Analysis of Distributed Denial of Service Attacks

Dr. Ketki Kshirsagar[1] ,Shivapooja Patil[2] ,Dr. Anup Ingle[3]

[1]Asso. Professor, Department of Electronics & Telecommunication, VIIT, Pune, Maharashtra, India.

[2]Student, Department of Electronics & Telecommunication, VIIT, Pune, Maharashtra, India.

[3]Asst. Professor, Department of Electronics & Telecommunication, VIIT, Pune, Maharashtra, India.

ketki.kshirsagar@viit.ac.in, shivapooja.22220150@viit.ac.in, , anup.ingle@viit.ac.in

Abstract:

Decoupling the network's control and data planes is a key component of software-defined networking technology. The control and data planes are divided, providing a dynamic, controllable, adaptable, and strong platform. Conversely, centralized network platforms pose security challenges, like a denial-of-service attack against the centralized controller. Single-contact failures are likely to occur in SDNs due to their centralized nature. A cooperative method for DDOS attack detection in a distributed SDN multi controller platform is suggested by this study. In addition, it examines how distributed controllers as opposed to centralized controllers in SDNs are subject to DDOS attacks. The study employs a monitoring solution that combines the POX controller with the Open vSwitch to detect attacks and provide an attack mitigation process.

Keyword:-*DDoS, Mitigation, DDoS classification, Protocol Attacks, Defence techniques*

I. Introduction

The majority of our dependence in today's online world is on technology. We can quickly access services and information thanks to internet connectivity, where security is a top priority and the basis for the CIA's acronym (confidentiality, integrity, availability). There are numerous security risks connected to each, but in recent times, a new class of security threats has surfaced, one that targets resource availability rather than their integrity or confidentiality. The term "Denial of Services" (DoS) Attacks refers to this recently evolved threat. A denial of-service (DoS) attack is a cyberattack that stops authorized users from accessing a particular network service or resource, like a website, web service, or system resource.There have been numerous DDoS-related incidents in the past and present, such as the disruption of the website of the Indian telecom regulator TRAI and the attacks on numerous organizations, including GitHub and MTN. That being said, numerous organizations are being negatively impacted by this new and extremely serious attack. Attackers are using DDoS attacks to cause many ecommerce websites to slow down. Attackers use a variety of techniques to launch DDoS attacks on the system they are targeting, but the most popular technique these days is reflection-based DDoS attack, which is one of the attackers' latest innovations.

The first DDoS attack to shut down all internet access in a city occurred in 1997, during a hacker's conference in Las Vegas, and was orchestrated by the attacker Khan C. Smith. As a result, numerous online attacks targeted Sprint, EarthLink, E-Trade, and other popular internet service providers. Smith created his first botnet in 2001, using fake domain names, email addresses, and websites to spam nearly a quarter of the internet [1]. The largest officially recorded DDoS attack on GitHub occurred in February 2018, with an incoming traffic volume of 1.3 Tbps and a packet transfer rate of 126.9 million per second [2]. This attack targeted the vulnerable open-source software system memcached, which is widely used to improve network and web service speeds. The attacker exploited the system by flooding GitHub with internet traffic, causing it to become overloaded and unable to process new requests, resulting in a denial of service. The attacker achieved a magnitude of 50,000 by flooding memcached with spoofed requests, leveraging its amplification effect. Figure 1 depicts how the DDoS attack was structured, from the attacker to the target server, using compromised systems as master and slaves.

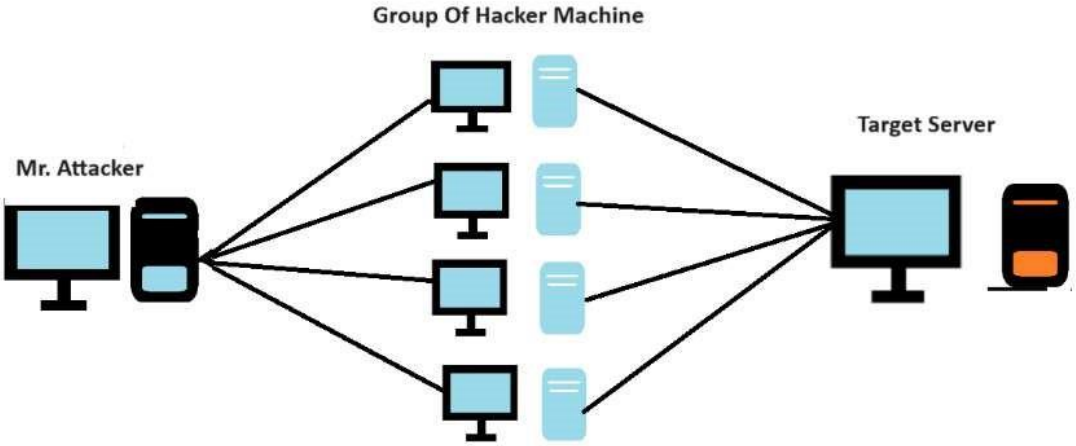

Figure 1: DDoS Attack Framework

To carry out a DDoS attack, the attacker usually needs to take control of hundreds or thousands of interconnected machines or devices. These devices, which include smartphones, computers, and other computing machines that are frequently connected to the internet, are infected with various types of malware, transforming them into bots. The primary attacker then remotely controls all the bots on the network using a master-slave architecture to form a botnet [3]. Users are frequently unaware that their devices have been compromised, and they unknowingly serve as slaves for the attacker.Once the botnet is up and running, the attacker can use remote commands to launch an attack on a specific server at a predetermined date and time [4]. The master primarily targets the victim's machine or IP address, and each slave is directed to send a large volume of request packets to the same victim machine or server, overwhelming the network or server and resulting in a denial of service. Because each compromised bot in the network appears to be a legitimate user, the attack can be difficult to trace. The combined power of numerous computers and devices enables significant attacks while concealing the attacker's identity.

In 2018, the Mirai attack emerged as a major IoT threat, accounting for 16% of all attacks [5]. Mirai's evolution has continued, with IBM X-Force reporting at least 63 Mirai variants as of mid-2019, a figure that is expected to double with the release of the next Mirai-like botnet, Gafgyt. Even smart home devices and kitchen appliances are now vulnerable to internet attacks due to weak passwords, unused default credentials, and insecure networks [6]. The transition from spam email botnets to IoT botnets indicates a possible increase in future attacks.GuyRosefelt of NSFOCUS emphasized the ongoing security challenges posed by IoT devices [7], stating, "As IoT innovation and advancement continue, IoT devices will become increasingly involved in DDoS attacks. Routers and cameras are especially vulnerable because they are frequently deployed in manufacturing and residential settings without adequate security measures. This trend is likely to fuel future attacks that use IoT devices.

The protocol-based amplification attack can be thought of as a layer on top of the IoT infrastructure that is in charge of controlling congestion. Novel protocols have been introduced to allow for faster communication between devices in both consumer and industrial applications. However, because of their novelty and lightweight nature, these protocols carry a high risk of exploitation. Protocols that use the User Datagram Protocol (UDP), such as memcached servers, are vulnerable to IP spoofing and packet amplification, allowing for large-scale DDoS attacks. Such attacks can cause amplification factors of 10 to 50 times the normal traffic. The proliferation of new devices that use lightweight protocols has grown in popularity, with the total expected to exceed 35 billion by the end of 2021 [8].
According to a recent ZDNet report citing an anonymous source, a significant portion of these devices may be used in DDoS amplification attacks, which are becoming more common and powerful. To protect against these threats, it is critical to change the default usernames and passwords on smart devices, use strong, unbreakable passwords, ensure secure network connections, monitor for suspicious activity, and regularly update firmware patches.The volume of DDoS activities in 2020 has increased by 154% over the previous year, with attacks up 154% from 2019. Neustar, an American company that specializes in DDoS attack mitigation, found that the size and frequency of attacks increased in 2020 when compared to previous years. Notably, Amazon Web Services experienced the largest DDoS attack in February 2020, with volumes peaking at 2.3 terabits per second [8].

II. Literature survey

For the purpose of conducting a literature review, recent surveys and research articles pertaining to DDOS attack prevention, detection, and mitigation have been considered from various angles. Mahjabin et al.'s [9] primary focus was on the mitigation, detection, and prevention of distributed denial-of-service attacks. With the help of illustrations, the attack targets, motivation, and tactics are all explained in detail. The various attack types and their mechanisms are examined, and recent tools for mitigation—such as prevention and detection— are also listed and contrasted with their benefits and drawbacks. Understanding the different types of attacks and the methods used to detect and prevent them is primarily helpful. There is also discussion of the DDOS attacks on modern technology and trends. It identifies the research gap to stop and identify attackers' future attacks.

A statistical traffic analysis-based method for identifying and thwarting DDoS attacks was presented in one of the early studies in this field. The suggested system analysed traffic using a sliding window technique to find anomalies, which were then used to start filtering mechanisms to lessen the attack. According to the study, this method worked well for both low- and high-rate DDoS attack detection and mitigation [10].

In a different study, a DDoS defence method based on game theory was presented, which encouraged truthful users to help with the mitigation process. The suggested method was predicated on the notion of a "public good game," in which each user could aid in the mitigation effort by directing lawful traffic, and the system offered rewards to the highest contributors. According to the study, the suggested technique effectively reduced DDoS attacks without compromising the flow of legal traffic.

A study that examined the characteristics of network traffic suggested a machine learningbased method for identifying DDoS attacks. The suggested method employed decision treebased classifiers to differentiate between legitimate and malicious traffic. Research indicated that the suggested method was successful in identifying application layer as well as volumetric attacks [11][14]. The development of anomaly detection techniques for DDoS attacks has been the subject of numerous studies. One such study suggested a method based on spectral clustering, which finds clusters of related data points to identify anomalies in network traffic. A different study put forth a nonparametric density estimation-based technique that estimates the traffic's probability density function in order to identify network traffic irregularities.The DDoS attacks on the Internet of Things were the main topic of Emina et al.'s study [12][15]. An overview of the Internet of Things' architecture layer is provided by the application, network, and sensor layer diagram. The explanation clarifies the various DDoS attack types on the IoT in relation to real-time scenarios. The obstacles and difficulties in identifying and thwarting attacks in the Internet of Things must be researched and implemented in a lightweight manner in accordance with the capabilities of the device and the available resources. This paper demonstrates the broad research area to address the security and attack-resistant performance of IoT devices.P. Kaur et al. [13][16] propose a real-time framework for combating DDoS attacks and preventing harm through source address analysis and filtration. Signature-based, anomalybased, and hybrid-based filtering are all considered for detecting various DDoS attacks, each with their own set of advantages and disadvantages. The paper describes various models for detecting attacks in real time, as well as defensive mechanisms for controlling them. The detection approaches are compared to existing detection approaches, along with their challenges and issues. Pritesh Kumar Prajapathi et al.[17] primarily surveys DDoS attacks at the application layer and recent detection methods. The paper clarifies the various attacks that occur in the application layer and their relationship with the protocol. The detection mechanism is compared and briefly discussed for the deployment of an intrusion system or smart controller in a Software Defined Network (SDN). Machine learning-based Artificial Neural Networks (ANN) and genetic algorithms can reduce false positives.

III. Targets and reasons for attacks

These attacks gain a lot of popularity among other attacks and threats, which are expanding quickly according to numerous studies carried out by cyber experts. The volume of recent attacks has increased significantly in a short amount of time. Various DDoS attacks can have different reasons, which can be used to characterize their motivations. These reasons account for a large portion of the attacks that fall into these categories.

- Ideology: The content and beliefs expressed on the websites and web servers contradict their own ideas and beliefs. After that, the attacker plans and launches a DDoS attack to bring the web server to a halt and stop the service. DDoS attacks are used by the attackers to target web servers or websites whose content and ideas conflict with their own.
- Business rivals: Internet companies can use DDoS attacks to take control of rival websites or prevent customers from accessing them, resulting in losses. This attack is being prepared by a number of the leading internet businesses in order to prevent customers from taking advantage of big holiday or festival sales. Businesses use this attack to sabotage rival companies in the same industry by interfering with their operations.
- Boredom: People who aspire to be regular hackers, are easily bored, and are drawn to cyber threats can write code to launch various DDoS attacks.
- Extortion: These highly skilled technicians who carry out DDoS attacks exploit their victims' businesses or individuals for financial gain by extorting money.
- Cyber warfare: In order to stop terrorist websites and the nation's enemy website, the government has planned and approved DDoS attacks.

The COVID-19 pandemic has presented numerous avenues for hackers to breach corporate networks and pilfer sensitive data. The majority of developed nations have documented attempts to breach the confidentiality of corona research work by pharmaceutical companies, academic institutions, and medical professionals. The pandemic has led to a sharp rise in work from home jobs, online shopping, and large financial transactions, all of which provide opportunities for cyber criminals to launch various forms of attack. SYN flooding continues to be the most common attack type in Q3, 2020, with 94.60%. ICMP attacks come in second place with 3.40%, followed by TCP with 1.40% and UDP with 0.60%. With 94.72% of attacks in Q2, 2020, the SYN flood accounted for the largest share. With ICMP at 4.90%, TCP at 0.22%, UDP nearly at the same place at 0.10%, and HTTP at 0.06%, it is evident that there were no attacks in comparison to the previous quarter.

In the second and third quarters of 2020, there were more SYN and ICMP flood attacks than any other[18] Figure 2 below illustrates the various attack types that happened in Q3, 2020.

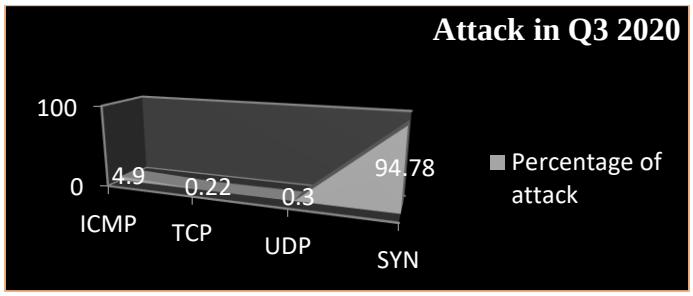

Figure 2: Attack in Q3 2020.

IV. Classification of attack

A number of types of distributed denial-of-service (DDoS) attacks can be broadly classified according to the attackers' techniques and the attacks' characteristics. In this review, we go over a few of the most prevalent DDoS attack types and provide diagrams to show how they work.

1. Attacks based on volume

The most prevalent kind of DDoS attack is volumetric, which involves flooding the target system with excessive traffic. Usually, a botnet a network of compromised devices under the attacker's control is used to launch these attacks. The purpose of a botnet is to overload the network bandwidth of the target system with UDP or TCP traffic. Attacks based on volume that result from UDP flooding. An amplification attack occurs when UDP services respond to a smaller initial request size with a larger size. Together, the amplification and reflection attacks cause the victim server to crash with minimal effort. When used in tandem, UDP applications and services have the potential to create massive amplification and reflection attacks against Domain Name Server as well as other supported protocols like NTP, SSDP, and SNMP.

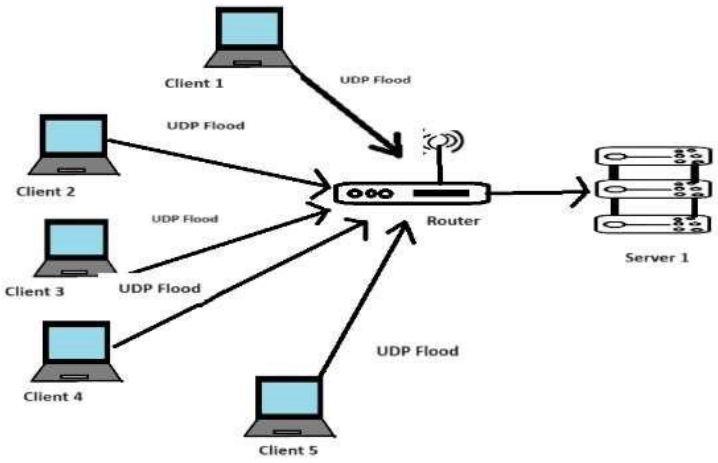

Figure 3: Volume based on attack

2. Protocol based attack:

By flooding a target server with SYN packets, an attack known as a SYN flood takes advantage of the standard TCP handshake process and overwhelms its ability to process valid connection requests. Anticipating acknowledgment (ACK) packets from the spoof IP addresses, the server becomes bogged down in the waiting for never-to-come responses, making it incapable of handling actual connection attempts.

Smurf attacks, on the other hand, profit from the ICMP protocol, more especially from ICMP echo requests and responses. The attacker sends out ICMP echo requests to IP broadcast networks by impersonating the victim's IP address. Following that, these networks broadcast the requests to every device inside their reach, causing every device to respond with an ICMP echo reply to the IP address of the victim. The victim's device is overloaded with responses, which interferes with regular operation. Smurf attacks are especially problematic because, unlike certain other DDoS attacks, they can be carried out without a botnet.

3. Attacks with Resource Exhaustion:

Resource Exhaustion Attacks aim to overload or crash the system's primary resources, including the CPU, memory, and sockets. There are two methods for carrying out these kinds of attacks. First, the attacker uses application layer, transport, and network protocols as leverage to accomplish their objectives. In the second method, attacks are carried out via malformed packets.

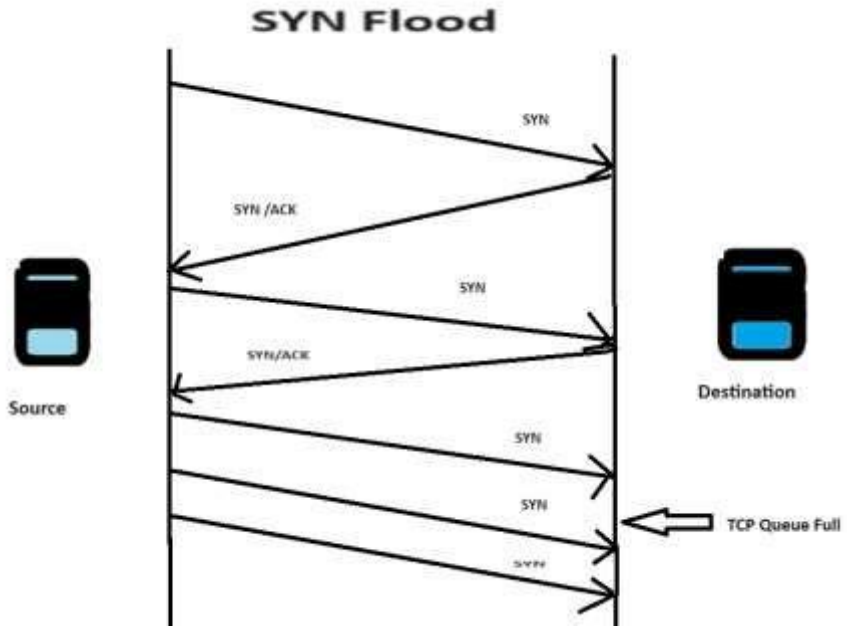

Figure 4: SYN Flood Attack

V. Defence Techniques

It's critical to implement efficient DDoS attack mitigation strategies. A multi-layered strategy that incorporates proactive measures, real-time detection, and efficient response tactics is needed to defend against DDoS attacks. Important techniques for reducing DDoS attacks include:

Network defence, such as To filter malicious traffic and safeguard network resources, intrusion detection systems (IDS), intrusion prevention systems (IPS), and firewalls are implemented. By using traffic filtering techniques, one can prevent suspicious traffic patterns from reaching the target system, identify and block them, optimize network and application resources to handle higher traffic volumes, and lessen the impact of DDoS attacks.

Put DDoS Protection Services in Place By filtering and blocking malicious traffic, specialized DDoS protection services can protect the target from the worst of the attack. Additionally, enhancing network security can be achieved by putting strong security measures in place like intrusion detection systems and firewalls, which can help detect and stop malicious traffic before it reaches its target. Educating staff members about DDoS attacks and any warning indicators can aid in early detection, response, and the creation of a response plan. Organizations can minimize the impact of an attack by responding quickly and effectively when they have a thorough DDoS response plan in place.

VI. Conversation

Table 1: Attack challenges and Impact

Sr.No	Challenge	Description	Impact
1.	Lack of Network Collaboration	Distributed nature of attacks & internet structure limit universal defence	Single network defences ineffective
2.	Global Audit & Accountability	Difficult to implement globally due to practical and socioeconomic reasons	Detection mechanisms hampered
3.	Zero-Day Attacks	New, sophisticated attacks emerge constantly	Reactive defence leaves systems vulnerable
4.	Rise of IoT Botnets	Insecure IoT devices create large botnets for attacks	Increased attack frequency and power
5.	Resource Consumption	DDoS attacks overwhelm victim server resources	Existing defence mechanisms can be resource-intensive
6.	Costly Defences	Some mitigation strategies require expensive deployments	System performance suffers due to resource usage

Table 1 shows Attacks changes, detailing and impact on networking systems

VII. Conclusion

DDoS attacks pose a serious threat to the interconnected world we live in because they can cause financial damage, interfere with online services, and jeopardize the security of vital infrastructure. By understanding the nature of these attacks, implementing efficient mitigation techniques, and keeping up with new threats, organizations can strengthen their defences against them. Enterprises of all sizes are at serious risk from these attacks. Understanding the different kinds of attacks, why they happen, and putting strong mitigation plans in place are critical steps in protecting online services and maintaining the stability of the digital ecosystem. The increasing complexity and scale of Distributed Denial of Service attacks have led to their rapid escalation, which emphasizes how critical it is for businesses to strengthen their defences against these growing threats.

In order to defend against DDoS attacks, one must be aware of how they work and examine common strategies. As technology develops, so too must our defences against these disruptive and potentially devastating attacks. Organizations can reduce the potential impact of DDoS attacks and effectively defend themselves from them by putting in place proactive security measures and a clear response plan.

VIII. References

[1] Smith, J. (2019). Is 2019 the year of DDoS? The hostdimeblog.https://www.hostdime.com/blog/2019-ddos-protection. (Accessed April 13, 2020).

[2] Cloudflare Inc., USA. Famous DDoS Attacks. The largest DDoS attacks of all time. http://www.cloudflare.com/ learning/ddos/famous-ddos-attacks. (Accessed April 13, 2020).

[3] Sandip Sonawane. (2018). A review of botnets and botnet detection methods. International Journal of Engineering Research and Technology, 7:12

[4] Ankur Lohachab. and Bidhan Karambir. (2018). Critical Analysis of DDoS, an Emerging Threat to IoT Networks. Journal of Communication and Information Networks, 3(3), 57-78. DOI:10.1007/s41650-018-0022-5

[5] Maria Korolov. (2019). What is the definition of a botnet? When an army of infected IoT devices attacks. Available online: https://www.csoonline.com/article/3240364/what-is-a-botnet.html (Accessed: April 15, 2020)

[6] Menachem Domb (2019). Smart Home Systems Based on the Internet of Things. The Internet of Things (IoT) for Automated and Smart Applications IntechOpen book edition. DOI: 10.57772/intechopen.84894.

[7] Devika Jain, (2018). 27 million attacks on H1 cyber security. Technical report for NSFOCUS. Available online at https://nsfocusglobal.com/2018-h1-cybersecurityinsights.(Accessed: April 23, 2020)

[8] Gilad David Maayan, (2020). The 2020 IoT Rundown: Statistics, Risks, and Solutions. Available online: https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for2020.aspx. (Accessed: April 23, 2020)

[9] Tasnuva Mahjabin, Yang Xiao, Guang Sun, and Wangdong Jiang. (2017). A survey of DDoS attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13:12. DOI: 10.1177/1550147717741463

[10] Jasmeen Kaur Chahal, Abhinav Bhandari, and Sunny Behal (2019). Distributed Denial of Service Attacks: Threat or Challenge? New Review of Information Networking, 24(1), 31-103. DOI: 10.1080/13614576.2019.1611468.

[11] Ingle, A., A. Gour, and K. Kshirsagar. "DDoS attack detection algorithms based on pattern classification and machine learning." Journal of University of Shanghai for Science and Technology 23.2 (2021): 132.

[12] Ambhore, Vishal, Sandhya Shevatre, Rushikesh Ambhore, Ketki Kshirsagar, and Parikshit N. Mahalle. "Capability Based Access Control Mechanism in IoT: a Survey of State of the Art." In International Conference on Information and Communication Technology for Intelligent Systems, pp. 525-535. Singapore: Springer Nature Singapore, 2023.

[13] Chishty, Shoaib, Ankita Langare, Somesh Sawant, and Ketki Kshirsagar. "Industrial Data Acquisition." International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET) 11, no. 12: 14590-14594.

[14] Sharma, K., & Gupta, B., B. (2018). Taxonomy of Distributed Denial of Service (Ddos) Attacks and Defense Mechanisms in Present Era of Smartphone Devices. International Journal of E-Services and Mobile Applications, 10, 2, 58–74. DOI: 10.4018/ijesma.2018040104.

[15] Ghafar A Jaafar., Shahidan M Abdullah., &Saifuladli Ismail. (2019). Review of Recent Detection Methods for HTTP DDoS Attack. Journal of Computer Networks and Communications, 2019, Article ID 1283472, 10. DOI:10.1155/2019/12834727

[16] Kaur, P., Manish, K., & Abhinav, B. (2017). A Review of Detection Approaches for Distributed Denial of Service Attacks. Systems Science &Control Engineering: An Open Access Journal, 5,1, 301-320. DOI:10.1080/ 21642583.2017.1331768.

[17] Priteshkumar Prajapathi., Nidhi Patel., &Dr. Parth Shah. (2019). A Review of Recent Detection Methods For HTTP DDoS Attacks. International Journal of Scientific and Technology Research, 8,12,1693-1696.

[18] leg Kupreev., Ekaterina Badovskaya., & Alexander Gutnikov. (2021). Q3 Q4 2020 DDoS attacks. Technical report. https://securelist.com/ddosattacks-in-q32020/99171, Oct 28, 2020. (accessed on Jan 5, 2021) https://securelist.com/ddosattacks-in-q4-2020/100650, Feb 16, 2021. (accessed on Feb 19, 2021)