DDoS attack Defense Framework for Cloud using Fog Computing

Deepali,
National Institute of Technology Kurukshetra,
deepalichaudhary2710@gmail.com

Kriti Bhushan,
National Institute of Technology Kurukshetra,
kriti.nitr@gmail.com

Abstract— Cloud is the requirement of today's competitive world that demand flexible, agile and adaptable technology to be at par with rapidly changing IT industry. Cloud offers scalable, on-demand, pay-as-you-go services to enterprise and has hence become a part of growing trend of organizations IT service model. With emerging trend of cloud the security concerns have further increased and one of the biggest concerns related to cloud is DDoS attack. DDoS attack tends to exhaust all the available resources and leads to unavailability of services in cloud to legitimate users. In this paper the concept of fog computing is used, it is nothing but an extension to cloud computing that performs analysis at the edge of the network, i.e. bring intelligence at the edge of the network for quick real time decision making and reducing the amount of data that is forwarded to cloud. We have proposed a framework in which DDoS attack traffic is generated using different tools which is made to pass through fog defender to cloud. Furthermore, rules are applied on fog defender to detect and filter DDoS attack traffic targeted to cloud.

***Keywords*— DDoS, Cloud Computing, Fog Computing.**

I. INTRODUCTION

World is changing very fast and technology is not behind. Everyday something new is created and deployed, and all of this is done over the Internet. In this era, organizations want more work to be done with least price possible and are ready to use information for competitive advantage. Furthermore, other important factors like globalization, aging data centre, storage growth, application explosion, cost of ownership and acquisition has lead organization to move towards cloud computing. Cloud computing is basically the collection of services hosted over the Internet in the virtual environment. Therefore, user can use resources according to their demand and only pay for them, as the demand increases or decreases these resources can be increased or released accordingly. As popularity of cloud is increasing so are the threats related to it. One such attack which is performed on cloud i.e. the DDoS attack is addressed in detail in this paper.

DDoS attack or Distributed Denial of service attack [2, 20] is one of the most common attacks nowadays, as it is very easy to carry out using some simple scripts or tools which are freely available online. In DDoS attack an attacker creates some zombie machines or bots by infecting machines over the Internet. Then these compromised machines are used to perform attack on victim. When traffic from so many machines are directed toward a single victim, victim's resources like bandwidth, CPU, memory etc starts getting exhausted and its services are no longer available to serve requests from legitimate users. This whole network of bots is called botnet, in botnets the bots may be controlled centrally by a C&C server or P2P. The commands are sent to bot systems directly by attackers or handlers which are again compromised machines over the Internet.

This paper mainly discusses the DDoS attack on cloud environment. When DDoS attack occurs in cloud environment, it exhausts all the resources of the VM and overburdens the system; cloud can handle this situation by allocating more resources to this VM to accumulate all the requests made to it. This allocation of more resources can go on to an extent where either cloud provider runs out of resources to allocate or the owner of VM cannot pay for usage of these resources anymore. Furthermore, to deal with this issue limit may be imposed on connection time or bandwidth but this would just make the idea of cloud computing disappear. Hence, a better approach is required to prevent cloud environment from this attack. Therefore, fog computing can be used to provides protection.

Fog computing [3] also referred as "edge computing" is a decentralized computing infrastructure where edge devices like routers, switches etc provides storage, computation, control, communication, management and measurement. It places some of the transactions and resources at the edge to reduce the need of going to cloud. Fog reduces the need for bandwidth by using distributed strategy which results in lower cost and improved efficiency. Furthermore, fog devices are present between the end devices and the cloud. They allow users machines to communicate directly to each other without going through cloud. Fog connects machines, sensors and devices directly to each other enabling real time decisions to be made without transmitting vast amount of data through cloud. Hence this paper introduces a framework where fog concept is used to mitigate DDoS attack in cloud environment. Basic architecture of fog computing is shown in figure 1. There are 4 layers in fog architecture [5] from which the centre two layers are the fog layers , whereas the top most layer i.e. layer 1 consists of cloud and layer 4 are sensor nodes or end devices.

In this paper we have introduced an approach to protect our cloud server from DDoS attack by mitigating it on intermediate fog layer and hence all the malicious traffic is detected and mitigated at fog layer i.e. before it reaches the cloud. Rest of the paper consists of following sections: section 2, discusses related work; section 3 explains our proposed model; section 4 discussed the results and evaluation of our framework along with some pre-requisites. Finally, section 5 concludes our paper with future scope of work.

978-1-5090-3704-9/17/$31.00 © 2017 IEEE

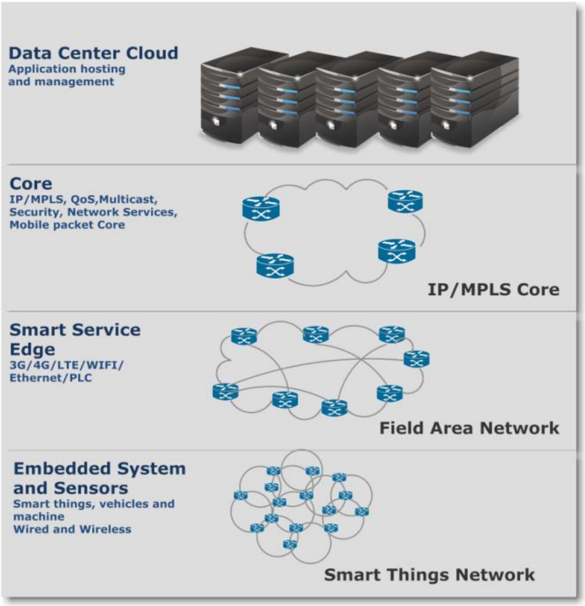

Data Center Cloud
Application hosting and management
Core
IP/MPLS, QoS,Multicast, Security, Network Services, Mobile packet Core
IP/MPLS Core
Smart Service Edge
3G/4G/LTE/WIFI/ Ethernet/PLC
Field Area Network
Embedded System and Sensors
Smart things, vehicles and machine
Wired and Wireless
Smart Things Network

Figure 1: Fog Architecture

II. RELATED WORK

In past few years many research have been done on cloud computing, DDoS attack, botnets and fog computing elucidating their various technological aspects like architectural issues, security aspects, development, tools etc. Somani et al. [8] proposed an infrastructure of cloud with many high capacity physical servers with multiple VMs running on them. This paper addresses the issue that whenever an attack is performed on a VM, horizontal or vertical scaling keeps them from crashing and it not just effect only that VM but other stakeholders like cloud provider, other users of cloud and other VMs. Palmeri et al. [1] proposed an approach through which network anomaly can be detected by independent component analysis. This approach works in two phase scheme of machine learning for zero day attack that alter traffic volume rate and flow characteristics, these two schemes are rule-based classifiers and Blind Source Separation (BSS). Gupta et al. [4] proposed a system for cloud which provides network intrusion detection and mitigation based on profiles which provides protection from malicious insider and outsider in cloud. It uses unsupervised learning algorithm which combines both Bayesian and fine-grained data analysis approach for DDoS detection. It mainly aims at detection of network based attacks likes TCP SYN flooding.

Whereas, Wang et al [7] proposed a DaMask model for DDoS attack defense in cloud and SDN. This model contained two modules i.e. DaMask-D which performs anomaly based DDoS detection and raises an alert whenever an attack is detected and DaMask-M module which implement countermeasure for attack packet and update its log containing signatures. Fayaz et al. [13] used SDN (Software Defined Network) and NFV (Network Function Virtualization) concept to deal with flexibility and scalability issues faced by traditional firewall. A DDoS defense system i.e. Bohatei was tested for defense against different type of DDoS attacks like TCP SYN, DNS amplification etc and it was observed that Bohatei was more responsive, scalable and adversary resilient. Further, Gupta and Joshi et al. [10] proposed a scheme to detect different types of flooding attacks like back, land, smurf etc and then characterize them. Characterization of malicious flow using threshold value was done using six sigma methods. Whereas, Buragohain et al. [9] proposed FlowTrApp an SDN based architecture which detects DDoS attack on basis of flow duration and flow rate and characterize them further as high and low rate, long or short lived traffic.

III. PROPOSED FRAMEWORK

In this paper, a framework is proposed for defense against DDoS attack in cloud i.e., the attack traffic directed to cloud will be detected and mitigation is performed so that it does not lead to wastage of processing power. In the proposed framework, a fog layer [12] is introduced between the cloud server and the user. All the traffic directed to cloud server passes through this intermediate fog layer before it reaches cloud. Defense from attack traffic is applied on the fog layer so that the malicious traffic is dealt with before it reaches cloud server as shown in figure 2. Therefore, it provides an efficient utilization of cloud resources and avoiding unnecessary wastage of time and resources in cloud. To implement this scenario malicious traffic is generated using various open source tools and scripts on different operating systems and cloud server was set up along with an intermediate fog layer through which the traffic was forwarded to cloud.

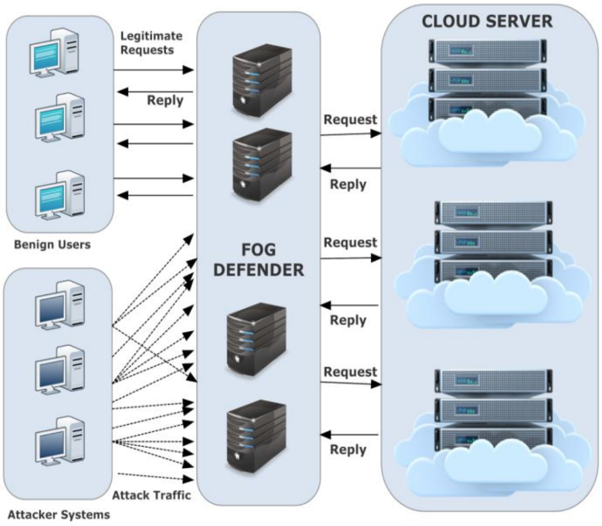


Figure 2: Framework for DDoS attack defense in cloud

In the proposed framework legitimate machines and attacker systems send request to access the cloud server and these requests are forwarded to cloud through intermediate fog devices. These intermediate fog devices are responsible for detecting the attack packets and deal with them allowing only legitimate requests to reach the cloud server. Hence, reducing the amount of traffic that reaches cloud and avoiding unnecessary use of cloud resources. Furthermore, whenever an attack is performed on a website or a system, it can be easily brought down by using a single attack. However, in case of cloud a lot more traffic is needed to make it unavailable as it provides resources as you go. Therefore, attack is generated from different machines using multiple tools and scripts to bring down the cloud server in our proposed framework.

Experimental Setup

In this experimental setup various linux and windows systems are used to generate traffic on user side. These linux and windows systems are hosted on VMware to generate traffic and a windows 10 machine accesses own Cloud as legitimate user, as shown in figure 3. Kali linux machine is used to perform SYN flood attack using metasploit interface which sends SYN packets to the victim and ettercap is used to perform DoS attack from spoofed source IP to any unused IP in the network, it generates around thousand packets in 30 seconds. Whereas, LOIC i.e Low Orbit Ion Cannon tool is run on windows 7 VM to attack the cloud server by entering server's URL or IP address. LOIC generates thousands of packets in 60 seconds and can generate TCP, UDP or HTTP traffic, for this experiment TCP traffic is generated using LOIC.

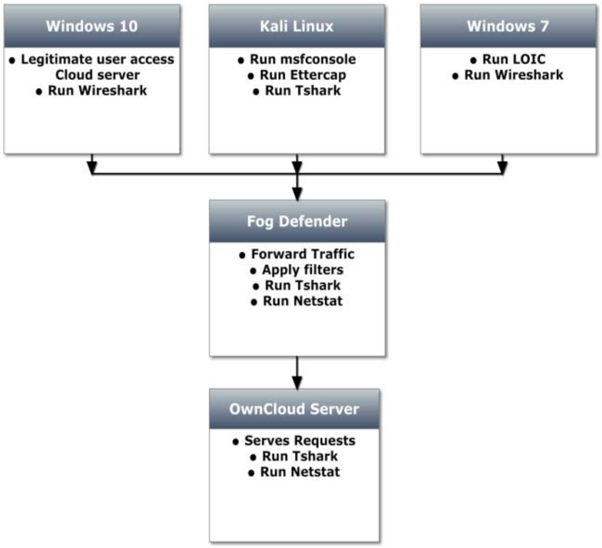


Figure. 3: Framework flow

Another module of our implementation model is fog defender; this module forwards the incoming traffic to the cloud server. Before the traffic reaches the cloud server it is analyzed and when DDoS attack is detected, the attack traffic is filtered and only the legitimate traffic is forwarded to cloud server. For our experimental setup, a linux VM and cloud server exists in fog defender layer where all these functions are performed. Furthermore, wireshark is used to captures traffic on kali and windows machines on user side whereas tshark is used on fog defender machine and Own Cloud server. Statistics of the traffic on the cloud server and linux machines is obtained using Netstat. Cloud server can be accessed by user through any machine on the network. Whenever enough DDoS traffic is generated to bring down the cloud server the users cannot access the own Cloud server anymore.

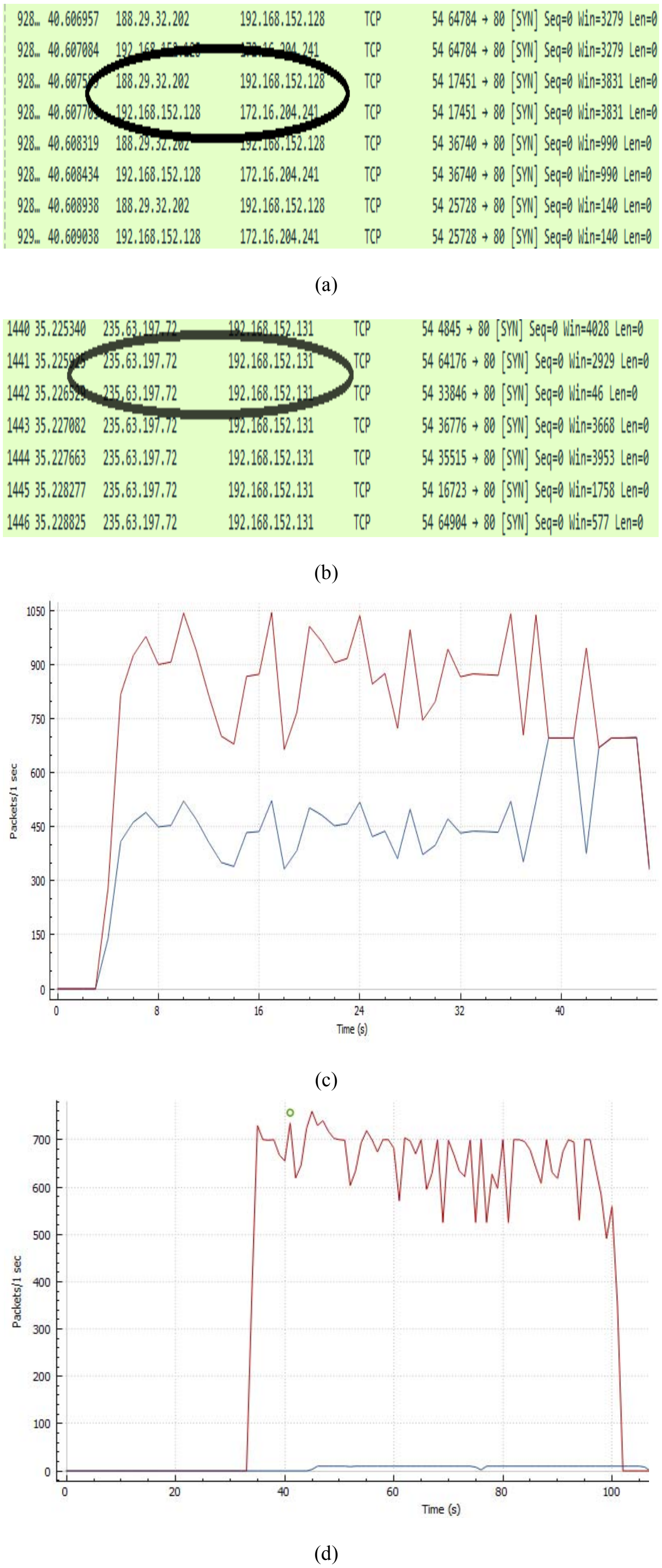
Results and Discussion

Traffic is captured when attack is performed on the system and again when attack traffic was filtered and only legitimate requests are allowed to pass through fog defender. Fog defender filters traffic on the basis of duration of attack, rate of packets, size of the packet and the protocol used. It was observed that the size of attack packets was smaller than the legitimate packets and the rate of packets of flooding attack is much higher than the legitimate packets.

Attack was performed in three phases using three different tools in our proposed scheme. First attack performed was SYN flood using metaspoit framework. It can be clearly observed in figure 4 (a) that all the attack packets originate from 188.29.32.202 IP then they passes through our fog defender machine with IP 192.168.152.128 to our cloud server i.e. 172.16.204.241. This figure shows us the flow of traffic before defense is applied on fog defender i.e, all the attack packets pass through it straight to cloud server. Moreover, figure. 4 (c) shows the total traffic on the network through red while the SYN flood traffic forwarded to cloud server is depicted using blue. The attack was performed for around 50 seconds and the attack traffic rate went to around 750 packets per second. Furthermore, figure. 4 (b) and (d) shows the scenario after defense is applied on fog defender to filter out the attack traffic. From the wireshark screenshot, it can clearly be seen that packets are not forwarded from fog defender machine i.e. 192.168.152.131 to cloud server (172.16.204.241) as they are dropped at fog defender. In the graph (figure. 4 (d)) red portrays the total TCP SYN traffic on the network during attack and blue shows the amount of TCP SYN traffic forwarded to the cloud server.

Second attack is performed using ettercap plugin for DoS attack using spoofed source IP. This attack generates a flood of TCP packets around 650 packets per second for few second and then stops. It can be seen in figure 5 (a) that attack is performed on the server for few seconds as shown by red and then this traffic is forwarded to cloud server by fog layer in burst of 40-50 icmp packets. When defense is applied on fog defender, it can be seen in figure 5 (b) that no more packets are forwarded to cloud server by fog defender as they are dropped.

Third attack is performed using LOIC tool which generate huge amount of traffic (around 10k) in matter of seconds. Tshark captured this attack traffic on cloud server as shown in figure 6 (a), this screenshot further shows the number of attack packets dropped by the cloud server defense. Whereas, figure 6 (b) depicts the total traffic on the network before applying defense along with the number of packets accepted and dropped by the cloud server after applying the defense rules.



```
928… 40.606957   188.29.32.202      192.168.152.128    TCP      54 64784 → 80 [SYN] Seq=0 Win=3279 Len=0
928… 40.607084   192.168.152.128    172.16.204.241     TCP      54 64784 → 80 [SYN] Seq=0 Win=3279 Len=0
928… 40.6075[illegible]   188.29.32.202      192.168.152.128    TCP      54 17451 → 80 [SYN] Seq=0 Win=3831 Len=0
928… 40.60770[illegible]   192.168.152.128    172.16.204.241     TCP      54 17451 → 80 [SYN] Seq=0 Win=3831 Len=0
928… 40.608319   188.29.32.202      192.168.152.128    TCP      54 36740 → 80 [SYN] Seq=0 Win=990 Len=0
928… 40.608434   192.168.152.128    172.16.204.241     TCP      54 36740 → 80 [SYN] Seq=0 Win=990 Len=0
928… 40.608938   188.29.32.202      192.168.152.128    TCP      54 25728 → 80 [SYN] Seq=0 Win=140 Len=0
929… 40.609038   192.168.152.128    172.16.204.241     TCP      54 25728 → 80 [SYN] Seq=0 Win=140 Len=0
```

(a)

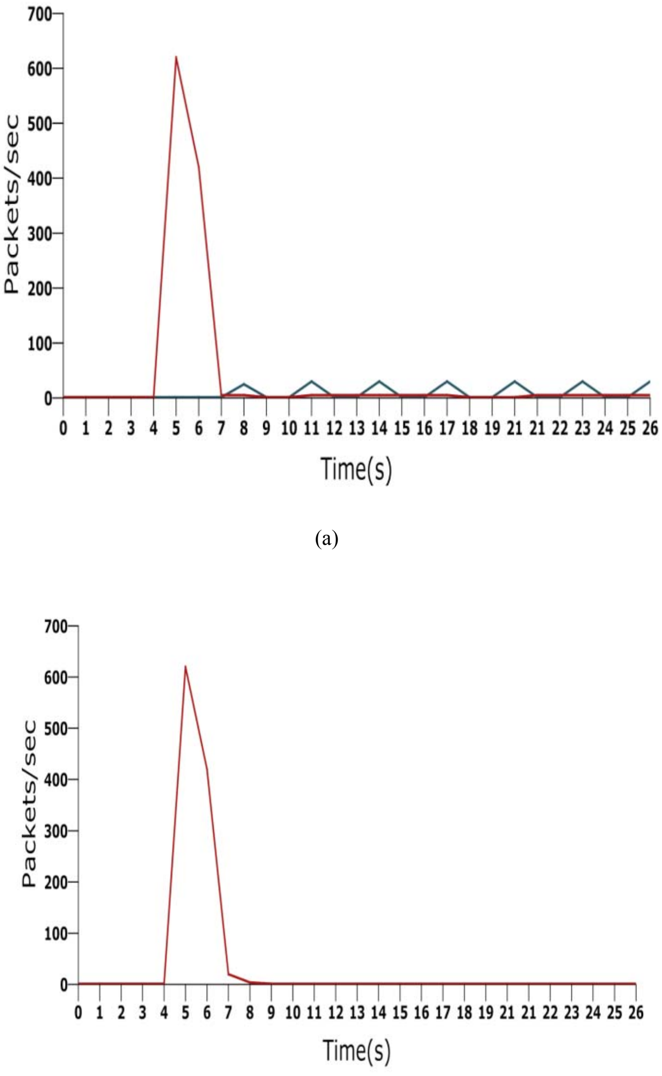
```
1440 35.225340   235.63.197.72      192.168.152.131    TCP      54 4845 → 80 [SYN] Seq=0 Win=4028 Len=0
1441 35.225925   235.63.197.72      192.168.152.131    TCP      54 64176 → 80 [SYN] Seq=0 Win=2929 Len=0
1442 35.226529   235.63.197.72      192.168.152.131    TCP      54 33846 → 80 [SYN] Seq=0 Win=46 Len=0
1443 35.227082   235.63.197.72      192.168.152.131    TCP      54 36776 → 80 [SYN] Seq=0 Win=3668 Len=0
1444 35.227663   235.63.197.72      192.168.152.131    TCP      54 35515 → 80 [SYN] Seq=0 Win=3953 Len=0
1445 35.228277   235.63.197.72      192.168.152.131    TCP      54 16723 → 80 [SYN] Seq=0 Win=1758 Len=0
1446 35.228825   235.63.197.72      192.168.152.131    TCP      54 64904 → 80 [SYN] Seq=0 Win=577 Len=0
```

(b)

(c)

(d)

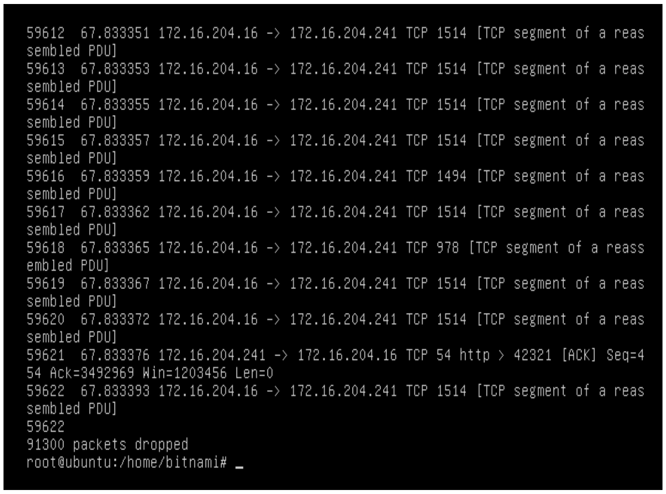
Figure 4 (a): Wireshark: traffic captured during DDoS in Cloud through fog layer, (b): Wireshark capture for attack traffic when defense is applied on fog defender, (c): Traffic captured during DDoS in Cloud through fog layer, (d): Attack traffic when defense is applied on fog defender



(a)

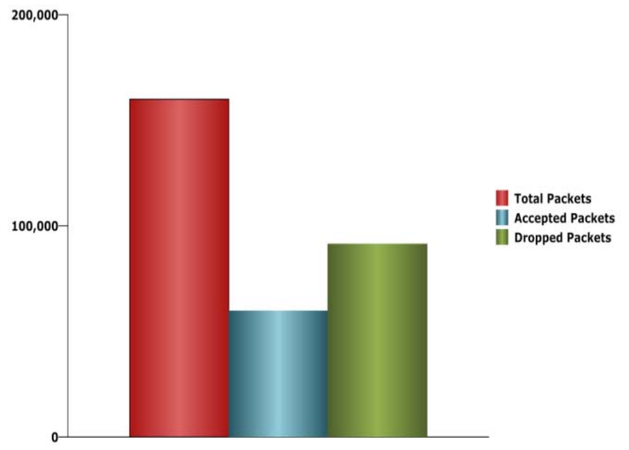
(b)

Figure 5 (a): Ettercap spoofed source IP DoS attack traffic before filtering, (b): Ettercap spoofed source IP DoS attack traffic after filtering.



```
59612  67.833351 172.16.204.16 -> 172.16.204.241 TCP 1514 [TCP segment of a reas
sembled PDU]
59613  67.833353 172.16.204.16 -> 172.16.204.241 TCP 1514 [TCP segment of a reas
sembled PDU]
59614  67.833355 172.16.204.16 -> 172.16.204.241 TCP 1514 [TCP segment of a reas
sembled PDU]
59615  67.833357 172.16.204.16 -> 172.16.204.241 TCP 1514 [TCP segment of a reas
sembled PDU]
59616  67.833359 172.16.204.16 -> 172.16.204.241 TCP 1494 [TCP segment of a reas
sembled PDU]
59617  67.833362 172.16.204.16 -> 172.16.204.241 TCP 1514 [TCP segment of a reas
sembled PDU]
59618  67.833365 172.16.204.16 -> 172.16.204.241 TCP 978 [TCP segment of a reass
embled PDU]
59619  67.833367 172.16.204.16 -> 172.16.204.241 TCP 1514 [TCP segment of a reas
sembled PDU]
59620  67.833372 172.16.204.16 -> 172.16.204.241 TCP 1514 [TCP segment of a reas
sembled PDU]
59621  67.833376 172.16.204.241 -> 172.16.204.16 TCP 54 http > 42321 [ACK] Seq=4
54 Ack=3492969 Win=1203456 Len=0
59622  67.833393 172.16.204.16 -> 172.16.204.241 TCP 1514 [TCP segment of a reas
sembled PDU]
59622
91300 packets dropped
root@ubuntu:/home/bitnami# _
```

(a)



(b)

Figure 6 (a): Tshark capture for attack traffic on Cloud Server, (b): LOIC Attack traffic defense

CONCLUSION AND FUTURE WORK

Cloud computing can clearly be seen as today's most alluring technology, at least in terms of being cost efficient and its flexibility. It helps accomplish more by paying less. But enterprises are reluctant to use cloud because they are concerned with the security issues in cloud like DDoS attack. In this paper, we have presented a framework where DDoS attack traffic while passing through fog defender was detected and filtered by applying rules at this layer and only legitimate requests were forwarded to ownCloud server. Therefore, the request that reaches cloud is legitimate ones. As detection and mitigation of DDoS attack is done at the edge of the network and not cloud, it leads to better response time and resource utilization in cloud. Whereas, this approach only provides defense from TCP and HTTP attack traffic. Hence, its can be improved to defend other protocol traffics like ICMP, UDP etc. Furthermore, if servers can be used as fog devices more intelligence can be brought to the edge of the network as servers can be used to perform load balancing and provide real time decision making for time critical applications.

REFERENCES

1. Palmieri, Francesco, Ugo Fiore, and Aniello Castiglione. "A distributed approach to network anomaly detection based on independent component analysis." Concurrency and Computation: Practice and Experience 26, no. 5, pp. 1113-1129, 2014.
2. B.B Gupta, and Omkar P. Badve. "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment."Neural Computing and Applications: pp. 1-28. Springer 2016.
3. Bonomi, Flavio, Rodolfo Milito, Preethi Natarajan, and Jiang Zhu. "Fog computing: A platform for Internet of things and analytics." In Big Data and Internet of Things: A Roadmap for Smart Environments, pp. 169-186. Springer International Publishing, 2014
4. Gupta, Sanchika, Padam Kumar, and Ajith Abraham. "A profile based network intrusion detection and prevention system for securing cloud environment." International Journal of Distributed Sensor Networks 9, no. 3: 364575.
5. Bonomi, Flavio, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli. "Fog computing and its role in the Internet of things." In Proceedings of the first edition of the MCC workshop on Mobile cloud computing, pp. 13-16. ACM, 2012
6. "Cloud Attack: Economic Denial of Sustainability (EDoS)", elasticvapor,.[Online].Available:http://www.elasticvapor.com/2009/01/cloud-attack-economic-denial-of.html. [Accessed: 07- Sep- 2016].
7. B Wang, Y. Zheng, W. Lou, Y. Hou "DDoS attack protection in the era of cloud computing and software-defined networking" , Computer Network, pp. 308-319, Elsevier, 2015.
8. Somani, Gaurav, Manoj Singh Gaur, Dheeraj Sanghi, and Mauro Conti. "DDoS attacks in Cloud Computing: Collateral Damage to Non-targets."Computer Networks, pp. 157-171, Elsevier, 2016.
9. Chaitanya Buragohain, and Medhi Nabajyoti. "FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers." In Signal Processing and Integrated Networks (SPIN), 3rd International Conference on, pp. 519-524. IEEE, 2016.
10. B.B.Gupta, Ramesh C. Joshi, and Manoj Misra. "Dynamic and auto responsive solution for distributed denial-of-service attacks detection in ISP network." arXiv preprint arXiv: 1204.5592, 2012.
11. Agarwal, Swati, Shashank Yadav, and Arun Kumar Yadav. "An Efficient Architecture and Algorithm for Resource Provisioning in Fog Computing." International Journal of Information Engineering and Electronic Business 8, pp. 48-61, MECS press, 2016.
12. Aazam, Mohammad, and Eui-Nam Huh. "Fog computing and smart gateway based communication for cloud of things." In Future Internet of Things and Cloud (FiCloud), International Conference on, pp. 464-470. IEEE, 2014.
13. Fayaz, Seyed K., Yoshiaki Tobioka, Vyas Sekar, and Michael Bailey. "Bohatei: Flexible and elastic DDoS defense." In 24th USENIX Security Symposium (USENIX Security 15), pp. 817-832, 2015.
14. Kishor, Kunal, and Vivek Thapar. "An Efficient Service Broker Policy for cloud computing environment." International Journal of Computer Science Trends and Technology (IJCST) 2, pp. 104-109, 2014.
15. Alomari, Esraa, Selvakumar Manickam, B. B. Gupta, Mohammed Anbar, Redhwan MA Saad, and Samer Alsaleem. "A Survey of Botnet-Based DDoS Flooding Attacks of Application Layer: Detection and Mitigation Approaches." In Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, pp. 52-79. IGI Global, 2016.
16. P. Djalaliev, M. Jamshed, N. Farnan, J. Brustoloni, "Sentinel: Hardware-accelerated mitigation of bot-based ddos attacks", Proceedings of 17th International Conference on Computer Communications and Networks, pp. 1–8, IEEE, 2008.
17. Gu, Guofei, Phillip A. Porras, Vinod Yegneswaran, Martin W. Fong, and Wenke Lee. "BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation." In Usenix Security, vol. 7, pp. 1-16. 2007.
18. Gu, Guofei, Roberto Perdisci, Junjie Zhang, and Wenke Lee. "BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection." In USENIX Security Symposium, vol. 5, no. 2, pp. 139-154. 2008.
19. Khattak, Sheharbano, Zaafar Ahmed, Affan A. Syed, and Syed Ali Khayam. "BotFlex: A community-driven tool for botnet detection." Journal of Network and Computer Applications 58, pp- 144-154, 2015.
20. Kriti Bhushan, and B.B. Gupta, "Security challenges in cloud computing: state-of-art", Int. J. Big Data Intelligence, Vol. 4, No. 2, pp.81–107, 2017.