INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 08 ISSUE: 01 | JANUARY - 2024 SJIF RATING: 8.176 ISSN: 2582-3930

DDoS Attack Detection Using ML/DL Techniques

Jyotsna.Nanajkar[1], Mayuresh.Warang[2], Pratik.Suthar[3], Shivam.Shinde[4], Atharv.Pawar[5]

Professor, Information Technology, ZCOER, Pune, India[1]

Student, Information Technology, ZCOER, Pune, India[2]

Student, Information Technology, ZCOER, Pune, India[3]

Student, Information Technology, ZCOER, Pune, India[4]

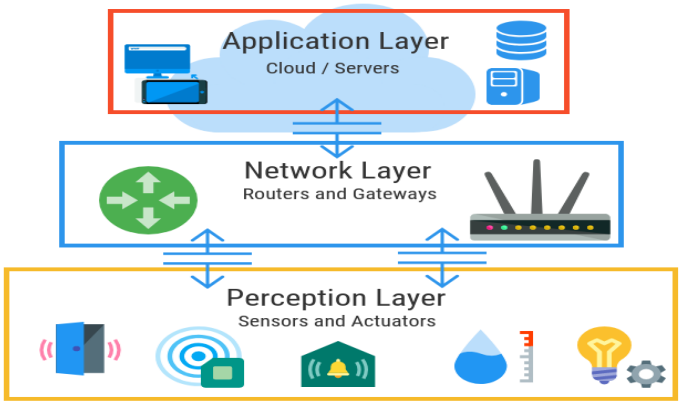
Student, Information Technology, ZCOER, Pune, India[5]

Abstract**—** *The increasing integration of IoT devices has heightened the vulnerability of networks to sophisticated and evolving cyber threats, particularly DDoS attacks, which can severely disrupt service availability. Leveraging machine learning algorithms, this research aims to enhance the proactive identification of anomalous patterns indicative of DDoS attacks within IoT environments. By employing a combination of feature extraction, classification, and ensemble learning methods, the proposed model demonstrates promising results in distinguishing between normal network behaviour and malicious activities associated with DDoS attacks. The study contributes to the advancement of security measures in IoT networks, offering a proactive and adaptive solution to mitigate the impact of DDoS attacks, ultimately bolstering the resilience of interconnected systems in the evolving landscape of cyber threats. This study presents a novel approach for the detection of Distributed Denial of Service (DDoS) attacks in Internet of Things (IoT) networks using machine learning techniques.*

I. INTRODUCTION

In the rapidly expanding landscape of the Internet of Things (IoT), the proliferation of interconnected devices has not only ushered in unprecedented levels of convenience and efficiency but has also introduced new security challenges. Among these challenges, Distributed Denial of Service (DDoS) attacks pose a significant threat to the availability and reliability of IoT networks.

This study addresses the critical need for robust security measures by introducing a machine learning-based approach for the detection of DDoS attacks in IoT environments. With the inherent complexity and dynamic nature of IoT networks, traditional security mechanisms fall short in effectively identifying and mitigating DDoS threats. Leveraging machine learning algorithms enables a more adaptive and proactive defence strategy, allowing for the real-time identification of anomalous patterns associated with DDoS attacks. This research aims to contribute to the ongoing efforts to fortify the security infrastructure of IoT networks, fostering a resilient ecosystem capable of withstanding the evolving landscape of cyber threats.



IoT Security Issues:

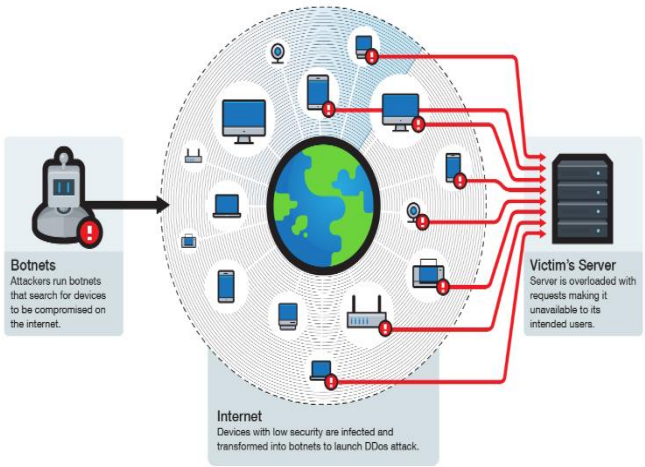
IoT (Internet of Things) security presents a multifaceted challenge, encompassing a range of issues that must be addressed to ensure the integrity and privacy of connected devices and networks. One of the primary concerns is the vulnerability of IoT devices to cyberattacks due to their often limited computing resources and inadequate security measures. Insecure communication channels and insufficient authentication mechanisms make these devices susceptible to unauthorized access and data breaches. Additionally, the sheer volume of interconnected devices creates a vast attack surface, expanding the potential points of entry for malicious actors[1]. Furthermore, the lack of standardized security protocols across IoT devices exacerbates the problem, making it difficult to

implement consistent and robust security measures. As IoT continues to proliferate in various sectors, addressing these security issues becomes paramount to safeguarding sensitive data, maintaining user trust, and ensuring the seamless integration of connected technologies into our daily lives.

[1] Ruchi Vishwakarma, Ankit Kumar Jain " A survey of DDoS attacking techniques and defence mechanisms in the IoT network" Springer Science+Business Media, LLC, part of Springer Nature 2019

DDoS Attack:

Distributed Denial of Service (DDoS) attacks represent a pervasive and disruptive form of cyber threat, targeting online services and networks by overwhelming them with a flood of traffic from multiple sources. In a typical DDoS attack, a multitude of compromised computers, often forming a botnet, is coordinated to generate an excessive volume of requests or traffic, thereby saturating the targeted system's resources and rendering it temporarily or completely inaccessible to legitimate users. These attacks exploit vulnerabilities in network protocols, servers, or applications, aiming to disrupt the availability of online services, websites, or entire networks. DDoS attacks can vary in scale and sophistication, ranging from relatively simple volumetric attacks to more intricate application-layer attacks that specifically target weaknesses in the targeted system's software. Mitigating the impact of DDoS attacks requires robust defense mechanisms, such as traffic filtering, load balancing, and the utilization of specialized DDoS mitigation services, to safeguard the availability and functionality of online services in the face of evolving cyber threats.



II RELATED WORK

Ismail1, Muhammad Ismail Mohmand1, Hameed Hussain, Ayaz Ali Khan, Ubaid Ullah1, Muhammad Zakarya, Aftab Ahmed, Mushtaq Raza, Izaz Ur Rahman, Muhammad Haleem [1] in their paper "A Machine Learning based Classification and Prediction Technique for DDoS Attacks" have proposed a complete framework for DDoS attacks prediction. For the proposed work, the UNWS-np-15 dataset was extracted from the GitHub repository and Python was used as a simulator. For this paper, they have used Random Forest and XGBoost classification algorithms. They have used machine learning algorithms for DDoS Attack Classification. In the first classification, the results showed that both Precision (PR) and Recall (RE) are 89% for the Random Forest algorithm. The average Accuracy (AC) of our proposed model is 89% which is superb and enough good. In the second classification, the results showed that both Precision (PR) and Recall (RE) are approximately 90% for the XGBoost algorithm.

Monika Roopa, Prof. Gui Yun Tian and Prof. Jonathon Chambers [2] in their paper "An Intrusion Detection System Against DDoS Attacks in loT Networks" have proposed an Intrusion Detection System (IDS) using the hybridization of the deep learning technique and multi-objective optimization method for the detection of Distributed Denial of Service (DDoS) attacks in the Internet of Things (loT) networks. In this paper, they have proposed an IDS founded on the fusion of a Jumping gene-adapted NSGA-II multi-objective optimization method for data dimension reduction and the Convolutional Neural Network (CNN) Integrating Long Short-Term Memory (LSTM) deep learning techniques for classifying the attack. They have used CISIDS2017 datasets on DDoS attacks and achieved an accuracy of 99.03 % with a 5-fold reduction in training time.

Vimal Gaur and Rajneesh Kumar [3] in their paper "Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices" proposed a hybrid methodology for selecting features by applying feature selection methods on machine learning classifiers. In this paper feature selection methods, namely chi-square, Extra Tree and ANOVA have been applied to four classifiers Random Forest, Decision Tree, k-nearest Neighbors and XGBoost are used for early detection of DDoS attacks on IoT devices. They have use the CICDDoS2019 dataset containing comprehensive DDoS attacks to train and assess the proposed methodology in a cloud-based environment (Google Colab). The proposed hybrid methodology provides superior performance with a

feature reduction ratio of 82.5% by achieving 98.34% accuracy with ANOVA for XGBoost and helps in the early detection of DDoS attacks on IoT devices.

Amal A. Alahmadi, Malak Aljabri, Fahd Alhaidari, Danyah J. Alharthi, Ghadi E. Rayani, Leena A. Marghalani, Ohoud B. Alotaibi and Shurooq A. Bajandouh [4] in their paper " DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions" proposed review selected studies and publications relevant to the topic of DDoS detection in IoT-based networks using machine-learning-relevant publications. There is an analysis of machine learning algorithms for different datasets like KDD-99, CICDoS17, BoT-IoT, NSL-KDD, TON_IoT, IoTID20, CIC-DDoS-2019 and many more.
Pravinder Singh Saini, Sunny Behal and Sajal Bhatia [5] in their paper "DDoS Attacks Detection using Machine Learning Algorithms" proposed a machine learning approach for detecting and classifying DDoS attacks in network and different types of network traffic flow. The proposed approach is validated for new datasets having new types of DDoS attacks such as HTTP Flood, SID DoS and normal traffic.WEKA is used for classifying various attacks and the J48 algorithm is used for classification which gives 98.64% accuracy better than RF and NB.

Umar Islam, Ali Muhammad, Rafiq Mansoor, Md Shamim Hossain, Ijaz Ahmad, Elsayed Tag Eldin, Javed Ali Khan, Ateeq Ur Rehman and Muhammad Shafiq [6] in their paper "Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring Systems of Banking Sector Using Machine Learning Models" propose to detect distributed denial-of-service (DDOS) attacks on financial organizations using the Banking Dataset. In this research, they have used multiple classification models for the prediction of DDOS attacks. They have further applied a support vector machine (SVM), K-Nearest Neighbors (KNN) and random forest algorithms (RF). The SVM shows an accuracy of 99.5%, while KNN and RF scored an accuracy of 97.5% and 98.74%, respectively, for the detection of (DDoS) attacks.

The provided tabular content showcases several researchers and their methodologies employed in the domain of intrusion detection and cybersecurity using various datasets and machine learning techniques. Amiya Kumar Sahu utilized CNN and LSTM models with SGD optimization on NSL-KDD and UNSW-NB15 datasets, achieving an accuracy of 96%. Naeem Firdous Syed employed Machine Learning and FFNN with SGD optimization across Four-class and Seven-class datasets, reaching an accuracy of 84%.

Imtiaz Ullah applied CNN1D, CNN2D, and CNN3D on multiclass binary datasets (BoTIoT, IoT-NI, MQTT, IoT23) achieving high accuracies of 99.97%, 99.95%, and 99.94%, respectively. Dinesh Chowdary Attota utilized federated learning-based intrusion detection (MV-FLID) with Adam and Grey Wolves Optimization, obtaining an accuracy of 98% on multiclass binary Lightweight MQTT protocol datasets. Sydney Mambwe Kasongo implemented RF, LR, NB, DT, and ET techniques with GWO optimization, achieving accuracies of 87.61% and 77.64% on binary multiclass UNSW-NB15 datasets.
Poulmanogo Illy applied SDN and various models on NSL-KDD dataset, achieving accuracies ranging from 84.1% to 87.8%. Finally, Andr´e L. Cristiani introduced Fuzzy Intrusion Detection System (FROST) for binary and multiclass UNSW-NB15 datasets, without specifying accuracy or optimization details. These summaries highlight diverse approaches and their respective accuracies in intrusion detection and cybersecurity using machine learning techniques across different datasets.

Mustafa Al Lail, Alejandro Garcia and Saul Olivo [7] in their paper "Machine Learning for Network Intrusion Detection—A Comparative Study" propose a method using machine learning (ML) to develop a NIDS system capable of detecting modern attack types with a very high detection rate. To this end, they implement and evaluate several ML algorithms and compare their effectiveness using a state-of-the-art dataset containing modern attack types. The results show that the random forest model outperforms other models, with a detection rate of modern network attacks of 97%.

Mengmeng Ge, Naeem Syed, Zubair Baig, Gideon Teo and Antonio Robles-Kelly [8] in their paper "Deep Learning-based Intrusion Detection for IOT Network" propose a novel intrusion detection scheme for IoT network that classifies traffic flow through deep learning concepts. They made the use of Feedforward Neural Network for binary and multiclass classification. The framework they used mainly includes four phases: feature extraction, feature preprocessing, training and then classifying. This paper uses five categories of attacks: DDoS, DoS, Reconnaissance, Information theft and normal traffic. For binary classification accuracy being above 0.999, high precision and recall values (all above 0.99) and a high F1 score above 0.999. Similarly for multiclass classification, 0.99 accuracy for detecting normal traffic, for DDOS and DOS and

for Reconnaissance 0.98 and for Information theft attack 0.89 accuracy.

Vinayakumar, Mamoun Alazab, Soman KP, Prabaharan Poornachandran, Ameer Al-Nemrat and Sitalashmi Venkatraman [9] in their paper "Deep Learning Approach for Intelligent Intrusion Detection System" propose deep neural network (DNN), a type of deep learning model is explored to develop a flexible and effective IDS to detect and classify unforeseen and unpredictable cyber-attacks. They have proposed a highly scalable and hybrid DNNs framework called Scale-Hybrid-IDS-AlertNet (SHIA). For computing architecture, the Apache Spark cluster computing framework is set up over Apache Hadoop Yet Another Resource Negotiator (YARN).In this paper for feature representation Bag-of-Words (BoW), N-grams and Keras Embedding are used. Datasets used are KDDCup 99, NSL-KDD, UNSW-NB15, Kyoto, WSN-DS, CICIDS2017.

Table : RESULTS ARE OBTAINED FROM FOLLOWING ALGORITHM

Author	Model	Classifiers	Datasets	Optimizers	Activation Functions	Accuracy
[11]Amiya Kumar Sahu	CNN	LSTM	NSL-KDD and UNSW-NB15	SGD	LReU and Softmax	96 %
[12] Naeem Firdous Syed	Machine Learning, FFNN	AODE, Decision Trees,Multi-Layer Perceptron	Four-class Seven-class datasets	SGD	Relu, logistic-sigmoid and tanh	84%
[13] Imtiaz Ullah	CNN1D CNN2D CNN3D	Multiclass Binary	BoTIoT, IoT-NI, MQTT, IoT23	Adam	Softmax	99.97% 99.95% 99.94%
[14]Dinesh Chowdary Attota	Federated learning-based intrusion detection- MV-FLID	Multiclass Binary	Lightweight MQTT protocol	Adam, Grey Wolves Optimization	-	98%
[15] Sydney Mambwe Kasongo	RF, Linear Regression (LR), Naïve Bayes (NB), Decision Tree (DT), Extra-Trees (ET),	NSL-KDD	-	-	-	87.61% 77.64%

[16] Poulmanogo Illy	Decision Tree,K-Nearest Neighbor, Random Forest, Bagging, AdaBoost, and Voting	SDN	NSL-KDD	-	-	84.1%, 85%, 86%, 87.6%, 87.8%, 86.6%
[17] Andr´e L. Cristiani	Fuzzy Intrusion Detection System for IoT Networks (FROST)	Binary and Multiclass	UNSW-NB15	-	-	-

III. METHODOLOGY

The methodology for proposed DDoS Attack Detection is demonstrated in the fig[2]. Initially Data is collected, pre-processed and then passed to the model, created using ML/DL algorithms. This helps us in representing the attack at the end.[2]

Collection of the different types of data is done through multiple sources which are proposed further. This collected data is then processed to normalized it. The normalized data is then fed to algorithm for feature selection to reduces the dimensions of the processed data. The reduced pre-processed data is then passed on to the model(based on deep learning algorithms). Model then using its layer with activation function, hyper-parameters and optimizers predict the DDoS attack.[12]

A. Data Collection, Data Processing and Feature Selection:

This stage of DDoS detection starts with collection of the data to train and test the model which will further classify the attack as normal or abnormal. For this we have collected various types of datasets. This Datasets will decide the performance of our model, so choosing the best is only an option as it will result in higher accuracy and classification of attack.[2]

Here are some datasets which are most suitable for above mention title:

1. BoT-IoT:-

BoT-IoT is a collection of the network traffic which mimic normal and malicious activity in an environment. This dataset was created by UNSW Canberra, their main goal was to create a dataset which will provide realistic and diverse dataset for intrusion detection. It contains various types of attack such as DoS, OS, DDoS and etc. It also contains normal

2. MQTT-IoT:-

MQTT-IoT-IDS2020 is a dataset which simulates MQTT network. It is a common protocol used for IoT Devices. The dataset contain normal and malicious traffic both within it, such as brute-force attack, flood, slowite and etc. The dataset is used to train and evaluate the model for IoT intrusion detection system.[12]-[17]

3. APA-DDoS:-

The APA-DDoS dataset is a collection of network traffic data that contains both normal and malicious packets. The dataset was created to study the detection and mitigation of ACK and PUSH-ACK DDoS attacks data packets. The dataset is intended to be used for developing and evaluating machine learning models for detecting DDoS attacks. The dataset has 151,201 entries and 22 attributes extracted from pcap files.

4. CICDDoS-2019:-

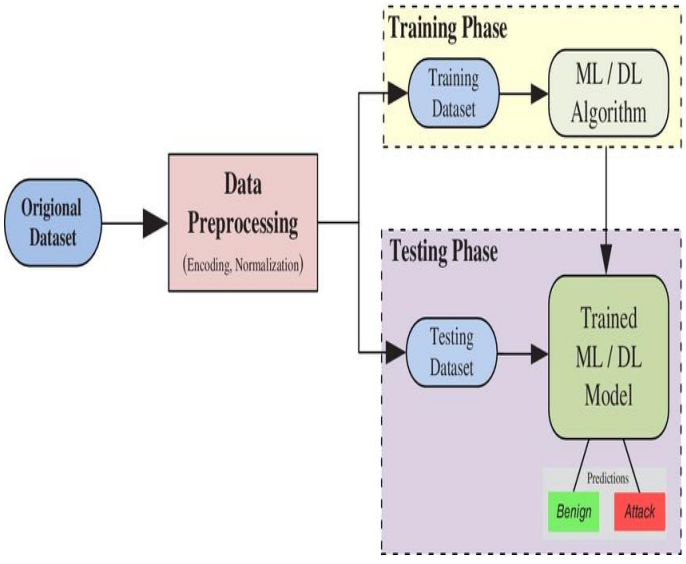
CICDDoS2019 is a dataset that contains network traffic data of benign and various types of DDoS attacks. It was created by the Canadian Institute for Cybersecurity to evaluate and compare different DDoS detection methods. The dataset has 86 features for each network flow and covers 13 types of DDoS attacks.[1] It contains various types of DDoS attacks, such as LDAP, MSSQL, NetBIOS, PortMap, UDP, SYN, and UDP-Lag.

The next step is to process the data. Data preprocessing is a procedure of converting a raw data and transforming it, which will be suitable for ML algorithms based model.[12] This technique involve steps like data cleaning, data imputation, data integration, data normalization

and etc. Data preprocessing is necessary as it enhance the quality and accuracy of data. Along with quality and accuracy it also reduces the complexity and dimensionality of the collected data. It also helps in preventing the machine learning model from overfitting and underfitting.

Further we must pass on the processed data for feature selection. Feature selection is the process of choosing a subset of relevant features from a large set of input features for a machine learning or deep learning model. It improves the performance, accuracy, and interpretability of the model, as well as reduce the computational cost and complexity.[2]

DDoS attack detection is the task of identifying and classifying network traffic flows that are malicious and aim to disrupt the normal functioning of a server, system, or application. DDoS attack detection can be done using various machine learning or deep learning algorithms, such as support vector machines, K-nearest neighbours, decision trees, multiple layer perceptron, and convolutional neural networks. These algorithms require a set of features that can capture the characteristics and patterns of normal and anomalous traffic flows. Feature selection helps to select the most informative and discriminative features for DDoS attack detection, and eliminate the redundant and irrelevant features that may degrade the performance of the model.



Some of important features for DDoS Attack Detection are as follows:-

Port-Map, LDAP, MSSQL, UDP, SYN, NTP, DNS, SNMP and etc.

B. Model Selection and Model Training:

Model selection for DDoS attack detection is the process of choosing the best algorithm and features to identify and prevent distributed denial-of-service (DDoS) attacks, which are malicious attempts to disrupt the normal functioning of a network or service by overwhelming it with traffic. Model selection aims to find the optimal balance between accuracy, generalization, complexity, and efficiency of the detection model.[2]

There are different methods and techniques for model selection, such as feature selection algorithms, model selection algorithms, and model optimization algorithms. Feature selection algorithms reduce the dimensionality of the data and select the most relevant and informative features for the detection task. Model selection algorithms compare the performance of different algorithms on the selected features and choose the best one. Model optimization algorithms fine-tune the parameters of the chosen algorithm to improve its performance.

Following are some algorithms used in DDoS attack detection model:-

1. Decision Tree:

A decision tree model for DDoS detection is a machine learning technique that uses a tree-like structure to classify network traffic as normal or malicious. The model is trained on a set of features that are extracted from the network packets, such as source IP, destination IP, protocol, packet size, etc. The model then splits the data into smaller subsets based on the values of these features, until it reaches a leaf node that represents a class label. The model can then use the learned tree to predict the class of new instances by following the path from the root node to the leaf node that matches the feature values of the instance.[17]

2. Random Forest:

A random forest model for DDoS detection is a machine learning technique that uses multiple decision trees to classify network traffic as normal or attack. Each decision tree is trained on a subset of the data and features, and then the majority vote of the trees is used to make the final prediction. This method can improve the accuracy and robustness of DDoS detection.[2]

3. KNN:

A KNN model for DDoS detection is a machine learning technique that uses the k-nearest neighbors algorithm to classify network traffic as normal or malicious. The model

compares the features of a new traffic sample with the features of k previously labeled samples, and assigns the label of the majority of the neighbors to the new sample. The model can be trained on different datasets and parameters to improve its accuracy and efficiency.

4. CNN:

A CNN model for DDoS detection is a deep learning approach that uses convolutional neural networks (CNNs) to extract features from network traffic data and classify them as normal or malicious. CNNs are composed of multiple layers of neurons that apply filters and pooling operations to the input data, resulting in a high-level representation of the data. A CNN model can learn to detect different types of DDoS attacks, by training on labelled datasets.[2] A CNN model improves the detection accuracy and reduce the false positive rate.

Then Model training is performed. Model training for DDoS attack detection is a process of developing machine learning or deep learning models that can identify and prevent distributed denial of service (DDoS) attacks. DDoS attacks are malicious attempts to disrupt the normal functioning of a network or a server by overwhelming it with fake traffic from multiple sources. These attacks can cause serious damage to the availability and performance of online services and applications.

To train a model for DDoS attack detection, one needs to collect and preprocess network traffic data, extract relevant features, select an appropriate algorithm, and evaluate the model's accuracy and robustness. Some of the common algorithms used for this task are recurrent neural networks, convolutional neural networks, autoencoders, and hybrid models. These algorithms can learn from the patterns and anomalies in the network traffic and classify them as normal or malicious. The trained model can then be deployed in a cloud computing environment or a cyber-physical system to monitor and protect the network from DDoS attacks.

C. Model Evaluation:

Model evaluation is a process of measuring how well a machine learning model can perform on new data. It involves calculating various metrics, such as accuracy, precision, recall, F1 score to assess the quality and suitability of the model for a given problem. Model evaluation helps to compare different models and select the best one for deployment.[17]

Some evaluation criteria are as follows:-

1. Accuracy:

It measures the correctness (true positives and true negatives) of predictions from every prediction made by model.

Accuracy = (TP+TN)/(TP+TN+FP+FN)

2. Precision:

It is a ratio of truly predicted DDoS attack to overall predicted attack, i.e it finds out true positive from overall positives.

Precision = (TP)/(TP+FP)

3. Recall:

Recall measures the capability of the model to rightly identify all positive cases in the dataset. It is a ratio of true positive to the number positive class values in data.

Recall = (TP)/(TP+FN)

4. F1 Score:

The F1-score is the harmonic mean of precision and recall, furnishing a balance between the two criteria.

F1 Score = 2*(Precision*Recall)/(Precision+Recall)

IV EXPECTED RESULT

The Internet of Things (IoT) has various kinds of security issues and upcoming and solving these issues is the most important aspect of IoT Security. CNN Model like RestNet is used for detecting and preventing DDOS attack in IoT network, such mole is called the "Twofold" model and has given up to 99% accuracy. Hybrid Neural Network with Stack Auto-Encoder has given up to 99% accuracy using ISCX-IDS-2012 and IDS-2017 datasets having binary as well as multiclass classification. Datasets are also equally important as they also contribute to setting the accuracy of the model using Ensemble Learning UNSW-NB15 and NIMS datasets have given 98.97% and 98.36% accuracy respectively. Using this information we expect that our model will detect the DDOS attack with accuracy between 90% to 95%.

V. CONCLUSION

In conclusion, the application of Machine Learning (ML) for the detection of Distributed Denial of Service (DDoS) attacks in IoT networks stands as a pivotal and proactive strategy in safeguarding the integrity of interconnected devices. The ever-evolving landscape of cyber threats, particularly DDoS attacks, necessitates sophisticated and adaptive defence mechanisms. ML algorithms, adept at analyzing complex patterns within network traffic data, offer a robust solution for early detection of anomalous activities indicative of DDoS incidents. By extracting and interpreting features from the data, these models enable swift identification and response to potential threats, contributing significantly to the resilience of IoT networks. The versatility of ML contributes to the scalability and effectiveness of DDoS detection in IoT environments, addressing the unique challenges posed by the interconnected nature of devices. This integration not only fortifies the security posture of individual devices but also bolsters the overall robustness of interconnected systems. However, it is important to acknowledge the challenges inherent in deploying ML for DDoS detection in IoT networks, including the need for continuous model training to adapt to emerging threats and the necessity of optimizing computational efficiency to accommodate resource constraints on IoT devices. In summary, the synergy of ML with DDoS detection in IoT networks offers a proactive and intelligent defence against the evolving threat landscape. As the IoT ecosystem continues to expand, the incorporation of ML-driven security measures becomes increasingly crucial for sustaining the functionality and security of interconnected devices.

REFERENCES

[1] Ruchi Vishwakarma, Ankit Kumar Jain " A survey of DDoS attacking techniques and defence mechanisms in the IoT network" Springer Science+Business Media, LLC, part of Springer Nature 2019

[2] Ismail1, Muhammad Ismail Mohmand1, Hameed Hussain, Ayaz Ali Khan, Ubaid Ullah1, Muhammad Zakarya, Aftab Ahmed, Mushtaq Raza, Izaz Ur Rahman, Muhammad Haleem "A Machine Learning based Classification and Prediction Technique for DDoS Attacks" IEEE Access, Volume 4, 2016.

[3] Monika Roopa, Prof. Gui Yun Tian and Prof. Jonathon Chambers "An Intrusion Detection System Against DDoS Attacks in loT Networks" 978- 1-7281-3783-4/20/£31.00 ©2020 IEEE.

[4] Vimal Gaur and Rajneesh Kumar "Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices" Arabian Journal for Science and Engineering https://doi.org/10.1007/s13369-021-05947-3.

[5] Amal A. Alahmadi, Malak Aljabri, Fahd Alhaidari, Danyah J. Alharthi, Ghadi E. Rayani, Leena A. Marghalani, Ohoud B. Alotaibi and Shurooq A. Bajandouh " DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions" Electronics 2023, 12, 3103. https://doi.org/10.3390/electronics12143103.

[6] Pravinder Singh Saini, Sunny Behal and Sajal Bhatia [5] "DDoS Attacks Detection using Machine Learning Algorithms" 978-93-80544-38-0 /20/$31.00c 2020 IEEE.

[7] Umar Islam, Ali Muhammad, Rafiq Mansoor, Md Shamim Hossain, Ijaz Ahmad, Elsayed Tag Eldin, Javed Ali Khan, Ateeq Ur Rehman and Muhammad Shafiq "Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring Systems of Banking Sector Using Machine Learning Models", Sustainability 2022, 14, 8374. https://doi.org/10.3390/su14148374.

[8] Mustafa Al Lail, Alejandro Garcia and Saul Olivo [7] in their paper "Machine Learning for Network Intrusion Detection—A Comparative Study" Future Internet 2023, 15, 243. https://doi.org/10.3390/fi15070243.

[9] Mengmeng Ge, Xiping Fu, Naeem Syed, Zubair Baig, Gideon Teo, Antonio Robles-Kelly "Deep Learning-based Intrusion Detection for IoT Networks" 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC) 2473-3105/19/$31.00 ©2019 IEEE DOI 10.1109/PRDC47002.2019.00056

[10] Vinayakumar R, Mamoun Alazab, (Senior Member, Ieee), Soman Kp, Prabaharan Poornachandran3, Ameer Al-nemrat, And Sitalakshmi Venkatraman "Deep Learning Approach for Intelligent Intrusion Detection System" IEEE Access, 2169-3536 © 2018.

[11] Amiya Kumar Sahu, Suraj Sharma, M. Tanveer, Rohit Raja " Internet of Things attack detection using hybrid Deep Learning Model" 0140-3664/© 2021 Elsevier https://doi.org/10.1016/j.comcom.2021.05.024

[12] Naeem Firdous Syed, Zubair Baig, Ahmed Ibrahim & Craig Valli "Denial of service attack detection through machine learning for the IoT" JOURNAL OF INFORMATION AND TELECOMMUNICATION 2020,

VOL.4,NO.4,482–503
https://doi.org/10.1080/24751839.2020.1767484

[13] Imtiaz Ullah, Qusay H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly detection in IoT Networks" IEEE Access, vol. 9, pp. 103906-103926, Jul 2021

[14] Dinesh Chowdary Attota , Viraaji Mothukuri , Reza M. Parizi , And Seyedamin Pouriyeh " An Ensemble Multi-View Federated Learning Intrusion Detection for IoT" IEEE Access 117734

[15] Sydney Mambwe Kasongo "An Advanced Intrusion Detection System for IIoT Based on GA and Tree Based Algorithms" IEEE Access VOLUME 9, 2021 , 113199

[16] Poulmanogo Illy , Georges Kaddoum , Kuljeet Kaur , and Sahil Garg " ML-Based IDPS Enhancement With Complementary Features for Home IoT Networks" IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 19, NO. 2, JUNE 2022

[17] Andre L. Cristiani, Douglas D. Lieira, Rodolfo I. Meneguette, Heloisa A. Camargo "A Fuzzy Intrusion Detection System for Identifying Cyber-Attacks on IoT Networks" 978-1-7281-8903-1/20 ©2020 IEEE