ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

A Survey: DDoS Attacks and its Effects on Cloud Environment

Nishalee Choubey[1], Prof. Saurabh Kapoor[2]

[1]Research Scholar, Dept. of Computer Science, Gyan Ganga Institute of Technology and Science, Jabalpur, Madhya Pradesh, India

[2]Assistant Professor, Dept. of Computer Science, Gyan Ganga Institute of Technology and Science, Jabalpur, Madhya Pradesh, India

ABSTRACT: In this paper, we survey different intrusions affecting availability, confidentiality and integrity of Cloud resources and services. Proposals incorporating Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in Cloud are examined. We recommend IDS/IPS positioning in Cloud environment to achieve desired security in the next generation networks.

KEYWORDS: DDoS; DoS; Counter measures; cloud computing; Attacks; virtual machine component;

I. INTRODUCTION

The term 'Security' in the world of digital computing refers to safeguarding the information that is being transmitted over the internet. Since all the operations performed in this era are automated and large volumes of data or storage upto giga, tera and petabytes is demanded, so security still remains a typical issue that has to be addressed. The evolving technologies like cloud computing uses a huge volume of storage, its data and services are also distributed among multiple users.

The most preferred technology by industries the "Cloud Computing" introduced by NIST is a large scale dynamic distributed computing technology. It is built in order to meet the demand for power and memory storage to lend a hand for the scientific research and industrialization [1]. The services are made available by the virtual hardware, simulated by one or more hypervisor that runs the virtual machines.

In Distributed environment, the computing is decentralized where two or more computers communicate over a network to establish a common goal independently. To retain the transparency, consistency, integrity, concurrency and availability of data it must be secured enough at each level of computing. Since the dynamic users share the data and hardware resources distributed over the network, the users and their data must be protected and should be available during relocation.

The five essential characteristics include On-demand service [3], Broad network access, Resource pooling, Scalable
& elastic and Metered services by NIST. The cloud computing offers three service models viz. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS) and four deployment models viz. public cloud, private
cloud, community cloud and hybrid cloud [4], [5]. DDoS Attacks and its Countermeasures

A. DDoS attacks and its history

DDoS attacks are initiated by a network of remotely controlled, well structured, and widely dispersed nodes called Zombies. The attacker launches the attack with the help of zombies. These zombies are called as secondary victims. The first massive DDoS attack has been encountered in the late june and early july, 1999 [2] followed by an Fapi tool attack in
1998 which is not well documented. The first DDoS attack was to flood a single computer in University of Minnesota.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

The occurrences of DDoS attacks with year are given in the table 1. The servers suffered from DDoS attacks during the
year 2000 [2] are Yahoo server, Amazon, Buy.com, CNN, and eBay, E*Trade and ZDNet, and NATO sites.
The recent attacks in 2013 include the attack in China's websites, Bitcoin, largest cyber attack by Cyber Bunker, NASDAQ trading market, Iranian Cyber attacks on FBI and so.

TABLE I. ORIGIN OF DDOS ATTACKS

DDoS tool	Possible Attacks	Year
Fapi	UDP, TCP(SYN and ACK) and ICMP floods	1998
Trinoo	Distributed SYN DoS attack	1999
Tribe Flood Network	ICMP flood, SYN flood, UDP flood, and SMURF style attacks	1999
Stacheldraht	ICMP flood, SYN flood, UDP flood, and SMURF attacks	1999
Shaft	packet flooding attacks	1999
mstream	TCP ACK Flood attacks	2000
Trinity	UDP, fragment, SYN, RST, ACK and other flood attacks	2000
Tribe Flood Network 2K	UDP, TCP, and ICMP Teardrop and LAND attacks	2000
Ramen	Uses back chaining model for automatic propagation of attack	2001
Code Red & Code Red II	TCP SYN attacks	2001
Knight	SYN attacks, UDP Flood attacks	2001
Nimda	Attacks through email attachments, SMB networking and backdoors attacks	2001
SQL slammer	SQL code injection attack	2003
DDOSIM-0.2	TCP based connection attacks	2010
Loris	Slowloris attack and its variants viz. Pyloris	2009
Qslowloris	Attacks the websites eg: IRC bots, Botnets	2009
L4D2	Propagation attacks	2009
XerXeS	Wiki Leaks attacks, QR code attacks	2010
Saladin	Web servers attacks, tweet attacks	2011
Apachekiller	Apache server attacks, scripting attacks	2011
Tor's Hammer	HTTP POST attacks	2011

From the above survey most of the victims of DDoS attacks are distributed and shared.

B. Taxonomy of DDoS Attacks
Variety of DDoS attacks are sprouting in the computing world. The taxonomy of the DDoS attacks has been depicted in the Figure 1.
1) Bandwidth Depletion Attacks
This type of attack consumes the bandwidth of the victim by
flooding the unwanted traffic to prevent the legitimate traffic from reaching the victim's network. Trinoo is one of the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

DDoS tools that cause the Bandwidth depletion attacks. These attacks can be further classified as:

a) Flood Attacks: This attack is launched by an attacker sending huge volume of traffic to the victim with the help of zombies that clogs up the victim's network bandwidth with IP traffic. The victim system undergoes a saturated network bandwidth and slows down rapidly preventing the legitimate traffic to access the network. This is instigated by UDP and ICMP packets.

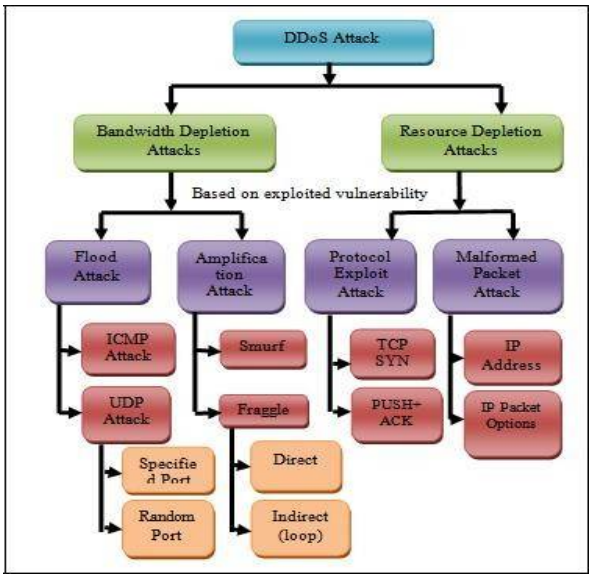

Fig. 1. Taxonomy of DDoS Attacks

An UDP flood attack is initiated by following steps:

1. An attacker sends a large number of UDP packets to the victim's random or specified ports with the help of zombies.
2. On receiving the packets, the victim looks the destination ports to identify the applications waiting on the port.
3. When there is no application, it generates an ICMP packet with a message 'destination unreachable'.
4. The return packets from the victim are sent to the spoofed address and not to the zombies.

As a result the available bandwidth has been depleted without servicing the legitimate users. This impacts the connections and systems located near the victim [6] [7].

An ICMP flood attack is set off by following steps:

1. An attacker sends a large number of ICMP_ECHO_REPLY packets to the victim with the help of zombies. These kind of packets requires a response message from the victim.
2. The victim sends the responses to the packets received
3. Now the network is clogged with request response traffic. The spoofed IP address may be used in the ICMP packet.

The bandwidth of the victim network connections is saturated and depleted rapidly without servicing the legitimate users.

Other variations of these attacks has been described in[8].

b) Amplification attacks:

The attacker sends a large number of packets to a broadcast IP address. In turn causes the systems in the broadcast address range to send a reply to the victim thereby resulting in a malicious traffic. This type of attack exploits the broadcast address feature found in most of the internetworking devices like routers. This kind of attack can be launched either by the attacker directly or with the help of zombies. The well known attacks of this kind are:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

The *Smurf attack* is caused by following steps:

1. Attacker sends packets to a network device that supports broadcast addressing technique e.g. Network amplifier. The return address in these packets are forged or spoofed with victim's address.
2. ICMP_ECHO_RESPONSE packets are sent by the network amplifier to all the systems in the broadcast IP address range. This packet implies the receiver to respond with an ICMP_ECHO_REPLY.
3. An ICMP_ECHO_REPLY message from all the systems in the range reaches the victim.

The *Fraggle attack* is the variation of Smurf attacks where the UDP echo packets are sent to the ports that supports character generation. It has following steps:

1. Attacker sends UDP echo packets to a port that supports character generation. The return address in these packets are spoofed with victim's address with the port supporting character generation thus creating an infinite loop.
2. This targets the port supporting character generation of all the systems reached by broadcast address.
3. All these systems in the range echoes back to the character generator port in the victim.
4. This process repeats since UDP echo packets are used. This attack is worse than the smurf attacks.

A variant of these attacks is the **reflector attack,** which involves a set of reflectors i.e. intermediary hosts to accomplish the specified task. The reflector keeps responding to the packets it receives. So the attackers make use of these reflectors for the attacks that requires responses. In this case the return IP- address will be spoofed with victim's system.

2) Resource Depletion Attacks:

The DDoS Resource depletion attack is targeted to strap the resources of the victim's system, so that the legitimate users are not serviced. The following are its types:

*a) Protocol Exploit Attacks:*These attacks is to consume the surplus quantity of resources from the victim by exploiting the specific feature of the protocol installed in the victim. TCP SYN attacks are the best example of this type [9].

b) *Malformed Packet Attacks:*The term malformed packet refers to the packet wrapped with malicious information or data. The attacker sends these packets to the victim to crash it. This can be performed in two ways:

i. IP Address attack: The malformed packet is wrapped with same source and destination IP address thus creating chaos in the victim's OS. It rapidly slows down and crashes the victim.

ii. *IP packet options attack:* This attack makes use of the optional fields in the IP packet to form the malformed packet. The optional fields are filled by setting all the quality of service bits to one. So the victim spends additional time to process this packet. This attack is more vulnerable when attacked by more than one zombie.

C. Countermeasures and Mitigating policies against DDoS Attacks

Various countermeasures had been adopted and still emerging for mitigating against the DDoS attacks

1) DDoS defense mechanisms- Intrusion based

Most of the DDoS attacks are influenced by an intruder attempting to make an unauthorized access in the victim system/network. The defense mechanisms are as follows:

a) Intrusion Prevention: The best mitigation policy against any attacks is to prevent the occurrence of the attacks. Some of the Intrusion Prevention techniques are [9-10]:

Ingress filtering and Egress filtering
Route based distributed packet

Secure Overlay Services and Disabling unused services History based IP filtering
Applying security patches,

Changing IP address and Disabling IP
broadcasts Load balancing and Honey pots

The intrusion prevention techniques do not completely remove the risk of DDoS attacks but increases the security.

b) Intrusion Detection: This system helps the victim to avoid the propagation of DDoS attacks and prevents it from crashing. The various methods in intrusion detection include:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

1. Anomaly detection: This method detects the attacks by recognizing the anomalies in the system's performance. This is done by comparing with certain normal behavior of the system's performance detected previously. This method identifies the false positives in the system's behavior. Some of the studies include the following [9-12]:

NOMAD

Management Information Base [MIB]

Packet sampling and filtering technique with congestion

D-WARD

MULTOPS – It is a data structure designed for the purpose of detecting DDoS attacks. It is based on the assumption that, if the IP addresses of the systems participating in a DDoS attack is possible, then measures are taken to block only these particular addresses.

2. Misuse detection: This method detects the DDoS attacks by maintaining the database of well-known signatures or patterns of exploits. Whenever one such pattern has been detected, DDoS attacks are reported. Various misuse detection techniques has been discussed in [6].

c) Response to the intruder detection: Once the DDoS attack has been detected, it has to be blocked/ prevented and the attacker must be traced to keep track the attacker's identity.

The attackers can be blocked in two ways: The automated process which is normally not preferred since it may lead to service degradation because of false alarm. The manual process involves the network administrator to identify and block the attacker through Access Control Lists (ACL).

Some of the commonly preferred approaches are discussed in this context [13].

IP traceback – refers to looking back the attack's path to find its originator. By this policy, the path and route traversed by the attacker can be identified [9].

ICMP traceback– In this mechanism each router samples the forwarding packets with a low probability and sends an ICMP traceback message to the destination. In such scenario, the victim will receive more no of ICMP messages. A chain of traceback messages has been constructed to identify the attacker.

Link-testing traceback [14] – In this technique the victim tests whether each of incoming link is probable for an attack or not. It does so by flooding the links with huge bursts of traffic and checks whether in causes any perturbation to the networks. It requires knowledge about network topology.

Probabilistic packet marking (PPM) [15] - This method can be deployed either during the attack or after the attack. Savage proposed an efficient way to encode the partial route path with IP traceback data without requiring any knowledge about network topology, router information, huge traffic and large packet size.

There are certain DDoS attacks which can be detected but cannot be prevented. In such cases the research has been focused to minimize the attack's impact by maximizing its

QoS. Systems with this provision are called as Intrusion

Tolerant system with following factors [16]:

a. *Fault tolerance*
b. *Quality of service*

II. DDOS ATTACKS IN CLOUD ENVIRONMENT

Of various attacks in the cloud environment 14% had contributed by DoS attacks by eighth annual Worldwide Infrastructure Security Report in 2012 [9]. In [17] the cloud attacks have been classified based on DoS, Data Confidentiality, Data availability and integrity with the current defense measures. The attacks in cloud environment affects the server, browser, application and network levels [1], [2], [4], [18]-[22] are depicted in the figure 2 and described briefly in the table 2.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

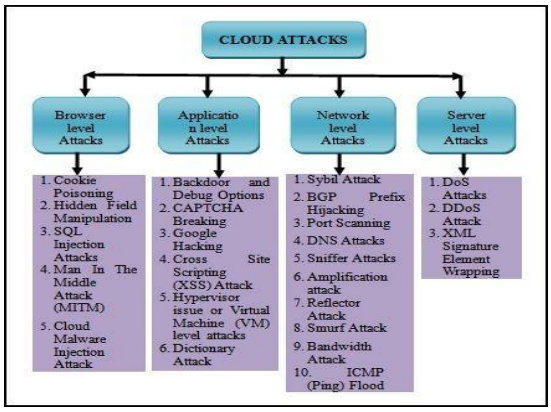

Fig. 2. Levels of Cloud Attacks

TABLE II. LIST OF CLOUD ATTACKS

Name of the attack	Definition	Detection / Prevention Technique
Virtual Machine (VM) level attacks	Caused due to the vulnerabilities in the hypervisor that runs the virtual Machines	Advanced cloud protection system that monitors the guest VM's
Bandwidth Attack	This kind of attacks consumes target system's entire resources	Multops, tree of nodes, detects the disproportional packets going and coming from the attacker
ICMP (Ping) Flood	This is the variation of bandwidth attacks that uses ICMP packets	ScreenOS
Amplification attack	The attacker makes a request there by inducing the device to generate larger responses	Using high performance OS, load balancer, Limiting the connection and connection rate.
Reflector Attack	In this kind of scenario third parties bounce the attack traffic from attacker to the target	DERM (Deterministic Edge Router Marking) identifies, tracks and filters the attack
Smurf Attack	Attackers make use of the ICMP echo request packets to generate DOS attacks	Ingress filtering
DNS Attack	While calling a server by name during the translation of a domain name to an IP Address, the victim may be directed to some cloud server which is different from the name specified	Radware carrier solution , DNS Security Extensions (DNSSEC)
BGP Prefix Hijacking	This kind of attacks takes place when a flawed announcement about the IP addresses related with the Autonomous system (AS) is made, allowing the malicious users to access untraceable IP addresses. This can even performed by some faulty AS.	Autonomous security system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

Port Scanning	Port attacks are due to some of the open ports eg. Port 80(HTTP) which is always open to provide web services.	1. Securing ports with Encryption 2. Firewall against port attacks

SNIFFER Attack	The term SNIFFER refers to "overhearing or detaining the data transmitted over the network". The SNIFFER attack may result in data loss by capturing sensitive data over the transmission channel	1. sniffing detection platform based on ARP and RTT 2. Encrypting the data transferred through the network
Issue of Reused IP Addresses	This kind of attacks is detected when an IP address of the user removed from the network still remains in the DNS cache memory and when it is assigned to new user	The DNS caches and cookies must be cleared or updated on each insertion and deletion of users
Cookie Poisoning	The malicious user uses the cookie data to view some unauthorized websites impersonating the legitimate user	1. The encryption scheme for cookies data can be implemented 2. Periodically cleanup of cookies should be done. 3. Web Application Firewalls (WAF) Hidden
Field Manipulation	The hackers tries to retrieve the contents of the hidden fields in the web pages eg: in the forms password fields	1. Security policies for encrypting the hidden fields should be incorporate 2. one session token instead of hidden form fields 3. Outgoing and Incoming Form digest- concatenation of name value pairs and appending the secret key in the outgoing and incoming messages of the form
SQL Injection Attacks	This attack occurs when the malicious code is injected into the SQL query destined for SQL server or indirectly by injecting the code into the Query destined for table	1. Parameterized Queries 2. Validate user Input for both type and format

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Man In The Middle Attack (MITM)	Third party tries to overhear the information when two parties are communicating	1.Encrypting the data using Cain, Airjack, Ettercap, Dsniff etc.
Cloud Malware Injection Attack	Attacker injects a malicious code which is similar to the instance running in the cloud, thereby gaining access to the resources as valid users and making the legitimate users to wait.	Utilization of File allocation Table that may list the set of application the customer will be running
Backdoor and Debug Options	The website developers publish their website in the internet with debug option enabled for making changes in the code at the backend. Sometimes un authorized user use this privileges to hack the website	Debug options should be enabled and disabled after use
CAPTCHA Breaking	CAPTCHA are mainly used by the developers to differentiate people from other malicious computers accessing the content. Attackers making use of the audio system to track the CAPTCHA	1. Implementing letter overlap 2. Variable length fonts of the letters used to design a CAPTCHA 3. Increasing the string length and using a perturbative background
Cross Site Scripting (XSS) Attack	This attack involves disguising a script in the URL variable and making the user to click on the link resulting in hazardous effects affecting the user's browser	1.Active Content Filtering 2. Content Based Data Leakage Prevention 3. Avoid clicking the unknown links
Dictionary Attack	The intruder makes use of all the possible word combinations for successful decryption of the data residing in/flowing over the network	1. Encrypted form of words for all the passwords in the dictionary 2. Challenge-response system
Sybil attack	A malicious user with multiple false identities apes to be distinct users and make communication with existing legitimate users. This is more vulnerable in social networks like Facebook, Orkut, Bebo where users share and maintain their photos, videos online are hacked by the attacker.	A firewall system to detect the user identity before getting access to the user data
Google Hacking	The hackers find's out a security loopholes for tracking the sensitive information through google search.	1. Standard security measures must be implemented 2. Avoid Custom implementation of authorization and authentication schemes 3. Back up policies
Denial of Service (DoS) Attack	DoS attacks are denying the intended service to the legitimate users. This kind of attack occurs when the number of requests received exceeds the capacity handled by the server.	Intrusion Detection System (IDS)
Distributed Denial of Service (DDoS) Attack	This is variation of DoS attacks where this attack is induced on a server (victim) by several compromised systems from different dynamic networks called "zombies" (slaves) directed by an attacker (Master).	1. IDS in the virtual machine 2. IDS in all physical machines
XML (Extensible Markup Language) Signature Element Wrapping	For each of the requests from the user's VMs via its browser a SOAP message (contains the structural information) is generated in the server which is translated in TLS layer. During this translation the hacker changes both the message and signature value in XML document.	Maintaining a digital certificate for each XML script

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

III. CONCLUSIONS AND FUTURE WORK

As DDoS attacks are on rise in all emerging technologies, we can expect a lot of security measures and corresponding vulnerabilities in future. This paper as a start provides a brief survey on DDoS attacks, taxonomy of attacks, its types and various counter measures to mitigate the DDoS attacks. This survey confers DDoS attacks detection, prevention and tolerance techniques. From the survey, the DDoS attacks are the major threat to the internet community and evolving distributed computing technologies.

A swing to the global IT industries is the emerging cloud computing technology for which most of the IT industries are transferring their services to. The effects of DDoS effects in the Cloud environment have been focused. Of various attacks in cloud environment 14% is contributed by DDoS attacks.

The future work is to design a secured cloud infrastructure mitigating the attacks identified and to withstand the future attacks.

REFERENCES

[1] Upma Goyal, Gayatri Bhatti and Sandeep Mehmi, "A Dual Mechanism for defeating DDoS Attacks in Cloud Computing Model," International Journal of Application or Innovation in Engineering & Management,
Volume 2, Issue 3, March 2013.

[2] Gary C. Kessler "Defenses Against Distributed Denial of Service Attacks," 4th edition of the Computer Security Handbook, November 2000

[3] Zakarya, M. and A.A. Khan, "Cloud QoS, High Availability and Service Security Issues with Solutions". IJCSNS, 2012.

[4] Rohit Bhadauria and Sugata Sanyal,"Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques.," International Journal of Computer Applications 47(18) , June 2012, pp:47-66.

[5] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing",Version,15,http://csrc.nist.gov /publications/nistpubs/800-145/SP800-145.pdf., 2011.

[6] Stephen M. Specht and Ruby B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures" Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550, September 2004

[7] Christos Douligeris , Aikaterini Mitrokotsa , "DDoS attacks and defense mechanisms: classification and state-of-the-art " , Elsevier International journal on computer Networks 44, 2004, pp 643-666.

[8] http://www.riorey.com/x-resources /2011/RioRey_Taxonomy_DDoS_Attacks_2.2_2011.pdf

[9] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," Computer Networks: the Int. J. Computer and Telecommunications Networking, Vol. 44, No. 5, April 2004, pp. 643–666.

[10] X. Geng, A.B. Whinston, "Defeating Distributed Denial of Service attacks," IEEE IT Professional 2 ,july 2000, pp. 36–42

[11] J. Mirkovic, G. Prier, P. Reiher, "Attacking DDoS at the source," 10 th IEEE International Conference on Network Protocols, Paris, France, 2002, pp. 312–321.

[12] Thomer M. Gil and Massimiliano Poletto, "MULTOPS: a data-structure for bandwidth attack detection," MIT, USA, 2001.

[13] Puneet Zaroo," A Survey of DDoS attacks and some DDoS defense mechanisms," Advanced Information Assurance (CS 626), 2003.

[14] H. Burch, H. Cheswick, "Tracing anonymous packets to their approximate source," USENIX LISA (New Orleans) Conference, 2000, pp. 319–327

[15] U.K. Tupakula, V. Varadharajan, "A practical method to counteract Denial of Service Attacks," Twenty-Fifth Australasian Computer Science Conference, Vol-16, 2003.

[16] M.B. Geoffrey, G. Xie, "A feeedback mechanism for mitigating Denial of Service attacks against differentiated services clients," the 10th International Conference on Telecommunications systems, Monterey,CA, October 2002, pp. 204–213.

[17] Gehana Booth, Andrew Soknacki, and Anil Somayaji, "Cloud Security: Attacks and Current Defenses," 8th Annual Symposium On Information Assurance (Asia'13), June 4-5, Albany, New York , 2013, pp.56-62.

[18] N Jeyanthi, N.Ch.S.N Iyengar, P C Mogan Kumar, Kannammal A 2013, "An Enhanced Entropy Approach to Detect and Prevent DDoS in Cloud Environment", International Journal of Communication Networks and Information Security, Vol. 5, No. 2, pp. 163-173.

[19] K. Vieira, A. Schulter, C. B. Westphall, and C. M.Westphall," Intrusion Detection for Grid and Cloud Computing," IEEEComputer Society, Vol.12, July/August 2010, pp.38-43.

[20] S. Roschke, F. Cheng, and C.Meinel,"Intrusion Detection in Cloud," 8th IEEE International Conference on Dependable, Automatic and Secure Computing, pp.729 – 734.

[21] Anindita Saha1, Abhijit Das "A Detailed Analysis of the Issues and Solutions for Securing Data in Cloud," IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 4, Issue 5, Sep-Oct.
2012, PP 11-18.

[22] Jeyanthi, N. , Iyengar, N.Ch.S.N. 2012, "Packet resonance strategy: A spoof attack detection and prevention mechanism in cloud computing environment", International Journal of Communication Networks and Information Security, Vol. 4, No. 3, pp. 163-173