# DDOS Attacks & Mitigation Techniques in Cloud Computing Environments

**Shubham Kumar Sahu, Dr. R. K. Khare**
sksdbest@gmail.com , rakesh_khare2001@yahoo.com
*Department of Computer Science & Engineering*
*Shri Shankaracharya Engineering College, Bhilai, Chhattisgarh*

## *Abstract*:

*In the current internet world , most of the services , businesses and other things are mostly relying on the cloud services let it be mail service , social medias , payment gateways , and nowadays traditional computing and data storage of businesses are done in the cloud environment , but are they safe enough that we are putting all our sensitive data on cloud , are they reliable , are they secure , so in this paper we are going to analyze the various DDOS(Distributed Denial of Service) attacks in cloud environments and their mitigation strategies and will conclude with which method is better and which methods need a little improvement or which method may harm your clients , because in DDOS the main aim is to provide access to legitimate user 24*7 but not to unauthorized user, along with that we have also proposed a methodology/ algorithm which is completely cloud based and this will remove some limitations from earlier technologies, We will discuss all types of DDOS attack and their mitigation strategies in this paper.*

***Keywords: Cloud computing, DOS, DDOS, Firewall, UDP Flood, SYN Flood, DNS***

## I. INTRODUCTION

Today when business is relying on the cloud services, it may be harmed by DOS (Denial of Service) attack, there are various types of attacks and there are multiple ways to bring a site or a service down that is available on the internet. The aim is always the constant; goal is to make the service/site unavailable for the legitimate users. So how can one bring the services down of any system, the simplest answer to this could be the by making the resources like bandwidth , processing capabilities , ram usage , CPU usage 100 % by spam traffic and when some legitimate user tries to access the content it show them error for service/site not available and this is done by various ways such as UDP, ICMP flooding by sending a lot of request and not responding to those request the server allocates some resources for each request and after lakhs of request the server may stop responding and causing legitimate user to keep away from accessing the original services. The magnitude of attack is measured in Request per Second (RPS), or packets per seconds when packet flooding. Difference between DOS and DDOS is DOS is performed by one system and DDOS is by multiple systems like botnet (Shown in Fig No. 1).

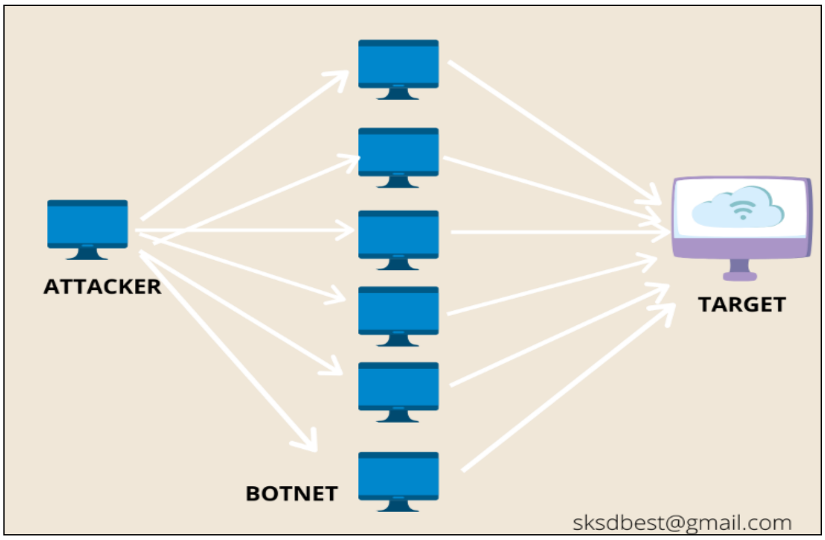

Fig No. 1 DDOS Attack Illustration

**Categorization of Attacks**

1. **Volume based Attacks**
   In this type of attacks , the attacker or the hacker who is trying to attack doesn't attack from one system , attacker creates a botnet(millions of infected system) of multiple trojan infected systems and one system is made controller of that botnet and then the controller gives order to botnet to perform attack from each system that's part of the botnet and is active and that botnet than performs attacks such as giving them instructions to access those sites or server , ping request, death of ping etc. but now a days attackers are using DNS amplification and cloud based servers so that they don't have to create the botnet and these are more dangerous than the botnet method.

2. **Protocol based Attacks**
   In this type of attack the attacker uses a protocol that's available between systems and uses it for wrong purpose like flooding ICMP packets and other packets such as UDP packets etc. so each request of packets received by the server it allocates some resources for it, so the aim is to send a lot of request that after sometime the server may stop responding so that legitimate users cant access the service/site.

3. **Application-layer based Attacks**
   In this type of attack the attacker basically targets the applications of the server, and flood those applications so that after sometime it may stop responding such as the most used method is http requests i.e. GETs/ POSTs launching millions of request per second so that after sometime the server gets crashed and the service/site is not available for the legitimate users.

## II. Types of Attacks & their Mitigation

### A. Ping of death / ICMP Flooding

Ping is a facility to check the connection between the two systems but unfortunately same ping service can be used by attacker to send ping request millions and billions of time so that the server may stop responding. For its mitigation either firewall is used but that also fails sometime so in the worst cases ICMP ping is disabled by the site or the server admin.

### B. SYN flooding / TCP flooding

In this attack the attacker sends SYN packet to the server from spoofed IP address and the server tries to respond it by sending the SYN/ACK packet but the if doesn't exist and the waits for the reply and allocates some resources to it , but the attacker floods this request a million/billion times so that the server may stop responding to the legitimate users. Mitigation is done using firewalls, Reducing SYN-RECEIVED timer, by Recycling the oldest half-open TCP.

### C. UDP flooding

In this attack the attacker Floods UDP packets to the Target from spoofed IP, now target tries to respond each by send ICMP packet replies thus causing the system to be irresponsive and unavailable for the legitimate users. Mitigation is done by limiting the rate of ICMP responses and using firewalls.

### D. Smurf Attack

In this attack the attacker uses a system and spoofs IP of the victim and broadcasts the ICMP packets to large no of systems and that all system sends replies to the victim causing the victim to overloaded by the heavy traffic and unavailable for the legitimate users. Mitigation is done by not responding to ICMP request and some cloud service providers filters the requests.

### E. Teardrop

In this attack the attacker sends a crafted packet with payload of greater size that the victim system can handle and eventually it causes to crash the system. Modern operating systems are safe from this attack only older operating systems are vulnerable Mitigation is done by inspecting traffic if they have violated the fragmentation rule or not.

### F. DNS Amplification

In this attack the attacker uses the DNS open resolver and uses the victims IP and sends victims IP through botnet to open recursive servers and that servers now sends large number of packets to the victim causing it to be irresponsive. Mitigation is done by rate limiting and blocking all the open recursive relay servers.

### G. SIP Invite Flood

Session Initiation Protocol (SIP) is used for making connection in VOIP (Voice over IP) and SIP Invite packets id used to start a VOIP Session and sending large number of SIP Invite packets to victim causes the victim to be irresponsive. It is hard to detect and mitigate, no perfect solution or security software exist which can mitigate this flood and verify the legitimate sip request.

### H. Sloworis Attack

Sloworis is an attack tool created by Robert Hansen and what this tool does is establishes large no of partial connection and tries to keep them active for longer duration causing the victim system to be unavailable for the legitimate users. Mitigation is done by increasing max number of allowed clients on the server.

### I. SSL DDOS Attack

In this attack the attacker uses the SSL handshake mechanism, and sends malicious request to server for the SSL Handshake and the server trying for handshake for large number of requests the SSL Mechanism uses encryption and decryption, causing more CPU usage and eventually making the server crash or unresponsive. Mitigation is not easy because SSL handshakes requires lot of resources and no successful mitigation technique developed that can guarantee 100% protection from this attack.

### J. Low/High orbit ion canon

LOIC (Low orbit ion canon) & HOIC (High orbit ion canon) are open source tools available on open repositories were made as pen testing tools to do the stress testing of web applications but unfortunately, they are used for DOS attacks. Mitigation is done by firewalls and traffic filtering.

### K. Zero-Day DDOS Attacks / One Packet Killer

In this attack the attacker can crash a system by one or more packets, zero-day means for the vulnerability that has not yet been detected by anyone no patched for that had been made and according the attacker crafts packet and sends to the victim causing system to crash. Mitigation is not easily possible; strategies needs to be planned instantly for this case.

## III. DDOS ATTACK LIFE CYCLE

The DDOS attack has 4 phases (shown in Fig No. 2) basically than an attacker needs to perform in order to attack any victim. These 4 phases are: -

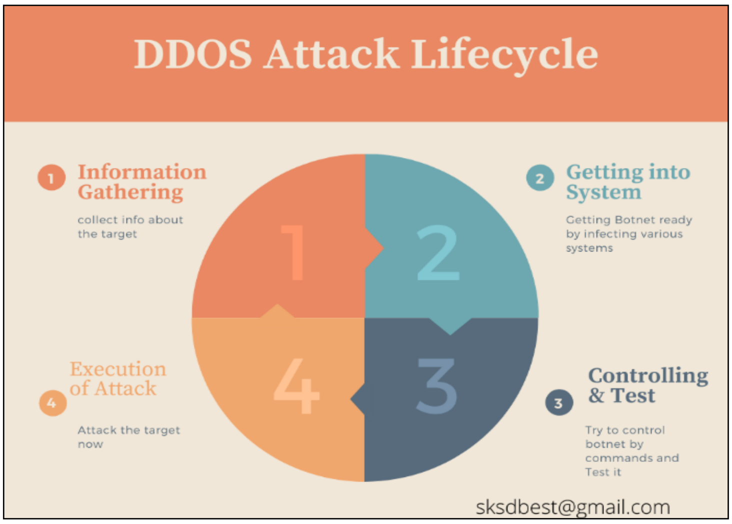

Fig No. 2 DDOS Attack Lifecycle

**A. Information gathering**

In this phase the attacker tries to collect as much information as possible about the target/victim such as location, IP address, employee details, security software details, Operating system details this thing can be very much useful while performing an attack.

**B. Getting in to system**

Now after collecting information about the target, the attacker needs a botnet or compromised cloud server so the attacker either hacks cloud servers or creates crack patch for famous software's along with the infected trojan file which will create the system as a part of botnet.

**C. Controlling & Test**

Once the botnet is ready it's time to check them that how many bots are active and are they listening to your commands or not , after you h find the active bots , it's time to test your attack on a dummy target once its successful than you are ready to go.

**D. Execution of Attack**

After the successful trial attack now, attacker performs the attack in the same manner to the original target and with another proxy, you can try and check that whether its accessible or not. If the target site or server is not opening or not responding or is lagging than the attack is completed.

## IV. DDOS Mitigation Lifecycle

DDOS Attacks are good and fun on attacker's end but more frustrating when you are the victim. So, mitigation of DDOS are basically done in six phases (Shown in Fig No. 3) and they are: -

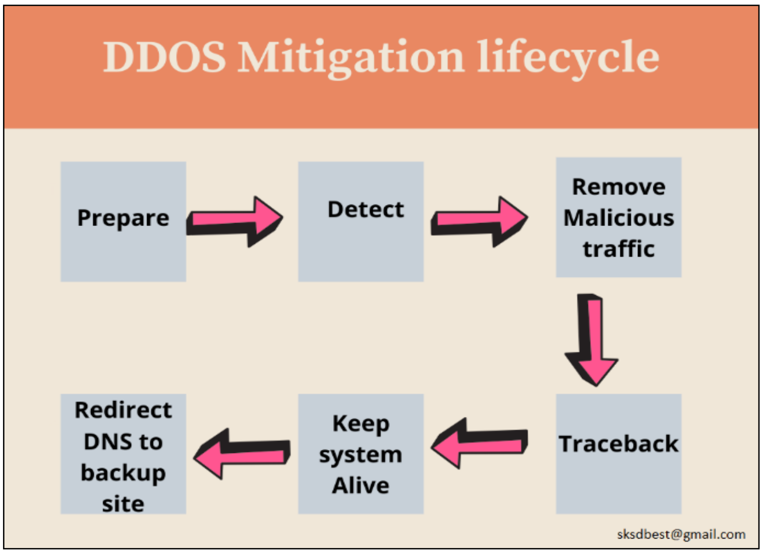

Fig No. 3 DDOS Mitigation Lifecycle

**A. Prepare**

prevention is always better than the cure , so organization and the site /server administrator needs to be prepared for the attacks from the very beginning or else it's too late, the preparation includes having good firewall, security policy checking, having a IDS software, check for system updates timely, have packet and traffic filters software and hardware based both, companies can also buy cloud DDOS mitigation services there are various online mitigation providers that provides cloud based services.

**B. Detect**

If any DOS attack is performed on your servers or site, you see abnormal system behaviors or the security software's alerts will tell you that it has detected an ongoing attack on your system sometime it may show what measures to do , sometimes it automatically performs and sometimes it can't even detect you have to manually check the things than.

**C. Remove Malicious traffic**

Once you have detected than you are in an ongoing DDOS attack , now find out which one is malicious and which ones are legitimate than drop those malicious traffic, most of the time when it's hard to differentiate what site admins mostly do is they shut down the server/site temporarily so that the attacker cannot attack to the server but actually its wrong , He has won now because his goal to shut or deny service to legitimate users is completed.

**D. Traceback**

Once you have detected that malicious traffic is coming to your server next step is to trace them try to know where they are coming from and who is doing is , this is very tough job , IF one has detected the IP address of each request they are getting from and then tracing from where they are receiving those commands from.

### E. Keep system alive

Now as Mentioned earlier from defending side your goal is to drop those malicious traffic not to shut the server, shutting server is simply letting the attacker win in his goal, try to redirect those malicious traffic somewhere else, because your main goal should be to provide access/ service to the legitimate users.

### F. Redirect DNS to backup server

Big organizations must have a backup server , extra bandwidth , extra resources always all-time ready 24*7 , so that if all your preventive measures aren't working and attacker is continuously increasing the magnitude of the attack than you must use your backup server are redirect those traffic to backup by changing the DNS records.

## V. CLOUD BASED PROPOSED ALGORITHM

We have discussed a lot of attacks and types and their mitigation methods, but all these things are tough for organizations without skilled technicians and small organizations can't even afford that skilled manpower, so there are numerous numbers of cloud DDOS mitigation service providers what they do is they basically redirect all your traffic to their servers and then they check those traffic and drop malicious one and forward the legitimate traffic to your server, they have skilled manpower and proper resources hardware's and software's needed for those mitigation services.

### A. Existing algorithm used by various cloud service providers

There are multiple Cloud DDOS Mitigation service providers like cloudflare, imperva, xiarch, but mostly the algorithm or methodology is same here is the algorithm most of them follow: -

1) Take all you traffic to their servers
2) Try to Detect the traffic for legitimate and malicious traffic
3) They detect using firewalls, security software's, IDS, Artificial Intelligence to detect & adapt patterns of attacks and various guidelines and security protocols they follow
4) If found malicious traffic, they redirect that traffic to somewhere else or drop those traffic
5) Sends the legitimate traffic to your server
6) Do analysis and try to traceback

### B. Limitations of Earlier Technologies or algorithms

Let's Take a Scenario, any E-commerce website like flipkart or amazon has a large sale, now on same time the attacker does DDOS attack using botnet, as there is a large sale this is guaranteed that there's going to be large amount of traffic to the site when compared to normal times now that's the aim of attacker to not to let legitimate user access those sales. Now in this situation what actually will happen is the detection fails or goes wrong, because the legitimate traffic may also create certain patterns and blocking or dropping the legitimate in this high business time can drop their sales and reputation too specially when even if single privileged customer of there is dropped than the image will start degrading.

### C. Proposed algorithm for cloud mitigation services

The best way to fight against DDOS in Distributed resources and distributed computing and using of DNS Load balancers, having more than one server for same site/service and also using multitenancy.

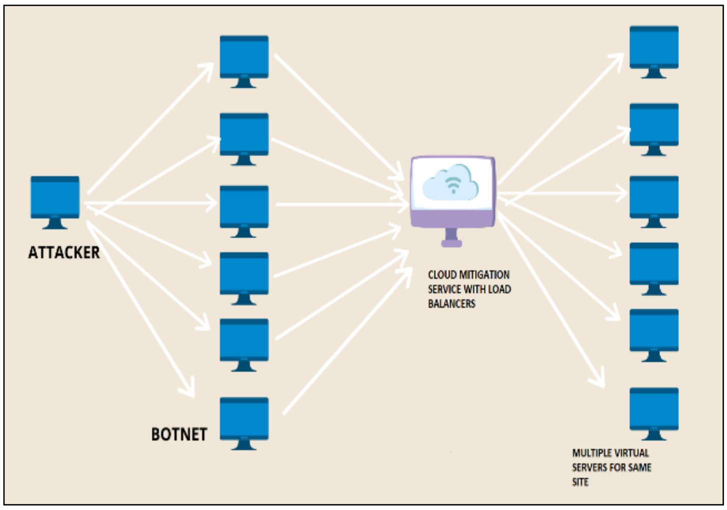
ATTACKER
BOTNET
CLOUD MITIGATION SERVICE WITH LOAD BALANCERS
MULTIPLE VIRTUAL SERVERS FOR SAME SITE

Fig No. 4 Basic view for proposed methodology

The proposed algorithm is as follows: -

1. Redirecting all traffic to cloud servers first.
2. Try to detect the malicious traffic and double confirm the malicious traffic because any legitimate user should always have access to the services
3. Detect using various firewalls of multiple layers also ensuring speed at the same time and security software’s and hardware’s to detect packets of the traffic and their pattern, whether the source is responding back or not, if the source is responding back than only its legitimate else it’s clear that its spoofed. Also follow guidelines and protocols and security standards and keep system also updated.
4. First complete the connection of the traffic with cloud servers i.e. the TCP handshake or SSL handshake should first be done with mitigation service servers and then if found legitimate than forward, this will ensure if the attack happens the cloud service is the victim not the original server.
5. Drop the malicious traffic if Mitigation service is the victim than drop all the traffic that are attacking the service.
6. Now there needs to be more than one server it can be either original for big organization’s or virtual cloud servers, synchronizing the database could be a bit of an issue here, but this could be managed using multitenancy
7. Managing loads that a single server doesn’t get all the traffic it should be managed using technologies like DNS load balancer
8. All servers should have active firewalls that with restricted actions so that any user can’t directly access the server all traffic should come through cloud mitigation service in the

servers and to database server all traffic will come through all virtualized servers only, this will also prevent large numbers of other attacks.

9. Proper Logs of everything and every connection should be maintained so that it could be easy to analyze and trace back

## VI. Result & Conclusion

After learning all types of attacks and their mitigation techniques, it's simple that handling all these by organization's isn't easy task so going with cloud DDOS mitigation service provider is beneficial for them in term of work load as well as in terms of costing and safety. But there are certain scenarios where they lack and which could be improved, so my proposed methodology aims to rectify those techniques. Adding extra layers of security is always helpful and as the DDOS works on distributed systems, if same distributed approach is given using multiple servers, multitenancy and load balancing, distributing the traffic than the chances of DOS condition is reduced to the maximum extent.

## VII. Discussion & Future scope

In this paper we have given a brief detail of all the DDOS attacks and their mitigation techniques used, along with that we have proposed an algorithm for cloud mitigation services, which is theoretically is better than the original one but this has not been implemented or tested yet , this is on principle of distributed computing, basically increasing resources wither physically or virtually so that capacity on server can be increased and they can withhold attack and stay alive. Now further works needs to be done i.e. implementing and efficiency testing for the proposed methodology.

## *REFERENCES*

1. *K. Abbas, and R. Jain, "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments" in IEEE Access, 2019, Volume 7, pp. 80813-80828*
2. *Neha Agrawal and Shashikala Tapaswi, "Defense Mechanisms Against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges" in IEEE Communications Surveys & Tutorials (Volume: 21, Issue: 4, Fourth quarter 2019), pp 3769 – 3795*
3. *V. Tajane and D. Sharma, "Effective Detection and Prevention of DDoS in Cloud Computing Environment," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-5.*
4. *R. Patil, H. Dudeja, S. Gawade and C. Modi, "Protocol Specific Multi-Threaded Network Intrusion Detection System (PM-NIDS) for DoS/DDoS Attack Detection in Cloud," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bangalore, 2018, pp. 1-7.*
5. *M. S. Elsayed and M. A. Azer, "Detection and Countermeasures of DDoS Attacks in Cloud Computing," 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, 2018, pp. 708-713.*

6. *A Cisco Guide to Defending Against Distributed Denial of Service Attacks, https://tools.cisco.com/security/center/resources/guide_ddos_defense*
7. *Cloudflare DDOS Learning Resources, https://www.cloudflare.com/learning/ddos*
8. *Bhushan, K., Gupta, B.B. Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. J Ambient Intell Human Comput 10, 1985–1997 (2019). https://doi.org/10.1007/s12652-018-0800-9*
9. *Chen, W., Xiao, S., Liu, L., Jiang, X., & Tang, Z. (2020). A DDoS attacks traceback scheme for SDN-based smart city. Computers & Electrical Engineering, 81,106503. https://doi.org/https://doi.org/10.1016/j.compeleceng.2019.106503*
10. *Tang, D., & Kuang, X. (2019). Distributed Denial of Service Attacks and Defense Mechanisms. IOP Conference Series: Materials Science and Engineering,612,52046. https://doi.org/10.1088/1757-899x/612/5/052046*
11. *B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed and W. M. Abduallah, "Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods," in IEEE Access, vol. 7, pp. 51691-51713,2019,doi: 10.1109/ACCESS.2019.2908998.*