A SURVEY ON COMPREHENSIVE TAXONOMY OF DDOS ATTACK IN CLOUD ENVIRONMENT

R.Saravana Prabhu[1], A.Prema[2]

[1] **Research Scholar,** Department of Computer Science,
Alagappa University, Karaikudi, Tamil Nadu, India

[2]**Assistant Professor,** PG & Research Department of Computer Science,
Sri Meenakshi Government Arts College for Women, Madurai, Tamil Nadu, India.

Abstract:

The Distributed Denial of Service (DDoS) is the crucial attack in cloud computing environment which brings more concentration to cloud users in the past score. The DDoS attack occurred, the memory resources are overloaded with higher usage and lead to the denial of necessary service for appropriate users forcefully. By regulating the resource utilization of the system, the DDoS attacks can be mitigated by which the user's request and the resources can be actually handled and further solubilizing of established connection of the attacker.

I Introduction

DDoS attacks are specially coded to drain the resources like memory, CPU refining, and network frequency, making them inaccessible to the customers by denying access to services**.**

Cloud computing is a new technology, which concentrate on providing virtualized resources
for its clients. It is novel system architecture, and also a current new computing technologies era. Cloud computing services are pay per usage, on demand access, Virtualization, scalability, flexibility with minimal hardware and also maintenance cost. Cloud service are classified with

1. Infrastructure as a Service (IaaS) or Hardware as a service (HaaS)

It allows clients to outsource their computing infrastructures such as servers, processing elements, networking services, storages, virtual computing machines, and some other resources. Clients or tenants can access these resources on using a pay-as-per use model via internet.

2. Platform as a Service (PaaS)

It provides a runtime environment for users. It allows the programmers to create, compile or tests, run are deploy web applications and also it works with back end scalability. It is maintain by the cloud service provider, end users no not need to worry about maintaining the hardware and platform services.

PaaS also provides the Programming languages, Application softaware frameworks, Databases, and Other software related tools.

3. Software as a Service (SaaS)

Users accede to an application rather than acquiring it once and installing it. Users can log into SaaS application from any compatible supported device over the Internet. The real application runs in the cloud servers that may be far from a user's location.

The most important cloud computing models are as follows

- Private cloud: This service is only for the cloud owner for private use only.
- Public cloud: A public cloud is another type of computing in which a service provider gives a resource to the public through the internet
- Community cloud: This service is shared between several organizations commonly used for people.
- Hybrid cloud: In this service where the applications are run in different combination of clouds that may be private, public or community clouds.

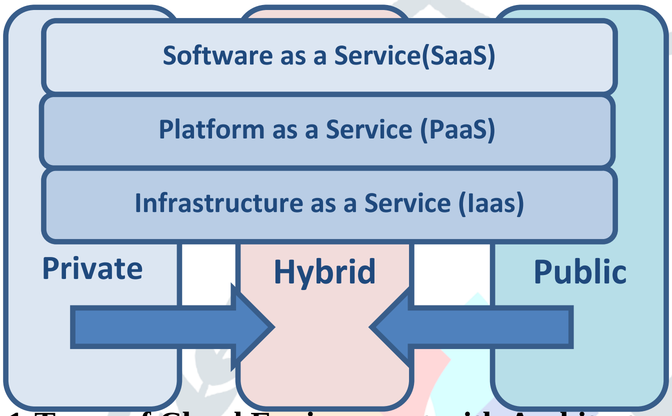

Software as a Service(SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (Iaas)
Private
Hybrid
Public

Figure 1:Types of Cloud Environment with Architecture

II Methodology

A set of literature surveys conducting a comprehensive pursuit on previous research papers and surveys and collecting a number of research papers related to the research topic. This study results from the recent research papers. In this research contributions contained in this survey are comprehensive and it includes a list of important contributions in the field up to date. In this research paper contains cloud security problems and security mechanisms focus on eradicating and highlighting them.in spite of the need to reinforce the existing security measures to provide more security in the cloud environment.

III Literature Survey

The research study on Distributed Denial of Service attack (DDoS) detection and prevention on cloud computing environment, it includes an elucidation called Cloud Trace (CT).
Cloud Trace is a distributed tracing system that it collects a delay before a transfer of data begins from your applications and displays.

Chonka et al., (2011) To detect the source of the HTTP and XML DoS attack. The researchers also introduced a Cloud Protector (CP) that uses a back propagation to detect and handle the attack.

Yu et al. (2014) gave a new technique in the form of Dynamic Resource Allocation (DSA) strategy for DDoS attack in the cloud. The authors utilized the idle cloud resources and give a solution to intrusion prevention servers for achieving speedy in filtering technique to control DoS attack.

Girma et al., (2015) analysed the current scenario of DDoS attack detection method with different parameters along with the list of advantages and disadvantages of each model. The authors also proposed a new hybrid statistical model that effectively mitigates the DDoS attacks.

Osanaiyeet al. (2015) finds and detected the DDoS attacks by analysing the characteristics of protocol TCP/IP packet headers that contain the source of the IP address in the data packet.

Liu et al., (2016) proposed a new method that takes the Frequency Domain Characteristics (FDC) from the auto correlation structure arrangement of the network data flow as a clustering feature and uses the BIRTH algorithm to find the abnormal network flow traffic.

Kim et al., (2006) proposed the Packet Score scheme (PSS) which uses the Bayesian formula to calculate the data packets. If it computed score of data is lower than the fixed given threshold, then the packet is identified as a vulnerable attacker's data packet. However, as the threshold is analysed and fixed that does not consider the intensity of the given volume of data, it is not suitable for handling a very large traffic in a cloud environments DDoS attacks. This novel idea is a base; for several researchers proposed a several new methods of detecting and preventing methods of DDoS attacks in the cloud environments.

Dou et al.,(2013) proposed a new filtering technique Confidence Based Filtering(CBF) method that groups a data for determining the authenticity of the data source.

Shamsolmo ali et al., (2014) presented a new model of using data mining and neural network techniques to identify and detect the DDoS attack. This model helps particularly to detect the TCP attacks.

Sahi et al. (2017) suggested a new defence model that detects DDoS flooding attacks by isolating data into several groups and establishing a blacklist to store the source IP address of vulnerable attack packets.

Jeyanthi et al. (2013) proposed a Deception Detection algorithm (DDA) for the detection of a large network traffic DDoS attack launched on a cloud server environment.

Navaz et al (2013) combined an entropy based new technique with anomaly detection systems to afford multilevel detection methods to detect a hidden small size of network traffic in DDoS attacks. In this method provides a good result for the DDoS attacks with large network traffic attack in the cloud environment, but the time taken to complete the task is slow.

Wang et al (2015) proposed a new DDoS attack mitigation architecture that can detects attack very fast. The author also suggested that the Software-Defined Networking (SDN) technology helps to defend against DDoS attacks. This framework was suggested to detect and mitigate the DDoS attack.

Saravanan et al., (2019). It makes very fast screening tests to prevent the cloud server from attacks and it uses a various controls to detect the attacks. It uses the two queues to mitigate the attacks. An algorithm that is based on the aggregate-based congestion control that can be deployed in routers that prevent from network bandwidth congestion attacks and resource consumption attacks. This technique was proposed by (Wang, 2008). Similarly, another model that detects and prevents the flooding DDoS attacks using distance based measures applied on Time to live (TTL) values specified in the data packets, it was suggested by Chapade et al.,(2013).

Kalliola et al. (2015) presented a new cloud architecture that combines a normal traffic, external blacklist of IP addresses, and flexible capacity that calls an automated defence against DDoS attacks, but it is very difficult to detect a minimum volume of flooding DDoS attack.

From afore said analysis made from the literature, few of the methods are not suggestable for handling a large traffic in a cloud environment. Some other methods are finding difficult to handle low rate DDoS attack with minimum traffic. Some few methods produce good result for both minimum and maximum rate of traffic; the time taken to complete the process is very slow.

IV Attack

In Cloud computing denial of service can be compromised in three ways: (1) the attack can come from the outside and the target system to be inside (external system to internal system), (2) It can even emanate from within the system (Internal system to internal system) and (3)It can even occur from within to target system the outside of the cloud environment [4]

(1)External to internal: In this case, the botnet is used to perform the attack comes from outside the target system. The attack can target the internet gateway of the Cloud infrastructure, or the Cloud servers. If a particular client system becomes the victim of an attack, it will also affect the other Virtual Machines working in the same Cloud environment.

(2) Internal to external: In this case, the attack begins by capturing the ownership of a Virtual machine running in the Cloud environment. The choice of which clients Virtual Machine to infect the client owns a number of Virtual Machines, spread over all other Virtual Machines, therefore making a botnet. The large computing power and resource availability of the Cloud computing environment becomes a factual threat from the external target.

(3) Internal to internal: In this case an internal botnet is formed and attack can be another target inside the system (such as a Virtual Machine or a cluster of Virtual Machine). All type of Cloud infrastructures may disrupt under these kinds of DDoS attacks.

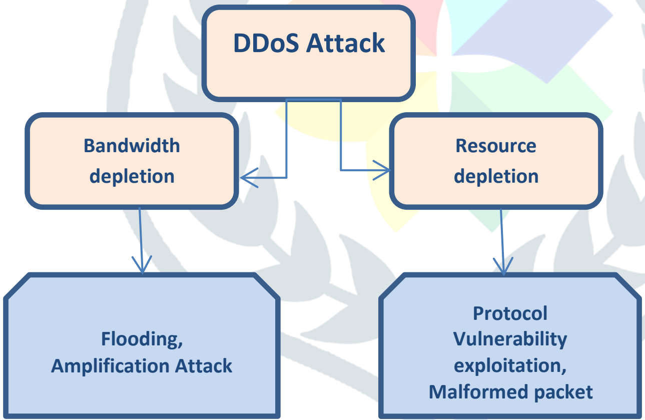

DDoS Attack
Bandwidth depletion
Resource depletion
Flooding, Amplification Attack
Protocol Vulnerability exploitation, Malformed packet

Figure 2: Taxonomy of DDoS attack

V DDoS Detective Controls

DDoS attack prevent is hard, however, it's possible to detect and recovering controls. There are some of the controls of DDoS attack.

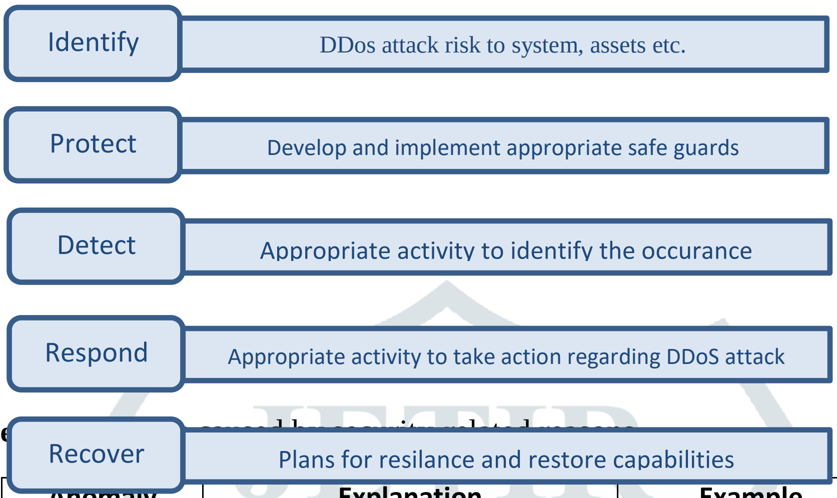
(1) Bot-Cloud Detection is the cloud infrastructure could be used for installing bots or developing botnets. This type of clouds is known as Bot-Clouds. The detection of any other bots are running inside Virtual Machines within the cloud potency need the support of the Cloud Service Provider(CSP) this model will be able to only prevent attacks at its origins. [1]

(2) Signature Based Detection:This technique is also termed as misuse detection. This type of method scans several exploit patterns or signatures of the exploits. If whether the result is in similar pattern, then it is marked as an attack. It is commonly accepted by many researchers that misuse detection is not an efficient against DDoS attacks.[2]

(3) Anomaly based detection is slightly deviate from the normal expected behaviour and are suspected from a security perspective. Anomalies are categorized in two ways: (1) performance related and (2) security related.[3]

List of six categories an anomalies caused by security-related reasons may be at one of below

Table 2. Anomalies caused by Performance-related reasons[5]



Identify — DDos attack risk to system, assets etc.

Protect — Develop and implement appropriate safe guards

Detect — Appropriate activity to identify the occurance

Respond — Appropriate activity to take action regarding DDoS attack

Recover — Plans for resilance and restore capabilities

Table caused by security related reasons

Anomaly	Explanation	Example
Infection	Distributing malicious code through the network	Worms and Viruses
Explosion	Overflowing systems with bugs	Buffer overflow
Probe	Gathering information about targets	NMAP scan
Cheating	Identity impersonation	MAC spoofing
Traverse	Try every possible key	Brute force attacks
Concurrency	Multiple connections	DDoS attacks

VI. Conclusion

The DDoS attack is one of the most vulnerable and high redundant attack in the Cloud Computing environment where it has different types that attack in the different cloud computing resources. The Distributed resources and the multiple virtual platforms inside these distributed resources are the most common vulnerability in the cloud computing services. In this paper the different kinds of the DDoS attacks that targeted the collection of resources in the cloud computing and give the different defending procedures that is used to identify, protect, detect, respond and recover the tracks of the DDoS attack and its destruction. This destruction may cause to stop the cloud service and may to losing the data stored in the cloud without any backup or reproduction. The main objective to protect the cloud is to define a policy for using the cloud resources and make new rules based on the statistics threshold of the earlier use of that service.

References

[1]. Future Directions. DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions. 2017.

[2] IEEE Systems Journal. Filtering-Based Defense Mechanisms Against DDoS Attacks : A Survey. pages 1–13, 2016

[3] Dhruba Kumar Bhattacharyya and Jugal Kumar Kalita. DDoS Attacks. 2016

[4] Latanicki, J.;Massonet, P.; Naqvi, S.; Rochwerger, B.; Villari,M. Scalable Cloud Defenses for Detection, Analysis andMitigation of DDoS Attacks. In Towards the Future Internet; IOS Press: Amsterdam, The Netherlands, 2010;pp. 127–137.

[5] https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[6] B S Kiruthika Devi and T Subbulakshmi. A Comparative Analysis of Security Methods for DDoS Attacks in the Cloud Computing Environment. Indian Journal of Science and Technology, 9(September):1–7, 2016

[7] R. Divyasree and K. Selvamani. Defeating the Distributed Denial of Service Attack in Cloud Environment : A Survey. 2017.

[8] Sanchika Gupta, Susmita Horrow, and Anjali Sardana. A Hybrid Intrusion Detection Architecture for Defense against DDoS Attacks in Cloud Environment. pages 498–499, 2012

[9] Adrien Bonguet † and Martine Bellaiche “A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing” Future Internet 2017, 9, 43; doi:10.3390/fi9030043 www.mdpi.com/journal/futureinternet.

[10] Somasundaram, Dr. V. S. Meenakshi “ DDOS Mitigation In Cloud Computing Environment By Dynamic Resource Scaling With Elastic Load Balancing” *Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 3346- 3362*

[11]Nagaraju kilari, Dr. R. Sridaran “An Overview of DDoS Attacks in Cloud Environment” International Journal of Advanced Networking Applications (IJANA) ISSN No. : 0975-0290

[12]Mohammad Masdari* and Marzie Jalali “A survey and taxonomy of DoS attacks in cloud Computing” SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks (2016) Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1539

[13] Rashmi V. Deshmukh, Kailas K. Devadkar “Understanding DDoS Attack & Its Effect In Cloud Environment” 1877-0509 © 2015 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license