iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59114

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Detection of DDoS Attack using Machine Learning Algorithms

Brahma Naidu Nalluri[1], Aditya Mandapaka[2], Ruzaina Suaad Mohammed[3], Hemanth Reddy Nagireddy[4], Induja Poonati[5]
[1]*Assistent Professor, Department of CSE, Vasireddy Venkatadri Institute of Technology (Autonomous), Guntur, AP*
[2, 3, 4, 5]*UG Students, Department of CSE, Vasireddy Venkatadri Institute of Technology (Autonomous), Guntur, AP*

Abstract: ***The utilization of the internet has greatly increased in recent decades, leading to a vulnerability in networking and cybersecurity. One of the most common resulting attacks is Distributed Denial of Service (DDoS), where overwhelming amounts of data are sent to legitimate websites or servers, causing delays or denying access to legitimate users. Single source attacks are known as denial of service (DoS), while attacks from multiple sources, such as a botnet, are considered distributed denial of service (DDoS). In our project, we employed three machine learning algorithms to identify DDoS attacks, and determined the most successful algorithm based on the accuracy metric. We trained and tested our data using the standardized dataset, dataset_sdn, and obtained experimental results. Out of all the algorithms used, the XGBoost algorithm proved to be the most effective with an accuracy of 99.9%. During preprocessing, any missing data was replaced with the column's mean value.***
Keywords: DDoS-Distributed Denial of Service, XGBoost , Multilayer Perceptron , Decision Tree.

I. INTRODUCTION

DDoS attacks function as digital traffic jams that can disrupt and prevent access to websites and online services. In simple terms, they involve a high volume of traffic originating from various sources, overwhelming a website's capacity and resulting in server slowdown or temporary unavailability. Although traditional methods, such as firewalls and intrusion detection systems, can identify these attacks, their effectiveness is limited. However, the use of machine learning algorithms is proving to be a game-changer in detecting and defending against DDoS attacks.

By learning and recognizing patterns and anomalies in network traffic, these algorithms can distinguish between legitimate user activity and malicious attacks. Their ability to rapidly analyze vast amounts of data in real-time is a key factor in their success. .The use of machine learning into cybersecurity methods presents a proactive way to protecting digital infrastructure, guaranteeing continuous access to essential online services, while DDoS attacks continue to grow in complexity and size.

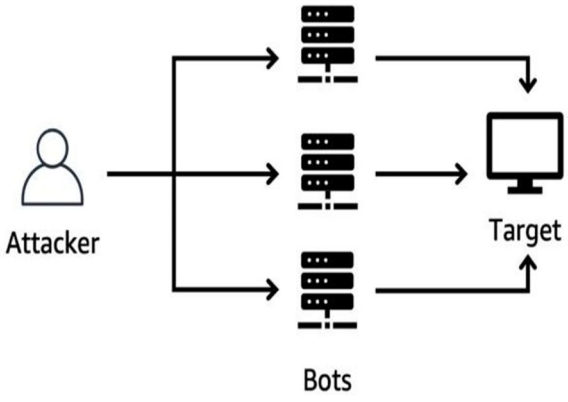


Fig. 1: Showing DDoS attack

A. Attacker

In Fig. 1, the attacker attacks the target with the help of bots. This can be carried out for various ways including financial gain, ideological motives, revenge , or simply to cause disruption.

The attack can be done in various ways such as flooding the target with traffic, exploiting vulnerabilities, or using amplification techniques to multiply the impact of the attack

B. Botnets

The botnet is a collection of networks which are controlled by a single entity, which is namely an attacker. The botnets are typically created by injecting malware into the devices which gives an access to the attacker remotely.

C. Target

The attacker attacks the target server. In this the target is overwhelmed by the resources, such as bandwidth, processing power, or memory, or any other internet-connected resource.

D. Machine Learning Algorithms used in DDoS Detection

The machine learning algorithms used in the detection of DDoS attacks are as follows:

1) Multi-Layer Perceptron
2) Extreme Gradient Boosting
3) Decision Tree

E. Multi-Layer Perceptron (MLP) in DDoS Detection

Utilizing a multi-layer perceptron for DDoS attack detection involves training a neural network to recognize patterns. The MLP, with the ability to model complex relationships, can analyze network traffic features and remove abnormal patterns associated with DDoS attacks. This approach enhances the adaptability and accuracy of DDoS detection systems and works against disruptive network attacks.

F. Extreme Gradient Boosting (XGBoost) in DDoS Detection

In order to detect DDoS assaults, Extreme Gradient Boosting trains a group of decision trees to recognize complex patterns in network traffic that are connected to illicit activities. It is excellent at managing nonlinear relationships and high-dimensional data, which helps it effectively handle anomalous patterns. Using boosting in conjunction with xgboost improves DDoS efficiency and accuracy and functions as a tool to detect and neutralize attacks in real-time applications.

G. Decision Trees in DDoS Detection

Using decision trees to identify DDoS assaults entails building a model based on trees that determines whether the attacks are malicious or benign.These trees are excellent at simulating intricate decision-making procedures,which aids in the timely identification of risks related to DDoS assaults. These assist them with useful tools for real-time applications by carrying out the work recursively.

II. LITERATURE REVIEW

Machine learning is a powerful tool used in various aspects of our lives, from analyzing images and predicting future trends to improving recommendations and enhancing healthcare, banking, defense, education, and robotics. Researchers across different fields rely on machine learning algorithms to make tasks smarter and more efficient.In this research, we employed three different machine learning techniques - eXtreme Gradient Boosting (XGB), multi-layer perceptron (MLP), and Decision Tree (DT) - to better detect DDoS attacks. We reviewed the latest studies on DDoS attack detection and compiled a summary for reference.

In [1], the authors introduced the SGB methodology for DDoS attack detection, utilizing a hybrid dataset from three open datasets. Their findings indicated that the SGB algorithm exhibited the highest accuracy among various algorithms. Meanwhile, in [2], the authors presented an MLP classifier model tailored for internal data to discern DDoS attacks at the application level. Their research involved identifying attack groupings to distinguish attackers, resulting in a highly accurate MLP classification model with a 98.99% detection rate and a low false positive rate of 2.1%.

The authors of [3], uses two datasets CICIDS2007 and UNSW-NB15. In this methodology Random Forest and MLP as a single model RF-MLP which analyses and evaluate the network traffic and establishes a security prediction model that accurately identifies DoS attack.

The authors of research paper [4], uses 10-fold cross validation and found the accuracy drastically increases from 94.88% to 99.2% in just 0.48 minutes by LGBM. A limitation was found that in their work all instances present in the dataset cannot be processed.In [5], the models logistic regression, Gradient Boosting and Naive Bayes gives best evaluation metric values, used cross-Fold validation and log loss methods to identify the better models.

In the paper [6], they employed several feature selection methods in order to select the most significant features they chose three sets of features from the dataset and employed four ml models.The authors of [7], perform correlation analysis and feature importance exploration using a decision tree where employed in feature engineering.
In [8], the study introduces and evaluated the OptMLP-CNN model for detecting DDoS attacks in SDN environments. The model combines the innovative SHAP-feature-selection method to identify the most crucial features and a hybrid DL
technique based on MLP and CNN architecture.The authors of [9], uses a network simulator (NS2) was used in this work, because NS2 can be used with high confidence due to its capability of producing valid results that reflects real environment. Three machine learning algorithms (MLP, Random Forest and Naive Bayes) were applied and MLP classifier achieved the highest accuracy rate.
The authors of [10], implemented the integrated approach for monitoring of DDoS attacks and defense strength is improved by using Lanchester Law and malicious packets are filtered.The authors of [11] conducted a comprehensive analysis on two distinct forms of DDoS attacks and considered eight machine learning algorithms for comparisons.The main motive of their experiment is to ascertain the capacity of each algorithm to distinguish between different types of DoS attacks in the dataset.
The researchers of [12],used 380,089 pieces of data for their study. They ran the model 80 times to see how accurate it was.
At the 80th try, the model was found to be 99.69% accurate.Out of all the Machine Learning techniques used, the method of feature reduction, specifically Information Gain and Correlation with J48 classifier, resulted in the highest accuracy, reaching 99.9%[13].
In the study[14], a method was developed using a wrapper feature selection (FS) model. It utilized the binary Particle Swarm Optimization (PSO) algorithm with the Decision Tree (DT) classifier to detect DDoS attacks.The experimental findings showed excellent performance, successfully identifying 19 significant features out of the 76 available in the dataset.

TABLE 1: COMPARISION TABLE FOR MODEL PAPERS

Base paper	Model and accuracies	Our models and accuracies
[2]	KNN (99.57), DT (96.65), RF (97.2), Ada Boost (99.55), NB(99.57)	MLP(98.65) XGBoost(99.98) DT(96.63)
[4]	XGBoost(99.1) LGBM(99.2)	MLP(98.65) XGBoost(99.98) DT(96.63)

We also looked at other types of machine learning models from numbers [19-34]. These models gave us ideas and support in creating our own model to solve the problem we identified.

III.METHODOLOGIES

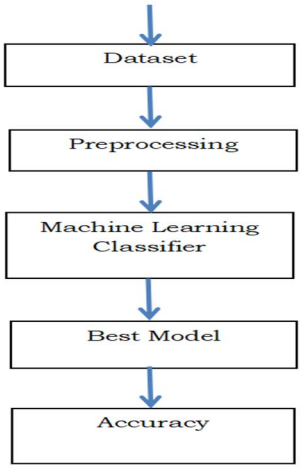


Fig. 2: Proposed Methodology

A. Dataset

Our dataset comprises a total of 23 attributes, encompassing the class label. These attributes can be divided into two groups: categorical and numerical. The categorical attributes primarily consist of destination address, source address, and utilized protocols and the remaining features are numerical type which are analyzed based on various visualization methods as shown in below figures[3-12].

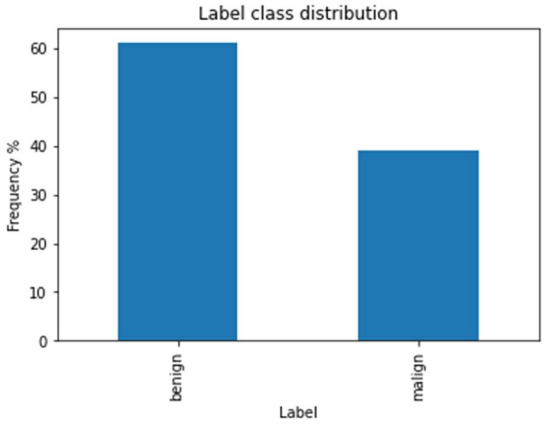


Fig. 3: Distribution of Label Class

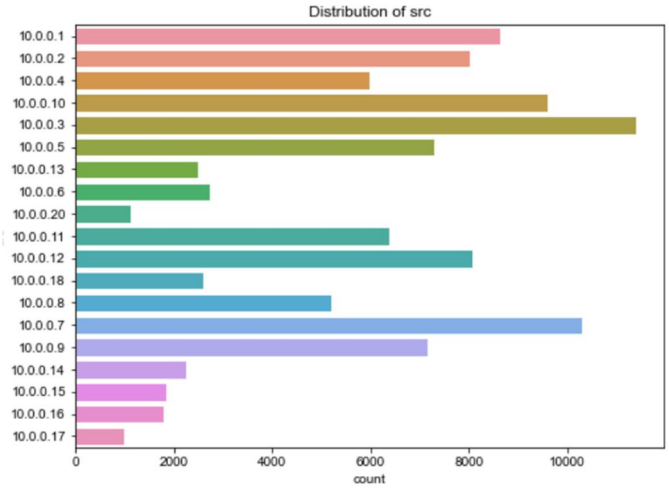


Fig. 4: Distribution of Source

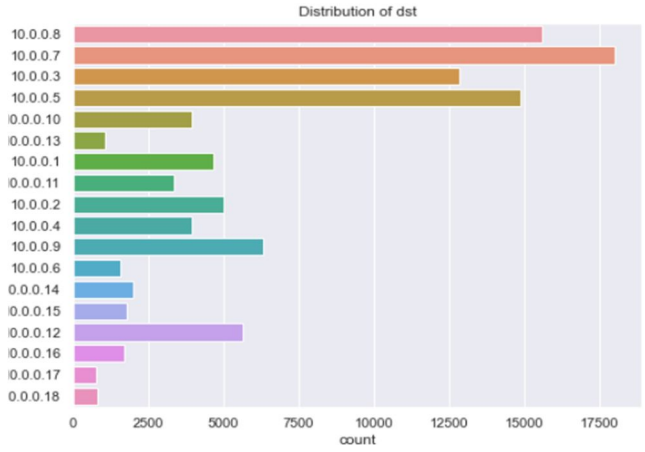


Fig. 5: Distribution of Destination

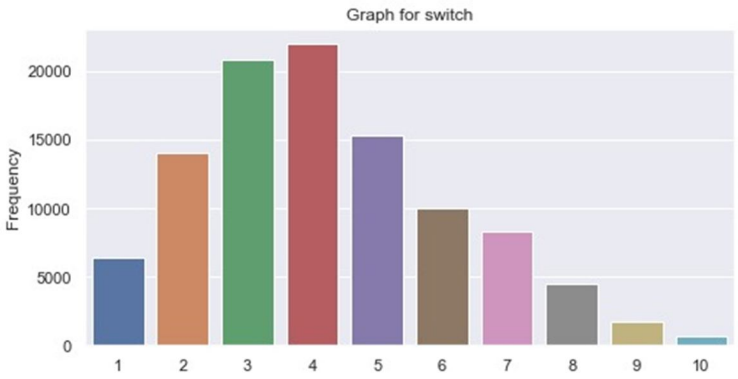


Fig. 6: Distribution of Switch

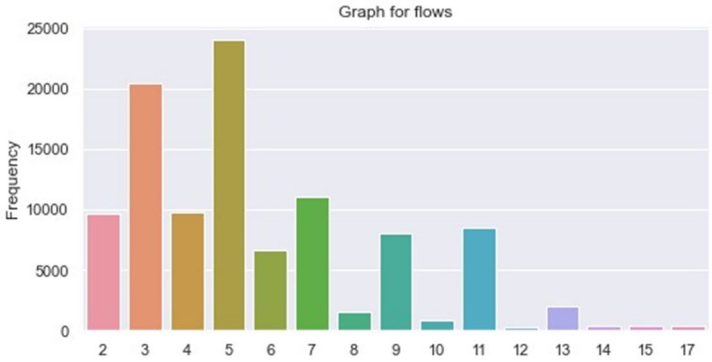


Fig. 7: Distribution of Flows

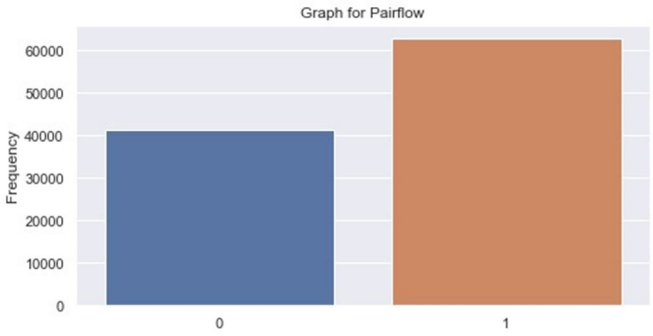


Fig. 8: Distribution of Pairflow

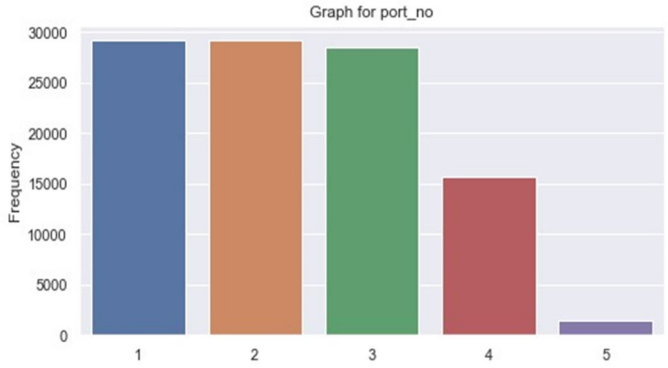


Fig. 9: Distribution of port_no

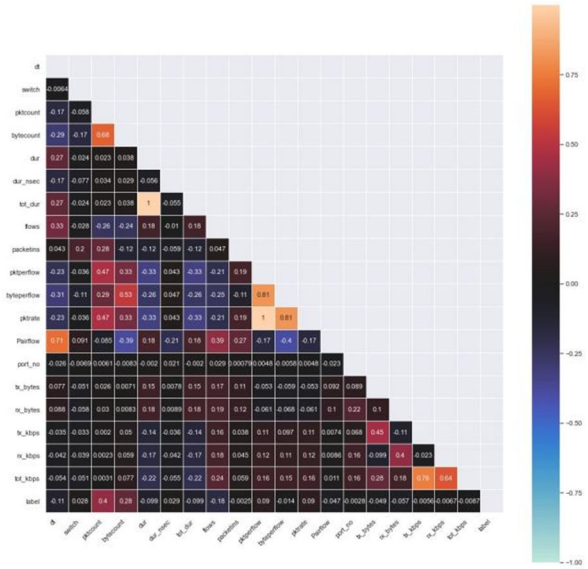


Fig. 10: Showing Heat map for correlation of features

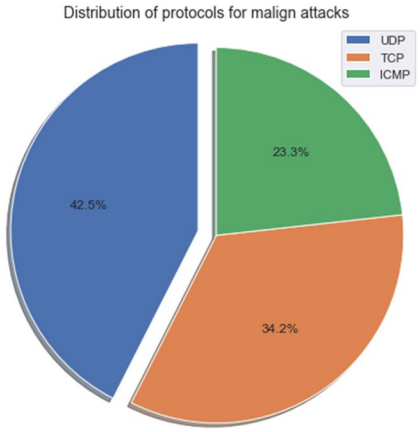


Fig. 11: Distribution of ddos attacks

- ICMP (Internet Control Message Protocol) is responsible for handling error reporting and diagnostic functions at the network layer in computer networks.
- TCP (Transmission Control Protocol) is a reliable, connection-oriented transport layer protocol that ensures the ordered and error-checked delivery of data between applications over a network.
- UDP (User Datagram Protocol) is a connectionless transport layer protocol that provides a faster, but less reliable, way of exchanging data between applications over a network.

The numerical attributes are further classified into two categories: continuous and discrete features. The continuous features include packet count, duration, and packet per flow, among others. On the other hand, the discrete features consist of switches, flows, and port numbers, among others. To determine the importance of features, we utilize the ExtraTreeClassifier. Based on the results of this classifier, we select the most significant features

B. ExtraTreeClassifier

The ExtraTreeClassifier is an ensemble learning method in machine learning that builds multiple decision trees and combines their predictions to enhance accuracy and robustness, known for its increased randomness during tree construction compared to traditional methods like Random Forest.

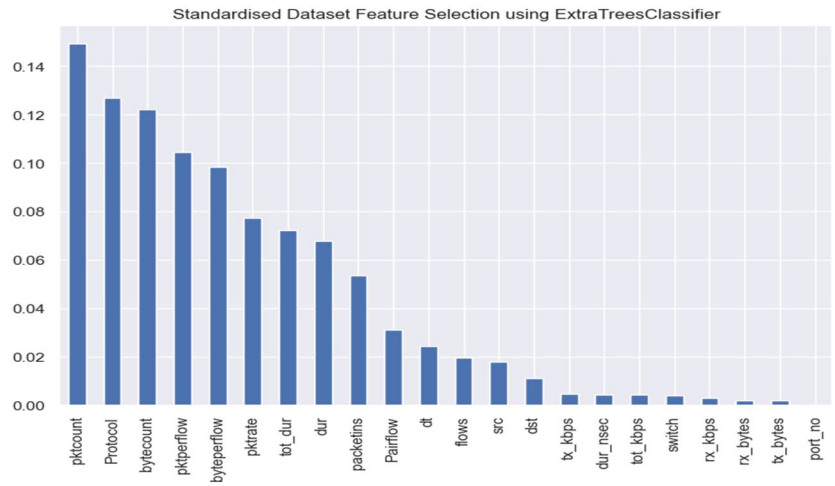


Fig. 12:Feature Selection

C. Preprocessing

In the Preprocessing stage, the null values in the dataset dataset_sdn are handled by the mean measure. The two columns rx_kbps and tot_kbps contain null values for each value of 506.The mean for the two columns is calculated, and we fill in the values that contain null values.

D. Machine Learning Classifiers

For the implementation of three models we used three classifiers namely

1) *MLPClassifier():* In this project we utilized MLPClassifier method from the scikit-learn library to implement a Multi-Layer Perceptron(MLP) algorithm for classification tasks. The purpose of this method is to create, train, and utilize a neural network model tailored for classification, with customizable parameters including the number of hidden layers, neurons, activation functions, and optimization algorithms. The MLPClassifier() model is capable of effectively addressing the classification requirements specific to the dataset.
2) *XGBClassifier:* The XGBClassifier helps with the implementation of classification tasks. It is a part of the XGBoost library, which is widely used in the machine learning domain for efficiency and effectiveness. This method works based on a technique in which the strength of decision trees is combined with gradient boosting. This model creates a robust model for classification, benefiting from its ability to handle complex relationships in data.
3) *DecisionTreeClassifier():* The DecisionTreeClassifier plays a very important role in the realm of DDoS attack detection within machine learning frameworks like Scikit-learn. The purpose of constructing decision tree-based models is to identify abnormal traffic patterns and have the leverage to remove them. This has the special ability to autonomously analyze network traffic features. With the help of this classifier, both professionals and researchers can enhance cybersecurity measures for real-time data detection.

IV. IMPLEMENTATION

There are several steps involved in the implementation of DDoS attacks with the help of machine learning algorithms. The trained machine learning model is saved from the Jupiter notebook with the help of the module pickle.

A. Pickle

Pickle is an effective tool that allows you to serialize and deserialize Python objects. A Python object is serialized when it is transformed into a byte stream, and it is deserialized when it is assembled back together from a byte stream. There are two primary functions offered by the pickle module:

- pickle.dump()
- pickle.load()

To serialize an item to a file-like object, use pickle.dump(); to deserialize an object from a file-like object, use pickle.load().

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

B. Generation of Normal Traffic

We generate random data based on the specified range values of the features. For integer data, we use the randInt() method, which helps in creating random whole numbers within a given range. Meanwhile, for categorical features (like types or categories), we use the choice() method. This method allows us to randomly select from a list of options, mimicking the variability seen in real-world scenarios.

C. Generation of Attack Traffic

The attack traffic is generated based on the analysis of feature values in the selected dataset. From the newly generated dataset, the tuples, which are attack types, are stored in a separate file for attack data. The dataset is used for attack traffic testing.

D. The DDoS Attack Detection done in Three Stages

The implementation procedure was split up into three phases. First, we used particular, chosen features to create normal traffic. In the second step, we entered the created dataset into a machine learning model that we had already stored. These two steps were repeated continually, and the outcomes were presented on the console. The final step involved creating attack data, combining it with regular traffic, and feeding it into the model that had been preserved. The traffic was shown as attack traffic in the results.

V. RESULTS & DISCUSSION

We've set up some measurements to figure out how well these programs are doing. One basic measure is accuracy, which tells us if the programs are generally correct in their decisions. We also look at precision and recall, which help us see how accurate the programs are when they say something is an attack or not. We check false alarms (saying there's an attack when there isn't) and true detection rates (spotting actual attacks) to get a better picture. There's a combined measure called the F1 score that gives us an overall idea of how good the programs are at this task.

- True Positive(TP): It is the total counts having both predicted and actual values are DDoS attacks.
- True Negative(TN): It is the total counts having both predicted and actual values are BENIGN.
- False Positive(FP): It is the total counts having prediction is DDoS attacks while actual value is BENIGN.
- False Negative(FN): It is the total counts having prediction is BENIGN while actual value is DDoS attack.

A. Accuracy, Precision, Recall

The model's performance can be evaluated using the accuracy metric. This measure is determined by dividing the total number of correct predictions by the total number of instances.

$$accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)}$$

Similarly, precision is used to assess the accuracy of a model's positive predictions. This metric is derived by dividing the number of true positive predictions by the total number of positive predictions made by the model.

$$precison = \frac{(TP)}{(TP+FP)}$$

Lastly, recall is used to measure the effectiveness of a classification model in identifying all relevant instances from a dataset. It is calculated as the ratio of the number of true positive instances to the total number of relevant instances in the dataset.

$$recall = \frac{(TP)}{(TP+FN)}$$

B. F1-Score

F1-score gives the overall performance of the classification model.

$$f1\_score = \frac{2*(precision*recall)}{(precision+recall)}$$

C. Classification Report

The Classification_report() method is used to generate the evaluation matrices like Precision, Recall,and F1-score.The following diagrams shows the classification reports for three different models. The below Tables (TABLE-1,TABLE-2,TABLE-3) shows that the precision , recall and f1-score vales of the three models respectively.

TABLE-1: CLASSIFICATION RESULTS FOR MLP

	Precision	**Recall**	**F1-score**
Benign	**0.98**	**0.99**	**0.99**
Malign	**0.99**	**0.97**	**0.98**
Macro Avg	**0.99**	**0.98**	**0.98**
Weighted avg	**0.99**	**0.99**	**0.99**
Accuracy			**0.99**

TABLE-2: CLASSIFICATION RESULTS FOR XGB

	Precision	Recall	F1-score
Benign	1.00	1.00	1.00
Malign	1.00	1.00	1.00
Macro Avg	1.00	1.00	1.00
Weighted avg	1.00	1.00	1.00
Accuracy			1.00

TABLE-3: CLASSIFICATION RESULTS FOR DT

	Precision	Recall	F1-score
Benign	0.98	0.96	0.97
Malign	0.94	0.97	0.96
Macro Avg	0.96	0.97	0.96
Weighted avg	0.97	0.97	0.97
Accuracy			0.97

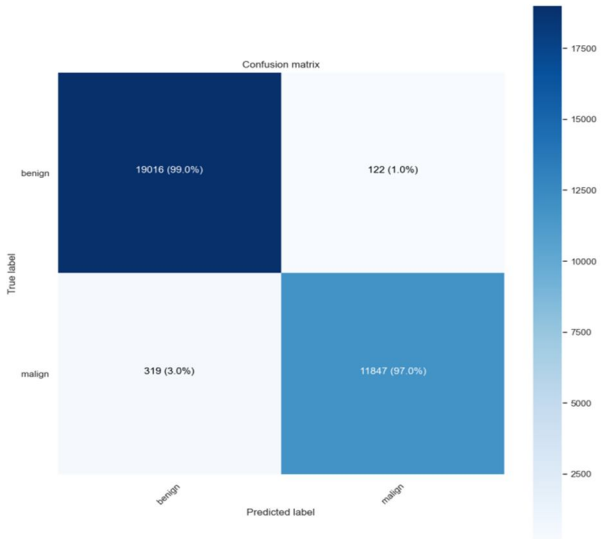


Fig. 13(a): Confusion matrix for MLP

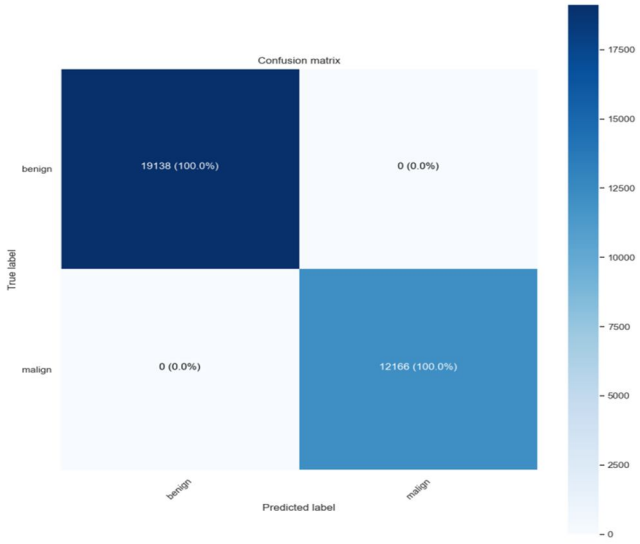


Fig. 13(b): Confusion matrix for XGB

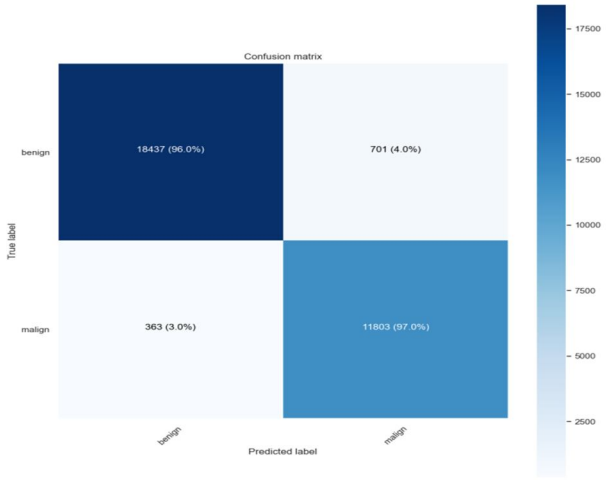


Fig. 13(c): Confusion matrix for DT

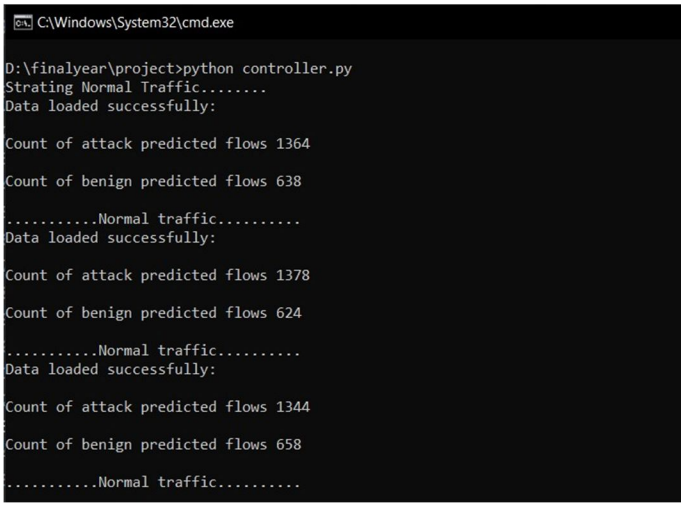


Fig. 14: The output when normal traffic runs

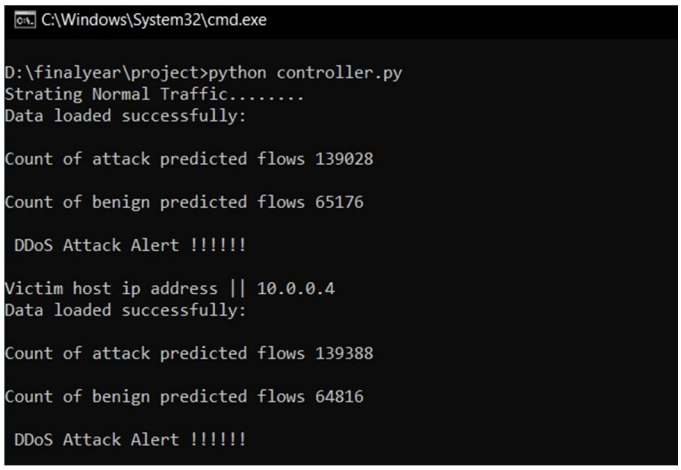


Fig. 15: The output when attack traffic runs

TABLE-4: ACCURACY COMPARISONS FOR DIFFERENT FEATURES

Features selected	MLP	XGB	DT
22-features	98.62	99.97	96.36
21-features	98.73	99.98	96.45
20-features	98.67	99.97	96.53
19-features	98.70	99.98	96.43
18-features	98.72	99.98	96.35
17-features	98.59	99.98	96.62
16-features	98.58	99.99	96.28
15-features	98.42	99.98	96.27
12-features	97.85	99.92	96.27
10-features	97.47	99.91	96.27

Figures 13(a), 13(b), and 13(c) display the confusion matrices for the chosen models.The console output of running the attack traffic module is displayed in Fig. 15, whereas the console output of running the normal traffic module is displayed in Fig. 14. The "controller.py" file, which creates the traffic flow and saves the flow values in a dataset, is where the entire execution process begins. The stored model is fed the dataset, and the total number of correctly and incorrectly recognized tuples is tallied. 70% of the assault type is the threshold figure that we have set. We determine the percentage of attack kinds based on the number of 1s and 0s. We console it as DDoS attack traffic if the percentage is more than the threshold value of 70%; if not, we console regular traffic.

From Table-4, We find that, with an average accuracy of 99.98%, the XGBoost classifier has the greatest accuracy for varying amounts of features. The MLP classifier yields an average accuracy of 98.67% for the other two classifiers, while the DT classifier yields an accuracy of 96.53%. We also infer that when the number of chosen characteristics diminishes, the accuracy of the MLP and DT classifier models rapidly declines.We conclude that with the following classifier parameter, the XGBClassifier() from our base article yields an accuracy of 98.10%:

XGBClassifier(max_depth=2,learning_rat=0.1,objective="binary:logistic",eval_matric="error")

Examine the following parameter values based on the above:

XGBClassifier(max_depth=3,learning_rat=0.2,objective="binary:logistic",eval_matric="error")

and by raising the max_depth to 3 and the learning rate to 0.2, we were able to get an accuracy of 99.98%.

VI.LIMITATIONS

One limitation is that we aren't generating real-time traffic for detecting DDoS attacks. Instead, we use custom Python code to create traffic by selecting specific features from an original dataset. To generate both normal and attack traffic, we've developed two separate methods and these methods use individually to generate both type of traffics.

VII.FUTURE WORK

In the future, because we don't have high-end systems, we will use a moderate dataset with over 100,000 rows. Our next step is to explore larger datasets and aim to build the best model for detection. Additionally, we plan to prevent DDoS attacks by developing real-time traffic monitoring software using mininet and controllers, where a mininet is a network used to create a virtual network and a controller is used to analyze the traffic requests in the network.

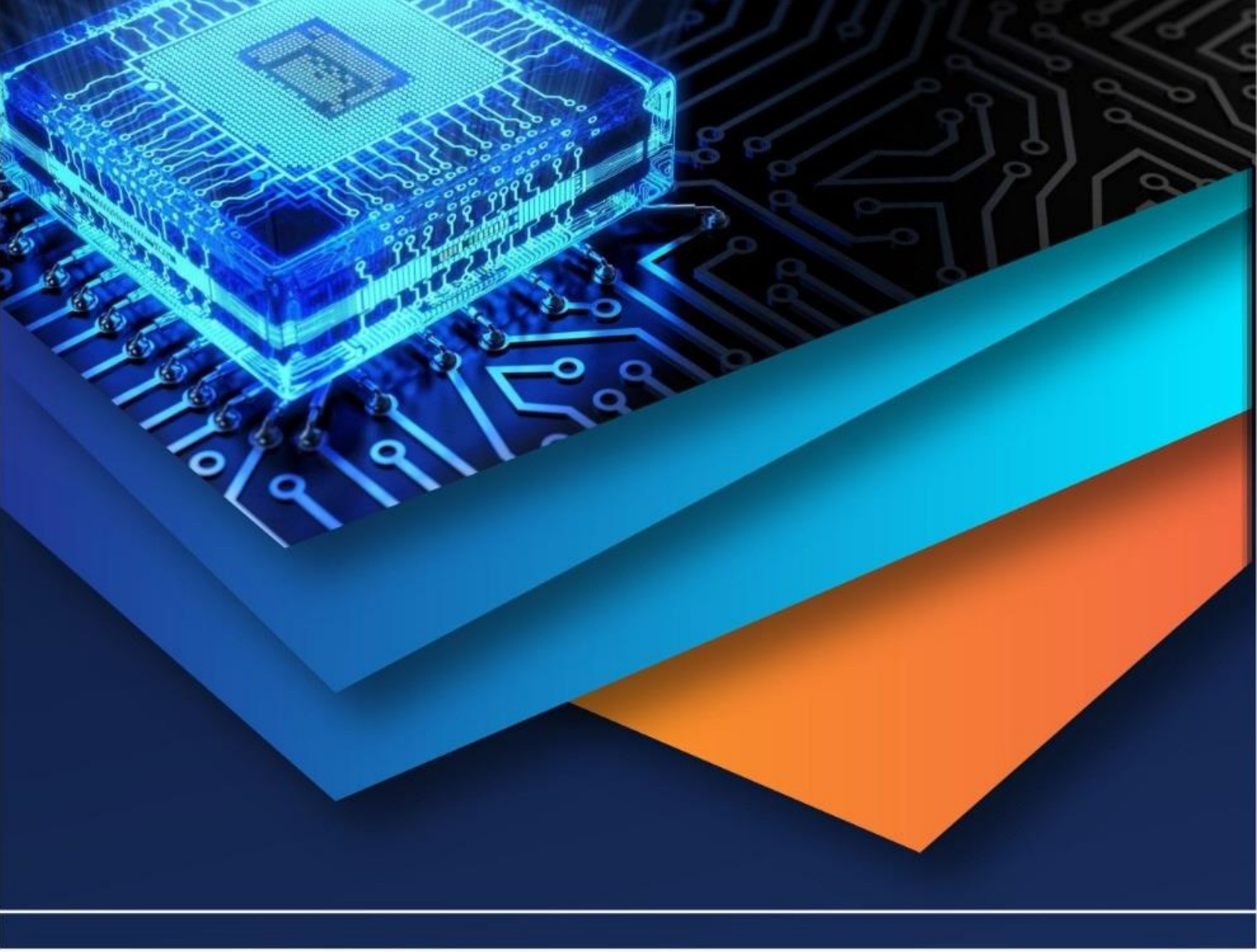
VIII. ACKNOWLEDGMENT

We would like to express our deepest gratitude to all those who contributed to the completion of this article on detecting DDoS attacks using machine learning algorithms. Special thanks to our mentor for their invaluable guidance and support throughout this project. We are also thankful to the researchers and developers whose work served as the foundation for this study. Additionally, we extend our appreciation to the reviewers for their constructive feedback, which greatly enhanced the quality of this work. Furthermore, we are grateful to the academic institutions and organizations that provided resources and facilities for conducting this research. Finally, we acknowledge the encouragement and understanding of our family and friends, whose unwavering support kept us motivated during challenging times.

REFERENCES

[1] M. Devendra Prasad. Prasanta Babu V, C Amaranth "Machine Learning DDoS Detection Using Stochastic Gradient Boosting " in 'JCSE International Journal of Computer Sciences and Engineering' , Vol.7, Issue -4, April 2019
[2] Sheeraz Ahmed, Zahoor Ali Khan, Syed Muhammed Mohsin, Shahid Latif, Sheraz Aslam. Hana Mujlid, Muhammad Adil and Zeeshan Najam, "Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron" in "Future Internet",2023
[3] Hongyan He, Guoyan Huang, Bing Zhang, and Zhangqi Zheng, "Research on Dos Traffic Detection Model Based on Random Forest and Multilayer Perceptron", in 'Wiley Hindawi' December 2023
[4] V. Kumar, A. Kumar, S.Garg, S R Payyavula , "Boosting Algorithms to Identify Distributed Denial of Service Attacks " in 'IOP Publishing(Journal of Physics: Conference Series)', 2022
[5] Kishore Babu Dasari, Nagaraju Devarakonda, "Detection of DDoS Attacks Using Machine Learning Classification Algorithm", in 'MECS Press', Vol.14, Issue-16, August 2019
[6] Ebtihal Sameer Alghoson, Onytra Abbass, "Detecting Distributed Denial of Service Attacks using Machine Learning Models" in (IJACSA) International Journal of Advanced Computer Science and Applications', Vol.12, Isssue-12,2021
[7] Saman Sarraf, "Analysis and Detection of DDoS Attacks using Machine Learning Techniques, in 'American Scientific Research Journal for engineering, Technology, Sciences',Vol.66,Issue-1, 2020
[8] Mohamed Ali Setitra, Mingyu Fan, Bless Lord Y. Agbley and Zine El Abidine Bensalem, "Optimized MLP-CNN Model to Enhance Detecting DDoS Attacks in SDN Environment" in 'MDPI' ,2023.
[9] Mouhammd Alkasassbeh, Ahmad B.A Hassanat, Ghazi Al-Naymat, Mohammad Almseidin , "Detecting Distributed Denial of Service Attacks Using Data Mining Techniques ", in 'IJACSA(International Journal of Advanced Computer Science and Applications), Vol.7, 2016.
[10] T.Subbulakshmi, P. Parameswaran, C. Parthiban, M. Mariselvi, J. Adlene Anusha and G. Mahalakshmi, " A Unified Approach for detection and prevention of ddos attacks using enhanced support vector machines and filtering mechanisms", in ICTACT, Vol.4, issue-2, 2013.
[11] Mohisha H M, Dr. M Ashok Kumar, "A Survey on Machine Leaning Techniques Used For Detection of DDoS Attacks" in Think India Journal, Vol.22, Issue-16, August 2019.
[12] A.O . Akinwumi , A.O.Akingbesote , O.O.Ajayi,F.O.Aranuwa,"DETECTION OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS USING CONVOLUTIONAL NEURAL NETWORKS" in 'Nigerian Journal of Technology (NIJOTECH) ' , vol.41 , Issue-06, November 2022
[13] Velisi Nirmala Priya , " Study on Detection of DDoS Attacks using Machine Learning Techniques " in 'International Journal of Research Publication and Reviews' , Volume. 3, Issue-10 , October- 2022
[14] Nimisha Panday , Pramod Kumar Mishra , "Detection of DDoS attack in IoT traffic using ensemble machine learning techniques" , in 'AIMS Presss' , Vol.18 , Issue-04, May 2023
[15] Christos Siaterlis, Basis Magaris, " Detecting DDoS attacks using a multilayer Perceptron classifier", in 'National Technical University of Athens Iroons Politechniou', March2004
[16] Velisi Nirmala priya, " Study on Detection of DDoS Attacks using Machine Learning Techniques" in 'International Journal of Research Publication and Reviews', Volume.3, Issue-10, October-2022
[17] Nimisha Pandey, Pramod Kumar Mishra, "Detection of DDoS attack in IoT traffic using ensemble machine learning techniques", in 'AIMS Presss', Vol.18, Issue-04, May 2023
[18] Aween Abubakr Saeed, Noor Ghazi Mohammed Jameel, "Intelligent feature selection using particle swarm optimization algorithm with a decision tree for DDoS attack detection" in 'International Jornal of Advances in Intelligent Informatics'. Vol.7, Issue-1, March 2021
[19] Sri Hari Nallamala, Dr. Pragnyaban Mishra, KLEF, Dr. Suvarna Vani Koneru, VRSEC, Breast Cancer Detection using Machine Learning Way, International Journal of Recent Technology and Engineering (IJRTE), Vol.8, Issue-2S3, July 2019, ISSN: 2277-3878.
[20] Sri Hari Nallamala, Dr. Pragnyaban Mishra, KLEF, Dr. Suvarna Vani Koneru, VRSEC, Pedagogy and Reduction of K-NN Algorithm for Filtering Samples in the Breast Cancer Treatment, International Journal of Scientific & Technology Research (IJSTR), Vol.8, Issue 11, November 2019, ISSN: 2277-8616.
[21] N B Naidu, Sri Hari Nallamala, Chukka Swarna Lalitha, Syed Seema Anjum, VVIT, Pertaining Formal Methods for Privacy Protection, International Journal of Grid & Distributed Computing, ISSN: 2005-4262, Vol. 13, No. 1, March – 2020.

[22] Kranthi Madala, Sushma Chowdary Polavarapu, VRSEC, Sri Hari Nallamala, Automatic Signal Indication System through Helmet, International Journal of Advanced Science and Technology, Vol. 29, No. 05, April/May – 2020, ISSN: 2005-4238.
[23] Sri Hari Nallamala, Dr. D. Durga Prasad, PSCMRCET, J. Ranga Rajesh, MICT, Dr. Pragnaban Mishra, KLEF, Sushma Chowdary P, VRSEC, A Review on Applications, Early Successes & Challenges of Big Data in Modern Healthcare Management, TEST Engineering and Management Journal,Vol. 83, Issue 3, May – June 2020, ISSN: 0193-4120.
[24] K B Prakash, KLEF, Rama Krishna E, NEC, Nalluri Brahma Naidu, Sri Hari Nallamala, VVIT, Dr. Pragyaban Mishra, P Dharani, KLEF, Accurate Hand Gesture Recognition using CNN and RNN Approaches, International Journal of Advanced Trends in Computer Science and Engineering, Vol. 9, No. 3, May – June 2020, ISSN: 2278-3091.
[25] Sushma Chowdary P, Kranthi Madala, VRSEC, M Sailaja, PVPSIT, Sri Hari Nallamala, Investigation on IoT System Design & Its Components, Jour of Adv Research in Dynamical & Control Systems, Vol. 12, Issue-06, June – 2020, ISSN: 1943-023X.
[26] Sri Hari Nallamala, Bajjuri Usha Rani, LBRCE, Anandarao S, LBRCE, Dr. Durga Prasad D, PSCMRCET, Dr. Pragnyaban Mishra, KLEF, A Brief Analysis of Collaborative and Content Based Filtering Algorithms used in Recommender Systems, IOP Conference Series: Materials Science and Engineering, 981(2), 022008, December 2020, ISSN: 1757-899X.
[27] Manukonda Vinay, Gonugunta Bhanu Sankara Sai Venkatesh, Malempati Venkata Priyanka, Dogiparthi Venkata Sai, Dr. Sri Hari Nallamala, VVIT, Deep Learning Based Face Mask Detection for User Safety from Covid-19, International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), e-ISSN: 2320-9801, p-ISSN: 2320-9798, Volume 10, Issue 5, May 2022.
[28] P. Radha Vyshnavi, M.V.N. Sai Niharika, M. Summayya, P. Pravallika, Dr. Sri Hari Nallamala, VVIT, Liver Disease Prediction Using Machine Learning, International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), e-ISSN: 2319-8753, p-ISSN: 2320-6710, Volume 11, Issue 6, June 2022.
[29] Y. Vineela Devi, T.Akshara, S.Mohitha, V.Venkatesh, N.Sri Hari, VVIT, Precision Farming By Analyzing Soil Moisture and NPK Using Machine Learning, International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), e-ISSN: 2319-8753, p-ISSN: 2320-6710, Volume 11, Issue 6, June 2022.
[30] Dr. N. Sri Hari, M. Ramya Sri, Mythri .P, N. Sai Harshitha, M. VenkataNaga Sai Kumar, Detection of Covid-19 using Deep Learning, IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCE, UGC CARE Listed (Group -I) Journal, Volume 11, Iss 12, Dec 2022; P-ISSN: 2319 1775, Online-ISSN: 2320 7876.
[31] Dr. N. Sri Hari, P. Vanaja, M. Ajay Kumar, M.D.V.S. Akash, K. Sivaiah, Multi Disease Detection using Machine Learning, IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCE, UGC CARE Listed (Group -I) Journal, Volume 11, Iss 12, Dec 2022; P-ISSN: 2319 1775, Online-ISSN: 2320 7876.
[32] Dr.N.Sri Hari, Shaik Nelofor, Siramdasu Leela Vardhan, Sura Rana Prathap Reddy, Sakhamuri Devendra, CycleGAN Age Regressor, International Journal for Innovative Engineering and Management Research, ISSN: 2456-5083, Volume 12, ISSUE 04, Pages: 45-51, April 2023.
[33] Sudheer Mangalampalli, Ganesh Reddy Karri, Amit Gupta, Tulika Chakrabarti, Sri Hari Nallamala, Prasun Chakrabarti, Bhuvan Unhelkar, Martin Margala, Fault-Tolerant Trust-Based Task Scheduling Algorithm Using Harris Hawks Optimization in Cloud Computing, Sensors 2023, 23(18), 8009; https://doi.org/10.3390/s23188009.
[34] K. Sudharson, …, Sri Hari Nallamala, et al., Hybrid Quantum Computing and Decision Tree based Data Mining for Improved Data Security, 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA), August 18-19, 2023, 979-8-3503-0426-8/23/$31.00 ©2023 IEEE



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY