ISSN: 2393-8528

IJICSE
Open Access

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 2 Issue 3; July-August-2015; Page No. 17-20

Review of Defence Techniques against DDoS Attack in Cloud Environment

Amandeep Saini

M.Tech CS, Jayoti Vidyapeeth Women's University

nickygoshi8@gmail.com

Sarvesh Singh

HOD (CS department), Jayoti Vidyapeeth, Women's University

sarvi899@gmail.com

ARTICLE INFO

Received: 30 May 2015
Accepted 07 July 2015

Corresponding Author:

Amandeep Saini

Computer Science & Engineering Department, JVWU, Jaipur, India

Email: nickygoshi8@gmail.com

ABSTRACT

Cloud computing is a revolution in IT technology that providing access to resources instantly as per the needs of the end user and pay only for the service they consumed. Security is one of the most challenges for both cloud consumer and provider. Distributed denial of service is the most serious attack that threats the availability of the cloud service. Cloud built on the fundamental of distributed environment. In DDoS attack, the intruder overload the target system with service request so that it cannot respond to any further request and hence resource will be made unavailable to its users. It is necessary to analyze fundamental features of DDoS defence techniques. This paper provide the review of certain techniques and defence mechanism that been implemented to DDoS attack.

INTRODUCTION

Cloud computing technology was a very old dreaming of computing as a service which is based in using the internet and remote server for preserving data and application. The system layer, the platform layer and application layer are three fundamental layers in cloud computing. The three essential component of cloud computing are SaaS (Software as a service) that gives ability to users for working with their software far from any anxiety of installing and running their applications on their own systems, PaaS (Platform as a service) provide a platform for users whom their applications can be run and IaaS (Information as a service) managing networks and maintaining user's information in a protected way. Cloud computing facing with several security problems like secrecy, authenticity, confidentiality and DDoS attack. The DDoS attack accrues to a server when attacker sends a huge amount of fake packets from a number of zombie computers which are already under the control of attacker. To improve resource availability of resources in cloud environment, it is essential to provide a mechanism to prevent DDoS attack. There exist few effective and detailed model frameworks available for the detection and prevention of DDos attack. This paper provides a number of defence mechanisms to avoid DDoS attack.

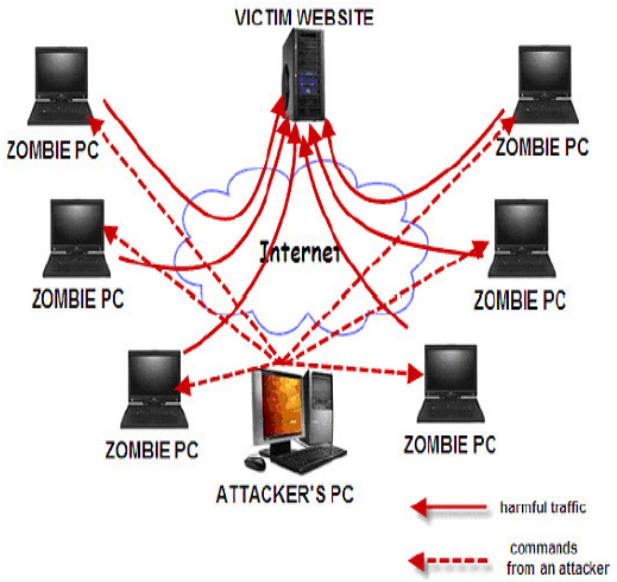

Figure: DDos attack

Types of DDoS attack on Cloud:

1 ICMP Floods attack: The sending of an abnormally large number of ICMP packets of any type (especially network latency testing "ping" packets) can overwhelm a target server that attempts to process every incoming ICMP request and this can result in a denial of service condition for the target server. The bandwidth

utilization maximizes ultimately resulting network inaccessibility to its users.

2 Ping of Death Attack: A ping of death involves sending a malicious ping to a computer generally of 32 bytes in size. This packet will be fragmented at the sender side and reassemble at the receiver side. Handling oversized packets affects the victim's machine inside the cloud environment and its resources hence the target system will crash.

3 SYN Floods Attack: TCP SYN flood DDoS exploits part of the normal TCP three way handshakes to consume resources on the targeted server and render it unresponsive. With SYN floods DDoS the offender sends TCP connection request faster than the targeted machine can process them. It causes network saturation.

4 IP Spoofing Attack: This attack accrues when the attacker modifies the header of sources IP field either by legitimate IP address or by an unreachable IP address hence the server will be unable to complete the task to unreachable IP address.

Defence Techniques and Methods against DDoS Attack:

1 Cloud Track Back Model (CTB):

The main objective of trackback model is to apply SOA (service oriented architecture) approach to trackback methodology in order to identify true source of DDoS. CTB introduce the use of a propagation neural network called cloud protector which was trained to detect and filter such attack traffic.

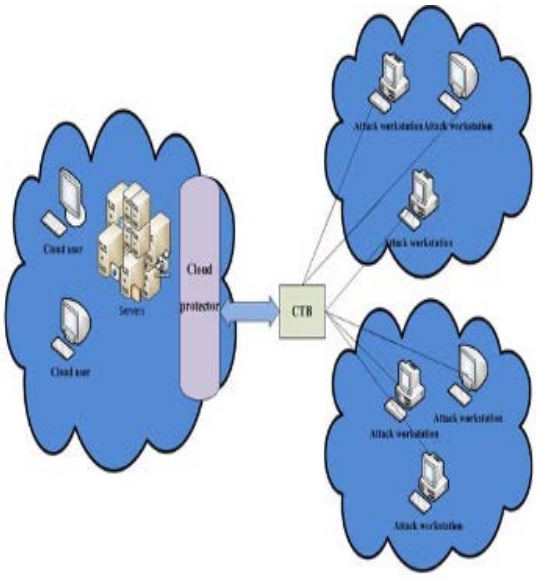

Figure2: CTB and Cloud protector

CTB and cloud protector located between each cloud web service to defence against XML based DDoS attack. CTB being located before the web server in order to place a cloud track back mark tag within the CTB header. All service requests are first sent to the CTB marking. This model gave ability to cloud network for detecting and filtering most of the attacks based on DDoS. The efficiency of the model is depends on the efficiency of neural network and hence training data set plays vital role in deciding the performance of CTB.

2 Cloud Intrusion Detection Systems:

Intrusion detection system is used in virtual machine for securing cloud networks against DDoS attack. It is located on virtual switch and examined all packets to find a type of attack base on predefined rules. Signature based ID systems are adequate to deal with misuse intrusions. The proposed model is based on a distributed cloud IDS which uses of multithreading method for enhancing IDS performance over the cloud infrastructure.

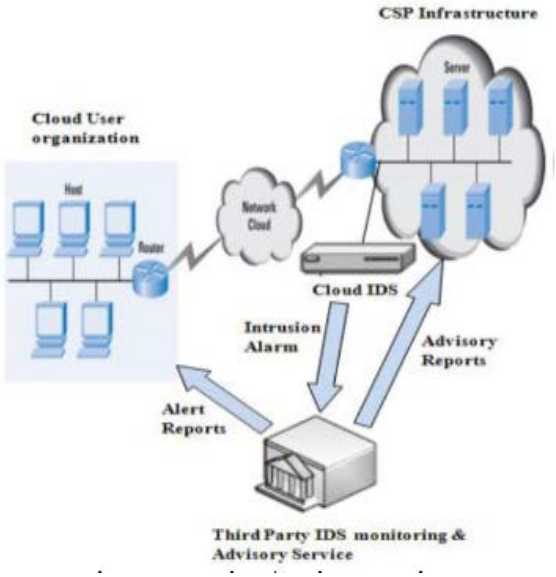

Figure3: Cloud Intrusion Detection System

The IDS consist of four components to perform the detection include intrusion detection, alert clustering, intrusion response and co-operative operations. Anomaly based IDS are based on tracking unknown unique behaviour pattern of detrimental activity. IDS help to detect and prevent from DDoS attack in cloud environment with more computational time.

3 Confidence Based Packet Filtering Method (CBF):

This method works on two periods namely a non-attack period or an attack period. During a non-attack period lots of legitimate packets are captured and analyzed for creating a normal profile according attribute pair inside the TCP and IP headers. Then it calculates a confidence value to determine correlation pattern between an attribute pair. The highest frequency of an attribute pair shows the higher confidence value it gets.

In attack period time, CBF score for each value is calculated which is the weighted average of confidence value of attribute pairs in it. If CBF score is higher than threshold value, the packet is legitimate or else discarded. The performance of CBF is depended to attack situations.

An algorithm is used for CBF packet filtering method:

Step1: Set the initial values to the required attributes
Step2: Declaring the Period whether it's attacking Period or Non attacking Period
Step3: If period is Non Attacking then Calculate the Confidence Value
If NP =NULL then
Update NP with the confidence value
Else
If Confidence Value< Value in NP then
Update the NP and attach in packets
IHL=IHL+1
Option Field=Confidence Value
Accept the Packet
Else
Attach in packets
IHL=IHL+1
Option Field=Confidence Value
Accept the Packet
End if
End if
Else
Set the Confidence value in the NP as discarding threshold
Calculate the Confidence Value of packet
If Confidence Value (packet) < Discarding threshold then
Discard the packet
Else
Accept the Packet
End if
End if

4 Entropy Based Anomaly Detection Method:

The Shannon-wiener index theory is an important theory to analyze the random data and determine the uncertainty associated with data. The more randomness in data has more entropy in it. The entropy will be minimum if the data coming from one IP or port. If data belongs to many classes, the entropy will be larger. The changes in entropy will show that the traffic is coming from different sources. A threshold value is computed and defined to detect the DDoS attack in the system. If the entropy increases beyond that threshold value, the system generates an alarm for DDoS.
This can be done in two steps:
(1) The user is allowed to pass through the router for first time and detection algorithm verifies the user.
(2) For the second time when user tries to pass through router, the entropy value is computed depending upon the packet size and user authenticity. If the entropy value does not meet the standard range value, it is considered as intruder and an acknowledgement is send to cloud provider. The entropy value is calculated for each data packet.

5 Machine Learning Automatic Defence Method:

This method detects anomalies and finds the attack traffic according to the trained neural network. When attack is detected, those packets with specific marks as the attack packets are filter out. Testing of incoming packets is done by the neural network. If result indicates anomalies, further investigation of compositions of marked packets takes place. If the no of packets that have the same address digest bits exceeds a threshold N drop, this flow of packets will be filtered.
The two steps design can not only protect legitimate traffic but also punish entirely the attack traffic.
(1) Neural network classifier with the assistance of concentration of the packets (same digest), the legitimate traffic will be less likely decided as an anomaly than by other coarse granite such as statistical model.
(2) Once the attack traffic flow is identified, the flow can be totally filtered by differentiating the identity.
(3)

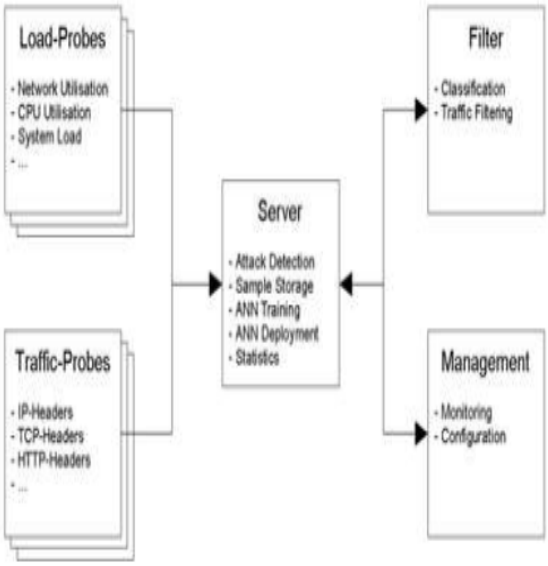

Figure 4: Automatic Machine Learning Defence

Comparative Analysis of Defence Techniques:

In this analysis, we have compared techniques that are discussed earlier. Each technique or methods have some pro and cons.

Technique	Deployed	Pros	Cons	Remarks
Cloud Track Back Model	Neural Network	Detect and filter DDoS in Cloud	Monitoring of packets continuously slow down the performance	CTB performance depends on neural network efficiency
Entropy Based Anomaly Detection	Cloud Gateway	Detect DDoS attack at cloud gateway	Entropy calculation of each packet is overhead	.....

CBF Packet Filtering Method	Cloud Database	Detect DDoS attack on Cloud Database	Reduce processing speed	.....
Cloud Intrusion Detection System	Virtual Switch	Detect DDoS attack on Cloud Environment	Generate large no of alert which slow down the performance	Exception generated should be updated on Node or Cluster.
Machine learning Automatic Defence Method	Trained Neural Network	Detect Anomalies and find Attack Traffic	Identify flow of packets reduce efficiency	.....

Conclusion:

Above table indicate a summary of mentioned defence methods and comparative analysis against DDoS attack on cloud environment. Cloud computing brings numerous benefits into the IT technology but with the widespread usage of cloud, the cloud security issues are also surfacing. One of the major breach in security is DDoS attack. It is essential to provide a mechanism to prevent from DDoS attack and improve availability of resources. This paper gives an idea and various approaches to defend against this kind of attack.

References:

1. Armbrust, M., et al., A view of cloud computing. Communications of the ACM, 2010.
2. Zhang, L.J. and Q. Zhou. Cloud computing open architecture. Web Services, 2009.
3. Jain, P., D. Rane, and S. Patidar. A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment. Information and Communication Technologies (WICT), 2011 World Congress on. 2011. IEEE.
4. Bakshi, A. and B. Yogesh. Securing cloud from ddos attacks using intrusion detection system in virtual machine. Communication Software and Networks, 2010. ICCSN'10. Second International Conference on. 2010.
5. Roschke, S., F. Cheng, and C. Meinel. Intrusion detection in the cloud. In Dependable, Autonomic and Secure Computing, 2009.
6. A.S.SyedNavaz, V.Sangeetha, C.Prabhadevi. "Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud" International Journal of Computer Applications (0975 –8887) Volume 62–No.15, January 2013.
7. PriyankaNegi, Anupama Mishra and B. B. Gupta."Enhanced CBF Packet Filtering Method to Detect DDoS Attack in Cloud Computing Environment".
8. Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu, "CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment", in Ninth IEEE InternationalConference on Dependable, Autonomic and Secure Computing, 978-0-7695-4612-4/11, 2011.
9. A.M. Lonea, D.E. Popescu, H. Tianfield. "Detecting DDoS Attacks in Cloud Computing Environment", INT J COMPUT COMMUN, ISSN 1841-9836 8(1):70-78, February, 2013.
10. Roschke,S., Cheng, F. and Meinel, C., "Intrusion Detection in the Cloud". In Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 729-734, 2009.
11. Bansidhar Joshi, A. Santhana Vijayan, BineetKumar Joshi, Securing Cloud Computing Environment Against DDoS Attacks, IEEE International Conference on Computer Communication and Informatics, 2012.
12. 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.
13. E.Anitha, Dr.S.Malliga, A Packet Marking Approach to Protect Cloud Environment against DDoSAttacks, International Conference on Information Communication and Embedded Systems, 2013.
14. 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 andComputer Science, 2012, vol-01,pp-9-12.
15. S. Renuka Devi and P. Yogesh, Detection Of Application Layer DDos Attacks Using Information Theory Based Metrics, CS & IT-CSCP 2012, pp.217–223.3.