Distributed Denial of Service Attacks on Cloud Networks

Aditya Singhania[1], Udit Vikhe[2]
[1,2]Student, B.Tech CS, Mukesh Patel School of Technology Management and EngineeringMumbai , Maharashtra, India

Abstract-*The latest buzzword in the world of Information Technology is Cloud Computing. As a result, a lot of work is being put in by the researchers in order to study the various aspects of cloud viz cloud network architecture, virtualization, I/o efficiency, data integrity and confidentiality, scheduling policies, performance scalability and data intensive applications. Being dynamic in nature, cloud computing has presented researchers with the opportunity to explore the new area of cloud forensics. However, with the increase in its use cloud computing has been facing some serious issues in the security domain. Various threats and attacks are being unveiled everyday as malicious minds try to breach the security of major conglomerates. Distributed Denial of Service (DDOS) is one of the widely used attacks in the cloud environment. This attack is favourable for the attackers as it is simple to execute yet difficult to resolve. With giant software companies opting for the use of cloud computing, the DDOS has become a serious threat to their data. Hence, it has become essential to develop mechanisms to prevent and detect the DDOS attacks which hamper the cloud environment.This paper presents a review of the impact of DDOS in the industry, the various tools used by infiltrators to disable the security mechanisms employed by the software companies and its effect on the OSI layers. The major focus of the paper is on the prevention and detection techniques used to abate the threat of DDOS attacks.*

Keywords: cloud computing, network security, DDOS attacks

I. INTRODUCTION

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

The attackers are tempted to take advantage of the loop holes associated with the cloud and thereby steal the sensitive data. Among so many threats to cloud networks, Denial of Service(DoS) attacks prove to be one of the most dangerous attacks and even the Cloud Security Alliance has identified it as one of the major threats [1]. In DoS attack, the maliciuos infiltrator overloads the targeted user with syncronised service requests so that response is unavailable for any further requests and hence resources will be made unusable to its users. Distributed Denial Of Service (DDoS) attackers make use of many compromised machines called zombies to launch DoS attack on the target machine and the service is disrupted. DDoS attacks are increasingly frequent these days and proper intrusion detection systems are needed. This paper discusses the various kinds of DDOS attacks possible, its effects on the variuos layers, detection techniques and the various countermeasures that need to be followed to prevent them.

II.TYPES OF DDOS ATTACKS

The DDoS attacks can be classified into three categories.

2.1 Volume Based Attacks/Bandwidth Based Attacks: the victim network is ovrloaded with large amounts of useless data thus consumig required network bandwidth and resources unnecessarily. Examples include UDP floods, ICMP floods [2] [3].

2.2 Protocol Attacks: To overload the target's resources the attacker takes advantage of the lacuna of various network protocols. Examples include Ping of Death, Smurf attack, SYN floods, fragmented packet attack etc [2] [3].

2.3 Application Layer Attacks: concentrating on specific web applicatins, this attack overloads the targeted user with HTTP requests breaking the limits of request handling. This kind of attack includes HTTP DDoS attack and XML DDoS attacks or REST based attacks [3]

III. DEPLOYMENT TOOLS FOR DDOS

The various tools for DDOS attack are:

3.1. Agobot: The first DDOS tool is Agobot; an IRC backdoor Trojan and network worm are used for establishing an IRC channel to a remote server granting an intruder control of the vulnerable computer. This worm will copy itself into the Windows system folder as SYSTEM32.EXE and may create the following registry entries so that it executes automatically on system restart: HKLM\software\windows version\Run\" "=System32.exe.

3.2. Mstream: The second tool of DDOS is a Mstream agent that ran on a compromised Linux system at a major university

which was targeting over a dozen IP addresses by flooding them with packets, using fake source addresses. Mstream is a three-tiered DDOS tool, enabling an attacker to force systems that have been inflicted with the Mstream agent to flood target system(s) with sustained bursts of TCP packets significantly slowing down the host by bombarding the CPU and even blocks network bandwidth.

3.3. Trinoo: This attack involves flooding servers with UDP packets sourced from multiple of machines. Source addresses are not tampered with, so systems running the offending daemons are contacted. However, the attacker responds by introducing new daemon machines into the attack. Nefariuos code has been introduced by taking advantage of buffer over-run by abnormalities present in the remote procedure call (RPC) services. The attacker can hack the key or use generated password combinations to gain access to the cloud consumers.

3.4 The Botnet command and control is a technique which is used for DDOS attack. It is a set of online programs which communicate with similar programs in order to send spam mail to the server.

IV. IMPACT OF DDOS ON NETWORK LAYERS

Higher layer protocols cannot be blocked by IDS and firewalls. Thus DDoS has a different impact on different layers of OSI. This results in increased complexity of detection mechanism and impact factor.The DDoS attacks over time have grown in terms of which layer they affect. This means that a DDoS attackgrows from the Network Layer to the Session layer and eventually to the Application layer. The figure 2 below shows how DDOS impacts each of the layers of OSI.The DDoS attacks can be implemented on different OSI layers. The attack detection mechanism and its complexity keep increasing as we move from a lower OSI layer to a higher one. For eg: the complexity of a DDoS attack on the session layer will be higher than that applied to the network layer and a DDoSattack on application layer would be more complex than that on the session layer.A DDoS attack on the application layer is a more severe form of threat which the attacker performs.If the simple net-DDoS fails the assaulter will shift his abominable motives to the victim's application layer. In order to bring the target user's server down the attacker runs a massive amount of queries in the victim's search engine. After the server is blocked the attacker proceeds to perform an attack on the session layer. This is done by jamming the target session by using DNS attacks.The simplest and most commonly used type of DDoS attack used by attackers is the network layer attack which is done using techniques like UDP flooding, SYN flooding, and ICMP flooding. To summarise, a DDoS attack can bring down not only a server but also the bandwith and resources.

According to the survey carried out by Arbor Networks, the application layer attacks are growing more as compared to traditional network flooding attacks. The following graph represents the survey carried out by Arbor Networks which depicts the impact of DDOS on Application layer

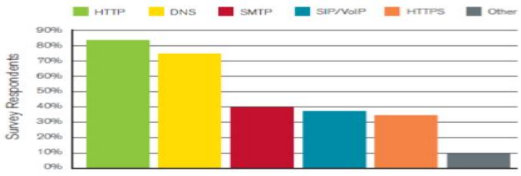

Fig.1.Graph showing Impact of DDOS on Application Layer

The following sections talk about the overall detection mechanisms and the prevention of DDoS attacks at different levels.

V. DETECTION TECHNIQUES

In [4] DIDS (Distributed Intrusion Detection System) is put forth. Author introduced signature related, open source network analyzer, snort to create logs. In this IDS collects and observes packet type ,if the type is matched then it simply drops it otherwise analyzes the packets for serious attacks .If identified as a malicious packet alert is sent to other IDSs and cooperative operation modules, which by majority vote adds a restriction rule. This system aims at providing security from malicious packets which can hamper the cloud environment functioning.This work is concerned with network layer of OSI .But no mechanisms have been given for the identification of the bad packet causing DDOS attacks in a cloud environment – classification technique for packet type detection is not included.

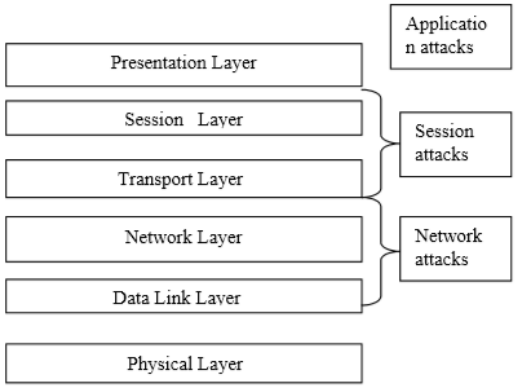

Fig.2 DDOS at Different layers of OSI

In [5] the application layer DDOS attack detection mechanism is shown. The author makes use of SQL server 2005 for procuring all the information of all the clients and

look into the browsing behavior of the users by using Hidden Markova Model. If the anomalous behavior is detected then access to the user is denied.

In [6] the user is given a score and an entropy value is generated in normal conditions as per user sessions.Entropy is defined as a measure of randomness. Each incoming request sessions' entropy is calculated and in comparison to a preset value in a system, if a large deviation is found then the user request of that session is declared as malicious. The Author also gives a solution to counter attack mechanisms by implementing rate limiter and scheduler.

In [7] semantic rule based approach is used to detect anomalities in the application layer.A deterministic finite automaton is used for representing different dubious characteristics. Six malicious characteristics have been using finite shown using automaton symbol and the rules are stated for example what is the probability of each user traversal if the user does not follow the rules laid down. On anomaly hit the score of each page is calculated and both algorithms are used to calculate final threshold value. The finalthreshold value on comparing with score determines the attacker.

In [8] Dempster Shafer Theory is applied for cloud threat detection. It is an approach for compounding evidence for attack conditions. The state space is defined as a UDP, Normal, TCP, and ICMP packet type. The mass of each element in state space is given by using basic probability assignment and then belief for the element is computed. The disadvantage of DST is the computational complexity of DST and conflicting beliefs. According to some authors, computational complexity of DST increases exponentially with a number of elements in the frame of discretion. If there are 'n' elements in the state the there will be 2n-1 elements in a mass function.In addition to detection mechanism, some prevention mechanisms have also been proposed by some authors.

Sr. no.	Concept used	Advantages	Disadvantages
1	Distributed IDS	Simplicity, accurate result compared to pure snort	Absence of classification technique
2	Hidden Markova Model	Simple implementeation	Unpredictable number of states
3	Entropy	Accuracy is high	Less concentration due to calculation mergers
4	Semantic Rule based approach	Easy to understand	Sometimes unpredictable
5	Dempster Shafer Theory	Dynamic changes taken into account	Increase in complexity is exponential

Table 1: Summarizing DDOS Detection Techniques

VI.PREVENTION TECHNIQUES

Various prevention techniques may be implemented once detection is successful. Some of these include:

Co-operative Intrusion Detection System:

It is a Snort dependent DIDS deployed in each cloud computing region which cooperate with each other to depreciate the effect of DDoS attacks in the network. The IDS is comaparable to the type of received packet which if ppresent in its block table shall be dropped immediately. If a match is not found, but maliciousness is detected, an alert is sent to all other IDSs. Each IDS exchange alerts the other IDS using majority vote method to decide true and fake alerts. If an alert is true, then the block table is modified with new block regulations to identify such kind of attacks in the coming future. The IDS consists of four components which perform the detection- intrusion detection, alert clustering and threshold calculation and comparison, intrusion response, blocking and cooperative operation [9]. The IDS helps to faciliatate early detection and prevention of DDoS attack in a cloud environment with more computational time.

Cloud Trace Back Model (CTB) and Cloud Protector The Cloud Trace Back (CTB):

These models are used to detect the source of the DDoS attack and Cloud Protector helps to differentiate and filter these attack patterns for the future. CTB is based on Distributed Packet Marking Page Algorithm (DPM) and Cloud Protector uses a backward propagation neural network to separate illegal message patterns. CTB is implemented prior to the web server to avoid direct DDoS attacks [10]. The efficiency of the model is greatly dependent on the efficiency of the neural network and the training data set plays a vital role in deciding the performance of CTB.

Confidence Based Filtering(CBF) Approach:

This approach works during two periods, a non-attack period and an attack period. Whilst a nonattack period, it discovers the unique correlation patterns among acceptable packets by identifying attribute pairs in their IP and TCP headers. Then it computes a confidence value to test the trustworthiness of a particular correlation pattern of an attribute pair. Higher the frequency of an attribute pair during normal packet flow, greater the confidence value it will get. The dataset can be termed as a nominal profile. During an attack, the CBF score for each packet is calculated which is the weighted mean of confidence values of all attribute pairs in it. Then the CBF score on comparing with discarding threshold decides whether the packet is legitimate or not. If

CBF score is greater than the threshold, the packet is legitimate and permitted to pass or else the packet is dumped [11]. The merits of CBF method include minimal storage space, high computational speed and efficiency which makes it very suitable for large network traffic.

CLASSIE Packet Marking Approach:

HX-DoS attack is a combination of XDoS and HDoS attacks. CLASSIE Packet Marking Approach is an IDS which is based on the decision tree classification system used to prevent HX-DoS attacks. CLASSIE is placed at a one-hop distance from the host to find out the anomalous packets by using its set of rules. The packets will be marked after evaluation by this method. Edge and core routers carry out the marking process. The decision to permit or drop the packet is made by the Reconstruction and Drop (RAD) which is positioned at a one hop distance from the user. As a result, the malicious packets will be marked at the attacker's end and dropped at the user's end [12]. The overhead created in packet marking and the rate of false DoS attacks is significantly reduced using this approach.

Filtering Tree Approach:

HDoS and XDoS are attacks which target the application layer, these attacks are curbed by following this approach. The user request is changed to XML format and then the SOAP message is doubly signed and embedded with client IP address, client puzzle and puzzles solution. The SOAP message is then forwarded to IP trace-back that makes a comparison between the incoming IP address and the value that is stored in its table. In the event of a match is found, the packet is dropped or else it is passed on to the Cloud Defender. Using five filters, namely hop count filter, sensor filter, Double Signature Filter, Puzzle Resolver Filter and IP Frequency Divergence Filter the Cloud Defender filters the malicious packets [13]. However, this method is incompetent in order to find out the DDoS attacks in transport and network layers of the cloud.

Information Theory Based Metrics Method:

There are two phases in this method viz behaviour monitoring and behaviour detection.

During the first phase, normal web user behavior is realized during the non-attack period and an entropy score for requests per session is calculated and a trust value is given to each user. During behavior detection phase, the entropy score for every request is computed and compared with a pre-set threshold value. If the threshold value is exceeded, then the request packets are considered dangerous and dropped immediately. If the computed entropy is less than the threshold value but the trust value of the user and difference in entropy score is very high, the rate delimiter restricts the user access. A scheduler is put to use to manage the workload of the system [14]. The following table shows the summary of various approaches used to prevent the DDoS attacks.

Sr. no.	Method	Features	Limitations
1	Co-operative IDS	1.Single point of failure attack is avoided. 2.Improved reliability	High computational time
2	Cloud Trace back Model	Discovers the identity of the attacker	1.Traning data set for neural networks is difficult to procure 2.Dependence on training data set
3	Confidence Based Filtering Approach	Storage size is small rendering high packet filtering efficiency	Low accuracy
4	CLASSIE Packet Marking Approach	1.HX-DOS attack identification 2. reduced false positive rate	Refers to only application layer
5	Filtering Tree approach	Filters attacks in multiple stages	Refers to only application layer
6	Information Theory Based Metrics Method	1.Uses entropy concepts 2.Easy implementation	May lead to information loss

Table 2: Summarizing DDOS Prevention Techniques

VII. CONCLUSION

It must be understood that cloud computing and the internet are complementry and so are the security issues. However, due to the cloud's variable nature, the outdated digital methods and technology fail to implement analysis for security in the cloud environment. This paper reviews the different approaches in order to detect and prevent DDOS in a Cloud Environment. As Cloud Computing is in its nascent state, a lot of rsearch is in order. Impacts of Ddos on the different layers of a network are also put to scrutiny.

REFERENCES

[1] The information week website. http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-securitythreats/d/d-id/1114085

[2] S.S. Chopade, K.U. Pandey, D.S. Bhade, Securing Cloud Servers against Flooding Based DDOS Attacks, in Proc. International Conference on Communication Systems and Network Technologies,2013.

[3] DDoS Attack. http:// www.incapsula.com/ddos/ddos-attack
[4] Chi-Chun Lo, Chun-Chieh Huang,Joy Ku ”A Cooperative Intrusion Detection System Framework for Cloud Computing Networks” 39th International Conference on Parallel Processing Workshops,2010,pp280-284.
[5] Sanjay B Ankali, Dr. D V Ashoka ”Detection Architecture of Application Layer DDoS Attack for Internet”, Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, pp:984-990 (2011).
[6] S. Renuka Devi and P. Yogesh “Detection Of Application Layer DDOS Attacks Using Information Theory Based Metrics, CS & IT-CSCP 2012, pp. 217–223.
[7] Chu-Hsing Lin, Chen-Yu Lee, Shin-Pin Lai1 and Wei-Shen Lai, “A Semantic Rule-based Detection Scheme against Flooding Attacks on Cloud Environment”, International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012.
[8] A.M. Lonea, D.E. Popescu, H. Tianfield, “Detecting DDoS Attacks in Cloud Computing Environment, International Journal of Computing and communication , ISSN 1841-9836 8(1):70-78, February, 2013.
[9] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, A Cooperative Intrusion Detection System Framework for Cloud Computing Networks, 39th IEEE International Conference on Parallel Processing Workshops, 2010, pp280-284.
[10] Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi, Securing Cloud Computing Environment Against DDoS Attacks, IEEE International Conference on Computer Communication and Informatics, 2012.
[11] Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu, CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment, Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2011.
[12] E.Anitha, Dr.S.Malliga, A Packet Marking Approach to Protect Cloud Environment against DDoS Attacks, International Conference on Information Communication and Embedded Systems, 2013.
[13] Tarun Karnwal, T.Sivakumar, G.Aghila, A Comber Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS attack, IEEE Students’ Conference on Electrical, Electronics and Computer Science, 2012, vol-01, pp-9-12.
[14] S. Renuka Devi and P. Yogesh, Detection Of Application Layer DDos Attacks Using Information Theory Based Metrics, CS & ITCSCP 2012, pp.217–223.