DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5695

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

PREVENTING CLOUD SYSTEMS AGAINST DDOS ATTACK USING HOP COUNT FILTER APPROACH

Patel Zalak N
IT Systems & Network Security
GTU PG School, Gandhinagar
Gujarat, India

Prof. Hardik Upadhyay
Computer Engineering
Gujarat Power Engineering & Research Institute
Gujarat, India

Abstract: Cloud Computing is the most dynamic field characterized by IT Industry. Most probably every industry, and some parts of it , are migrating their data to the cloud. The cloud has become the part of the critical global infrastructure. Security has become the major concern for this computing environment. The Cloud has the distributed nature, so it has become the target of distributed attacks like DDoS and DoS. DDoS and Simple DoS attack us one of the biggest threat in the Cloud networks which prevents the authorized users from using the Cloud Services. Cloud Servers can be crashed down , when it gets too many unnecessary requests or SYN Packets. So, the appropriate solution must be identified to strengthen the security and privacy of the cloud. In this Paper, we have proposed the algorithm, which uses Hop Count Filter Approach, which can block the spoofed packets and can strengthen the security of the cloud.

Keywords: cloud; computing; DoS; Distributed Denial of Services; Availability; Hop Count;

I. INTRODUCTION

Cloud Computing is being an emerging technology, as it has many advantages to reduce costs of infrastructure so, it is becoming more popular in IT industry [3]. It has emerged a new trend in IT industry[6]. Cloud Computing is defined as everything like "storage, management, processing information and other data stored on the specific server. It makes computer infrastructure available as per need , on "pay per use".

Cloud computing uses virtualization to provide various kind of provisioned services. In recent time, it has come in focus of current IT industry,[3] but important aspect of it is, there are too many vulnerabilities in the cloud models like "IaaS, PaaS, SaaS"[2]. Numbers of threats are increasing from the perspective of data security and network security [7]. Impact of variety of attacks on cloud computing includes, maintenance of secrecy, Privacy of data [1]. So, it is important to find out the most appropriate solution to strengthen the security and privacy of the cloud environment. All the systems connected to the internet can be affected by the attacks like, DoS ,DDoS, Man-in-the-middle, spoofing, sniffing, flooding etc. DDoS attack is one of the most prominent threats on cloud infrastructure which can prevent the authorized users to use the cloud services and it can crash down the cloud servers.

II. DDOS ATTACK CLASSIFICATION

Denial of Service is an attack on a computer or a network that reduces accessibility of system resources to its legitimate users [4]. In DoS attack, the attacker flood a victim system with non legitimate service requests or traffic to overload its resources [4]. DoS attack leads to unavailability of particular resources and slow network performance.

DDoS attack is almost the same as DoS attack, but results of DDoS attacks are massive. DDoS attack is executed by the method of distributed computing called as "botnet army". It is created by infecting too many computers with a form of malware that gives the botnet owner access to the computer.

DDos attack is the serious threat to the cloud infrastructure , as it reduces the availability of the resources to the authorized users.

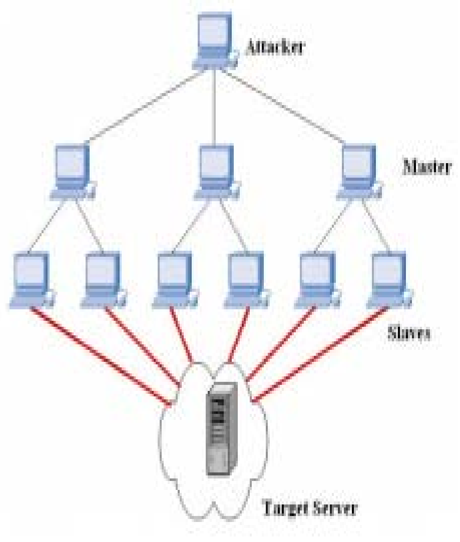

Figure 1: Architecture of DDoS attack

The DDoS attack is classified in following categories [4].

- **Volumetric Attacks**: consumes the bandwidth of the target network or service.
- **Fragmentation Attacks** : overwhelms targets' ability of re-assembling the fragmented packets.
- **TCP-State Exhaustion attacks:**consumes the connection state tables presents in the network infrastructure components such as load-balancers, firewalls and application servers.

- **Application layer attacks**: Consumes the application resources or services there by making it unavailable to other legitimate users.

Some of the common DoS attacks are discussed below [8].

1. SYN Flood attack

Syn flooding takes advantages of a flow in how most hosts implement the TCP three-way handshake. The malicious host can exploit the small size of the listen queue by sending the multiple SYN requests to the host, but never replying to the SYN/ACK. The victim’s listen queue isquickly filled up. This ability of holding up each incomplete connection for 75 seconds can be used as DoS attack.

2. Spoof attack

A spoofing attack means , when hacker or any any malicious code successfully acts on another persons’ behalf by impersonation data.

3. Peer-to-Peer Attack

Attackers instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network to connect to the victim’s fake website. Attackers exploit flaws found in the network using Direct Control protocol that is used for sharing all types of files between instant messaging clients. Using this method, attackers launch massive denial of service and compromise websites.

4. Distributed Reflection Denial of Service

DRDoS(Distributed Reflection Denial of Service) also known as spoofed attack, involves the use of multiple secondary machines that contribute to the actual DDoS attack to the target machine or website. Attacker launches this attack by sending requests to the intermediary hosts, these requests are then redirected to the secondary machines which in turn reflects the network traffic to the network.

5. Service requests Flood

A group of zombies attempts to exhaust server resources by setting up and tearing down TCP connections. It floods servers with high rate of connections from valid sources.

III. LIMITATION OF EARLY METHODS OF DEFENSE FOR DDOS ATTACK

Whether the DDoS attack is determined by the volumetric change [5]. The volumetric change is identified by flow collection and analysis tool. A defense footprint or signature works to match the attack packets while allowing the authorized traffic. The footprint or signature based defense systems only block the attack traffic but cannot create false positives. False positives are very common error in most mitigation techniques. By tracing back to the source of the attack, it can be detected from where the attack was happened.

IDS/IPS is the traditional mitigation technique for defense of DDoS attack. This systems have the existing signature which match to the incoming network traffic, if any anomaly is observed, it block that network traffic. These packets are dropped to mitigate the attack. But this process can affect the availability of the cloud environment as this method can block the authorized requests.

It is advised that CSPs(Cloud Service Providers) should filter the incoming traffic that they receives from the clients. The packets that don’t belong to the legitimate clients must be dropped. Some security product vendors have announced the security products which can find out the source of TCP SYN flood, flood attack. But it is more tough to find out the source of the spoof attack.

There are many methods has been carried out by the researchers like distance estimation[1], cloud trace back[4], filter tree approach and tools like usnort[2] which is kind of intrusion detection system.

The limitation of such mitigation methods is that , it mostly creates the false positive errors and they block the traffic according to the estimation, signature, footprint so, these techniques don’t have the accuracy to figure out the actual source of the attack, they block the legitimate traffic with the attack traffic.

IV. PROPOSED METHOD

Our proposed algorithm used the Hop Count Filter approach to prevent the spoofed attack which can be used as DoS&DDoS attack. It makes sure that the false positive error can be reduced, as before given techniques has this limitation , and the legitimate user can not be blocked while dropping down the connection of the attack traffic.

In this algorithm, the Hop count method is used, Hop count means the number of intermediate devices between source and destination through which data would have passed.

Here the hop count is calculated in reverse look up, from destination to source , and it should check , whether the hop count can be find out or not, if the Source IP of which the hop count is being calculated, is not existed on the “verbose” system, the hop count of that could not be found out. That means, as per this algorithm, if the request is coming from any non existed IP, that IP would be spoofed IP because the Hop count cannot be calculated of the non existed IP.

IP Spoofing

This approach is used for the DOS and DDOS attack by hiding the identity of the real source of the attack[3]. It means the attacker change the false IP address in the IP packet header and send the request to the victim so, he can hide his own identity by IP changing in the IP header, it is called IP spoofing.

It can be understood that , if the IP spoofing is done by the attacker, the spoofed IP is changed in the IP header , but that IP is not existed on the “verbose” system, so as per this proposed algorithm, if the IP is not on the verbose system, the hop count cannot be calculated, so that IP can be spoofed.

Proposed Algorithm
This algorithm will work in two states:

1st state : Detection of spoofed IP

- Analyze network traffic.
- Extract the Continuously repeated IPs from where requests are being generated.
- Extract Source IP (SIP) from the packet P in one file.

- In reverse look back, Calculate **Hop Count HC = TF – TI** from destination to the source.
- If it cannot be counted the hops of particular IP, that means it is spoofed, Send it to the 2ndstate .
- If it can be find out the hops then allow that IP.

<u>2ndstate : Prevention or blocking of spoofed IP</u>

- For each Source IP,
- If Source IP = spoofed
- Drop that IP to the Blocking Module
- Else
- Accept IP

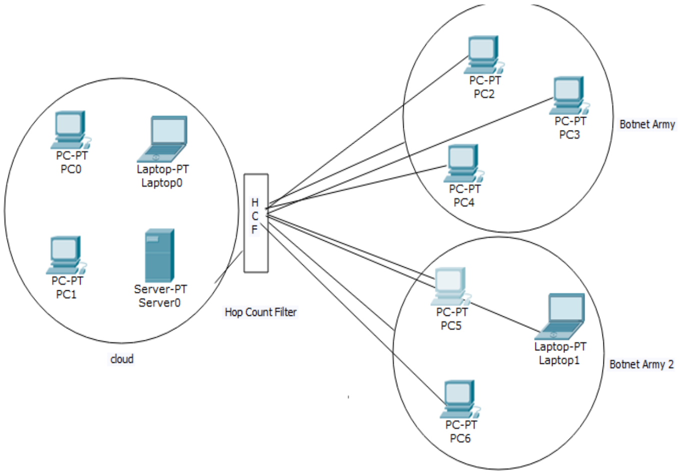

Figure 2: Design Model of the Proposed System

As per the above figure, when the spoofing attack is done by the attacker on the cloud server to crash it down, the requests must be gone through the Hop count filter (HCF) and the firewall of the server. When the attack is happened, the changes in the network traffic can be showed by the packet sniffer or tcpdump. When the changes in the IPs can be got, the changed IPs should be given to one file and the Hop count Filter will count the Hop for the IPs given in the File. If the Hops of the source IP can be got , that IP should be allowed, but if the Hops cannot be found out for any IP, block that IP, as that IP can be spoofed.

As if the IP is existed on the “verbose” machine, the hop count can be calculated in the reverse look up, but if the IP is not existed on any “verbose” machine, the request coming from that Ip can be spoofed.If attacker would give the IP spoofing attack, the HCF will find out , whether that coming from the IP is existed on any running machine or not, it would be found out in reverse look up from destination to source in reverse.

V. IMPLEMENTATION & RESULT

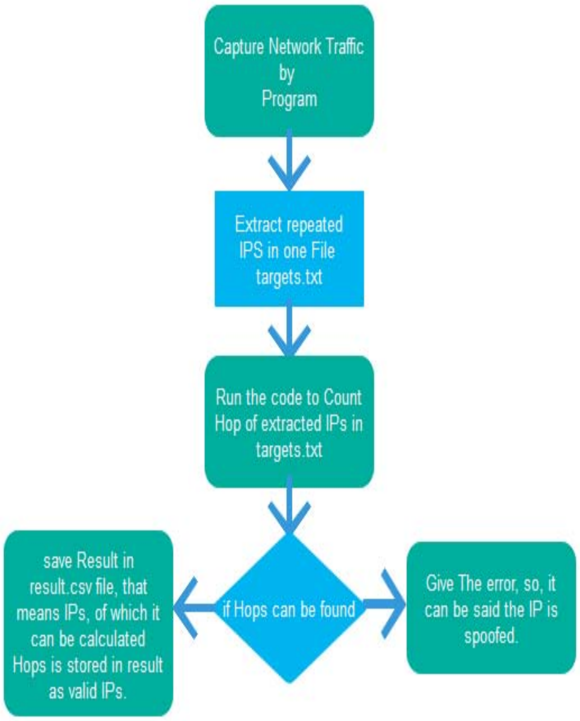
Capture Network Traffic by Program
Extract repeated IPS in one File targets.txt
Run the code to Count Hop of extracted IPs in targets.txt
if Hops can be found
save Result in result.csv file, that means IPs, of which it can be calculated Hops is stored in result as valid IPs.
Give The error, so, it can be said the IP is spoofed.

Figure 3 : Implementation phases

As per the given phases, the Hop Count Filter (HCF) can be used to derive the spoofed IPs from the network traffic. By this method, it is assured that any authorized IP cannot be blocked in the network traffic. So the false positive error can be reduced by this technique.This approach would only figure out the , spoofed IP, which are not existed on running machine.

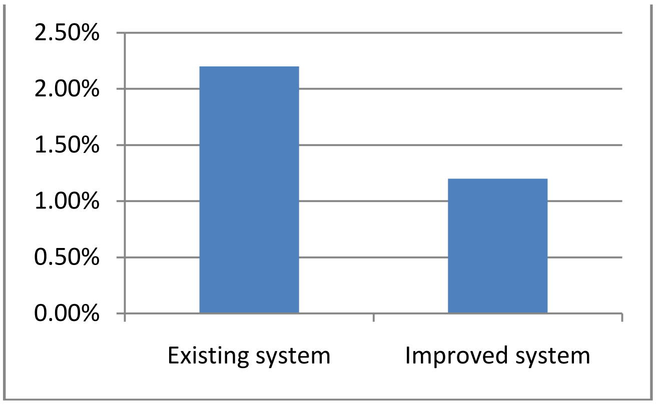

Figure 3: comparison graph of false positive error

© 2015-19, IJARCS All Rights Reserved

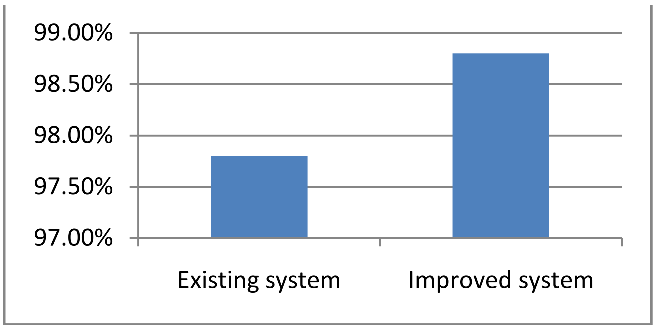

Figure 4 : comparision of accuracy

VI. CONCLUSION

In this paper, we have used, the Hop count filter approach to prevent IP spoofing attack which can be used to launch DDOS attack, which count hops of the source IPs that source IPs are spoofed or not. This method can reduce the false positive error which is the limitation of the earlier techniques.

VII. FUTURE WORK

This paper provide the basic research for the field of network security. If someone try to make the tool using this approach it can be the secure solution to the problems in the cloud networks. This research could also be the backbone to the future work for the security.

VIII. REFERENCES

[1] Shin-Jer Yang and Yu-Zhan Li "Design Issues of Enhanced DDoS Protecting Scheme under the Cloud Computing Environment " Networking and Network Applications (NaNA), 2016 International Conference , IEEE 2016

[2] Awatef Balobaid, Wedad Alawad and Hanan Aljasim "Distributed Denial of Service attack on Cloud: Detection and Prevention ": Computing and Communication (IEMCON), 2015 International Conference ,IEEE 2015

[3] Neeta Sharma, Mayank Singh, Anurajan Mishra, " Prevention against DDos attacks on cloud Systems using Triple filter : An Algorithmic Approach" Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference ,IEEE 2016

[4] Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi "Securing Cloud Computing Environment Against DDoS Attacks" Computer Communication and Informatics (ICCCI), 2012 International Conference, IEEE ,2012R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[5] S.S. Chopade, K.U. Pandey, D.S. Bhade D.M.I.E.T.R, Wardha "Securing Cloud Servers against Flooding Based DDOS Attacks" Communication Systems and Network Technologies (CSNT), 2013 International Conference ,IEEE 2013

[6] Waqar Ali , Jun Sang ,Hamad Naeem, "Wireshark window authentication Based Packet capturing scheme to prevent DDos related security issues in cloud network nodes" Software Engineering and Service Science (ICSESS), 2015 6th IEEE International Conference ,IEEE 2015

[7] Jeanette Smith-perrone , Jeremy Sims "Securing Cloud, SDN and Large Data Network Environments from Emerging DDoS Attacks "Cloud Computing, Data Science & Engineering - Confluence, 2017 7th International Conference ,IEEE 2017

[8] B. Prabadevi, PhD Scholar, N.Jeyanthi , Professor "Distributed Denial of service Attacks and its effects on Cloud Environment- a Survey "IEEE,2014

© 2015-19, IJARCS All Rights Reserved