TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 16553 - 16560

A Survey on Distributed Denial of Service Attacks and Counter Measures

Sharath Kumar Allam[1], Dr.Gudapati Syam Prasad[2]

[1]Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, AP, India.
[2]Principal, VKR,VNB&AGK College of Engineering, Gudivada, AP, India.
Email: sarath.allam@gmail.com, syamprasad.gudapati@gmail.com

Article Info
Volume 82
Page Number: 16553 - 16560
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 28 February 2020*

Abstract:
Distributed Denial of Service (DDoS) attack is a Denial of Service (DoS) attack that is made in large scale over a potential service in distributed environment. Adversaries targeting such attack makes a sustainable effort to exploit software vulnerabilities in computers through which attack is made on a target server. Such computers that unwittingly cooperate attacker are known as zombies where attacker keeps malicious piece of software known as agent. As countermeasures are being developed from time to time, the attackers are enhancing their tools to launch DDoS attacks. In this context, it is essential to have counter measures that defend existing and future DDoS variants. However, it needs thorough understanding pertaining to scope and detection methods for handling such massive attacks. This paper provides insights on different terms associated with DDoS attacks, different attack types and counter methods existing. It also covers the attacks and countermeasures in cloud computing. Provided comprehension of the DDoS attacks and their scope, it is possible to device new countermeasures for well-known and future DDoS attacks. Especially the problem of low-rate DDoS attacks in container based and SDN based cloud environments is to be addressed.

Keywords *–DoS attack, DDoS attack, low-rate DDoS attack, cloud security, container based cloud computing*

I. INTRODUCTION

Denial of Service (DoS) attack causes legitimate service disruption. A server node will not be able to serve legitimate clients in presence of this attack [1]. On the other hand, if the attack is made in large scale in distributed environments, it is known as Distributed Denial of Service (DDoS). It is the well organized and long-time planned attack with thousands of zombies or compromised nodes. Attacker injects many agents into compromised nodes in order to launch the DDoS attack. The victim server is known as primary victim from which services aredenied. The compromised nodes that cooperate the attacker in launching attack are known as secondary victims. With zombies only the attacker is able to increase the volume of attack. The client/server networking technology helps the attackers to prepare zombies and inject attack agents prior to launching actual attack [2].

Ever since the first DDoS attack identified in 1993 [3], there were many attacks occurred. A major attack was found in February 2000 on Yahoo.com. It caused revenue losses to Yahoo [4] besides other drawbacks. Later on in 2002 a Domain Name Service (DNS) compromising of 13 servers was subjected to DDoS attack. As the DNS service is essential for the functioning of Internet, the damage caused can be easily imagined. The attack lasted only one hour but its effects are noticeable as 7 servers were down [5]. If such attacks are not prevented, it leads to potential risk to all Internet related services.

The main contribution of this paper is the review of important literature to ascertain the DDoS attacks, tools and the methods used to prevent them both

January - February 2020
ISSN: 0193 - 4120 Page No. 16553 - 16560

traditionally and in the era of cloud computing. Relatively DDoS attacks are not well understood by many people in terms of the modus operandi and architectures. Therefore, this paper strives to provide more details about DDoS attack types, networks and characteristics. Comprehension on DDoS attacks can help in taking corrective measures. There are different mechanisms to prevent DDoS attacks that can be used as digital forensics, defensive and preventive measures.
The remainder of the paper is structured as follows. Section 2 focuses on DDoS attack models. Section 3 throws light on DDoS attack taxonomy. Section 4 provides countermeasures of DDoS attacks. Section 5 focuses on DDoS attacks and counter measures in cloud computing. Section 6 concludes the paper and provides directions for future work.

II. DDOS ATTACK MODELS

DDoS attack networks are of two types. They are based on Inter Relay Chat (IRC) model and Agent Handler (AH) model. Figure 1 shows the two kinds of DDoS attack networks.

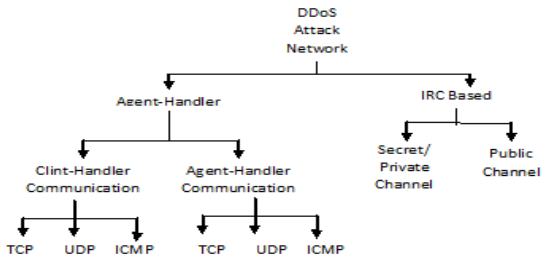

Figure 1: Different types of DDoS attack networks

As presented in Figure 1, there are two basic types of DDoS networks. They are known as agent-handler based and IRC based networks. More details on them are provided in the following sub sections.

2.1 Agent-Handler Model

Agent-Handler model has many components. As shown in Figure 2, there are agents, handers and clients. The client platform plays important role in assisting attacker to deal with other parts of the network. Handlers are software based packages that are kept in computer nodes. In the compromised nodes an agent (attack agent) is kept for actually launching attacks. The handlers are used to find the attack agents' readiness to launch attack. There may be multiple handlers and agents based on the attack network for launching DDoS attacks. Attackers try to keep handlers in router systems. There are many protocols used for communication. They include ICMP, UDP and TCP. The users of the compromised nodes are not aware of the presence of agent software in their system.

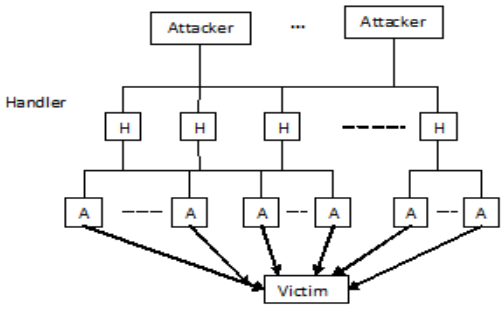

Figure 2: Agent-Handler model

The handlers are used to operate agents. The attacker launches large scale DoS attack in distributed environment with compromised nodes of zombies that contain agent software. The aim of the attacker is to reach the primary victim effectively and gain the benefits for which attack is intended.

2.2 IRC-Based DDoS Attack Model

Internet Relay Chat (IRC) is the distributed system that involves many computers and users. It includes IRC servers communicating with many computers across the Internet [6]. There are different channels created by IRC users. They are known as secret, private and public channels. In case of public channels, users in large scale are using their systems for chatting [7]. Whereas the secret and private channels help to communicate with only pre-selected users. Names and messages can be protected in both secret and private channels [8]. The secret channels are different to reach however; private channels can be detected by adversaries in terms of their presence.

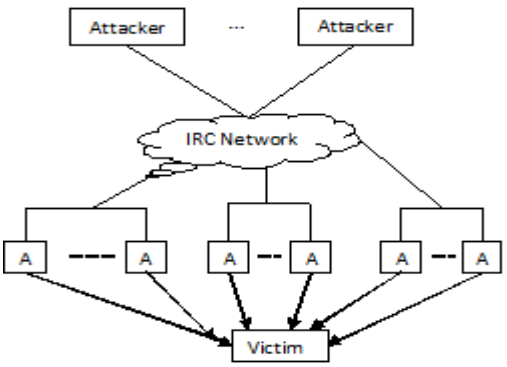

Figure 3: IRC-Based DDoS attack model

In case of IRC based attack, a client is connected to agents instead of maintaining handlers explicitly. With this kind of architecture, attackers have

January - February 2020
ISSN: 0193 - 4120 Page No. 16553 - 16560

benefits as they can use legitimate ports for instructing agents [9]. With actually makes it difficult to detect DDoS commands. As the IRC generates large volumes of traffic, it makes it easier for the attacker to hide his presence. Yet another advantages are that the attacker need not to maintain list of agents as the IRC server provides the details of agents [9]. The agent in IRC model communicates with attacker about its presence and activity. There is ease of file sharing with IRC model. Passively agent code is transferred with file sharing further making the job of attacker easy.

III. DDOS ATTACK TAXONOMY

DDoS attacks are basically of two kinds. They are known as resource depletion attacks and bandwidth depletion attacks. Resource depletion ties up computing resources with the victim system while bandwidth depletion is made with flooding of fake traffic to victim network. This causes the victim denial of service to legitimate nodes.

3.1 Bandwidth Depletion Attacks

Bandwidth depletion attacks are of two types namely flooding attacks and amplification attacks. Flooding DDoS attack causeszombies to send fake traffic in large scale to the primary victim. It congests the victims in such a way that it cannot entertain genuine clients. In other words, victim's bandwidth is depleted unnecessarily. An amplification attack on the other hand involves sending of messages to IP address from which they are broadcasted to the victim system. As this method amplifies the illegitimate traffic it effectively reduces bandwidth of the victim.

3.1.1 Flood Attacks

DDoS flooding attack is made up of large scale IP traffic from zombies. This will cause the victim to slow down or crash and saturate in terms of network bandwidth. In this kind of attack, UDP packets are sent to victim. Victim ports are randomly selected to do so. This leads to victim unable to process legitimate traffic [3].

ICMP Flood Attacks: There are packets used for network management. They are known as Internet Control Message Protocol (ICMP) packets that track round trip time and number of hops besides location of destination and source. Such packets help in requesting server to get response along with roundtrip time. Such requests are sent by ICMP flood attacks in large scale to server. This will saturate the bandwidth of the victim [3]. In case of UDP flooding there is possibility of spoofing source IP address.

3.1.2 Amplification Attacks

Amplification attack targets routers to amplify and reflect DDoS attacks. This will help attacker to achieve more by specifying address of broadcast IP. Then the messages will be sent to victims that are amplified by the routers thus increasing the volume of the attack further. This also enables attacker to use computers in the broadcast networks as zombies and install the malicious agent code. This kind of attack is further classified as Smurf and Fraggle attacks.

Smurf Attacks: In case of Smurf attack, packets are sent to amplifier but they return is spoofed return address to the IP address of the victim. Typically, ICMP ECHO requests are the packets used for the attack. Then they cause generation of ICMP ECHO reply packets as discussed in [10]. Thus the fake requests are sent to all systems in the range of broadcast by the router or amplifier the ICMP ECHO replies are obtained [11]. Thus this attack has more effect on the victim.

Fraggle Attacks: This kind of amplification attack also sends packets to amplifier. However, it makes use of UDP ECHO packets [12]. Different ports are used to spreads this kind of attack with variations and the return address is spoofed to victim's echo service in order to have an iterative effect [13]. This attack is capable of generating more bad traffic and it has more devastating effect then Smurf attack.

3.2 Resource Depletion Attacks

This kind of DDoS attacks use packets that misuse communications and tie the resources and no resources are left to serve legitimate users.

3.2.1 Protocol Exploit Attacks

TCP SYN attack is a kind of protocol exploit attack. TCP makes use of protocol handshake between to communicating parties. SYN request is sent by an initiating system. Then the receiving system is expected to send ACK back to the initiating system. When SYNX packet is received by the receiver and it does not get an expected ACKY+1 as response to SYNY, the packet is sent back and receiver resends ACK+SYNY as explored in [14]. This kind of attack requests zombies to send fake requests (TCP SYN) to victim in order to tie the resources of the victim and it cannot handle genuine requests. This kind of attack exploits the traditional three-way handshake between two parties. When SYN requests are processed in large scale by the server, it does not get ACK+SYN responses and the server resources are wasted. After some time, the server runs out of resources and cannot serve legitimate requests from clients.

January - February 2020
ISSN: 0193 - 4120 Page No. 16553 - 16560

PUSH + ACK Attacks are other kind of attacks in which the packets set to receiver are buffered in the stack until it is full. Then the packets are sent to the receiver system. However, the sender can use PUSH bit in order to influence receiver not wait till the stack is full. There is a flog named PUSH with the header of TCP packet [15]. TCP maintains large volumes of incoming traffic and then sends it to victim thus the server gets overloaded with fake requests.

3.2.2 Malformed Packet Attacks

Packets can be malformed as part of DDoS attack. Attacker influences compromised nodes to send malformed IP packets to victim in order to make it busy and even crash. Malformed packet attacks are of two kinds. In one kind of attack an IP packet is created with both sender and receiver IP addressed to confuse the victim's operating system. On the other hand, in IP packet options attack, a randomized optional fields are malformed. The QoS bits may be set to 1 forcing the victim to process traffic accordingly. When there are many agents to launch this kind of attack, it has capability to crash the victim server. In the research carried out in [16]- [22] different approaches are found. However, there is need for focusing in the context of cloud as enterprises are using it widely.

IV. DDOS ATTACKS IN CLOUD COMPUTING

DDoS attacks in cloud computing is an active research area as the enterprises depend on cloud resources. Cloud computing provides computing resources on-demand without the need for investment in pay per use manner. The host machines in cloud use virtualization technology to make it affordable. Therefore, infrastructure in cloud is effectiveutilized with virtualization. Virtual Machines (VMs) are provisioned on demand. There are many services to cope with different applications in cloud. A typical cloud environment with servers and VMs is shown in Figure 4.

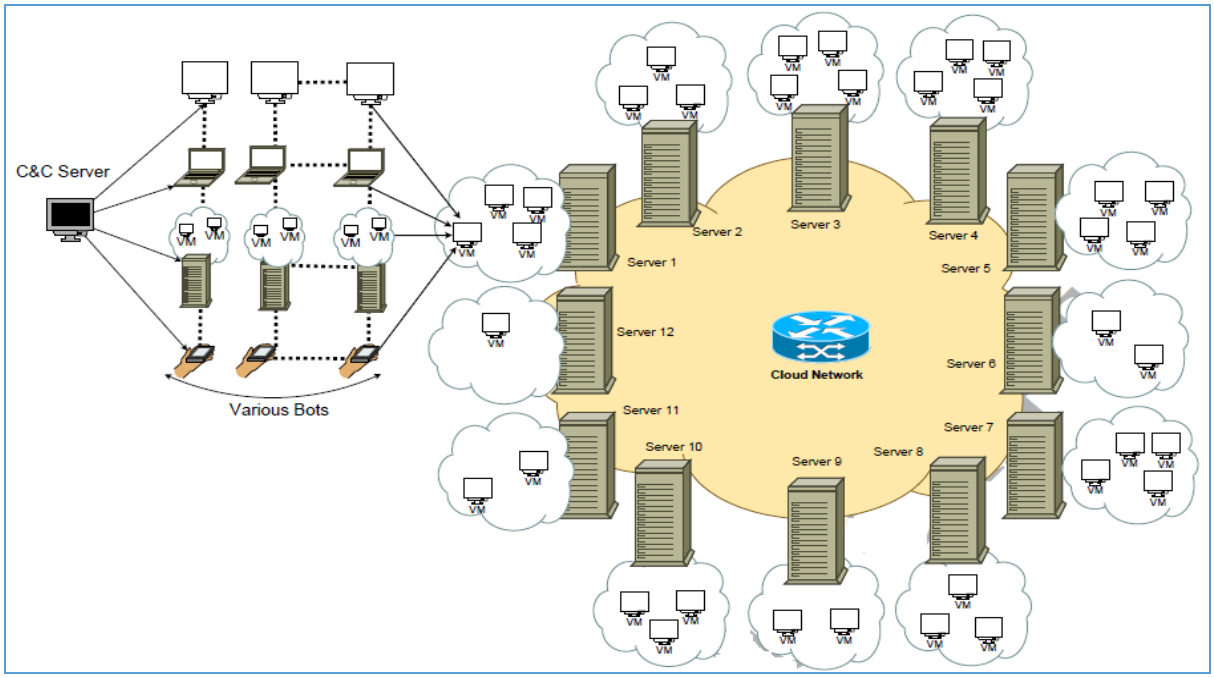

Figure 4: Typical cloud environment where DDoS attacks may occur

There are many instances in which DDoS attacks are made on the cloud infrastructure as explored in [8]. There are different features that are exploited by attackers to launch such attacks in cloud computing scenarios. Those features are actually help cloud service provisioning. However, DDoS attackers exploited those features. They are known as auto-scaling, flexible pricing system and multi-tenancy.

4.1 Auto Scaling

January - February 2020
ISSN: 0193 - 4120 Page No. 16553 - 16560

Due to virtualization of hardware, there is a feature known as shrink-expand resources associated with a VM at run time. Thus it is possible to reconfigure and allocate resources related to storage, bandwidth, main memory and CPU power dynamically. It also helps in removal resources that have been allocated if they are found to be idle. Auto scaling [16] is thus an important feature exhibited by all cloud computing service providers. There is concept of horizontal and vertical scaling based on the utility of computingresources. This will help attackers to exploit the feature to successfully launch DDoS attack.

4.2 Pay-as-you-go accounting

On-demand provisioning of computing resources became very popular model in cloud. The reason behind this is that the consumers are charged only based on the usage of the resources. Thus consumers may use VMs with low or higher resources at runtime based on the requirement. As the service providers take care of infrastructure and other facilities, the consumers are least bothered about it. Consumers can use the resources as needed and pay that much to cloud service providers. In this context, this will become cheaper to DDoS attackers as well. Due to flexible cloud accounting attackers are able to use resources needed and launch attacks in an affordable manner.

4.3 Multi-Tenancy

The concept of multi-tenancy helps to run many VMs of different providers in a particular server. This will leverage hardware virtualization further and the ROI is more to the cloud service providers. A singe physical server thus may have different kinds of VMs associated with different applications running.

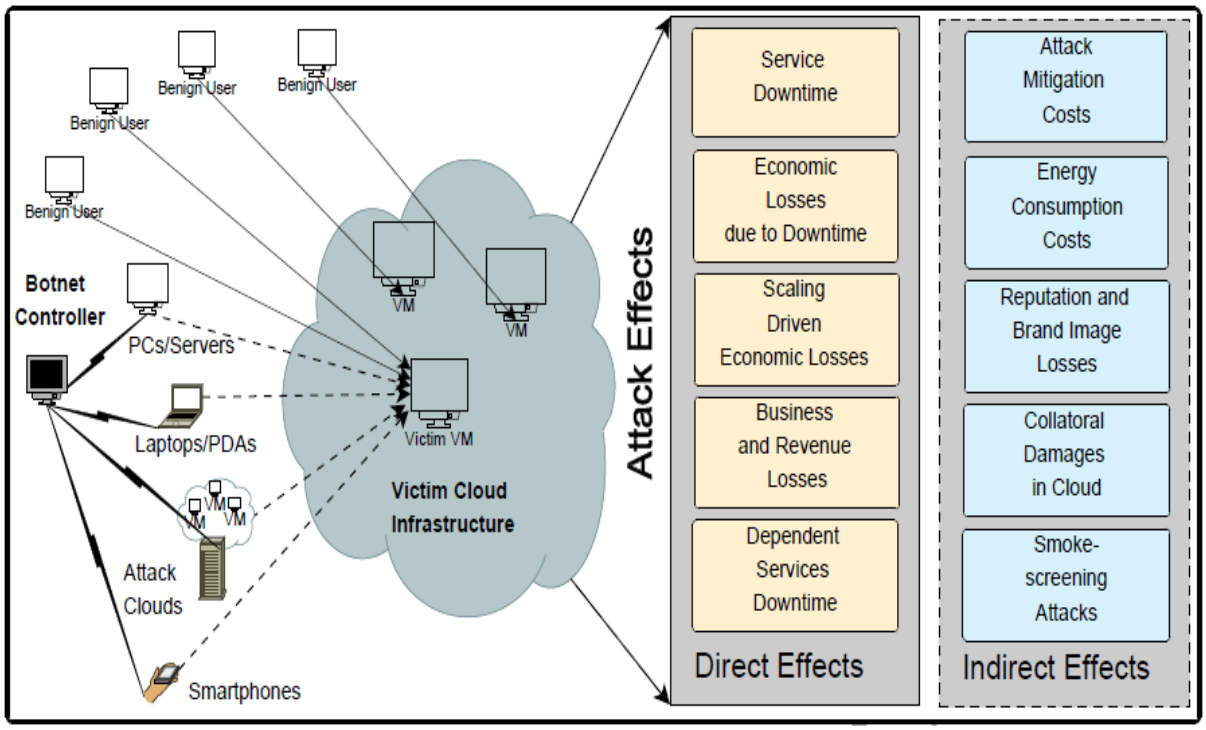

Figure 5:DDoS attack in cloud, its effects

As presented in Figure 5, there are direct and indirect effects of DDoS attacks. The direct attacks include service downtime, economic losses to the victim organization due to service downtime, scaling driven economic losses, business and revenue losses and dependent services downtime. There are indirect effects of DDoS attacks in cloud computing. They include smoke screening attacks, collateral damages in cloud, reputation and brand image losses, energy consumption costs and attack mitigation costs.

January - February 2020
ISSN: 0193 - 4120 Page No. 16553 - 16560

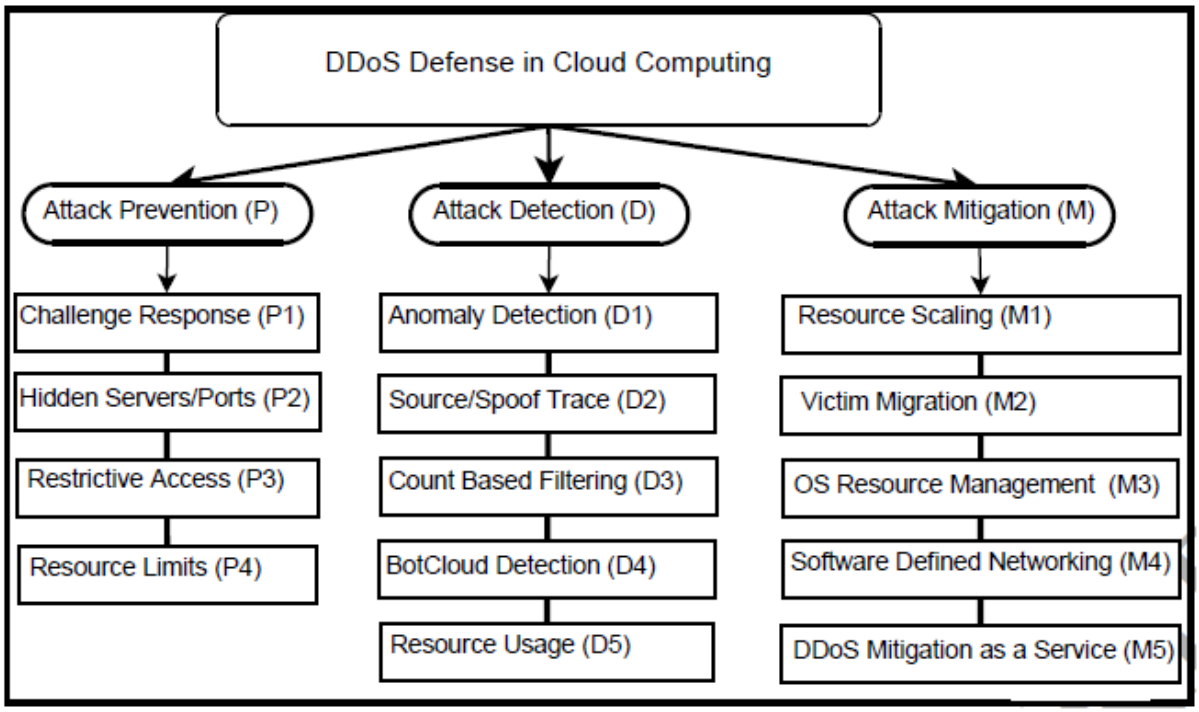

Figure 6: DDoSdefence mechanisms in cloud computing

As presented in Figure 6, there are many attack prevention approaches such as a challenge response system, hidden servers, restrictive access and resource limits. Attack detection methods include anomaly detection, source/spoof trace, count based filtering, Bot Cloud detection and resource usage. Attack mitigation methods on the other hand include resource scaling, victim migration, OS resource management, software defined networking (SDN) and DDoS Mitigation as a Service.

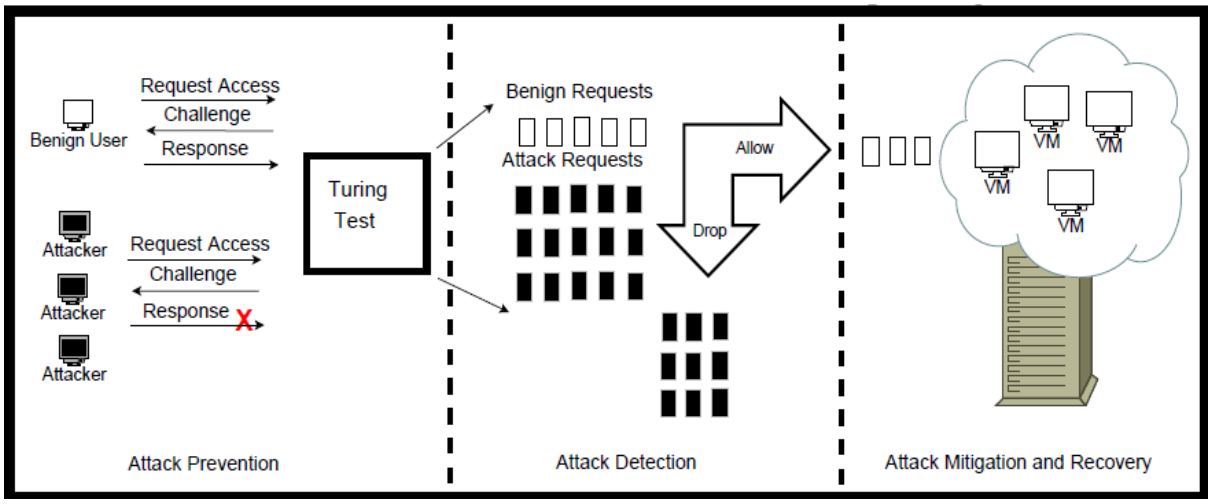

Figure 7: Protection against DDoS attack at different levels

As shown in Figure 7, challenge response system is followed to prevent attacks. When a challenge is thrown by the system, there will be no response from the attacker. Such requests will not be processed. Some attacks overcome this. In such cases attack detection is carried out followed by attack mitigation and recovery.

January - February 2020
ISSN: 0193 - 4120 Page No. 16553 - 16560

4.4 Low Rate DDoS Attacks in Cloud Computing Environments

According to Li et al. [23] low-rate DDoS attack is the kind of attack which is very difficult to detect. In a stealthy fashion, this kind of attack eludes mechanisms used to detect. The mitigation mechanism proposed in [23] is dynamic in nature and it effectives maximizes QoS. The attacks are associated with container based cloud environment with micro service architectures. Their method defeats low-rate DDoS attack with its mitigation strategy. Zhijun et al. [24] on the other hand employed factorization machine in presence of Software Defined Network (SDN). Features are extracted from flow rules to detect such attacks. It has mechanism to have dynamic deletion of flow rules for more fine-grained detection of the aforementioned DDoS attacks.

V. RESEARCH GAPS

In the context of container based cloud computing environments, the low-rate DDoS attack detection is the challenging problem to be addressed. Li et al. [23] proposed a dynamic strategy to mitigate DDoS attacks. However, it still has certain drawbacks. First, detection of low-rate DDoS attack in the presence of scalable micro service with unlimited resources is yet to be investigated. Second, in the presence of unlimited resources the dynamics of pricing issues when defending DDoS attacks is not yet studied. Third, they only considered low-rate DDoS attacks in container based cloud environments. However, there is possibility to explore other kinds of DDoS attacks.

Zhijun et al. [24] explored detection of low-rate DDoS attacks against SDN data layer. Since SDN usage in cloud computing is a common phenomenon, this is the potential risk with low-rate DDoS attacks. In [24] a method named Factorization Machine (FM) is proposed to detect low-rate DDoS attacks. It is machine learning based approach that could provide better performance. However, it needs to be improved further in terms of accuracy with deep learning methods with their innovations.

VI. CONCLUSIONS AND FUTURE WORK

DDoS attacks caused huge losses to organizations. It is reported that these attacks are occurring frequently. It is the problem that needs sustainable effort. The existing solutions may not be sufficient in future as the attackers invent new model operandi for launching such attacks. Therefore, it is essential to have knowledge on various attacks and counter measures in cloud computing or in distributed computing in general. This paper provides review of many kinds of DDoS attacks, their counter measures. It also covers DDoS attacks that target servers in cloud computing environment including attack scenario, methods for detection, prevention and mitigation besides the procedure followed to handle DDoS attacks. From the review, it is understood that, providing counter measures to DDoS attack is not a onetime solution. It is therefore an open problem to improve the state of the art from time to time for business continuity and growth. As found the research gaps, in future, we intend to focus on the novel methods to detect low-rate DDoS attacks in container based and SDN based cloud environments.

References

1. Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016). *Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. IEEE Communications Surveys & Tutorials, 18(1), 602–622.*
2. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., &Buyya, R. (2017). *DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, 30–48.*
3. Yan, Q., & Yu, F. R. (2015). *Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine, 53(4), 52–59.*
4. Gupta, B. B., &Badve, O. P. (2016). *Taxonomy of DoS and DDoS attacks and desirable defence mechanism in a Cloud computing environment. Neural Computing and Applications, 28(12), 3655–3682.*
5. Karthikeyan, T., Sekaran, K., Ranjith, D., Vinoth kumar, V., Balajee, J.M. (2019) "Personalized Content Extraction and Text Classification Using Effective Web Scraping Techniques" *International Journal of Web Portals* (IJWP), 11(2), pp.41-52.
6. Opeyemi.A.Osanaiye. (2015). hort Paper: IP Spoofing Detection for Preventing DDoS Attack in Cloud Computing . *International Conference on Intelligence in Next Generation Networks*, p139-141.
7. Carlin, A., Hammoudeh, M., &Aldabbas, O. (2015). *Defence for Distributed Denial of Service Attacks in Cloud Computing. Procedia Computer Science, 73, 490–497.*

January - February 2020
ISSN: 0193 - 4120 Page No. 16553 - 16560

8. Choi, J., Choi, C., Ko, B., & Kim, P. (2014). *A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment. Soft Computing, 18(9), 1697–1703.*
9. Vinoth Kumar, V., Arvind, K.S., Umamaheswaran, S., Suganya, K.S (2019), "Hierarchal Trust Certificate Distribution using Distributed CA in MANET" *International Journal of Innovative Technology and Exploring Engineering*, 8(10), pp. 2521-2524
10. Wang, B., Zheng, Y., Lou, W., &Hou, Y. T. (2015). *DDoS attack protection in the era of cloud computing and Software-Defined Networking. Computer Networks, 81, 308–319.*
11. Maithili, K , Vinothkumar, V, Latha, P (2018). "Analyzing the security mechanisms to prevent unauthorized access in cloud and network security" *Journal of Computational and Theoretical Nanoscience*, Vol.15, pp.2059-2063.
12. Alosaimi, W., Alshamrani, M., & Al-Begain, K. (2015). *Simulation-Based Study of Distributed Denial of Service Attacks Prevention in the Cloud. 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies.* P1-6.
13. V.Vinoth Kumar, Ramamoorthy S (2017), "A Novel method of gateway selection to improve throughput performance in MANET", *Journal of Advanced Research in Dynamical and Control Systems*,9(Special Issue 16), pp. 420-432.
14. Liu. (2015). *Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment. 2015 12th International Conference on Information Technology - New Generations.* P1-6.
15. Somani, G., Gaur, M. S., Sanghi, D., & Conti, M. (2016). *DDoS attacks in cloud computing: Collateral damage to non-targets. Computer Networks, 109, 157–171.*
16. Ruby Lee, David Karig, Patrick McGregor and Zhijie Shi, "Enlisting Hardware Architecture to Thwart Malicious Code Injection", *Proceedings of the International Conference on Security in Pervasive Computing (SPC-2003), pp. N/A*, March 2003.
17. Umamaheswaran, S., Lakshmanan, R., Vinothkumar, V. et al. New and robust composite micro structure descriptor (CMSD) for CBIR. *International Journal of Speech Technology* (2019), doi:10.1007/s10772-019-09663-0.
18. Joao B. D. Cabrera, Lundy Lewis, Xinzhou Qin, Wenke Lee, Ravi K. Prasanth, B. Ravichandran, and Ramon K. Mehra, "Proactive Detection of Distributed Denial of Service Attacks Using MIB Traffic Variables – A Feasibility Study", *Integrated Network Management Proceedings, pp. 609-622*, 2001.
19. Dhilip Kumar V, Vinoth Kumar V, Kandar D (2018), "Data Transmission Between Dedicated Short-Range Communication and WiMAX for Efficient Vehicular Communication" *Journal of Computational and Theoretical Nanoscience*, Vol.15, No.8, pp.2649-2654.
20. Nathalie Weiler. "Honeypots for Distributed Denial of Service", *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops, 2002. pp. 109-114.* 2002.
21. Vern Paxon, "An Analysis of Using Reflectors for Distributed Denial of Service Attacks", *ACM SIGCOMM Computer Communication Review, Vol. 31, Iss. 3*, July 2001.
22. Kouser, R.R., Manikandan, T., Kumar, V.V (2018), "Heart disease prediction system using artificial neural network, radial basis function and case based reasoning" *Journal of Computational and Theoretical Nanoscience*, 15, pp. 2810-2817
23. Shalini A, Jayasuruthi L, Vinoth Kumar V, "Voice Recognition Robot Control using Android Device" Journal of Computational and Theoretical Nanoscience, 15(6-7), pp. 2197-2201
24. Jayasuruthi L,Shalini A,Vinoth Kumar V.,(2018) " Application of rough set theory in data mining market analysis using rough sets data explorer" *Journal of Computational and Theoretical Nanoscience*, 15(6-7), pp. 2126-2130