REVIEW OF DISTRIBUTED DENIAL OF SERVICE ATTACK ON THE CLOUD ENVIRONMENT

Rohit Goyal, Gourav Patil, Milind Gupta, Arpit raj, Payal Kaur

Students of Ajeenkya DY Patil University, Pune, India

Abstract: - The number of users on the cloud is increasing day by day as the cloud ensures availability securing of data services and resources. DDoS(Distributed denial of services) attacks are the second most commonly cybercrime. This attack can drain the cloud resources, consumes most of its bandwidth and damage the entire cloud services within a short period of time. There are many procedure which can be approved to ease the DDos attack such as classification, encryptions techniques. In this paper, we describe the attack perform in the cloud environment.

Keywords:- Cloud computing, DDos, cloud security

INTRODUCTION

Distributed denial of service attack is a derived class of Denial of service attack which is an attempt to maliciously disrupt the normal traffic of a targeted server, services or network by overflowing the target with the flood of internet traffic. It compromises multiple computer systems as sources of attack traffic. It aims to make our website and server unavailable to legitimate users rather than attempting to breach our security perimeter. So many companies use the virtual data Center and cloud services, so it becomes the main target of D-Dos attack and cloud is accessible through the internet by which is subject to the distributed denial of service attack. With the help, od D-Dos attack attackers make the target server.

As in today's world, cloud computing is emerging to multiple users, so is the security of data being a challenging issue. Cloud computing offers users on-demand service of resources such as a server, network, storage, etc. Also as mentioned in an electronic cybercrime study published by KPMG in collaboration with e-crime congress in 2009, most of the cloud virtual clients are under threats and these threats increases as time pass.

The main idea of a Dos attack is making the service unavailable.it can be done if the performance on the machine can be brought down. Some of the DDoS attacks are as follows

1. **Ping of death**: - there is a fact in the TCP/IP model which states that the maximum size of packets can be 65535 bytes. And this fact is exploited by the ping of death attack. In this type of attack, the packets are more in size of the packet when the packet fragments are added up and the computer does not know generally what to do. so it ends up freezing or crashes the system entirely.

2**. Reflected attack**:- Botnet plays a major role in this type of attack. In this, the attacker sends the hosts of innocent computers a connection request using the botnet(also called reflectors). Now connection comes from the botnet looks like the connection is coming from the victim and this is done by spoofing. this makes the host system set an acknowledge to the victim computer. since there are multiple requests from the different system on the same machine then this overload the computer and crashes it.

3. **Mail bomb**:- In this type of attack mail servers are made targeted generally. In which the random oversized emails filled with garbage values are sent by the attacker to the targeted email server. This made a sudden load on email servers and crashes the email server.

4. **Teardrop attack**:- In this attack, the fragmented packets are sent to the target system and the system receiving such packets cannot reassemble them because of the bug due to which the packets overlap with others which results in the crashing of the target system.

Dos attack in the cloud environment

Cloud computing has been greatly improved in both pieces of research as well as in industry technology. DDoS is one of the security threats that challenge the availability. Cloud Security Alliance says that DDoS is the ninth threat to the cloud computing environment. 14% of attacks are DoS attacks out of many attacks on the cloud. Many websites like yahoo have been affected by DDoS before 2000. In May 2001, The website of grc.com was hit by huge DDoS. The company was hooked on the internet for their production work and business was greatly squeezed. VeriSign gave the contract to Forrester consulter in March 2009 to perform a study on DDoS threats and protection.

The study of DDoS attacks in the cloud says that the use of cloud is directly proportional to the DDoS attack which means as the use of cloud increases the rate of DDoS attacks will also raise at a fast hop. In the Cloud environment when the workload increases on a service, it will start providing computational power to withstand the additional load. This means Cloud system works against the attacker, but to some extent it supports the attacker by enabling him to do the most possible damage on availability of service, starting from a single attack entry point. Cloud service consists of other services provided on the same hardware servers, which may suffer by workload caused by flooding. Thus, if a service tries to run on the same server with another flooded service, this can affect its own availability. Another effect of flooding is raising the bills for Cloud usage drastically. The problem is that there is no "upper limit" to the usage 12. And one of the potential attacks on the cloud environment is neighbor attacks i.e. VM can attack its neighbor in the same physical infrastructures and thus prevent it from providing its services. These attacks can affect cloud performance and can cause financial losses and can cause harmful effects on other servers in the same cloud infrastructure.

Working of D-Dos attack

In the D-Dos attack, the attacker gains control over the network to which multiple computers are connected and infects them with malware. Turning each system as bot then remotely controlling the group of bots known as a botnet. After the establishment of bots, the attacker directs the machines by sending updated instructions. When the IP address of a victim is targeted by the botnet, each bot will respond by sending requests to the target, which causes the targeted server or network to overflow requests, resulting in a denial of service to the normal traffic.

MAIN MOTIVE OF DDOS ATTACK

1. **Hacktivism:-** Hacktivists use DDos attack to express criticism of everything from the politicians, government and the current events. They put up some demands over them and If they disagree then they can shut your site down. Anonymous is one of the best hacktivism group. They are the only responsible group for the cyberattack that held in February 2015 against ISIS

2. **Cyber vandalism:-** Cyber vandalism is often done by teenagers to show their anger, frustration against an institute or person. Cyber vandals block the site or server of a specific institution to show their anger with respect to their personal priorities.

3.**Extortion:-** The main motivation for DDoS attacks is extortion, which means a cybercriminal demands money in exchange for stopping the DDoS attack, this is the main reason for which the cybercriminal is practicing it. Many online software companies such as Meetup, BITLY, Vimeo, Basecamp have been receiving DDoS extortion notes.

4. **Personal rivalry**:- These attacks are often performed to settle personal scores or to dispute online competitions. These attacks happen in the context of multiplayer online games, where the player performs DDos on one another, and on the gaming servers too.

5. **Business competition:-** Nowadays DDos has been used as a competitive business tool. Some launch these assaults to keep the competitor away from participating in a specific event while others are launched in priority to shut down the competitor online business for the month.

CLASSIFICATION OF DDOS ATTACKS:

The below section explain the classification of DDoS attacks as per the degree of automation, attack rate dynamics, vulnerabilities exploited and impact of an attack.

1. **As per Degree of Automation**:- In this attacks the attacker scanning the network, IP addresses, machines for vulnerabilities, and deploy code and executes malicious payload for remote control access of that user system which is kept ready to launch an attack on the attacker's command.semi-automatic attacks involve deploying attack scripts that scan and compromise the user machines and download a payload and installing the codes. these victim's systems are bots under control of the handlers who choose when and how about the target victims and type of attacks. Automatic attacks, on the other hand, are carried with a high degree of automation, with the compromised user systems having the attacking code and software with the predetermined type of attack, duration, victims IP address. The attacker has minimal interaction once the payload gets deployed or during the automatic attack.

2. **As per the exploitation of vulnerabilities:-** Bandwidth Depletion attacks involve flooding and amplification clogging the WAN pipes with attack network packets. Flooding involves zombies and bots sending huge volumes of traffic to clog and congest the targets bandwidth pipes. The response from the victim slows down with the increase in such flood request, saturating the Amplification attacks involve the zombies and bots sending messages to targets by broadcast. Resource depletion attacks involve the use of malformed data packets having incorrect IP packets being sent by the zombies with the malicious intent to crash it and protocol exploits which involve exploitation of a specific protocol feature to have the victim consume resources and ultimately make it unavailable.

3. **As per attack Rate Dynamics:-** Continuous and variable rate DDoS attacks are the most common. Continuous rate attacks are executed without break or lowering the force of an attack. This leads to the disruptions in services quickly however, this attack gets detected as well. Variable-rate attacks vary the attack frequency and force, carefully avoiding detection which rangers from having the attack increase in force or have a fluctuating rate of attack.

4. **As per the impact of attacks:-** Disruptive and degrading are two common types of attack.while the impact of disruptive attacks is complete shutdown and leads to a full denial of services to legitimate clients. Degrading attacks consume the victim resource bit by bit in small portions. This is much smaller than other attacks, making the attack difficult to attack.

Note: - FOR INFRASTRUCTURE LEVEL DIRECT NETWORK LAYER ATTACKS: For TCP flood attacks where transmission control protocol having a three-way handshake before establishing actual packet exchanges with connection-oriented protocol features. Each SYN message sent by a connecting host has acknowledged with SYN +ACK and the handshaking process completes with ACK, finally establishing a connection between two hosts. Attackers exploited the three-way handshake feature by initiating connections that were half-open leading to the huge number of transmission block allocations exhausting the kernel memory {wong and tan 2014}. Zargar et al. (2013) reached on network and transport layer protocols to flood a host using TCP SYN, UDP and ICMP floods.

FOR INFRASTRUCTURE LEVEL DIRECT APPLICATION LAYER ATTACKS: HTTP flood attacks on this layer target cloud services by sending web packets to target web application server using HTTP packets.WONG and TA0N reported one-third of the global DDoS attacks to target this layer while one-fourth is HTTP attacks.

Detection of DDoS attacks

a) DDOS attacks

DDOS can be performed in two different ways

1. Directly
2. Indirectly

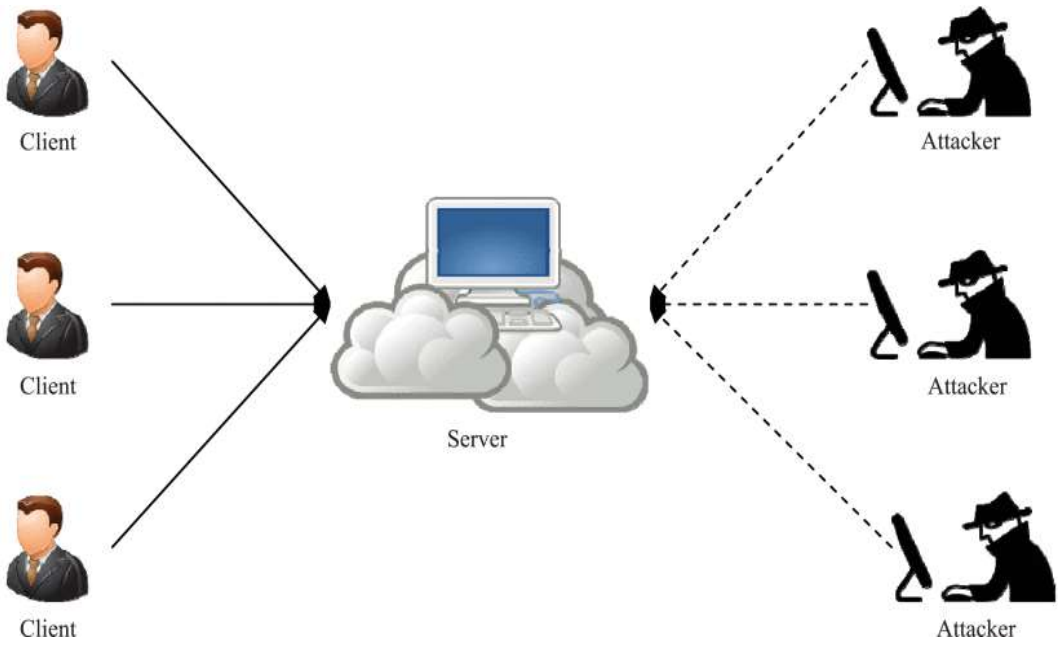
1. **Direct attack**:- In this the attacker directly attacks the weakness of the victim machines

2. **Indirect attack**:- In this, the attacker does not target the victim machine directly, they prey on other elements with which the victim machines are associated and create trouble in their work. DDOS attacks take place using the software on a virtual cloud environment, Wireshark advanced IP scanner, etc was used to capture and trace traffic both before and during the attack.

Firstly, using TCP Ping, we sent 50 TCP test probes (pings) to a server (server machine 10.25.129.5:80). The reply took 1.3 ms on average, as shown below:

- Ping statistics for 10.25.129.5:80
- 50 probes sent.
- Approximate trip times in milliseconds:
- Minimum = 0.25 ms, Maximum = 26.065 ms,

- Average = 1.323 ms



The TCP protocol uses different flags to manage the state of a connection in a packet header mainly the two flags are used to establish TCP connection

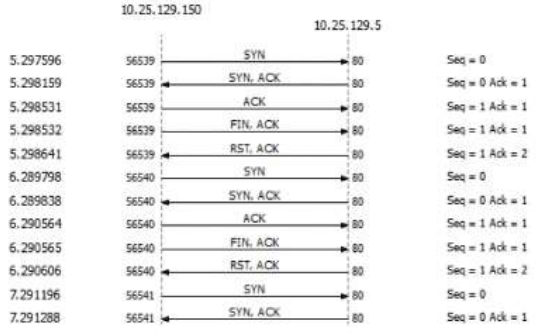
- SYN (Synchronize) which represents the initiation of a connection; and
- ACK (Acknowledge) which represents data received.

We monitored the traffic of the 50 probes at the server machine using Wireshark, by capturing the packets that were associated with the server using the filter "ip.address = = 10.25.129.5". As the traffic was normal, the server machine replied to all requested packets according to the TCP protocol, as shown in Figure 2 (a and b).

ip.addr == 10.25.129.5 Expression... + Apply this filt

No.	Time	Source	Destination	Protocol	Length	Info
275	36.355443	10.25.129.5	10.25.129.150	TCP	66	80 → 56570 [SYN, ACK] Seq=0 Ac…
276	36.355652	10.25.129.150	10.25.129.5	TCP	60	56570 → 80 [ACK] Seq=1 Ack=1 W…
277	36.355653	10.25.129.150	10.25.129.5	TCP	60	56570 → 80 [FIN, ACK] Seq=1 Ac…
278	36.355699	10.25.129.5	10.25.129.150	TCP	54	80 → 56570 [RST, ACK] Seq=1 Ac…
279	37.356926	10.25.129.150	10.25.129.5	TCP	66	56571 → 80 [SYN] Seq=0 Win=819…
280	37.357022	10.25.129.5	10.25.129.150	TCP	66	80 → 56571 [SYN, ACK] Seq=0 Ac…
281	37.357418	10.25.129.150	10.25.129.5	TCP	60	56571 → 80 [ACK] Seq=1 Ack=1 W…
282	37.357419	10.25.129.150	10.25.129.5	TCP	60	56571 → 80 [FIN, ACK] Seq=1 Ac…
283	37.357525	10.25.129.5	10.25.129.150	TCP	54	80 → 56571 [RST, ACK] Seq=1 Ac…
287	38.359532	10.25.129.150	10.25.129.5	TCP	66	56572 → 80 [SYN] Seq=0 Win=819…
288	38.359629	10.25.129.5	10.25.129.150	TCP	66	80 → 56572 [SYN, ACK] Seq=0 Ac…
289	38.360030	10.25.129.150	10.25.129.5	TCP	60	56572 → 80 [ACK] Seq=1 Ack=1 W…
290	38.360031	10.25.129.150	10.25.129.5	TCP	60	56572 → 80 [FIN, ACK] Seq=1 Ac…
291	38.360137	10.25.129.5	10.25.129.150	TCP	54	80 → 56572 [RST, ACK] Seq=1 Ac…

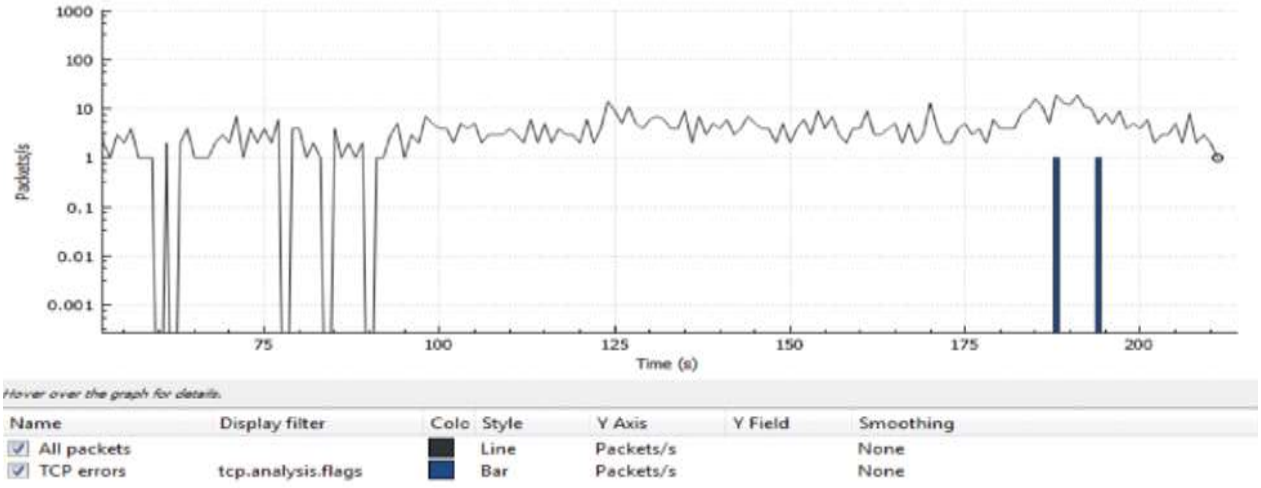
(a)



(b)

Captured packets and TCP flags (normal). (a) Captured packets (b) TCP flags.

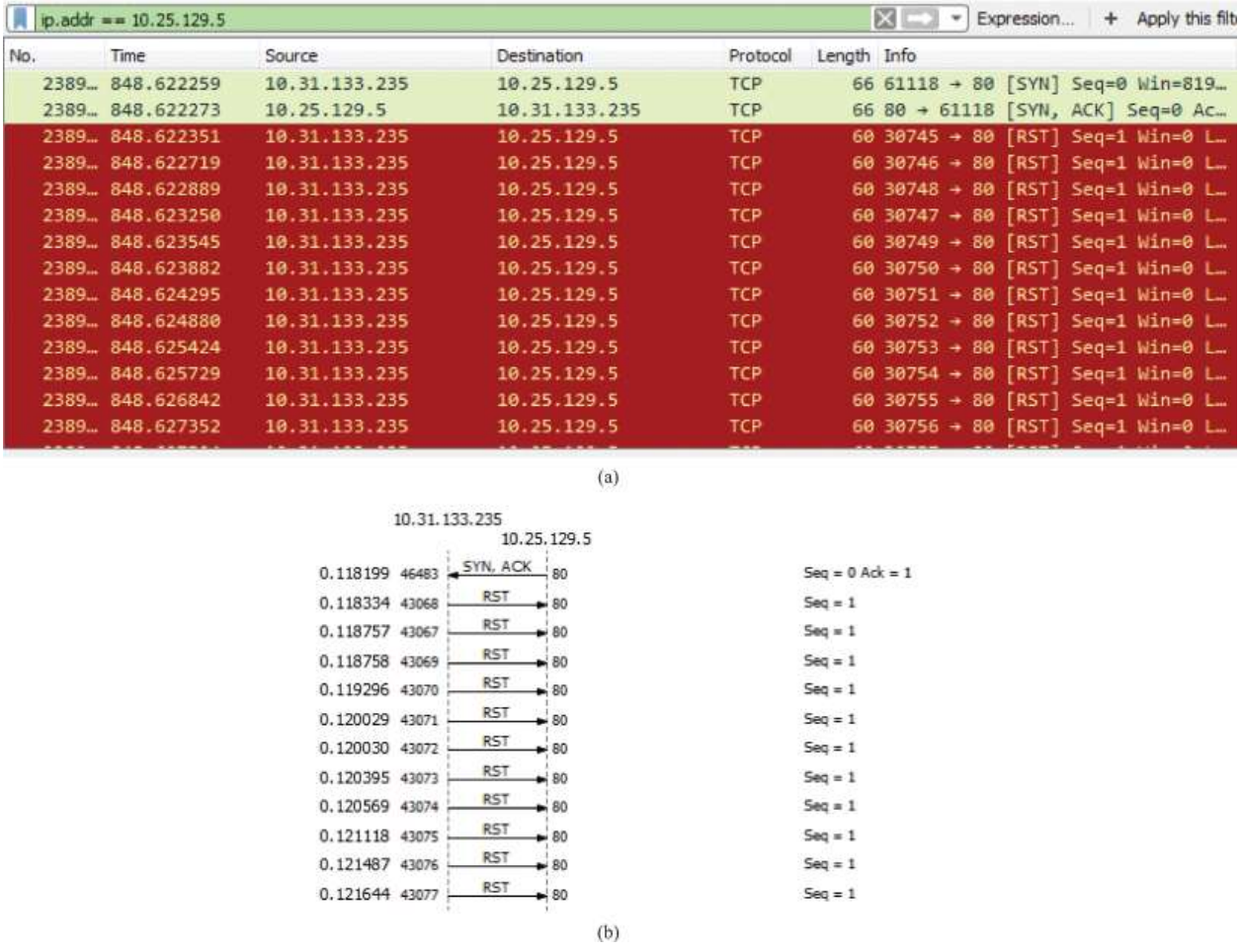
In addition, the I/O graph was stable. All packets were answered and almost no TCP errors occurred. Note that the number of requesting packets was approximately less than 10 per second, as shown in fig. below



b) During the attack

An attack was performed with the help of software which performs a DDOS attack on a server. once the attack takes place on the victim machine in a cloud environment, the arriving packets were much more in number as compared to normal traffic that the server can handle. consequently, the server could not handle the requesting packets from either normal user or the attackers.

Note:- that 10.25.129.5 was the IP address of the victim server and 10.31.133.235 was the IP address of the attacker. The first request packet from the attacker was successful, as it was treated as a normal requesting packet. The subsequent ones were not successful, as the server was too busy and could not respond. A screenshot of the packet capture is shown in Figure 4 shown below.



Captured packets and TCP flags (abnormal). (a) Captured packets. (b) TCP flags.

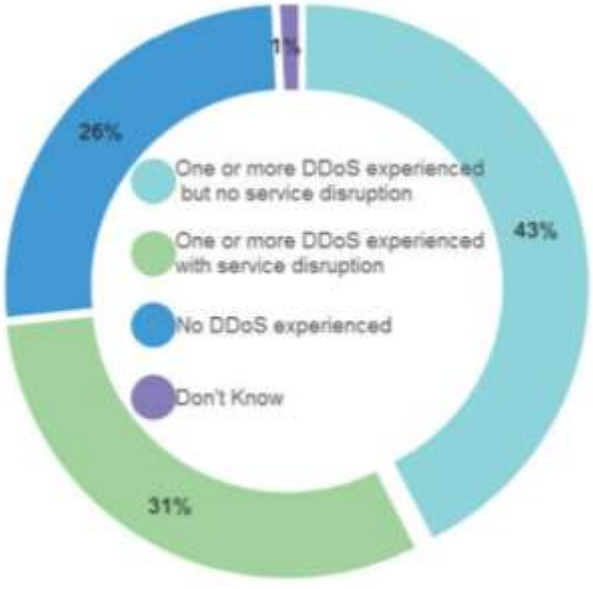
Finally, we sent 50 TCP test probes within a few seconds to the victim machine during the attack period to test the connection. The reply time was 9.6 ms on average, which differs considerably from the first test as shown below:

- Ping statistics for 10.25.129.5:80
- 50 probes sent.
- Approximate trip times in milliseconds:
- Minimum = 0.181 ms, Maximum = 152.341 ms,
- Average = 9.586 ms

Factors for Selecting Defense Solution

While selecting a DDoS solution many things need to be considered.

- **Functional**: The solution should be functional enough, which means it should be able to reduce the impact of the attack irrespective of how powerful the attack is.
- **Transpicuous**: The solution must be easy to implement i.e. it should not require modifying the existing network and its infrastructure.
- **Lightweight**: Most importantly the solution should not overhead the system.
- **Precise**: The solution selected should not give lots of false positive. Many methods need the traffic to be dropped or discarded and the solution must not drop genuine traffic.



CONCLUSION

DDoS attacks are on rising in cloud computing. This paper provides a brief survey on DDoS attacks, then taxonomy of attacks, its types and various countermeasures to mitigate the DDoS attacks. This survey confers DDoS detection, prevention, and tolerance techniques. The paper concludes by providing some points to be considered while selecting a DDoS defense solution.

The DDOS attack affects the cloud environment in a short period of time, slowing down the response or even can stop working of the server completely the TCP errors are increasing day by day, therefore, an efficient and effective detection and prevention technique are required.

References

1. https://www.edureka.co/blog/what-is-ddos-attack/
2. https://dzone.com/articles/everythimg-you-neet-to-know-about-DDos/
3. https://quizlet.com/95418390/modern-malware-flash-cards/
4. https://www.imperva.com/learn/application-security/denial-of-service/
5. https://www.techapprise.com/cybersecurity/ddos-attack/
6. https://d-scholorship.pitt.edu/19225/finalversion.pdf
7. http://ijame.ump.edu.my/images/volume%2014%20issue
8. https://iranarze.ir/wp-content/uploads/2017/04/6554/
9. http://ijmtst.com/NCRASE2017/15NCRASE15.pdf