A Survey on DDoS Detection and Prevention Mechanism

Foram Suthar [1,] * and Nimisha Patel [2]

[1] Indus University, Ahmedabad, India
[2] Gandhinagar Institute of Technology, Gandhinagar University, Gandhinagar, India
*Correspondence: foramsuthar@outlook.com (F.S.)

***Abstract*—The internet is an obvious target for a cyberattack nowadays. The population on the internet globally is increasing from 3 billion in 2014 to 4.5 billion in 2020, resulting into nearly 59% of the total world population. The attacker is always looking for loopholes and vulnerabilities of internet-connected devices. It has been noticed from the last decade, there are more Denial-of-Service Attack (DoS) or DoS attacks and their variant Distributed Denial-of-Service (DDoS) or DDoS attacks performed by the attacker. This creates a serious problem for the network administrator to secure the infrastructure. The attacker mainly targets reputed organization/ industries and try to violate the major parameter of cyber security—Availability. The most commonly performed attack by the attacker is a Transmission Control Protocol (TCP) Synonym (SYN) DDoS attack, caused due to the design issue of the TCP algorithm. The attacker floods the packets in the network causing the server to crash. Hence, it is important to understand the source of the DDoS attack. Therefore, a real-life and accurate TCP SYN detection mechanism is required. Numerous techniques have been used for preventing and detecting various DDoS flooding attacks, some of which are covered in the literature review. The paper highlights the strengths and weaknesses of the available defense mechanism. To understand the performance status of the system we have implemented a DoS by the hping3 tool. This gives us better clarity in shortlisting and analyzing the parameters for the detection of DDoS attacks. Also, we try to analyze the impact of TCP SYN attack on the network in DDoS attacks.**

***Keywords*—Distributed Denial-of-Service (DDoS) attack, Transmission Control Protocol (TCP) Synonym (SYN), packet sniffer, detection mechanism, DDoS prevention, hping3, DDoS prevention and detection survey**

I. Introduction

The internet revolution has changed everything. As per the research, the United State household now has 5.7 internet-connected devices, and most of these are smartphone, laptops, and tablets which always comes with vulnerabilities. The cyber-attacks are the exploitation of those vulnerabilities. Cyber-attacks are a set of instructions performed by unauthorized or external person to extract and collect the information of the organizations. Cyber-attacks are on the rise and may reach 10.5 trillion dollars' worth by 2025. Cyberattacks happen on an average every 39 seconds. As former Director of the FBI Robert S. Mueller said in his 2012 speech at the RSA Cyber Security Conference, "there are only two types of companies: those that have been hacked and those that will be". Cyberattacks are predicted to cost more than $10 trillion globally, growing by 15% annually. In the United State, a data breach typically costs $3.8 million to remediate. Public corporations lose, on average, 8% of their stock value following a successful breach, which is another worrying fact. The "Melissa Virus" was the very first cyber-attack which has been performed by the programmer David Lee Smith. As per the Common Vulnerabilities and Exposures, DoS or Denial-of-Service attacks and their variant DDoS or Distributed Denial-of-Service attacks are mostly performed by the attacker and creates serious issues for the network administrator. The attacker mainly targets reputed organization or industries and try to violate one of the major parameters of cyber security—Availability. Such attacks are aimed to utilize the resources like CPU, Memory, and Network Bandwidth.

An attack categorized as a DoS attack not only affects all type of enterprises comprising of all sizes, at all locations but also attack from all sectors (e-gaming, Banking, Government, etc.). Such attacks reflect hackers' frustratingly high levels of creativity and tenacity—this creates difficult and dynamic challenges for anyone responsible for cyber security. History suggests the DoS attack occurred in 1974 for the first time, because of David Dennis—a high school student who was just 13-year-old. CERL was just across the street from his residence at the University of Illinois Urbana-Champaign. Although the large-scale DDoS attack took place in Aug'99, the hacker applied "Trinoo"—a tool to restrict the computer network of the University of Minnesota for more than two days. The DoS attack completed its 40th anniversary in the year 2014 [1].

A. Motivation

The encouragement behind such research is the rapid increase in DDoS attacks. As per NETSCOUT's report during the COVID-19 pandemic situation, DDoS crosses the 10 million attack threshold. According to the security engineering team of NETSCOUT [2], nearly 2.9 million

Manuscript received October 8, 2022; revised November 2, 2022; accepted November 28, 2022; published May 15, 2023.

DDOS attacks were introduced in the first quarter of 2021 which was 31% more as compared to 2020 [3]. E-commerce, online learning, and healthcare industries are highly targeted by an attacker during the pandemic. Around 53% of DDoS attack has been increasing year over year. As per the Kaspersky analysis, most DDoS attacks were directed at US-based resources (36%) followed by China (10.28%) [3]. Table I shows a list of the most prominent DDoS attacks in June 2022. As per the data, many finance, energy, government, and entertainment sectors are targeted by the attacker.

TABLE I. WORLDWIDE DDOS ATTACK DURING THE MONTH OF JUNE 2022

Date of attack	Country	Industry	Downtime	Company Affected	Attack Details
June 27	Israel	Finance Sector	Not Mentioned	Israel's Banking Site	The denial of services attack performed at all banks sites including Bank of Israel. The intensity of the attack was 200 megabytes per second which slowdown all the sites.
June 26	UK	ISP	7 Days	Zzoomm	The attack, which was launched by a hostile party to extort money, swamped the network and disrupted service for users.
June 11	Puerto Rico	Power Distribution Company	Not Mentioned	Luma Energy	The attack affected user's ability to access account information by generating 2 million hits each second.
June 6	Spain	Cryptocurrency	24 Hours	zkSNACKs	User's addresses were exposed during the DDoS attack on the Wasabi bitcoin wallet to arbitrary outside servers.
June 4	Germany	Information Technology Sector	24 Hours	Fiducia & GAD IT AG	The attack targeted over 800 cooperative banks across Germany and shutting down or slowing websites.
June 1	USA	Gaming	Not Mentioned	Respawn Entertainment	The attackers overwhelm the Apex Legend game's server by sending a massive flood of internet traffic which cause server offline.
June 1	USA	Video Game	144 Hours	Blizzard Entertainment	High latency and disconnections were caused by crippled servers at the release of the well-known video game "Burning Crusade Classic."

Multiple investigations have been done in DDoS detection and prevention research. Kshirsagar and Kumar *et al.* [4] uniquely proposed a feature reduction method that combined the Correlation (CR) feature and Information Gain (IG) selection techniques. Gaurav and Gupta *et al.* [5] tried discriminating between DDoS attack data and regular communication with statistical and Machine Learning (ML) techniques and achieved a 92.8% accuracy rate. Kebede and Tiwari *et al.* [6] worked to defend brute force SSH, brute force File Transfer Protocol (FTP), Heartbleed, infiltration, Transmission Control Protocol (TCP) Synonym (SYN), User Datagram Protocol (UDP), and Hypertext Transfer Protocol (HTTP) with port scan attacks. The author has proposed a DDoS prevention mechanism considering various parameters such as Throughput, Prescriber's Digital Reference (PDR), End-to-End Delay, and NRL. Zeng and Peng *et al.* [7] have introduced a framework for DDoS detection to solve the problem of false associations, based on causal reasoning. Liu *et al.* [8] have implemented two levels of the DDoS detection method based: Information Entropy and DL. Zewdie and Girma *et al.* [9] attained simultaneous evaluation in detecting DoS and DDoS using investigation and proposing a framework for different ML methods. Saha and Priyoti *et al.* [10] used research work to conduct a comprehensive analysis using both ML and DL models, the UNSW-NB15 dataset for evaluating the performance of different FS techniques in DDoS attack classification. Dwivedi and Vardhan *et al.* [11] used GOIDS which is a hybrid algorithm of grasshopper optimization algorithm (GOA) with ML algorithm. This approach can distinguish between legitimate and malicious traffics, and it is based on creating an Intrusion Detection System (IDS) to fulfill the requirements of the monitored environment. Basicevic and Blazic *et al.* [12] Investigates the detection of DoS attacks with some possibilities for the use of the Principal Component Analysis (PCA) algorithm in it. Balaji and Reddy *et al.* [13] have proposed their scheme to tackle Domain Name System (DNS) DoS and DDoS attacks using Hidden MARKOV model (HMM). Thus, an AI-based DDoS detection model can be helpful to prevent the organization at an early stage. Therefore, to emphasize the impact of the researchers in the field of Machine learning, the article is made to detect TCP SYN DDoS attacks as early as possible.

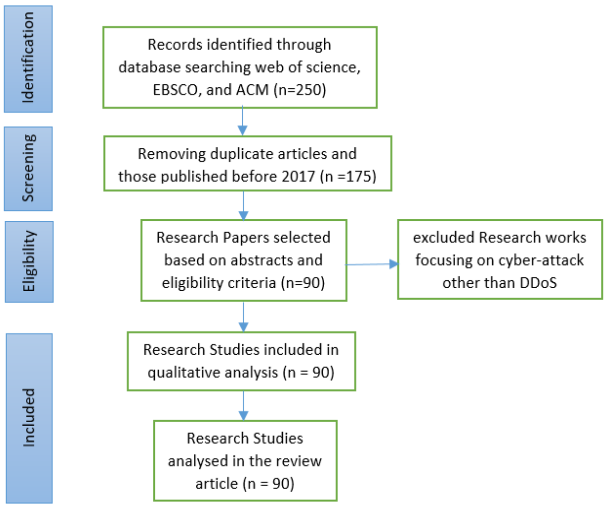

Figure 1. PRISMA flowchart.

B. *Literature Shortlisting Process*

A systematic review was conducted using PRISMA guidelines. For selecting research articles efficiently, the use of various electronic databases, i.e., EBSCO, IEEE, the web of science, ACM, etc. was done. The complete content or metadata of scholarly writings is openly available on the above-mentioned indexes. The selection of the articles was done on basis of the queries—(DDoS attack) or (TCP SYN Flood Attack) or (Early Detection) or (ML) or (Early Prevention). Fig. 1. Presents the PRISMA flowchart which depicts how the screening of the collected papers has been done, in detail. The published articles between 2017 to April 2021 are included in this survey, covering a total of 250 studies. 175 unique studies were shortlisted after removing the duplicate ones. The studies which focused on the detection and prevention mechanism of DDoS attack, TCP SYN flood attack, and cyber-attack was shortlisted, and the list of studies was reduced to 90.

Investigations:

Analysis 1: To predict the outcome, which Learning Approach has been used?

Analysis 2: Which training dataset of DDoS attack has been utilized extensively?

Analysis 3: The number of case-studies published related to DDoS attack were maximum in which year?

Analysis 4: What are the different categories of DDoS attacks performed at network layer?

Analysis 5: What are the various existing detection mechanisms against DDoS attack?

C. Contribution and Structure of Paper

We piloted a far-reaching survey of the entropy-based and ML models proposed in DDoS research. A proportional study of the existing research works is highlighted in the paper, which used different detection techniques for the network layer, application layer, and transport layer DDoS attack. The majority of the methods proposed in the different papers were based on the ML model and provides relevant likelihood outcomes. This paper explains the DDoS attack, the impact of DDoS attacks at a different layer, and the limitations of the existing algorithm. Also, we have implemented three different DDoS attacks to measure the CPU and memory utilization of both the machines Ubuntu and Windows.

The remaining paper is structured as follows. Section II covers the approach towards the selection of literature. Section III emphasizes the DDoS attack including the experiment of three different DDoS attack (HTTP, Internet Control Message Protocol (ICMP), and UDP). Section IV shows the CPU and memory performance analysis of the DDoS which is performed in a lab environment. Sections V and VI considers concludes and future directions respectively.

II. Literature Review

Recently for the past one or two years, the progress of our lives is revolving around Artificial Intelligence (AI) and it has taken society's inspiration and built attention to its potential. Now, ML techniques become demanding in the security domain. Because of the increasing number of cyber-attacks, security become a crucial part of the organization. It leads to the need for an efficient mechanism to improve security. This section consists of different DoS/DDoS detection techniques. Table II shows the different comparison studies of various DDoS detection approaches used by the research.

Carl and Kesidis *et al.* [14] used a supervised classification random forest algorithm to train the dataset which was used to detect DoS attacks. They worked on the packet size and packet length parameters to separate the packets like TCP, UDP, DNS, ICMP, etc. Verma and Kumar [15] has applied the "Graph-Based approach" to detect the DoS attack. GBAD tool identified the anomalous instances related to the DoS attack after 5 seconds. Paudel and Harlan *et al.* [16] have proposed a "Random Forest" ML algorithm to detect DoS attacks. Evaluation based on CIC-DoS, CICIDS2017, and CSE-CIC-IDS2018, which are the three intrusion detection benchmark datasets. Filho and Francisco *et al.* [17] have used "Naïve Bayes" and "Random Forest" machine learning algorithms. This system detects DDoS attacks through traffic flow. The author has achieved 90.90% accuracy by Naïve Bayes and 78.71% accuracy by random forest algorithm. Ajeetha and Madhu Priya [18] have implemented a detection algorithm for Leidos (LDoS) attacks where the traffic speed does not have a noteworthy difference as compared to legitimate traffic. The author has detected LDoS traffic with the help of the hybrid algorithm PSD-entropy function and Support Vector Machine (SVM) from normal traffic.

TABLE II. Comparative Analysis of Different DDoS Detection Approaches

Methodology	Technique	Limitations	Benefits
Anomaly-based detection	-Entropy -Source IP Index -Packet Rate	-Accuracy and adaptability wise low	-Less computational time -Less False-Positive (FP)/ False-Negative (FN) -High detection throughput
Machine learning	-DNN	-High computational time	-High accuracy
Statistical	-FGPA	-High detection time -Complexity -Low Flexibility	-Incoming traffic can detect Nine types of DDoS attacks
Rate limiting	-FlowSec	-Low accuracy -High FP rate	-Low computational time -High detection throughput
Statistical	-Switch statistics	-Complexity -High FP / FN rate	-Low computational time -High detection throughput -Flexibility
Machine learning	-FT (F test (FT)) -RF -LGBM	-High Time-Consuming process	-High Accuracy

Zhang and Wu *et al.* [19] have identified the source IP addresses using the SVM algorithm which includes an entropy-based detection framework for DDoS attacks. This algorithm is used for android devices only. Khosroshahi and Ozdemir [20] have implemented a new system to detect and analyze TCP & HTTP flood insider DDoS attacks in a simulated environment. Algorithm1 uses PSH & ACK flags to identify TCP flood—packets and by counting the number of flags they decide if they are normal or malicious. Algorithm 2 get requests from specific IP address and is dependent on counting under a certain time, if the counter surpasses the predefined threshold, then the attack gets detected. Shaaban and Abdelwaness *et al.* [21] implemented ML algorithm RF and Neural Network algorithm MLP to detect DoS attacks. DoS attack includes CIC IDS 2017 dataset as per this algorithm. The system needs to be trained for every new dataset. Attacks such as Hearbleed, slowhttptest, slowloris, and HTTP flood are not classified by the proposed system. Wankhede and Kshirsagar [22] provides services offered by the server to the clients who have authority using the client puzzles as Proof-of-Work (PoW). The major disadvantage of the challenge selector algorithm is it generates the puzzle on basis of a random number. The puzzle algorithm is encrypted using the customer's IP address. If the attacker gets an idea about the customer's IP address, then the puzzle can be decrypted by the attacker.

TABLE III. COMPARISON OF EXISTING DDOS DETECTION TECHNIQUES

Author	DDoS Type	Methodology Used	Outcome	Future Scope
Conti *et al*. [23]	SDN based DDoS attack	-CuSum (Cumulative Sum). -adaptive threshold	-Detection rate = 4.15 seconds -Average false alarm rate = 11.64%.	Experimental results are based on a single SDN controller. Dataset used by the author is old. In future work, we can take multiple SDN controllers along with the latest dataset to check the efficiency of the model.
Sahi *et al.* [24]	TCP Flood attack	-LS-SVM	-Single Source: Accuracy = 97% Kappa coefficient=0.89 -Multiple Source: Accuracy = 94% Kappa coefficient=0.9	We can overcome the problem of DDoS using spoofed IP addresses. Also, can identify the attackers even when they satisfy the threshold value
Aborujilah *et al.* [25]	HTTP Flood attack	-Multivariate correlation analysis-based detection approach	-Detection rate = 86.77% Accuracy = 86.32%	Need to verify model on multiple datasets
Yuan *et al.* [26]	HTTP, ICMP ping, IMAP, Flowgen, MiscApplication, SecureWeb, Unknon_TCP, IRC, DNS< SMTP	-DeepDefense	-Accuracy = 97.606%, Error Rate = 2.394%	Increasing the diversity of DDoS in different environments, vectors, and system settings can be a future scope to test the model's robustness. Also taken dataset is older and has limited features. The model can also be tested using the latest dataset.
Jiao *et al.* [27]	TCP Flood attack	-Decision Tree classifiers	-Detection rate > 99% -False alarm rate < 1%.	Used a total of three datasets: one simulated dataset, a second ISP dataset, and public datasets. The public dataset is outdated. In the simulated dataset, they have focused on two identified attack modes: fixed source IP attacks and random source IP attacks. For fixed source IP attacks around 31 features have been selected which are not required. In the future scope, we can reduce the features count to make the model faster.
He *et al.* [28]	SSH, Brute-Force, DNS reflection, ICMP flooding and TCP SYN attacks	-DeepDefense	-Accuracy = 99.73% -False Positive = 0.068%	The prepared hybrid model of different ML techniques for improved performance, especially unsupervised learning performance. In future work, integration of features into a current system based on more investigation of DDoS attacks can be possible.
Ahanger *et al.* [29]	-Land Attack, -Ping of death attack data, Smurf attack data	-LVQNN classifier	-Detection Rate = 99.8%	Need to verify the model with the existing dataset as they have used simulated dataset only.
Merouane *et al.* [30]	TCP, UDP and HTTP Flood	-SNORT IDS	With new rules they have improved the detection rate of 43.95%.	SNORT worked based on the rules. If you have not designed the rules properly that might increase the false positive rate.
Bhaya *et al.* [31]	TCP, UDP and HTTP Flood	-Unsupervised clustering algorithm (CURE),	Detection rate = 96.29%, False Positive Rate = 0%	The used dataset (DARPA2000, CAIDA2007, and CAIDA2008) is outdated. In future scope, we can try several methods to analyze the frequency of attacks packets during the network flow
Kwon *et al.* [32]	Not Specified	Author has proposed a proactive security method that estimates distributed denial of service (DDoS) attack volume	The proposed model is helps to predict the volume of the DDoS attack in the network based on the bot agents.	In the future scope, we can analyze additional intrusion factors to predict not only the type and intensity but also the time and target of potential attacks.

Zhang *et al.* [33]	Not Specified	The author did survey of 6 ML techniques. Total7 features have been considered for the survey.	As per the result analysis, they recommend that random forest tree and Naive Bayes	The detailed implementation has not been mentioned. We can implement and test the results with the latest dataset to increase accuracy and performance.
Idhammad, *et al.* [34]	More than 9 types of attacks like. Fizzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms attacks	-Extra-Trees ensemble classified - entropy estimation	-Accuracy = 98.23% -False Positive Rate = 0.01%	The proposed model is tested in a lab environment only. It should be tested in the real-life world.
Girma *et al.* [35]	Flood Attack	-DBSCAN Clustering Technology with Entropy	They have not implemented the algorithm.	Data analysis and regressive testing of both vulnerable sides of cloud computing can be done in the future to implement a comprehensive approach.
Sahoo *et al.* [36]	Smurf, UDP flood, & HTTP flood attack	-The author did comparison of 7 ML algorithm with respect to accuracy and time. They have tested the results at three different time zone.	The average prediction accuracy achieved by LR is98.652%. RF achieved 98.409%with less execution time than LR	Higher testing accuracy for Smurf and UDP-Flood can be focused on future tasks
Koay *et al.* [37]	IRC Botnet attack	- Multiple entropy-based features and ML classifiers called E3ML.	-Detection Rate = 94.74%	The improvement of time consumption can be possible in future work.
Yudhana *et al.* [38]	TCP Flood attack	-Artificial Neural Network, Naïve Bayes	-Accuracy: ANN = 95.2381% and naïve Bayes = 99.9%	Research can be conducted on various parameters which include variations of hidden layers, increasing sample size input patterns shown to the network, decreasing the target error, and apply more training processes.
Idhammad *et al.* [39]	HTTP attack	-Information Theoretic Entropy and Random Forest	-Accuracy = 99.54%, -False Positive Rate = 0.4%	Used CIDDS-001 public dataset. We can test the experiment with the latest updated dataset. We can deploy the model in a real-world environment and can evaluate it against several HTTP DDoS tools.
Alzahrani *et al*. [40]	Not Specified	-Anomaly-based distributed artificial neural networks (ANNs) and signature-based approach (Suricata)	-Accuracy = 99.98%, -Detection Rate = 98.15%, -False Positive Rate = 0.0%	In future work, we can test the model in the real world as they have tested it with a simulated dataset only.
Nam *et al.* [41]	SDN based Flood attack	1.SOM +k-NN 2.SOM distributed centre	1. False Positive Rate = 2.14 %, Processing Time = 2.810 % 2. False Positive Rate = 22.36 %, Processing Time = 0.004 %	The model is choosing features automatically. Need to investigate the auto-selected feature extraction algorithms for more efficiency.
Chen *et al.* [42]	TCP Flood attack	Extreme Gradient Boosting	-Accuracy = 98.53% -False Positive rate = 0.008 %	The feature selection part needs to be lookout again as less relevant features of TCP have been selected.

Prachi and Gupta [43] used Sequential Minimal Optimization (SMO) algorithm to detect DoS/DDoS. They tested two different training datasets and apply SMO. The algorithm is depending on the network traffic. That model needs to be retrained every time based on network traffic. Proper network log analysis is required because they have created a dataset on basis of firewall logs. Daneshgadeh and Baykal *et al.* [44] have proposed a modified hop count filtering method with VBSF. Based on the correlation between Time-To-Live (TTL), the IP address of the incoming packet, and the destination port number reserved, the spoofed IP packets get separated from the normal ones by the mitigation technique. Mir and Quadri [45] have implemented a hybrid algorithm LPTR-PSO using HRTE and PSO algorithms. A three-phase scheduling algorithm can be accomplished based on three distinct situations of the server. The conventional round-robin approach is implemented if the server is not under attack. A novel LPTR algorithm is called if the buffer is full. The PSO algorithm gets incorporated to plan the activities and arrived requests by optimizing if the buffer is still overflowed. Ahmed and Hameed *et al.* [46] have applied ML techniques to detect the DDoS attack. A total of 49 features have been extracted for all types of DDoS attacks. They have received 94 % accuracy using the ML algorithm. Swami and Dave *et al.* [47], they used the Naïve Bayes ML algorithm to detect SYN flood attacks. The researcher has calculated the score of each feature available in the dataset but some of them are not relevant to train the model.

Many types of techniques and methodologies have been used by the researcher to detect the DoS/DDoS attack. Most of the detection mechanisms are detecting the attack after analysing the traffic in the network.

This section shows the comparison between various researchers for DDoS detection. Table III summarized the comparative analysis based on various evaluation parameters of detection mechanism. As shown in the comparative study, various research works have been examined for DDoS detection using threshold value, ML, and DL methods. The prediction scores obtained are observed to be having high accuracy and have performed well mostly when ML techniques were used.

III. Experiment and Methods of DDoS Attack

A. DDoS Attack

DDoS attacks are performed with a high intensity as compared to DoS. DDoS attacks containing thousands of botnets that attack a single network make the web server inaccessible. This attack causes massive network congestion. The purpose of a DDoS attack is to compromise availability by sending excessive requests to the server. Botnets are highly responsible to perform the DDoS attack. Those are handled and managed by the attacker. During DDoS, the resources of the victim server will exhaust, and the legitimate user will not be able to send the request. DDoS are generally classified based on attack techniques. TCP/IP layer-based classification of DDoS attacks is shown in Table IV.

TABLE IV. DDoS Attack Possibility by TCP/IP Layer

TCP/IP Layer	Protocol	Example of DDoS Technique	Impact of DDoS attack
Application Layer	FTP, HTTP, PoP3, DNS & SMTP	HTTP Flood Attack, Cache-Bypass, Slow Loris, DNS flood. FTP Flooding	Attackers send seemingly legitimate requests to take down the application
Transport Layer	TCP & UDP	SYN Flood, UDP Flood, TCP Null Flood	Occupied full bandwidth or connection limits of the hots or networking equipment
Internet Layer	IP, ICMP, RIP, IPSec & router	Ping Flood, Ping of Death, Smurf Attack	Affect available network bandwidth and impose extra load on the firewall
Network Layer	VLAN, MAC, DHCP, ARP,	ARP Spoofing, VLAN Hopping, MAC Flooding	Compromised the security of the network devices and target the victim machine

One of the state exhaustion DDoS attacks is the TCP SYN flood, it tries to consume the connection state due to the design issue of the TCP protocol. TCP protocol works on a three-way handshake mechanism. The client initiates the request and sends SYN packets to the server. [48, 49] The server acknowledges this by sending SYN-ACK packets to the client. At last, the client confirms the connection with the final ACK packets. Once the connection is established, the data transmission process is occurring. The probability of SYN flood increases whenever the TCP layer is saturated. In Fig. 2. the attacker floods the TCP request packets on the network in a very less amount of time. During the process, the server sent back the SYN-ACK packets as a confirmation and waited for the ACK from the client side. But the malicious client is unable to send the ACK back to the server and the server waiting for the acknowledgment, which leads to the connection being half-open. So TCN SYN also refers to as a “Half-open “attack. Such half-open connections are responsible for server exhaustion and ultimately bring it offline. If an authentic client tries to make a connection with a server, the user will get the indication/revert as the resource of the server are utilized by the attacker [50]. The detection of DDoS at an early stage is very important for the organization. Four fundamental actions should be taken in a timely way:

1. Vulnerability Assessment
2. Assets potential damage
3. Deploy Detection Mechanism
4. Implement DDoS Prevention solution

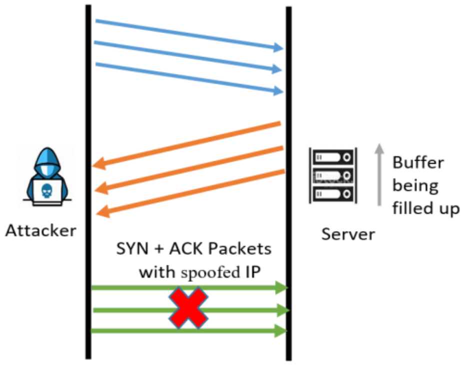

Figure 2. TCP SYN Attack scenario.

B. Attack Environment Configuration

The probability of TCP SYN flood increases whenever the TCP layer is saturated and that should be the pioneer reason to detect and prevent the organization at an earlier stage. To understand the pattern of the DoS attacks we have implemented UDP, TCP, and ICMP flood DoS attacks on both Windows and Ubuntu machines using the hping3 tool. The detailed configuration of the machines is mentioned in the Table V in this scenario, one kali machine is used as an attacking machine and two machines (1. Windows version 10 pro, and 2. Ubuntu version 20.04) are separately used as a victim machines.

TABLE V. Specification of the Victim And Attacking Machine

Machine	Machine OS	Processor	Installed Memory (RAM)	System Type
Victim 1-Windows	Windows-10 Pro	Intel® Core i5	32 GB	64-bit OS
Victim 2-Ubuntu	Ubuntu 20.04	2 GHz dual core processor	4 GB	64-bit OS
Attacking	Kali Linux	AMD E1 processor	4 GB	64-bit OS

Table VI Represent the command used to perform a DDoS attack where -S: SYN flag, -c: packet count, -p: destination port, -V: this parameter support verbose mode which provides the accurate result, -1: ICMP mode, --udp: UDP packet, --tcp: TCP packet, --fast: fast parameter send 10 packets for a second on target machine.

TABLE VI. HPING3 COMMANDS USED TO PERFORMED DDOS ATTACK

Attack Type	Command
UDP	hping3 -S --udp -c 500 -p 8000 --fast <target ip>
TCP	hping3 -S –tcp -c 500 -p 8000 -V <target ip>
ICMP	hping3 -1 -c 500 --fast <target ip>

IV. RESULT AND DISCUSSION

The section shows the results analysis part of the DDoS attack performed in Section III. Table VII represents the detailed analysis of the results after performing TCP, UDP, and ICMP flood attacks. The CPU and memory utilization got impacted a lot in the system performance. When a DDoS attack happens, the consumption of CPU and memory increases drastically which blocks the legitimate process to use the resources of the machine. Here, all the attack has been performed by considering four different packets size: 500, 1000, 5000, 10000 bytes.

TABLE VII. CPU-MEMORY UTILIZATION DURING DOS ATTACK

	Windows Machine						Ubuntu Machine					
Attack Type	UDP Flood	TCP Syn	Ping Flood	UDP Flood	TCP Syn	Ping Flood	UDP Flood	TCP Syn	Ping Flood	UDP Flood	TCP Syn	Ping Flood
Packet Size (Byte)	Memory Utilization			CPU Utilization			Memory Utilization			CPU Utilization		
500	77%	75%	70%	23%	13%	10%	42%	43%	39%	20%	30%	23%
1000	77%	76%	75%	26%	13%	11%	42%	45%	39%	21%	30%	28%
5000	78%	76%	76%	30%	16%	13%	45%	45%	40%	23%	32%	30%
10000	78%	79%	77%	33%	16%	14%	47%	46%	40%	26%	34%	31%

The utilization of CPU and memory on the Windows machine during UDP, TCP and ICMP is shown in the Fig. 3 and Fig. 4, respectively. The results indicate that during UCP flood attack the highest CPU and memory have been utilized as compared to TCP and ICMP attack. Fig. 5 and Fig. 6 give the idea about CPU and memory utilization on Ubuntu machine during the three different attacks. On Ubuntu machine the impact of TCP SYN attack is higher as compared to UDP and ICPM flood attack. On an average 31% CPU and 45% of memory has been utilized during the TCP SYN flood attack.

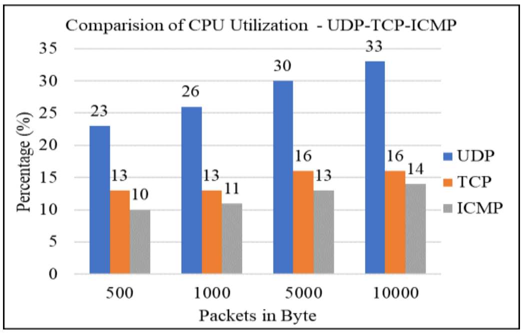

Figure 3. CPU utilization of Windows machine during UDP-TCP-ICMP flood attack.

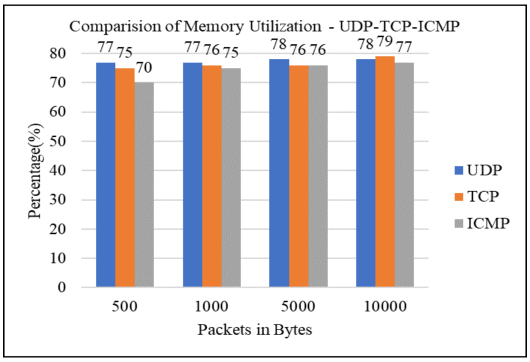

Figure 4. Memory utilization of Windows machine during UDP-TCP-ICMP flood attack.

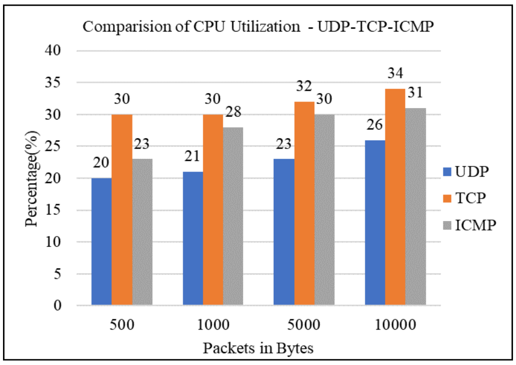

Figure 5. CPU utilization of Ubuntu machine during UDP-TCP-ICMP flood attack.

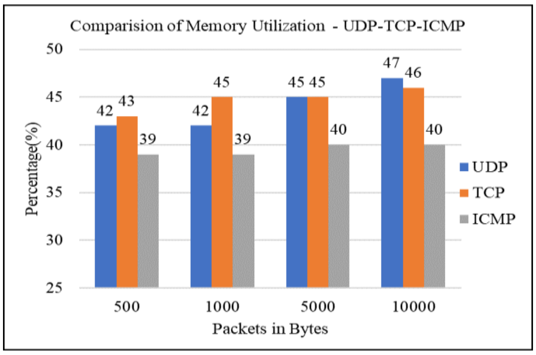

Figure 6. Memory utilization of Ubuntu machine during UDP-TCP-ICMP flood attack.

We have also performed DDoS attack using 10 different attacking machine (Kali Linux) and one victim machine (Windows & Ubuntu) in the lab environment. The details of the attack have been mentioned in Table VIII. All the attacking machines attacked the victim system at the same time on port number 80 with packets size 50,000. Every single packet has been sent in 20 microseconds. When the attack is performed, around 50,000 packets have been transferred to the network.

TABLE VIII. TCP SYN FLOODING DDOS ATTACK PARAMETER

Connection	**Source IP**	**Destination IP**	**Attacking Port**	**Packets Size**	**Single Packets sending interval in a microsecond**
C1	192.168.56.1	172.16.27.100	80	50000	20
C2	172.16.27.101	172.16.27.100	80	50000	20
C3	10.2.1.57	172.16.27.100	80	50000	20
C4	10.2.1.61	172.16.27.100	80	50000	20
C5	10.2.1.64	172.16.27.100	80	50000	20
C6	10.2.1.58	172.16.27.100	80	50000	20
C7	10.2.1.59	172.16.27.100	80	50000	20
C8	10.2.1.82	172.16.27.100	80	50000	20
C9	10.2.1.83	172.16.27.100	80	50000	20
C10	10.2.1.85	172.16.27.100	80	50000	20

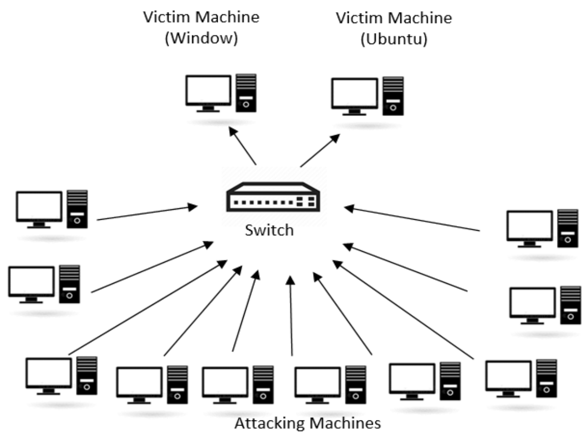

Figure 7. Architecture of DDoS attack.

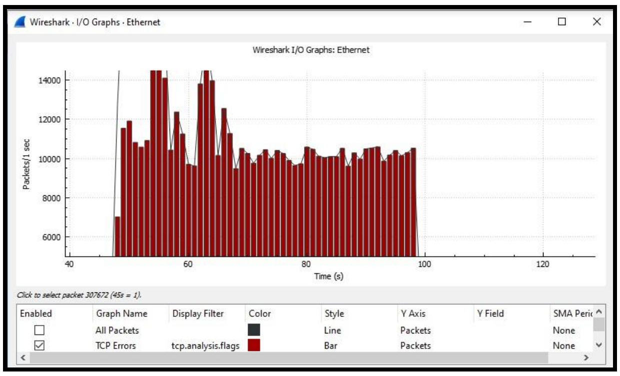

Figure 8. Wireshark — I/O graph during TCP SYN DDoS attack by 10 different machines.

The architecture of DDoS attack is shows in Fig. 7, where 10 machines have been highlighted as an attacking machine and two are used as a victim machine. We can see the traffic on the windows operating system of the TCP SYN packets in the I/O Wireshark graph Fig. 8. All the red bars indicating TCP packets that were transfer per second. While the system operates in regular mode, around 5% and 18% of the CPU and Memory have been utilized on the windows machine. When one system is flooding TCP packets around 33% and 46% of the CPU and Memory are utilized but when ten systems are attacking 85% and 79% of the CPU and memory are getting utilized on the windows machine, which is shown in Fig. 9.

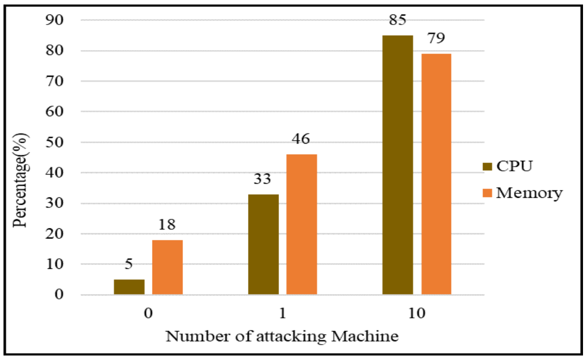

Figure 9. Comparison of CPU and Memory utilization using different attacking machines.

V. CONCLUSION

This paper gives the summary about the latest worldwide DDoS attack in June 2022. The paper also shown the comparison study of the different existing DDoS detection mechanism. We have highlighted the pros and cons of the prevention and detection mechanisms of various research. We have also performed DDoS attack in lab environment and calculated the CPU and Memory utilization during UDP, TCP, ICMP attack. This study helped us understand that duplicate IP address, no. of requests in minimum duration, port count of attacking machine, spoofed IP address etc. are important for early detection of DDoS attack. As per the generated results of CPU and memory utilization, we have concluded that the impact of TCP SYN attack is high, 85% and 79% respectively, compared to other DDoS attacks. We also conclude that anomaly-based approaches are better to detect the attack as it gives accurate results as compared to signature-based algorithm.

VI. FUTURE SCOPE

Many techniques have been applied by the researcher to identify the DDoS attack built on numerous approaches like time consumption, memory consumption, security level, and size of the organization but the false positive rate and time complexity always become a major parameter for the organization. To secure any organization from the attack, early detection is very important. Our future work is to design accurate mechanism learning model with less false positive rate which will be helpful to detect the TCP SYN DDoS at early stage. We will work on the parameter mentioned in conclusion and implement new algorithm using Machine Learning model.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Foram Suthar has conducted the research, performed lab experiment, generated data, and wrote the paper; Nimisha Patel has analyzed and verified the data; all authors approved the final version.

REFERENCES

[1] Radware. (Sep. 15, 2017). DDoS attacks history. Radware. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/

[2] Key metrics from the 2H 2020 NETSCOUT threat intelligence report. NETSCOUT. [Online]. Available: https://www.netscout.com/threatreport/apac/india/

[3] Kaspersky. (2022). DDoS attacks hit a record high in Q4 2021. [Online]. Available: https://www.kaspersky.com/about/press-releases/2022_ddos-attacks-hit-a-record-high-in-q4-2021

[4] D. Kshirsagar and S. Kumar, "A feature reduction based reflected and exploited DDoS attacks detection system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 1, pp. 393–405, 2022.

[5] A. Gaurav, B. B. Gupta, and P. K. Panigrahi, "A novel approach for DDoS attacks detection in COVID-19 scenario for small entrepreneurs," *Technological Forecasting and Social Change*, vol. 177, 121554, 2022.

[6] S. D. Kebede, B. Tiwari, V. Tiwari, and K. Chandravanshi, "Predictive machine learning-based integrated approach for DDoS detection and prevention," *Multimedia Tools and Applications*, vol. 81, no. 3, pp. 4185–4211, Jan. 2022.

[7] Z. Zeng, W. Peng, D. Zeng, C. Zeng, and Y. Chen, "Intrusion detection framework based on causal reasoning for DDoS," *Journal of Information Security and Applications*, vol. 65, 103124, 2022.

[8] Y. Liu, *et al.* "Software-defined DDoS detection with information entropy analysis and optimized deep learning," *Future Generation Computer Systems*, vol. 129, pp. 99–114, 2022.

[9] T. G. Zewdie and A. Girma, "An evaluation framework for machine learning methods in detection of DoS and DDoS intrusion," in *Proc. 2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, IEEE, 2022, pp. 115–121.

[10] S. Saha, A. T. Priyoti, A. Sharma, and A. Haque, "Towards an optimal feature selection method for AI-based DDoS detection system," in *Proc. 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, 2022, pp. 425–428.

[11] S. Dwivedi, M. Vardhan, and S. Tripathi, "Defense against distributed DoS attack detection by using intelligent evolutionary algorithm," *International Journal of Computers and Applications*, vol. 44, no. 3, pp. 219–229, 2022.

[12] I. Basicevic, N. Blazic, and S. Ocovaj, "On the use of principal component analysis in the entropy-based detection of denial-of-service attacks," *Security and Privacy*, vol. 5, no. 2, p. e193, 2022.

[13] M. B. Bharatwaj, M. A. Reddy, T. S. Kumar, and S. Vajipayajula. "Detection of DoS and DDoS Attacks using hidden markov model," in *Proc. Inventive Communication and Computational Technologies*, Springer, Singapore, 2022, pp. 979–992.

[14] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Computing*, vol. 10, no. 1, pp. 82–89, 2006.

[15] V. Verma and V. Kumar, "DoS/DDoS attack detection using machine learning: A review," in *Proc. the International Conference on Innovative Computing & Communication (ICICC)*, 2021.

[16] R. Paudel, P. Harlan, and W. Eberle, "Detecting the onset of a network layer dos attack with a graph-based approach," in *Proc. The Thirty-Second International Flairs Conference*, 2019.

[17] L. Filho, F. Sales, F. A. F. Silveira, A. M. B. Junior, G. Vargas-Solar, and L. F. Silveira, "Smart detection: An online approach for DoS/DDoS attack detection using machine learning," *Security and Communication Networks*, 2019.

[18] G. Ajeetha and G. M. Priya, "Machine learning based DDOS attack detection," in *Proc. 2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*, IEEE, 2019, vol. 1, pp. 1–5.

[19] X. Y. Zhang, Z. J. Wu, J. W. Zhang, and J. S. Chen, "An adaptive network traffic prediction approach for LDoS attacks detection," *International Journal of Communication Systems*, vol. 31, no. 5, p. e3505, 2018.

[20] Y. Khosroshahi and E. Ozdemir, "Detection of sources being used in ddos attacks," in *Proc. 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, IEEE, 2019, pp. 163–168.

[21] A. R. Shaaban, E. Abdelwaness, and M. Hussein, "TCP and HTTP flood DDOS attack analysis and detection for space ground network," in *2019 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, IEEE, 2019, pp. 1–6.

[22] S. Wankhede and D. Kshirsagar, "DoS attack detection using machine learning and neural network," in *Proc. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, IEEE, 2018, pp. 1–5.

[23] M. Conti, A. Gangwal, and M. S. Gaur, "A comprehensive and effective mechanism for DDoS detection in SDN," in *Proc. 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, IEEE, 2017, pp. 1–8.

[24] A. Sahi, D. Lai, Y. Li, and M. Diykh, "An efficient DDoS TCP flood attack detection and prevention system in a cloud environment," *IEEE Access*, vol. 5, pp. 6036–6048, 2017.

[25] A. Aborujilah and S. Musa, "Cloud-based DDoS HTTP attack detection using covariance matrix approach," *Journal of Computer Networks and Communications*, 2017.

[26] X. Y. Yuan, C. H. Li, and X. L. Li, "DeepDefense: Identifying DDoS attack via deep learning," in *Proc. 2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, IEEE, 2017, pp. 1–8.

[27] J. H. Jiao, B. J. Ye, Y. Zhao, R. J. Stones, G. Wang, X. G. Liu, S. Y. Wang, and G. J. Xie, "Detecting TCP-based DDoS attacks in Baidu cloud computing data centers," in *Proc. 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, 2017, pp. 256–258.

[28] Z. C. He, T. Zhang, and R. B. Lee, "Machine learning based DDoS attack detection from source side in cloud," in *Proc. 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, 2017, pp. 114–120.

[29] T. A. Ahanger, "An effective approach of detecting DDoS using artificial neural networks," in *Proc. 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, IEEE, 2017, pp. 707–711.

[30] M. Merouane, "An approach for detecting and preventing DDoS attacks in campus," *Automatic Control and Computer Sciences*, vol. 51, no. 1, pp. 13–23, 2017.

[31] W. Bhaya and M. EbadyManaa, "DDoS attack detection approach using an efficient cluster analysis in large data scale," in *Proc. 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, 2017, pp. 168–173.

[32] D. W. Kwon, H. W. Kim, D. H. An, and H. T. Ju, "DDoS attack volume forecasting using a statistical approach," in *Proc. 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, IEEE, 2017, pp. 1083–1086.

[33] B. Y. Zhang, T. Zhang, and Z. J. Yu, "DDoS detection and prevention based on artificial intelligence techniques." in *Proc. 2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, IEEE, 2017, pp. 1276–1280.

[34] M. Idhammad, K. Afdel, and M. Belouch, "Semi-supervised machine learning approach for DDoS detection," *Applied Intelligence*, vol. 48, no. 10, pp. 3193–3208, 2018.

[35] A. Girma, M. Garuba, and R. Goel, "Advanced machine language approach to detect DDoS attack using DBSCAN clustering technology with entropy," in *Information Technology-New Generations*, Springer, Cham, 2018, pp. 125–131.

[36] K. S. Sahoo, A. Iqbal, P. Maiti, and B. Sahoo, "A machine learning approach for predicting DDoS traffic in software defined networks," in *Proc. 2018 International Conference on Information Technology (ICIT)*, IEEE, 2018, pp. 199–203.

[37] A. Koay, A. Chen, I. Welch, and W. K. G. Seah, "A new multi classifier system using entropy-based features in DDoS attack

detection," in *Proc. 2018 International Conference on Information Networking (ICOIN)*, IEEE, 2018, pp. 162–167.

[38] A. Yudhana, I. Riadi, and F. Ridho, "DDoS classification using neural network and naïve bayes methods for network forensics," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, 2018.

[39] M. Idhammad, K. Afdel, and M. Belouch, "Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest," *Security and Communication Networks*, 2018.

[40] S. Alzahrani, "Detection of Distributed Denial of Service (DDoS) attacks using artificial neural networks on cloud," PhD diss., Tennessee State University, 2018.

[41] T. M. Nam, P. H. Phong, T. D. Khoa, T. T. Huong, P. N. Nam, N. H. Thanh, L. X. Thang, P. A. Tuan, and V. D. Loi, "Self-organizing map-based approaches in DDoS flooding detection using SDN," in *Proc. 2018 International Conference on Information Networking (ICOIN)*, IEEE, 2018, pp. 249–254.

[42] P. Gulihar and B. B. Gupta, "Anomaly based mitigation of volumetric DDoS attack using client puzzle as proof-of-work," in *Proc. 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, IEEE, 2018, pp. 2475–2479.

[43] S. Daneshgadeh, N. Baykal, and Ş. Ertekin, "DDoS attack modeling and detection using smo," in *Proc. 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, IEEE, 2017, pp. 432–436.

[44] S. Q. Mir and S. M. K. Quadri, "Victim based statistical Filtering: A new deterrent against spoofed DoS Traffic," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 9, no. 4, July 2017.

[45] A. Ahmed, S. Hameed, M. Rafi, and Q. K. A. Mirza, "An intelligent and time-efficient DDoS identification framework for real-time enterprise networks: SAD-F: Spark based anomaly detection framework," *IEEE Access*, vol. 8, pp. 219483–219502, 2020.

[46] R. Swami, M. Dave, and V. Ranga, "Detection and analysis of TCP-SYN DDoS attack in software-defined networking," *Wireless Personal Communications*, vol. 118, no. 4, pp. 2295–2317, 2021.

[47] Z. Ahmed, M. Mahbub, and S. J. Soheli, "Defense against SYN flood attack using LPTR-PSO: A three phased scheduling approach," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 9, 2017.

[48] B. N. Ramkumar and T. Subbulakshmi. "TCP SYN flood attack detection and prevention system using adaptive thresholding method," in *Proc. ITM Web of Conferences*, vol. 37, EDP Sciences, 2021, 01016.

[49] M. A. Alotaibi, A. F. Altwairqi, A. F. Alotaibi, and S. M. Alzaharni, "Distributed denial of service attacks simulation and defense," *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol. 11, issue 10, pp. 1606–1620, October 2020.

[50] H. S. Salunkhe, S. Jadhav, and V. Bhosale, "Analysis and review of TCP SYN flood attack on network with its detection and performance metrics," *International Journal of Engineering Research & Technology (IJERT)*, vol. 6, no. 1, pp. 250–256, 2017.