iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48673

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 11 Issue I Jan 2023- Available at www.ijraset.com

Literature Review of Distributed: Denial of Service Attack Protection

Raj Kumar Patel[1], Dr. Lalan Kumar Singh[2], Dr. Narendra Kumar[3]
[1]*Research Scholar, Magadh University, Bodh-Gaya*
[2]*Associate Prof. Dept. of Mathematics, K.S.M. College, Aurangabad (Bihar)*
[3]*Dept. of Computer Science, UMC, Raigarh (C.G)*

Abstract: ***In the current environment, cloud computing has developed into a commercial technology that enables users to quickly access resources via the internet on a pay-per-use basis. The customer receives these resources in the form of services. The three service models offered by the cloud services are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). As a result of the enormous improvement in cloud computing technology, it is now widely employed by a variety of business applications, industry apps, Enterprise organizations that have committed to multi-cloud designs, and most IT expenditures are based on the cloud.***

However, security is the main issue that requires more attention. Recent research indicate that resource availability is the main security issue that cloud users must deal with. The distributed denial of service attack is the main cause of this availability problem. A more advanced form of denial of service is the Distributed DoS assault.

It is used by everyone to share knowledge, not just researchers. Therefore, the internet is used to transmit all information to any location in the world. As a result, the internet needs to be more dependable, secure, and safe. The number of attacks has increased exponentially with the growth of the internet. Among all attacks, DDOS is the most upsetting and intensive attack for reducing the network's resource or bandwidth. In this study, we will look at various DDoS attack types, their tactics, and associated defences. The treatment of several DDoS attack defence tactics, such as detection, defence, and mitigation, is explored in this study as well.

Keywords: Distributed-DoS, Cloud Network, DoS, IaaS, PaaS, SaaS, Cyber Attack Vulnerabilities;

I. INTRODUCTION

For many of the applications, computer network technology may be crucial. Security is therefore crucial for these applications. There aren't many security measures that can be quickly put into place, despite the fact that network security is a major requirement in expanding networks.

Since there is a communication gap between those who develop network security technologies and those who develop networks, there are various gaps in network security. An established procedure, network design is mostly based on the Open System Interface (OSI) model. The OSI model has several benefits for network architecture. The OSI paradigm provides flexibility, modularity, usability, and protocol standardization.

Any attempt to jeopardize the security of the data held by any organization is considered a security attack. There are numerous classifications for these attacks. Some of the assaults aim to discover system or personnel knowledge. Other assaults are employed to obstruct the system's intended operation. Some attacks employ the system's resources to their fullest potential. Security breaches can be divided into active and passive attacks.

It is simple to integrate the protocols that are used at various OSI model layers to build a stack that enables module creation. The OSI model's individual layer implementations can be altered later on without requiring additional changes, giving network development flexibility. Secure network design is a less developed method than network design in general. For managing the complexity of security requirement complexity, there is no established methodology. Secure network design does not have the same benefits as regular network design. The importance of the network as a whole being secure must be emphasized while thinking about network security.

While transmitting the data, the communication route between the two parties shouldn't be exposed to security breaches. The network's middle attacker might assault the communication channel, steal the data, decode the information, and then re-insert the fake message.

©IJRASET: All Rights are Reserved

Denial of service attacks have the potential to disconnect web servers from the Internet. Such attacks result in device flooding from many types of devices, which poses a serious threat to cyber security.

DDoS assaults can take many different shapes. In the course of the application stage, pattern identification for attack detection often takes place in the specifics of the received packets.

No matter how large the bombardment, the fundamental concept remains the same. overburden a server with requests that it is unable to handle Repeat this until it crashes or becomes unresponsive. It can commonly take hours to repair service outages, which can cost a lot of money.

Data transmission is severely constrained by a DDoS attack on an intrusion detection system, which results in a tremendous influx of packets carrying thousands of infected computers. As a result, the victim system makes it difficult to handle essential infrastructure.

A botnet is a collection of tens of thousands of commonly infected PC users who are being used or produced by a criminal organization. A DDoS attack is currently organized in this manner. Although DDoS poses a serious safety risk and is the topic of continuous research, it is not a threat that is becoming worse.

DDoS attacks are a severe risk to different data centers, and from 2003 to 2021, many safety precautions were put in place. By managing the complex interactions between many defenses and techniques, DDoS invasions have been decreased. However, this results in very complex processes that are challenging to predict and keep track of because of greatly improved software and infrastructures. We prepared to address these issues by identifying gaps in the assessment and application of these solutions through a review of the literature and a mapping analysis.

II. DEFINING DISTRIBUTED DENIAL-OF-SERVICE ATTACK

Distributed – DdoS Attack is a sort of attack in which the perpetrator multiplies the influence of an attack resulting from a significant number of computer agents on the victim. Before assaulting, the attacker has remote access to a sizable number of computers. By using hacking techniques or malicious code insertion, the attacker takes advantage of these computers' vulnerabilities to take over and control them. Typically, these machines are referred to as zombies. The phrase "botnet" refers to the zombie collective.

The size of the botnet determines how powerful the attack will be. The attack will be more devastating and severe the larger the botnet. In a botnet, the attacker chooses handlers who carry out control tasks and relay all instructions to the zombies as well as information about the victim that they learn from the zombies. Each handler is accompanied by a group of zombies, and these handlers interact with both the zombies and the attacker**[1]**.

Zombies and handlers are computers from the public network, but the users of these computers are unaware that they are part of a botnet. A DDOS attack launches an attack using numerous computers. A coordinated DOS assault is launched by the attacker against one or more target systems. By utilizing many unaware PCs as the attack's platform, the attacker attempts to maximise the impact of the DOS by exploiting client-server technologies. One of the PCs using the stolen account has the most crucial DDOS main application loaded.

The master software connects with any number of applications installed on various computers located in various locations that serve as agents at a specific time. The agent launches the attack after receiving the order. The primary software placed on a certain machine can quickly start hundreds or thousands of agents programmes using client-server technology.

III. MECHANISM OF DISTRIBUTED – DOS ATTACKS

A huge number of compromised computers are used to launch DDoS assaults, which are coordinated large-scale internet attacks. Using client-server technologies, the source attacker can significantly boost the effectiveness of the Denial of Service by utilizing the capabilities of several ignorant assistant computers.

When given orders from a machine (master) under the attacker's control, a set of machines (agents) conducts a DDoS attack by sending packets to a victim host. Master agents under the attacker's control collaborate with him. agent servants More specifically, the attacker sends an attack order to those machines, forcing them to awaken from their resting state and start attacking. This activates all attack processes on master agents.

Then, master agents send attack commands to slave agents via those processes, instructing them to conduct a DDoS assault on the target. The target is bombarded with a large number of packets from the agent computers (slaves) in this method, overloading the target's system and exhausting all of its resources.

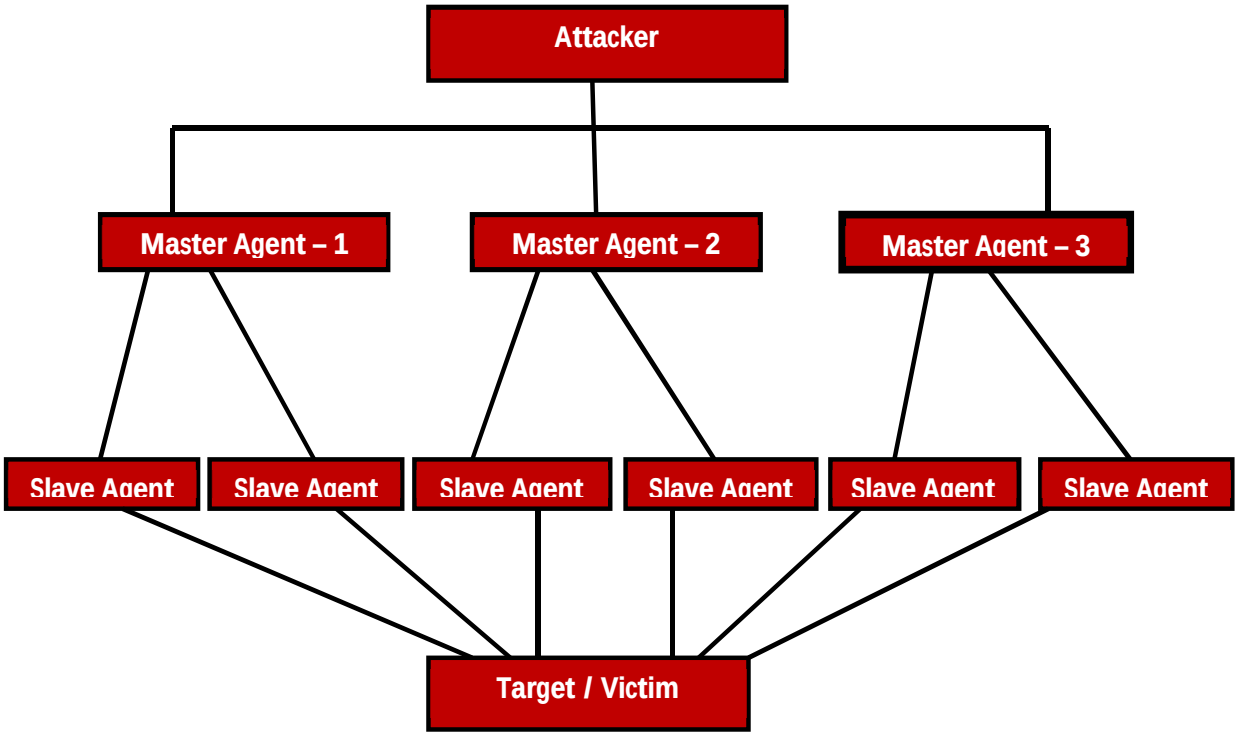


Fig. 1: A Common DDoS Attack Architecture

IV. MAIN MOTIVE BEHIND THE DDOS ATTACKS

Although there may be a wide range of motivations or intentions behind DDoS assaults, we have included some of the most significant and common attack types below.

1) *Ransom:* This is the most likely and frequent reason for attacks. DDoS attacks typically end with the attacker demanding a ransom. However, occasionally a ransom note that announces an attack will also be delivered.
2) *Business Revelry:* DDoS assaults can be strategically used by business organizations to shut down rival websites and online activities.
3) *Cyber Warfare:* Business companies might use DDoS attacks strategically to halt competing websites and online operations.
4) *Hacktivism:* DDoS attacks could also be the outcome of a careless attempt by novice or inexperienced attackers.

V. OUTLINING VARIOUS TYPES OF DDOS ATTACK

DDoS attacks have already been reported in their hundreds in various parts of the world, and the number is rising daily. A DDoS attack is launched using a variety of methods. However, the following three broad categories can be used to group all types of DDoS attacks.

1) *Volumetric Attack:* With bandwidth being the main concern, the objective is to flood the target with traffic in order to deplete hardware or network resources. Volumetric attacks consist of flooding and amplification/reflection attacks. High traffic quantities are used in flooding attacks to attempt to exhaust all available processing power, bandwidth, or other network resources [2]. In contrast, reflection attacks prey on spoofing weaknesses by faking requests to deliver traffic to the target from many devices [3].
2) *Protocol-Attack:* This kind of threat seeks to eat connection status tables produced by some network devices and exploit vulnerabilities in network protocols **[4].** This includes SYN floods, Smurf DDoS, attacks using fragmented packets, Ping of Death, and numerous other attacks.
3) *Application-Layer Attack:* HTTP and SSL are examples of application layer protocols with flaws that are exploited. Application code may be exposed when secure coding standards are disregarded. These attacks are extremely dangerous because there is no need to generate a lot of traffic. Because they are stealthy and employ genuine traffic, attacks at the application layer are particularly difficult to detect **[5],** contains GET/POST floods, slow-and-slow attacks, Apache attacks, Windows or OpenBSD vulnerabilities, and numerous other attacks.

VI. LITERATURE REVIEW

The largest risk associated with DDoS assaults is the volume of packets used, not the content of the packets themselves. The main problem with these attacks is the deterioration of standard network protocols. Flooding DDoS attacks are a problem for contemporary network topologies. In order to analyse and select some of the top prevention and detection strategies to discuss in this review paper, we read more than 45 papers in total.

1) P. Ferguson et. al (1998) router does not accept any such packets whose source IP address is not specified, according to Andrew's suggested Network Ingress Filtering technique [6]. Ingress filtering protects the network from packets having fictitious sources. A network's firewalls have an interface that connects to both the internal network and the internet. By applying ingress filtering to the internet interface and discarding any packets with internal network source addresses, firewalls can prevent an attacker from passing as a host on the same network throughout their attack. On packets from the internal interface that are leaving the network, an egress filtering technique is utilised. During egress filtering, the firewall rejects all n packets with local network-incompatible source addresses. Utilizing these methods on the network will help prevent DDOS assaults that use IPspoofing.

2) Jin et al (2003), proposed that attackers can spoof any byte in a packet [7]. On the other hand, the time-to-live (TTL) field is more difficult to counterfeit, therefore forged packets are more likely to traverse through fewer hops than those from genuine networks. Since the system only accepts packets from sources with the anticipated TTL value, the authors created a mechanism to determine the TTL values of packets from real networks (s). This mitigation technique, however, cannot take into account things like route changes, therefore it cannot guarantee the false positive/negative rates.

3) TFN employs a command line interface to make communication between the attacker and the control master programme easier rather than provide encryption between the attacker and masters or between the master and slave programmes **[6]**. The control masters and slaves communicate with one another using ICMP echo reply packets. It is possible to use attacks like Smurf, SYN Flood, UDP Flood, and ICMP Flood.

4) Low rate DDoS attacks are the most harmful sort of attack, claims Yang Xiang (2011). Two novel methods—generalized entropy and information distance approaches—are taken into account to detect low frequency D-DoS attacks [8]. Additionally investigated and contrasted with the novel methodologies in this study were the Shannon entropy and the Kullback - Liebler distance. The alpha values of the generalized entropy and information distance metrics were changed to improve the detection rate. These two additional indicators would make it easy to discern between real traffic and regular traffic. In the end, the IP trace back method is used to identify the attacker's origins. This method allows you to stop an attack by focusing on the attacker. In order to identify attack-related low-rate traffic and further reduce the attack rate, this research shows how to implement the suggested technique.

5) Ilker Ozcelik (2013), the technique for identifying Denial of Services was elaborated by Ilker Ozcelik. [9]. Metrics that take anomalies into consideration are used for the detection. The Cumulative Sum (Cusum) technique has been used to assess the impact of the attack on the network. This technique works in both high- and low-bandwidth networks. This work's main objective is to show how the Cusum algorithm achieves better detection outcomes while utilizing less network resources. The project was completed using the background traffic from the scenario in the article.

6) Saman Taghavi (2013) Because DDOS flooding assault is a challenging issue to prevent in terms of network security, Saman Taghavi examined it [10]. These assaults involve forces that are ready to strike. A multitude of machines, frequently referred to as zombies or botnets, are employed by the attacker. A coordinated attack is launched by all employed computers. DDOS flooding attacks must be prevented with the right protection technology. The purpose of this essay is to provide readers with more knowledge about DDOS flooding problems and several solutions. Regarding earlier countermeasures against DDOS Flooding attacks, the study is worried. This study's main objective is to give a survey of traditional and contemporary handling methods.

7) To get over the drawbacks of the earlier DDoS assault detection techniques, Ahmad Sanmorino (2013) proposed a pattern of matching detection mechanism [11]. It is straightforward to tell whether a packet is malicious or not since network traffic is inspected based on the established pattern. This method of detection has the benefit of having less infrastructure because it merely uses pre-existing routers and switches. Innovative technology, like multi-core CPU technology, is not utilized. Three topological settings with three phases are shown in this work.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

8) Giotis et al. (2014) successfully identified DDoS, port-scan attacks, and worm propagation by using a well-liked entropy-based approach [12]. The source and destination IP addresses as well as the source and destination ports are flow-related traffic parameters that are utilized to spot irregularities. In order to identify abnormalities, thresholds on changes in the entropy values have been used.

9) Distributed IDS System was presented by Hu et al. in 2013 [13]. Using an event processing engine, this IDS technique finds the network attack. A sub-controller, an event bus, an event channel, and hyper-controlled logic are some of the parts of this engine. Synchronizing the sub-controller and spotting any fraudulent traffic flow that was buffered from an event channel and sent across the event bus are the duties of the hyper-responsibility controller. Based on the programmable (SDN) aspect of the technology, Skowyra [14] released a Learning-IDS that has the adaptability to change network state in response to malicious intent.

10) In the context of the cloud computing environment, Masdari et al. (2016) examined DDoS attack types with new attacks on virtual machines and hypervisors [15]. The authors also include well-known network protection techniques and cloud computing DDoS defenses.

VII. CONCLUSION

In order to provide defences against the various DDoS attacks, numerous studies are being done. However, despite advances in technology and strong security measures, DDoS attacks continue to occur. Instead, the attackers are expanding the size and frequency of the strikes across a variety of dimensions. Any time a new threat or attack materialises, researchers will work to identify its root cause and develop remedies to stop it. According to recent research, the main reason why new DDoS attacks can't be stopped is that there isn't enough support across different network nodes.

This is due the Internet (networks of networks) preventing the widespread adoption of international cooperation. Due to socioeconomic challenges, it will be difficult to implement new preventive measures internationally.

Defensive methods cannot be implemented against DDoS attacks since they are dispersed in nature and attackers use multiple networks. The DDoS assault detection method can be improved by setting up efficient audit and accountability on the internet as a whole, however this is not practical in real life.

REFERENCES

[1] L. Zhang, S. Yu, D. Wu and P. Watlers, “A Survey on Latest Botnet Attack andDefense”, In Proceedings of 10th International Conference on Trust, Security andPrivacy in Computing and Communications, IEEE, pp. 53-60, 2011.

[2] 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

[3] 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

[4] 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

[5] 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

[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] Ilker Ozcelik, Yu Fu , Richard R. Brooks ,DoS Detection is Easier Now, 2013 Second GENI Research and Educational Experiment Workshop.

[10] 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)

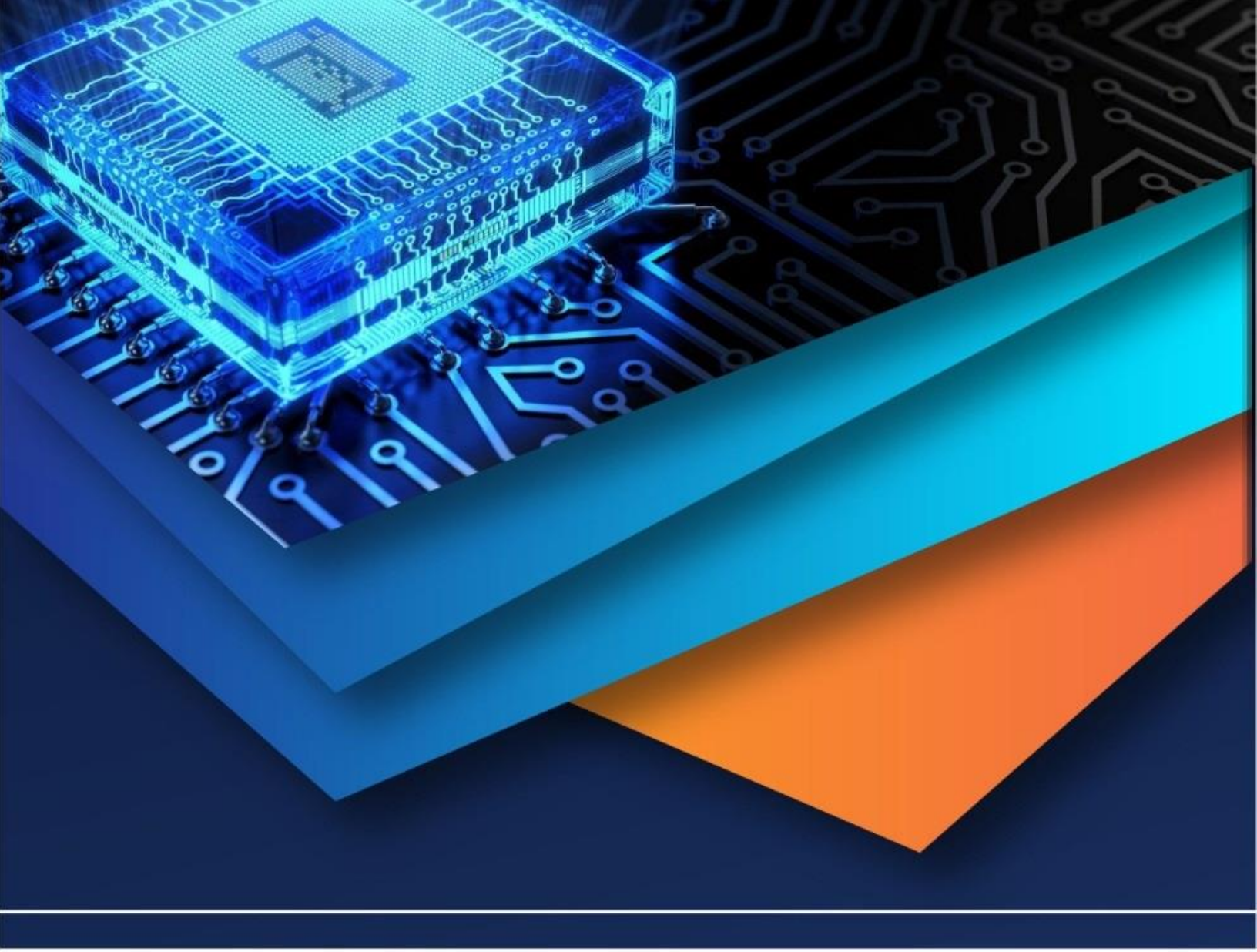
[11] Ahmad Sanmorino1, Setiadi Yazid2, DDoS Attack detection method and mitigation using pattern of the flow,2013 International conference of Information and communication technology(ICoICT)

[12] 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.

[13] 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.

[14] R. Skowyra, "Software-Defined IDS for Securing Embedded Mobile Devices," in IEEE High-Performance Extreme Computing Conference (HPEC), 2013.

[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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)