ISSN: 2393-8528

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 2 Issue 3; July-August-2015; Page No. 30-35

DDOS Attacks Detection and Prevention with Cloud Trace Back

[1] Akshita Sharma, [2]Sarvesh Singh

[1] M.tech. CSE, Jayoti Vidyapeeth Women's University Jaipur, Rajasthan

akshita2606@gmail.com

[2] HOD CSE, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan

sarvi899@gmail.com

ARTICLE INFO

Received: 01 July 2015
Accepted 18 July 2015

Corresponding Author:

Akshita Sharma

Department of Computer Science and Engineering, Jayoti Vidyapeeth Women's University, Jaipur

Email: akshita2606@gmail.com

Keywords:

Cloud Computing, DDOS attacks, CTB

ABSTRACT

Cloud Computing makes computing real as a tool and in the form of services. Cloud Computing is simply defined as a type of computing that depends on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud Computing is typically a metaphor for the internet. A strong thrust on the use of virtualization technology to realize Infrastructure-as-a-Service (IaaS) has led enterprises to leverage subscription-oriented computing capabilities of public Clouds for hosting their application services. The dynamic nature of cloud presents researchers new area of research that is cloud forensics. Cloud Forensics is the branch of forensics for applying computer science knowledge to prove digital artifacts. The DDOS is the widely used attack in cloud environment. To do the forensics of DDOS if it is identified a possible detection and prevention mechanisms would aid in cloud forensics solutions and evidence collection and segregation. In this paper, we propose a method of DDOS detection, Open Stack and prevention by using Cloud Trace Back Model (CTB).

1. INTRODUCTION

Cloud Computing is currently one of the most hyped information technology areas and has become one of the fastest growing segments in IT industry. NIST identifies the five key characteristics of cloud computing as on- demand self- service, resource pooling, broad network access, rapid elasticity and measured service [1]. As large magnitudes of data are moving onto the cloud, the attackers are keener to exploit the vulnerabilities associated with cloud and thereby to steal the sensitive data. Among the various threats to cloud computing, Denial of Service(DOS) attacks can prove to be the deadliest attack and even the Cloud Security Alliance has identified DOS attack as one of the nine major threats [2]. The introduction of resource-rich cloud computing platforms, where users are charged based on the usage of the cloud's resources, known as "pay-as-you-use" or utility computing, has transformed the Distributed Denial of Service (DDOS) attack problem in the cloud to a financial one.

Distributed Denial of Service is a type of attack that aims to make services or resources unavailable for indefinite amount of time by flooding it with useless traffic. The two main objectives of these attacks are, to exhaust computer resources (CPU time, Network bandwidth) so that it makes services unavailable to legitimate users.

In a general DDOS attack, the attacker usually disguises or 'spoofs' the IP address section of a packet header in order to hide their identity from their victim. This makes it extremely difficult to track the source of the attack. IP trace back is a scheme that provides an effective way to trace the source of DDOS attacks to its point of origin. The DDOS attacks which took place in recent years have aroused the need for taking stern steps against it.

2. TYPES OF DDOS ATTACKS

The DDOS attacks can be classified into three categories.

2.1 Volume Based Attacks/Bandwidth Based Attacks

This attack makes an attempt to overload the victim with large amounts of junk data thereby consuming the network bandwidth and resources. Examples include UDP floods, ICMP floods [3] [4].

2.2 Protocol Attacks

The attack tries to take advantage of the lacuna associated with various network protocols to overload the target’s resources. Examples include Ping of Death, Smurf attack, SYN floods, fragmented packet attack etc [3] [4].

2.3 Application Layer Attacks

The attack concentrates on specific web applications and sends HTTP requests beyond the limits it can handle. This kind of attack includes HTTP DDOS attack and XML DDOS attacks or REST based attacks [4].

3. TOOLS OF DDOS

Abuse and Nefarious use of cloud computing is the top threat identified by cloud security Alliance. The threats which comes under this category are Password and key cracking, DDOS,launching dynamic attack points , Hosting malicious data, Botnet command and control, Building rainbow tables ,CAPTCHA solving. Distributed Denial of Service attack, which means many nodes systems attacking one node all at the same time with a flood of messages. The DDOS attack can be performed by guest virtual machine who takes the control of physical host infrastructure [5].After taking the control of host machine, the attacking VM then exploit computing resources.

The tools for DDOS attack are - Agobot, Mstream, Trinoo.

- The first DDOS tool is Agobot which is an IRC backdoor Trojan and network worm which establishes an IRC channel to a remote server in order to grant an intruder access to the compromised computer. This worm will copy itself into the Windows system folder as SYSTEM32.EXE and may create the following registry entries so that it can execute automatically on system restart: HKLM\software\windows version\Run\” ”=System32.exe.
- The second tool of DDOS is An Mstream agent runs on a compromised Linux system at a major university this system was targeting over a dozen IP addresses with a flood of packets, using forged source addresses. Mstream is a three tiered DDOS tool, allowing an attacker to direct systems that have been infected with the Mstream agent to flood target system(s) with sustained bursts of TCP packets, which significantly slows down the host by overburdening the CPU and even restricts network bandwidth.
- The third tool of DDOS mentioned above is Trinoo, this attack involved flooding servers with UDP packets originating from thousands of machines. Source addresses were not spoofed, so systems running the offending daemons were contacted. However, the attacker responded simply by introducing new daemon machines into the attack. Malicious code had been introduced through exploitation of buffer over-run bugs in the remote procedure call (RPC) services. The attacker can hack key or use combinations of password to get access of cloud consumers. Hosting unauthorized data is again another threat of cloud computing. The Botnet command and control is another technique which is used in participating DDOS attack. It is a set of internet connected programs which communicates with similar programs in order to send spam email to server. Rainbow table is a pre-computed Table which is used for reversing password hashes.

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 shows the survey carried out by Arbor Networks which shows the impact of Application layer DDOS.

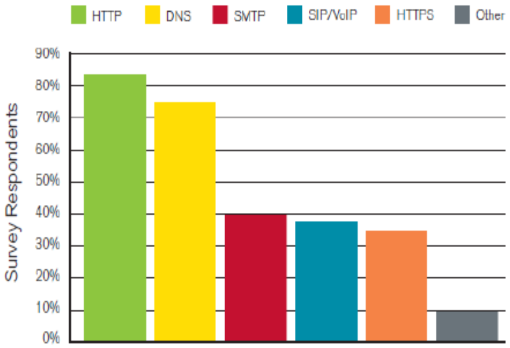


Fig.1.Graph showing Impact of DDOS on Application Layer

4. PROPOSED METHOD

In this section, a method for DDOS detection and prevention by Cloud Trace Back Model (CTB) is proposed. DDOS attacks can be performed by using command ‘hping3’, which means that attacker is hiding source IP address i.e. destination machine will see source from random source IP address than actual(IP masquerading), and destination machine will get overwhelmed within 5 minutes and stop responding.

For carried out criminal activities i.e. DDOS attacks, the environment can be setup using Desktop PC’s running ubuntu with OpenStack by using OpenStack Cloud Manager.

4.1. OpenStack

OpenStack is open source cloud computing software that provides infrastructure as a service cloud deployment for public and private cloud. OpenStack was first introduced in June 2010, born with its initial code from NASA’s Nebula platform and Rackspace’s Cloud Files platform. Openstack mission according to [6] is “To Produce the ubiquitous open source cloud computing platform that will meet the needs of public and private cloud providers regardless of size, by being simple to implement and massively scalable”. Although OpenStack is portable

Software but many Linux Distributions provide it as an operating system also like Ubuntu Canonical [7].

- **Openstack Architecture**

Openstack is organized around three main modules i.e. compute, storage and networking. Along with these three, dashboard become an important component in providing interface to administrators and users for provisioning and release of resources. These components and their interaction with user's application and underlying hardware over which other OpenStack services do run can be represented as sown in figure 2. OpenStack compute is designed for provisioning of virtual machines providing scalable cloud computing platform. OpenStack storage provides objects storage to be used for storing necessary images to run virtual machines or virtual instances. OpenStack network provides necessary services which are used for communication with in virtual machine i.e. inter-VM and external to virtual machines.

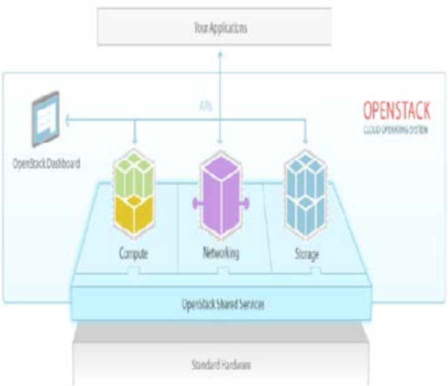


Fig. 2: Open Stack Architecture

4.2. Cloud Trace Back Model (CTB)

We propose a novel mitigation technique against DDOS attack in Cloud Computing. Cloud Trace Model (CTB) Is based upon Deterministic Packet Marking (DPM) Algorithm [8][9]. DDOS attacks are shielded by forwarding the first request to a verifier node in our proposed architecture. This verifier node is responsible for the verification process and for updating the white and black lists based on the results of this process. The subsequent requests coming from the bots will be blocked by a virtual firewall since their IP addresses will be found in the black list. On the other hand, the subsequent requests coming from legitimate clients will be forwarded directly to the target cloud service since their IP addresses will be found in the white list.

The main focus of proposed model shown in Fig. 3 is to offer a solution to Trace Back through our application module Cloud Trace Back (CTB) to find the source of DDOS attacks, and introduce the use of a back propagation neutral network, called Cloud Protector, which was trained to detect and filter such attack traffic.

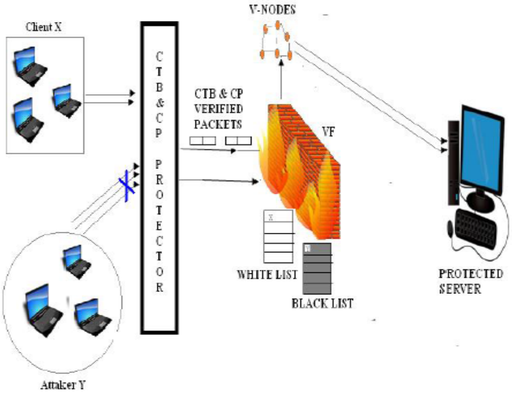


Fig.3: The Proposed Model

- **Cloud Trace back (CTB)**

Cloud Trace Back Architecture's (CTB) main objective is to apply a SOA approach to Trace Back methodology, in order to identify the true source of a DDOS. CTB is deployed at the edge routers in order to be close to the source end of the cloud network. Usually, if no security services are in place for web services, the system becomes quite vulnerable to attacks. Fig.3 demonstrates how CTB can remedy this by being located before the Web Server, in order to place a Cloud Trace Back Mark (CTM) tag within the CTB header. As a result, all service requests are first sent to the CTB for marking, thereby effectively removing the service provider's address and preventing a direct attack.

In an attack scenario, the attack client will request a web service from CTB, which in turn will pass the request to the web server. The attack client will then formulate a SOAP request message based on the service description. Upon receipt of SOAP request message, CTB will place a CTM within the header. Once the CTM has been placed, the SOAP message will be sent to the Web Server. Upon discovery of an attack, the victim will ask for reconstruction to extract the mark and inform them of the origin of the message. The reconstruction will also begin to filter out the attack traffic. The message is normal, the SOAP message is then forwarded to the request handler for Processing requests or any outgoing message.

- **Cloud Protector**

CTB does not directly eliminate a DDOS attack message. This is left for the filter section of a defense system called Cloud Protector. The Cloud Protector is a trained back propagation neural network (NN), to help detect and filter out DDOS messages. A neural network is a set of connected units made up of input, hidden and output layers [10] [11]. Each of the connections in a neural network has a weight associated with it. Threshold logic unit (TLU) inserts input objects into an array of weighted quantities and sums up to see if they are above the threshold. The cloud protector system is implemented in five different phases as shown in Fig. 4

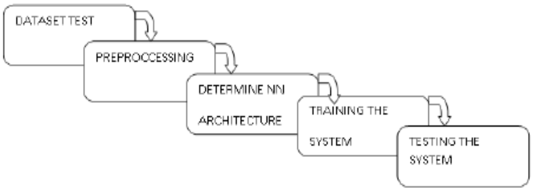


Fig. 4: Implementation phases

➢ DDOS SHIELD AND MITIGATION ARCHITECTURE AND APPROACH

Fig. 3 shows the proposed architecture of the DDOS shield for mitigating the DDOS in a cloud computing environment. The Main components of the architecture are virtual firewalls (VF) and verifier cloud nodes (V-Nodes). The virtual firewalls work as filter mechanisms based on white and black lists that hold IP addresses of the originating nodes. And, the verifier cloud nodes update the lists based on the results of the verification process. The virtual firewall can be implemented in the cloud as a virtual machine that has the capabilities of filtering and routing. The VF uses two lists, a white list and a blacklist, to make a decision regarding the incoming packets from outside the cloud and destined to some services hosted in the cloud.

The white list is used to track the authenticated source IP addresses so that the incoming traffic originating from these addresses will be allowed to pass the firewall towards the destined services. The blacklist is used to hold those unauthenticated source IP addresses so that the firewall will drop the incoming packets originating from these IP addresses, these two lists have to be updated periodically.

Another component in our proposed architecture is the verifier nodes (V-Nodes) which are represented by a pool of virtual machine nodes implemented based on the cloud infrastructure. The V-Nodes constitute a cloud-based overlay network. A V-Node has the capabilities to verify legitimate requests at the application level using unique Turing tests, such as UNIQUE QUESTION TESTING. Another role of the VNode is to update the lists used by the VF as was explained earlier.

If the application request gets verified successfully, then the source IP address of that request will be added to the white list and the request will be forwarded to the destined service in the cloud. If the application request fails, then the source IP address of that request will be added to the blacklist, and subsequent packets originating from that source IP address will be dropped.

Fig. 5 shows a case of a legitimate request from a client *X*, where the first request gets verified by a V-Node and passes the Question test.

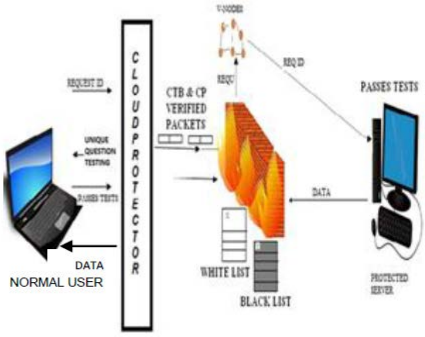


Fig.5: Normal Request Scenario

Thus, its source IP address, *X*, has been added to the whitelist and the subsequent requests from *X* to the Destination *D* have been forwarded directly to *D.*

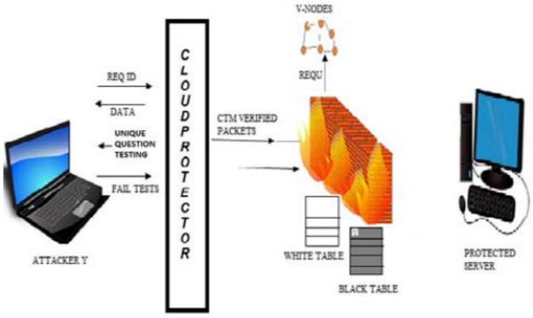


Fig.6: Request from Hacker

Fig. 6 Shows a case of a request coming from an attacker (a bot), *Y*, where the first request gets verified by a V-Node and fails the Turing test. Thus, its source IP address, *Y*, has been added to the blacklist and the subsequent requests from *Y* to the destination *D* have been blocked by the VF. Since the requests originating from the bots, i.e., compromised machines, will fail at the verification stage, all the automated malicious requests will not reach the victim in the cloud. Therefore, the customer will not be charged for such attacker.

➢ ALGORITHMIC APPROACH FOR DDOS ATTACKS

Algorithm 1 and Algorithm 2 show the actions taken by the VF and the V-Node when considering that the architecture is protected against the IP spoofing attacks.

Algorithm 1: CTM Actions

```
 If (CTB places CTM in header)
{
 Soap message will be sent to the server
 }
 Else
{
Wait for place the CTM in headers
}
End if
If (Soap message sent to web server=TRUE)
{
If (verifies the message=no victims)
```

```
{
SOAP message is then forwarded to the request handler for processing to the web server (Respond to HTTP Request).
}
Else
{
Ask for reconstruction to extract the mark and inform them of the origin of the message.
}
End
End
```

Algorithm 1: VF Actions

```
    Input:
    P ← Packet
    S← Packet source IP address
    D← Packet destination IP address
    B← Blacklist
    W←Whitelist
    Begin:
    If (S ϵ W && S∉B)
    Forward P to D
    Else If (S ϵ  B) Drop p Else forward p to a V-node
End
```

Algorithm 2: V-NODE Actions

```
    Input:
    P ←Packet
    S← Packet source IP address
    D← Packet destination IP address
    B← Blacklist
    W←Whitelist
    Begin:
    If (S ∉ B && S ∉ W) {
    Send to S a unique Question test
    If (Question test passes) {
    W_W+S
    Forward P to D.
    }
    Else
    B_B+S
  END
```

5. RESULT

Back propagation uses learning technique for training the network, fig.7 shows learning rate.

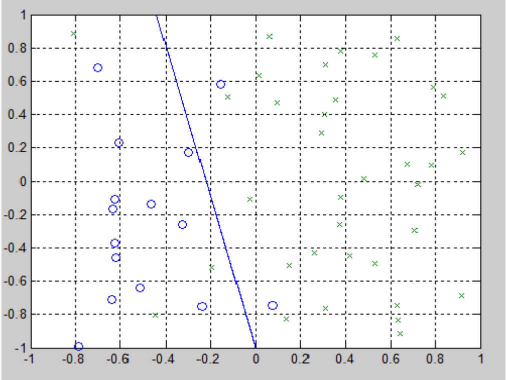


Fig.7

Activation function maps weighted inputs to the output. These functions are logistic function which ranges from 0 to 1, hyperbolic tangent function which ranges from -1 to 1 and identify function which ranges from -10 to 10. Fig 8 (a) (b) & (c) shows graph of these functions.

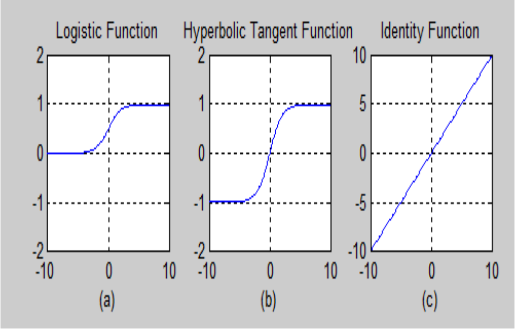
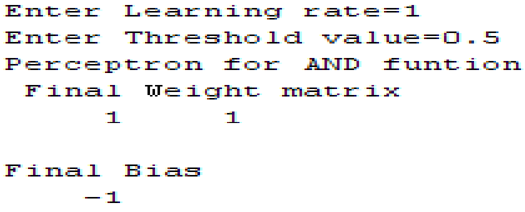


Fig. 8

Here, threshold function for learning rate 1 and threshold value 0.5 is shown in fig. 9.



```
Enter Learning rate=1
Enter Threshold value=0.5
Perceptron for AND funtion
 Final Weight matrix
     1      1

Final Bias
    -1
```

Fig. 9

6. CONCLUSION AND FUTURE SCOPE

The cloud computing and internet are interrelated. All the issues are related to internet are applicable to cloud including threats. But traditional digital methods and technology fails to do forensics in cloud environment due to its dynamic nature. One of the most serious threats to cloud computing security itself comes from Distributed Denial of Service attacks. These types of attacks are simple and easy to implement by the attacker, but to security experts they are twice as difficult to stop. So, a solution model is offered to Trace Back through proposed Cloud Trace Back (CTB) to find the source of real attacks, and introduce the use of a back propagation neutral network, called Cloud Protector.

In the future, we will be setting up to begin real-time data gathering and testing of Cloud Protector. This will allow us to fine tune CTB to better detect and filter DDOS attacks and the v-frame and v-node actions are the best approaches to shield the DDOS attacks.

7. REFERENCES

1. National Institute of Standards and Technology- Computer Security Resource Center. www.csrc.nist. gov
2. The information week website. http://www.Informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085
3. 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.
4. DDoS Attack. http:// www.incapsula.com/ddos/ ddos-attack
5. George Sibiya , Hein s. Venter2 and Thomas Fogwill, "Digital Forensic Framework for a Cloud Environment" IIMC International Information Management Corporation, 2012,pp-2-8.
6. Tutorial, OpenStack. CloudCom, IEEE. [Online] 2010. http://salsahpc.indiana.edu/CloudCom2010/slides/ PDF/tutorials/OpenStackTutorialIEEECloudCom.pdf.
7. Ubuntu cloud. *ubuntu.* [Online] www.ubuntu.com.
8. Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi,"Securing cloud computing environment against ddos attacks"International Conference on Communication, Volume 5.
9. Edos-Shield - A Two-Steps Mitigation Technique against Edos Attacks In Cloud Computing," 2011 Fourth IEEE International Conference on Utility and Cloud Computing"
10. Trostle J, (2006), "protecting Against Distributed Denial of service attacks Using Distributed Filtering," Securecomm and Workshops, Aug 28 2006- sept1 2006, pp 1-11
11. Iftikhar A., Azween B. A., Abdullah S.A.,(2009), "Application of Artificial neural Network in Detection of DoS attacks," SIN'09, Oct 6-10.