Impact of Denial of Service Attack on the Virtualization in Cloud Computing

Kanika[1] and Navjot Sidhu[2]
[1,2]Centre for Computer Science and Technology, Central University of Punjab, Bathinda, India
E-mal: [1]kanikagoyal05@gmail.com, [2]navjotsidhu8@gmail.com

***Abstract*—Cloud computing is the fastest growing technology in the IT world. The technology offers reduced IT costs and provides on the demand services to the individual users as well as organizations over the Internet. Cloud computing offers infrastructure as a service (IaaS). IaaS provides infrastructure including software, hardware, storage space, network bandwidth to the users on demand over the internet. Cloud computing makes use of virtualization to provide infrastructure as a service. Virtualization is based on the concept that multiple tenants can use the same physical machine with multiple operating systems. Virtualization comprises the vulnerability of Denial of Service (DOS) attack that can affect the performance of cloud computing. A malicious VM attacker can compromise the other guest VM or the host OS. The paper explores the TCP SYN flood attack over the other guest VM by a malicious VM attacker co-existing in the virtualized cloud infrastructure. Different Parameters are analyzed over the victim VM to detect the TCP SYN flood attack**

Keywords: Cloud Computing, Virtualization, Hypervisor, Network Security

I. INTRODUCTION

Cloud computing is the Internet-based computing, where sharing of resources, software and platforms are provided to the users on demand in a distributed computing environment. Cloud computing is the growing trend for storing and processing data in a resource sharing environment. The term cloud in the cloud computing specifies storage space, hardware, networks combination to deliver computing services. Cloud services include delivery of software, platform to develop applications and providing a complete infrastructure over the Internet. Cloud computing relies on sharing of computing resources rather than having local servers. Cloud computing creates exciting opportunities like reduced costs and flexibility to the users.

A. Cloud Computing Service Models

Cloud service providers offer services that are separated into three categories as [1]:

1) Software as a Service (SaaS)

In SaaS, software are offered as a service on demand to the users. Users are billed on the basis of usage and there is no need for investment in servers or software licenses.

2) Platform as a Service (Paas)

PaaS provides complete platform required to develop user specific applications and services over the Internet. Platform as a service offers combination of operating system and application servers, such as Linux, Apache, MySql and PHP etc.

3) Infrastructure as a Service (IaaS)

IaaS offers complete infrastructure such as servers, basic storage systems, networking equipments over the Internet. Here multiple tenants share a virtualized environment. Tenants are coupled with managed services for OS and application support.

B. Essential Characteristics

The five characteristics of the cloud which represents its services are [10] [12]:

1) On-demand self-service

Consumers can automatic provision computing resources without requiring interaction with cloud service provider.

2) Broad network access

Cloud services are provisioned over the network and can be accessed via multiple devices such as mobile phones, laptops, PDA, etc.

3) Resource pooling

The cloud service provider's resources are pooled in a multi tenant environment. Resources are dynamically allocated to the tenants according to their demand. The tenants don't know the exact location of the resources. The shared resources include storage, processing, memory, etc.

4) Rapid elasticity

Cloud services can be automatically scaled at any time and at any quantity depending upon the user's demand.

5) Measured service

Customer's usage of the provider's services is automatically monitored and reported providing transparency for both the customer and provider.

II. MULTI-TENANCY AND VIRTUALIZATION

In a multi-tenant environment, tenants have their own private space to save private data as well as global

space shared among all tenants. By sharing resources and creating standard offerings, multi-tenancy offers reduced cost and optimum use of resources in a shared environment [1].

With SaaS, data of multiple tenants is stored on the same database and may share the some tables. In IaaS, multiple tenants share infrastructure resources such as hardware, servers and storage devices [4] [13].

Resources shared among multiple tenants can be:

1. Basic storage space.
2. CPU processing.
3. Memory.
4. Network bandwidth.

Multi-tenancy is obtained by the use of virtualization. It allows multiple operating systems to run on a single machine simultaneously. In cloud computing virtualization used to serve several end users by creating virtual version of storage space, operating system, hardware platform [16].

Virtualization divides a physical computer to several virtual machines known as guest machines. Multiple virtual machines run on a host computer, each having its own OS and applications. Virtualization gives an illusion to the users that they are running their processes on a physical computer independently, but in reality they are sharing the resources of a single host machine. The software which permits multiple operating systems to use the resources a physical machine is called a hypervisor. The hypervisor resides between the operating system of the host machine and the virtual environment [4] [14].

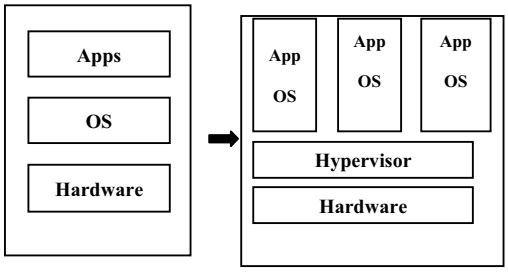

Fig. 1 Independent OS to Virtualization of OSs

The Fig. 1 shows how an individual operating system running its applications on the independent physical hardware can be placed in a virtual machine.

All the OSs share the same physical system with other virtual machines. The machine with administrative capabilities lower to hypervisor is said to be Host machine which controls the hypervisor and other virtual machines said to be guest OS.

As the tenants sharing the same physical host with unknowns, there are various kinds of risks associated with the multi-tenancy environment in the cloud computing. So it is important aspect to isolate the multiple users on same physical [5], [6].

The hypervisor, a software layer which manages the virtualization, allows virtual machines to execute simultaneously on a single machine. This provides hardware abstraction to the running Guest OSs and efficiently manages underlying hardware resources. There are numerous hypervisors ranging from open-source such as KVM, Xen and virtual box, to commercial hypervisors such as VMware vSphere and Microsoft Hyper-V etc [11].

III. Security in Multi-Tenant Environment

As the multiple tenants sharing the same physical host with unknowns, there are various kinds of risks associated with the multi-tenancy environment in the cloud computing. An attacker may use guest OS (Virtual Machine) try to communicate and compromise other Virtual Machines on the same physical host, therefore breaking the isolation characteristic of VMs. The most common attacks under this are Measure cache usage, Sniffing attack, Spoofing attack, denial of Service (DoS) attack [7], [13] .

A. TCP DDOS Attack

In virtualization environment, resources such as CPU, memory, disk and network are shared by VMs and the host. An attacker aims to exhaust the resources from a physical host in order to deny service to the other VMs in the machine [8], [15].

Denial of service attack [2], [3] is one of the most dangerous network attacks, in which the one victim machine receives more TCP-SYN requests than its capacity, so that other machines requests could not be served by the main host in the cloud environment. TCP SYN Flood attack can be most dangerous than unclouded environment because of VMs are sharing their resources with the neighbour VM and Host. Under TCP SYN Flood, one virtual machine is used as a source of denial of service attack to another virtual machine present in same infrastructure.

IV. Related Work

TCP is a connection oriented protocol that needs “handshaking” to start communication in client-server architecture. The protocol provides reliable delivery of data. The client sends a “SYN” packet to server to whom it wants to establish the connection.

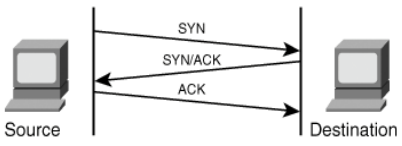

Fig. 2 TCP Three Way Handshake

The server replies with a “SYN/ACK” packet that to accept the connection. Then the client sends an

"ACK" packet to establish the connection. The connection complete connection is established in three steps, so the procedure known as "Three Way Handshaking" [2].

A. TCP SYN Flood

TCP 3-way handshake structure is exploited to perform Denial of service attacks by TCP SYN flood. The attacker overloads the victim with large number of TCP connection requests and it will not able to respond to legitimate requests.

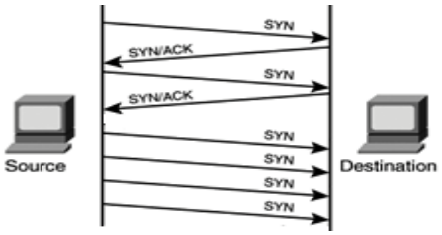

Fig. 3 TCP SYN Flood

The victim saves each new TCP connection to its buffer and transmits SYN-ACK packet to establish the connection. The attacker does not respond to the SYN-ACK. A large number of half open connections are left on the victim's queue and it gets overflow. The queue of the server is limited, and legitimate client's request cannot be fulfil due to unavailability of the resources (space) in the queue [3] [9].

B. IP Spoofing

IP spoofing is done by the attacker to create the IP packets with forged IP source address. In DoS attack, the attacker uses the IP spoofing to flood the TCP SYN packets from false IP identity. The attacker does not care about receiving response back to the IP packet. IP spoofing uses randomized IP addresses to start the three way handshake. Spoofed IP addresses are difficult to filter since each spoofed packet appears to come from a different address. The attackers also use subnet spoofing, spoofs a random address within the address space of the sub network [17].

V. EXPERIMENT ARCHITECTURE

To conduct the experiment, the private cloud infrastructure is deployed using VMware ESXi and vSphere client. The physical server VMware ESXi hosted hypervisor is installed that provides sharing of different resources such as the CPU, memory, Network Interface Card (NIC) to multiple VMs. The vSphere Client is the interface that accesses and manages the multiple the VMs remotely.

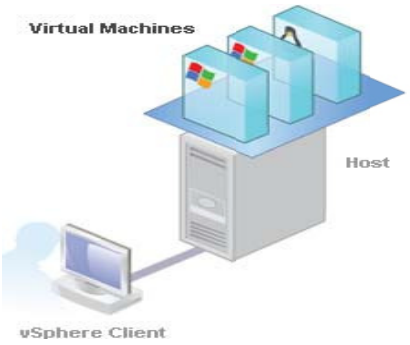

Fig. 4 Virtualized Cloud Infrastructure

Ten guest virtual machines are installed over the hypervisor and accessed through the vSphere client. Among the guest OS (VMs) one machine with the IP address 192.168.43.129 is the malicious node and sniffs the network traffic to know about the other tenants present in the network. The attacker VM acts as a source of the TCP SYN flood packets to another VM existing in the same network. The victim VM with the IP address 192.168.43.138 and TCP backlog 1024, receives TCP SYN packets more than its capacity, and its resources get exhausted. The other virtual machines are used as Zombie that is connected on the same network segment as the host and guest virtual machines.

VI. TCP-SYN FLOOD ATTACK

Using the 'nmap' tool the attacker virtual machine performs the scan to know about the other virtual machines IP addresses present in the network.

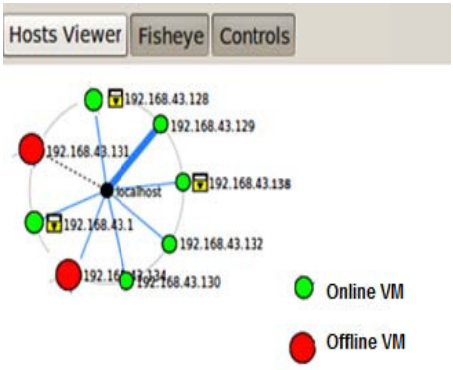

Fig. 5 Nmap Scanning Result

The VMs with green symbol are currently online, and the VMs with red symbol are currently offline in the network. The attacker VM picks the online co-existing VM with IP address 192.168.43.138 to perform TCP-SYN flood. The attacker VM scans the VM to check for the open TCP ports to perform the attack with the 'nmap'.

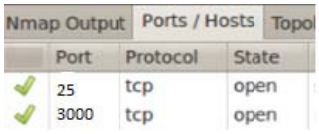

Fig. 6 'nmap' Tool Scanning for the Open Ports

The scan showed for the IP address '192.168.43.138' TCP port 25 and TCP port 3000 are open.

The attacker virtual machine makes use of hping3 tool to SYN flood the TCP port 3000 in a distributed manner with the direct IP address and spoofed IP addresses of other virtual machines that are offline or online in the network.

A. Direct Attack

The attacker VM rapidly sends TCP SYN packets with its own IP address as the source.

The command used to flood TCP SYN request is:

Sudo hping3 -flood -S -p 3000 192.168.43.138

The attacker VM initiates the TCP connection by sending SYN packets and the victim VM replies with the SYN-ACK packet, and then the attacker doesn't send the final acknowledgement to complete the three-way handshake. At the victim VM site, high numbers of half-opened connections are left.

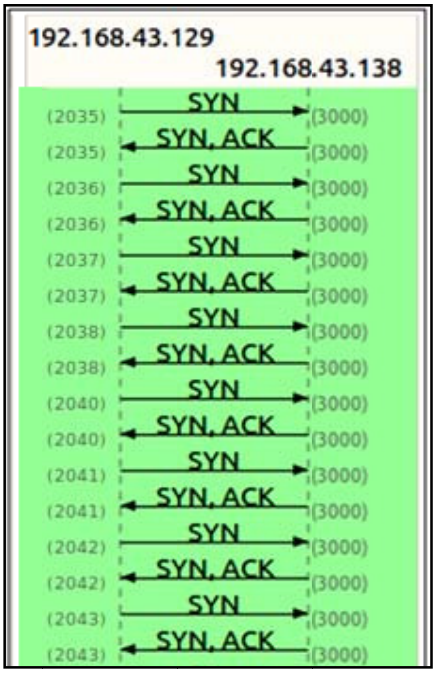

Fig. 7 SYN Flood with own IP Address

The queue that is storing the half opened connections is of finite size that can have 1024 backlog at any instant of time, and it is made to overflow by intentionally creating too many half-open connections. The victim keeps on waiting for the final ACK packet and after the RTT (round trip time) expires; it resends the SYN-ACK packets to the attacker. The victim VM is not able to further create new TCP sessions for the legitimate network traffic.

B. IP Spoofing with Offline VM

The attacker floods the TCP SYN packets with the spoofed IP addresses of other co-existing VMs that are offline at that instant.

The command used to flood TCP SYN request is:

Sudo hping3 -flood -S -p 3000 192.168.43.138 – a 192.168.43.131

Sudo hping3 -flood -S -p 3000 192.168.43.138 – a 192.168.43.134

In a short period of time there are a number of connection attempts by the IP 192.168.43.131 and 192.168.43.134 to the VM 192.168.43.138. Within a private network When the VM wants to send data to the co–existing VM, ARP cache is used to find out the MAC address corresponding to the VM.

The victim VM tried to resolve the MAC address of the VMs (offline). But when no response is received by the offline VMs, the victim VM not having the physical address of the host, it cannot send an ACK-SYN to the same to continue with the three-way handshaking. The TCP/IP stack of the server has to wait for a set time for each connection. During this time more packets keep arriving that create new connections. At the victim side, for each connection that tries to be made, a structure in memory called TCB (Transmission Control Block) is created.

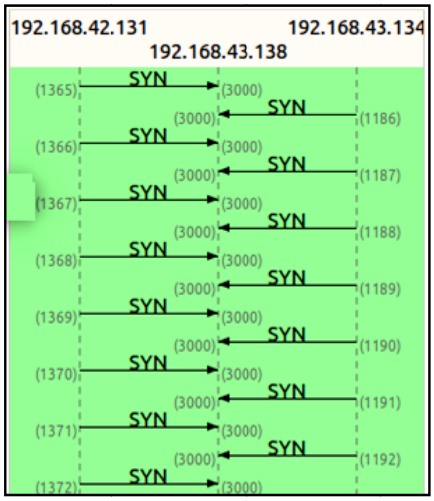

Fig. 8 SYN Flood with Offline VM Spoofing

The TCB holds the SYN packet information before the connection is fully established. It holds only 1024 half opened connections. The attacker sends SYNs that causes the allocation of so many TCBs that a victim VM's kernel memory is exhausted.

C. IP Spoofing with Online VM

The attacker VM sends SYN packets to the victim VM, with the spoofed IP addresses of the VM that are online on the same network. The spoofed VMs act as zombie.

The command used to flood TCP SYN request is:

Sudo hping3 -flood -S -p 3000 192.168.43.138 – a 192.168.43.130

Sudo hping3 -flood -S -p 3000 192.168.43.138 – a 192.168.43.132

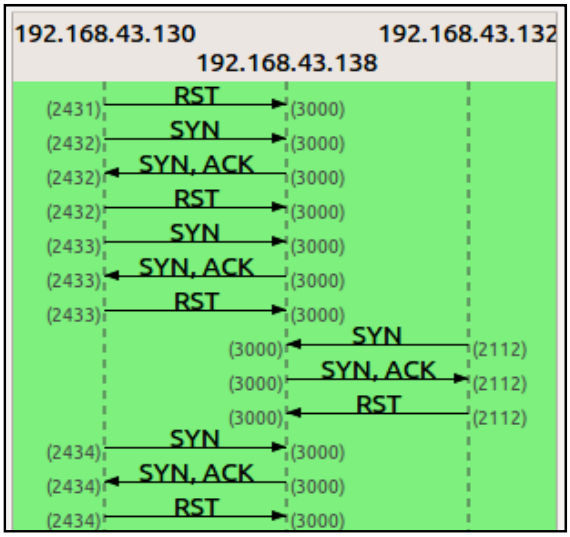

Fig. 9 SYN Flood with Online VM Spoofing

As the flow graph shows the victim VM sends the ACK-SYN packets to the respective IP addresses. The zombie VM won't be expecting the SYN/ACK (because, it has not really sent the SYN), so the zombie VM responds to the victim VM with a RST. The attacker keeps the victim busy in handling the spoofed packets and consuming the resources. The victim VM's resources are depleted; it is not further create new TCP sessions legitimate network traffic.

VI. Detection of TCP-SYN Flood

To detect the attack effect, the attacker Virtual Machine trying to communicate with the victim Machine. 20 seconds after communication, attacker starts sending attack traffic that lasts for 40 seconds. The attacker virtual machine floods the victim at the maximum possible rate allowed by operating system.

Wireshark, Bandwidth monitor, Netflow, Netstat commands and IPtraf are few of the tools used to analyze the system under attack .The research to measure the performance of victim virtual machine over the TCP DOS attack by a malicious guest VM. The performance of the victim VM under attack is determined on the basis of network traffic, average number of SYN requests over the system, SYN to FIN|RST ratio, resource utilization, etc.

A. Number of SYN Requests Captured

The SYN packet is sent to initiate the TCP Three-way handshake. The attacker floods the victim VM by sending a large number of TCP SYN requests. Wireshark captures the SYN packet passing through the eth0 port. The Ethernet port was monitored during a TCP SYN flood attack.

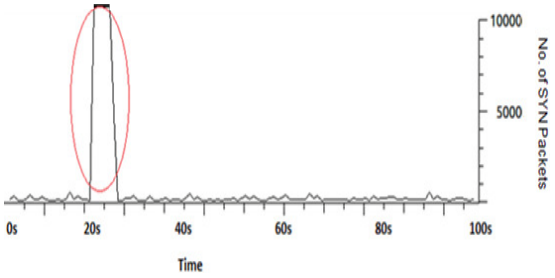

Fig. 10 Number of SYN Packets at the Victim VM with Attack

The Fig. 10 shows the result of the incoming traffic for the TCP Port 3000. During TCP-SYN flood attack (from 20 sec to 30 sec) the number of SYN requests more than 10000 as compared to normal traffic that is about 5 to 10 SYN requests per second.

B. SYN and FIN/RST Packet Ratio

TCP is a bi-directional protocol. The TCP connection is terminated by the FIN packet. The TCP connection performs half-duplex termination by sending RST packet from either side. The RST packet aborts the TCP connection. The number of FIN packets and the SYN packets are almost same under the normal TCP sessions. TCP session may be terminated by a RST packet without a FIN packet. But when the attack occurs, the relation between the SYN packets and FIN|RST Packets completely breaks. Detection of TCP SYN Flood is done based on the change of the difference between the number of SYN and the number of RST | FIN.

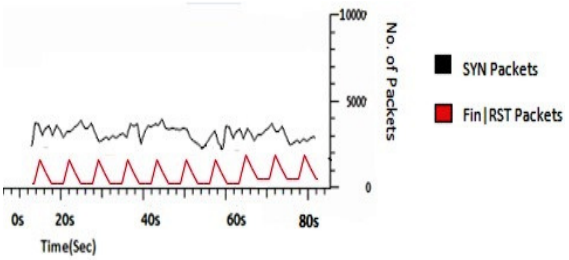

Fig. 11 Normal SYN to FIN|RST Packet rate

The Fig. 11 shows that the number of SYN and FIN|RST packets is almost same under normal network behaviour. The number of connections opened by the legitimate users is equal to the number of connections closed under the normal TCP session.

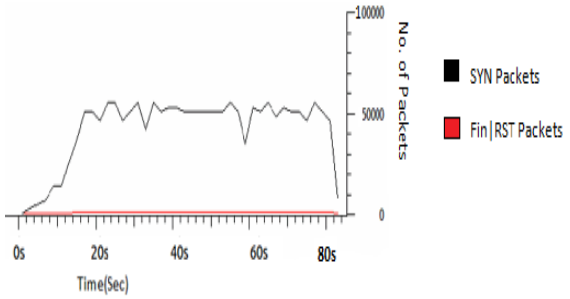

Fig. 12 SYN to FIN|RST Packet Rate with SYN Flood

When the attacker performs the SYN Flooding to the VM, it doesn't terminate the connection at the victim VM side. The Fig. 12 shows the number of SYN and FIN|RST packets rate when the system is under attack. The number of SYN requests is very high as compared to the FIN|RST packet which is almost zero.

C. *The Start and End Time of an Attack*

The exact time when the attack starts is analyzed with the post processing of the TCP SYN packets. Incoming traffic rate increases abruptly during the TCP SYN flood attack as compared to normal traffic rates.

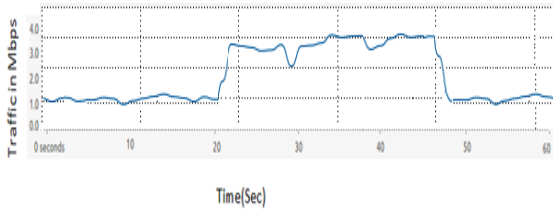

Fig. 13 Time duration of attack

From the Fig.13, it could be seen that the normal incoming traffic rate is almost 1 Mbps and the traffic rate goes up to 3Mbps at the time of TCP SYN flood from 20thsec to 50th sec. The SYN Flood attack is detected based on the incoming traffic rate that increases abruptly as compared to the traffic rates under normal network behavior.

D. *Resource Utilization on the Host OS*

As under the virtualized cloud infrastructure the single CPU is shared among multiple VMs. CPU utilization refers to hypervisor's usage of processing resources. For each TCP connection, that tries to be established, a queue is maintained in the memory that holds all the information about a TCP connection.

It could be seen from the figure that CPU % utilization for the single virtual machine increases to 65% when it is under the attack. The memory utilized by the victim VM under the attack is up to 30%.

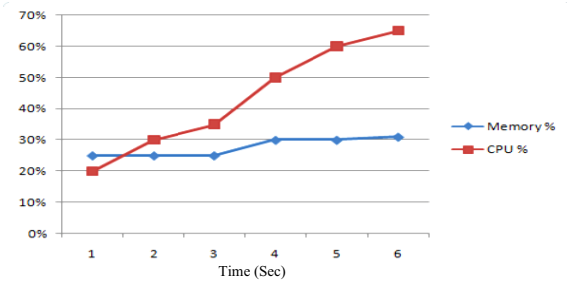

Fig. 14 Resource Utilization of Host OS

VII. CONCLUSION

Multi-tenancy in virtualization not only allows more effectiveness of the infrastructures to the cloud service providers, but also introduces new attack vectors in the cloud. Cloud computing security issues need to be approached cautiously. The paper includes the experiment that shows the vulnerability that how a malicious virtual machine can attack over another virtual machine in a virtualized cloud. The vulnerability of the Denial of Service attack by a malicious virtual machine over co-existing virtual machine in the private cloud infrastructure is explored along with a mechanism on how to approach it. The malicious virtual machine exhausted the common resources by flooding the co-existing VM with high rate of unreasonable network traffic.

The malicious virtual machine is detected on the basis of different parameters over the victim operating system. Network Traffic is analysed over the victim VM. The traffic over the victim increases at a very high rate as compared to average traffic whenever there is an attack in the system and corresponding to that more resources wastages at the victim. The results showed that the arrival rates of normal TCP SYN packets and attacked SYN Flood varies with large difference. On the basis of daily network behaviour a SYN Packet arrival rate is decided. The presence of TCP-SYN Flood attack is determined based on the average number of SYN requests to the VM, SYN to FIN|RST packet ratio. This research may prove to strengthen virtualization and reduces the risks of cloud computing. Immediate extensions to the research work include prevention and mitigation of TCP SYN Flood by configuring the firewalls at the VM level and the hypervisor level.

REFERENCES

[1] A. Jasti, P. Shah, R. Nagaraj, R. Pendse "Security in multi-tenancy cloud, " in IEEE International Carnahan Conference on Security Technology (ICCST), pp.35-41, 2010.

[2] A.Habib, M. Hefeeda, B. Bhargava, "Detecting service violations and DoS attacks" 2003.

[3] A. Bakshi, B. Yogesh, "Securing cloud from DDOS Attacks using Intrusion Detection System in Virtual Machine, " in Second International Conference on Communication Software and Networks, pp. 260-264, 2010.

[4] B. Grobauer, T. Walloschek, E. Stocker, "Understanding Cloud Computing Vulnerabilities, " Security & Privacy, IEEE, vol. 9, pp. 50-57, 2011.

[5] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" Cloud Security Alliance, 2009, Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf [Accessed: 08-Jan-2014].

[6] G. Wang, T.S.E. Ng, "The impact of virtualization on network performance of amazon ec2 data center, " in Proc. IEEE INFOCOM, pp. 1–9, 2010.

[7] H. Wu, Y. Ding, C. Winer, L. Yao, "Network security for virtual machine in cloud computing, " in Proc. 5th International Conference on Computer Sciences and Convergence Information Technology, pp.18-21, 2010.

[8] M. A. Bamiah, S. N. Brohi, "Seven Deadly Threats and Vulnerabilities in Cloud Computing, " International Journal Of Advanced Engineering Sciences And Technologies, Vol No. 9, Issue No. 1, pp. 87 – 90, 2011.

[9] N. H. Bhandari, "Survey on DDoS Attacks and its Detection & Defence Approaches, " International Journal of Science and Modern Engineering (IJISME), pp. 67-71, 2013.

[10] P. Mell, T.Grance, "The NIST definition of Cloud Computing, " NIST, Special Publication 800–145, 2011.

[11] P. Nomnga, M. S. Nyambi Scott, "Technical Cost Effective Network-Domain Hosting through Virtualization: a VMware ESXi and vSphere Client Approach, " International Journal of Computer Applications. Pp. 39-47, 2014.

[12] R. Buyya, J. Broberg, A. M. Goscinski, "Cloud Computing: Principles and Paradigms, " vol. 87, John Wiley & Sons, 2010.

[13] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing, " Journal of Network and Computer Applications, pp. 1-11, 2011.

[14] S. Brohi, M.Bamiah, "Challenges and Benefits for Adopting the Paradigm of Cloud Computing", International Journal of Advanced Engineering Sciences and Technologies (IJAEST), vol. 8, pp. 286 - 290, 2011.

[15] S. N. Brohi, "Identifying and analyzing security threats to Virtualized Cloud Computing Infrastructures, " in International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM), pp. 151-155, 2012.

[16] W. Dawoud, I. Takouna, C. Meinel, "Infrastructure as a service security: Challenges and solutions, " In the 7th International Conference on Informatics and Systems (INFOS), pp. 1-8, 2011.

[17] Y.S.Choi "Integrated DDoS attack defense infrastructure for effective attack prevention, " in IEEE International Conference on Information Technology Convergence and Services, pp.1-6, 2011.