Recognizing DDoS Attacks & Their Impact in Cloud Environments

Ravula Kartheek[1], Matla Rajakumari Yadav[2], B. Siva Kanaka Raju[3], Kamarajugadda Indumathy[4]

[1]Assistant Professor, St.Ann's Engineering College: Chirala
[2]Assistant Professor, Rise Krishna Sai Group Of Institutions: Ongole
[3]Assistant Professor, Guru Nanak Institutions Technical Campus: Ibrahimpa
[4]Assistant Professor, Rise Krishna Sai Group Of Institutions: Ongole

Abstract:

Cloud computing is a growing technology that is being utilized by numerous businesses. However, there are other concerns, one of which being DDOS.

It may have an impact on enterprises who rely on the cloud for their operations. This paper outlines DDoS attacks, their impact on cloud computing, and the factors to consider when picking DDoS security techniques.

Keywords: Cloud computing; cloud security; distributed denial of service; DDOS

1. Introduction:

The National Institute of Standards and Technology (NIST) defined cloud computing in 2009 as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." Pay per usage, virtualization, on-demand access, flexibility, and lower hardware and maintenance costs are some of the elements driving cloud computing's appeal. Cloud computing service models include Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS). SaaS allows you to run and use software/applications without having to install them on your own PC. IaaS uses virtualization technologies to provide infrastructure by sharing hardware with a large number of clients or tenants. Virtualization contributes significantly to cloud computing by making efficient and systematic use of available hardware. Recently, virtualization has been applied at different stages such as networks, CPU, memory, storage, and so on. It improves system availability while simultaneously lowering costs and presenting a more adaptable system. DDoS attacks are a major source of downtime. The attacker can severely weaken or completely disrupt the victim's network connectivity. The attacker compromises several agents or hosts before launching the attack by depleting the target network. The primary goal of a DDoS assault is to prevent the target from using the resources. In the majority of instances, the targets might be web servers, CPUs, storage, and other network resources. DDoS can drastically decrease the performance of cloud services in the cloud environment by harming virtual servers.

1.1. Recognizing the Attack

DDoS assaults are started by influencing the victim in the following ways:

- The attacker may discover a defect or weakness in the software implementation, causing the service to be disrupted.
- Some assaults consume all of the victim's bandwidth or resources.

Attackers scan the network for machines with vulnerabilities, and these machines are subsequently used as agents by the attacker. These are known as zombie machines. Zombie machines employ spoof IP addresses. The internet's design creates numerous scenarios that can result in denial of service attacks. This section will go over some of these characteristics. Hosts are responsible for internet security. Attackers undermine host security to launch DDoS attacks, and often employ faked IP addresses, making it harder to track down the source of the attack. The internet is currently at capacity. It provides the attacker with a plethora of alternatives from which to select vulnerable hosts. DDoS attacks primarily target network resources such as bandwidth and CPU, which are limited. If these resources are raised, the impact of the attack can be reduced, but resources will still be wasted, resulting in monetary loss.

1.2. Previous DDoS Attacks

DDoS attacks are launched by Zombies, a network of remotely managed, well-structured, and widely scattered nodes. The attacker initiates an attack with the assistance of zombies. These are referred to as secondary victims. Recent attacks in 2013 include attacks on Chinese websites, Bitcoin, the largest cyber-attack by Cyber Bunker, the NASDAQ trading market, and Iranian cyber-attacks on the FBI, among others. According to the results of the survey, the majority of DDoS victims are spread and shared. Aside from the ones listed, there are several anonymous tools that are being developed on a daily basis. Table 1 shows the evolution of DDoS attacks over the years.

Table 1 shows previous DDoS assaults.

Year	Details
1998	DDoS tools were uncovered for the first time. Although these technologies were not frequently utilized, point-to-point DoS assaults and Smurf amplification attempts persisted.
1999	A trinoo network was used to flood a single system at the University of Minnesota, rendering it inoperable for more than two days. A major Shaft attack was also observed. Sven Dietrich studied the data collected during the attack and presented it in a paper at the USENIX LISA 2000 conference in early 2000.
2000	Michael Calce (Mafiaboy), a 15-year-old boy, conducted an attack on Yahoo's website. He was then sentenced to 8 months in a juvenile prison center. He then proceeded to degrade the servers of CNN, eBay, Dell, and Amazon, demonstrating how simple it was to disrupt such large websites.
2001	The scale of the attack increases from Mbps to Gbps. A 3 Gbps DDoS attack impacted Efnet.
2002	According to reports, 9 of the 13 root internet servers were under significant DDoS attack. Congestion caused by the attack rendered a few root name servers inaccessible from various portions of the worldwide Internet, leaving many valid searches unanswered.

2003	Mydoom was used to disable the SCO Group's online service. Thousands of computers were infected in order to transfer data to the target server.
2004	Authorize-IT and 2Checkout were two online payment processing companies targeted by DDoS in April. It was then revealed that the attackers extorted money and threatened to shut down their websites.
2005	Jaxx.de, a gaming website, was under DDoS attack in August 2005, and the perpetrator demanded 40,000 euros to end the attack.
2006	Several DDoS assaults were launched against Michelle Malkin's blog. The attacks began on February 15 and lasted until February 23.
2007	During the Russian riots in December 2007, government websites were subjected to significant DDoS attacks. Many of them were denied access to IP addresses outside of Estonia for several days.
2008	During the Russian riots in December 2007, government websites were subjected to significant DDoS attacks. Many of them were denied access to IP addresses outside of Estonia for several days.
2009	On July 4th (Independence Day in the United States), 27 websites belonging to the White House, the Federal Trade Commission, the Department of Transportation, and the Department of the Treasury were targeted. On August 1, various social networking sites' blogging pages (Twitter, Facebook, etc.) were hit by a DDoS attack directed at "Cyxymu," a Georgian blogger.
2010	Operation Payback: DDoS assaults against the websites of Visa, MasterCard, and PayPal in response to their decision to cease providing support to WikiLeaks.
2011	The CIA website (cia.gov) was attacked by the hacktivist organization LulzSec.
2012	A lot of the DDoS attacks against US banks use the itsoknoproblembro program. There are a lot of these DIY toolkits available.
2013	DDoS attacks at 150 Gbps are growing.

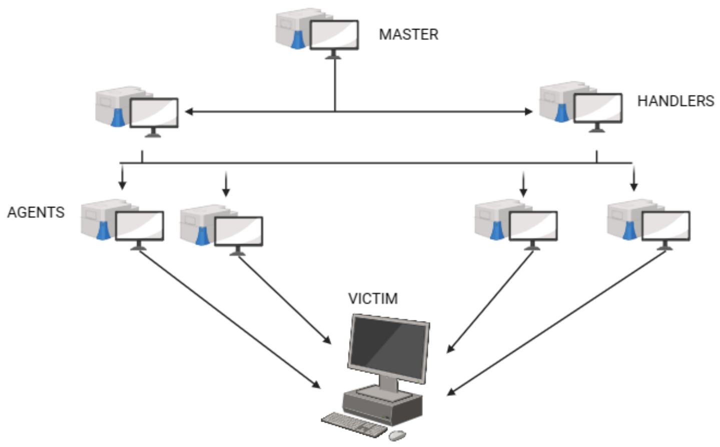

Fig. 1. DDoS Components

1.3 DDoS Inherents

Botnets have become a common tool for DDoS assaults in recent times. The tools and botnet topologies used to initiate DDoS flooding assaults are described in this section. A DDoS attack is launched using a large number of computers. Client-server technology is utilized. A DDoS assault typically consists of a Master, Handler, Agents, and Victim (Fig. 1). The master uses the zombies, also known as agents or bots, to create a botnet. The onslaught will be more disruptive the more zombies there are. Agents and the Master converse through handlers.

For instance, handlers are installed applications on a group of hacked devices (such network servers) that hackers use to convey commands to one another. Via handlers, the attacker commands and manages their agent. Devices that have been compromised by their controllers are known as bots.

The real attack on the victim's machine is executed by the bots. An attacker searches for a susceptible machine using a variety of scanning techniques.

The most basic technique, known as Random Scan, randomly searches the whole IPv4 address space because the worm is unable to determine the host's location. Because IPv6's address space is too large, it is only functional for IPv4. A list of IP address susceptible hosts on the Internet can be found on Hitlist Scan. This list has undergone scanning. A portion of the first hit list will be forwarded to the machine it turns into a host. When BGP routing prefixes are employed, route-based scanning narrows the search space significantly by using the information included in these prefixes. By having multiple hosts scan distinct regions of the address space, the Divide-and-Conquer Scan approach saves resources.

In addition to these, there exist additional tactics such as Topological Scan, Local Preference Scan, and Permutation Scan. After scanning, the host must be located and its vulnerabilities must be discovered in order to take control of it. You can find out more about these vulnerabilities online. Common Vulnerabilities and Exposures, for instance, refer to

1.4. Categorization

In the field of computing, DDoS attacks are becoming more and more varied. The two main categories of assaults are resource- and bandwidth-based. Both kinds use up all of the exploited network's resources and bandwidth.

Using the results of the investigation, taxonomy is shown in Fig. 2. It is further subdivided into many forms based on the exploited vulnerability.

Attacks known as "**bandwidth depletion**" occur when an attack overloads the victim's or target system's bandwidth, preventing legitimate traffic from entering the victim network. These attacks are typically carried out with tools like Trinoo. Attacks that cause bandwidth depletion are further divided into:

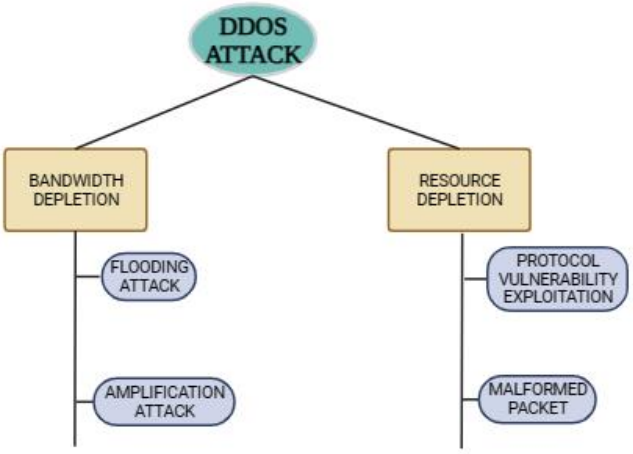

Fig. 2: DDoS Attack Taxonomy

- **Flood Attacks:** In this type of attack, an attacker uses zombies to send massive amounts of traffic to the target, clogging the victim's network bandwidth with IP traffic. The victim system experiences a network bandwidth overload and quickly slows down, making it impossible for legitimate traffic to connect to the network.

UDP (User Datagram) and ICMP (Internet Control Message Protocol) packets are what cause this.
The following actions start a UDP flood attack:

1. Using zombie assistance, an attacker transmits a significant volume of UDP packets to random or designated ports on the victim machine.
2. The victim system searches the destination ports after receiving the packets to find the apps that are waiting on the port.
3. It sends out an ICMP packet with the message "destination unreachable" in the absence of an application.
4. Rather than going to the zombies, the victim's reply packets are sent to the spoof address.

Consequently, the bandwidth that was available was used without providing service to the authorized customers. This affects the networks and infrastructure close to the victim. Fragmentation, DNS flood attack, VoIP flood attack, media data flood assault, and so forth are further forms of this approach.

The steps below are involved in an ICMP flood attack:

1. With the use of zombies, an attacker delivers a significant quantity of ICMP ECHO REPLY, or ping, packets to the victim system. The recipient of these packets must reply with a message.
2. In response to the packets received, the victim sends the answers.
3. Request-response traffic is currently congested on the network. The ICMP packet may contain the faked IP address.

Without providing service to the authorized users, the victim network connections' bandwidth quickly becomes saturated and exhausted. The other variations are DNS flooding, Ping flooding, and fragmentation.

Attacks using amplification: The attacker bombards a broadcast IP address with a lot of packets. ultimately results in malicious traffic since the systems inside the broadcast address range respond to the victim system. The majority of internet-working equipment, including routers, include a broadcast address feature that can be exploited by this kind of attack. Zombies can assist the attacker or the attacker alone can begin this type of DDoS attack.

Smurf and Fraggle attacks are the most well-known examples of this type of attack.

The following actions are what lead to the Smurf attack:

1. An attacker uses the broadcast addressing approach to deliver packets to a network device. These packets have the victim's address spoofing or forging the return address.
2. The network amplifier broadcasts ICMP ECHO RESPONSE packets to every system within the broadcast IP address range. The recipient of this packet is expected to reply with an ICMP ECHO REPLY.
3. The victim receives an ICMP ECHO REPLY message from every machine within range.

The Smurf attack variant known as "Fraggle" occurs when UDP echo packets are routed to ports that enable character generation. It follows these procedures:

1. The attacker uses a port that allows character creation to receive UDP echo messages. These packets contain an indefinite loop because the victim's address is spoofing or forging the return address on the port that supports character creation.
2. All systems reached by broadcast address are targeted, with the port that supports character creation being the target.
3. The victim's character generator port receives echoes from every system in the range.
4. Because UDP echo packets are used, this process keeps repeating.

The smurf attacks pale in comparison to this one. The reflector assault is a variation of these attacks that uses a group of reflectors to complete a certain objective. The reflector is a host or device that acts as an intermediary to initiate amplification assaults. The reflector's unique quality is that it continuously reacts to the packets it receives. Therefore, these reflectors are used by the attackers for attacks that call for a response. In this instance, the victim's system will receive a faked return IP address.

Attacks on Depleting Resources: The goal of a Distributed Denial of Service (DDoS) attack is to deplete all available resources on the victim system, preventing service to authorized users.

The types of resource depletion that exist are as follows:

- **Protocol Exploit Attacks**: By taking advantage of a particular characteristic of the protocol that the victim has installed, these attacks aim to consume the excess quantity of resources from the victim. The most effective example of this kind of assault is TCP SYN. The PUSH + ACK attack, the authentication server assault, and the CGI request attack are more instances of protocol exploit attacks.

Malformed Packet Attacks: A packet that contains harmful data or information is referred to as being malformed. In order to bring down the target, the attacker sends it these packets. There are two ways to go about doing this:

IP address attack: The malicious packet causes havoc in the victim's operating system by using the same source and destination IP addresses. It crashes the victim by drastically slowing down in this manner.

Attack on IP packet options: Every IP packet has an optional field that can hold extra data. These fields are used in this attack to create the corrupted packet. To complete the optional fields, all quality of service bits must be set to one. The victim must so invest more time in processing this packet. When multiple zombies strike at once, this attack becomes more susceptible.

1.5. Protection Mechanism

A number of countermeasures have been implemented and are continually being developed to mitigate the effects of DDoS attacks. The majority of DDoS assaults are caused by an intrusive party trying to gain unauthorized access to the network or system that is being attacked.

The protective mechanisms are depicted in Figure 3.

Methods of Prevention

Preventing attacks is the best defense against any kind of assault. The use of filters is one such method.

- **Ingress filtering**: this procedure identifies and blocks incoming packets that have an invalid source address. For this, routers are employed. By using this method, the DDoS assault brought on by IP address spoofing is avoided.
- **Egress filtering**: this method makes use of an outgoing filter. This method permits packets with valid IP addresses within the range designated by the network to exit the network.

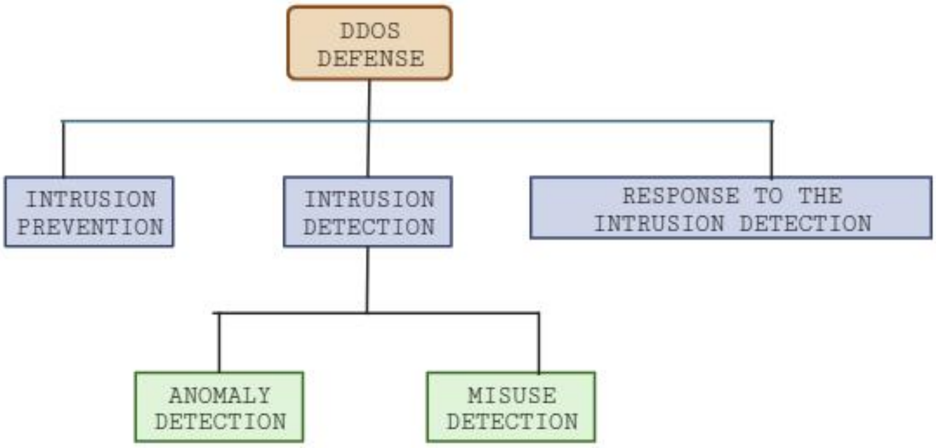

Fig. 3: DDoS protection strategies

- **Route-based distributed packet filtering:** This method stops attacks by capturing and filtering IP address-spoofing packets using route information. Additionally, IP trace back uses it. However, it needs worldwide knowledge of the network topology.
- **Secure Overlay Services (SOS):** SOS is a distributed architecture designed to protect the victim system.

If an incoming packet originates from a legitimate server, it is presumed to be authentic. The overlay filters out other packets. To access the overlay network, a client must authenticate via replicated access points, or SOAP.

Disabling unnecessary services, updating security patches, altering IP addresses, blocking IP broadcasts, load balancing, and using honeypots are some other preventative measures. The possibility of DDoS attacks is not entirely eliminated by intrusion prevention solutions, but they do offer a foundation or boost security.

Detection Methodologies

The intrusion detection system keeps the victim's system from failing and assists in preventing DDoS attacks from spreading. Among the several techniques used in intrusion detection are:

- **Anomaly detection**: This technique finds assaults by identifying unusual system performance abnormalities or behaviors. To do this, current measurements are compared to previously identified normal system performance. This technique finds the false positives in the behavior of the system.

Among the studies on anomaly detection methods are the following ones:

NOMAD is a scalable network monitoring system that examines IP packet header data to identify network irregularities.

Technique for sampling and filtering packets with congestion: A statistical analysis of the subset of dropped packets was done, and a signal is sent to the router to filter the malicious packets when an anomaly is found.

D-WARD-identifies the initial victim of the DDoS attack. It stops the victim's neighbors from becoming targets of the attack. At the edge router, D-WARD is configured to identify incoming and outgoing network traffic.

MULTOPS: MULTOPS is a data structure intended for DDoS attack detection. It operates under the premise that steps are taken to block just the specific IP addresses of the system taking part in a DDoS assault, if it is possible to identify those addresses. By operating in attack-oriented mode or victim-oriented mode, respectively, it maintains track of which systems are attacking and which ones are being attacked. Maintaining the packet rate statistics at various aggregate levels is done by a multi-level tree. However, new RAM and router reconfiguration are needed.

Misuse detection: This technique keeps track of popular signatures or exploit patterns in order to identify DDoS attacks. Reports of DDoS attacks are made whenever one of these patterns is found. Numerous methods for detecting misuse have been covered in.

Reaction to identification

If a DDoS assault is discovered, the next course of action is to block it and track down the attacker to determine who they are. Either automatically or manually using ACL, this may be completed in two days.

Some techniques for tracking down and identifying the assailant are given in Table 2. In addition, there are numerous methods for preventing DDoS attacks, but not all of them can be identified and stopped. The only thing that can be done is lessen the attack's impact.

Table 2: Retracement Techniques

Method	Overview
ICMP retracement	The technique sends an ICMP traceback message to the destination in addition to forwarding low probability packets to each router. The majority of ICMP messages, which are used to identify attackers, encounter problems such as extra bandwidth, challenging packet validation, and path detection overhead of data from route maps.
IP tracing	This approach tracks the attacker's route backward to identify the attack's starting point. Using this method, the attacker's route is traced back to its origin. However, this becomes challenging if the internet is stateless and source accountability in the TCP/IP protocol is turned off.
Link-checking retraction	This system examines every incoming link to determine the likelihood that it is an attack. To achieve this, massive amounts of traffic are flooded, and any network disruptions are tested for. However, a system that can flood traffic with information about network topology is a prerequisite for doing this.
Stochastic	The disadvantages of link-testing traceback are addressed by this technique,

packet identification	which does not require prior knowledge of network topology, high traffic volumes, etc. This benefit also causes overhead for the systems, however there are numerous ways to prevent this overhead, as suggested in.

1.6. DDoS Intrusion Within A Cloud Setting

As we cover in our paper, cloud computing has been increasingly prevalent in commercial technology and academic study in recent years. One of the security risks that jeopardizes availability is DDoS. DDoS is one of the top nine hazards to a cloud computing environment, according to Cloud Security Alliance. In the clod environment, 14% of all attacks are DoS attacks. Early in the new millennium, DDoS attacked numerous well-known websites, including Yahoo. A massive DDoS attack occurred on the grc.com website in May 2001. The company's production activities depended heavily on the internet, which had a negative effect on profitability. VeriSign hired Forrester Consulting in March 2009 to conduct research on DDoS risks and defense. A total of 400 respondents from the US and Europe participated in the poll, and 74% of them reported having dealt with one or more DDoS attacks in their firms. Of these 74%, 31% claim that the attacks disrupted services, while 43% claim that the attacks have no effect on services, as seen in Fig. 430. According to a poll on DDoS assaults in the cloud, the frequency of DDoS attacks would rise quickly along with the usage of cloud computing. When a service in a cloud environment experiences an increase in workload, it will begin to provide processing resources to handle the added stress. This means that while the cloud system acts to hinder the attacker, it also helps him in certain ways by giving him the capacity to cause the greatest amount of harm to the service's availability, beginning at a single point of attack.

Other services offered on the same hardware servers that house cloud services could be adversely affected by flooding-related workload. Therefore, a service's own availability may be impacted if it attempts to operate on the same server as another overloaded service. An additional consequence of floods is a sharp increase in cloud computing costs. The lack of a "upper limit" on usage is the issue. Neighbor attacks, in which a virtual machine (VM) assaults its neighbor in the same physical infrastructure and stops it from offering services, are another possible attack vector against cloud environments. These attacks have the potential to impair cloud performance, result in monetary losses, and endanger other servers inside the same cloud architecture.

1.7. Considerations When Choosing a Defense Solution

There are several factors to take into account while choosing a DDoS solution.

- **Functional:** The remedy must be sufficiently functional to mitigate the effects of the attack, regardless of the attack's strength.
- **Transpicuous:** The solution must be simple to apply, meaning that altering the current network's infrastructure is not necessary.
- **Lightweight:** The solution must, above all, not burden the system.
- **Precise**: A lot of false positives should not be produced by the chosen solution. Numerous techniques require that the traffic be abandoned or dropped, however the solution can't drop legitimate traffic.

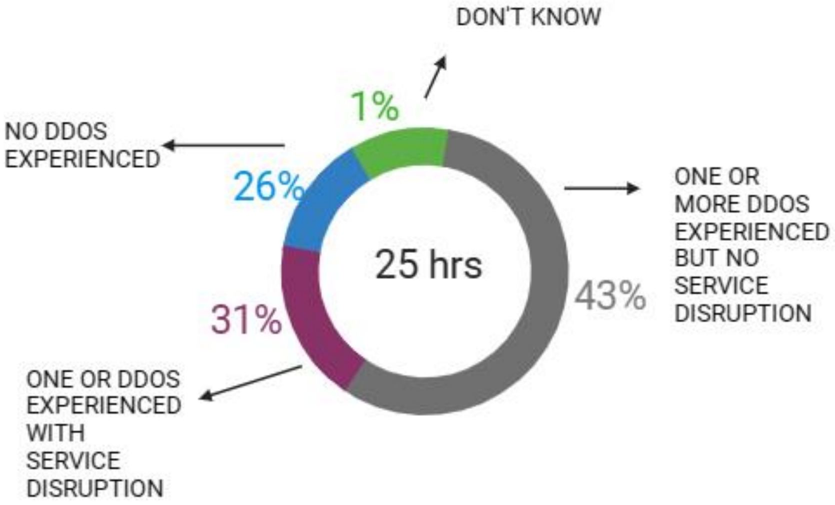

Fig. 4. Organizations' experiences with DDoS

2. Synopsis / Conclusion

Given the increase of DDoS assaults in cloud computing. In addition to a brief overview of DDoS attacks, this paper also discusses their types, taxonomy, and countermeasures. Techniques for DDoS detection, prevention, and tolerance are provided by this survey. The paper's conclusion offers some considerations for choosing a DDoS defense solution.

References

1. P. Mell and T. Grance, “The NIST definition of cloud computing (draft),” NIST special publication, vol. 800, no. 145, p. 7, 2011.
2. Reference Architecture Doc 2011 NIST-CloudComputing.pdf.
3. T. Dillon, C. Wu, and E. Chang, “Cloud Computing: Issues and Challenges,” in 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), 2010, pp. 2733.
4. Denial of Service Attack, http://en.wikipedia.org/wiki/Denial-of-service attack
5. DDoS attack tool timeline, http://staff.washington.edu/dittrich/talks/sec2000/timeline.html
6. History of DDoS, http://www.timetoast.com/timelines/history-of-ddos
7. DoS and DDoS Evolution, http://users.atw.hu/denialofservice/ch03lev1sec3.html
8. CERT Coordination Center, Overview of attack trends, Feb. 2002. http://www.cert.org/archive/pdf/attack trends.pdf.
9. B. Grobauer, T. Walloschek, and E. Stocker, “Understanding Cloud Computing Vulnerabilities,” Security Privacy, IEEE, vol. 9, no. 2, pp. 5057, Mar. 2011.
10. 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. 643666.
11. CERT Advisory CA-1998-01, Smurf IP Denial-of-Service Attacks, January 5, 1998, Available: http://www.cert.org/advisories/CA-1998-01.htm
12. Meiko Jensen, Jorg Schwenk, Nil Gruschka “On technical issues in cloud computing”, IEEE International Conference on cloud computing, 2009.

13. The Notorious Nine, Cloud Computing Top Threats in 2013, https://downloads.cloudsecurityalliance.org/initiatives/topthreats/TheNotoriousNineCloudComputingTopThreatsin2013.pdf
14. N. Weiler, Honeypots for Distributed Denial of Service, in Proceedings of the Eleventh IEEE International Workshops Enabling Technologies:Infrastructure for Collaborative Enterprises 2002, Pitsburgh, PA, USA, June 2002, pp. 109114.
15. P. Ferguson, D. Senie, Network ingress filtering: defeating Denial of Service attacks which employ IP source address spoofing, in: RFC 2827,2001.
16. Global Incident analysis Center Special Notice Egress filtering, Available from http://www.sans.org/y2k/egress.htm.
17. K. Park, H. Lee, On the effectiveness of route-based packet filtering for Distributed DoS attack prevention in power law Internets, in: Proceedings of the ACM SIGCOMM 01 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, 2001, pp. 1526.
18. A. Keromytis, V. Misra, D. Rubenstein, SoS: secure overlay services, in: Proceedings of the ACM SIGCOMM 02 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, 2002, pp. 6172
19. C. Zou, D. Towsley, and W. Gong, the performance of internet worm scanning strategies, 2003.
20. V. Paxson S. Staniford and N. Weaver, How to own the internet in your spare time, in 11th Usenix Security Symposium, San Francisco, August 2002.
21. V. Paxson S. Staniford and N. Weaver, How to own the internet in your spare time, in 11th Usenix Security Symposium, San Francisco, August 2002.
22. C. Zou, D. Towsley, W. Gong, and S. Cai, Routing worm: A fast, selective attack worm based on ip address information, 2005. Common Vulnerabilities and Exposures, http://cve.mitre.org/cve/
23. J. Mirkovic, G. Prier, P. Reiher, Attacking DDoS at the source, in: Proceedings of ICNP 2002, Paris, France, 2002, pp. 312321
24. R.R. Talpade, G. Kim, S. Khurana, NOMAD: Traffic based network monitoring framework for anomaly detection, in: Proceedings of the Fourth IEEE Symposium on Computers and Communications, 1998.
25. Y. Huang, J.M. Pullen, Countering Denial of Service attacks using congestion triggered packet sampling and filtering, in: Proceedings of the 10th International Conference on Computer Communiations and Networks, 2001.
26. T.M. Gil, M. Poleto, MULTOPS: a data-structure for bandwidth attack detection, in: Proceedings of 10th Usenix Security Symposium, Washington, DC, August 1317, 2001, pp. 2338.
27. S. Savage, D. Wetherall, A. Karlin, T. Anderson, Network support for IP traceback, IEEE/ACM Transaction on Networking 9 (3) (2001) 226237.
28. H. Burch, H. Cheswick, Tracing anonymous packets to their approximate source, in:Proceedings of USENIX LISA (New Orleans) Conference, 2000, pp. 319327
29. S. Bellovin, The ICMP traceback message, Network Working Group, Internet Draft, March 2000, Available S. Bellovin, The ICMP traceback message, Network from ¡http://lasr.cs.ucla.edu/save/rfc/draft-bellovin-itrace-00.txt¿

30. Rashmi D. and Kailas D. mitigating ddos attack in cloud environment with packet filtering using iptables in International Journal of Computer Engineering and Applications, Volume VII, Issue II, August 14