International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

DDoS Attack Mitigation using Distributed SDN Multi Controllers for Fog Based IoT Systems

R. Ramalakshmi [1*], D. Kavitha [2]

Submitted: 05/09/2023 **Revised**: 22/10/2023 **Accepted**: 06/11/2023

Abstract - Software Defined Networking is an important platform today for handling huge like Internet of things and fog edge based networking devices. SDN is also a most prominent network platform for today's industrial diversity of setup such as cloud data storage, Industrial Internet of Things (IIoT), Network Function Virtualization (NFV), and Security attacks. So, SDN is handling application layer resources and physical layer edge devices along with security protection. Resources like cloud database storage is not capable enough for handling today's world huge data's. Similarly, a huge data's are originated from the various end devices via IoT based switches and gateways to the target resources. But due to the attacks like Denial of service (DoS) and Distributed denial of service attack (DDoS), the network is easily contaminated and destroyed the target resources and available bandwidth. So, in this scenario handling these data traffic and mitigating the attacks with privacy and authentication is an efficient task provided by SDN controller. But SDN controller will take only the managing and controlling part of the network. But still security is a very big concern in the today's huge data collection from IoT and other smart devices. So, Fog computing framework plays a vital role today to reduce the DDoS attacks from the different edge data sources by creating a micro clouds or fog nodes before accessing the cloud resources to manage and mitigate the DDoS attacks with the help of Distributed SDN multi controller and provides the additional layer of security for the network. This paper proposed the Machine Learning (ML) based DDoS attack mitigation process in IoT based SDN environment with Fog computing approach and secures the network from malicious packets with good detection accuracy.

Keywords: *SDN, DDoS, Fog computing, IoT, Machine Learning, Distributed multi controller.*

1. Introduction

Software defined networking is the most efficient powerful platform for the vast computational world devices and applications. SDN is having a decoupling behaviour of the networks data. So that, it could easily manage the resources for doing both controlling and forwarding activities in all the network intermediate nodes without delay. SDN architecture was improved in past decades from the single controller to distributed multi controller for the fast network growth [1] . Then distributed multi controller is capable of doing the controlling, managing, and security activities to the entire smart based network with the default open flow interfaces as well as integrating with new paradigm like edge computing devices and cloud computing applications too. So this work introduced the SDN controller along with Edge computing like smart IoT devices in forwarding layer with the help of fog computing middle layer framework and cloud computing resource access in application layer.

The SDN controller must be centralised in operation. As a result, DDoS assaults on the SDN controller for exploiting the cloud to fog are a distinct possibility. Some techniques may be used to develop a secure and dependable SDN controller to defend against various assaults. The internet services are rendered inaccessible during a Distributed Denial of Service (DDoS) attack by flooding them with unsolicited data traffic from various sources. The attack takes place in the compromised system's network layer or application

[1] *Research Scholar, Department of Electronics and Communication Engineering,*
Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil, Tamilnadu -626126, India, rama@klu.ac.in
**Correspondence: R. Ramalakshmi, E-mail: rama@klu.ac.in*
[2] *Professor, Department of Computer Science and Engineering,*
Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil, Tamilnadu -626126, India, Kavithadurairaj1984@gmail.com

layer, depending on how it is connected to the network [2].

The controller, as the centre point of an SDN network, is very vulnerable to a cyber assault and might have a significant impact on the entire network. Still, some features of SDN, such as traffic analysis, logically centralised control, a view of the network's global state, and dynamic updation of forwarding rules, make it a good choice for detecting and defending against DDoS attacks in both cloud and fog contexts. Regarding network security, it's also crucial to talk about traffic information such as flow-based and traffic-pattern-based load balancing in the SDN domain. [3]. DoS and DDoS assaults are the kind of attacks that can completely degrade the availability of a system. DDoS attacks are designed to make a machine or network resource unavailable to their target customers carried out by multiple people or bots. TCP, UDP, ICMP, and DNS packets are used to disrupt target clients by draining their network resources, or to deplete server resources such as sockets, ports, RAM, databases, and input/output bandwidth. The attack is known as network level flooding, and application level DDoS flooding, which is commonly done on an HTTP webpage.

Thousands of billions of IoT devices are connected to one another around the world. However, if all of those devices attempted to load the entire computation to the cloud for merely functionality work, there would be insufficient bandwidth to let all of these devices to connect with the cloud server on a continuous basis. It is critical to make the Internet of Things (IoT) concept understandable. This predicament is triggering a slew of new technologies and techniques to deal with all of the industrial and production-related data and information that is at the heart of the IIoT. This is the main concept that led to the term "fog computing" being coined. Fog computing has been known to use the phrase "edge computing" interchangeably on occasion. There is, however, a distinction between the two conceptions. Edge computing and fog Both entail bringing processing and intelligence capabilities closer to the point where the data is generated [4].

FC is a highly virtualized computing paradigm that is beneficial for providing additional support to the cloud environment, and it was initially launched by Cisco [5]. It works in a similar fashion to cloud, however it is not as centralised. Fog systems can be used to do local data analysis in edge devices, facilitating networking, computation, infrastructure, and storage support as a backbone for end user computing, primarily for IoT and IIoT smart devices. Security is a major issue and worry for both industry and academia while conducting data transactions through the cloud. However, security and privacy are two important issues that have stymied the development of fog computing and cloud computing. However, attacks such as DDoS and others have always put a strain on this. SDN (Software-Defined Network) is a new networking architecture that offers numerous benefits over traditional distributed computing. It simplifies networking for the development of new protocols and the deployment of new applications. Machine learning methods are used by the SDN controller to capture suspicious data flow and infer their validity.

The following are the contributions to this work:

1. To minimise DDoS attacks, a source-based defence technique is developed that might be employed in fog as well as in an IoT-based Distributed SDN Network configuration. The SDN controller has a defence module built in.

2. The cited study proposes an Ensemble machine learning (ML) based light detection approach that involves examining packet characteristics beforehand and utilising a suitable ML model to improve detection and processing rates.

3. It employs SDN technology, with the DDoS defender module deployed to counter DDoS attacks at the network/transport level.

There are difficulties in designing distributed and coordinated DDoS mitigation methods that successfully overcome the limitations of existing mitigation solutions, such as low detection efficiency, high computation power, and cost for all real-time applications and computation resources. The fundamental contribution of this research is to use the Fog computational technique in an IoT-enabled data environment to minimise DDoS attacks by assigning compute power and dispersing workload to provide faster and more accurate attack detection.

Fog will work as a firewall in lower-level end computing devices and as a router for higher-level application devices such as cloud storage and

control servers from a variety of resources. The prototype architecture of the Fog platform deployment in a network environment is shown in Figure 1. This study not only focuses on the fog network, but it also discusses the importance of the fog layer in SDN-based DDoS attack detection and mitigation in an IoT-based SDN network. This paradigm consists of n number of bottom layer nodes connected to a middle layer called fog, which incorporates fog nodes to handle more sensor and other computing devices from various users in the data plane, and then all of this is connected and controlled by SDN controllers with the end resources in the control plane.

In Section II, we'll go through the background knowledge of the SDN-based IoT system and the existing work on DDoS mitigation. Section III describes the design and operating processes for our DDoS mitigation scheme. Section IV details the algorithm's implementation and testing, and Section V concludes with a summary of the proposed algorithm.

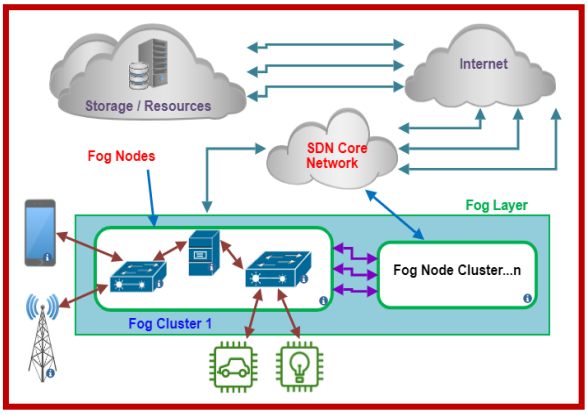

Fig1: Overview of Fog based SDN Network architecture

2. Background And Related Work

SDN is a good tool to handle DDoS attacks. DDoS defence mechanisms using SDN in three categories which are source-based, network- based and destination-based mechanisms. Many recent works have discussed about the design and security of fog based cloud and other network combinational environments also. This scheme considers a different network approach for IoT based SDN security using Fog computing approach. A peer reviews discusses the various dimensions like Fog based cloud without SDN, Fog based SDN, IoT based Fog, Fog based cloud on SDN, and so on using Machine learning or Simulation method of implementation. So, in this section some relevant works specific to the SDN based DDoS attack mitigation using Fog based edge computing paradigm. Most of the DDoS attack and its detection are based on network monitoring methods and some statistical analysis methods using ML approach. This paper focusing on SDN based DDoS detection via Fog layer environment. This proposed work was designed by many motivating factors such as existing literature and other real time analysis discussed below.

This section discussed about the DDoS attacks in the SDN based IoT domain. IoT devices are constantly producing massive amounts of data. All of this information is useless and must be extracted. This data processing at the network's edge is overcome using fog computing. As a result, fog computing is able to solve some of the most processing big data issues. Da Yin et.al [6] have discussed about the distributed denial-of-service (DDoS) attack and vulnerabilities in IoT. The emerging software-defined paradigm provides a way to safely manage IoT devices. It composed of an SD-IoT controller pool with controllers, SD-IoT switches integrated with the IoT gateway, and terminal IoT devices to find the real DDoS attacker, and block the DDoS attack at the source. Finally, this work proposed to extend the load balancing controller in SD-IoT based domain along with DDoS detection.

Song Wang et.al [7] have discussed about the SDN based IoT for DDoS attack control using secure control and dataplane (SECOD) algorithm. It handled only TCP and UDP traffics for DDoS attack detection and it is not suitable for all real-time IoT based traffic applications. M. Ejaz Ahmed and Hyoungshick Kim [8] have discussed about the SDN based DDoS security in IoT and by the way of mitigating the DDoS attack by using intermediate SDN domain before reaches the target network. Luying Zhou et.al [9] demonstrates the DDoS attack detection time and effectiveness on IIoT systems. Detecting and blocking DDoS attacks at the source has the benefit of effective protection and preservation of network resources, but it also has the disadvantage of making it difficult to distinguish between legitimate and attack traffic. Because the volume of traffic near the attacking sources may be low before the attack traffic converges on the victim's side. DDoS attack sources might be dispersed over multiple domains,

making it challenging to accurately detect and filter attack flows. It provides the distributed DDoS detection scheme with the multilevel architecture approach.

DA Yin et.al [10] have proposed the SD-IoT based DDoS attack detection . It detected the attacks by IoT controllers or switches itself. But, it could not handle heterogeneous type of packets from different IoT devices. So, this work could extend the SDN-IoT based attack mitigation for better performance. Myo Myint Oo et.al [11] have implemented the DDoS attack detection using SDN testbed with ML algorithm. It provided the better results of attack detection but not included the online data traffics. Amir Modarresi et.al [12] have demonstrated the fog based edge computing to manage the massive growth of IoT devices. This paper used the Fog layer with traditional approach to mitigate spoofing attacks by SDN controller. Rojalina Priyadarshini et.al [13] discussed about the Fog based SDN for DDoS attack detection using ML techniques based on Network monitoring and traffic engineering techniques. This paper analyzed the DDoS attack detection using Fog based SDN 3 layer environment and demonstrated the CPU utilization between before and after attack detection.

Sabireen [14], Zhang peiyun et.al [15], patwary et.al [5], Ashkan Yousefpour et.al [16] discussed about the various infrastructure issues in Fog with IoT edge computing in SDN domain as well as other privacy issues, authentication and all other challenging survey issues in IoT, sensor devices , SDN along with Fog layer and cloud centres. Saad Khan et.al [17] have also discussed about the Fog computing importance to overcome the problems due to the growth of IoT devices and its security challenges. Simer preet singh et. al [18] discussed about the fog computing storage and computational issues at the edge of the network and also discussed how fog computing overcomes the cloud computing drawbacks and challenges in big data processing. Ruilong Deng et.al [19] investigates about the power consumption and transmission delay in fog and cloud computing. It discussed about the workload allocation to decompose the problems into sub problems. But this paper works with only centralized manner. In order to efficiently handle unexpected traffic volume and attack types, DDoS mitigation based on fixed locations, such as source or destination, may need to overprovision features and capabilities.

Luying Zhou et.al [20] discussed about the DDoS attack detection using Fog approach in IIoT systems and implemented the virtualized rule based firewall three layer systems to detect the DDoS attacks using Snort method in industrial environment. Jianbing Ni et.al [21] discussed and surveyed the Fog computing security issues with IoT applications in terms of various attributes like storage, computation, security and threats . The function of fog nodes in IoT applications was also examined in this research, including real-time services, transitory storage, data dissemination, and decentralised computation. Bhumika Paharia and Kriti Bhushan [22] have discussed about the Fog based security against DDoS attacks between cloud and end users without SDN. The fog computing level is made up of controller clusters and servers that gather traffic data, identify DDoS attacks using network traffic data, and restrict DDoS attacks depending on detection.

Sarang Kahvazadeh et.al [23] discussed about the security issues in Fog to cloud Based network by reducing the distance between them using SDN centralized controllers. But still F2C security issues remain due to centralized controller. Rojalina Priyadarshini and Barik [24] have proposed the fog architecture between cloud and end computing devices to filter out the attack packets by deep learning method. It provides legitimate packets to the cloud resources via the Fog layer. The DDoS attacks are prevented on the Fog layer itself. Ola Salman Imad et .al [25] have presented the SDN Fog security for IoT data challenges. This work proposed the IoT security by using SDN and Fog based networks. Luying Zhou et.al [26] have discussed about the DDoS attack protection by using Fog computing approach in SDN testbed for huge number of deployed IoT and other local components and allocation of traffics in industrial automation domain. It proven the Fog computing based security against DDoS provides the better efficiency than the normal computing approach. This work focuses on detecting DDoS attacks using SDN-based fog computing technology. The report also discusses numerous obstacles, applications, benefits, and real-time applications of fog computing technology, pointing researchers in the right direction for future research.

3. Proposed Method

This study presents a framework for defending against DDoS attacks in a SDN-Fog environment. The goal is to identify and neutralise any attack traffic before sending it to the resources. A fog layer is being constructed between the cloud resource server and the bottom layer client to achieve this goal. All data flow passes through this transitory fog layer before reaching the cloud resources. The fog layer is where the malicious traffic is managed and dealt with, and this is where the attack traffic protection mechanism is placed along with the SDN controller. SDN distributed multi controller with Fog middle layer and the bottom layer with IoT components are setup by using the Mininet tool with Pox controller. The huge amount of IoT and sensor devices from the bottom layer /physical layer/ components layer are connected to the Fog intermediate layer via Fog based switches/ routers/ as Fog nodes. These various fog based middle layer nodes are connected the SDN centralized/Distributed Multi controller to access the Data base applications. All these layered structure are connected by Open flow interface protocols. This Fog based SDN controller is trained by machine learning programming against the DDoS attack generated from the bottom layer nodes such as IoT nodes. Our Fog is associated with the SDN controllers programming setup by various factors to detect the DDoS attack and block the attack by the SDN controller instructions. SDN controller is connected with both end that is application layer cloud/database and lower layer edge computing devices to capture the various packets. All the legitimate and malicious packets are received from the various nodes from the network devices and it is processed by the various Machine Learning process to detect the attack packets perfectly before reaching the resources via Fog with SDN controller. This method provides a better way of attack detection among network packets from different sources with Fog based SDN controller and without Fog based SDN controller. All the incoming packets are checked in Fog layer itself whether should be blocked or allowed to reach the destination resources. This proposed model architecture is shown in figure 2.

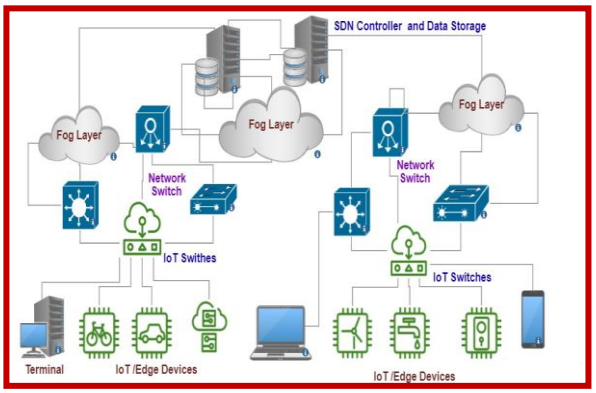

Fig 2: Proposed model DDoS attack detection on Fog based SDN-IoT Network

3.1 SDN- FOG-IOT based Network System

Software Defined Networking is a very important platform in all networking architecture and it makes a better flexible platform for any software and hardware implementation. This work concentrates an extension of the previous DDoS attack detection in IoT based systems by ML technique. In continuation of that edge computing devices like Fog layer is involved to connect various IoT and sensor digital devices from the physical layer to the centralized SDN controller for providing more security in today's huge network connection setup and large volume of traffics.

An application layer cloud resources are connected with the centralized/Distributed SDN controller. These SDN controllers are further connected with the distributed Fogs are located around the network. SDN distributed controllers are responsible for communication and security to the cloud resources from the edge layer. All the distributed Fog nodes are connected and controlled by SDN controller in one end and which are connected with the various end nodes via the gateway or switches. This section describes mainly about the edge devices, Fog layer nodes, and then SDN controllers. Finally all these are connected to the end resources like storage, security, management, and resource allocation.

This system design is developed based on that layer architecture for DDoS attack detection originated from the end nodes and it is crossed over via Fog layer controller unit from all the pool of distinct Fog nodes and then first stage of filtered datas are again verified in the master distributed SDN controller unit. Edge- Fog- SDN Controller- Resources are the

layered architecture to process the data to mitigate DDoS attacks using Machine learning method.

In existing works the DDoS attack detection was done by many ways like threshold based detection, snort rule based filtering, ML and DL based detection in SDN test bed only. But, recent years middle ware based edge computing security protection was playing a major role with the help of SDN controller and the various software techniques.

But, still many of the research work is not yet implemented for IoT systems based DDoS attack detection via Fog techniques in SDN domain. Mostly, it is under survey level. But, this proposed work has implemented the Fog based DDoS attack mitigation for IoT systems in SDN domain by using Machine learning method.

3.2 Machine Learning Attack detection method

Private data (e.g., IoT device data) generated from end users to application resources and vice versa should be monitored and detected by effective security rules and filtering techniques. Real DDoS attacks are used in this research, and a test bed is created to validate the model. With the help of the Mininet open source tool, DDoS assaults are carried out on TCP, UDP, and ICMP protocols via several random virtual computers.The Machine learning model is then used to process the attacked packets. The performance measures are chosen as a percentage of accuracy on test data. The DDoS Defence model was compared to current models that used ML and SDN in the past. A fog network is typically connected to a large number of small devices. When data from multiple devices is combined, the total amount of data becomes difficult to manage. As a result, filtering each network packet requires more processing time. So that SDN presents on Fog layer to identify and mitigate the DDoS attack presents in the network. All the distributed SDN supported Fog layers are connected to the core SDN controller network to access the cloud resources. So, the DDoS attack detection security scheme is handled and constructed by the machine language programme on the SDN controller through Fog layer.

The fog server is the point of presence where SDN controller is hosted. The packets coming from each node in the system are to be controlled by this. Different tools and scripts are being used to cause the attacks from source machines. The SDN Controller server is prior trained with the machine learning algorithms with the data that obtained some significant characteristics of the incoming data pattern. So that it could be able to classify the incoming packets as legitimate or not by using both binary and multiclass attributes. If they are found legitimate, then only be forwarded to the Application server. Else, the IP address of the corresponding packet is filtered and is forwarded to the flow table to be added to the Block list of switches pragmatically. The whole working mechanism of the model which is described above is depicted in Figure 3.

3.3 Fog based DDoS attack detection scheme

We can simulate both exhausting resources-based and protocol vulnerability-based DDoS attacks using field devices. The experiment also simulates a DDoS attack by sending packets from multiple networks at the same time in order to overwhelm the central controller, and such attack traffic could evade detection by the local server. The accuracy and reaction time of detection of such distributed DDoS attacks in the fog environment processing are used to evaluate the mitigation scheme's performance. The goal of any fog-based local network's DDoS detection module is to aggregate all traffic collected from own field devices and assess hidden correlation. This anomaly detection module, which runs as a virtualized functionality (NFV) on a local server, seeks to uncover hidden DDoS behaviours by creating network activity baselines and performing specification-based anomaly identification. If a hidden DDoS activity is proven, the detection module will notify the administrator for further mitigation activities, such as modifying the local fog node rules with SDN.

Both benign and malignant packets are transmitted from client sites that may request access to target services in this proposed effort. However, before reaching the destination service, all data flow must travel through the fog layer. The fog layer is made up of a number of fog devices and a fog server, which houses the SDN controller. The SDN controller serves as a central controller that inspects all incoming packets from different nodes. The data traffics are screened there, and the Fog server captures some specific characteristics that are used to determine if an incoming packet is legitimate or malicious. The attacks are created using a range of

tools from several source machines (i.e. Hping, scapy, wire shark, and scripts). The Machine learning algorithm is used to train the Fog server i.e. SDN controller. The algorithms are taught using collected features of incoming data traffic, which includes IoT devices. In other words, the server uses classifier models to determine if incoming packets are authentic or malicious. The packets are forwarded through the classifiers in response to an incoming request to determine if the requests are authentic or not. The packet is forwarded to the target server if it is determined to be valid. If it is determined to be suspicious, the IP address of the relevant packet is added to the prohibited list of the SDN controller's flow table of switches. At the switch level, enough programming is done to prevent the packet from being transmitted to the target server.

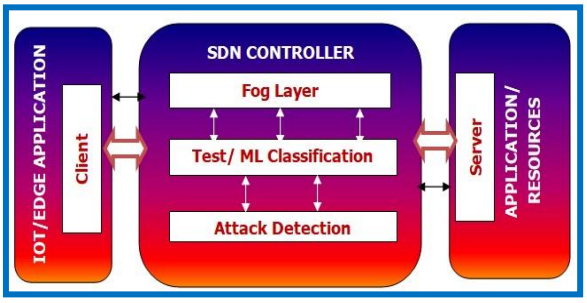

Fig 3: Working Mechanism of Fog based SDN-IoT Network model

3.4 Central SDN Analysis and consolidation

When the SDN central controller receives reports of suspicious DDoS behaviour from a particular fog local network, it examines the suspicious behaviour by comparing traffic characteristics from other distributed local networks to find patterns of similarity and detect distributed DDoS attack traffic that appears legitimate. The DDoS mitigation functions are distributed and performed in three multiple levels of the architecture. Packets are received from IoT systems, and then functions are executed from the local distributed Fog layer nodes. Finally, SDN controllers performs the computation schemes with Machine learning intelligence to filter out the anomalies such as DDoS attack and allow the legitimate packets to reach the resources. So, the local Fog nodes report the suspicious packets information such as "packet type, source address, destination address, type of protocols, etc.," to the associated SDN controller. Likewise, information are targeted from the multiple distributed networks and controlled by the central controller and produces the efficient output to the network. As a result, the Fog server, controller, and switch provide effective pre-processing security against attackers. SDN controller can quickly disconnect the pool from the extensive network security processing, even if the local fog pools are compromised by any malicious code, including DDoS, DoS, Ransom ware, Mirai, etc.

4. Experimental Results And Discussion

In the following section, the proposed design methodologies and testbed setups are applied, and the experimental findings are recorded and discussed. Existing literature rarely uses an industrial system as a test environment for DDoS mitigation, making a fair comparison between the proposed technique and existing methods difficult. As a result, we examine the suggested algorithm from a variety of angles and scenarios in order to demonstrate its efficacy in preventing DDoS attacks in the SDN- Fog- IoT context. Here, data such as detection time and rate are recorded and reported. Normally with or without DDoS attack packets, the SDN network with Fog computing approach start detecting attack packets and block the attacks. The studies are designed to assess the efficacy of the suggested approach, demonstrating that the Fog computing approach can respond quickly to a DDoS attack, effectively moderate the attack, and save network resources.

4.1 Data Sources

This study uses a customised network dataset that includes hosts, fog nodes, SDN controllers, IoT devices, and attack nodes. Mininet, Hping, scapy, Nmap, and Wire shark were used to build and create the dataset from an SDN-controlled Fog-IoT customised network. The information was created and traced from about 100 network activity nodes, and includes protocols used in both normal and attack settings. As part of our security study, we've tested DOS and DDoS attacks. Certain DDoS attack types, including ipsweep, multihop, smurf, snmpguess among others, are researched for attack detection and mitigation. The various attributes like Ipaddress, port, packet flow, temperature, humidity, motion status, pressure, protocol, source, destination, size, bytes, etc., Total dataset contains Approx. 2, 50,000 Packets. The following Table 1

shows the number of anomaly packets and normal packets from the raw IoT mixed dataset.

Because the central SDN server provides an entire system view of the traffic status, the fog computing solution delivers a faster detection time via SDN controller coordination, whereas the Fog level observes local traffic and takes longer to determine the assault traffic pattern. Several SDN Controller configuration rules are created using Ubuntu features. The Smurf assault, for example, is a typical DDoS attack that uses a large number of botnets to flood ICMP traffic at the victims. Botnets relate to a wide range of field devices, including IP cameras, Remote terminal units, and other similar devices. As shown in Tables 1 and 2, the Fog computing approach is used to measure the DDoS attack detection for different attack traffic types. For the SDN-Fog based distributed multi-controller IoT network, the proposed study employs the LR, KNN, MLP, and ID3 classifiers to detect assaults and assess their performance.

Table 1: Attack and Normal packet size.

S. No	Category	Label
1.	Anomaly	233864
2.	Normal	16008
3.	Total	249872

Table 2: A summary of dataset classification

S. No	Type	Count
1.	ICMP	165967
2.	TCP	30182
3.	UDP	23644
4.	Normal	16008
5.	Others	14071

The performance metric of machine learning models such as recall (R), F1-score (F1), accuracy (A), and precision (P) are used to calculate the performance of the attack detection.

- True Positive (TP): Number of true samples classified as true
- False Positive (FP): Number of false samples classified as true
- True Negative (TN): Number of false samples classified as false
- False Negative (FN): Number of true samples classified as false

The above measures are prescribed as follows:

$$Precision = \frac{TP}{TP+FP} \quad (4.1.1)$$

$$Recall = \frac{TP}{TP+FN} \quad (4.1.2)$$

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (4.1.3)$$

$$\text{F1\_score} = 2 \times \frac{\text{recall} \times \text{precision}}{\text{recall}+\text{precision}} \quad (4.1.4)$$

The equations 4.1.1, 4.1.2, 4.1.3 and 4.1.4 are used to calculate the DDoS attack detection from the data set and produce the results and its performance measures.

4.2 Results and Analysis

The proposed network testbed is created with Mininet SDN system, Python-based controller, and virtual Oracle VMware were utilised to detect SDN attacks. The setup has switches and routers, (1-100) range of IoT and other terminal nodes, two SDN-based controllers and two Fog-based controllers. Our experimental machine learning training model on an 8GB RAM and a 2TB hard drive hardware configuration. The operating system Windows 10, and Anaconda Jupyter Notebook with Python 3.6 as support were the programmes used. The SDN with IoT network datasets, including DDoS attack packets from traffic created in real-time, were the main components of the ML attack detection and mitigation setup. Figure 4 shows a sample SDN-FOG-IOT network architecture. It tells about the clients with normal and attack nodes connected to the SDN Controller along with Fog switch/gateway/controller. Based on the number nodes network traffic details will be varied.

Here, the various types of end nodes or physical layer nodes are mingled in. The fog layer, which is the middle layer, has switches that connect the IoT and SDN controllers to the fog controller. Root SDN controller is present in the higher layer.

Distributed connections between controllers have been made. Both regular and assault end nodes continuously send packets across switches and the fog controller.

Here, the packets connected with the SDN controller will undergo some local examination by the Fog controller, gateway, and router Similar to how each Fog and its associated pools of devices pre-processed packets and detected attacks using information from the SDN controller. Finally, the Root SDN controller receives all of the filtered packets so that it can fully mitigate attacks and stop abnormalities. Thus, the SDN controller's workload has been lightened while maintaining a high detection rate.

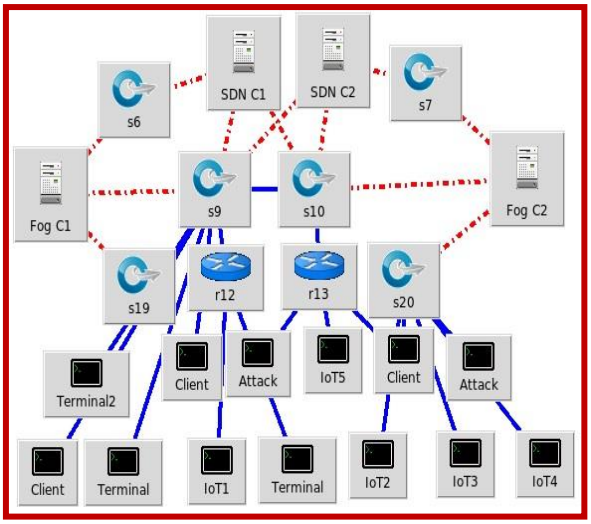

Fig 4: Model Experimental setup of Fog based SDN-IoT Network model

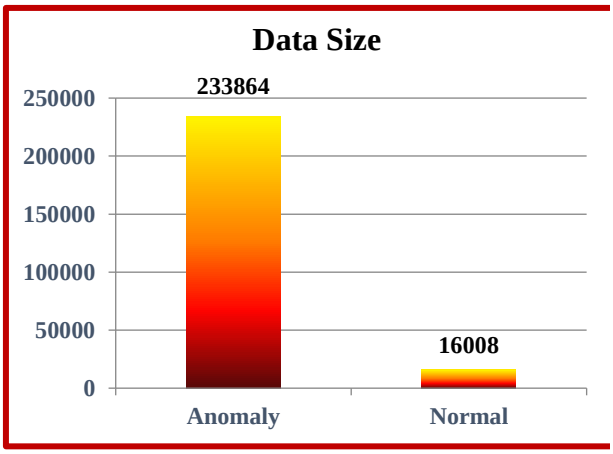

Fig 5: Attack and normal packets size

Figure 5 shows the representation of the total raw packet sizes of attack and normal.

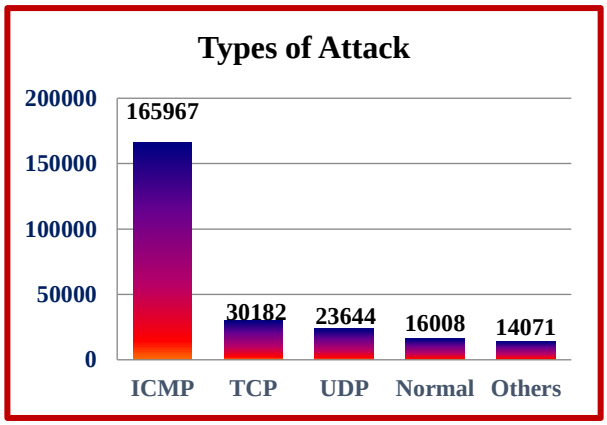

Fig 6: A summary of dataset classification

Figure 6 represents the results of dataset classifications for various DDoS attack types taken for the ML processing.

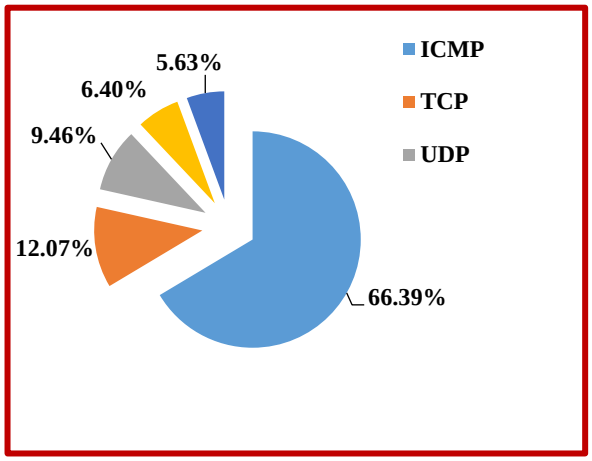

Fig 7: Percentage of the Attack and Normal packets.

The Figure 7 shows the percentage of dataset contributions in the given work to detect and mitigate the DDoS attack presents in the form of various packets as Tcp, Udp, Icmp, other packets, and non anomalies packets also.

Table 3: Time taken for DDoS attack mitigation

S. No	Type of Classifier	Time taken (Sec)
1.	LR	26.60
2.	KNN	26.67
3.	DT	26.73
4.	MLP	24.41

Table 3 gives the DDoS attack detection and mitigation time taken i.e. starting and ending time

difference of the respective classifiers to find out the various attacks from the dataset in seconds.

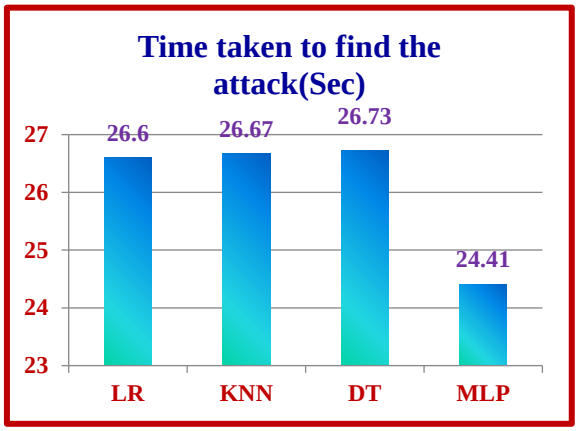

Fig 8: Output representation of the Accuracy

The Figure 8 shows the classifier resultant accuracy for DDoS attack packets with various classifiers. Out of these 4 classifiers decision tree gives the better performance. It produced the results in 26.73 seconds.

S. No.	Type of Classifier	Accuracy	Precision	Recall	F1_Score
1.	LR	0.52	0.49	0.49	0.45
2.	KNN	0.50	0.76	0.48	0.60
3.	DT	0.77	0.79	0.85	0.81
4.	MLP	0.44	0.45	0.43	0.37

Fig 9: Overall performance measurement.

The parameters obtained from the dataset processing for the identification of attack packets using the LR, KNN, DT, and MLP algorithms are explained in the figure 9. Based on the TP, TN, FP, and FN findings obtained from the relevant classifiers, attack performance metrics such as accuracy, precision, recalls, and F1-score are calculated. The overall accuracy of the model is calculated from the measured findings. As a result, the decision tree has produced the improved results for attack detection as demonstrated by the results above.

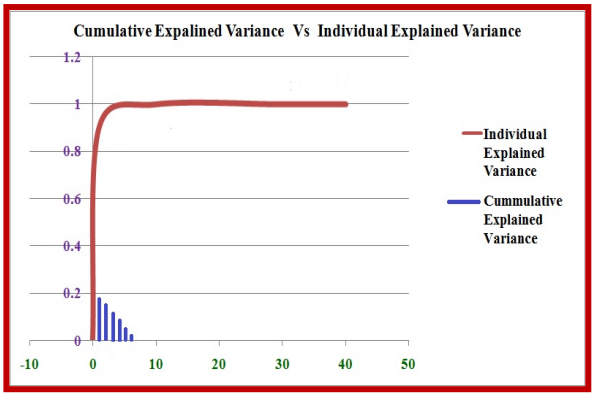

Fig 10: Output of variance by Machine Learning

The variance taken for ML processing for attack detection by different classifiers using the individual and cumulative explained variance method of analysis is depicted in Figure 10 as the number of variances.

These various variance parameters are derived from the characteristics of the dataset and used to compute the Eigen vectors and Eigen values to yield effective results. The ratio of each individual variance extracted from the dataset is shown via an Eigen vector.

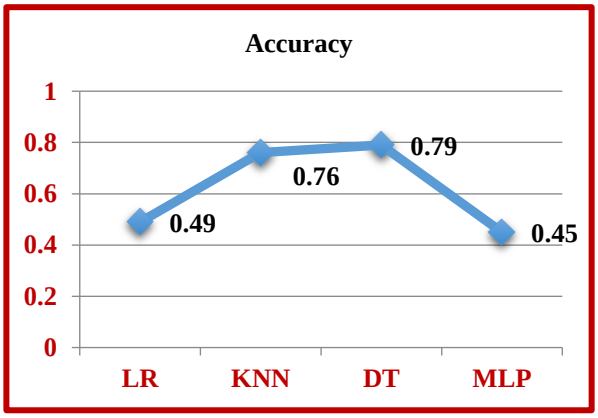

Fig 11: Output for Accuracy

Figure 11 illustrates the reliability of the results that were detected. The outcome is displayed using equation 4.1.3. The best accuracy is shown by Decision Tree, whereas MLP shows the least accuracy.

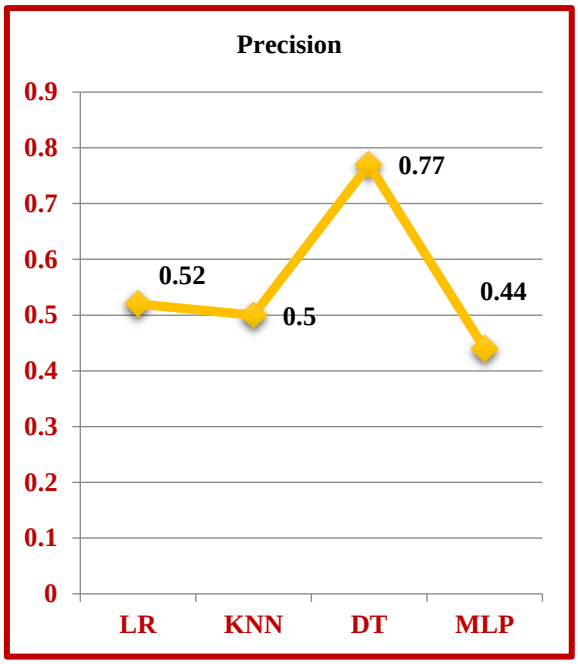

Fig 12: Output for Precision

The Precision of the Detected Results is displayed in Figure 12. The outcome is shown using equation 4.1.1 as a guide. MLP displays less precision value, while Decision Tree displays the best outcome.

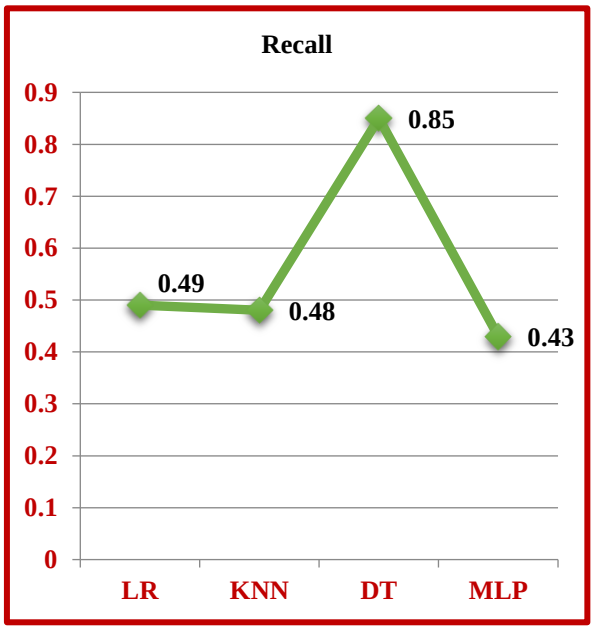

Fig 13: Output for Recall

Recall of the outcomes that were found is shown in Figure 13. Equation 4.1.2 is used to display the result. Decision Tree has the best sensitivity outcomes; while MLP displays the least remember values.

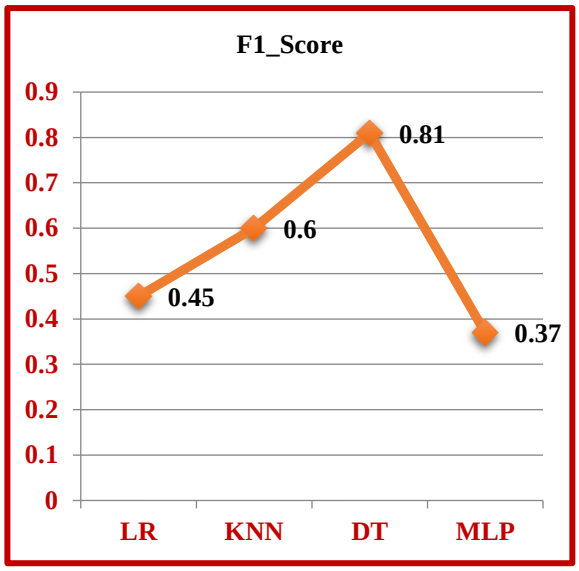

Fig 14: Output for F1_Score

The results that were found are shown in the F1score in Figure 14. The F1 score is nearly equal to the mean average of the two findings shown in equation 4.1.4. Decision tree displays the high F1 score together with the remaining values.

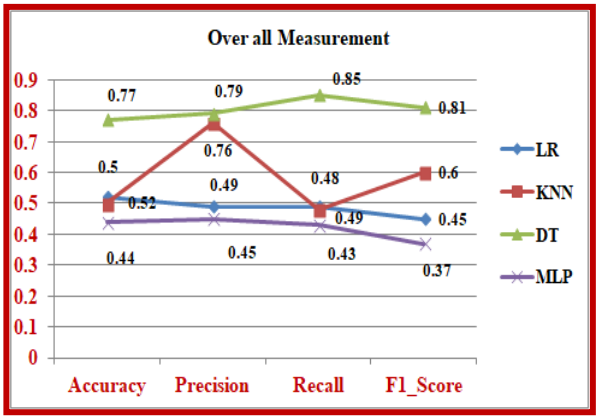

Fig 15: Output for the overall measurements

Figure 15 shows the overall measurements of the Accuracy, Precision, Recall, and F1 Score respectively. Decision tree produces the better detection performance than the other classifiers.

5. Conclusion

The technique of IoT and fog edge based DDoS attackdetection and mitigation utilising distributed SDN Multi Controller Network has been addressed in this suggested study. In order to create the network, this study employed a python-based open source setup together with additional tools and packages for creating packets with information

about normal and abnormal packets using a customised network. This machine learning mechanism processes a customised dataset made up of roughly 2,50,000 packets which also contains 2, 33, 864 abnormal packets and 16,008 regular packets for the detection of DDoS attacks using TCP, UDP, ICMP attack, and other regular packets. This Python-based Machine Learning model takes some time to recognize and analyze the assault before producing results in 26.60, 26.67, 26.73, and 24.41 seconds, respectively. Decision tree created the quick and efficient attack processing and detection findings from these results. The findings of this work's analysis of performance on the basis of accuracy, precision, recall, and F1-score were 77%,79%, 85%, and 81%, respectively. Based on these findings, Decision Tree outperforms other classifiers in terms of performance. Fog node middle layer gateway data to SDN controller dataset is used in this work. SDN intelligence will find both fog and IoT assaults. However, the benefit of a fogpool is that, should it become compromised, it can be quickly removed from the network. The Fog node will serve as a controller in future work and assist the SDN controller in conducting effective network analysis and providing increased protection. Finally, this work produced the better detection results and speed including Fog-IoT with SDN server using ML method in compare to the existing survey.

References:

[1] D. Kavitha, R. Ramalakshmi, R. Murugeswari, The Detection and Mitigation of Distributed Denial-of-Service (DDOS) Attacks in Software Defined Networks using Distributed Controllers, 2019 Int. Conf. Clean Energy Energy Effic. Electron. Circuit Sustain. Dev. INCCES 2019. (2019). https://doi.org/10.1109/INCCES47820.2019.9167698.

[2] D. Kavitha, R. Ramalakshmi, Fog-based SDN for DDOS Attack Mitigation in IoT Systems : A Survey , 13 (2020) 4161–4173.

[3] S. Prabakaran, R. Ramar, Software defined network: Load balancing algorithm design and analysis, Int. Arab J. Inf. Technol. 18 (2021) 312–318. https://doi.org/10.34028/iajit/18/3/7.

[4] S. Khan, S. Parkinson, Y. Qin, Fog computing security: a review of current applications and security solutions, J. Cloud Comput. 6 (2017). https://doi.org/10.1186/s13677-017-0090-3.

[5] A.A. Patwary, R.K. Naha, S. Garg, S.K. Battula, M. Gong, Towards Secure Fog Computing : A Survey on Trust, (2021) 1–52.

[6] L. Zhang, K.U.N. Yang, A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework, 6 (2018).

[7] S. Wang, K. Gomez, K. Sithamparanathan, M.R. Asghar, G. Russello, P. Zanna, applied sciences Mitigating DDoS Attacks in SDN-Based IoT Networks Leveraging Secure Control and Data Plane Algorithm, (2021).

[8] M. Ejaz Ahmed, H. Kim, DDoS attack mitigation in internet of things using software defined networking, Proc. - 3rd IEEE Int. Conf. Big Data Comput. Serv. Appl. BigDataService 2017. (2017) 271–276. https://doi.org/10.1109/BigDataService.2017.41.

[9] L. Zhou, H. Guo, G. Deng, A fog computing based approach to DDoS mitigation in IIoT systems, Comput. Secur. 85 (2019) 51–62. https://doi.org/10.1016/j.cose.2019.04.017.

[10] D. Yin, L. Zhang, K. Yang, A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework, IEEE Access. 6 (2018) 24694–24705. https://doi.org/10.1109/ACCESS.2018.2831284.

[11] M. Myint Oo, S. Kamolphiwong, T. Kamolphiwong, S. Vasupongayya, Advanced Support Vector Machine-(ASVM-) based detection for Distributed Denial of Service (DDoS) attack on Software Defined Networking (SDN), J. Comput. Networks Commun. 2019 (2019). https://doi.org/10.1155/2019/8012568.

[12] A. Modarresi, S. Gangadhar, J.P.G. Sterbenz, A Framework for Improving Network Resilience Using SDN and Fog Nodes, (2017) 1–7.

[13] R. Priyadarshini, R. Kumar Barik, H. Dubey, Fog-SDN: A light mitigation scheme for DDoS attack in fog computing framework, Int. J. Commun. Syst. 33 (2020) 1–13. https://doi.org/10.1002/dac.4389.

[14] H. Sabireen, V. Neelanarayanan, A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges, ICT Express. 7 (2021) 162–176. https://doi.org/10.1016/j.icte.2021.05.004.

[15] P. Zhang, M. Zhou, G. Fortino, Security and trust issues in Fog computing : A survey, Futur. Gener. Comput. Syst. 88 (2018) 16–27. https://doi.org/10.1016/j.future.2018.05.008.

[16] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, J.P. Jue, All one

needs to know about fog computing and related edge computing paradigms: A complete survey, J. Syst. Archit. 98 (2019) 289–330. https://doi.org/10.1016/j.sysarc.2019.02.009.

[17] S. Khan, S. Parkinson, Y. Qin, Fog computing security: a review of current applications and security solutions, J. Cloud Comput. 6 (2017). https://doi.org/10.1186/s13677-017-0090-3.

[18] S.P. Singh, A. Nayyar, R. Kumar, A. Sharma, Fog computing: from architecture to edge computing and big data processing, J. Supercomput. 75 (2019) 2070–2105. https://doi.org/10.1007/s11227-018-2701-2.

[19] R. Deng, R. Lu, S. Member, C. Lai, Optimal Workload Allocation in Fog-Cloud Computing Towards Balanced Delay and Power Consumption, X (2016) 1–11. https://doi.org/10.1109/JIOT.2016.2565516.

[20] A. Wani, S. Revathi, DDoS Detection and Alleviation in IoT using SDN, J. Inst. Eng. Ser. B. (2020). https://doi.org/10.1007/s40031-020-00442-z.

[21] J. Ni, K. Zhang, X. Lin, X.S. Shen, Securing Fog Computing for Internet of Things Applications: Challenges and Solutions, IEEE Commun. Surv. Tutorials. 20 (2018) 601–628. https://doi.org/10.1109/COMST.2017.2762345.

[22] B. Paharia, Fog Computing as a defensive approach against Distributed Denial of Service (DDoS): a proposed architecture, (2018).

[23] X. Masip-bruin, E. Marn-tordera, R. Diaz, Securing combined Fog-to-Cloud system Through SDN Approach, (n.d.).

[24] R. Priyadarshini, R.K. Barik, A deep learning based intelligent framework to mitigate DDoS attack in fog environment, J. King Saud Univ. - Comput. Inf. Sci. (2019). https://doi.org/10.1016/j.jksuci.2019.04.010.

[25] O. Salman, A. Chehab, PT US AC CR, Comput. Networks. (2018). https://doi.org/10.1016/j.comnet.2018.07.020.

[26] L. Zhou, H. Guo, G. Deng, A Fog Computing Based Approach to DDoS, Comput. Secur. (2019). https://doi.org/10.1016/j.cose.2019.04.017.

[27] Carlos Silva, David Cohen, Takashi Yamamoto, Maria Petrova, Ana Costa. Ethical Considerations in Machine Learning Applications for Education. Kuwait Journal of Machine Learning, 2(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/192

[28] Reddy, B.R.S., Saxena, A.K., Pandey, B.K., Gupta, S., Gurpur, S., Dari, S.S., Dhabliya, D. Machine learning application for evidence image enhancement (2023) Handbook of Research on Thrust Technologies? Effect on Image Processing, pp. 25-38.

[29] Dasi , S. ., & Rao, G. M. . (2023). Design and Analysis of Metamaterial Absorber using Split Ring Resonator for Dual Band Terahertz Applications. International Journal on Recent and Innovation Trends in Computing and Communication, 11(1), 128–132. https://doi.org/10.17762/ijritcc.v11i1.6059