Detecting DNS Reflection Amplification DDoS Attack Originating from the Cloud

Ahmed K. Soliman, Dr. Cherif Ramzy Salama,Prof Dr. Hoda K. Mohamed
Computer Engineering and systems department
Faculty of Engineering, Ain Shams University
Cairo, Egypt
Eng.ahkamal@gmail.com, cherif.salama@eng.asu.edu.eg, hoda.korashy@eng.asu.edu.eg

***Abstract*— Different sizes of businesses are currently moving to the cloud as it is considered a key business enabler due to its benefits like minimizing the go live time and reducing the associated resources. Moving to the cloud introduces several confidentiality, integrity, and availability concerns. One of the key issues that affect availability is Distributed Denial of Service (DDoS). In such attacks, a cloud can be the source or the victim. DDoS attacks on a cloud can be much more harmful than its impact on a single physical server. One of the most recognized DDoS types is DNS reflection amplification attack. In this paper, we introduce a new technique to limit the sources of DNS reflection amplification attacks. In particular, we make use of the role of cloud hypervisors in managing all the virtualization environment traffic. The proposed technique can prevent scenarios ISP edge router ingress filtering will fail to prevent and is easier to implement.**

Keywords—DDOS, DNS Reflection Amplification Attack, Cloud, Hypervisors

I. Introduction

As per National Institute for Standards and Technology (NIST)'s definition [1], cloud computing is a model for enabling ubiquitous, convenient, on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing has three main service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). It has four deployment types: private cloud, community cloud, public cloud, and hybrid cloud.

Different sizes of businesses are currently moving to the cloud as it is considered a key business enabler due to its huge benefits like minimizing the go live time and reducing the required resources [2]. Moving to the cloud introduces several confidentiality, integrity, and availability concerns [3]. One of the key issues that affect availability is Distributed Denial of Service (DDoS)[4].

In this paper, we propose a technique that helps mitigate some types of DDoS attacks. Our main contributions are:

- We propose a novel hypervisor based ingress filtering technique, that we label HIF.
- We provide attack scenarios that cannot be prevented by traditional filtering techniques and can be successfully prevented by HIF.
- We provide a prototype implementation for the HIF and demonstrate its success in detecting suspicious traffic.

The next section introduces DDoS attacks with emphasis on the type targeted by this work. In Section III, we discuss known mitigation techniques and their limitations. We present our proposed solution in Section IV and detail our implementation in Section V. Section VI discusses the obtained results.

II. DDoS Attack

Distributed denial of service is one of the major attacks happening in our world these days. The first reported incident took place in 1999 [5]. DDoS focuses on making the computing resources lose their main function by not providing it to their legitimate users. In 21 October 2016, one of the largest DDoS attacks took place, and had a very bad impact on the Internet service [6]. In the following subsections, we will expand on the DDoS components; on IP spoofing, a technique typically needed by DDoS attackers; on DDoS attack categories and types, and on DDoS effect on the cloud.

A. DDoS Components

A DDoS attack has four components [7] as illustrated in Fig.1.

These components are:

1) Attack Master: The one behind the attack. He starts his work by scanning the Internet to find out nodes with vulnerabilities so he can use them in his attack. The attack master is very hard to find due to the usage of IP spoofing.

2) Handlers: Control the bots on behalf of the attack master.

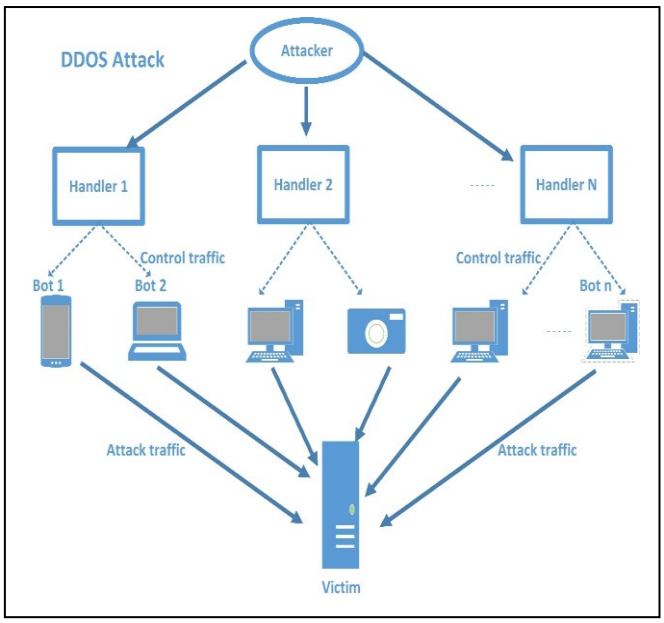

Fig. 1. DDoS Components (Adapted from [7])

3) Handlers: Control the bots on behalf of the attack master.

4) Bots: Agents already compromised by the attack master (PCs, Laptops, and lately IoT devices) and used to overwhelm the victim. There are three main categories of bots Internet Relay Chat based (IRC-based), Web-based, and Point to Point based (P2P-based) [7].

5) Victim: The attack target.

B. IP spoofing

IP spoofing is one of the major pillars for DDoS attack especially in case of a DNS reflection amplification attack. In IP spoofing, the attacker forges the IP address of the packet source IP field then send these packets to a server who will reflect this traffic to the victim. The attacker can repeat this behavior from several bots at the same time to maximize the attack's magnitude [8].

C. DDoS Attack Categories

DDoS attacks have different formats, but in general, they can be grouped into two main categories:

- The first category is traffic targeting a specific vulnerability, or sending malformed packets to a specific protocol.
- The second category is traffic targeting the service provider resources (e.g., connectivity, network resources) or server resources (e.g., sockets, Memory, CPU, I/O Bandwidth).

The proposed technique in this paper mitigates the latter category of DDoS attacks.

D. DDoS Attack Types

The following is a list of different types of DDoS attacks:

- Flood Attack: The attacker overwhelms the victim bandwidth by a huge volume of traffic with the help of botnets, so that the victim legitimate users cannot get the service they should have.
- Smurf attack: It is the first of its kind DDoS amplification attack. The attacker sends Internet Control Message Protocol (ICMP) requests to one of the network's router broadcast addresses with the source address forged with the victim IP. The router then forwards these packets to all the devices behind it causing them, in turn, to reply to the victim's IP with ICMP responses. Using this mechanism, the traffic is amplified by the number of devices behind the router. This technique depends on the idea that ICMP does not have handshaking so the destinations cannot verify whether the source is legitimate or not.
- Fraggle attack: It is an attack somehow similar to the Smurf attack in which the ICMP packets are replaced with User Datagram Protocol (UDP) packets targeting the character generating ports in the devices behind the router, which makes the traffic size larger.
- SYN flood attack: This attack exploits the vulnerability of TCP's 3-way handshake. The normal TCP transaction starts by the sender sending a SYN packet to the receiver for which the receiver responds by sending a SYN-ACK packet and then the sender responds with an ACK packet. In the SYN flood attack, the sender sends too many SYN packets without responding later with an ACK packet. Sending all these SYN packets makes the victim reserve a large amount of its resources, which slow down its response for its legitimate users. SYN flood attacks either can be direct, spoofed-based, or distributed [9].
- HTTP (GET-POST) attack: This attack requires more understanding of the victim business. Using HTTP attack does not require a huge traffic to affect the victim, and it is so hard to be identified, as the attack traffic is similar to the regular traffic.
- DNS reflection amplification attack: The attacker triggers DNS servers to respond with a huge traffic size to overload all the victim servers. DNS reflection amplification attack requires the attacker to implement two steps. First, the attacker spoofs the IP address of the victim and sends queries to DNS servers using the victim's source IP. Second, he generates queries having response sizes more than 60 times the request size [10], [11]. DNS reflection amplification attack can be categorized to three main subtypes; repeated attacks, varying query attacks, and distributed attacks [11]. All these subtypes rely heavily on the usage of IP spoofing and on having response sizes that are multiples of the main request size. Commands like ANY, DNSKEY, NS, or RRSIG used to generate this large attack size.

DNS amplification attacks form 34.9% of the large DDoS attacks [12]. The technique proposed on this paper focuses on this particular attack type although it can also help in the detection of any DDoS attack that uses IP spoofing.

E. *DDoS Effect on the Cloud*

Cloud computing is giving the world a new dimension with how easy/fast to have many new machines live. Cloud computing may be the victim or the attack source specially if the cloud Hypervisor is compromised, and in both cases DDoS impact is magnified. If the cloud is the source of attack imagine the size of traffic coming from this huge number of resources, and if it is the victim imagine the number of services, affected by this attack.

Not like physical servers Clouds have huge number of resources so to mitigate DDoS effect Clouds dedicate extra resources to the effected services which means extra cost to be paid for illegitimate traffic as the Cloud is based on the concept pay as you use which introduce a new type of DOS which known as Economic Denial of Service (EDOS).

III. DDoS MITIGATION TECHNIQUES

DDoS mitigation techniques can be categorized in different ways, some of these are [7]: -

- Deployment location: Either source based, destination based, network based, or hybrid.
- Point in time: Before, during, or after the attack
- Since this paper's work focus on DNS reflection amplification attacks, we will concentrate on techniques that mitigate this type.

F. *Ingress/egress filtering*

In general ingress/ egress filtering is one of the DDoS prevention techniques which take place at the attack source ISP edge router level by which the ISP prevent traffic from source IP out of the range of the network this traffic is coming from. This prevention technique initiated after BCP38 [13] to defeat IP spoofing. Ingress filtering has some limitations as the attacker may still spoof IPs for victims within the same range IPs as shown in Fig. 2, and that some ISPs do not find incentive in deploying costly firewalls to apply ingress filtering. As per [14] until now 25% of ISPs still allow IP spoofing.

G. *Firewalls*

Using firewalls [10], you can block any unwanted traffic according to its (source, type, request type, etc.) so we can configure the firewall block all ANY requests as it is not essential for most users, but this have the following drawbacks:-

- This can block a percentage of legitimate traffic.
- The attacker can change the used queries like Resource Record Signature (RRSIG), DNSKEY that will have bad effect also.
- Blocking the traffic from specific source may be one of the targets of the attacker to disconnect the victim from the world.

H. *Request Count and hop count*

In this type [15], a threshold is set so that if the number of requests exceeded this threshold the traffic from this source IP is considered as possible attack source. Then packets form this suspicious source IP is forwarded for further investigation. The attacker can forge any part in the packet except the Time to live (TTL) part as it is decreased by each network device the packet pass through. To distinguish between legitimate traffic and spoofed traffic the hop counts to the source IP is counted, packets having same TTL are handled as legitimate traffic, and the rest of the traffic from this IP is dropped.

IV. PROPOSED TECHNIQUE

Hypervisors are the core component in a cloud system. All traffic getting from/to virtual machines (VMs) are passing through them. Hypervisors are aware of the VMs details like their legitimate IP and MAC addresses and to which network the VMs are attached.

Our main idea is to take advantage of the hypervisor's knowledge to detect suspicious traffic. We propose a new ingress filtering technique that we call Hypervisor Ingress Filtering (HIF) to filter attacks coming from the clouds.

This proposed technique has fewer limitations than the ISP edge router ingress filtering have since the hypervisor has more knowledge. HIF is used to monitor, highlight, and prevent spoofed traffic coming from any VM managed by the hypervisor.

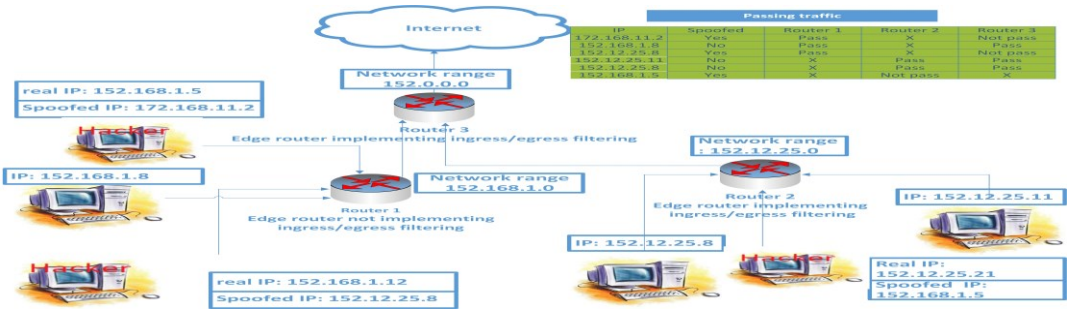

Fig. 2. :Ingress/ Egress filtering

One of the steps of VM creation is the assignment of MAC address, then attaching this VM to specific network interface with an IP address (DHCP, or static IP). This allows the hypervisor to know the full legitimate details about the VM connectivity.

We will add a function so that if a suspicious / spoofed traffic is coming out from this VM, the hypervisor will be able to capture it, and forward it for further investigation.

Generally, HIF have many features, which make it better solution to handle DNS reflection amplification DDoS attacks originating from the cloud:-

- The number of hypervisors vendors are so limited in compare to the number of ISPs all over the world.
- Most of the current hypervisors are software based so to have HIF implemented just software update is needed meanwhile implementing ISP edge router ingress filtering require having firewalls deployed at the ISP level (including what this entire means from technical details, and high cost).
- The implementation cost of HIF is cheaper in compare to the implementation of ISP edge router ingress filtering.

V. IMPLEMENTATION

The implementation of this technique and its trial main components are:-

I. Hypervisor

To run this experiment we made use of open source hypervisor, which is Virtual Box [17]. Virtual Box is free to use under GNU General Public License. Using Virtual Box, we can host the VMs that will generate/ receive the attack.

J. Host

We used a PC with 8G RAM, processor core I7 virtualization enabled, and windows operating system.
We created two VMs (attacker, and victim) to simulate the regular traffic, and the attack. Each VM is running Windows 2008.

K. Traffic generator

To generate attack like traffic, ready-made tools are available with the fame of having mal-wares.

Raw socket library was one of the options to generate the needed traffic, but while working under windows I discovered that, the Windows OS already put some restrictions to RAW socket usage to limit the opportunity to generate spoofed traffic.

PcapDotNet SDK used to generate the required traffic. To simulate the DNS amplification reflection attack, the generated attack traffic should be (Ethernet, IP, UDP, DNS (QR= query), question type (QTYPE) =Any, DNSKEY, NS, or RRSIG)) as declared in Fig. 3, and Fig. 4.

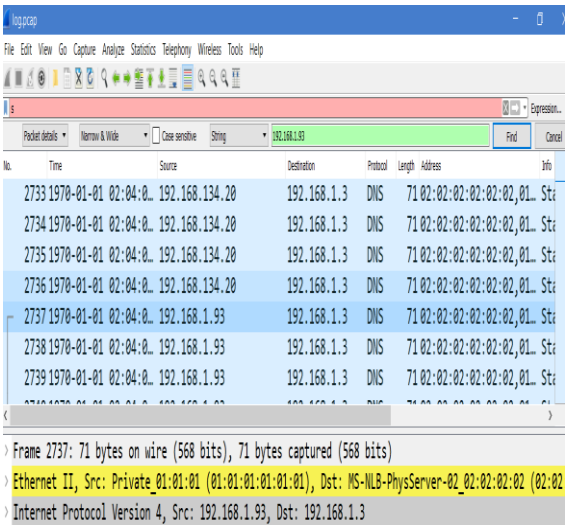

Fig.3. : Attack traffic generated using PcapDotNet

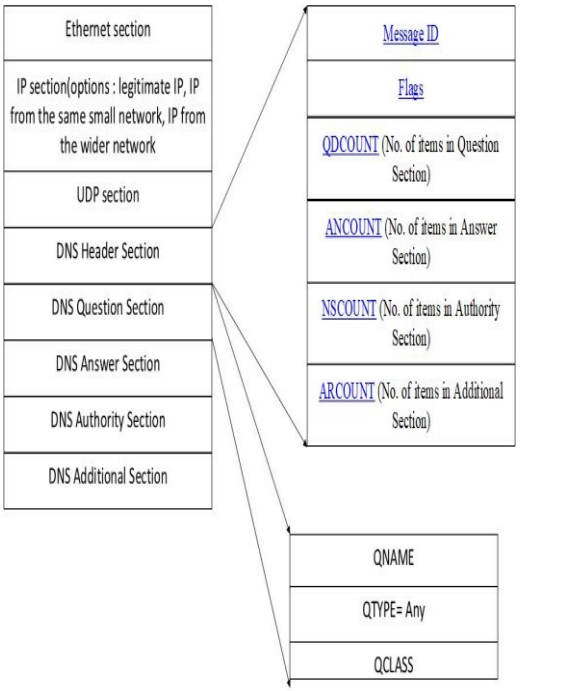

Fig.4. : Attack traffic packet structuregenerated using PcapDotNet

The traffic options will be:

- Legitimate traffic (same as virtual machine IP)
- Spoofed traffic with IP address within the same network range (section four of the IP address is different)
- Spoofed traffic with IP address within the larger network range (section 3,then 2,then 1 of the IP address is different
- than the machine IP address)

L. Traffic inspection by the hypervisor

To inspect the traffic generated by the VMs, and passing through the hypervisor (Virtual Box in our case) there were different options:-

- Amend the hypervisor source code to add function that can monitor the traffic, and alert when there is probability for attack, but this was hard to implement due to the long list of prerequisites to be prepared before starting.
- Communicate with the Virtual Box using the supported COM library, or web service. In our case, we used the COM library.

M. The experiment

First, the monitoring is enabled on the hypervisor for the attacker VM, and log file path is determined. This is done while the VM is in shutdown mode. Second, start traffic generation from the VM using the traffic generator program. The traffic generated logged into the log file (Pcap format) this log file will be read continuously using our monitoring program. Each packet sent out of the VM is checked, if its source IP is different from the VM legitimate IP more checks are applied as declared in Fig. 5 :-

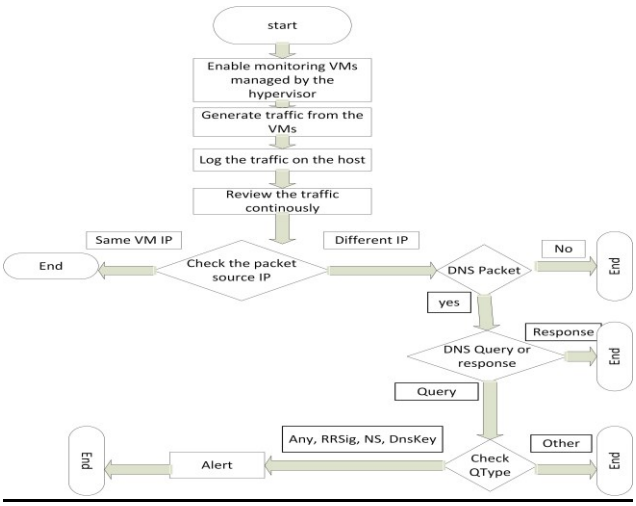

Fig.5. : Packet inspection flow chart

- Check if it is DNS packet.
- If yes, check if it is a Query, not response,
- If yes, check the DNS Question type if it is (Any, RRSIG, NS, DNSkey)
- If yes, an alert that there is possible DNS reflection amplification attack generated from this specific VM.

VI. RESULTS

We made four runs using the traffic generator, and applied the inspection program. The results can be seen in table 1.

Table 1

Run	**Legitimate traffic (192.168.1.20)**	**Attack from the same network (section four of the IP address is different) 192.168.1.X**	**Attack from wider network (section 3,then 2 of the IP address is different than the machine IP address) 192.168.X.20, 192.X.1.20**	**Number of detected packets**
Run 1	2482	2507	5012	7519
Run 2	2496	2483	5022	7505
Run 3	2502	2526	4973	7499
Run 4	2502	2463	5036	7499

Fig.6 shows how the HIF handle the transmitted packets.

A comparison between both HIF and ISP edge router ingress/egress filtering is made, the following scenarios shows that HIF is giving better results:-

- When the legitimate VM IP is 192.168.1.20, and the attacker generated traffic from the same VM with spoofed IP 192.168.1.93, and if the ISP edge router ingress/egress filtering was applied on the network range 192.168.1.X, the ISP edge router ingress/egress filtering will fail to detect such attack, but it was detected by HIF. (as shown in Fig.7)
- When the legitimate VM IP is 192.168.1.20, and the attacker generated traffic from the same VM with spoofed IP 192.168.20.93, and if the ISP edge router ingress/egress filtering was applied on the network range 192.168.1.X both techniques will detect the attack.
- When the legitimate VM IP is 192.168.1.20, and the attacker generated traffic from the same VM with spoofed IP 192.168.20.93, and if the ISP edge router ingress/egress filtering was applied on the network range 192.168.X.X the ISP edge router ingress/egress filtering will fail to detect such attack, but it was detected by HIF.

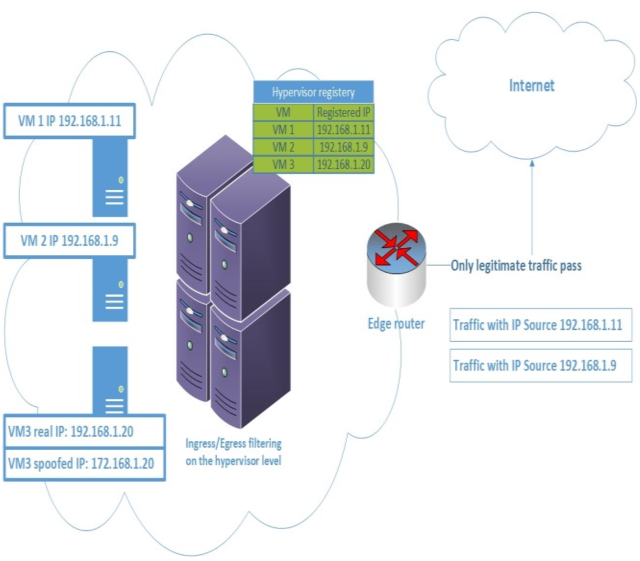

Fig.6. : HIF

```
DNS Qtype is Any  -> suspicious traffic - 192.168.1.93: -> 192.168.1.3:Udp InformationRequest
DNS Qtype is Any  -> suspicious traffic - 192.168.1.93: -> 192.168.1.3:Udp InformationRequest
DNS Qtype is Any  -> suspicious traffic - 192.168.20.93: -> 192.168.1.3:Udp InformationRequest
DNS Qtype is Any  -> suspicious traffic - 192.168.1.93: -> 192.168.1.3:Udp InformationRequest
DNS Qtype is Any  -> suspicious traffic - 192.168.1.93: -> 192.168.1.3:Udp InformationRequest
DNS Qtype is Any  -> suspicious traffic - 192.168.1.93: -> 192.168.1.3:Udp InformationRequest
DNS Qtype is Any  -> suspicious traffic - 192.168.1.93: -> 192.168.1.3:Udp InformationRequest
DNS Qtype is Any  -> suspicious traffic - 192.168.1.93: -> 192.168.1.3:Udp InformationRequest
DNS Qtype is Any  -> suspicious traffic - 192.168.1.93: -> 192.168.1.3:Udp InformationRequest
DNS Qtype is Any  -> suspicious traffic - 192.168.1.93: -> 192.168.1.3:Udp InformationRequest
DNS Qtype is Any  -> suspicious traffic - 192.168.184.20: -> 192.168.1.3:Udp InformationRequest
DNS Qtype is Any  -> suspicious traffic - 192.168.184.20: -> 192.168.1.3:Udp InformationRequest
```

Fig.7: Suspicious traffic

- When the legitimate VM IP is 192.168.1.20, and the attacker generated traffic from the same VM with spoofed IP 192.160.20.93, and if the ISP edge router ingress/egress filtering was applied on the network range 192.X.X.X the ISP edge router ingress/egress filtering will fail to detect such attack, but it was detected by HIF.

So as shown HIF can detect scenarios that cannot be detected by ISP edge router ingress/egress filtering.

As mentioned before the DNS amplification attacks form 34.9% of the large DDoS attacks. So, applying the HIF will help decrease this percentage.

VII. Conclusion and Future Work

As the adoption of cloud computing increase, the risks related to it increase as well. One of the main risks is DDoS attacks specially that cloud can be its source or its victim. In this paper, we discuss DDoS attacks. Specially DNS reflection amplification DDoS attacks originating from the clouds, and propose new solution, which is Hypervisor ingress filtering (HIF) which is based on BCP38.

HIF implementation is easier than the implementation of ISP's edge routers filtering, and can handle scenarios cannot be handled by ISP's edge routers filtering.

In the future if this is implemented natively in all hypervisors the DNS amplification reflection attack generation from VMs hosted on the cloud will be minor.

References

[1] Peter Mell, Timothy Grance, "The NIST definition of cloud computing.", National institute of standards and technology, U.S. department of commerce, special publication 800—145, September 2001.

[2] Yiyun Zhu, "Cloud computing: current and future impact on organizations, " Western Oregon University, student theses, Papers and projects (computer science), March 2017

[3] Zhifeng Xiao, and Yang Xiao, "Security and privacy in cloud computing ," IEEE communications surveys & tutorials , July 2012

[4] M. Durairaj, and A. Manimaran, "A study on securing cloud environment from DDoS attack to preserve data availability," the international journal of science and technoledge, February 2015

[5] P. J. Criscuolo, "Distributed denial of Service, tribe flood network 2000, and Stacheldraht CIAC-2319," Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 2000.

[6] Kyle York, "DDoS attack," ORACLE+DYN, vantage point, Company news, October 2016.

[7] Saman Taghavi Zargar, James Joshi, and David Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks,".IEEE Communications surveys & tutorials, Volume 15, Issue 4, March 2013.

[8] G. Velmayil, and S. Pannirselvam, "Detection and removal of IP spoofing through extended-inter domain packet filter architecture", International journal of computer applications (0975-8887), volume 49-no.17, July 2012.

[9] Manish Kumar, Arvind Panwar, Achin Jain M. Tech. (IS) AIACTR, Geeta Colony, "An analysis of TCP SYN flooding attack and defense mechanism," New Delhi International Journal of Engineering Research & Technology (IJERT), Vol. 1, Issue 5, July 2012.

[10] ushar Deshpande, Panagiotis Katsaros, Stylianos Basagiannis† and Scott A. Smolka, "Formal analysis of the DNS bandwidth amplification attack and its Countermeasures using probabilistic model checking," High-Assurance systems engineering (HASE), 2011 IEEE 13th international symposium, December 2011.

[11] High Thijs Rozekrans, Javy de Koning, "Defending against DNS reflection amplification attacks," University of Amsterdam, System & Network Engineering RP1, February 2013.

[12] Igal Zeifman, "2013- 2014 DDoS threat landscape report," Incapsula, March 2014.

[13] Paul Ferguson, Daniel Senie, "Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing ," Network working group, request for comments 2827, May 2000.

[14] Douglas C. MacFarland, Craig A. Shue, and Andrew J. Kalafut, "Characterizing optimal DNS amplification attacks and effective mitigation," conference paper, international conference on passive and active network measurement, March 2015.

[15] Arpita Narayan, UpendraKumar, "A defense mechanism: DNS based DDoS attack," Ranchi, Jharkhand International Journal of Computer Trends and Technology (IJCTT), Volume 33, Number 1, March 2016

[16] PcapDotNet SDK https://github.com/PcapDotNet/Pcap.Net

[17] "Virtual box," https://www.virtualbox.org/wiki/Downloads