Mitigating DDoS Attacks on Cloud Networks with Hypervisor Based Security

Sonia Narula[1], Jyoti Sahni[2*] & Kavita Khanna[3]

[1]M. Tech Student, Department of CSE, The NorthCap University, Gurugram, India

E-mail Id: *narula.sonia@gmail.com*

[2]Assistant Professor, Department of CSE, The NorthCap University, Gurugram, India

[*]Corresponding Author E-mail Id: *jyotika.sahni@gmail.com*

[3]Associate Professor, Department of CSE, The NorthCap University, Gurugram, India

E-mail Id: *kvita.khanna@gmail.com*

Abstract: Distributed Denial of Service (DDoS) attacks are a major threat to Cloud based systems. This is because DDoS attacks can lead to large financial losses to any revenue generating services hosted on Cloud platforms. To deal with the distributed denial of service (DDoS) attacks, one critical issue is to effectively isolate malicious traffic from the normal traffic. In this work we have proposed a Cloud based DDoS attack detection mechanism that uses PEFT (Penalizing Exponential Flow-spliTting). PEFT is an unequal cost Traffic Engineering approach and can prove to be efficient mechanism to improve DDoS detection over Cloud data center topologies. The proposed method employs PEFT to identify exponential traffic coming from malicious users that can then be redirected to outside the Clouds intranet. The routers can direct malicious traffic to paths outside the network, with an exponential penalty on malicious paths that are used by the attacker. Experimental results indicate that the proposed technique presents an efficient way to identify DDoS attacks.

Keywords: Cloud Computing, Security, DDoS, VM Hypervisor

I. INTRODUCTION

Now a day, technology plays a crucial role in human life. In recent times every business is being carried out with the help of Internet and associated services. Cloud computing is a new technology in the IT marketplace which delivers computing services as a public utility on a pay per use model. It however requires that the Cloud service consumers are connected to excessive-speed Internet connection so as to access the Cloud services hosted in Cloud datacenters. Cloud platforms offer huge advantages in comparison to fixed on-premise infrastructures. These advantages include pay as you go billing, on-demand resource availability, better hardware utilization, no protection overhead and no in-house depreciation losses. On the other hand, there are numerous questions that need to be addressed before Cloud is adopted to its full potential [1-2]. Most of these questions are particularly related to security and information protection [3]. Although, many security approaches exist that are targeted to the traditional non-Cloud IT infrastructures; however, these approaches are not suitable for Cloud centered security as there are certain issues in a Cloud platform that are different from non-Cloud platforms [3]. As a result, there is a strong need for implementing efficient security mechanisms for Cloud platforms.

Out of many attacks that can target an Internet based service, Denial of Service is one of the drastic attacks which target the servers with millions of packets so that legitimate users are unable to login into the main server or the target website [4]. DoS attackers' target the server that supplies the services to its customers. DDoS attackers, behave like a valid consumer and attempt to flood the service's active server with a large number / variety of requests so that the provider faces a flood of requests at its service queue and subsequently becomes unavailable. A special case of DoS is Distributed DoS, or DDoS, wherein attackers are a collection of machines that focus on a provider [5]. There has been an

excessive increase in the variety of incidents of DDoS, in recent years, which makes it one of the most crucial and deadly attack amongst many [5]. More than 20% of organizations have mentioned DDoS occurrence at their Cloud services [6]. Examples include Lizard Squad that attacked the Microsoft gaming services, a Cloud service, on the day of Christmas 2015. Sony, also faced similar DDOS attack on their gaming services resulting in shutting down of all the services in the same year [7]. One of the other surprising DDOS cases include the one on Cloud servers of Amazon. Due to this attack, Amazon had to face heavy downtime, commercial enterprise loses and a lot of long time and short-time period effects on its commercial enterprise processes [8]. DDOS attacks have the capability to destroy all the layers of a Cloud platform. VeriSign defense Security Intelligence Services [9] suggests that the DDoS attacks target mostly the IaaS and SaaS layer in Cloud platforms. This work focusses on security at the IaaS layer.

The rest of this paper is organized as follows. Section 2 details the levels of security at IaaS layer in Cloud. Related work is presented in section 3. Section 4 presents the proposed model, followed by experimental evaluation in section 5. Finally, section 6 presents the results.

II. LEVELS OF SECURITY IN IAAS

Security in IaaS can be implemented at two levels (Figure 1):

a) Hypervisor

b) Virtual Machine (VM)

Figure 1: Levels of Security at IaaS

a) Hypervisor Security

As per NIST [11], Hypervisor is a layer that separates the host machines from the guest machines. Hypervisor, thus, is the centralized controlling agent for all the VM's and have its own security zone. There are many in built safety programs in a VM environment, but these are not efficient to cater to the attacks being made presently [3]. There might be vulnerability in hypervisor due to which an attacker may take over the complete control of the hypervisor. For example, Virtual escaping [12] is an attack that takes full control of a hypervisor. To conquer with Virtual escaping, several secure APIs are built to govern and disable this operation within VMs, but this API affects the performance of the hypervisor. Hypervisor security is the practice of ensuring that the hypervisor is safe throughout its life including during development time, at time of implementation, provisioning, management and de-provisioning.

b) Virtual Machine Security

Hypervisor technology enables Infrastructure Service users to have access to virtual machine's which are implemented upon physical servers. A VM can be used through Internet, so it becomes necessary to take adequate defensive measures so as to secure the network access to VMs and provide adequate security to hosted services. Infrastructure Service involves a threat when a new VM is installed, modification in the VM configuration is made etc., which creates VM's or servers unsafe. Thus,

protecting the VM in Cloud need powerful secure mechanisms. Some recommendations have been proposed in [10] to ensure security of VMs.

III. RELATED WORK

This section discusses the related work in identification of DDoS attacks in Cloud.

A detailed survey on DDoS attacks in Cloud computing is presented in [13]. The survey presents a detailed insight into the characterization, prevention, detection, and mitigation mechanisms of the DDoS attacks. The survey also presents a detailed discussion on the important metrics that can be used to evaluate various solutions for handling DDoS attacks. It further gives a comprehensive taxonomy to classify the different solutions proposed in literature to cater to the different DDoS attacks.

O. A. Wahab et al. in [14] target the security issues arising in Cloud when services owned by different providers are grouped together. They proposed a three-fold solution that includes: trust establishment framework; bootstrapping mechanism and trust-based hedonic coalitional game. Their approach is resilient to collusion attacks and targets minimizing number of malicious services.

Wahab, Omar Abdel, et al, in [15] proposed a hypervisor-based model for detection of DDoS attacks that caters to the issues that occur due to Cloud's elastic and multi-tenant properties. They proposed a two-fold solution that allows establishing a credible trust relationship between a hypervisor and the guest Virtual Machines (VMs). This is achieved by employing a mix of objective and subjective trust sources and aggregating them using Bayesian inference. They further designed a trust-based maximin game between DDoS attackers and the hypervisor. The DDoS attackers try to minimize the Cloud system's detection while the hypervisor tries to maximize this minimization under limited budget of resources. The game solution guides the hypervisor in determining the optimal detection load distribution among VMs in real-time that maximizes the possibility of DDoS attacks' detection.

A defense system, Dolus has been proposed in [16] to diminish the impact of DDoS attacks on important services hosted in SDxI-based Cloud platforms. The proposed Dolus device can initiate a 'pretense' in a scalable, collaborative way to prevent the attack. This is done using a two-stage ensemble learning scheme that is based on the risk intelligence received from attack feature evaluation. Dolus makes use of elastic capability provisioning and SDxI policy co-ordination across multiple network domains to confuse the attacker by creating a false sense of success.

Somani et al. in [17] formulate the DDoS mitigation trouble as an OS degree resource control trouble. They proposed a resource containment technique to impose the victim server's resource limits. Their approach focusses on providing isolated timely resources so as to ensure availability of other critical services.

Gupta and Kumar in [18] uses the fact that during DDoS attack packets are sent at a very heavy rate and propose a profiling and back off based detection strategy for detection of DDoS attacks in Cloud. The solution proposed provides lowest resource requirements at the same detection speed.

IV. PROPOSED APPROACH

In this work a DDOS attack security mechanism for Cloud computing environment is proposed where malicious traffic is identified by using Penalizing Exponential flow-splitting (PEFT) method [19]. PEFT is an unequal cost Traffic Engineering (TE) technique and can prove to be the most effective and feasible mechanism to provide security and to improve performance for the Cloud networks. Cloud providers manage the traffic flow in their networks by using the configuration of the inbuilt routing methods in the Hypervisor. PEFT algorithm can be used to identify the presence of exponential traffic coming from malicious users. These can then be redirected to dummy unused paths in the network. PEFT algorithm has specially two functions: traffic computation and traffic peak identification. Traffic computation involves distribution of the traffic and traffic forwarding. Traffic peak identification

function is mainly used to find out the traffic patterns when there is exponential rise. They help in predicting the shortest path for forwarding the packets. PEFT also helps in balancing the distribution of traffic and in finding out the time slots when the DDOS attack happens. Penalizing exponential flow splitting method mainly involves the following steps:

- Traffic computation
- Peak Identification
- Packet forwarding

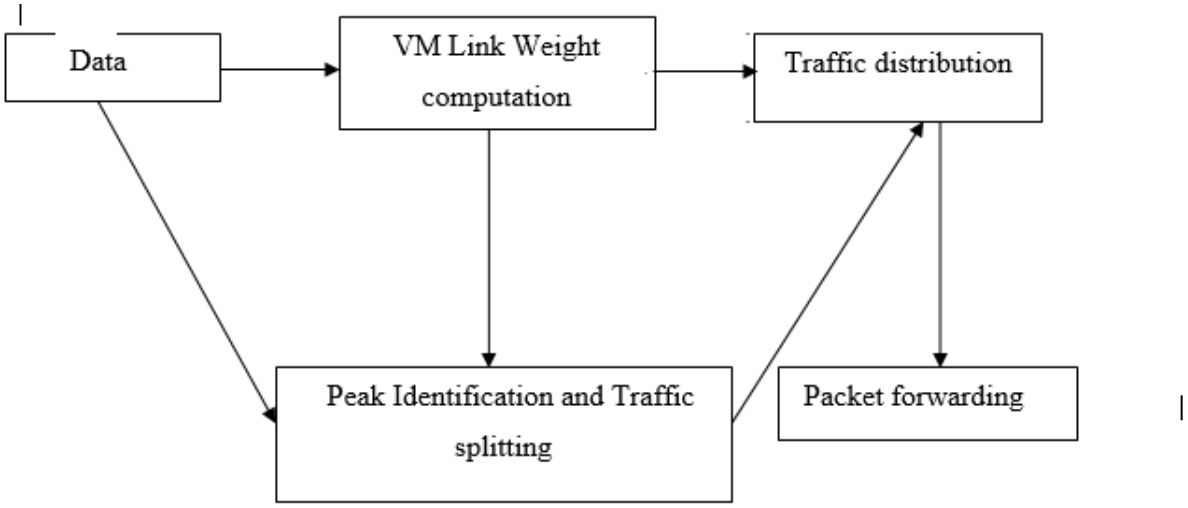

Fig 2: Proposed Hypervisor based PEFT for DDoS Malicious Traffic identification

V. EXPERIMENTAL EVALUATION

This section presents the experiments performed for evaluation of the proposed model.

The experiments have been performed using oracle VirtualBox [20] for building our Cloud testbed, Wireshark [21] for traffic analysis, and Matlab [22] for implementing PEFT and DDoS detection. Virtual Box is a cross-platform virtualization application. Wireshark is a tool for the analyzing the packets and capture the packet data from the network. MATLAB is a multi-paradigm numerical computing environment that allows manipulation of matrices, graph plotting, algorithm implementation etc. Table 1 gives the details of the experimental setup.

Table 1. Experimental Setup

Hypervisor	Oracle VM
No of Attacks	25-100
Attack Type	DDOS – Ping of Death
NO. OF VM	3
VM Configuration	1 CPU, 512 MB RAM, CPU execution cap 50%

For the experiments, DDOS attack were initiated on one of the VMs using the other two VMs in parallel by executing the ping of Death attack. Figure 4 shows the comparison of the traffic observed under normal conditions and the traffic observed during DDoS attack. The proposed method identifies the traffic peaks which are then employed for identification of DDoS attacks using PEFT (figure 5).

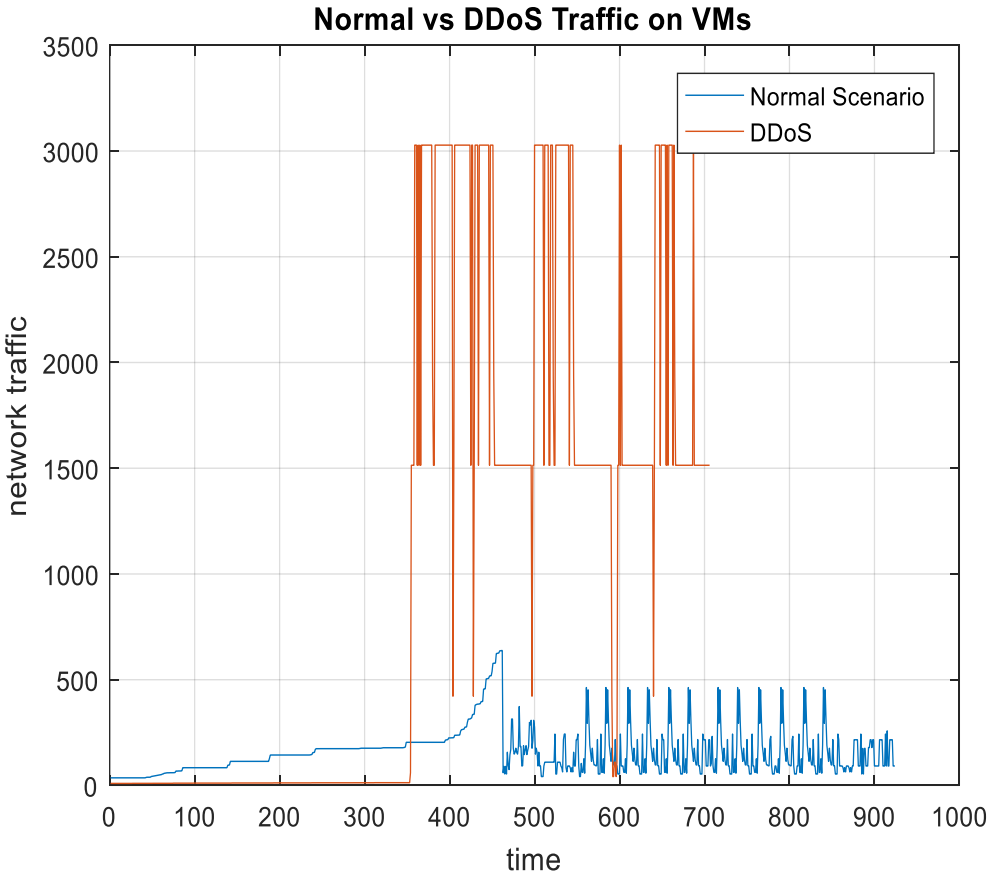

Figure 4. Comparison of Normal V/S DDoS Traffic

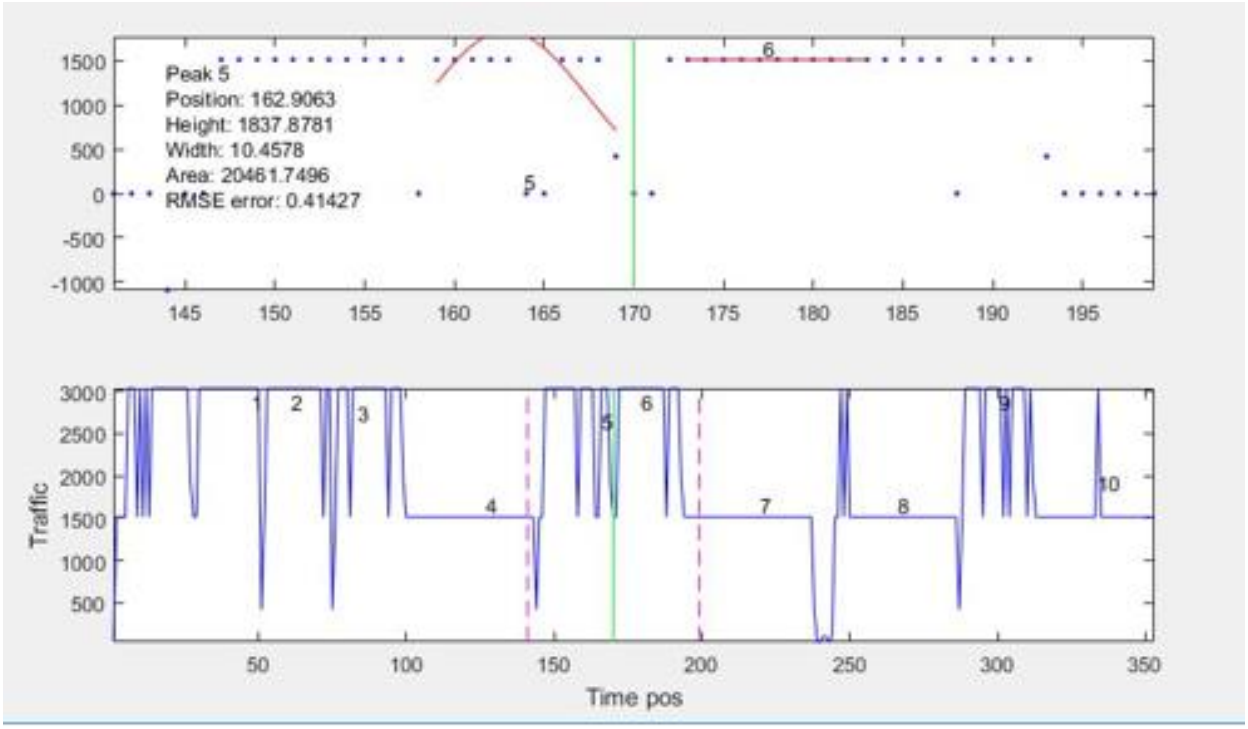

Figure 5. Traffic peaks identified during DDoS attack

The traffic peaks are then input to PEFT for identification of possibility of a DDoS attack. Table 2 lists the detection accuracy of the proposed method, which is found to be 91.84%.

Table 2. DDoS Detection Accuracy of the proposed work

Scenario	*Actual Attack Times*	*Predicted Attack Times*
1	7	6
2	12	9
3	8	10
4	6	5
5	6	6
6	9	7
7	5	6
8	7	5
9	11	10
10	14	14
11	13	12
	98	90
Detection Accuracy		91.84%

VI. CONCLUSION

This work proposed a DDoS detection mechanism in Cloud Computing Environment. Penalizing Exponential Flow Splitting algorithm has been employed for detection of DDoS attacks. Experimental results indicate that the proposed Algorithm is very effective in identification of DDoS Attacks with accuracy rate of 91.84%. In future we intend to extend the proposed work to include traffic profiling information that may be used for early detection of DDoS attacks.

Conflict of interest: The authors declare that they have no conflict of interest.

Ethical statement: The authors declare that they have followed ethical responsibilities.

REFERENCES

[1] Kaufman, L.M., 2010. Can public-cloud security meet its unique challenges? IEEE Security & Privacy, 8(4), pp.55-57.
[2] Kaufman, L.M., 2009. Data security in the world of cloud computing. IEEE Security & Privacy, 7(4).
[3] Zissis, D. and Lekkas, D., 2012. Addressing cloud computing security issues. Future Generation computer systems, 28(3), pp.583-592.
[4] Mirkovic, J. and Reiher, P., 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), pp.39-53.
[5] Mansfield-Devine, S., 2015. The growth and evolution of DDoS. Network Security, 2015(10), pp.13-20.
[6] Available at: https://www.kaspersky.co.in/, Global IT Security Risks Survey 2014 - Distributed Denial of Service (DDoS) Attacks, last accessed May 25, 2018
[7] Available at: https://en.wikipedia.org/wiki/Lizard_Squad, last accessed May 25, 2018
[8] http://www.networkworld.com/article/2900125/malwarecybercrime/criminals-/moving-into-Cloud-big-timesays-report.html ,Cybercriminals Moving into Cloud Big Time, Report Says, last accessed May 25, 2018
[9] Available at: http://www.infosecurity-magazine.com/news/q1-2015-ddos-attacks-spike/, Q1 2015 DDoS Attacks Spike, Targeting Cloud, last accessed May 25, 2018
[10] Securing Virtualization in Real-World Environments 2009, Virtualization White paper IBM.
[11] Available at: https://www.nist.gov/topics/cloud-computing-virtualization,

[12] Available at: https://en.wikipedia.org/wiki/Virtual_machine_escape, Virtual machine escape, last accessed May 25, 2018

[13] Somani, G., Gaur, M.S., Sanghi, D., Conti, M. and Buyya, R., 2017. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, pp.30-48.

[14] Wahab, O.A., Bentahar, J., Otrok, H. and Mourad, A., 2016. Towards trustworthy multi-cloud services communities: A trust-based hedonic coalitional game. IEEE Transactions on Services Computing

[15] Wahab, O.A., Bentahar, J., Otrok, H. and Mourad, A., 2017. Optimal load distribution for the detection of VM-based DDoS attacks in the cloud. IEEE Transactions on Services Computing

[16] Neupane, R.L., Neely, T., Chettri, N., Vassell, M., Zhang, Y., Calyam, P. and Durairajan, R., 2018. Dolus: Cyber Defense using Pretense against DDoS Attacks in Cloud Platforms

[17] Somani, G., Gaur, M.S., Sanghi, D., Conti, M. and Rajarajan, M., 2017. DDoS victim service containment to minimize the internal collateral damages in cloud computing. Computers & Electrical Engineering, 59, pp.165-179

[18] Gupta, S. and Kumar, P., 2017. Profile and back off based distributed NIDS in cloud. Wireless Personal Communications, 94(4), pp.2879-2900.

[19] Xu, D., Chiang, M. and Rexford, J., 2011. Link-state routing with hop-by-hop forwarding can achieve optimal traffic engineering. IEEE/ACM Transactions on networking, 19(6), pp.1717-1730.

[20] Available at: https://www.virtualbox.org/, Oracle VM VirtualBox, last accessed May 25, 2018.

[21] Available at: https://www.wireshark.org/, Wireshark, last accessed May 25, 2018.

[22] Available at: https://in.mathworks.com/products/matlab.html, Matlab, last accessed May 25, 2018.

This volume is dedicated to Late Sh. Ram Singh Phanden, father of Dr. Rakesh Kumar Phanden.

