International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Detection and Prevention of Distributed Denial of Service (DDoS) Attacks using Metaheuristic and Machine Learning Techniques

Ameer Sameer Hamood Mohammed Ali

University of Babylon TOEFL Center, University of Babylon, Babylon, Najaf Street, 51002, Iraq
Email: *pre225.ameer.sameir[at]uobabylon.edu.iq*

Abstract: ***The Internet of Things (IoTs) is vulnerable to DDoS attacks, which provide a significant risk to many web-based networks. The intruder's capacity to manage the potential of diverse collaborative gadgets in order to initiate an attack further complicates its administration. The level of complexity can be further heightened when several attackers endeavor to overwhelm a device through a sustained attack. In order to mitigate and safeguard against contemporary DDoS attacks, several efficacious and robust methodologies have been employed within scholarly discourse. These methodologies encompass the utilization of data mining and artificial intelligence within the realm of Intrusion Detection System (IDS). However, it is important to acknowledge that these methodologies are not without their limits. In order to address the current constraints. In this paper, we propose DDoS attack detection and preventing approach using Hybrid model integrated Particle Swarm Optimization (PSO) metaheuristic algorithm and Machine Learning techniques as PSO-ML model. The proposed PSO in IoT network is used for optimizing performance, reducing energy consumption, load balancing, and ensuring scalability, it making IoT suitable for complex and multidimensional optimization problems often encountered in IoT resource management. It evaluates the fitness of each particle by training a DDoS attack detection model with machine learning classifier on the selected features and measuring its performance. PSO-ML model is capable of distinguishing between normal and malicious network traffic. The results showed that the Hybrid PSO-ML DDoS defense system is useful for automating the feature selection process, enhancing the efficiency of DDoS attack detection, high accuracy of DDoS attack detection, best accuracy of UNSW-NB15 dataset is 99.64 % of MLP, CICIDS2017 Dataset is 99.53% of RF, DDOS attack SDN Dataset is 99.54 %, KDDCUP99 Dataset is 97.52 % of RF. Besides, the Average processing time is 41.651 seconds, 149.766 seconds, average packet delivery ratio is 99.65%, 17.35%, average network utilization is 9.791 KB, 0.812 KB, resource utilization 32.061%, 4.572% and Average throughput is 23446.861 KB, 3374.847 KB of PSO-ML Model and Without Optimization within DDos attack respectively.***

Keywords: Internet of Things (IoTs), Distributed Denial of Service (DDoS), Machine Learning, PSO metaheuristic algorithm

1. Introduction

In recent times, there has been a significant surge in interest and scholarly focus on the IoT, which has emerged as a prominent and susceptible domain for academic investigation. IoT systems are characterized by their complexity and the presence of integrated operations. These resources are accessible on a global scale, mostly composed of limited supplies, and are formed via the omission of connections [1]. Hence, it is imperative to apply significant alterations to existing security frameworks for information and wireless networks in order to provide efficient techniques for ensuring security in the context of the IoT [2]. Maintaining the security need within the expansive attack surface of the IoT system is a formidable challenge. Nevertheless, IoT devices mostly operate inside an unsupervised setting. Therefore, it is possible for an unauthorized individual to establish physical contact with these devices. In order to meet the security criteria, it is imperative that solutions incorporate comprehensive considerations [3]. As a result, the security of IoT systems is more vulnerable compared to other computing systems. Conventional security techniques, including encryption, authentication, access control, network security, and defense against DDoS attack, are insufficient when applied to extensive systems including several interconnected devices [4].

The occurrence of a DDoS assault poses a significant risk to the security of cyberspace. The target system or network often has limitations in terms of bandwidth, memory, or processing capability. Typically, a DDoS assault is characterized by its distributed nature, including a large-scale and coordinated effort [5].

The utilization of this technology is widespread in both wired and wireless network connections within the realm of internet connectivity. Presently, there is a notable increase in the magnitude of DDoS assaults targeting internet security. These types of attacks can be initiated by deliberately exploiting vulnerabilities within a target's system, such as a host, entire network, or router [6]. Another method involves overwhelming the target's system with a significant volume of network traffic in order to seize specific resources, including processor time, memory, and network bandwidth. Consequently, the resources that are accessible to normal users or consumers are limited or frequently unavailable. The individuals who were affected by the DDoS assault have been disclosed in [5], while effective strategies to minimize the impact of such attacks have been thoroughly investigated in [6]. In recent years, a considerable body of literature has emerged with the aim of developing IDS as a means of safeguarding against DoS attacks.

To address the issue of DDoS assaults in the healthcare IoT ecosystem, a suggested approach is the deployment of a mutual identification mechanism between the gateway and the end user. The authentication approach employed in this context is founded upon the DTLS handshake protocol. The gateway will encompass an inclusive list or table of nodes

that have been preauthorized to establish interactions with other nodes within the medical IoT ecosystem [7]. The gateway maintains an active session feature to guarantee that whenever a node is engaged in communication with another node, it is prevented from communicating with any other nodes within the IoT ecosystem. According to the cited source [8], the gateway will increment the count whenever the node initiates an association with other nodes. If the count beyond a certain threshold, the gateway will ultimately prohibit the connection. The approach being presented effectively mitigates both DDoS assaults and Replay attacks. Theoretical examination of the preventative approach is conducted, without any mention of actual application [9]. The proposed approach addresses the limitation observed in previous studies, namely the insufficient processing capacity in the IoT layer, by centralizing all computational tasks on the Smart e-Health gateway [10]. It alleviates on medical sensors that are incapable of performing intensive processing tasks. Metaheuristic optimization is a field of study that focuses on solving optimization issues through the utilization of metaheuristic methods. Optimization is a pervasive concept that finds application in several domains, including technical design, economics, holiday planning, and Internet routing. The efficient allocation of limited financial, material, and temporal resources is of paramount importance [11].

The proposed system applied to decreased these main problems:

- Effective prevention mechanisms are essential to safeguard IoT networks against DDoS attacks. While detection is crucial, preventing attacks from overwhelming network resources is equally important. Many IoT devices have limited computational capabilities, making them susceptible to resource exhaustion during an attack.
- How do identify the normal and abnormal traffic to make a decision by the proposed DDoS detection and preventing model.
- DDoS attacks issues in the IoT network which effects the network behavior by increasing delay, and lost packets.
- Flooding traffic due to DDoS attack which effects on the network performance and consumes network resources.

Besides, the proposed system contributes the following goals:

- Develop and implement efficient and lightweight DDoS detection algorithms tailored to the characteristics of IoT devices by using an integration between machine Learning and Metaheuristic techniques to detect and prevent of DDoS.
- Providing early warnings of DDoS attacks to enable rapid response and mitigation, preventing the attacks from disrupting IoT operations.
- Recognizing data traffic using Maximum Data Traffic (MDT) as normal data traffic (allow), abnormal data traffic(deny).
- Optimizing the use of computing resources, energy, and network bandwidth, ensuring that DDoS prevention mechanisms do not excessively burden IoT devices.
- Anomaly detection by utilizing machine learning techniques to identify abnormal traffic patterns and behavior that may indicate DDoS attacks in IoT networks, especially when traditional signature-based methods may be insufficient

2. Related Works

The most related works in term of improving the security of IoT networks by detection and preventing of DDoS Attacks using Metaheuristic and machine/deep learning Techniques have been discussed and overviewed as follows:

An intrusion detection mechanism is proposed in [12] that is a combination of a filter-based selection approach and a machine learning algorithm known as the IGIDS. Furthermore, IGIDS employs a feature selection technique to identify the most pertinent attributes from the initial IDS datasets. These attributes aid in differentiating between common low-speed DDoS attacks. Subsequently, the chosen attributes are utilized as input for the classifiers, namely SVM, C4.5, NB, and MLP, to effectively detect such attacks. The datasets utilized for research purposes include KDD Cup 99, CAIDA DDOS Attack 2007, CONFICKER worm, and UNINA traffic traces. The results showed integrated IGIDS-C4.5 decision tree classifiers, achieves a high detection accuracy with low false-positive ratio.

In [13] they proposed a hybrid approach to intruder detection based on feature selection algorithm (FS) which is based on decision tree in selecting the proposed features based on some out-of-water machine learning as a baseline to evaluate the proposed system based on UNSW-NB15 dataset. DR algorithm achieved 97% and proved its effectiveness compared to other works.

In [14] Big data and deep learning techniques were combined to improve the performance of intrusion detection by monitoring data traffic in the network, based on the deep feed-forward neural network algorithm (DNN) and the gradient boosting tree (GPT). The algorithms were evaluated on the UNSW NB15 and CICIDS2017 datasets. DNN results achieved high accuracy of 99% for the UNSW NB15 dataset for the DNN algorithm and achieved 97% for the GPT algorithm for the CICIDS2017 dataset.

In [15] Hybrid two multi-objective approaches are proposed to efficiently detect attacks in the network based on the multi-objective genetic method (NSGAII) algorithm and the artificial neural network (ANN) algorithm to extract network features that affect the data traffic and extract features for this data while maintaining diversity control. The results show the superiority of the proposed system compared to other solutions in the echo works.

In [16] they proposed an intrusion detection system to identify attacks and notify system administrators to increase security in the network, as it relied on a hybrid analysis to prevent electronic attacks by deep learning and expanding the scope of input data. The Hybrid Metaheuristics with Deep Learning Enabled Cyberattack Prevention (HMDL-CAP) model and hybrid convolutional neural network with recurrent neural network (HCRNN) model was applied to detect intrusions. The results showed an increase in the accuracy of detection of intruder attacks in the network.

In [17] a metaheuristics with deep learning-based DDoS attack detection model (MDL-DDoSAM) for detecting DDos attack numbers on deep learning in the Internet of Things network. This technique mainly aims to identify the occurrence of attacks in this environment and is based on pre-processing of network data by designing a feature selection technique based on search enhancer to select a dedicated set of features that contribute to detecting the attack to rely on the whale optimization algorithm (IWOA) optimization algorithm. The DDos attack was tested and the results showed an improvement in performance compared to other related works.

3. The proposed system methodology

The proposed integrated PSO-ML system is based on detecting and preventing of DDoS Attacks using integrated model based on PSO Metaheuristic and machine learning Techniques. Particle Swarm Optimization (PSO) metaheuristic for DDoS attack detection and prevention in IoT involves multiple steps. The main step-by-step as follows:

3.1 Problem Definition

Define the problem by specifying the objectives of your DDoS detection and prevention system. Determine what you want to optimize and the constraints involved.

3.2 Data Collection

Data was collected for training the network from IoT devices and offline datasets on which the system was trained and tested during simulation, including data on the behavior of devices in the network, information transfer, and the extent of interconnection between IoT devices. A set of training datasets was used to test the PSO algorithm and machine learning algorithms as follows:

The UNSW-NB 15, CICIDS2017, KDDCUP99, DDOS attack SDN datasets that contain a mixture of intrinsic modern normal operations and contemporary synthetic attack behaviors. Table 1 showed the used dataset parameters.

Table 1: Compares the Datasets based on a variety of criteria

Parameter	*UNSW-NB 15*	*CICIDS 2017*	*KDDCUP 99*	*DDOS attack SDN*
Years	2015	2017	1999	2020
Modern attacks	Yes	Yes	No	Yes
Feature selection	49	2	41	23
Publicly available	Yes	Yes	Yes	Yes
Label data	Yes	Yes	Yes	Yes

3.3 Feature Selection

It is considered one of the important stages of the proposed system, where features related to the nature of the data that contribute to the detection of distributed denial of service attacks are determined. These features include packet size, packet frequency, IP address of the sending and receiving device, packet delivery time, and packet length.

3.4 Preprocessing

The proposed system includes a set of data preprocessing methods for cleaning and processing methods to deal with missing values and outliers to ensure that the data is in a consistent format that contributes to improving the performance of the PSO-ML resource optimization model. The used preprocessing methods for the proposed DDoS attack system as follows:

1) Data Cleaning: remove duplicates: eliminate duplicate records from the dataset to prevent bias in the model. It achieved by handle missing data that address missing values by imputation or data removal, depending on the nature and extent of missing data.
2) Features Normalization and Scaling: normalize numerical features to bring them to a common scale, often between 0 and 1, to facilitate model convergence. Also, standardize features to have zero mean and unit variance, making it easier for the model to learn.
3) Feature Engineering: select relevant features: Identify and select the most relevant features for DDoS detection while removing irrelevant or redundant ones. It is happened by creating new feature that capture meaningful information, such as traffic patterns, request rates, or anomalies.
4) Data Transformation: apply a logarithmic transformation to skewed or highly variable data to make it more normally distributed. It achieved by one-hot encoding that convert categorical variables into binary vectors, making them suitable for machine learning models.
5) Resampling: It involves reducing the quantity of samples in the majority class in order to get a more balanced distribution of classes.

3.5 Particle Swarm Optimization (PSO) metaheuristic algorithm for DDoS attacks

PSO algorithm used for improving and allocating resources inspired by natural systems in analyzing the use of resources and falls within the methodologies of intelligence swarm algorithms, where it addresses the tasks of improving and researching the simulation of the social behavior of flocks of birds or fish in a manner that suits it in the field of resource allocation in machine learning and engineering for data analysis and operations research which determines the collective effort of a number of individuals or processes represented by particles to reach an ideal solution through repeated adjustments to the locations of individuals within a solution space which is characterized by several dimensions all of which are invested in decision-making processes to distribute tasks ideally to all nodes in the system.

The individuals, or particles, are guided by their own experiences and the experiences of the best-performing individuals in the swarm. PSO is often used to find the optimal solution to a problem where the objective function is defined, and the goal is to minimize or maximize it. The main fundamental concepts and components of the PSO algorithm as follow [83]:

- The particles inside the swarm serve as individual representations of potential solutions to the given optimization issue. Particles in a solution space are distinguished based on their locations and velocities.

- Updating the object's position and speed, as the particles undergo updates in their positions during each iteration, taking into account their current speed. The particle's speed is modified based on the individual experiment, through which the best position is determined compared to the position discovered by the entire swarm.
- Choosing the general position by determining the best solution position found by any particle in the swarm. This position is used as a preference to direct the swarm's movements towards the optimal solution for decision-making.
- The best personal result is achieved by tracking each particle to its best location in the current space based on the objective function. This location is determined personally by the entire motion of the particle.

3.6 Training PSO-based DDoS

It applied by using the historical data obtained to search for optimal configurations and parameters which enhanced decision making process.

3.7 Model Evaluation

The proposed system is evaluated based on network evaluation and machine learning evaluation. Network evaluations are:

- Average processing time: It refers to the average time (in seconds) that an IoT device takes to process a data packet from the moment it is received until it is redirected. This metric is important in assessing how efficiently a network can handle incoming requests during heavy traffic such as DDoS attacks [18].
- The average packet delivery ratio (PDR): It is a measure of the rate of confirmation that packets have reached the destination without errors during the transmission process [19].
- Average network utilization: It is the average network usage of the available bandwidth during a specific period of time, which indicates how efficiently the network capacity is used during a communication session [20].
- Resource utilization: It is a measure of the high usage of resources such as CPU, memory and RAM of devices within the network. High inefficient usage leads to performance degradation and increased slowness of execution of the device operations in the network [21].
- Average throughput: It represents the average amount of data transferred correctly over the network within a specific time frame and is measured in kilobytes, reflecting the actual data transfer rate, which is affected by factors such as congestion, packet loss, and multiple denial of service attacks [22].

Besides, the efficacy of the machine learning model by utilizing the testing dataset measurements are accuracy, precision, recall, F1 score, and AUC.

The proposed machine learning system was evaluated using Accuracy [23], F1 Score [24], Recall [25] and Precision [26]:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP+TN+FP} + \text{FN}} \quad (4)$$

$$\text{F1} - \text{score} = \frac{(2*\text{TP})}{(2*\text{TP+FN+FP})} \quad (5)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (6)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (7)$$

3.8 Continuous Monitoring and Maintenance

Regularly monitor the performance of your deep learning-based DDoS detection system in a real-world environment. Update the model as needed to adapt to new attack patterns or changing network conditions. In addition, the system should be up-to-date with the latest threat intelligence and DDoS attack traffic requests.

The DDos attack detection algorithm in IoT network involves integrated model PSO and machine learning (PSO-ML model).

Input: Data traffic
Output: Classified data traffic into normal allow and abnormal deny

Initialize DDoS Detection Model
Step 1: **While** True **do**
- Collect network traffic data = CollectNetworkData()
- Preprocessed data = PreprocessData(network_data)
- Verification: is_ddos_attack then Apply DDoS= DDoSDetectionModel(preprocessed_data)

Step 2: **if** is_ddos_attack **then**
- Log : DDoS attack detected
- Mitigate DDoS Attack(network_data)

Step 3: Alarm notification
- Notify network administrator as NotifySecurityTeam()
- Waiting (Interval) for a specified interval

End algorithm

The algorithm steps are summarized as follows:

- The DDoS detection model is initialized to detect anomalies in network traffic.
- The loop continuously collects network traffic data and preprocesses which make it suitable for the detection model using PSO metaheuristic algorithm.
- The DDoS detection model is applied to the preprocessed data to determine if a DDoS attack is detected.
- If a DDoS attack is detected, it logs the attack, triggers mitigation measures, and notifies the network administrator or security team.
- The loop continues to monitor network traffic with a specified time interval.
- Creating Dataset contains classified data traffic as normal and abnormal.
- Building trained classifier model with machine learning algorithms.
- Classify data traffic to prevent DDoS attack in network traffic.

4. The proposed System Architecture

4.1 IoT Device Layer

It consists of the various IoT devices, sensors, actuators, and other elements that are responsible for collecting data, interacting with the environment, and transmitting information to the next layers of the IoT architecture. These devices are connected to local simulated network, enabling

them to send and receive data, making them a crucial part of the IoT ecosystem.

4.2 Network Elements

a) Access point
It is part of the network elements and extends the range of the wireless network and connects IoT devices together and send the request to router.

b) Router
It is part of the network elements and is received the request from access point and IoT devices and send the request to gateway/edge, in short, it redirects the packet to the server.

c) Gateway / Edge Device
It is part of the network elements and it contains on the proposed PSO algorithm, like the router device that has algorithmic characteristics and is located before the area which want to protect. Through it, it can filter and manage the traffic when high traffic comes in, it did not go to the server directly, but it filters the traffic with max data traffic model, and it is filtered through to two points max data traffic and time. The traffic filtration is allowed for normal and deny for abnormal traffic. The main tasks of this device are as follows:

- Anomaly Detection: Using the optimized parameters, the gateway/edge devices analyze the incoming traffic for anomalies. Sudden spikes in traffic, unusual patterns, or a high number of requests from a single IP address can trigger an alarm.
- Response Mechanism: When a potential DDoS attack is detected, the gateway/edge devices can take action, such as rate-limiting, blacklisting IP addresses, or signaling the central network for additional protection.

4.3 Server

It is the device that accepts and responds to requests made over a network from network elements devices. Network architecture showed in Figure 1.

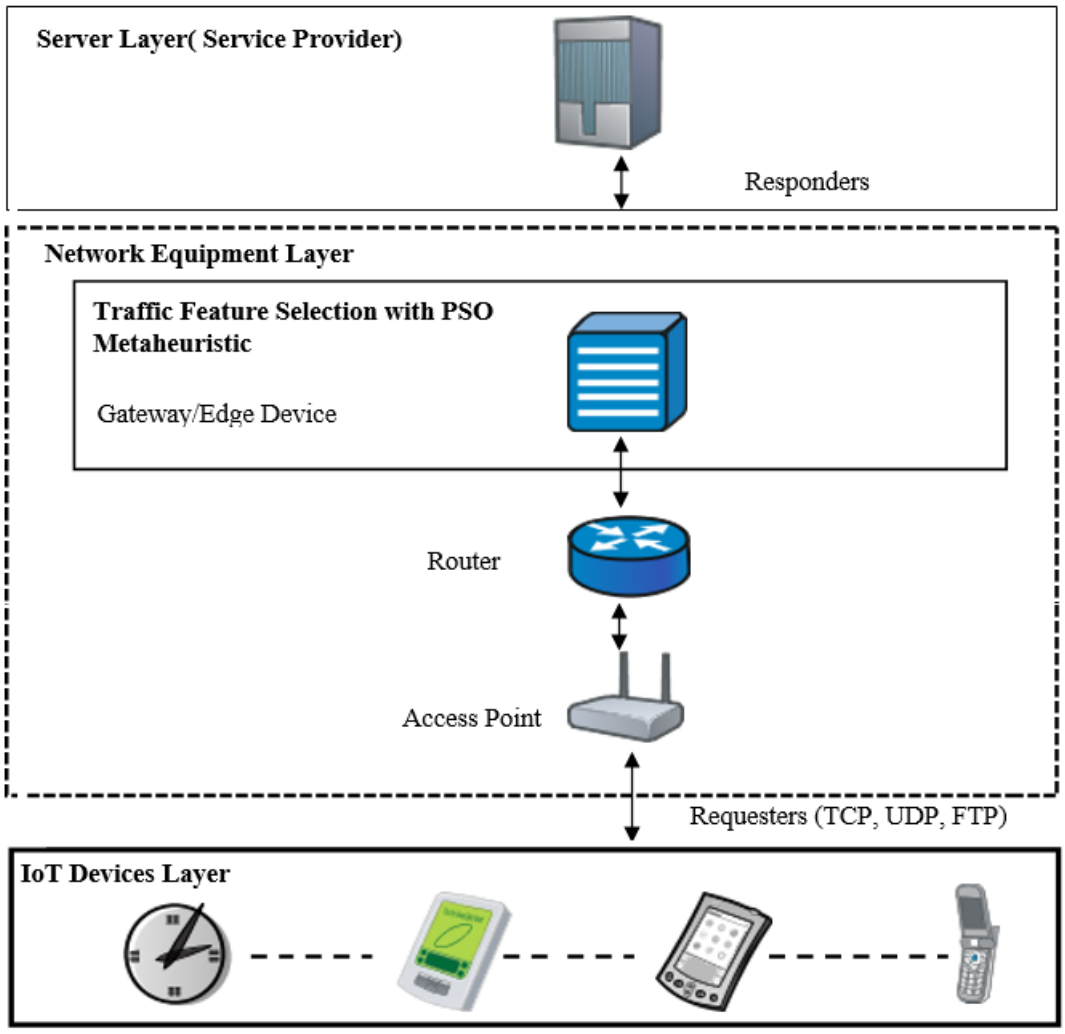

Figure 1: Block diagram of the proposed system architecture in IoTs environment

The proposed DDoS attack detection model has the advantage of dealing with attacks of unknown anatomy and different strengths through training phase with legitimate traffic, and then it decides the normal from abnormal traffic based on the log file traffic model of data traffic for each wireless device as the network analyzer model to verify each hosts. The proposed method in Gateway/Edge device to control traffic feature selection with PSO Metaheuristic creates two log configuration rule. The first one is normal rule with allow feature for normal request from source IP, source MAC address, max traffic rate and time stamp under or equal to the used threshold in PSO and then add the Host

details to the white list. The second abnormal rule deny for abnormal request with source and MAC addresses and verify it after matched with the used value and add the Host details to the black list.

It assigned a trust host IP identifier for every wireless host relying on a threshold maximum data traffic (MDT) value that changes dynamically and assists in detecting the DDoS attack by measuring maximum data rate for each interface port and identify normal wireless with allow rule data packets and abnormal wireless with deny rule data packets, The objective is to mitigate the effects of the DDoS assault, characterized by a substantial influx of data, on the network. This is to ensure that ordinary users may effectively carry out their duties without experiencing compromised network performance and excessive latency. as it showed in Figure 2.

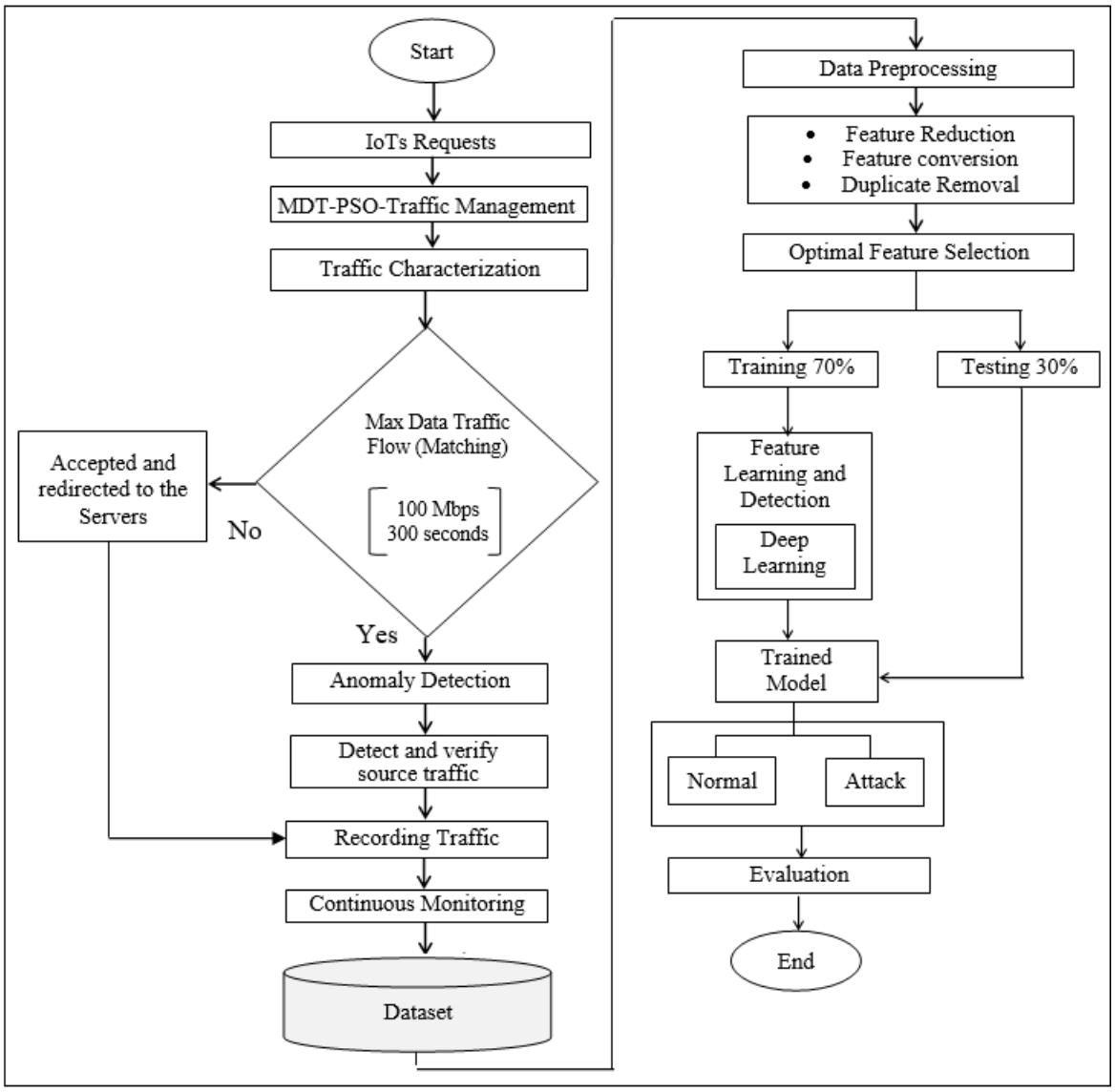

Figure 2: The Proposed Methodology of DDoS attack detection and prevention in IoT network

5. Implementation and Results

The proposed network system is simulated in OMNET++ and machine learning model is programmed in Java Eclipse IDE-2023. Simulation specification is shown in Table 2.

Table 2: Simulation parameters and considered values of the proposed system.

Simulation Parameters	*Considered Value*
Network Area	1500m x 1500m
Number of IoT nodes	20
Data Type | File Data signal size	1024 KB
Simulation Time	1800 seconds
Type of Channel	Wireless
Simulator Name	OMNET ++, Eclipse
RAM size	8 GB
CPU	Core i 7
Operating System	Windows 10

5.1 Results of Network traffic without DDos Attack

The results in Figures 3 to Figure 6 indicates that the network traffic without the DDos attack in a stable and efficient operational network, which allows data to be processed in a timely manner with minimal delay and can be processed with low latency and high response, which indicates the reliability of the network in sending and receiving data successfully without loss. This performance is of paramount importance in contributing to maintaining user satisfaction and operational efficiency, especially in an environment where data integrity and speed are essential to the user. It also demonstrates the extent to which the PSO algorithm has improved in maintaining strong network performance in the absence of external threats such as DDoS attacks.

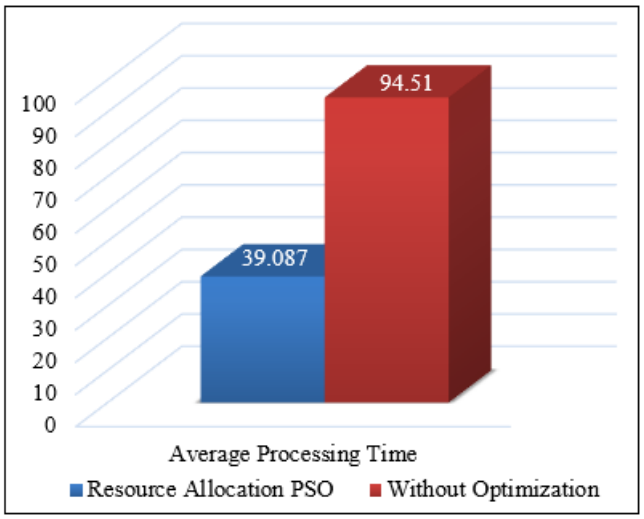

Figure 3: Average processing time of network traffic without DDos attack.

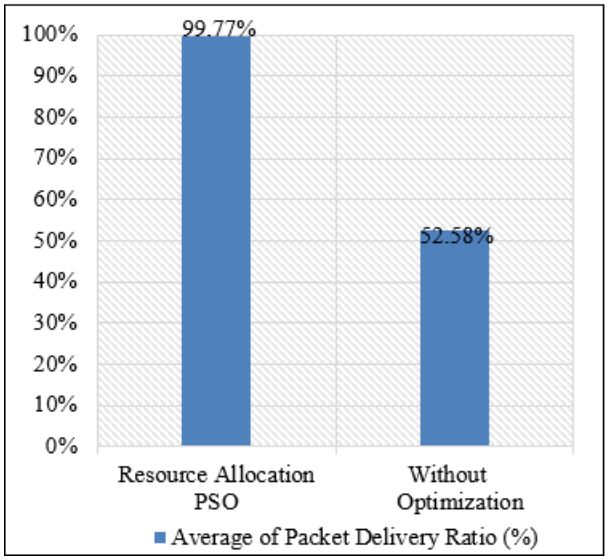

Figure 4: Average packet delivery ratio (PDR) of network traffic without DDos attack.

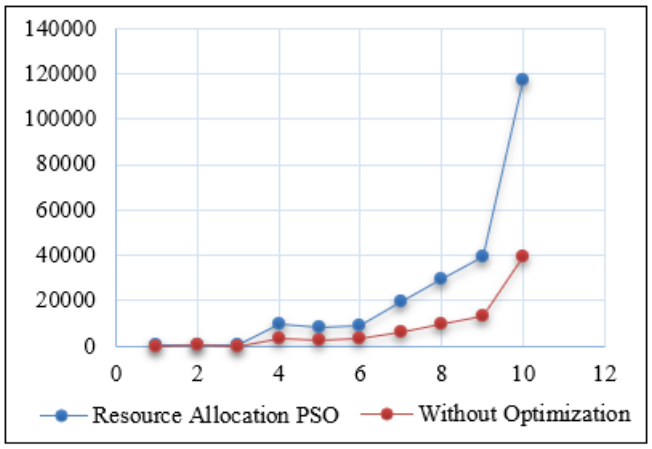

Figure 5: Total Average of Network and Resource Utilization of network traffic without DDos attack.

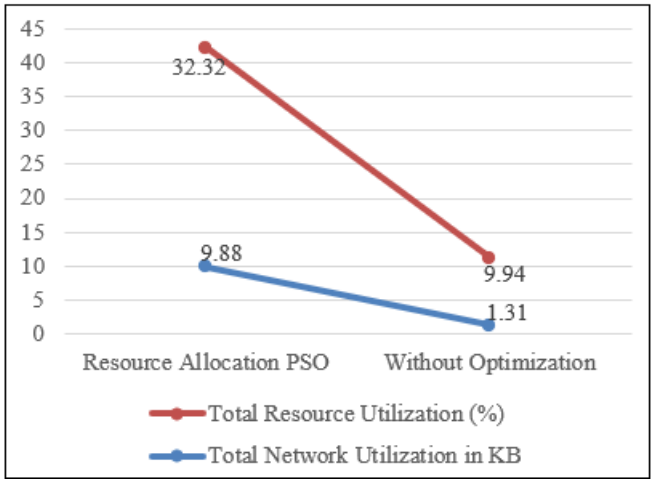

Figure 6: Throughput of network traffic without DDos attack.

5.2 Results of DDos attack

The results in Figure 7 to Figure 10 showed the performance metrics of traffic during DDos and how it impacted on network efficiency, the average traffic has been affected as a result of the increase in the passage of unauthorized and malicious packets in the network, which caused an increase in the processing time due to their large size, which affects legitimate packets by waiting for a longer period for processing. The packet delivery rate decreased slightly for the proposed system due to the reliability of the network and its training according to high-pressure and load performance during sending and receiving packets. The impact of DDos attacks on network resources and bandwidth also led to resource depletion as a result of congestion and additional degradation in service, but to a small extent in the proposed system due to the distribution of the load by the PSO algorithm, which was trained on four databases with high data transfer sizes that require effort to complete tasks, and contributed to reducing the stress of resource use and enhancing the network's resilience against threats.

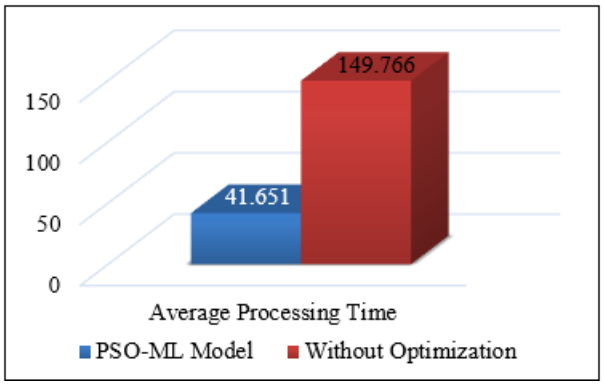

Figure 7: Average processing time of network traffic with DDos attack

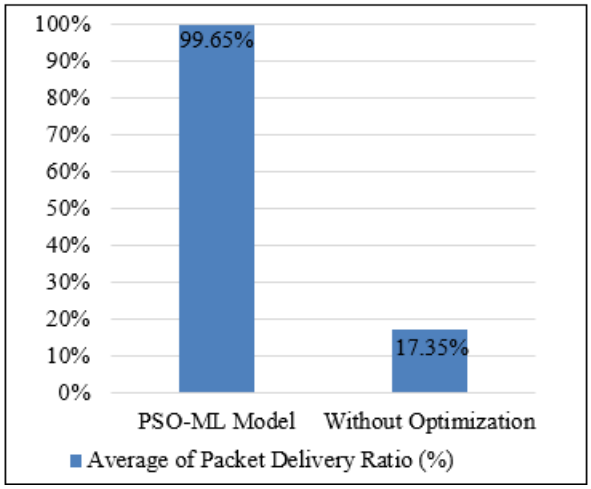

Figure 8: Average packet delivery ratio (PDR) of network traffic with DDos attack.

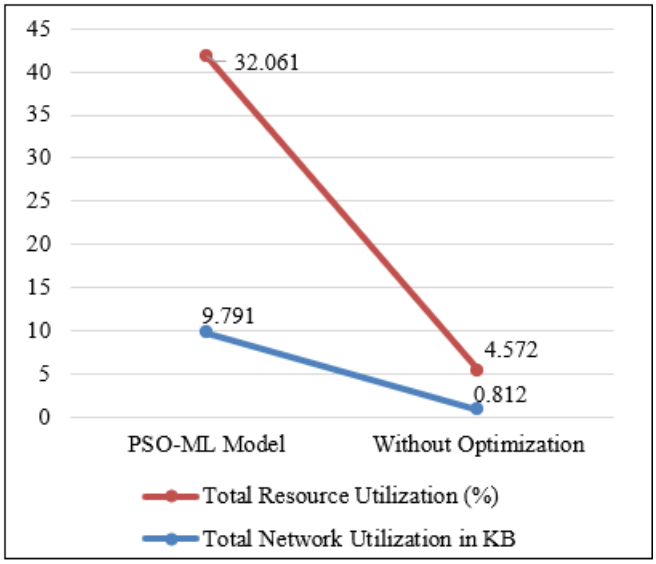

Figure 9: Total Average of Network and Resource Utilization of network traffic with DDos attack.

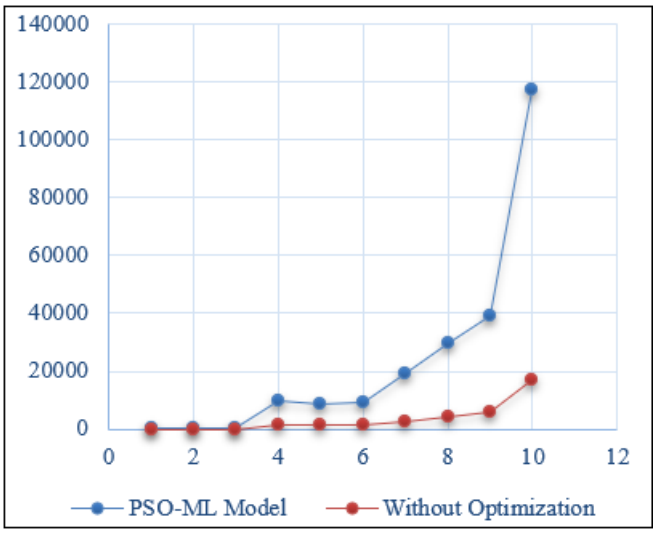

Figure 10: Throughput of network traffic without DDos attack.

5.3 Results of machine learning

The results explanation in Table 3 to Table 8 for different datasets showed the effectiveness of different machine learning algorithms in detecting DDoS attacks with noticeable differences in accuracy and processing time, and other evaluation metrics across different datasets. The Random Forest algorithm was superior for the CICIDS2017 DatasetDDOS attack SDN Dataset KDDCUP99 Datasets due to its effectiveness in identifying attack patterns, while the SVM algorithm showed lower accuracy overall. Although it is a popular choice for intrusion detection, it may not be the most effective for all datasets. The MLP algorithm for the UNSW-NB15 dataset also showed superior results due to its ability to learn complex patterns in network traffic and presented challenges KDDCUP99 due to its inherent problems such as duplicate records that distorted the results affecting the overall performance of the model. These results emphasized the importance of choosing appropriate algorithms based on the specific characteristics of each dataset to improve detection accuracy and processing efficiency in distributed DDoS attack by considering the allocation of resources in the entire network devices. The proposed system is evaluated with four datasets UNSW-NB15, CICIDS2017, KDDCUP99 and DDOS attack SDN. Table 3 showed

Table 3: Accuracy and required time to build mode of the proposed system.

Method Name	*UNSW-NB15 dataset*		*CICIDS2017 Dataset*		*DDOS attack SDN Dataset*		*KDDCUP99 Dataset*	
	Accuracy	*Time*	*Accuracy*	*Time*	*Accuracy*	*Time*	*Accuracy*	*Time*
RF	99.43 %	230 ms	99.53%	563 ms	99.54 %	568 ms	97.52 %	2008 ms
SVM	99.62 %	68 ms	99.44%	201 ms	99.48 %	159 ms	96.71 %	5388 ms
MLP	99.64 %	75 ms	99.45%	2990 ms	99.45 %	2483 ms	96.997 %	8521 ms

Table 4: Evaluation metrics of UNSW-NB15 dataset

Evaluation Parameters	*UNSW-NB15 dataset*		
	RF	*SVM*	*MLP*
Precision	1	1	1
Recall	0.99425	0.99616	0.9961
F-Measure	1	1	1
Kappa Coefficient	0.9797	0.9853	0.9921
Area Under Curve (AUC)	0.0175	0.025	0.025
Error Rate	0.00574	0.0039	0.00383

Table 5: Evaluation metrics of CICIDS2017 dataset

Evaluation Parameters	*CICIDS2017 Dataset*		
	RF	*SVM*	*MLP*
Precision	1	1	1
Recall	0.99526	0.99439	0.9943
F-Measure	1	1	1
Kappa Coefficient	0.9901	0.9885	0.9884
Area Under Curve (AUC)	0.00981	0.01186	0.01677
Error Rate	0.00473	0.00560	0.0056

Table 6: Evaluation metrics of DDOS attack SDN dataset

Evaluation Parameters	*DDOS attack SDN Dataset*		
	RF	*SVM*	*MLP*
Precision	1	1	1
Recall	0.9953	0.99447	0.9944
F-Measure	1	1	1
Kappa Coefficient	0.9903	0.9887	0.98867
Area Under Curve (AUC)	0.00952	0.0116	0.0137
Error Rate	0.00466	0.005524	0.00552

Table 7: Evaluation metrics of KDDCUP99 dataset

Evaluation Parameters	*KDDCUP99 Dataset*		
	RF	*SVM*	*MLP*
Precision	1	1	0.8666
Recall	0.1292	0.9671	0.1023
F-Measure	0.2289	1	0.1830
Kappa Coefficient	0.2238	0.0	0.1773
Area Under Curve (AUC)	0.3272	0.0328	0.2337
Error Rate	0.0248	0.0328	0.0300

That is superior to all algorithms as well in terms of detection accuracy, as in Table 8.

Table 8: The proposed system comparison.

Author	*Dataset*	*Algorithm*	*ACC*
[13]	UNSW-NB15 dataset	RF	86.42%
[14]	UNSW NB15 and CICIDS2017	DNN	99.19%
[15]	KDDCUP99 and UNSW-NB15	RF	94.8%
[16]	Benchmark dataset	HMDL-CAP	99.40 %
[17]	DDOS attack SDN Dataset	MDL-DDoSAM	99.03 %
The proposed System	**UNSW-NB15**	**RF**	**99.43%**
		SVM	**99.62%**
		MLP	**99.64%**
	CICIDS2017	**RF**	**99.53%**
		SVM	**99.44%**
		MLP	**99.45%**
	KDDCUP99	**RF**	**97.52%**
		SVM	**96.71%**
		MLP	**96.99%**
	DDOS attack SDN	**RF**	**99.54%**
		SVM	**99.48%**
		MLP	**99.45%**

References

[1] Aliar, A. A. S., Gowri, V., & Abins, A. A. (2024). Detection of distributed denial of service attack using enhanced adaptive deep dilated ensemble with hybrid meta-heuristic approach. *Transactions on Emerging Telecommunications Technologies*, *35*(1), e4921.

[2] Musa, N. S., Mirza, N. M., Rafique, S. H., Abdallah, A., & Murugan, T. (2024). Machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks-current research solutions. *IEEE Access*.

[3] Gadallah, W. G., Ibrahim, H. M., & Omar, N. M. (2024). A deep learning technique to detect distributed denial of service attacks in software-defined networks. *Computers & Security*, *137*, 103588.

[4] SaiSindhuTheja, R., & Shyam, G. K. (2021). An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment. *Applied Soft Computing*, *100*, 106997.

[5] Kamel, H., & Abdullah, M. Z. (2022). Distributed denial of service attacks detection for software defined networks based on evolutionary decision tree model. *Bulletin of Electrical Engineering and Informatics*, *11*(4), 2322-2330.

[6] Mohammadi, S., & Babagoli, M. (2021). A hybrid modified grasshopper optimization algorithm and genetic algorithm to detect and prevent DDoS attacks. *International Journal of Engineering*, *34*(4), 811-824.

[7] Hasan, M. M. (2021). Distributed denial of service attack detection in cloud computing environment using machine learning.

[8] Paidipati, K. K., Kurangi, C., Uthayakumar, J., Padmanayaki, S., Pradeepa, D., & Nithinsha, S. (2024). Ensemble of deep reinforcement learning with optimization model for DDoS attack detection and classification in cloud based software defined networks. *Multimedia Tools and Applications*, *83*(11), 32367-32385.

[9] Talpur, F., Korejo, I. A., Chandio, A. A., Ghulam, A., & Talpur, M. S. H. (2024). ML-Based Detection of DDoS Attacks Using Evolutionary Algorithms Optimization. *Sensors*, *24*(5), 1672.

[10] Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Damaševičius, R., & Bahaj, S. A. (2022). Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT). *Electronics*, *11*(3), 494.

[11] RM, B., K Mewada, H., & BR, R. (2022). Hybrid machine learning approach based intrusion detection in cloud: A metaheuristic assisted model. *Multiagent and Grid Systems*, *18*(1), 21-43.

[12] Dwivedi, S., Vardhan, M., & Tripathi, S. (2020). Distributed denial-of-service prediction on IoT framework by learning techniques. *Open Computer Science*, *10*(1), 220-230.

[13] Umar, M. A., Zhanfang, C., & Liu, Y. (2020, January). Network intrusion detection using wrapper-based decision tree for feature selection. In *Proceedings of the 2020 International Conference on Internet Computing for Science and Engineering* (pp. 5-13).

[14] Faker, O., & Dogdu, E. (2019, April). Intrusion detection using big data and deep learning techniques. In *Proceedings of the 2019 ACM Southeast conference* (pp. 86-93).
[15] Golrang, A., Golrang, A. M., Yildirim Yayilgan, S., & Elezaj, O. (2020). A novel hybrid IDS based on modified NSGAII-ANN and random forest. *electronics*, *9*(4), 577.
[16] Arun Prasad, P. B., Mohan, V., & Vinoth Kumar, K. (2024). Hybrid metaheuristics with deep learning enabled cyberattack prevention in software defined networks. *Tehnički vjesnik*, *31*(1), 208-214.
[17] Alkanhel, R., Rafiq, A., Saleh, M., Muthanna, A., Singh, D., Muthanna, A., & Aziz, A. (2024). Leveraging Metaheuristics with Deep Learning for DDoS Attack Detection in SDN based IoT Networks.
[18] Maheshwari, V., Bhatia, A., & Kumar, K. (2018, January). Faster detection and prediction of DDoS attacks using MapReduce and time series analysis. In *2018 International Conference on Information Networking (ICOIN)* (pp. 556-561). IEEE.
[19] Sankar, S. M., Dhinakaran, D., Deboral, C. C., & Ramakrishnan, M. (2023). Safe routing approach by identifying and subsequently eliminating the attacks in MANET. *arXiv preprint arXiv:2304.10838*.
[20] Mellette, W. M., Das, R., Guo, Y., McGuinness, R., Snoeren, A. C., & Porter, G. (2020). Expanding across time to deliver bandwidth efficiency and low latency. In *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)* (pp. 1-18).
[21] Gul, B., Khan, I. A., Mustafa, S., Khalid, O., Hussain, S. S., Dancey, D., & Nawaz, R. (2020). CPU and RAM energy-based SLA-aware workload consolidation techniques for clouds. *IEEE Access*, *8*, 62990-63003.
[22] Syed, N. F., Baig, Z., Ibrahim, A., & Valli, C. (2020). Denial of service attack detection through machine learning for the IoT. *Journal of Information and Telecommunication*, *4*(4), 482-503.
[23] Raj, R., & Kang, S. S. (2022, December). Mitigating DDoS attack using machine learning approach in SDN. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 462-467). IEEE.
[24] Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication systems*, *73*(1), 3-25.
[25] Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K. M., Almotairi, S., & Gulzar, Y. (2021). Distributed denial of service (DDoS) mitigation using blockchain—A comprehensive insight. *Symmetry*, *13*(2), 227.
[26] Sahosh, Z. H., Faheem, A., Tuba, M. B., Ahmed, M. I., & Tasnim, S. A. (2024). A Comparative Review on DDoS Attack Detection Using Machine Learning Techniques. *Malaysian Journal of Science and Advanced Technology*, 75-83.

Author Profile

Ameer Sameer Hamood born in Babylon, Iraq, on 06/01/1991. He is a dedicated and accomplished professional with a Master of Information Technology from University of Babylon, Babylon, Hilla/Iraq, 2018. He is an Assist Lecturer at University of Babylon's, Faculty of Information Technology, Department of Information Networks. He is member of PEARSON VUE Technical IT Administrator and Member of IEEE. Publications are Keywords Sensitivity Recognition of Military Applications in Secure CRNs Environments and Cognitive radio network security status and challenges in IEEE journal. He developed a robust understanding of network architecture, Artificial Intelligence, Cybersecurity, Cognitive Radio Networks specialist, Internet of Things, Software Defined Network, Wireless Sensor Network, Information and Communication Technology, Network Security, Cryptography, Machine and deep Learning.