International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 02 Feb 2024, pp: 547-557 www.ijaem.net ISSN: 2395-5252

A Model for Detecting DDoS Botnet Attacks on IoT Devices Using Deep Learning

Stow, May Tamara
Department of Computer Science and Informatics, Federal University Otuoke, Nigeria

Date of Submission: 28-02-2024 Date of Acceptance: 08-03-2024

ABSTRACT- Internet of Things (IoT) devices are vulnerable to various threats, such as DDoS attacks, which can undermine their security and performance (Empirical, simulation-generated datasets like Bot-IoT and IoTID20 have enabled the study of attacks on the IoT ecosystem, including botnet attacks. This paper examines a DDoS dataset through Exploratory Data Analysis (EDA) methodologies to reveal crucial insights for future modeling efforts. Random undersampling technique was used to solve the data imbalance problem. Random Forest Classifier was used to identify essential predictors through feature ranking for feature extraction. An MLP model is utilized for detecting DDoS Botnet attacks, resulting in an exceptional accuracy rate of 99.99%. The evaluation metrics precision, recall, and F1-score demonstrate the model's effectiveness in reliably distinguishing between "Normal" and "DDOS" classes, with no misclassifications shown in the confusion matrix. This paper highlights the significance of Exploratory Data Analysis (EDA) in comprehending data features. It confirms the effectiveness of Multi-layer Perceptron (MLP) models in identifying DDoS attacks on Internet of Things (IoT) devices.

Keywords- Distributed Denial of Service, IoT devices, MLP, Random Forest Classifier

I. INTRODUCTION

DDoS botnet attacks targeting IoT devices are a significant worry because of their ability to interrupt services and create extensive harm. These attacks utilize botnets, such as the Mirai IoT Botnet, to create a significant amount of traffic aimed at a specific target, causing it to become unresponsive (Pedreira et al., 2021). IoT devices are vulnerable to various threats, such as DDoS attacks, which can undermine their security and performance (Silva et al., 2020). Empirical, simulation-generated datasets like Bot-IoT and IoTID20 have enabled the study of attacks on the IoT ecosystem, including botnet attacks (Albulayhi et al., 2021).

These attacks present security dangers beyond single devices to affect entire IoT networks, introducing new vulnerabilities and threats. The interconnection of IoT devices and the variety of devices connected in IoT create a wide range of possible security risks, such as DDoS botnet attacks (Costa et al., 2021). The constraints of IoT devices, primarily related to battery life and computational capabilities, add to the difficulties in addressing DDoS botnet attacks (Alimi et al., 2020). It also can severely disrupt many services, as evidenced by the significant impact of the Mirai botnet on various IoT devices in 2016 (Koutras et al., 2020). Moreover, IoT devices are prone to attacks, such as DDoS botnet attacks, due to an average of 25 exploitable vulnerabilities, with 70% of IoT devices being susceptible to these attacks (Dasari et al., 2020).

Machine Learning (ML) is a promising method for identifying and reducing Distributed Denial of Service (DDoS) botnet attacks on Internet of Things (IoT) devices. ML-based DDoS attack-detection algorithms have been suggested by Mrabet et al. in 2020. Reinforcement learning techniques, such as Q-learning, are proposed for IoT device authentication and identifying jamming and malware attacks using environmental learning without needing a pre-existing training dataset (Ahmed et al., 2021). The Internet of Things (IoT) is vulnerable to Distributed Denial of Service (DDoS) attacks carried out by botnets due to its wireless, interconnected digital gadgets that can gather, transmit, and save data autonomously (Kelly et al., 2020; Pedreira et al., 2021). Moreover, machine learning on edge devices using low-power communication protocols, such as LoRa, has been proposed as a solution (Merenda et al., 2020). The analysis focused on studying attacks on the IoT ecosystem using datasets created through simulations and empirical data, including the Bot-IoT and IoTID20 databases (Albulayhi et al., 2021). The significant growth of networked IoT devices and their limited ability to use modern security measures make them a prime target for malicious attacks (Ankergård et al., 2021). The Mirai botnet, which targeted IoT devices, caused a major DDoS attack, demonstrating the susceptibility of IoT devices to such attacks (Koutras et al., 2020; Kalbo et al., 2020).

The combination of cloud and edge computing platforms in IoT is highlighted to overcome IoT devices' restricted processing power and storage capacity and offer efficient and secure services for end-users (Kayes et al., 2020). Cloud applications are known to create universal machine learning models by training them using data gathered from Internet of Things devices in different settings (Hamdan et al., 2020). Security in the connection between the IoT network and wireless spectrum database can be improved by utilizing secure sockets layer (SSL) or transport layer security (TLS) certificates, combined with authentication through hypertext transfer protocol secure (HTTPS) (Guimarães et al., 2021). Implementing intricate security algorithms and protocols on IoT devices is difficult because of constraints such as low battery life and processing capacity (Ahad et al., 2020). Furthermore, implementing physical unclonable functions (PUFs) for securing secret keys in IoT devices has been suggested to improve hardware security (Günlü & Schaefer, 2020).

Utilizing machine learning to identify and reduce DDoS botnet attacks on Internet of Things (IoT) devices is a crucial research focus. Robust security methods must be developed to protect IoT devices from threats, utilizing machine learning, cloud, edge computing, and hardware security mechanisms.

II. LITERATURE REVIEW

Hussain et al. (2021) propose a robust dual machine learning approach to prevent and detect IoT botnet attacks. A ResNet-18 deep learning model is first trained to detect scanning activities, which are essential in the initial phases of an attack, to prevent IoT botnet invasions. Another ResNet-18 model is implemented to identify DDoS attacks, enhancing the system's capacity to detect and mitigate these threats effectively. The results demonstrate high-performance metrics: 98.89% accuracy, 99.01% precision, 98.74% recall, and 98.87% f1-score, highlighting the effectiveness of the suggested method. The work supports its assertions by thorough experimentation, comparing the dual approach with other models using different datasets, confirming its better effectiveness in preventing and identifying botnet attacks. The study effectively argues for implementing the suggested methodology as a strong defense strategy against IoT botnet threats.

Albulayhi et al. (2021) introduced an IoT intrusion detection classification system and framework, emphasizing anomaly detection in IoT networks. The study suggests a lightweight Intrusion Detection System (IDS) that utilizes payload modeling to identify Distributed Denial of Service (DDoS) attacks on Internet of Things (IoT) networks. This methodology is in line with identifying DDoS botnet attacks on IoT devices. The study's results offer valuable insights into the possibility of anomaly detection in IoT networks for identifying DDoS attacks.

McDermott et al. (2018) describe using deep learning to utilize a Bidirectional Long Short-term Term Memory Recurrent Neural Network (BLSTM-RNN) and Word Embedding for botnet detection. The study involves comparing the BLSTM-RNN model with a unidirectional LSTM-RNN to determine if the BLSTM-RNN's use of contextual information from both past and future results in better accuracy or loss metrics for the analyzed dataset. Both models provide good accuracy and low loss metrics when tested against the four attack channels used by the Mirai botnet malware. The validation accuracy for Mirai, UDP, and DNS attacks is 99%, 98%, and 98%—the validation loss metrics range from 0.000809 to 0.125630. The BLSTM-RNN model is highly effective in improving botnet identification, particularly in situations with intricate assault patterns.

Mrabet et al. (2020) conducted a survey on IoT security using a layered architecture involving sensing and data analysis. The suggested approach allows for gathering IoT data, extracting characteristics, and categorizing IoT traffic into two groups to identify malicious traffic that triggers DDoS attacks. This method is suitable for the purpose since it offers a thorough approach to identifying and categorizing DDoS attacks on IoT devices. The study's results provide valuable insights into the possibilities of layered architecture for efficient DDoS attack detection.

Alzahrani and Bamhdi (2022) introduce a robust system to recognize botnet attacks on IoT devices by combining a convolutional neural network with an extended short-term memory algorithm. It focuses on detecting common attacks, such as BASHLITE and Mirai, on four different types of security cameras. Lab-connected cameras in IoT contexts collected data, resulting in ideal performance metrics. The system demonstrated vital precision and recall rates, achieving 88% precision, 87% recall, and an F1 score of 83% for detecting botnets on the Provision PT-737E camera. On the Provision PT-838 camera, the system showed a recall rate of 89%, an F1 score of 85%, and a precision rate of 94%. The results highlight the system's ability to reliably detect and counter botnet attacks, demonstrating its potential to enhance cybersecurity in IoT environments.

Silva et al. (2020) introduced a classification system of DDoS attack prevention methods using SDN technology in IoT environments. The study emphasized the difficulties in deploying new strategies to reduce DDoS attacks in IoT environments because of the intricate details and diverse tactics required. The issues revealed in this study are relevant for understanding the difficulty of detecting DDoS attacks in IoT systems, even though they do not directly focus on detecting DDoS botnet attacks.

Pedreira et al. (2021) conducted a comprehensive analysis of cyber threats, weaknesses, and protective measures within Industry 4.0, highlighting the use of botnets like Mirai IoT Botnet for launching DDoS attacks. The study examined how botnets might enhance the effectiveness of attacks, specifically focusing on identifying DDoS botnet attacks on IoT devices. This study's findings enhance comprehension of the vulnerabilities and attack techniques linked to DDoS botnet attacks in IoT settings.

Rabbani et al. (2021) examined machine learning methods for detecting harmful network behavior within new technologies. The study examined the constraints of the clustering algorithm, namely in detecting attacks like DDoS. The limits discussed are crucial to comprehending the difficulties in detecting DDoS botnet attacks on IoT devices despite the primary focus being identifying malicious behavior.

Alkahtani and Aldhyani (2021) introduced a hybrid deep learning system, CNN-LSTM, to identify botnet attacks (BASHLITE and Mirai) on nine commercial IoT devices. The study conducted thorough empirical research using an authentic N-BaIoT dataset obtained from a real system consisting of benign and malignant patterns. The CNN-LSTM model demonstrated higher performance with accuracies of 90.88% and 88.61% in detecting botnet attacks from doorbells (Danminin and Ennio brands). In comparison, the suggested method attained an accuracy of 88.53% in identifying botnet attacks from thermostat devices. The suggested system's accuracies in identifying botnet attacks from security cameras were 87.19%, 89.23%, 87.76%, and 89.64% based on accuracy criteria. The CNN-LSTM model effectively detected botnet attacks from different IoT devices with high accuracy.

Abosata et al. (2021) extensively studied IoT, focusing on system integrity. They highlighted the significance of communication models between devices to implement security measures, including anomaly detection and combating cyber-attacks. The results of this study are crucial for comprehending the broader context of safeguarding IoT systems from DDoS botnet attacks.

Hezam et al. (2021) introduce the BiLSTM-CNN model, a hybrid approach merging Bidirectional Long-Short Term Memory Recurrent Neural Network (BiLSTM) and Convolutional Neural Network (CNN) techniques for enhanced data processing and feature optimization in classification tasks. Evaluated against three standard deep learning models (CNN, RNN, and LSTM-RNN) using the N-BaIoT dataset, which includes multi-device IoT data with DDoS attacks from Bashlite and Mirai botnets, the BiLSTM-CNN model outperforms all other classifiers, achieving an accuracy of 89.79% and a low error rate of 0.1546. With a precision of 93.92%, an f1-score of 85.73%, and a recall of 89.11%, the BiLSTM-CNN excels in various performance metrics. While RNN achieves the highest accuracy among individual models (89.77%), LSTM follows closely (89.71%), and CNN trails with the lowest accuracy of 89.50%. The paper underscores the importance of realistic datasets for comprehensive model evaluation. It highlights the efficacy of the proposed BiLSTM-CNN approach in improving classification accuracy for IoT-based DDoS attack detection.

III. METHODOLOGY

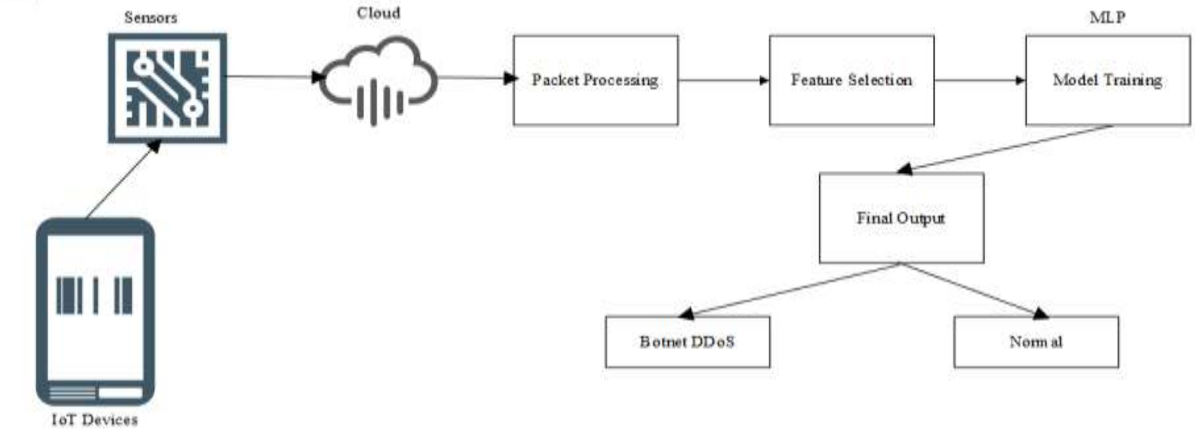


Figure 1: Architecture of the proposed system

To detect Botnet DDoS attacks on IoT devices, the proposed architecture involves several components:
IoT Device: This terminal device is outfitted with sensors for data collection. These devices, usually connected to a network, are susceptible to several types of attacks, such as DDoS attacks.
Sensor: The sensor component collects data from the IoT device, including network traffic, system logs, and behavior patterns. Subsequently, this data is sent to the cloud for additional analysis.
Cloud: The cloud is the central processing unit where data from various IoT devices is collected for analysis. It contains the packet processing module, feature selection algorithm, and model training components.
Packet Processing: The cloud conducts Packet processing to extract pertinent information from the network traffic upon receiving data from IoT devices. This stage examines incoming packets to detect patterns or irregularities that could suggest DDoS attacks.
Feature Selection (Random Forest): The feature selection process uses the Random Forest method to determine the most relevant features from the data. Random Forest is a machine learning technique that constructs numerous decision trees and identifies the most important features by their importance scores.
Model Training (MLP): The chosen features are inputted into a Multi-layer Perceptron (MLP) model to be trained. MLP is a form of artificial neural network recognized for its capacity to comprehend intricate patterns inside data. The model is trained with labeled data to differentiate regular network traffic from DDoS attacks.
Final Output (DDoS or Normal): The system categorizes incoming network data as either regular or indicative of a DDoS assault using the trained MLP model, resulting in the final output. The result is a binary judgment used to detect and reduce any risks to IoT devices.

IV. RESULTS AND DISCUSSION

The result involves conducting exploratory data analysis on the dataset to gain insight into the data and training the Multi-Layer Perceptron (MLP) model for detecting botnet DDoS on IoT devices.

4.1 Exploratory Data Analysis (EDA)

In this section, an Exploratory Data Analysis (EDA) was carried out to extract valuable insights from the DDoS dataset by utilizing visualizations. Exploratory Data Analysis (EDA) is an essential initial step that allows for a comprehensive understanding of the data's features and establishes the basis for future modeling efforts. Figure 2 shows the countplot of the proto column.Figure 3 shows the correlation matrix of numerical features. The correlation matrix shows the relationship between features of the dataset.Figure 4 highlights the distribution of classes within the dataset, notably emphasizing the countplot of different target classes. A crucial measure is implemented to solve the imbalance problem, as emphasized in Figure 5. Finally, a random forest classifier was used to rank the dataset features. The ranking of the features can be seen in Table 1 and Figure 6.

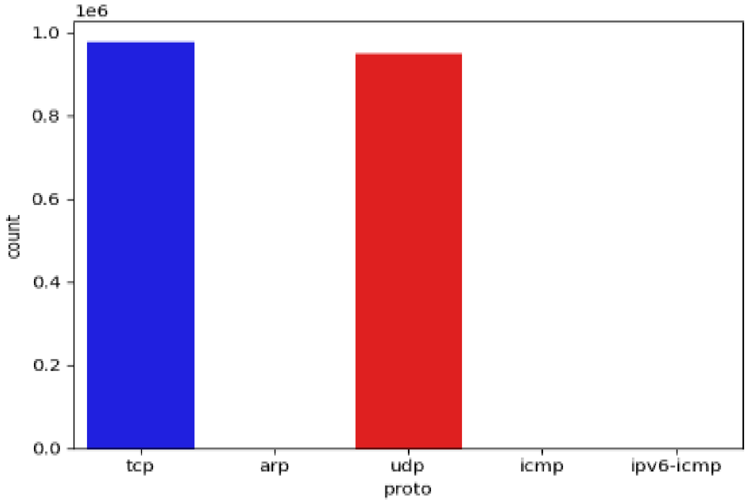


Figure 2: Countplot of the proto column

The countplot indicates that TCP and UDP are the most common protocols in the dataset, as they have the maximum number of bars, demonstrating their prevalence compared to other protocols. This knowledge helps comprehend network traffic structure or examine particular communication patterns in the dataset.

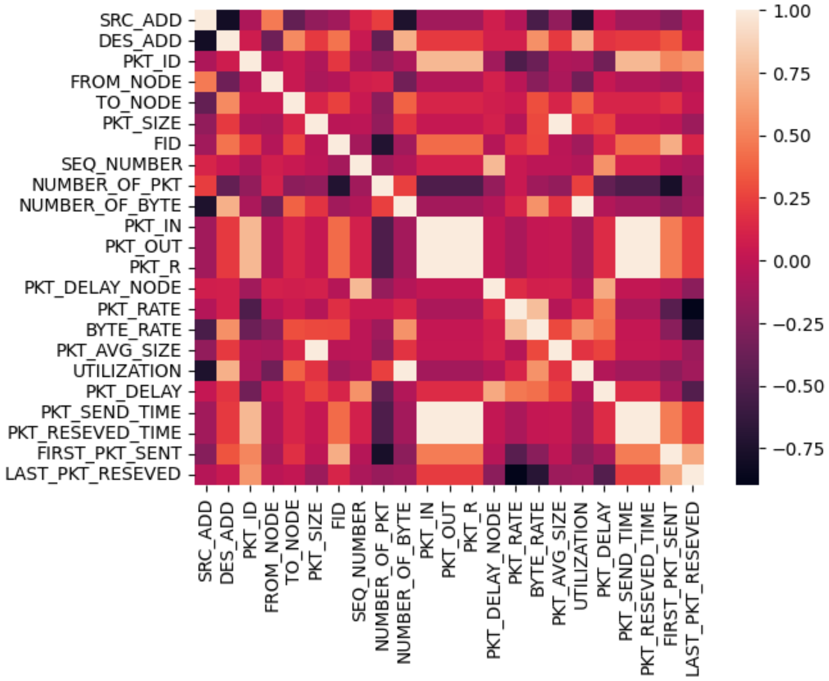


Figure 3: Correlation Matrix of the dataset features

The correlation matrix shows the relationship between the numerical features of the dataset. The correlation matrix shows a relationship between the dataset's features.

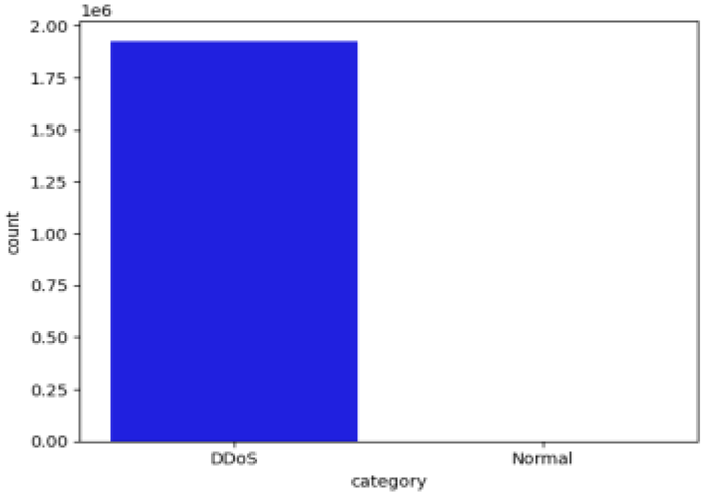


Figure 4: Countplot of the Imbalanced Data

The countplot demonstrates an uneven distribution of classes. Due to this inherent imbalance, it is necessary to implement deliberate interventions to prevent the model from becoming biased towards the majority class.

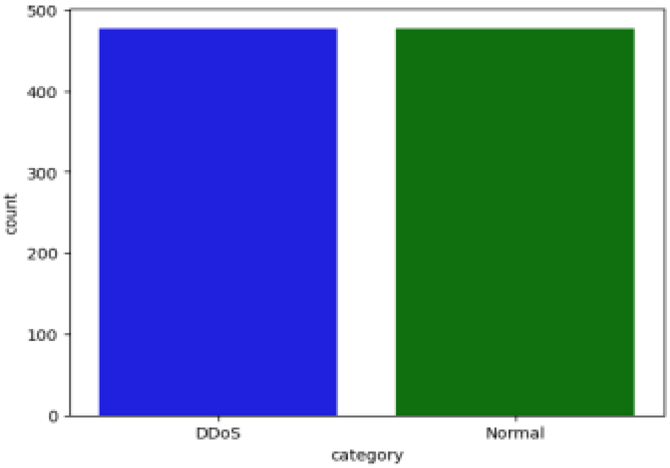


Figure 5: Countplot of the balanced Data

This visual representation illustrates a count plot of the dataset after applying undersampling. It demonstrates a balanced distribution where each class now consists of an equal number of instances, specifically 500.

Table 1: Feature Ranking

Features	Important_Features
N_IN_Conn_P_DstIP	0.175132
time	0.174542
time	0.168909
pkSeqID	0.126626
Pkts_P_State_P_Protocol_P_DestIP	0.073316
TnP_PDstIP	0.060084
TnP_Per_Dport	0.04451
N_IN_Conn_P_SrcIP	0.032013
dur	0.024691

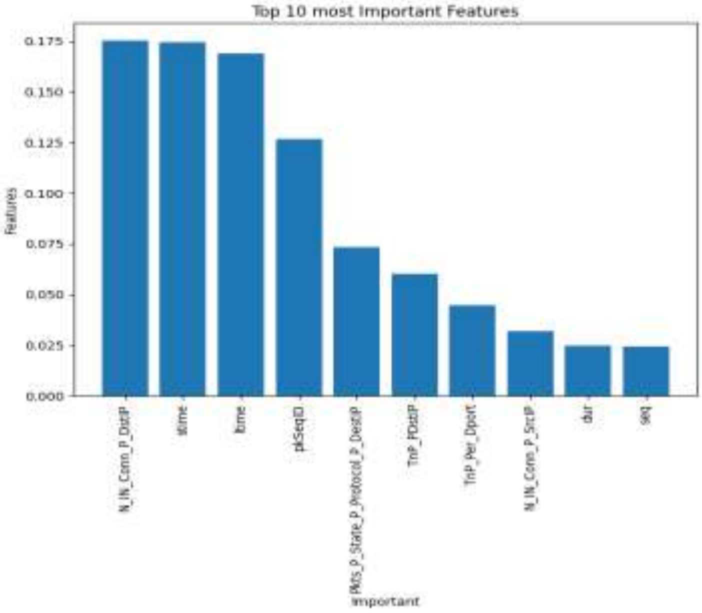


Figure 6: Histogram of the ten most important features

The histogram depicts the first ten most essential features. The feature with the highest bar signifies the most important feature, while the feature with the lost bar represents the least important feature.

4.2 Implementation of MLP For Detecting DDoS Botnet Attacks

A sequential model with three dense layers is employed in implementing a Multi-layer Perceptron (MLP) for fault detection in autonomous vehicles. The first layer consists of 50 units, utilizes the rectified linear unit (ReLU) activation function, and takes the input shape derived from the flattened training data. The second hidden layer also comprises 50 units with ReLU activation. The final layer, with five units and a softmax activation function, serves as the output layer, representing the five distinct fault classes. The model is compiled using the Adam optimizer, categorical cross-entropy loss function, and accuracy as the evaluation metric. This architecture is designed to capture complex relationships within the input data and detect botnet attacks accurately on IoT devices. The training process of the MLP can be seen in Table 2. Figure 7 shows the accuracy of the MLP model for training and testing, and Figure 8 shows the loss values of the MLP model for both training and testing. Figure 9 shows the classification report of the MLP model, and Figure 10 shows the confusion matrix for the MLP model.

Table 2: MLP Training Steps For Botnet DDoS Detection on IoT Devices

```
Epoch 1/10

24/24 [==============================] - 2s 24ms/stop - loss: 0.3425 - Accuracy: 0.8702 - val_loss:
0.1195 - val_accuracy: 0.9895
Epoch 2/10
24/24 [==============================] - 0s 9ms/stop - loss: 0.0576 - Accuracy: 0.9987 - val_loss:
0.0298 - val_accuracy: 1.0000
Epoch 3/10
24/24 [==============================] - 0s 8ms/stop - loss: 0.0162 - Accuracy: 1.0000 - val_loss:
0.0112 - val_accuracy: 1.0000
Epoch 4/10
24/24 [==============================] - 0s 7ms/stop - loss: 0.0072 - Accuracy: 1.0000 - val_loss:
0.0062 - val_accuracy: 1.0000
Epoch 5/10
```

```
24/24 [==============================] - 0s 10ms/stop - loss: 0.0043 - Accuracy: 1.0000 - val_loss:
0.0040 - val_accuracy: 1.0000
Epoch 6/10
24/24 [==============================] - 0s 11ms/stop - loss: 0.0029 - Accuracy: 1.0000 - val_loss:
0.0028 - val_accuracy: 1.0000
Epoch 7/10
24/24 [==============================] - 0s 9ms/stop - loss: 0.0021 - Accuracy: 1.0000 - val_loss:
0.0021 - val_accuracy: 1.0000
Epoch 8/10
24/24 [==============================] - 0s 8ms/stop - loss: 0.0015 - Accuracy: 1.0000 - val_loss:
0.0017 - val_accuracy: 1.0000
Epoch 9/10
24/24 [==============================] - 0s 8ms/stop - loss: 0.0012 - Accuracy: 1.0000 - val_loss:
0.0013 - val_accuracy: 1.0000
Epoch 10/10
24/24 [==============================] - 0s 7ms/step - loss: 9.7540e-04 - accuracy: 1.0000 - val_loss:
0.0011 - val_accuracy: 1.0000

CPU times: total: 4.3 s
Wall time: 4.18 s
```

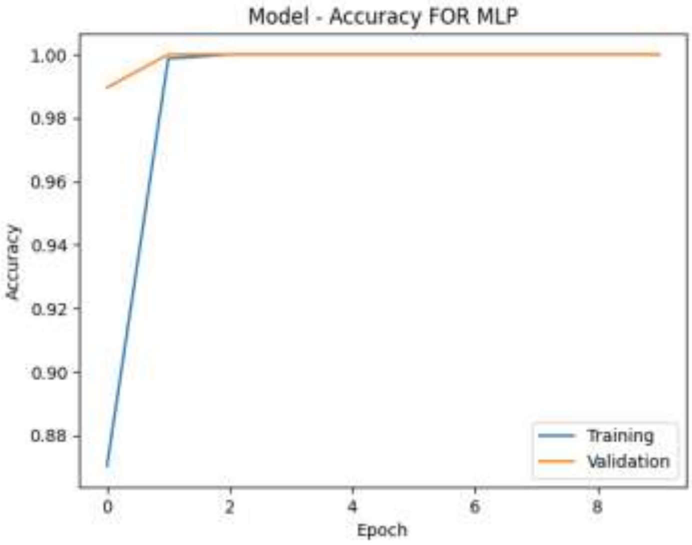


Figure 7: Accuracy of the MLP model for both Training and Testing

The accuracy demonstrates how well the model performed during training. This shows that the model achieved an accuracy of 99.99% for the training data and99.99% for the validation or testing data. The blue line represents the model training accuracy, whereas the orange line represents the validation test accuracy. A validation test means the evaluation of the model performance by using testing data.

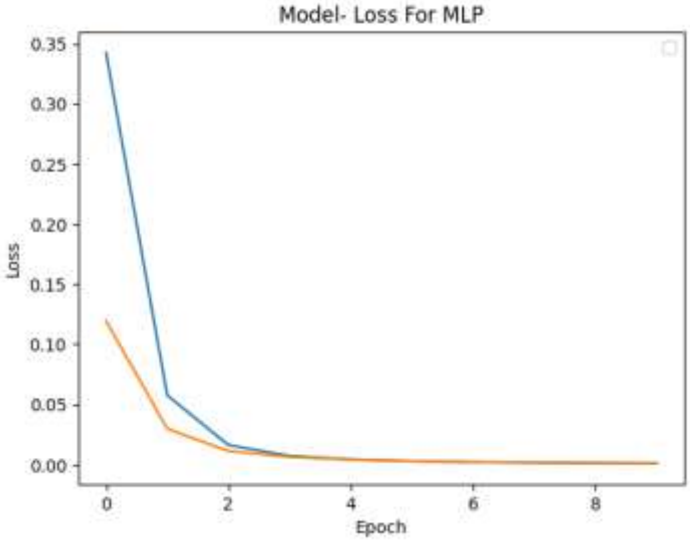
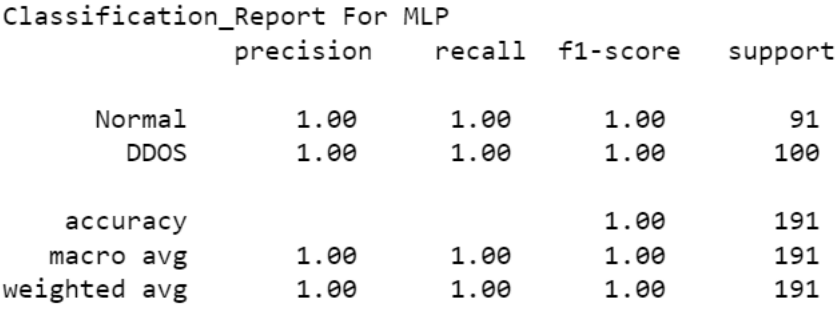


Figure 8: Loss values for the training and testing of the MLP model.

The line graph above represents the losses acquired by the model during training and testing. The green line indicates the loss acquired by the model during training, and the orange line indicates the loss acquired during testing. The loss values are acquired at each training step, starting from step 1 to step 10. Loss values mean the losses the model had during training. This shows that the model achieved a loss value of about 0.02% for the training and validation or testing data.



```
Classification_Report For MLP
               precision    recall  f1-score   support

      Normal        1.00      1.00      1.00        91
        DDOS        1.00      1.00      1.00       100

    accuracy                            1.00       191
   macro avg        1.00      1.00      1.00       191
weighted avg        1.00      1.00      1.00       191
```

Figure 9: Classification Report of the MLP model

The classification report indicates the outstanding performance of the Multi-layer Perceptron (MLP) model with flawless precision, recall, and F1-score for the "Normal" and "DDOS" classes. This shows that the model correctly classified all occurrences of both classes in the dataset. The 100% accuracy rate solidifies the model's ability to differentiate between the two classes. The MLP model shows outstanding classification performance with great precision, recall, and accuracy, making it reliable.

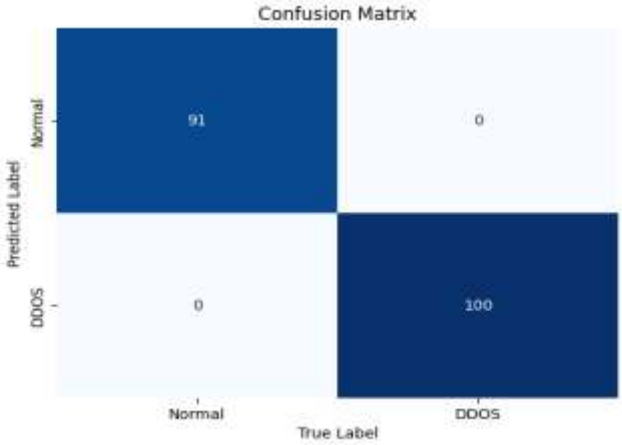


Figure 10: Confusion Matrix of the MLP model

The confusion matrix shows the number of correct and incorrect model predictions on the test data. The result of the confusion matrix shows that the MLP model makes correct predictions for all the classes with misclassification of 0%.

V. CONCLUSION

This paper highlights the significance of comprehensive Exploratory Data Analysis (EDA) as the first step in comprehending the complexities of DDoS datasets. Visualizations offered insights on protocol dispersion, feature correlations, and class imbalances, guiding further modeling endeavors. The Random Forest Classifier was used to rank features and find essential predictors in the dataset. The Multi-layer Perceptron (MLP) model showed outstanding effectiveness in identifying DDoS Botnet attacks, with an accuracy rate of 99.99%. Evaluation measures confirmed the model's reliability by demonstrating its precision, recall, and F1-score inappropriately categorizing the "Normal" and "DDOS" classes. The results highlight the effectiveness of MLP models in dealing with cybersecurity issues, especially in identifying DDoS attacks on IoT devices. This research offers valuable insights for creating robust defense mechanisms against cyber threats.

VI. ACKNOWLEDGMENT

I conducted this research with the opportunity provided by the Department of Computer Science, Federal University Otuoke, Nigeria. Therefore, I express my gratitude and acknowledge their support.

REFERENCES

[1]. Abosata, N., Al-Rubaye, S., Tsourdos, A., & Emmanouilidis, C. (2021). Internet of Things for system integrity: A comprehensive survey on security, attacks, and countermeasures for industrial applications. Sensors, 21(11), 3654. https://doi.org/10.3390/s21113654

[2]. Ahad, A., Tahir, M., Sheikh, M., Ahmed, K., Mughees, A., & Numani, A. (2020). Technologies trend towards 5g network for smart health-care using iot: a review. Sensors, 20(14), 4047. https://doi.org/10.3390/s20144047

[3]. Ahmed, K., Tahir, M., Habaebi, M., Lau, S., & Ahad, A. (2021). Machine learning for authentication and authorization in iot: taxonomy, challenges and future research direction. Sensors, 21(15), 5122. https://doi.org/10.3390/s21155122

[4]. Albulayhi, K., Smadi, A., Sheldon, F., & Abercrombie, R. (2021). IoT intrusion detection taxonomy, reference architecture, and analyses. Sensors, 21(19), 6432. https://doi.org/10.3390/s21196432

[5]. Alimi, K., Ouahada, K., Abu-Mahfouz, A., & Rimer, S. (2020). A survey on the security of low power wide area networks: threats, challenges, and potential solutions. Sensors, 20(20), 5800. https://doi.org/10.3390/s20205800

[6]. Alkahtani, H., & Aldhyani, T. H. (2021). Botnet attack detection by using CNN-LSTM model for Internet of Things applications. Security and Communication Networks, 2021, 1-23.

[7]. Alzahrani, M. Y., & Bamhdi, A. M. (2022). Hybrid deep-learning model to detect botnet attacks over Internet of Things environments. Soft Computing, 26(16), 7721-7735.

[8]. Ankergård, S., Dushku, E., & Dragoni, N. (2021). State-of-the-art software-based

remote attestation: opportunities and open issues for internet of things. Sensors, 21(5), 1598. https://doi.org/10.3390/s21051598

[9]. Costa, V., Oliveira, L., & Souza, J. (2021). Internet of everything (ioe) taxonomies: a survey and a novel knowledge-based taxonomy. Sensors, 21(2), 568. https://doi.org/10.3390/s21020568

[10]. Dasari, V., Kantarci, B., Pouryazdan, M., & Girolami, M. (2020). Game theory in mobile crowdsensing: a comprehensive survey. Sensors, 20(7), 2055. https://doi.org/10.3390/s20072055

[11]. Guimarães, D., Pereira, E., Alberti, A., & Moreira, J. (2021). Design guidelines for database-driven Internet of Things-enabled dynamic spectrum access. Sensors, 21(9), 3194. https://doi.org/10.3390/s21093194

[12]. Günlü, O. and Schaefer, R. (2020). An optimality summary: secret key agreement with physical unclonable functions. Entropy, 23(1), 16. https://doi.org/10.3390/e23010016

[13]. Gutierrez, L., Rabbani, K., Ajayi, O., Gebresilassie, S., Rafferty, J., Castro, L., … & Banos, O. (2021). Internet of things for mental health: open issues in data acquisition, self-organization, service level agreement, and identity management. International Journal of Environmental Research and Public Health, 18(3), 1327. https://doi.org/10.3390/ijerph18031327

[14]. Hamdan, S., Ayyash, M., & Almajali, S. (2020). Edge-computing architectures for internet of things applications: a survey. Sensors, 20(22), 6441. https://doi.org/10.3390/s20226441

[15]. Hezam, A. A., Mostafa, S. A., Baharum, Z., Alanda, A., & Salikon, M. Z. (2021). Combining deep learning models for enhancing the detection of botnet attacks in multiple sensors internet of things networks. JOIV: International Journal on Informatics Visualization, 5(4), 380-387.

[16]. Hussain, F., Abbas, S. G., Pires, I. M., Tanveer, S., Fayyaz, U. U., Garcia, N. M., ... & Shahzad, F. (2021). A two-fold machine learning approach to prevent and detect IoT botnet attacks. Ieee Access, 9, 163412–163430.

[17]. Kalbo, N., Mirsky, Y., Shabtai, A., & Elovici, Y. (2020). The security of IP-based video surveillance systems. Sensors, 20(17), 4806. https://doi.org/10.3390/s20174806

[18]. Kayes, A., Kalaria, R., Sarker, I., Islam, M., Watters, P., Ng, A., … & Kumara, I. (2020). A survey of context-aware access control mechanisms for cloud and fog networks: taxonomy and open research issues. Sensors, 20(9), 2464. https://doi.org/10.3390/s20092464

[19]. Kelly, J., Campbell, K., Gong, E., & Scuffham, P. (2020). The internet of things: impact and implications for health care delivery. Journal of Medical Internet Research, 22(11), e20135. https://doi.org/10.2196/20135

[20]. Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. (2020). Security in some communications: a survey. Sensors, 20(17), 4828. https://doi.org/10.3390/s20174828

[21]. McDermott, C. D., Majdani, F., & Petrovski, A. V. (2018, July). Botnet detection in the Internet of Things using deep learning approaches. In 2018 International Joint Conference on Neural Networks (IJCNN) (pp. 1-8). IEEE.

[22]. Merenda, M., Porcaro, C., & Iero, D. (2020). Edge machine learning for aI-enabled IoT devices: a review. Sensors, 20(9), 2533. https://doi.org/10.3390/s20092533

[23]. Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. Sensors, 20(13), 3625. https://doi.org/10.3390/s20133625

[24]. Pedreira, V., Barros, D., & Pinto, P. (2021). A review of attacks, vulnerabilities, and defenses in Industry 4.0 with new challenges on data sovereignty ahead. Sensors, 21(15), 5189. https://doi.org/10.3390/s21155189

[25]. Rabbani, M., Wang, Y., Khoshkangini, R., Jelodar, H., Zhao, R., Ahmadi, S., … & Ayobi, S. (2021). A review on machine learning approaches for network malicious behavior detection in emerging technologies. Entropy, 23(5), 529. https://doi.org/10.3390/e23050529

[26]. Silva, F., Silva, E., Neto, E., Lemos, M., Neto, A., & Esposito, F. (2020). A taxonomy of DDoS attack mitigation approaches featured by sdn technologies in IoT scenarios. Sensors, 20(11), 3078. https://doi.org/10.3390/s20113078