Analyzing the prevention mechanisms and mitigation techniques for handling DDoS attacks problems

Dr. Amit Kumar Chaturvedi[*1] & Divya Mahajan[#2]

*[*1]CSE Dept. Govt. Engineering College, Ajmer, [#2]Ph.D. Scholar, Bhagwant Univ., Ajmer*

Abstract: Cloud computing is a distributed open architecture of computing. It provides facility to hire all type of computing resources on pay per use manner and these resources are shared between multiple clients of the same cloud network. There are multiple providers of all type of computing services and users have multiple options to hire the service. Definitely it will create a competition between service providers to provide the better service with effective cost and the users of these services will get the good offers. Any cloud service can be started anytime, anywhere in the world by just paying for the service online. All the cloud services are accessed by using the internet. The biggest threat on the cloud service providers are the online attacks on the cloud servers, on user's data (financial, official or personal). In this paper we are more focused on DDoS attacks. During the last ten months of covid-19 pandemic, these DDoS attacks are increases in multiple. Such attacks should be detected and managed to minimize the losses to the user's data. In this paper, we are presenting an analysis report on the available preventions mechanisms and mitigation techniques for handling the issues against DDoS attacks. .

Keywords: **Attack, DDoS, cloud, security, prevention mechanisms, mitigation techniques.**

1. INTRODUCTION

Security is an essential service required for every online application. As we know that security cost is calculated on the basis of clients or account limit and the database size. In case of cloud computing, which is an open architecture, the security matters becomes very important. As most of the cloud computing applications have weak security setup and hence there are more chances of breaching the security of the cloud computing based applications. DDoS attacks are the primary and most happened attack on the cloud computing based applications.

As per the NexusGuard Q1 2020 Threat report, " DDoS Attacks increased by 542% within the first quarter of the year compared to the last quarter of the previous year". As per the Kaspersky Report, "Longest DDoS attack of Q2 2019 lasted 509 hours, almost 21 days". The comparison done for the Q1 2019 and Q1 2020 on DDoS attack then it is found that around 278% DDoS attacks rises. As we know that during the covid-19, most consumers including professionals of different field are dependent on the online solutions and it was noticed that the small-sized, short attacks known as "invisible killers" are more active during convid-19 pandemic. The increase in DDoS attack between Q3 2019 and Q1 2020 is noticed upto 542%. So, the preventive and security tools requirement also increases during such type of situation.

During Covid-19 pandemic in the last six months, most of the work throughout the world is now performed through online solutions. Now the cloud web servers are more prone to DDoS attacks and these web servers are the easy target for the hackers. The hacker attempts to make a network resources unavailable using Denial of Service (DoS) attack. Such attacks usually interrupt the host machine or web server for some time or for an indefinite time, which is connect to the internet. In the recent time, it was noticed that the web servers of organizations having important financial and personal information are jammed and asked to pay a big amount for releasing the control on the machine or information.

Some of the indicators of the DoS attacks are slow network performance, unavailability of a particular web site, inability to access any web site, Dramatic increase in the no of

spam emails received, Long-term denial of access to the web service, etc. The different types of DoS attacks are Single IP Single Port, Single IP Multiple port, Multiple IP Single Port, Multiple IP Multiple Port.

The DDoS attack is an attempt to make an online service or a website unavailable by overloading it with huge floods of traffic generated from multiple sources. Unlike a Denial of Service (DoS) attack, in which one computer and one Internet connection is used to flood a targeted resource with packets, a DDoS attack uses many computers and many Internet connections, often distributed globally in what is referred to as a botnet. A large-scale volumetric DDoS attack can generate a traffic measured in tens of Gigabits (and even hundreds of Gigabits) per second.

A DDoS flood can be generated in multiple ways. For example −

- Botnets can be used for sending more number of connection requests than a server can handle at a time.
- Attackers can have computers send a victim resource huge amounts of random data to use up the target's bandwidth.

Due to the distributed nature of these machines, they can be used to generate distributed high traffic which may be difficult to handle. It finally results in a complete blockage of a service. Actually DDoS attack is a bit difficult to detect because you do not know the host that is sending the traffic is a fake one or real.

2. Types of DDoS Attacks

DDoS attacks can be broadly categorized into three categories: (i) Volume-based Attacks, (ii) Protocol Attacks, and (iii) Application Layer Attacks

(i) **Volume-Based Attacks :** Volume-based attacks include TCP floods, UDP floods, ICMP floods, and other spoofed packet floods. These are also called Layer 3 & 4 Attacks. Here, an attacker tries to saturate the bandwidth of the target site. The attack magnitude is measured in Bits per Second (bps).

a) **UDP Flood** − A UDP flood is used to flood random ports on a remote host with numerous UDP packets, more specifically port number 53. Specialized firewalls can be used to filter out or block malicious UDP packets.

b) **ICMP Flood** − This is similar to UDP flood and used to flood a remote host with numerous ICMP Echo Requests. This type of attack can consume both outgoing and incoming bandwidth and a high volume of ping requests will result in overall system slowdown.

c) **HTTP Flood** − The attacker sends HTTP GET and POST requests to a targeted web server in a large volume which cannot be handled by the server and leads to denial of additional connections from legitimate clients.

d) **Amplification Attack** − The attacker makes a request that generates a large response which includes DNS requests for large TXT records and HTTP GET requests for large files like images, PDFs, or any other data files.

(ii) **Protocol Attacks :** Protocol attacks include SYN floods, Ping of Death, fragmented packet attacks, Smurf DDoS, etc. This type of attack consumes actual server resources and other resources like firewalls and load balancers. The attack magnitude is measured in Packets per Second.

a) **DNS Flood** − DNS floods are used for attacking both the infrastructure and a DNS application to overwhelm a target system and consume all its available network bandwidth.

b) **SYN Flood** – The attacker sends TCP connection requests faster than the targeted machine can process them, causing network saturation. Administrators can tweak TCP stacks to mitigate the effect of SYN floods. To reduce the effect of SYN floods, you can reduce the timeout until a stack frees memory allocated to a connection, or selectively dropping incoming connections using a firewall or **iptables**.

c) **Ping of Death** – The attacker sends malformed or oversized packets using a simple ping command. IP allows sending 65,535 bytes packets but sending a ping packet larger than 65,535 bytes violates the Internet Protocol and could cause memory overflow on the target system and finally crash the system. To avoid Ping of Death attacks and its variants, many sites block ICMP ping messages altogether at their firewalls.

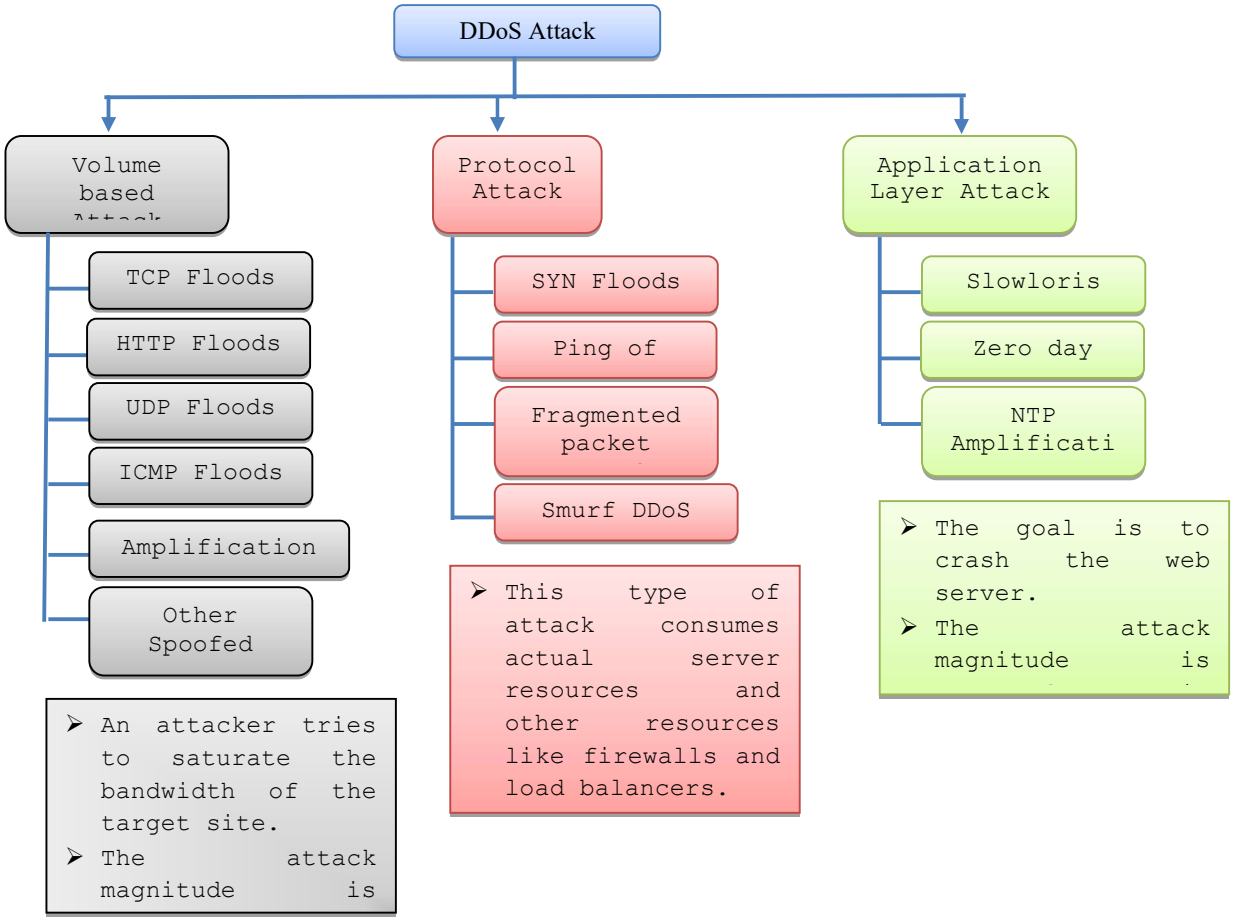

Figure 1: Types of DDoS attack

(iii) **Application Layer Attacks:** Application Layer Attacks include Slowloris, Zero-day DDoS attacks, DDoS attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Here the goal is to crash the web server. The attack magnitude is measured in Requests per Second.

a) **Application Attack** – This is also called **Layer 7 Attack**, where the attacker makes excessive log-in, database-lookup, or search requests to overload the application. It is really difficult to detect Layer 7 attacks because they resemble legitimate website traffic.

b) **Slowloris** − The attacker sends huge number of HTTP headers to a targeted web server, but never completes a request. The targeted server keeps each of these false connections open and eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.

c) **NTP Amplification** − The attacker exploits publically-accessible Network Time Protocol (NTP) servers to overwhelm the targeted server with User Datagram Protocol (UDP) traffic.

d) **Zero-day DDoS Attacks** − A zero-day vulnerability is a system or application flaw previously unknown to the vendor, and has not been fixed or patched. These are new type of attacks coming into existence day by day, for example, exploiting vulnerabilities for which no patch has yet been released.

3. Comparison of Prevention and mitigation Techniques for DDoS attacks

As discussed in the previous section that there are three major categories of DDoS attacks: Volume based attacks, Protocol attacks, and Application Layer attack. The attacker applies different strategies according to its goals of attack. As shown in the figure 1 that in case of volume based attacks, it tries to saturate the bandwidth of the target site and the attack is measured in Bits per Second. In case of protocol attack, it consumes actual server resources and other resources like firewalls and load balancers and such attacks are measured in packets per second. In case of application layer attack, the goal is to crash the web server and such attacks are measured by request per second.

Keeping in view, we have done a study on this issue of DDoS attack and presented the study that how DDoS protection options should be selected and proceed further to provide the security in a flow chart shown in figure 2.

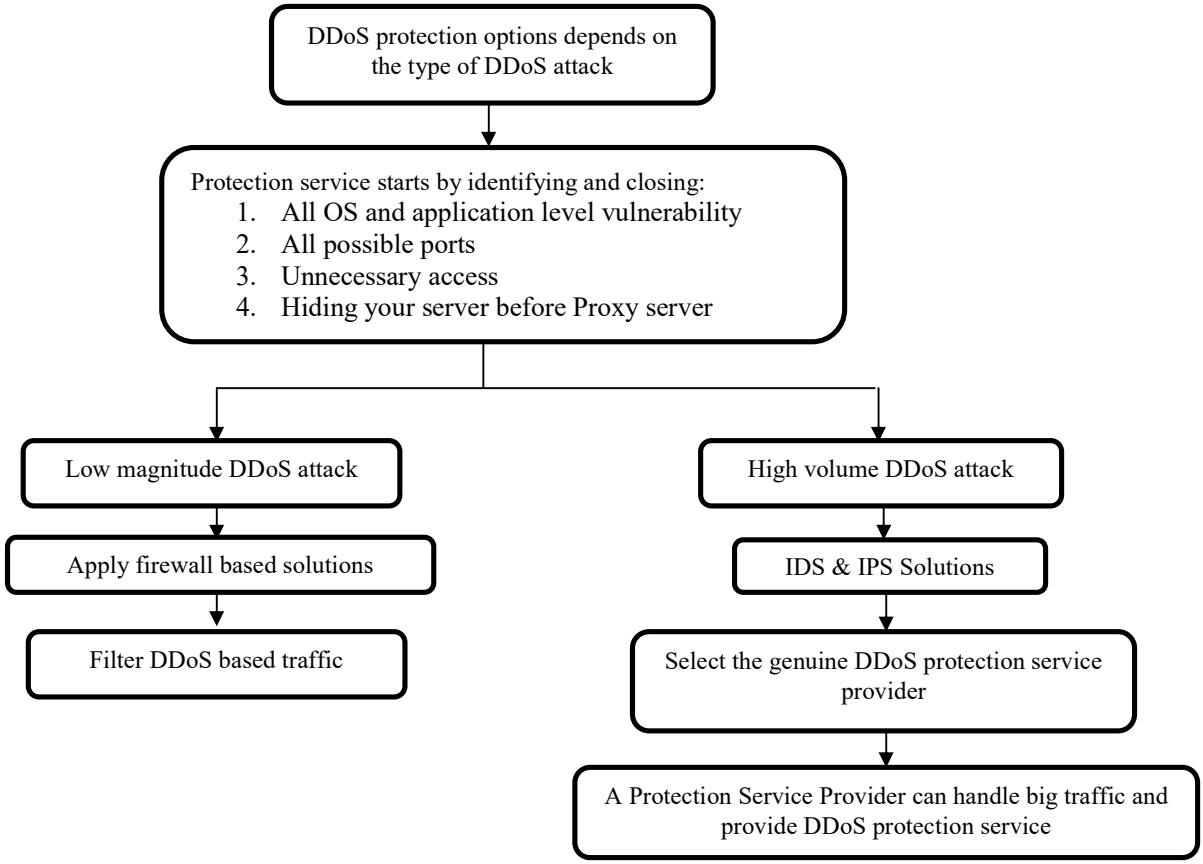

Figure 2: DDoS attack prevention process flow chart

As mentioned in the figure 2 that the selection of Intruder Detection System and Intruder Prevention System should be done on the basis of attack's type and its probability in your system/ server. Here in this paper, we are focused on the Volume based attacks that are mostly flooding attacks and proposing a model and methodology accordingly.

Comparison between different mechanisms preventing the DDoS attack is presented in table 1 below:

Table 1: Comparison between Prevention Mechanisms from DDoS Attacks

MECHANISM	WORKING APPROACH	DRAWBACKS
THROTTLING	It works by gathering the information at the router interface recorded in the making of packets, the victim can find out back the traffic of attack to attack the source. It is done at router site. It is the technique in which the attacker here communicates with the handlers, which in return hold the terminal to launch a DDoS attack.	The drawback of throttling is that it is difficult to decode or decipher the actual traffic out of malicious traffic
BLACKHOLING	Also known by name "null routing". This technique turns out all the traffic to an IP address that is not existing (invalid). This approach directs the new acceptable traffic to this IP address(non-existing), preventing the actual visitors from using that site	The drawback of Blackholing is that: -the targeted Ip address that is big enough is put offline by attackers as they actually want
SINKHOLING	In this technique or mechanism , a database is used that contains the information of malicious IP address and turn the direction of traffic coming from these IP addresses away. Basically, sinkhole is a server or we can say that a network to which malicious traffic is diverted.	The drawback of sinkholing is that it has no privilege to either prevent a malicious traffic from being executed and also can't prevent to being spread to other computers.
INGRESS/ENGRESS FILTERING	The work of ingress/egress filtering is that it permits the allowing or leaving the network by traffic only if its source address met its range expectations	It is very difficult to implement this filtering universally:-let us suppose if an attacker being very careful chooses a network without ingress/engress technique to launch a deceived DDoS attack then the attack will go undetected.it means this technique is ineffective here. It doesn't control multipath routing
PUSHBACK	Pushback is a technique used against safeguarding Ddos attack. Here Ddos attack act like congestion control problem here but as we know this congestion is caused by malicious host that does not agreed	The pushback technique is divided into two components: (1) A Local aggregate Congestion Control, and (2) A cooperative pushback mechanism. So, there is complexity in its implementation.

	upon traditional end to end congestion. Pushback technique purely works on congestion control problem.	

After discussing the prevention techniques, let us discuss and compare between most popular three DDoS attack mitigation techniques: (1) CDN (Content Delivery Network) dilution, (2) Clean Pipe, and (3) Anti-DDoS Protection Proxy. The comparison is shown below in Table 2:

Table 2: Comparison between DDoS Mitigation techniques

CDN Dilution	Clean Pipe	Anti-DDoS Protection Proxy
• It utilizes CDN in mitigating bot traffic. • It is a system of a distributed network. • It delivers pages and other web content to a user. • CDN uses a virtual server to distribute the content to the user from a location that is much closer to the user than the original server. • It uses the huge bandwidth offered by the CDN technology to mitigate and absorb DDoS attacks, especially volumetric DDoS attack. • It is context-aware. • It is an always-on solution with no lead time, making it a very comprehensive DDoS protection for web applications. • It is only applicable to web applications and not proprietary TCP/UDP allocations.	• It is the most common technique. • In this technique, all incoming traffic must pass through the "clean-pipe" centre, or also known as "scrubbing centre", where the system identifies and blocks malicious traffic, allowing only the legitimate traffic to access the server. • It is effective in handling **volumetric DDoS attacks**, but it is not very effective in handling **vulnerability based attacks**. • This technique is very versatile and can be considered as a jack of all trades, master of none DDoS mitigation techniques. • It is not an always-on solution. When an attack vector is detected, it will need some time to reroute the traffic to the scrubbing centre, which will require at least serveral minutes before the actual mitigating kick in. • Your IP prefix is not hidden, so an attacker can detect your ISP and analyse your infrastructure to find vunerability. • Due to its complexity, it might require human intervention. • It is also infamous for its difficulty to implement • You would need a BGP (Border Gateway Protocol) router and a dedicated device capable of terminating the GRE tunnel.	• It works in a similar principle to CDN. • It is also an always on solution with no lead time and can be very effective in protecting the system/ network from DDoS. • It is the best approach against slow DDoS attacks. • You can't get the real client's IP, since the source IP has changed for the backend.

4. Conclusion

From the study of prevention and mitigation techniques of DDoS attacks, it is found that among the prevention techniques, pushback technique is one of the most promising technique to defend against DDoS attacks. In this technique, a downstream router coordinates with the upstream routers to control the attack traffic leading to downstream router congestion. The pushback technique is divided into two components: (1) A local aggregate congestion control (ACC), and (2) A cooperative pushback mechanism (CPM). A local Aggregate Congestion Control (ACC) control the incoming aggregate traffic by setting up rate limits, whereas Cooperative Pushback Mechanism (CPM) supports the required cooperation between native router and its upstream routers, when the attack is severe.

For mitigating the DDoS attacks, Clean pipe is the most common technique although it is difficult to implement and not very effective in handling vulnerability-based attacks, but is very effective in handling volumetric DDoS attacks.

Acknowledgments

Security of data in every system is important and the risk of data theft is increases more when all the users are working online with their valuable data. During covid-19 pandemic, DDoS attacks are increases and hence it is an attempt to summarize all the information on such attacks. We are thankful to all the persons directly or indirectly helps us to prepare this paper.

REFERENCES

[1] *E. Alomari, B.B. Gupta, S. Kanuppayah, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art", International Journal of Computer Applications (0975 - 8887), Volume 49- No.7, July 2012, pp. 24-32*

[2] *N.Z. Bawany, J. A. Shamsi, K. Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions", Arab J Sci Eng (2017) vol. 42, pp. 425-441*

[3] *Esraa Almoari, B.B.Gupta, S. Karuppayah, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art", IJCA, Vol. 49, No. 7, July 2012, pp. 24-32.*

[4] *A. Shameli-Sendi, M. Pourzandi, M. Fekih-Ahmed, and M. Cheriet, "Taxonomy of Distributed Denial of Service mitigation approaches for cloud computing," Journal ofNetwork and Computer Applications, vol. 58, pp. 165-179,*

[5] *B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller,"A blockchain-based architecture for collaborative ddos mitigation with smart contracts," in Security of Networks and Services in an All-Connected World, D. Tuncer, R. Koch, R. Badonnel, and B. Stiller, Eds. Cham,Switzerland: Springer, 2017, pp. 16-2*

[6] *S. Behal, K. Kumar, and M. Sachdeva, "D-FACE: an anomaly based distributed approach for early detection of DDoS attacks and flash events," Journal of Network and Computer Applications, vol. 111, pp. 49-63, 2018.*

[7] *S. Hameed and U. Ali, "HADEC: hadoop-based live DDoS detection framework," EURASIP Journal on Information Security, vol. 2018, no. 1, p. 11, 2018.*

[8] *Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M.; Buyya, R. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Comput. Commun. 2017.*

[9] *Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2018). REATO: REActing TO Denial of Service attacks in the Internet of Things. Computer Networks,137, 37-48.*

[10] *Muhammad Yeasir Arafat et al.,"A Practical Approach and Mitigation Techniques on Application Layer DDoS Attack in Web Server,"International Journal of Computer Applications (0975 - 8887) Volume 131 - No.1, December 2015*

[11] *K. J. Singh and T. De, "MLP-GA based algorithm to detect application layer DDoS attack," Journal of Information Security and Applications, vol. 36, pp. 145-153, 2017.*

[12] *B. Meng, W. Andi, X. Jian, and Z. Fucai, "DDOS attack detection system based on analysis of users' behaviors for application layer," in Proceedings of IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, July 2017.*

[13] *A. Rai and R. K. Challa, "Survey on recent DDoS mitigation techniques and comparative analysis," in Proceedings of 2016 Second International Conference on Computational Intelligence & Communication Technology (CICT), pp. 96-101, Ghaziabad, India, February 2016*

[14] *Z. Mašeti?, D. Ke?o, N. Do?ru, and K. Hajdarevi?, "SYN flood attack detection in cloud computing using support vector machine," TEM J., vol. 6, no. 4, pp. 752-759, 2017*

[15] *S. Indraneel and V. Praveen Kumar Vuppala, "HTTP Flood attack Detection in Application Layer using Machine learning metrics and Bio inspired Bat algorithm," Appl. Comput. Informatics, 2017.*

[16] *Zakaria Abou el Houda , Abdelhakim Senhaji Hafid ,And Lyes Khoukhi , "Cochain-SC: An Intra- and inter Domain ddos mitigation scheme based on blockchain using SDN and smart contract:IEEE Access volume 7,2019.*