thus rendering legitimate user unable to access the service.

ISSN 2348 – 7968

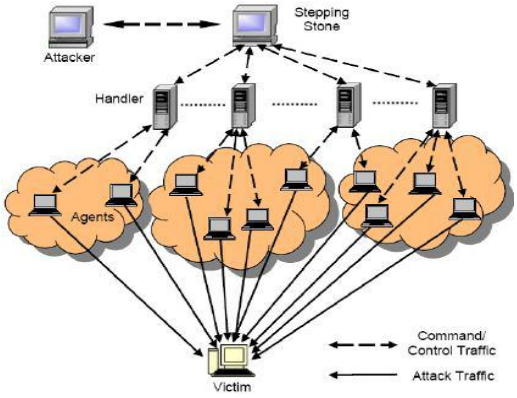

Fig. 1. DDoS Architecture [1]

III.Types Of DDoS Attacks

A. Network Layer/Transport Layer DDoSAttacks:Attack on these two layers Layer 3 and Layer 4 DDoS attacks are types of volumetric DDoS attacks on a network infrastructure. Layer 3 (network layer) and 4 (transport layer) DDoS attacks rely on extremely high volumes (floods) of data to slow down web server performance, consume bandwidth and eventually degrade access for legitimate users. Some of these kinds of attacks include:

A.1 TCP SYN Flooding Attacks:TCP SYN flooding is an example of a simple flooding attack. In TCP SYN flooding, the attacking system sends a TCP SYN request to a host with a spoofed source IP address. While these TCP SYN requests look legitimate, the spoofed address refers to a client that doesn't exist so the final ACK message is never sent to the victim host. The result is half-open connections at the victim site. A backlog queue stores these half-open connections, which bind the server's resources so that no new legitimate connections can be made, resulting in Denial of Service[4].

A.2 UDP Attacks: In a UDP flood attack, large number of UDP packets are sent to random ports on the target by the attacker. As the UDP does not have a congestion control system, the attacker can potentially send a very large number of packets. This attack uses IP address spoofing, so that the attacker's identity cannot be detected in the network[13].

A.3 DNS Amplification Attack: DNS amplification attack uses DNS queries. The size of the reply to a DNS query can be much larger than the DNS query. The attacker creates a reliable domain name server and registers a garbage text of large size. Next, the attacker commands zombies to send queries to their domain name servers with the zombies' IP address which is spoofed to be the victim's IP address. When the domain name servers that receive queries allow recursion, they recursively query the reliable name server and get the reply to the source IP address, which is the address of the victim[13].

***A.4 Internet Control Message Protocol (ICMP) Flood Attacks*:** In ICMP flood attacks, the attacker overwhelms the targeted resource with ICMP echo request (ping) packets, large ICMP packets, and other ICMP types to significantly saturate and slow down victim's network infrastructure[13].

A.4.1 Smurf Attacks:Another type of ICMP-based attack is a smurf attack. In a smurf attack, an attacker broadcasts a large number of ICMP packets with the victim's spoofed source IP to a network using an IP broadcast address. This causes devices in the network to respond by sending a reply to the source IP address.

B.Application Layer Attacks: Application-layer attacks can be difficult to detect in the cloud, as they can be difficult to differentiate from genuine traffic, leaving the availability of services at risk. Some of the Application layer DDoS attacks are:

B.1 Request-Flooding Attacks: These attacks send high rates of legitimate more number of requests than usual (e.g., HTTP GETs, DNS queries and SIP INVITEs) to a server in an attempt to overwhelm its session resources[10].

B.2 Asymmetric Attacks: In these attacks, client sends"high-workload" requests to the server. The objective of these attacks is to consume large amounts of server resources such as CPU, memory or disk space in order to severely degrade the service or bring it completely down[12].

B.3 Repeated One-Shot Attacks: These send a high workload request across many TCP sessions. This is a stealthier means of executing request-flooding and asymmetric application-layer attacks, but the goal is still the same—to degrade or bring down the service[17].

B.4 Application-Exploit Attacks: These deliberately target vulnerabilities in applications which causes a fault in a server's operating system or applications and allowing the attacker to gain control of the application, system. Structured Query Language (SQL) injection attack is one of its common type[12].

C. DDoS Attacks Against Web Services:These type of attacks target the web based application in clouds. These attacks include:

C.1 HTTP Attacks: The attacker floods a web service with non-specific HTTP requests. As the web service tries to process all requests and the particular service requires heavy use of resources, a denial-of-service is easily achieved[6].There are many types of HTTP attacks:

ISSN 2348 – 7968

C.1.1 HTTP Malformed Attacks: These attacks send invalid HTTP packets to Web servers in order to consume server resources. The Zafi.B worm is an example of an attack.

C.1.2 HTTP Request Attacks: These flood Web servers with different types of legitimate HTTP requests (e.g., HTTP GETS, POSTS, etc.) in an attempt to consume server resources.

C.1.3 HTTP Idle Attacks: An attack that opens HTTP connections but then goes idle without actually sending a complete HTTP request. This attack is generally known as "slowloris" and involves indefinitely dribbling out a small number of bytes per packet to keep the connection from timing out, but which never manages to complete the request.

C.2 XML Attacks: XML attacks target web services that communicate through XML documents. SOAP mostly uses XML for exchange of information or data between the client and server. Attackers construct malformed XML requests and send these to the web service. Even a single malformed request might be extremely resource intensive to process. Hence, the attacker can cause considerable harm with a minimum amount of resources[6].

IV. Detection Techniques Against DDoS Attacks

A. Covariance matrix Approach : Covariance-matrix statistical approach has been used for flooding based DoS attack detection, covariance-matrix depend on study and monitor of network traffic features correlativity changes and compare the covariance matrix of normal traffic and any new observed traffic and classify the comparison results according predefined threshold and finding the degree of anomaly of new captured traffic and normal traffic profile, and implementation of this approach has proven more accuracy and efficiency through simulation experiments to two of most famous flooding based attack Neptune and Smurf attacks[16].

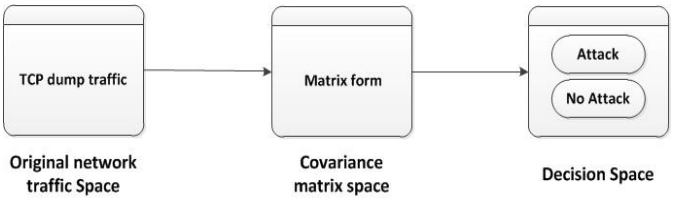

Fig. 2. Covriance Matrix View [16]

B.Cloud Trace Back Method:The Cloud Trace Back (CTB) is a method where the detection is performed at the edge routers in between the clients and web servers. The main objective of this method is to apply a SOA approach to Trace Back

methodology, inorder to identify the true source of a DDoS. In a CTB framework, Cloud TraceBack Mark (CTM) is placed within a web service message [6].It marks the request from the client with CTB Marker within header. All service requests are first sent to CTB which prevents the direct attack on the web servers. The attack client will then formulate a SOAPrequest message based on the service description. Upon receipt of SOAP request message, CTB will place a CTMwithin the header. Once the CTM has been placed, theSOAP message will be sent to the Web Server. When attack is detected the victim will ask for reconstruction to extract the mark. This will help in tracing the source. The cloud protector detects and filters the attack. However, the detection and filtering of attack starts only after the attack traffic reaches the victim.The message is normal, the SOAP messageis then forwarded to the request handler for processing. Upon receipt of the SOAP request; the Web Service willprepare a SOAP response. The web server then takes theSOAP response and sends it back to the client. as part of theHTTP response.

C.Intrusion detection system (IDS): It is an essential component of defensive measure to protect network and computer system against various attacks. It is defined as techniques which are used to detect and respond to the intrusion activities from malicious host or network. The key feature of IDS is its ability to provide the view of unusual activity and to generate the alerts in order to notify the administrators and/or block the suspended connection. IDS tools are capable of distinguishing between the insider attacks, inside the organization and external ones (attacks and the threats by hackers). If an intrusion has been detected, IDS issues alert as notification[11]. These alerts are based on true positives or true alarms when actual intrusion takes place and false alarms in case of wrong detection of the system.There are two types IDS:

C.1 Signature based detection: This method uses specifically known patterns of unauthorized behavior, called signatures, to predict and detect subsequent similar attempts. This method is extremely accurate for known attacks. It produces a low false alarm. With the help of this technique, we can cover a broader range of unknown attacks.

The advantage of this approach is that signatures are easy to create and understand only if the network behavior is known that is required to identify. The disadvantage of this method is that its efficiency decreases as the number of new attacks increases because it has to create a new signature for every new attack as it can only detect intrusion that matches a predefined pattern. Signature based detection does not work well when the user uses advanced technologies like nop generators, payload encoders and encrypted data channels[11].

C.2 Anomaly based detection: Anomaly detectors are designed to identify abnormal patterns of behavior on a host or network. It functions on the assumption that attacks are different from normal activity and can be detected by systems

ISSN 2348 – 7968

that recognize these variations. Anomaly detectors create a list of profile data as a normal data representing normal behavior. It automatically detects any deviation of it and generate alarm. It has the capability to detect new types of errors.Oneadvantage of using this kind of intrusion detection is that we can add new rules without modifying existing ones. It has the ability to detect novel attacks. But this approach produces many false alarms and time consuming to obtain updated, accurate and comprehensive profiles of normal behavior which leads to large set of training data with network environment system logs[11].

D. Entropy Based Method: The entropy algorithm first builds a profile of the network's normal behaviour monitored at selected networks nodes, in the absence of any attack. In fact given a certain PSN setup (i.e. topology, routing algorithm, and source load) a natural level/value of entropy, a sort of "fingerprint" of the given PSN setup, characterizes normal PSN operation, i.e. normal traffic. Whenever, the entropy deviates from this profile, it means that some vulnerable traffic anomaly is emerging. Detecting shifts in entropy in turn detects anomalous traffic. These changes may be detected by calculating entropy of packet traffic monitored at a small number of selected routers.Thus, one can detect anomalies in packet traffic using entropy based detection methods because the values of entropy of packet traffic sharply decrease from the "fingerprint" profiles shortly after a start of DDoS attack.We have observed that strong DDoS attacks cause significant and almost immediate changes in entropy of packet traffic monitored even at a small number of routers regardless of their position and type of routing algorithm used. Thus, entropy provides promising tool to detect DDoS attacks[8],[10].

V. Prevention Techniques Against DDoS Attacks

A. Hop-Count Filtering method: This method uses the relationship of source IP address and TTL value to carry out filtering. The inspection algorithm extracts the source IP address and the final TTL value from each IP packet. The algorithm infers the initial TTL value and subtracts the final TTL value from it to obtain the hop-count. The source IP address serves as the index into the table to retrieve the correct hop-count for this IP address. If the calculated hop-count matches the stored hop-count, the packet has been "authenticated" otherwise; the packet is likely spoofed[2].

B. CBF (Confidence-Based Filtering) method: This method focuses our probe on transport and network layers.In order to discriminate attack packets from legitimate ones, this method utilizes correlation patterns. CBF utilizes the attribute value pairs in TCP and IP headers to construct correlation patterns. The concept of correlation refers to the situation that some interior characterstics and there are indeed some unique correlation patterns in legitimate packet flows.

In user browsing behaviors, when a person logs on a certain website, his/her focuses tend to make up a certain pattern. For example, since the majority of NBA fans who live in Los Angeles love the team Los Angeles Lakers, the website of ESPN will have more packets containing correlations between visits of Lakers webpage and the IP addresses from the area around Los Angels.Considering that there are a large amount of correlation patterns like this or even more complicate ones, it is quite hard for attackers to notice and mimic these patterns when carrying out DoS or DDoS attacks. The correlation patterns in network and transport layers are the co-appearances between attributes in IP header and TCP header. These attribute pair patterns are distinctive because certain characteristics of the operating system,network structure and even hobbies of users can affect the values of these attributes, and thus make some attribute pairs related. This method uses two concepts: the one named confidence for measuring correlation patterns, and the one named CBF score for judging the legitimacy of packets[5].

C. Port Hopping Technique: This approach is an end point based solution to DoS/DDoS protection, in that changes are made to the servers or clients, but not to the Internet routers. The tests are carried out by the end hosts, and can be conducted at the network layer (IP), transport layer (TCP) application layer.

PRNGs are algorithms that use mathematical formulae or simply precalculated list of tables to produce sequences of numbers that appear randomly. A good example of a PRNG is the linear congruential method. In this scheme, different port numbers are used in different time slots for the same communication service .Let Pi represents the port number used by the server in time slot Si. k is a shared cryptographic key between the server and the client communication and f is a pseudo-random number generator. When a client needs to communicate with the server, it will identify the server's current port number Pi using the shared secret key k and the time slot number i. When the server receives packets of data that carry "invalid" port numbers, they can be easily detected and filtered off. There is no need for the server to examine the contents of the packets in order to identify if a packet is malicious. As a result, the computational resources needed to detect and filter off the malicious data packets is reduced [15].

D. Ingress/Engress Filtering: Ingress Filtering, proposed by Ferguson et al., is a restrictive mechanism to drop traffic with IP addresses that do not match a domain prefix connected to the ingress router. Egress filtering is an outbound filter, which ensures that only assigned or allocated IP address space leaves the network. A key requirement for ingress or egress filtering is knowledge of the expected IP addresses at a particular port[18].

ISSN 2348 – 7968

VI. CONCLUSION

Existence of vulnerabilities in Cloud computing allow illegitimate users to affect the confidentiality, availability and integrity of cloud resources as well as services. Detection of highly effective DoS/DDoS attack are major security concerns in the Cloud.In this paper we have briefly gone through various types of DDoS attacks and various mitigation techniques including detecting and preventing methods to protect the cloud environment.

REFERENCES

[1] Chopade, S. S., Pandey, K. U., & Bhade, D. S. (2013). *"Securing cloud servers against flooding based DDOS attacks"*. *Proceedings - 2013 International Conference on Communication Systems and Network Technologies, CSNT 2013* (pp. 524–528).

[2] V. Chouhan and S. K. Peddoju, "Packet Monitoring Approach to Prevent DDoS Attack in Cloud Computing," no. 2315, pp. 38–42, 2012.

[3] W. Paper, "WHITE PAPER," pp. 1–11, 2002.

[4] http://www.akamai.com/dl/akamai/akamai-ebook-guide-to-multi-layered-web-security.pdf

[5] W. Dou, Q. Chen, and J. Chen, "A confidence-based filtering method for DDoS attack defense in cloud environment," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1838–1850, 2013.

[6] T. Vissers, T. S. Somasundaram, L. Pieters, K. Govindarajan, and P. Hellinckx, "DDoS defense system for web services in a cloud environment," *Futur. Gener. Comput. Syst.*, vol. 37, pp. 37–45, Jul. 2014.

[7] P. Negi, A. Mishra, and B. B. Gupta, "Enhanced CBF Packet Filtering Method to Detect DDoS Attack in Cloud Computing Environment," pp. 2–6.

[8] A. S. S. Navaz and V. Sangeetha, "Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud," International Journal of Computer Applications(0975-8887), vol. 62, no. 15, pp. 42–47,January 2013.

[9] S. Seenivasan, "Secure Cloud Computing Environment Against DDoS and EDoS Attacks," International Journal of Engineering Research & Technology, vol. 3, no. 1, pp. 3453–3459,January – 2014

[10] A. Khajuria and R. Srivastava, "Analysis of the DDoS Defence Stratigies in Cloud Computing," INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN MANAGEMENT & COMPUTER APPLICATIONS ,ISSN NO: 2319-7471 vol. 2, no. 2, pp. 1–5,February 2013.

[11] I. Raghav, "Intrusion Detection and Prevention in Cloud Environment : A Systematic Review," International Journal of Computer Applications (0975 – 8887), Volume 68– No.24, April 2013.

[12] S. T. Zargar, J. Joshi, D. Tipper, and S. Member, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding,"IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION, pp. 1–24, 2013.

[13] P. Shamsolmoali, "C $_2$ DF : High Rate DDOS filtering method in Cloud Computing," Computer Network and Information Security no. August, pp. 43–50, 2014.

[14] S. Rajesh, "Protection from Application Layer DDoS Attacks for Popular Websites," *Int. J. Comput. Electr. Eng.*, vol. 5, no. 6, pp. 555–558, 2013.

[15] T. Siva, E. S. P. Krishna, S. Vidyanikethan, and C. Dist, "Controlling various network based ADoS Attacks in cloud computing environment : By Using Port Hopping Technique," International Journal of Engineering Trends and Technology (IJETT), vol. 4,no. 5 pp. 2099–2104, May 2013.

[16] M. N. Ismail, "New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment," no. 6, pp. 226–237.

[17] F. Wong and C. X. Tan, "A S URVEY OF T RENDS IN M ASSIVE DDOS A TTACKS AND C LOUD -B ASED M ITIGATIONS," vol. 6, no. 3, pp. 57–71, 2014.

[18] S. B. Ankali, "Detection Architecture of Application Layer DDoS Attack for Internet," vol. 990, pp. 984–990, 2011.