

DDoS Detection Framework Using Machine Learning with Adaptive AI and Moving Target Defence

Anusree Vinod¹, Alaigha KR², Sambath Kumar S³

^{1,2,3} Department of CS and IT
^{1,2,3} Jain Deemed-To-Be University

Abstract - DDoS attacks are some of the major cyber threats that pose a serious risk to computer networks through their capacity to cause a significant burden of traffic on servers and network infrastructures, resulting in their unavailability to legitimate users and causing disruptions. In recent times, there has been a significant rise in the occurrence of DDoS attacks due to an increase in new technologies like cloud computing and IoT, hence reducing the effectiveness of security solutions in terms of their ability to detect such attacks. In order to solve this problem, this research work suggests the adoption of a machine learning approach as an effective technique for detecting and defending against DDoS attacks. Several machine learning models are developed for DDoS attack detection using the CIC-DDoS2019 dataset containing attacks such as DNS amplification, LDAP reflection, and NTP attacks among others. It is found out that Random Forest and XGBoost achieve better performance in terms of high detection accuracy of greater than 99%. In addition to the above-discussed detection method, the proposed solution features an adaptive AI-based defense system that can respond to emerging risks. With the use of a self-learning engine, the system will be able to update itself in real time using machine learning techniques. In addition to that, Moving Target Defense (MTD) can be applied to change configurations and resources of the attacked network in order to boost system resistance.

Key Words: Distributed Denial of Services (DDoS), Machine Learning, Network Intrusion Detection, Random Forest, XGBoost, Online Learning, Adaptive AI-Based Defence, Moving Target Defence.

I. INTRODUCTION

Digital technologies, cloud services, and connected systems are growing very quickly, which has made network infrastructure much more important for everyday tasks. These technologies

have made it easier to talk to people and get online services. But this growth has also brought about a number of security problems. The most unfortunate event that could befall modern networks is a distributed denial-of-service attacks [2], [10]. In situations where a huge number of hacked computers all bombard one particular server or network simultaneously; the resultant situation is known as a DDoS attack. Such an attack will overwhelm the network, slow it down, and cause the users not to access their services. The nature of DDoS attacks has grown over the years to become complicated, thus making it difficult to combat them. Hackers usually take advantage of devices that are easily hackable, especially IoT devices, so as to cause a business loss through unavailability of services among others. Many of today's DDoS attacks also use reflection methods, which make the traffic bigger and harder to find and stop [4], [9]. Firewalls and intrusion detection systems that are made to find and block suspicious traffic are two examples of traditional ways to protect a network [8], [12]. Because of this, accurate machine learning-based detection here is a growing need for intelligent and automated systems that can analyse large amounts of network traffic and detect malicious behaviour in real time [1],[11]. In recent years, ML techniques have shown strong potential for improving network intrusion detection systems [2],[7]. Machine learning algorithms can study complex patterns in network traffic data and learn to distinguish between normal and malicious activities. Several algorithms such as Random Forest, XGBoost, and Support Vector Machine, have been widely used for network traffic classification because they can handle large datasets and identify meaningful patterns from many features [10],[11]. Although machine learning models have shown promising results in detecting DDoS attacks, many existing studies mainly focus only on the detection process and do not provide effective methods to prevent or reduce the impact of attack after they are detected [10],[11],[15],[18]. Detection alone may not be enough if the system cannot respond quickly

to stop or reduce the damage caused by the attack. Thus, the integration of intelligent detection methods and adaptive defence methods is one of the major research areas in the current cybersecurity scenario.

This research proposes a framework for the efficient detection of DDoS attacks using various ML methods to improve networks security through an adaptive defence system. Various ML methods are employed to evaluate the efficiency of these methods in detecting DDoS attack from various networks traffic data sets containing various DDoS attack scenarios [10],[11]. In addition to the detection system, the proposed framework is also provided with an adaptive AI defence system, that can respond to the detection system when the latter detects an attack. The proposed framework also includes a self-learning system that can continuously update the detection system with the newly learned attack patterns. In addition, the proposed framework includes Moving Target Defence, an efficient defence system for DDoS attacks as the network is constantly changing, making it difficult for the attackers to launch attacks in the long run [12], [17]. By integrating an efficient machine learning-based detection technique along with adaptive and dynamic defence mechanisms, the proposed framework attempts to increase the robustness of modern network infrastructure against DDoS attack threats in an ever-changing environment [1],[11]. By combining accurate machine learning-based detection with adaptive and dynamic defence mechanisms, the proposed framework aims to improve the resilience and reliability of modern network infrastructures against evolving Distributed denial of Service attack threats [1],[11].

The main things that this research does is come up with a way to defend against attacks. This defence framework uses intelligent that can teach itself learn from the internet and prevent attack in a smart way. It also uses something called Moving Target Defence to make it harder for Distributed Denial of Service attacks to work. This means the systems can keep learning all the time, about dealing with threats and change the network settings to reduce the damage from attacks [12],[17].

The rest of this paper is set up like this. Section II talks about what other people have found out about detecting Distributed

Denial of Service attacks using machine learning [2],[10]. Section III proposes the adaptive AI-based architecture for the detection and mitigation of DDoS attacks. Section IV explains the experimental setup and the machine learning algorithm used for traffic classification [10],[11]. Section V describes the results and performance evaluation of the proposed system using various detection and prevention mechanisms. Finally, section VI concludes the proposed system.

II. LITERATURE REVIEW

Recent research has investigated diverse methodologies for identifying Distributed Denial of Service (DDoS) attacks through ML and DL techniques [1],[2],[5],[10]. Researchers have employed various network traffic datasets and implemented a range of methodologies, including feature selection, anomaly detection, ensemble learning, and hybrid DL frameworks. The goal of these studies is to make it easier and more accurate to find wrong traffic in modern networks like cloud computing. The Internet of Things (IoT) and Software Defined Networks (SDN). Table 1 below summarizes the most important research contributions from fifteen chosen studies. It shows the most important research contributions from fifteen chosen studies. It shows the datasets used, the algorithms used and the results of finding DDoS attacks.

Table 1: Overview of Existing DDoS Detection Approaches in Literature.

Sl.No	Author	country	Dataset	Methods Applied	Task	Algorithm used	Result
1	Becerra- Suarez et al. [1]	Spain	Network Traffic	Feature Selection and Dimensionality	Detection and classification of DDoS attacks	Machine learning algorithm models	Improves detection accuracy by selecting relevant features and removing unnecessary data
2	Musa et al. [2]	Malaysia	SDN Network Traffic	Anomaly detection in Software Defined Networks	Detection of DDoS attacks in SDN	ML and DL models	Enhanced detection performance and improved identification of abnormal traffic patterns
3	Altalhihan et al. [3]	Saudi Arabia	IoT Network Traffic Dataset	Traffic pattern	Detection of DDoS attack in IoT environments	Machine Learning Algorithms	Successfully detected abnormal traffic generated by malicious IoT devices.
4	Al-Zubidi et al. [4]	Iraq	Network Traffic Dataset	Hybrid deep learning Framework.	Detection and prediction of Dos and DDoS attacks	Hybrid Deep Learning Models	Achieved higher classification accuracy compared with traditional approaches.
5	Alashhab et al. [5]	United Arab Emirates	SDN Traffic Dataset	Ensemble learning approach	Detection of DDoS attacks in Software Defined Networks	Ensemble Online ML	Improved adaptability and accuracy in dynamic network environments.
6	AlSaleh et al. [6]	Saudi Arabia	Cloud Network Traffic Dataset	Data fusion with deep learning	Detection of DDoS attacks in cloud computing environments	Bayesian Convolutional Neural Network (CNN)	High performance in analyzing complex cloud network traffic.
7	Ahmed et al. [7]	Egypt	Network traffic dataset	Deep learning-based classification	Detection of DDoS attacks	Multi-Layer Perceptron (MLP)	Achieved high classification accuracy for multiple attack types.

8	Mittal et al. [8]	India	Multiple Benchmark Network datasets	Comparative study of deep learning techniques	Analysis and detection of DDoS attacks	Various Deep Learning Algorithms	DL models performed better than traditional ML methods
9	Elbeyd & Yilmaz-Kaplan [9]	Turkey	SDB Network Dataset	Hybrid Deep Learning architecture	Detection of DoS and DDoS attacks	Hybrid Deep Learning Models	Improved detection accuracy and robustness.
10	Kumar et al. [10]	India	Network traffic Dataset	Temporal traffic pattern analysis	Detection of DDoS attacks	Recurrent Neural Network (RNN)	Effectively detected attack patterns over time
11	Dhanya et al. [11]	India	Network Attack Dataset	Comparative analysis of ML and DL models	Network attack detection	Machine Learning and Deep Learning Algorithms	Deep Learning models achieved higher detection accuracy
12	Ramesh et al. [12]	India	Network Traffic Dataset	Hybrid learning approach	Network protection against DDoS attacks	Hybrid Machine Learning Models	Produced more reliable and accurate detection results.
13	Mustapha et al. [13]	Nigeria	Network Security Dataset	Adversarial neural network training	Detection of DDoS attacks	Adversarial Neural Networks	Increased robustness against sophisticated cyber-attacks.
14	Salmi & Ough Dir et al. [14]	Morocco	Wireless Sensor Network Dataset	Lightweight deep learning analysis	Detection of Dos attack in WSN	Deep Learning algorithms	Efficient detection with lower computational cost.
15	Alahmadi et al. [15]	Saudi Arabia	IoT Network Datasets	Survey of ML-based detection methods	DDoS detection in IoT network	Various Machine Learning Techniques	Identified research gaps and highlighted the need for light weight detection models

ML- Machine Learning

DL- Deep Learning

SVM – Support Vector Machine

Distributed Denial of Service (DDoS) attacks are a problem. People have been studying how to detect these attacks. They found out that using ML and DL methods can really help improve the detection process for DDoS attacks in network environments [8].

Many people have done research to improve the detection process for Distributed Denial of Service attacks. They used hybrid and ensemble methods to make the detection process more accurate for DDoS attacks. Most of these studies only focus on detecting Distributed Denial of Service attacks. They do not have solutions to prevent and stop these Distributed Denial of Service attacks.

This means we need to come up with plans that include both detecting and preventing Distributed Denial of Service attacks. So, the goal of this research is to address these issues by including both detection and prevention strategies, for Distributed Denial of Service attacks [9].

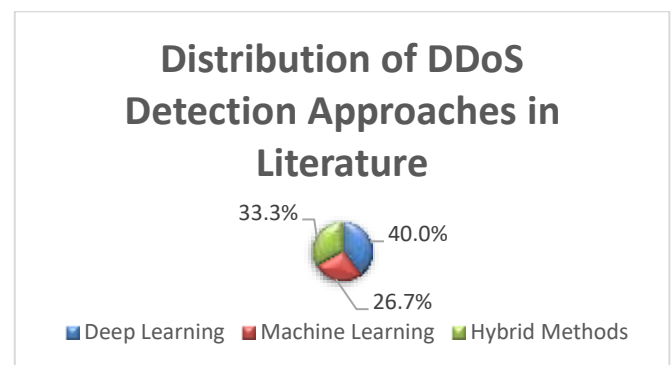


Fig.1. Distribution of ML, DL, and hybrid approaches used in DDoS detection literature [10].

The pie chart illustrates the distribution of different approaches used in existing research for DDoS attack detection. Deep learning techniques represent the largest proportion of studies, followed by hybrid approaches that combine ML and DL methods. Traditional machine learning techniques are also widely used but appear slightly less frequently compared to deep learning-based solutions [11].

III. PROPOSED METHODOLOGY

This part is about the design of the system that can find and stop DDoS attacks. The system uses ML and adaptive defence mechanisms to do this. The goal of the system is to find network traffic and take action against attacks that it finds.

The system is made up of machine learning and adaptive defence mechanisms that work together to keep the network safe from Distributed Denial of Service attacks. The system always checks the network traffic. Looks at the traffic to see if it is good or bad. It uses machine learning to do this. When the system finds an attack, it looks at how bad the attack is and chooses the best way to stop it. If the attack is very bad the system uses a mechanism called Moving Target Defence to stop the attack. This mechanism changes the network settings to minimize the damage from the attack on the network.

The system focuses on Distributed Denial of Service attacks and utilizes ML along with adaptive defence mechanisms to detect and prevent these attacks. Distributed Denial of Service attacks are stopped by the system using Moving Target Defence mechanism when they are very bad. The system is designed to keep the network safe, from DDoS attacks by using ML and adaptive defence mechanisms. The proposed methodology consists of multiple components that work together to provide both detecting and prevention of DDoS attacks.

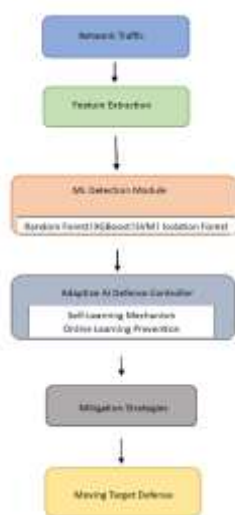


Fig. 2. Proposed Adaptive AI-Based DDoS Detection and prevention Architecture

This figure illustrates that proposed adaptive framework for detecting and preventing Distributed Denial of Service attack. The system begins with monitoring incoming network traffic, from which relevant features are extracted for further analysis. These extracted features are then processed by the machine learning detection module, which utilizes algorithms such as Random Forest, XGBoost, and Support Vector Machine to classify network traffic as either benign or malicious. Once an attack is detected, the adaptive AI-based defence controller dynamically determines the appropriate mitigation strategy. Finally, the system activates the Moving Target Defence Layer, which modifies network configuration to reduce the effectiveness of forced attacks and improve overall network resilience.

A. Components of Proposed Methodology

1. Network Traffic Monitoring

The first stage of the proposed system involves continuous monitoring of incoming network traffic. Network packets are captured and analysed to identify potential abnormalities in traffic patterns. Monitoring tools and packet capture mechanisms are used to collect traffic data such as packet size, flow duration, source and destination addresses and protocol information. This collected traffic data forms the input for the subsequent feature extraction process.

2. Feature Extraction

After capturing network traffic, relevant features are extracted to represent the behaviour of network flows. Feature extraction plays an important role as in transforming raw packet data into meaningful attributes that can be processed by machine learning algorithms. Main feature extraction process includes packet rate, flow direction, number of packets per flow, protocol type, and statistical metrics related to traffic behaviour. These features help differentiate between normal traffic patterns and malicious DDoS traffic.

3. Machine Learning Detection Module

The extracted features are then passed to the machine learning detection module, which classifies network traffic as benign or malicious. Several machine learning Algorithms are evaluated in this study, including Random Forest, XGBoost, and SVM.

These models are trained using labelled network traffic datasets to learn patterns associated with DDoS attacks. Once trained, the models can accurately detect malicious traffic in real-time network environments.

4. Adaptive AI-Based Defence Controller

Once an attack is detected by the machine learning module, the system activates the adaptive defence controller. This component analyses the force of attack and characteristics of the detected attack and determines the most appropriate mitigation strategy. The adaptive AI-Based defence mechanism continuously learns from newly detected attack patterns and updates its response accordingly. By adapting to the changing attack behaviours, the system also improves its ability to mitigate evolving cyber threats.

The adaptive AI-driven defence controller makes use of self-learning and online learning techniques which help the controller to constantly evolve its mitigation strategy through continuous learning from new attack.

5. Moving Target Defence Layer

The system must be capable of adapting and responding to changing conditions. So, the new plan for the system includes something called Moving Target Defence. This Moving Target Defence is a way to stop people from getting into the system. It does this by changing things like how the systems set up and the addresses that the computers use to talk to each other. The paths that the information takes to get from one computer to another also gets changed. This means that the attackers will only have time figuring out how to get into the system because it is always changing. The Moving Target Defence makes it hard for the attackers to launch an attack on the system. The system is better able to with stand attacks from the people because of the Moving Target Defence. The Moving Target Defence helps to stop the people from doing a lot of damage, to the system with bis attacks.

6. Dataset

Several Datasets representing various Distributed Denial of Service attack scenarios are employed to evaluate the effectiveness of the proposed DDoS detection and prevention system. These datasets include real-world traffic situations and

the network traffic flows recorded during different attack simulations. The CICDDoS2019 dataset, which is frequently used in cybersecurity research for training and assessing machine learning intrusion detection systems, is the source of the datasets [1],[10]. Every dataset contains parameters about the flow of network traffic and describes a specific type of DDoS attack. These parameters enable one to differentiate between the normal network traffic flow and the abnormal network traffic caused by DDoS attacks and cover certain features of the network traffic such as packets per second, flow duration, and source of attack traffic. The datasets utilized in this work cover many types of attacks like DNS amplification attacks, LDAP reflection attacks, SYN flooding attacks, NTP amplification attacks.

The list of datasets used in the experimental evaluation includes:

1. DrDoS DNS
2. DrDoS LDAP
3. DrDoS MSSQL
4. DrDoS NetBIOS
5. DrDoS NTP
6. DrDoS SNMP
7. DrDoS SSDP
8. DrDoS UDP
9. SYN
10. TFTP
11. UDP Lag

Each of these datasets contains labelled traffic instances categorized as either attack traffic or begin traffic. These labelled samples serve as the training and testing data for evaluating the performance of the ML detection models.

TABLE 2: Overview of DDoS Attack Datasets Utilized in this study

Dataset	Samples	Features	Attack Types
DrDoS DNS	14971	80	DNS Amplification
DrDoS LDAP	14719	80	LDAP Reflection
DrDoS MSSQL	14782	80	MSSQL Amplification
DrDoS NetBIOS	14552	80	NetBIOS Attack
DrDoS NTP	14948	80	NTP Amplification
DrDoS SNMP	14605	80	SNMP Amplification
DrDoS SSDP	14680	80	SSDP Reflection
DrDoS UDP	14890	80	UDP Flood
SYN	14720	80	SYN Flood Attack
TFTP	14910	80	TFTP Amplification
UDP Lag	14650	80	UDP Flood

Table 2 shows the datasets we use for testing. Each dataset is a DDoS Attack case with network flow features. These features come from captured traffic. Tell us a lot about how the network behaves. This helps machine learning algorithms tell the difference, between traffic and malicious traffic patterns in a DDoS attack. The dataset represents DDoS attack scenarios.

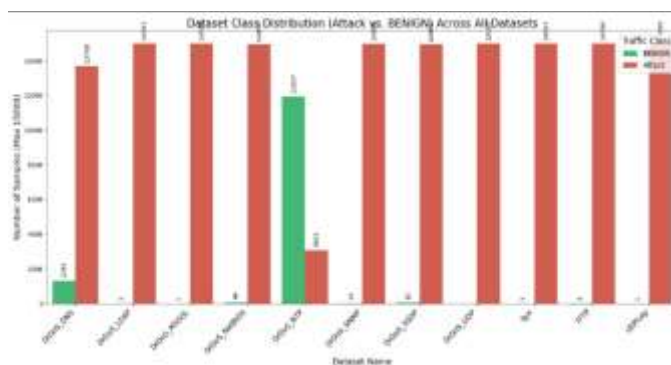


Fig. 3. Class distribution of attacks and begin traffic datasets

The distribution of be and attack traffic in the dataset is illustrated in Figure 3. It can be seen that there are more attacks than normal traffic in the dataset. This is because such types of DDoS datasets are predominantly filled with attack data.

IV. EXPERIMENTAL SETUP

This section addresses the ML approaches utilized to detect malicious traffic generated from DDoS attacks. In order to examine their ability to distinguish between malicious attack traffic and begin traffic, several machine learning models were selected [10], [11]. In order to evaluate how effective the algorithms are in detecting DDoS attacks, a mixture of supervised and unsupervised learning algorithms was employed. Random Forest, XGBoost, and Support Vector Machine models can be used in supervised learning algorithms [10], [11]. Such models need training on network traffic data

that has already been classified into either malicious or begin. This training is performed on data which is referred to as “labels data”. Furthermore, begin an isolation forest model based on unsupervised learning can be used [8], [13]. Unlike supervised learning models, an isolation forest model does not rely on labeled data to detect anomalies in network traffic. This ensures that any anomalies in the data can be detected by the model which could suggest a potential DDoS attack. Features extracted from network traffic data were used to train both models. The performance of both models was assessed using metrics such as F-1, Accuracy, Precision and Recall.

A. Random Forest

From the generation of a final classifying output, an ensemble learning method called Random Forest constructs multiple decision trees as part of its process. To enhance classification accuracy and minimize the risk of overfitting, the Random Forest algorithm employs a group of decision trees instead of relying on a single decision tree. The final prediction is decided by majority vote after each tree independently classifies the input data. Random Forest is robust and dependable to this method, even when working with complicated datasets that have a lot of features. Random Forest can analyse several aspects of network traffic at once in the context of network intrusion detection and find patterns that differentiate DDoS attack traffic from regular traffic.

B. XGBoost

A very powerful ML algorithm called XGBoost (Extreme Gradient Boosting) employs a boosting method of prediction. In boosting predictions, an ensemble of weak learners is trained in aa sequential fashion so that each new prediction corrects the errors of the previous predictions. XGBoost creates one single tree at a time and the result produced by each tree provides additional information to allow better prediction tree approaches. In addition, XGBoost uses a form of gradient optimization to improve accuracy over time. XGBoost excels at producing prediction models using structured datasets because of numerous advantages offers by the algorithm including regularization to reduce overfitting, parallel computing to improve calculation time, and tree

pruning to remove branches that are not required. XGBoost is well suited for detecting sophisticated forms of DDoS attack by utilizing analysis of the patterns of network traffic and examination of the hidden associations between the features of the data sample.

C. Support Vector Machine (SVM)

The Support Vector Machine is a ML technique that people use to group things. The most important things that the Support Vector Machine does is find a line that separates the different kinds of data that it is processing. The Support Vector Machine also looks for special points called support vectors when it is learning from the data. These are the points that are closest to the line that separates the different kinds of data that the SVM is working with.

The SVM is really good at looking at a group of data that has a lot of different things to consider. This makes the Support Vector Machine really useful for looking at the data that comes from a network because the data that comes from a network can sort through all the network data and help find the attackers by separating the good traffic from the attackers by finding the line that separates the two different kinds of traffic.

D. Isolation Forest

The Isolation Forest algorithm is used in the study to find strange traffic patterns in the network data. The model works by picking features at random and then splitting the data into different branches of decision trees over and over again. Data more quickly. The isolation forest helps find flows that don't follow normal patterns when used on networks traffic data. Since DDoS attacks generate irregular and abnormal traffic behaviour, these attacks-related data points can be detected as anomalies. In this research, Isolation Forest is primarily used for comparison with supervised ML models to assess the effectiveness of anomaly detection methods in identifying DDoS attacks [8],[10],[11],[13].

V. RESULTS AND DISCUSSION

To evaluate how well the proposed detection framework can identify Distributed Denial of Service (DDoS) attack

traffic, several commonly used performance metrics are applied [2],[10]. These metrics help determine how accurately the machine learning models can distinguish between attack traffic and normal (begin) network traffic [10],[11]. The evaluation is based on the confusion matrix, which summarizes the prediction results by comparing the actual labels of the data with the labels predicted by the models. The confusion matrix contains four key elements: True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN).

- True Positive (TP): Instances where attack traffic is correctly identified as an attack.
- True Negative (TN): Instances where normal traffic is correctly identified as begin.
- False Positive (FP): Instances where normal traffic is mistakenly classified as an attack.
- False Negative (FN): Instances where attack traffic is mistakenly classified as normal.

Using these values, various evaluation metrics such as accuracy, precision, recall, and F1-score can be calculated. These metrics provide a clear understanding of the effectiveness of the ML models in detecting DDoS attacks and help compare the effectiveness of various models within the framework [10],[11].

Table 3: Performance evaluation metrics used for assessing the effectiveness of machine learning models in DDoS attack detection.

Metric	Description
Accuracy	Proportion of accurately predicted cases to the overall number of cases.
Precision	The proportion of true positive predictions out of all positive predictions made.
Recall	The proportion of true positive predictions compared to the total number of actual positive cases.
F-1 Score	The harmonic average of a model's precision and recall values.

The main performance measure applied for assessing the efficiency of the ML models are summarized in Table 3. In most cases the following measures are used when addressing classification problems like Accuracy, Precision, Recall and F-1 score. Precision is used as a measure of the success rate of

correctly detected stack attack cases against all predicted attacks, whereas accuracy is an indicator showing how accuracy the model predicts attacks. On the other hand, recall is an indicator evaluating how effective the model detects genuine attacks, meanwhile, the F-1 score is a composite measure considering both the accuracy and the recall measures. When combined these metrics offer a thorough evaluation of the model's performance in identifying DDoS assaults in network traffic datasets.

A. Accuracy

The accuracy of a classifier is determined by the performance of the classifier based on the number of classifications executed. Accuracy is measured by the number of classifications made on attack and non-attack traffic.

The accuracy is calculated as:

$$Accuracy = \frac{TP+TN}{TN + FP + FN} \quad \text{-----}(1)$$

A higher accuracy value shows that the performance that are differentiating between legitimate and illegitimate traffic is better.

B. Precision

The precision measures give us information about the number of true attacks found among all attacks that the classifier believes are attacks. This will let us know if the classifier can find the traffic.

The precision is calculated as:

$$Precision = \frac{TP}{TP + FP} \quad \text{-----}(2)$$

If the precision value is high that means the model does not give us false warnings when it is looking for attack traffic. Precision is what we use to measure how good the model is, at finding attacks.

C. Recall

Recall, also known as sensitivity or detection rate, measures the model's accuracy in detecting actual samples. It shows how well the algorithm finds harmful activity in the dataset. It shows how well the algorithm finds harmful activity in the dataset.

The recall is calculated as:

$$Recall = \frac{TP}{TP + FN} \quad \text{-----}(3)$$

A high recall value indicates that the majority of the assault cases in the dataset are correctly identified by the model.

D. F1 Score

Precision and recall are balanced by the F1 score. When a dataset contains more of one type of data than another, like in network security, it is beneficial.

Precision and recall are used to determine the F 1 score:

$$F1 \text{ Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad \text{-----}(4)$$

Finding malicious traffic and making fewer incorrect predictions are key components of a higher F1 score. When assessing performance, precision, memory, and the F1 score are crucial. The F 1 score is especially helpful when it comes to datasets.

E. Confusion Matrix

The confusion matrix is a performance evaluation tool which visually represents the classification result of the machine learning model. It shows how many samples are correctly and incorrectly classified. The matrix consists of four values:

Table 4: Confusion matrix representation for evaluating the classification performance of the DDoS detection model.

	Predicted Attack	Predicted Begin
Actual Attack	True Positive	False Negative
Actual Begin	False Positive	True Negative

Table 4 shows the confusion matrix used to validate the performance of the proposed DDoS detection model. It compares the actual network traffic with the predicted results and includes four outcomes: True Positive, False Positive, True Negative, and False Negative, which help in measuring the accuracy of the classification model.

1. Experimental Results

This section represents the experimental results obtained from evaluating the proposed machine learning based DDoS detection framework. Multiple classification models were trained and tested on different attack datasets in order to analyse their detection capability and classification performance. The performance of the model is evaluated using metrics such as accuracy, precision, recall, and F-1 score.

The following subsections represents a comparative analysis of the evaluated models.

I. Accuracy Comparison

To compare the performance of different ML algorithms, the detection accuracy of each model was calculated across multiple DDoS attack datasets. Accuracy measures the percentage of accurate samples among the total number of samples. Table 2 presents the accuracy results obtained by the evaluated models.

Table 5: Model Accuracy Comparison Across DDoS Datasets

Dataset	Random Forest	XGBoost	SVM	Isolation Forest
DrDoS DNS	99.93%	99.93%	97.59%	7.94%
DrDoS LDAP	99.96%	99.96%	99.96%	0.03%
DrDoS MSSQL	100%	100%	100%	0%
DrDoS NetBIOS	99.96%	99.96%	99.96%	0.34%
DrDoS NTP	99.83%	99.89%	99.66%	80.30%

Table 5 compares the detection accuracy of the evaluated machine learning model across multiple DDoS attack datasets.

I. Accuracy Comparison Graph

To better visualize the performance differences among the evaluated models, an accuracy comparison graph is presented. The graph illustrates the accuracy achieved by each machine learning model across the selected candidates.

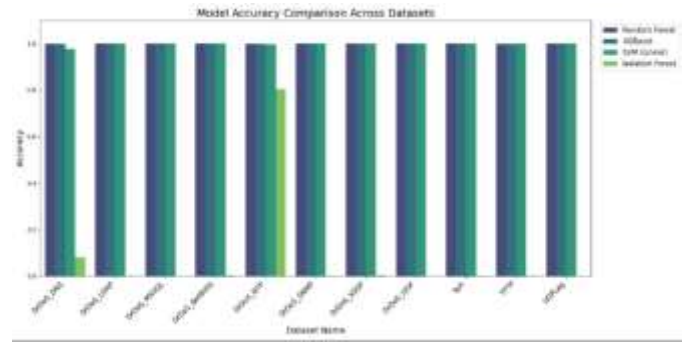


Fig. 4. Accuracy Comparison of machine learning models across DDoS datasets.

Fig 4 illustrates that ensemble learning models achieve consistently higher accuracy compared to the anomaly detection-based Isolation Forest model.

I. Confusion Matrix Visualization

In addition to the accuracy comparison, confusion matrices are often used to analyse the classification behaviour of the ML model in detail. The confusion matrix offers a clear representation of accurately and inaccurately identified cases for both attack and benign traffic.

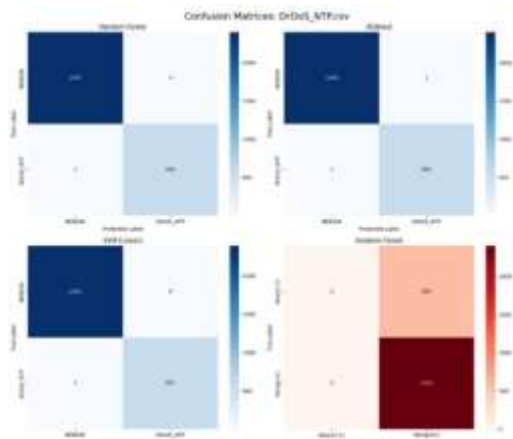


Fig. 5. Confusion matrices of machine learning model evaluated on the DrDoS NTP dataset

The confusion matrices presented in Figure 5 illustrate the classification outcomes of the evaluated models. Each matrix illustrates the quantities of true positives, true negatives, false positives, and false negatives for attack and benign traffic classification.

I. Model Performance Analysis

The experimental result show that ensemble learning model like Random Forest and XGBoost have the best detection accuracy on most datasets. These models can accurately capture complicated patterns in network traffic features, which makes classification work better. The Support Vector Machine model works well too, but in some datasets, it is not as accurate as methods that use multiple models. This could be because linear separation doesn't work well with network traffic data that has a lot of dimensions. The Isolation Forest Model, on the other hand, has much lower classification accuracy for a number of datasets [8], [13]. Isolation Forest is an unsupervised anomaly detection algorithm, which makes it less effective at telling the difference between good or bad traffic than supervised learning methods [8], [13].

In summary, the findings suggests that ensemble-based machine learning models provide more reliable detection performance for Distributed Denial of Service attack identification [10],[11].

II. Proposed Integrated Defence Framework

The suggested system uses Self-Learning AI, Online Learning, Adaptive AI-based Prevention, and Moving Target Defence (MTD) to make a smarter and flexible defence system that can find and stop DDoS attacks in network environments. The system can learn from network traffic all the time, change the network configurations to make ongoing attacks less effective, and adapt to new attack patterns. Traditional DDoS defence systems use predefined rules, which do not necessarily adapt to newly developed methods of attacks. In the proposed system, learning and adaption process will be constantly ongoing.

Components of the Proposed System

1. Self- Learning AI Module

The Self-Learning AI module's function is to monitor and analyse network traffic, detecting any abnormalities that could be indicative of an incoming attack. The AI module begins by learning the normal behaviour of the network by analysing various network traffic attributes such as the rate at which

packets arrive in the aspects of network traffic, where each request is made from an IP address, traffic bursts, connection lifetime, and the distribution of protocols. With the knowledge of normal network behaviour, the system would be able to identify any abnormality that would be suggestive of an attack. In contrast to only pre-training using datasets, the self-learning AI module continually updates its databases by analysing network traffic in real-time.

2. Online Learning Module:

Online Learning is incorporated into the process to ensure that the AI models remain current in terms of any data that may be collected from the network as and when it becomes available. Many conventional systems incorporate machine learning - based models which are trained offline on pre-texting datasets. Then they are deployed without any further updating of the model parameters. This tends to increase the time required for detecting any new attacks or changing patterns of attack. Online learning helps in modifying the model parameters gradually during the runtime phase of the application to overcome this difficulty.

3. Adaptive AI-Based Prevention module:

The Adaptive AI-defence is applied after detection of any suspecting traffic. Instead of taking any predefined actions against the threat, it takes into account several parameters, such as the seriousness of the attack, network traffic, available resources, and the type of the attack itself. Depending on the result of such analysis, the system decides what kind of counteraction should be taken for example, blocking suspecting traffic, separating suspecting nodes, or applying additional security measures like Moving Target Defence.

4. Moving Target Defence (MTD) Module:

Another security measures included within this security framework is Moving target Defence. This measure changes the structure of the network so that the attacker cannot easily recognize the target or fixate on a particular target. For example, some measures that might be taken include changing IP addresses of the servers, dynamically changing service ports, changing the network route, and moving services around

different servers. These measures ensure that the chances of services interruption are reduced, and any attack that can be made becomes increasingly difficult.

5. Discussion

In order to detect and mitigate the risks posed by network attacks, the proposed system will go through several stages in its operations. Packet capture and traffic analysis will be used to constantly observe the network traffic. Relevant attributes such as packet rate, flow size, and request frequency will be extracted and resented in the form of feature vectors. These feature vectors will then be analysed using the Self-Learning AI module in order to determine any irregular traffic behaviour that may be indicative of a possible attack. To augment the capacity of the detection model to detect new attacks, the online learning process will incrementally update the model with current traffic data. Using information on the detected threat level, the Adaptive -AI module will select the most appropriate responses. Through the Moving Target Defence module, changes to the network configurations will be implemented in order to mitigate the effects of the attack.

Table 6: Accuracy comparison of different AI-based prevention methods across various DDoS attack datasets.

Dataset	Self-Learning AI	Online Learning	Adaptive AI	MTD
DrDoS DNS	97.90%	96.36%	99.90%	99.93%
DrDoS LDAP	0.14%	99.90%	99.97%	99.93%
DrDoS MSSQL	0.30%	99.93%	99.97%	NA
DrDoS NetBIOS	99.73%	99.97%	99.97%	99.93%
DrDoS NTP	94.92%	94.92%	99.83%	99.70%

Table 6 indicates the accuracy archived by different AI-enabled preventive measures when defending against various forms of DDoS attacks including DrDoS, DNS, DrDoS LDAP, DrDos MSSQL and DrDoS NTP. Some of these methods include Self-Learning AI, Online Learning, Adaptive AI and Moving Target Defence (MTD). The use of adaptive AI approach detects all forms of attack accurately, with an accuracy value near 99.9%. The Moving Target Defence (MTD) techniques also ensure that these attacks are ineffective by making necessary changes on the networks in real time. In contrast, the self-learning AI and

online approaches vary with regard to accuracy based on datasets used.

VI. CONCLUSION

DDoS attacks represent one of the major issues faced by current-day network systems. They are characterized by saturating servers with large amount of traffic and preventing normal services from being provided. For this reason, in the present research an innovative solution for identifying and mitigating the occurrence of DDoS attacks was developed. Such a solution is characteristics by the application of intelligence and ML algorithms in order to analyze traffic flows in the network and identify their characteristics. By analyzing the traffic, the relevant parameters were established while machine learning algorithms such as established while machine learning algorithms such as Random Forest and XGBoost were used in order to differentiate normal traffic from the attackers one. The conclusions drawn from this study confirm the possibility of using ML algorithms in order to detect abnormal network activity associated with DDoS attacks. While some machine algorithms proved their efficiency in separating malicious and normal traffic, other such as Isolation Forest could distinguish abnormal traffic flow patterns regardless of the training process. Combining these models increases the system's capacity to identify DDoS attacks in dynamically evolving networks. The Adaptive AI-Based Defence Controller also contributes to increasing the efficiency of the proposed system, being able to respond to attacks from outside. In the case when an attack has been detected, the system is capable of performing different actions, such as monitoring suspicious request slowing down, analysing or blocking attackers IP addresses. In case of a serious attack, the system activates Moving Target Defence strategy, which causes changes in the network configuration making it more difficult for the attacker to continue their activity. In general, it is possible to say that this system represents a solution that allows detecting and mitigating DDoS attacks by means of implementing machine learning for attack detection and defence strategies.

VII. REFERENCE

- [1] F. L. Becerra-Suarez, I. Fernández-Roman, and M. G. Forero, "Improvement of Distributed Denial of Service Attack Detection through Machine Learning and Data Processing," *Mathematics*, vol. 12, no. 9, 2024, doi: 10.3390/math12091294.
- [2] N. S. Musa, N. M. Mirza, S. H. Rafique, A. M. Abdallah, and T. Murugan, "Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks - Current Research Solutions," *IEEE Access*, vol. 12, no. January, pp. 17982–18011, 2024, doi: 10.1109/ACCESS.2024.3360868.
- [3] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms," *Sensors*, vol. 24, no. 2, 2024, doi: 10.3390/s24020713.
- [4] A. F. Al-Zubidi, A. K. Farhan, and S. M. Towfek, "Predicting DoS and DDoS attacks in network security scenarios using a hybrid deep learning model," *Journal of Intelligent Systems*, vol. 33, no. 1, 2024, doi: 10.1515/jisys-2023-0195.
- [5] A. A. Alashhab et al., "Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model," *IEEE Access*, vol. 12, no. April, pp. 51630–51649, 2024, doi: 10.1109/ACCESS.2024.3384398.
- [6] I. AlSaleh, A. Al-Samawi, and L. Nissirat, "Novel Machine Learning Approach for DDoS Cloud Detection: Bayesian-Based CNN and Data Fusion Enhancements," *Sensors*, vol. 24, no. 5, 2024, doi: 10.3390/s24051418.
- [7] S. Ahmed et al., "Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron," *Future Internet*, vol. 15, no. 2, pp. 1–24, 2023, doi: 10.3390/fi15020076.
- [8] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review," *Soft Computing*, vol. 27, no. 18, pp. 13039–13075, 2023, doi: 10.1007/s00500-021-06608-1.
- [9] H. Elubeyd and D. Yiltas-Kaplan, "Hybrid Deep Learning Approach for Automatic DoS/DDoS Attacks Detection in Software-Defined etworks," *Applied Sciences (Switzerland)*, vol. 13, no. 6, 2023, doi: 10.3390/app13063828.
- [10] D. Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DDoS Detection using Deep Learning," *Procedia Computer Science*, vol. 218, pp. 2420–2429, 2022, doi: 10.1016/j.procs.2023.01.217.
- [11] K. A. Dhanya, S. Vajipayajula, K. Srinivasan, A. Tibrewal, T. S. Kumar, and T. G. Kumar, "Detection of Network Attacks using Machine Learning and Deep Learning Models," *Procedia Computer Science*, vol. 218, pp. 57–66, 2023, doi: 10.1016/j.procs.2022.12.401.
- [12] G. Ramesh, V. A. K. Gorantla, and V. Gude, "A hybrid methodology with learning-based approach for protecting systems from DDoS attacks," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 5, pp. 1317–1325, 2023, doi: 10.47974/JDMSC-1747.
- [13] A. Mustapha et al., "Detecting DDoS attacks using adversarial neural network," *Computers and Security*, vol. 127, 2023, doi: 10.1016/j.cose.2023.103117.
- [14] S. Salmi and L. Oughdir, "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network," *Journal of Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00692-w.
- [15] A. Alahmadi et al., "DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions," *Electronics (Switzerland)*, vol. 12, no. 14, pp. 1–24, 2023, doi: 10.3390/electronics12143103.
- [16] Ahmed, Sheeraz, et al. "Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron." *Future Internet*, vol. 15, no. 2, 2023, pp. 1–24, <https://doi.org/10.3390/fi15020076>.
- [17] Ahmim, Ahmed, et al. "Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model." *IEEE Access*, vol. 11, no. November, 2023, pp. 119862–75.
- [18] Bhayo, Jalal, et al. "Towards a Machine Learning-Based Framework for DDOS Attack Detection in Software-Defined IoT (SD-IoT) Networks." *Engineering Applications of Artificial Intelligence*, vol. 123, no. May 2023, 2023, p. 106432.
- [19] Ma, Ruikui, et al. "A DDoS Attack Detection Method Based on Natural Selection of Features and Models." *Electronics (Switzerland)*, vol. 12, no. 4, 2023.
- [20] Sadhwani, Sapna, et al. "A Lightweight Model for DDoS Attack Detection Using Machine Learning Techniques." *Applied Sciences (Switzerland)*, vol. 13, no. 17, 2023.