iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46882

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: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

Literature Review of Distributed Denial of Service (DDoS) Attacks, its Detection Techniques and Prevention Mechanisms

Shankar Kumar[1], Dr. Nandeshwar Pd Singh[2], Dr. Narendra Kumar[3]
[1]*Research Scholar, Magadh University, Bodh-Gaya*
[2]*Associate Prof., Dept. of Mathematics, S.M.S.G. College, Sherghati, Gaya*
[3]*Assistant Prof., Dept. of Computer Applications and IT, A. M. College, Gaya*

Abstract: ***Denial of service (DoS) or distributed denial of service (DDoS) are usually deliberate attempts to eat up the victim's bandwidth or obstruct the use of services by authorized users. The traditional internet architecture is susceptible to DDoS attacks, giving an attacker the chance to set up attack networks or "Botnets" that provide them access to a huge number of infected computers. An attacker launches a massive, well-coordinated attack against one or more targets after setting up an attack network or botnet. Numerous DDoS attack Detection, Prevention, and Trace-back procedures have been proposed as a result of the ongoing development of new assaults and the expanding variety of vulnerable hosts on the internet.***
When a system is targeted by Distributed Denial of Service (DDoS) assaults for commercial monitoring typically involves many packets. They clog up the network, overburden the bandwidth, and overwhelm thousands of infected hosts. Due to DDoS, there is no effective leverage on the crucial support of infrastructure. This entirely mitigate the legitimate end users of the system resources. In this paper, we tend to examine several DDoS attack kinds, their methodologies, and related countermeasures. This paper also elaborates treatment of numerous DDoS assault defense strategies, including as detection, defense, and mitigation.
Keywords: DDoS, Cloud Network, Botnets, DoS, Attacks, DDoS Defense, Vulnerabilities

I. INTRODUCTION

A disruptive assault called denial of service might stop web servers' connectivity to the Internet. Such attacks expose cyber-security to severe danger by causing device flooding from various sorts of devices.

DDoS attacks come in a number of different forms. Pattern identification for attack detection normally happens in the specifics of the received packets during the application stage. The basic idea is the same regardless of the size of the onslaught. Overwhelm a server with requests that it cannot process. Do this repeatedly until it crashes or stops responding. Repairing service interruptions can frequently take hours and result in significant financial losses.

A DDoS attack on an intrusion detection system causes a massive influx of packets containing thousands of infected hosts, which severely limits data transmission. The victim system thus interferes with the ability to manage crucial infrastructure. A botnet is a group of tens of thousands of common malware-infected PC users that is created or employed by a criminal company. This is how a DDoS attack is currently structured. DDoS is a significant safety risk and a subject of ongoing research, but it is not a growing hazard. DDoS attacks pose a serious hazard to the various data center, and from 2003 to 2016, numerous protection measures were established. DDoS incursions have been reduced by dealing with the many relationships between different defenses and strategies. However, because of vastly enhanced software and infrastructures, this leads to incredibly sophisticated processes that are difficult to forecast and monitor. Through a review of the literature and a mapping analysis, we prepared to handle these problems by identifying gaps in the evaluation and use of these solutions.

Given the damage it causes to organizations' assets, the distributed denial of service (DDoS) assault has drawn a lot of attention in the computer security industry. The significant growth in computer access speed and internet user traffic, however, presents challenges.

II. PROCEDURE OF DDOS

DDoS attacks are large-scale coordinated internet attacks that are launched indirectly through a large number of compromised computers. By taking use of the resources of numerous uninformed assistant computers, the source attacker can dramatically increase the effectiveness of the Denial of Service by using client-server technologies.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

A group of machines (agents) launches a DDoS assault by sending packets to a victim host in response to instructions from a machine (master) under the attacker's control. The attacker commands master agents, who coordinate with him. agent slaves. More specifically, the attacker activates all attack processes on master agents by sending an attack order to those machines, causing them to awaken from their slumber state and begin attacking. Then, master agents direct slave agents to launch a DDoS assault on the target by sending attack commands to them via those processes. In this approach, the agent computers (slaves) start sending the target a lot of packets, overloading its system and using up all of its resources.

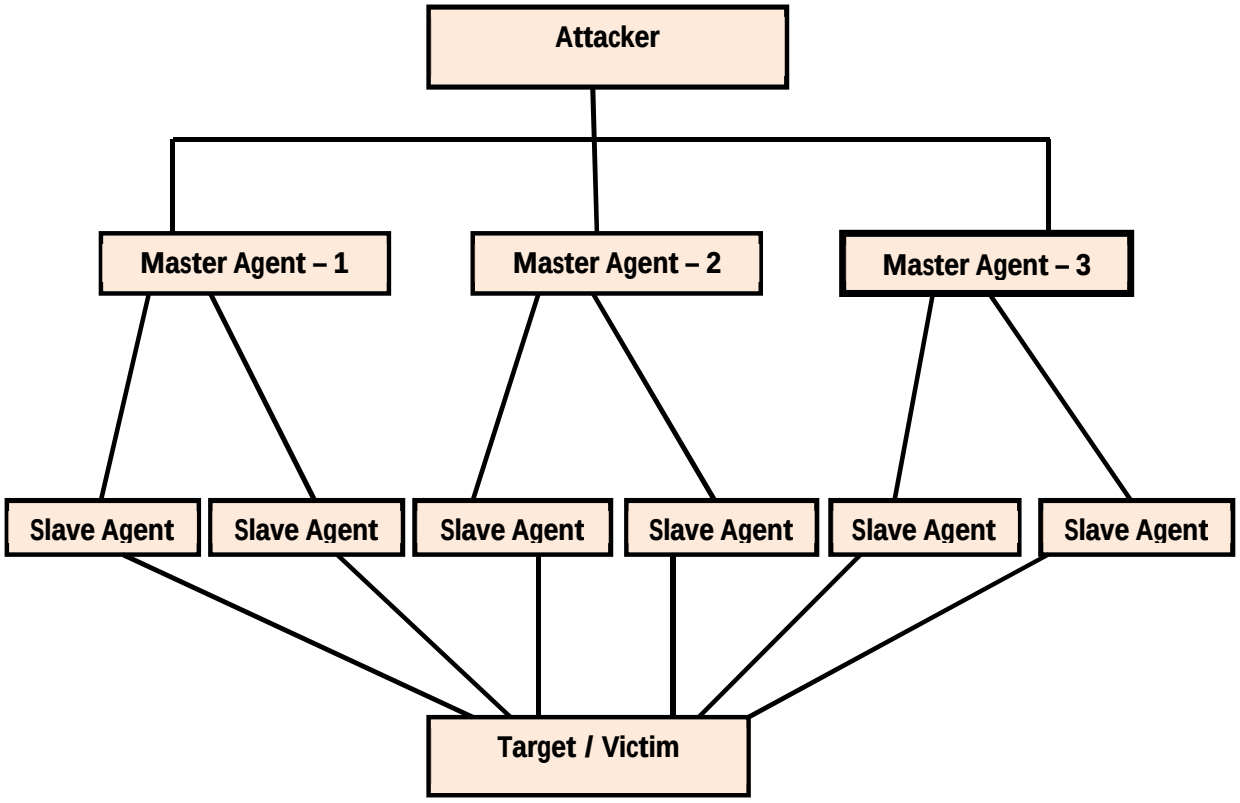


Fig. 1: A Typical DDoS Attack Structure

III. PURPOSE OF DDOS ATTACK

There could be many various reasons / intensions to launch DDoS attacks, however, we are briefly describing below some of the most important and prevalent DDoS attack types.

1) *Ransom:* This is most possible and frequent motive of attackers. DDoS attacks are generally followed by a ransom demand from the attacker. However, a ransom note that foreshadows an attack may occasionally also be sent.
2) *Business Quarrel:* DDoS assaults can be strategically used by business organizations to shut down rival websites and online activities.
3) *Cyber Warfare:* Government-approved DDoS assaults can be used to take down rival nation's infrastructure as well as opposition websites.
4) *Hacktivism:* This is an act of hacking to advance a political objective, particularly by damaging or taking down websites.
5) *Random Try:* DDoS attacks may also be result of random try by incompetent and amateur attackers.

IV. DDOS ATTACK TYPES

Hundreds of DDoS attacks have been reported so far around the world and the number is still increasing every day. Various techniques are being used to launch a DDoS attack. However, we can put all sorts of DDoS attacks under the following three broad categories.

1) *Volumetric Attack:* The goal is to overwhelm the target with traffic in order to exhaust hardware or network resources, with bandwidth being the primary concern. Flooding and amplification/reflection attacks fall under the category of volumetric attacks. Flooding attacks use high volumes of traffic to try and use up all available bandwidth, processing power, or other network resources **[1]**. In contrast, reflection attacks take advantage of spoofing flaws, where the attacker sends traffic to the target from multiple devices via forging requests **[2]**. Amplification attacks make modest requests that result in larger responses, such as repeatedly asking a Domain Name System (DNS) server for the entire DNS database and ultimately bringing down the DNS server. This type of attack includes UDP floods, ICMP floods and several other spoofed packets floods.
2) *Protocol Attack:* This type of threat aims to take advantage of holes in network protocols and devour connection state tables that some network devices create **[3]**. This includes SYN floods, Smurf DDoS, fragmented packet attacks, Ping of Death, and many more.
3) *Layer – 7 (Application Layer) Attack:* Application layer protocols like HTTP and SSL have vulnerabilities that are exploited. When secure coding guidelines are ignored, application code itself can be susceptible. Since there is no need to create a lot of traffic, these attacks are the too much hazardous. Attacks at the application layer are especially challenging to identify since they are covert and use legitimate traffic **[4]**. includes GET/POST floods, low-and-slow assaults, attacks on Apache, Windows or OpenBSD vulnerabilities, and many others.

V. LITERATURE REVIEW

Instead of the substance of the packets, the volume of packets used in DDoS attacks poses the biggest hazard. The degradation of common network protocols is the primary issue with these assaults. Modern network topologies have an issue with flooding DDoS attacks. We have studied more than 50 papers to analyze and find out some of the best prevention and detection techniques to discuss in this review paper.

P. Ferguson et. al (1998) proposed Network Ingress Filtering mechanism where a router does not accept any such packet whose source IP address is not defined [5]. The network is shielded from packets with fake sources thanks to ingress filtering. The firewalls that are a part of a network have an interface that is linked to both the internal and internet networks. Firewalls can stop an attacker from disguising their attack as a host on the same network by applying ingress filtering to the internet interface and dropping all packets with internal network source addresses.

A sort of filtering called egress filtering is used on packets from the internal interface that are leaving the network. The firewall rejects all n packets with source addresses that are not on the local network during egress filtering. Applying these techniques to the network will aid in thwarting DDOS attacks that employ IPspoofing.

TFN does not provide encryption between the attacker and masters or between the master and slave programs; instead, it uses a command line interface to facilitate communication between the attacker and the control master program [6]. Using ICMP echo reply packets, the control masters and slaves communicate with one another. Attacks like Smurf, SYN Flood, UDP Flood, and ICMP Flood can be implemented.

Jin et al (2003), acknowledged the ability of attackers to spoof any byte in a packet [7]. The time-to-live (TTL) field, on the other hand, is more challenging to forge; as a result, forged packets are more likely to travel through fewer hops than those from authentic networks. As a result, the authors developed a method to determine the TTL values of packets from real networks, and the system only accepts packets from sources with the predicted TTL value (s). However, this mitigation mechanism does not guarantee the false positive/negative rates, for instance, it cannot account for circumstances like route alterations.

Low rate DDoS attacks are the most devastating kind of attack, according to

Yang Xiang (2011) [8]. To identify the low frequency ddos assaults, two new approaches, generalized entropy and information distance approaches, are taken into consideration. In this study, Shannon entropy and the Kullback-Liebler distance were also examined and compared to the novel techniques. To increase the detection rate, the generalized entropy and information distance metrics' alpha values were modified.

It would be simple to distinguish between authentic traffic and typical traffic with the aid of these two new metrics. In the end, the attacker's source is discovered using the IP trace back approach. By looking at the attacker, this technique can be used to interrupt the attack. Therefore, this research demonstrates how the suggested technique is used to identify attack-related low-rate traffic and further lower the attack rate.

Saman Taghavi (2013) discussed DDOS flooding assault because it is a difficult problem to prevent in terms of network security [9]. In this kind of assault, forces are prepared to attack. An attacker hires a variety of computers, sometimes known as zombies or botnets. All hired computers engage in a coordinated attack. To stop DDOS flooding attacks, the proper defense system is needed.

This essay's goal is to learn more about DDOS flooding issues and the different solutions available. The study is concerned with taking into account prior defenses against DDOS Flooding attacks. The primary goal of this study is to provide a survey of classic and modern handling techniques

IlkerOzcelik (2013) elaborated the method for detecting Denial of Services [10]. The detection is based on metrics that account for anomalies. To determine how the assault has affected the network, the Cumulative Sum (Cusum) technique has been used. This method operates both in networks with high and low bandwidth. The major goal of this work is to demonstrate how the cusum algorithm produces superior detection results while using less network resources. The background traffic from the scenario in the article was used to complete the entire project.

A pattern of matching detection strategy has been put up by Ahmad Sanmorino (2013) as a means of overcoming the limitations of the previous DDoS assault detection methods [11]. Traffic passing across the network is examined based on the predetermined pattern, making it simple to determine whether a packet is malicious or not. Since this method of detection simply uses already-existing routers and switches, it has the advantage of requiring less infrastructure. It does not make advantage of cutting-edge equipment like multi-core CPU technology. In this study, three topological environments with three phases are illustrated.

Hu et al (2013), presented a Distributed IDS System [12] The network attack is discovered by this IDS method using Event Processing Engine. The components of this engine include a sub-controller, an event bus, an event channel, and hyper-controlled The hyper-responsibility controller's is to synchronize the sub-controller and identify any malicious traffic flow that was buffered from an event channel and forwarded via the event bus. Skowyra [13] put out a Learning-IDS that is based on the programmable (SDN) nature of the technology and has the adaptability to alter network state in response to harmful intent.

Giotis et al. (2014), adopted a popular entropy-based strategy to successfully identify DDoS, port-scan assaults, and worm propagation [14]. The flow-related traffic attributes that are used to identify anomalies include the source and destination IP addresses as well as the source and destination ports. Predetermined thresholds on changes in the entropy values have been utilized to detect the presence of abnormalities.

Belyaev et al. presented a new Load Balancing technique to increase the server's period of survival in the face of a DDoS attack [15]. The load balancing algorithm begins to take precedence over the routing table when the server is under attack. To distribute the assault traffic, the Bellman-Ford method is utilized to define the shortest pathways routes to the endpoint servers.

Masdari et al. (2016), studied DDoS attack types with new attacks on virtual machines and hypervisors in the cloud computing environment [16]. The authors also include popular network defensive strategies and cloud computing defenses against DDoS attacks.

VI. CONCLUSION

Many studies are being conducted to develop defenses against the various DDoS attacks. However, despite the development of technology and effective security measures, DDoS attacks still cannot be stopped. Instead, the attackers are increasing the attacks' size and frequency over a range of dimensions. The researchers will determine the underlying cause of any new threat or attack that occurs in the world as well as solutions to prevent them. According to current study, the fundamental problem with not being able to stop new DDoS attacks is that there is insufficient support amongst various network nodes. This is because Internet (networks of networks) prevents widespread implementation of global collaboration. It will be difficult to apply new preventive measures internationally due to socioeconomic difficulties. Because DDoS attacks are spread in nature and attackers employ many networks, it cannot be accomplished by deploying defensive mechanisms in a single network. Setting up effective audit and accountability on the internet at large can enhance the DDoS attack detection mechanism, however this is not feasible in the actual world.

REFERENCES

[1] S.T. Zargar, J. Joshi, D. Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks”, IEEE Communications Surveys & Tutorials, 15 (4) (2013), pp. 2059-2068, 10.1109/SURV.2013.031413.00127

[2] D. Dittrich, “The Tribe Flood Network Distributed Denial of Service attack tool,” University of Washington, October 21, 1999. Available at: http://staff.washington.edu/dittrich/misc/tfn.analysis.txt

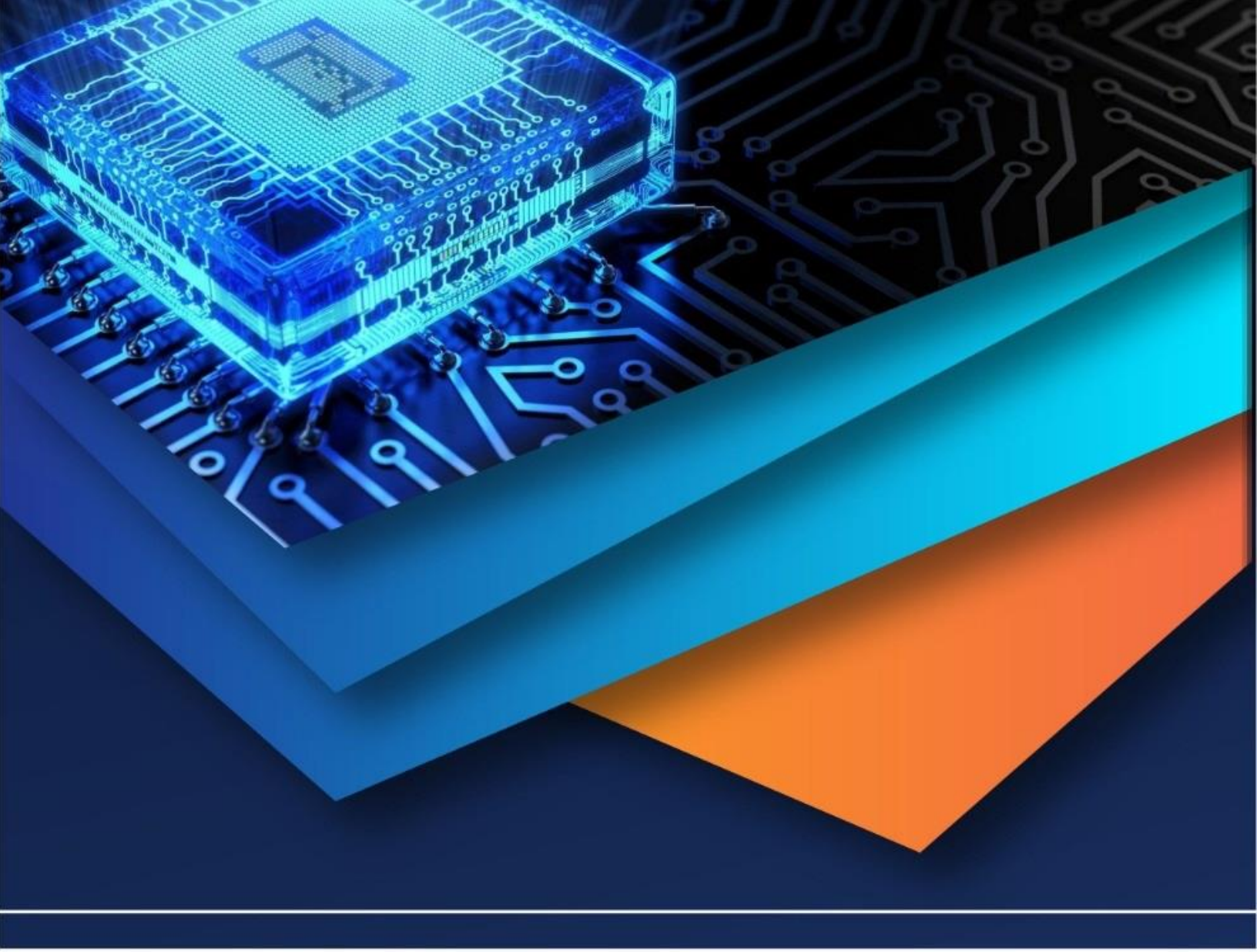
[3] A. Furfaro, G. Malena, L. Molina, A. Parise, “A Simulation Model for the Analysis of DDoS Amplification Attacks” Conference on Modeling and Simulation (2015), pp. 266-273

[4] K.S. Bhosale, M. Nenova, G. Iliev, “The Distributed Denial of Service attacks (DDoS) prevention mechanisms on application layer”, Conference on Advanced Technologies, Systems and Services in Telecommunications, IEEE (2017), pp. 136-138

[5] A. Praseed, P.S. Thilagam, “DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications**”,** IEEE Communications Surveys & Tutorials, 21 (1) (2019), pp. 668-679, 10.1109/COMST.2018.2870658

[6] P. Ferguson et. al., “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, Technical report, The Internet Society, 1998.

[7] Cheng Jin, Haining Wang, and Kang G. Shin. 2003. Hop-Count Filtering: An Effective Defense against Spoofed DDoS Traffic. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03), 30–41. doi: 10.1145/948109.948116.
[8] Yang Xiang, Ke Li, and Wanlei Zhou, Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011
[9] Saman Taghavi Zargar, Joshi, Member, IEEE, and David Tipper,A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION (2013)
[10] Ilker Ozcelik, Yu Fu , Richard R. Brooks ,DoS Detection is Easier Now, 2013 Second GENI Research and Educational Experiment Workshop.
[11] Ahmad Sanmorino1, Setiadi Yazid2, DDoS Attack detection method and mitigation using pattern of the flow,2013 International conference of Information and communication technology(ICoICT)
[12] Y.-L. Hu and W.-B. Su, "Design of Event-Based Intrusion Detection System on OpenFlow Network," in 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2013.
[13] R. Skowyra, "Software-Defined IDS for Securing Embedded Mobile Devices," in IEEE High-Performance Extreme Computing Conference (HPEC), 2013.
[14] Giotis A, Ahmed L**., "**A Source-end Defence against flooding denial of Service Attacks", In IEEE Transactions on Dependable and Secure Computing", Vol. 2, pp. 219-228, 2014.
[15] Masdari, M.; Jalali, M. "A survey and taxonomy of DoS attacks in cloud computing. Security. Commun. & Networking", **2016**, 9, 3724–3751; SCN-15-0746.R1.
[16] M. Belyaev and S. Gaivoronski, "Towards Load Balancing in SDN-Networks During," in International Science and Technology Conference (Modern Networking Technologies) (MoNeTeC), Moscow, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY