iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IV **Month of publication:** April 2020

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

A Study and Categorization of DOS Attacks in Cloud Computing Environment

Yogita Barse[1], Deepak Agrawal[2]
[1,2]*Department of Computer Science, Indore Institute of Science & Technology, Indore (M.P.)-India*

Abstract: ***Cloud computing is an emergent technology imparts on-demand accessibility of shared resources like servers, storage, databases, networking, software, analytics, and intelligence over the Internet. With a rise in Cloud Service Providers, massive Internet users are switching to Cloud platforms since it has the threat of security breach by unauthorized users. Nowadays one of the chief attacks among all which challenges the security in cloud is the DoS attacks. The availability, SLA, and performance of the cloud is targeted by the DoS attack. This review presents various DoS attacks and its classification in cloud computing environment.***

Keywords: Cloud security; DoS; DDoS; Attacks; Performance; Services; Resources

I. INTRODUCTION

Cloud Computing is an eminent technology which provides shared pool of resources over the internet. Over recent years, a swift increase is seen for large companies and private sectors. With various benefits cloud computing also suffers from the security issues like data privacy that causes the threats in cloud [1]. Cloud supports Virtualization which plays very important role in the cloud computing technology since with its assistance user share the data present in the clouds like application etc, but in reality with the help of virtualization users shares the Infrastructure. The combination of virtualization and some emergent technologies will be the future of computing.

A. Cloud Services

The cloud computing technology offer services that are categorized as follows [2]:

1) *Software as a Service (SAAS):* It is also known as "on demand software" as the providers provide the access to software application and are used for huge collection of tasks over the internet using the cloud services.
2) *Platform as a Service (PAAS):* It offers a platform for creating all the hardware and software components required to build cloud-based application delivered over the web.
3) *Infrastructure as a Service (IAAS):* It provides services such as storage, security tools, and networking to the end user like the on demand infrastructure such as virtual machines, storage drives, servers, operating systems & networks.

B. Cloud Deployment Models

The cloud computing deployment models are [3]:

1) *Private Cloud:* Systems and services are only accessible for the cloud owner.
2) *Public Cloud:* Deployed for public clients and owners of an organization that sells the cloud services
3) *Community Cloud:* Which is shared between several organizations that belongs to a same community.
4) *Hybrid Cloud:* Which is a integrated from two or more clouds that may be public, private, or community clouds.
5) *Clouds Federation:* Which is the interconnection of multiple clouds to accommodate unexpected spikes of demand.

C. Security Threats on Cloud

Since cloud is scalable to variable demands and it offers the necessary environment which varies instantly, hence cloud computing have many challenges primarily in the security area. Wrapping, flooding, side channel, malware injection, authentication, and man-in-the-middle cryptographic attack are some attacks that can be conducted against the cloud computing. One of the attack is DoS which alleviates cloud to perform its function in most capacity. Since the DoS attack results in service unavailability in cloud environment hence cloud technology needs great protection from such attacks. When the DoS attacks in a distributed manner it is known as distributed denial of service (DDoS) attack. The DDoS generally takes place when the system floods the resources or bandwidth of a targeted system which results in multiple compromised systems and intense traffic in the network.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV Apr 2020- Available at www.ijraset.com

II. DENIAL OF SERVICE (DOS) ATTACKS

DoS is the most frequent attack in cloud computing environment. Neither the user related data gets not modified nor is the unauthorized access gained but it disrupts the standard communication between the legitimate users through the huge number of requests. The DoS attacks are classified into three categories-

1) Volume based/bandwidth based
2) Protocols attack
3) Application layer attacks

The volume based or bandwidth attacks are ICMP floods and UDP floods which occur to devastate the server with junk of data sent over the network. This compromises the network performing the normal services for a period of time.

The protocol attacks are the result of protocol vulnerabilities. Ping of death, SYN flood, fragmented packet attack and Smurf attacks are some of the protocol attacks which crush the server down by achieving the defects of protocol.

In application layer attacks the flood of connection requests is sent to the victim in order to consume all the available resources and to make it out of stock for the genuine user. HTTP request attack, XML attack and Rest attack are some of the application layer attacks.

A. Distributed Denial of Service (DDoS) attacks

With the help of several transitional systems the attacker performs the DoS attack remotely to stay undetected as it can be blocked by the firewalls or intrusion detection systems of the victim location easily. On behalf of the attacker when several intermediate systems are used to compromise the victim site with DoS attack then,It is known as Distributed Denial Of Service (DDoS) attacks. The Figure 1.1 shows the overall working of DDoS attacks [4]. The DDoS attack perform the malicious activities with the help of Botnets, which are a collection of several compromised hosts by the attacker .A command and control (C&C) server is used by the attacker to send its orders. These systems coordinate and trigger a botnet [5]. The orders involve the launching of DDoS attack against a victim through attack packets from the botnet.

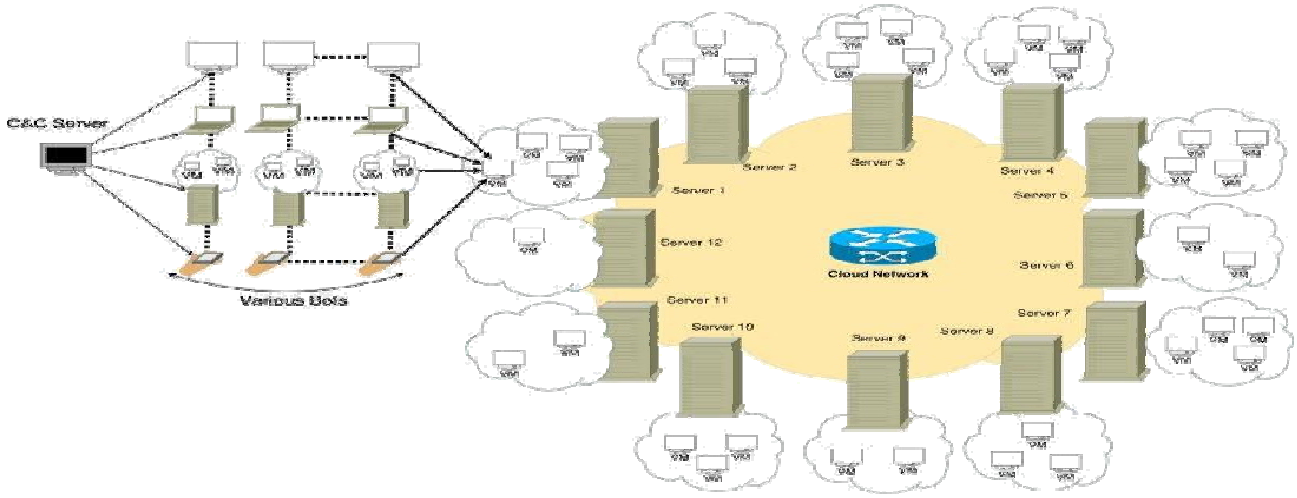


Fig1. Botnet attack in cloud environment

III. DOS AND DDOS STUDY

Based on a survey report of Prolexic's Q1 2013 Global DDoS Attack, the attacks are directed to infrastructure (Layer 3 and 4), against bandwidth capacity and routing infrastructure which is above 75% and the left attacks are on the application layer [6]. There are many security challenges exist in cloud computing some of the issues are-

1) Identity
2) Authentication
3) Authorization
4) Confidentiality
5) Integrity
6) Isolation
7) Availability

Similarly each layer has some vulnerability for the DoS and DDoS attacks. Ever since Infrastructure layer and application layer are frequently suffer from these attacks. In Infrastructure layer the network bandwidth and routing of information is overwhelmed by the attack through huge forged requests. In application attack, the limitations of some specific applications are exploited which causes performance degradation, service unavailability's and which results in crashing of the remote servers.

A. Overwhelm the Resources

1) Exhausting Memory: These attacks could use the vulnerabilities of networking devices and protocols the example of such attack is SYN (Synchronize) flood attacks which can be prevented by proxy applications. In the survey the authors presented a discussion on the recent most popular DDoS attack (DNS Reflection attacks, SYN floods, UDP floods, ICMP floods and HTTP Flood Attacks) types in the Infrastructure and Application layers. They have also discussed the effective cloud based mitigation and protection techniques [7,8] .The Principle of SYN flooding attack is to initiate a TCP connection with a three way handshake. The client system commenced it by sending SYN message to the server and the SYN-ACK message is sent to the client for acknowledgement. In return the client acknowledges the server with an ACK message. Afterwards the connection is open between the client and server for communication. When the server system acknowledges the SYN ACK back to the client but yet not receives the ACK message from the client, at this point the possibility of maltreatment is raised [8]. A transmission control block (TCB) holds the connection information is allocated and only half open prior to ACK message is received from the client and later than the SYN packet has been received by the servers. Through these incoming SYNs the servers kernel memory being exhausted and results in the establishment of too many TCB allocations. To circumvent the memory exhaustion with a listening socket the operating system uses a backlog parameter but the main goal of the SYN flood is to exhaust all these backlogs through sending SYN segments to seal the entire backlog resulting in the denial of services to the new connection requests [7].

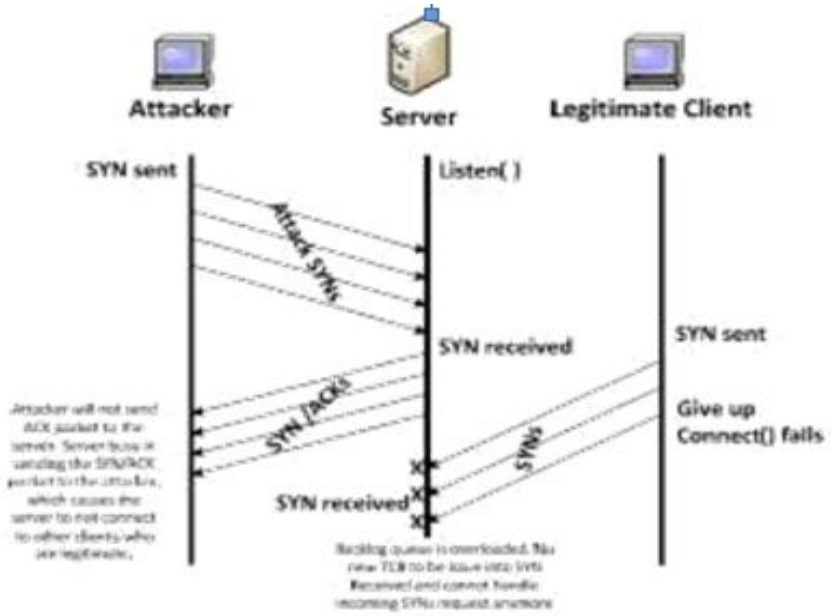


Fig.2 TCP SYN Flooding attack [7]

To overcome with these attacks the author presented a framework on monitoring the flow of SYN packets by using a correlation engine or a flow traffic tool like snort, wireshark, along with detection and prevention stages. This framework supports to construct a tough design for security as well as reliable cloud services in the field of cloud computing [9].

B. Exhausting Computing time and Bandwidth

These attacks steals the computing bandwidth and time computing from the other users and results in the process cycle wastes. The author identified the DoS attacks by monitoring the usage of computing resources of a cloud with the help of two test scenarios in an open cloud. CPU and memory usage, rate of incoming and outgoing bytes in each network interface, number of disks read and write requests.The results reveals that with the help of k-Nearest Neighbors (kNN) and decision tree (CART) DoS can be recognized accurately [10]

C. HTTP-DoS and XML-DoS

In the applicatoion layer the DoS targets definite services with a web flood, In an effort to overwhelm the server resources, these web floods sent with high rates of genuine application layer requests to a server. Though the flood consist of legitimate requests to the victim server, this attack is less likely to be identified.

According to Prolexic's Q1 2013 Global DDoS Attack Report, in application (layer 7) attacks 23.46% of the Total DDOS attacks appeared, and 19.33 % attacks appeared in the form of HTTP GET floods of the total DDOS attacks [6]. Therefore the DDoS attacks approaches in two manners, HTTP GET flood and HTTP POST Flood, attackers to POST huge amounts of data to applications. HTTP floods can be initiated with three types [11]

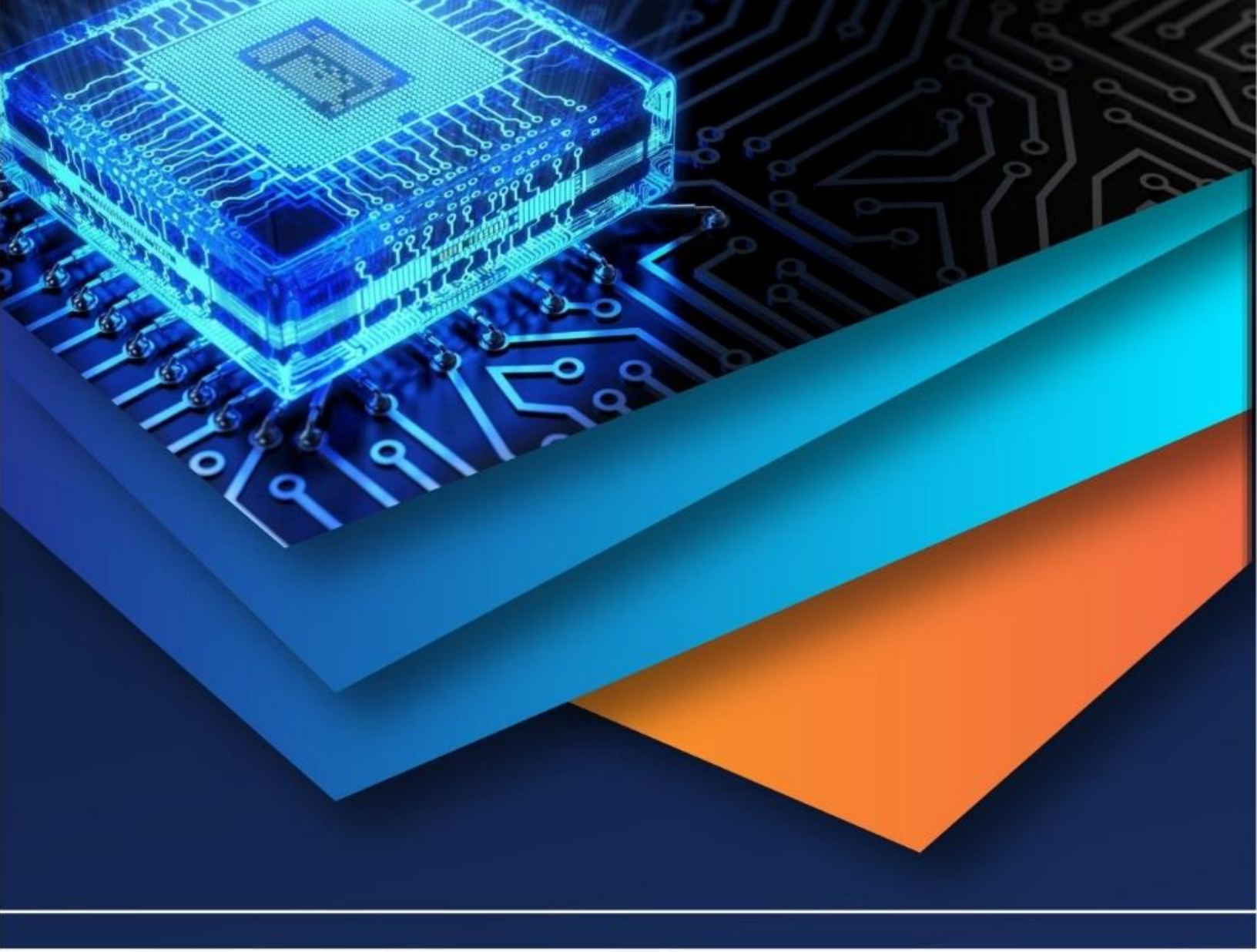
1) *HTTP Malformed Attacks:* These attacks target the web server resources by exhausting them by sending invalid HTTP packets. Zafi.B worm is the example of this attack that uses malformed HTTP GET Requests.
2) *HTTP Request Attacks:* Various legitimate HTTP requests (Both Get and Post) are sent to web servers to exhaust the server resources by flooding them.
3) *HTTP Idle Attacks:* This attack takes place when a HTTP open connection gone idle without sending a complete HTTP request by an attack. Slowloris is the HTTP idle attack which never manages to complete the request due to drooling of small number of byes per packet to keep the connection from time out.

IV. CONCLUSION

Nowadays the security of cloud is the major obstruction among various organizations which results in preventing the adoption of cloud technology. DoS attack is one of the serious threat for cloud computing environment as it targets the resources and services provided to the user and make it unavailable. Since the study of recent and most popular DDoS and DoS attack types are presented in this survey. A complete analysis and a discussion on recent popular DDoS attack types on cloud environment are followed. Some techniques that have been proposed by various researchers are also discussed extensively. With this survey a directional guidance towards DDoS defense would be achieve.

REFERENCES

[1] Goyal S, Mathew R: Security Issues in Cloud Computing, International conference on Computer Networks, Big data and IoT,ICCBI 2019: Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2019) pp 363-373
[2] Udendhran R. New framework to detect and prevent denial-of-service attack in cloud computing environment. Asian Journal of Computer Science and Information Technology 2014; 4(12): 87–91.
[3] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems 2012; 28(3): 583–592.
[4] Somani G ,Manoj SinghGaurbDheerajSanghicMauroContidRajkumarBuyyae DDoS attacks in cloud computing: Issues, taxonomy, and future directions, Computer Communications,Elsevier,Volume 107, 15 July 2017, Pages 30-48
[5] Yu S. Distributed Denial of Service Attack and Defence. Springer: London, UK, 2014.
[6] Prolexic Technologies, "Prolexic Quarterly Global DDoS Attack Report Q1 2013," Florida2013.
[7] Wong F and Tan C, A survey of trends in massive dDoS attacks and cloud-based mitigations, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014,Pages 57-71
[8] T. Peng, C. Leckie, And K. Ramamohanarao, "Survey Of Network-Based Defense Mechanisms Countering The DoS And DDoS Problems," Acm Comput. Surv., Vol. 39, P. 3, 2007
[9] Udendhran, R. New Framework to Detect and Prevent Denial of Service Attack in CloudComputing Environment.Asian Journal of Computer Science and Information Technology, [S.l.], v. 4, n. 12, p.87-91, dec. 2014. ISSN 2249-5126.
[10] João H. G. M. Corrêa,On Machine Learning DoS Attack Identification from Cloud Computing Telemetry,LANCOMM'19, May 7, 2019, Gramado, Brazil, arXiv:1904.06211v1 [cs.CR] 11 Apr 2019
[11] Arbor Networks, "The Growing Threat Of Application-Layer DDoS Attacks," 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY