Quest Journals
Journal of Software Engineering and Simulation
Volume 11 ~ Issue 6 (June 2025) pp: 62-74
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Leveraging Transfer Learning for Predictive Défense Against Evolving Denial of Service Attack Patterns

G.O. Diri [1], E.E. Kalu[2] , P.H. Amadi[3]

[1] *Department of Computer Science, Ignatius Ajuru University of Education, Rivers State, Nigeria*
[2] *Department of Cyber Security & Networking, Glasgow Caledonian University, Scotland*
[3] *Department of Computer Science, Kenule Benson Saro-Wiwa Polytechnic, Rivers State, Nigeria*

Abstract - *In network security, the prompt identification and alleviation of Denial of Service (DoS) attacks are very important. This study examines the efficacy of Long Short-Term Memory (LSTM) models and transfer learning techniques in enhancing the detection capabilities of these attacks. A substantial dataset comprising 28 unique features and 2,160,667 instances is utilised to train a Long Short-Term Memory (LSTM) model. The model, comprising two LSTM layers and a Dense layer, achieves notable accuracy rates of 93.66% in training and 93.57% in validation, accompanied by minimal loss values. Transfer learning is implemented by utilising a pretrained LSTM model as a feature extractor, followed by a CNN-ANN architecture. This approach demonstrates promising outcomes on a secondary dataset, with training and validation accuracies of 99.68% and 99.79% respectively, with negligible loss. The precision, recall, and F1-score metrics underscore the model's efficacy in classifying occurrences of network traffic. The findings underscore the effectiveness of employing LSTM models and transfer learning techniques to tailor security protocols for novel DoS attack patterns. This provides network security specialists with robust capabilities to safeguard against potential threats.*

Keywords – *Distributed Denial of Service Attacks, Transfer learning, Network security, Deep learning*

R*eceived 14 June., 2025;* ***R****evised 24 June., 2025;* ***A****ccepted 29 June., 2025 © The author(s) 2025.*
P*ublished with open access at* ***www.questjournas.org***

I. Introduction

Current network security standards need new strategies because Denial of Service (DoS) attacks have become both more complicated and widespread than before. Transfer learning models enabled to learn from one domain gradually adapt these capabilities toward different domains to develop predictive security protocols against shifting attack patterns. Within the Internet of Things (IoT) context the extensive network of connected devices reveals a large attack surface which traditional security methods struggle to protect [1]. The implementation of transfer learning technology enables IDS researchers to develop highly effective defences for detecting DoS attacks which strengthen network infrastructure protection capabilities [2][3].

Researchers have demonstrated the success of transfer learning through deep learning breakthroughs as they face increasingly complicated attack paths from various sources. Mathematical research demonstrates deep transfer learning models effectively detect strange data patterns alongside harmful traffic characteristics prevailing in IoT systems despite their sparse and variable information structures [3][4]. The combination of transfer learning and federated learning yields privacy-enhanced models which draw knowledge from distributed data sources through decentralized systems [5]. The combined approach enhances IDS detection performance alongside authentication of privacy standards establishing itself as essential for contemporary cybersecurity operations [6].

The use of transfer learning techniques dramatically boosts both the flexibility and operational effectiveness of security frameworks for intrusion detection systems. Rapid threat identification becomes achievable for organisations through pre-trained models which reduce training duration and resource requirements [7][8]. The detection of DoS attacks especially benefits because their dynamic characteristics frequently change fast. Transfer learning grants security systems domain-independent learning skills which helps maintain their effectiveness when attack patterns shift [9]. The utilization of transfer learning techniques results in superior Intrusion Detection Systems performance while advancing active security measures against complex threats.

II. Literature Review

Musa [10] proposes a method for identifying DDoS assaults utilising both conventional machine learning and deep learning classifiers. The research underscores the need of utilising machine learning in cybersecurity, especially for IoT networks. The findings demonstrate elevated accuracy rates, with several classifiers attaining precision levels over 90%. Nevertheless, the paper acknowledges constraints in the scalability of the models when utilised with larger datasets.

Churcher et al. [11] conduct a comparative examination of various machine learning techniques, including k-nearest neighbours (KNN), support vector machines (SVM), and random forests (RF), for the classification of attacks in IoT networks. The study indicates accuracy rates between 80% and 95%, contingent upon the algorithm employed. The authors emphasise the difficulty of feature selection and the necessity for robust datasets to enhance model performance.

Bagdadi [12] concentrates on multi-class categorisation of DDoS attacks employing ensemble methodologies. Their findings indicate that ensemble approaches can markedly improve classification accuracy, attaining results over 90%. Nonetheless, the study recognises that the intricacy of ensemble models may result in prolonged training durations and heightened demands on computer resources.

Qasim [13] examines progress in time series analysis for the identification of DDoS attacks. The research illustrates that time series methodologies can proficiently detect assault patterns, attaining accuracy rates exceeding 90%. However, dependence on previous data may constrain the model's flexibility in addressing novel attack vectors.

Wu [14] investigates a DDoS detection technique utilising many machine learning algorithms, such as support vector machines and decision trees. The study indicates a 92% accuracy rate in attack detection, although it highlights the possibility of false positives, which may impede operational efficiency in real-time systems.

Sharma [15] presents an extensive analysis of machine learning methodologies for DDoS detection, emphasising the efficacy of deep learning models. The research demonstrates that deep learning methodologies can attain accuracy rates over 95%, while also highlighting the difficulties related to the quality of training data and the interpretability of models.

Talpur [16] presents an innovative methodology that integrates evolutionary algorithms with machine learning techniques for DDoS detection. The study indicates elevated categorisation accuracy, with certain models attaining precision rates exceeding 98%. Nonetheless, the intricacy of the optimisation algorithms may provide difficulties in real applications.

Alabsi et al. [17] introduce a Conditional Tabular Generative Adversarial Network (CTGAN) for the detection of DDoS attacks in IoT networks. The findings indicate encouraging accuracy levels; yet, the research underscores the necessity for comprehensive training data to guarantee the model's resilience against various assault scenarios.

Goparaju and Rao [18] employ PCA for dimensionality reduction alongside SVM for DDoS detection in their research. The study attains an accuracy of 91%, although it underscores the constraints of PCA in maintaining essential information during feature reduction.

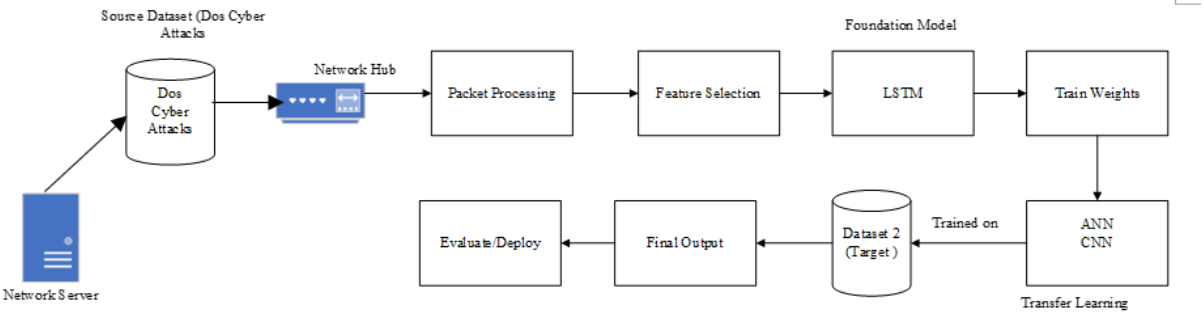
Dasari and Devarakonda [19] concentrate on the velocity and precision of machine learning classification techniques for DDoS detection. Their research demonstrates that machine learning methods surpass conventional methodologies, with accuracy rates of 90% or greater. They warn of the risk of model overfitting if not adequately validated.

Silvery et al. [20] examine deep learning-based multi-class classification for the detection of DoS and DDoS attacks. The study indicates an accuracy of 94%, while also highlighting the difficulties associated with training deep learning models, especially with data requirements and computer resources.

John and Nagappasetty J [21] examine the identification of sluggish DoS assaults in software-defined networks with an intelligent approach. Their findings demonstrate a significant detection rate; yet, the study underscores the necessity for ongoing surveillance and adjustment to changing assault methodologies.

The analysed literature illustrates the efficacy of diverse machine learning algorithms in identifying DoS and DDoS attacks, with accuracy rates often between 80% and 99%. Nevertheless, issues such feature selection, model complexity, and the necessity for high-quality training data persist as substantial limits that necessitate additional study and improvement.

III. Methodology



Architecture Diagram

1. **Network Server**: The Network Server is the brain of the operation, controlling how information travels between nodes. It connects the network hardware to the monitoring software. It takes in data from various network log sources and forwards them on.
2. **Network Hub**: The Network Hub collects and organises data from various network log sources. It makes sure the information is structured and sorted in the right way for further examination. This part is essential for the system's smooth operation as it controls the flow of information.
3. **Packet Processing**: Packet Processing is for inspecting and analysing data packets in a network in search of irregularities. This section filters incoming information using traffic profiling, anomaly detection, and signature-based detection to identify possible DDoS attacks.
4. **Feature Selection**: Feature Selection is picking out valuable characteristics from the data collected in the network logs. This feature aids in data extraction, revealing the presence of DoS attacks. It helps narrow down the data to its most relevant aspects for analysis.
5. **Transfer Learning**: Transfer learning in DDoS attack detection utilises pre-trained models on extensive network traffic datasets to extract pertinent features and trends, enabling the effective real-time identification of hostile actions.

a. Transfer Learning in Artificial Neural Networks (ANN):

Artificial Neural Networks (ANN) have demonstrated effectiveness in learning complex patterns from data and have been widely employed in cybersecurity tasks, including intrusion detection. Transfer learning in ANN involves initializing the network with weights learned from a pre-trained model on a large dataset, followed by fine-tuning on a smaller dataset specific to DoS attack detection. By leveraging features learned from the pre-trained model, ANN can effectively capture the underlying characteristics of DoS attacks, even with limited labeled data.

b. Transfer Learning in Convolutional Neural Networks (CNN):

Convolutional Neural Networks (CNN) excel in extracting spatial features from input data and have found success in image classification and sequential data analysis. In the context of DoS attack detection, CNNs can be employed to extract relevant features from network traffic data. Transfer learning with CNNs involves utilizing pre-trained models, such as those trained on image datasets, for feature extraction. The learned features are then utilized as input to another classifier, enhancing the discriminative power of the model for DoS attack detection.

c. Transfer Learning in Long Short-Term Memory (LSTM) Networks:

Long Short-Term Memory (LSTM) networks are a type of recurrent neural network (RNN) capable of learning long-term dependencies in sequential data. In DoS attack detection, LSTM networks can effectively capture temporal patterns indicative of attacks within network traffic data. Transfer learning with LSTMs involves initializing the network with weights from a pre-trained model on a related sequential data domain and fine-tuning on DoS attack-specific data. By leveraging knowledge learned from the pre-trained model, LSTM networks can adapt to the unique characteristics of DoS attacks and achieve improved detection performance.

6. **Final Output**: The Final Output component summarises the analysis done in the preceding sections. A comprehensive report of potential DDoS attacks and their characteristics is generated. This output is essential for making well-informed decisions
7. **Evaluate and Deploy**: The function of this subsystem is to evaluate the effectiveness of the detection mechanism. To evaluate the system's efficacy, the false positive rate, and the response time, it must be put through a battery of tests mimicking actual attacks. Once the system's efficacy has been verified, it can be proactively deployed in a production network to monitor for DDoS attacks.

DDoS Dataset Description

The dataset appears to contain network log data, likely captured from network devices or systems. Here's a brief description of each of the fields:

Table 1: Dataset 1

1.	**SRC_ADD**: Source address - The IP address or identifier of the sender.
2.	**DES_ADD**: Destination address - The IP address or identifier of the receiver.
3.	**PKT_ID**: Packet ID - Unique identifier for each packet.
4.	**FROM_NODE**: Node identifier or address where the packet originates.
5.	**TO_NODE**: Node identifier or address where the packet is destined.
6.	**PKT_TYPE**: Type of packet (e.g., TCP, UDP, ICMP).
7.	**PKT_SIZE**: Size of the packet in bytes.
8.	**FLAGS**: Flags associated with the packet.
9.	**FID**: Flow ID or identifier for the flow the packet belongs to.
10.	**SEQ_NUMBER**: Sequence number of the packet within its flow.
11.	**NUMBER_OF_PKT**: Total number of packets in the flow.
12.	**NUMBER_OF_BYTE**: Total number of bytes in the flow.
13.	**NODE_NAME_FROM**: Name or identifier of the sending node.
14.	**NODE_NAME_TO**: Name or identifier of the receiving node.
15.	**PKT_IN**: Number of packets received.
16.	**PKT_OUT**: Number of packets sent out.
17.	**PKT_R**: Number of packets routed.
18.	**PKT_DELAY_NODE**: Packet delay within a node.
19.	**PKT_RATE**: Packet transmission rate.
20.	**BYTE_RATE**: Byte transmission rate.
21.	**PKT_AVG_SIZE**: Average packet size.
22.	**UTILIZATION**: Utilization of the network.
23.	**PKT_DELAY**: Packet delay.
24.	**PKT_SEND_TIME**: Time when the packet was sent.
25.	**PKT_RECEIVED_TIME**: Time when the packet was received.
26.	**FIRST_PKT_SENT**: Time when the first packet was sent.
27.	**LAST_PKT_RECEIVED**: Time when the last packet was received.
28.	**PKT_CLASS**: Class or category of the packet.

IV. Experimental Analysis

This section discusses the use of transfer learning in providing predictive measures for evolving Denial of Service Attack Patterns. The algorithms used for the transfer learning are Long Short Term Memory (LSTM), Convolutional Neural Network (CNN), and Artificial Neural Network (ANN). The LSTM algorithm was trained on a dataset with twenty eight (28) features with 2160667 instances, and the weight of the LSTM model was used together with the CNN-ANN algorithm to train the final model on the second dataset, which has twenty three (23) features with 104345 instances. Further explanation of the experiment conducted can be seen in three phases. The first phase has to do with exploratory data analysis for the first and second dataset, the second phase has to with the training of the LSTM model on the first dataset, and the third phase has to do with the training of the ANN-CNN model on the second dataset using the weight of the LSTM to get a final model.

4.1 Exploratory Data Analysis

This section presents an Exploratory Data Analysis (EDA) conducted to derive significant insights from the DDoS dataset through the use of visualisations. Exploratory Data Analysis (EDA) is a crucial preliminary phase that facilitates a thorough comprehension of the data's characteristics and lays the groundwork for further modelling endeavours. Figure 2 presents an aesthetically engaging heatmap that effectively illustrates the cleanliness levels within the dataset. The homogeneity of the heatmap indicates the absence of missing values in the dataset. This preliminary assertion lays the groundwork for a comprehensive analysis of the relationships and patterns within the data.

Figure 3 illustrates the correlation matrix of numerical attributes. The correlation matrix illustrates the interrelationships among the dataset's features.

Figure 4 illustrates the distribution of classes within the dataset, particularly stressing the count plot of various Denial of Service (DoS) assault types. The visual representation reveals a concerning observation—the dataset exhibits an imbalanced distribution of classes. Given this intrinsic imbalance, it is essential to execute intentional interventions to avert the model from developing bias towards the majority class. This bias may undermine the model's ability to accurately detect and classify minority classes.

A critical measure is implemented to rectify this difference, as highlighted in Figure 5. This visual representation depicts a count plot of the dataset subsequent to the application of under sampling. It illustrates an equitable distribution in which each class comprises an identical quantity of examples, exactly 240,000.

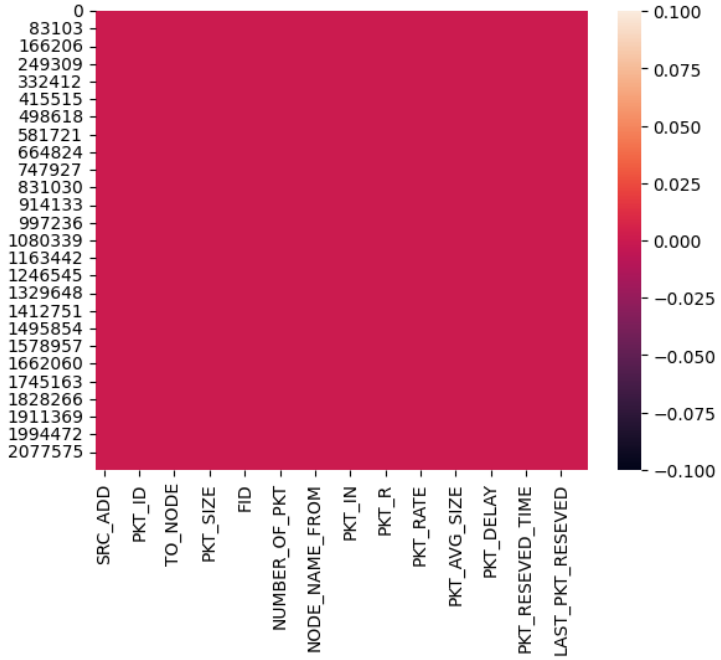


Figure 2: Visualized image of the cleaned data.

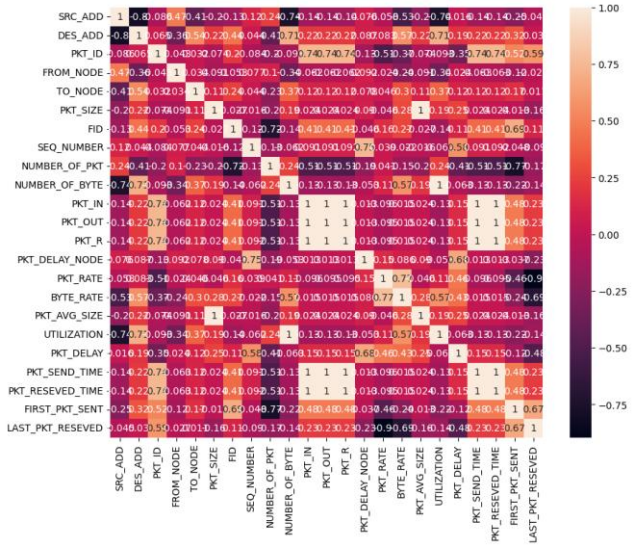


Figure 3: Correlation Matrix

The correlation matrix shows the relationship between numerical features of the dataset. From the correlation matrix.

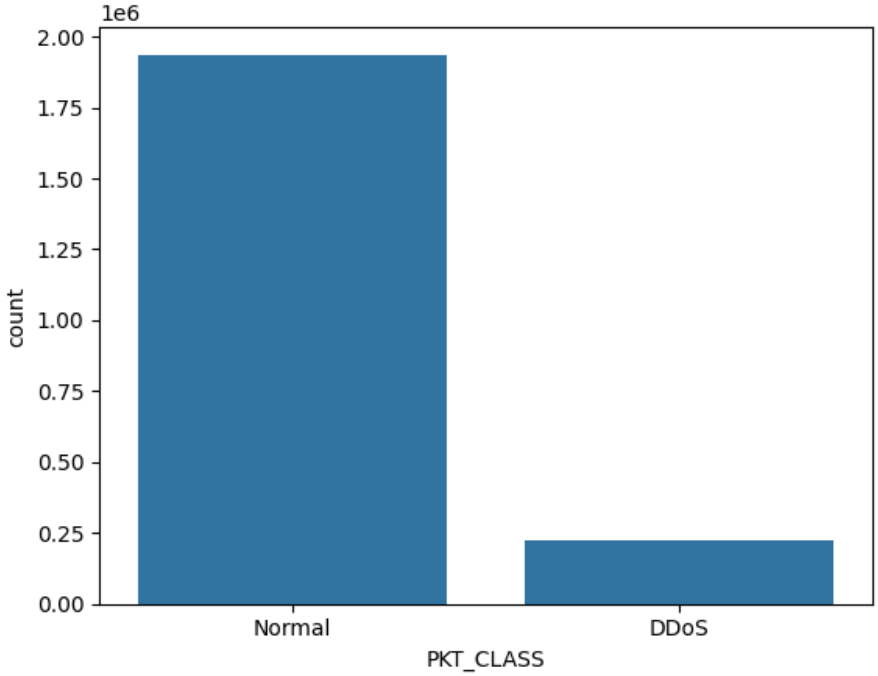


Figure 4: Countplot of the Imbalanced Data

The countplot shows that the dataset is imbalanced, with normal class having higher bar than the DDoS class.

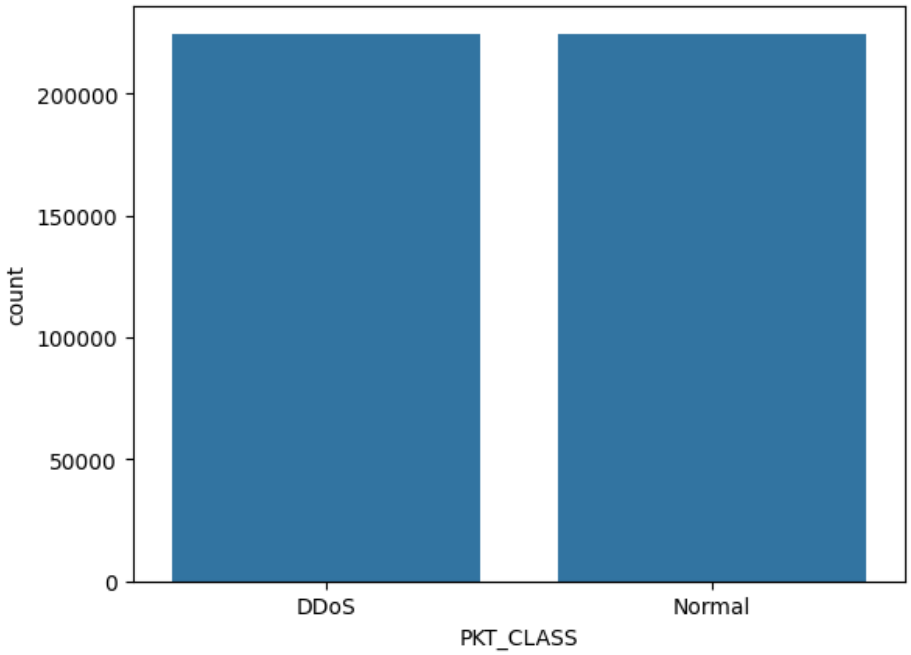


Figure 5: Countplot of the balanced Data

From Figure 5, the data imbalance problem has been resolved with all class having equal number of instances.

4.2 Implementation of LSTM model on the First Dataset

The LSTM model was trained on the first dataset including 28 features and 500,000 instances (the balanced dataset). The implementation utilises TensorFlow's Keras API to develop a Long Short-Term Memory (LSTM) model for identifying DoS threats. The model's architecture comprises two LSTM layers succeeded by a Dense layer. The initial LSTM layer is set with 50 units, intended to handle input data of a specific shape, employing the Rectified Linear Unit (ReLU) activation function, and produces sequences as output. The second LSTM layer consists of 50 units and utilises the Rectified Linear Unit (ReLU) activation function. The Dense layer comprises two units utilising softmax activation, making it ideal for multi-class classification. The model is created via the Adam optimiser alongside the categorical cross-entropy loss function. Training commences for 20 epochs with a batch size of 128. Validation data is provided to evaluate performance on unobserved samples

during training, and the training history is preserved for analysis. Upon completion of training, the LSTM model's weights were preserved for subsequent integration with CNN-ANN. The outcomes of the LSTM model training are presented in Table 2. The LSTM model was assessed by accuracy, loss, classification report, and confusion matrix. These are illustrated in Figures 6, 7, 8, and 9.

Table 2: Training Result of LSTM Model For the First Nine Epochs

Epoch 1/20
2809/2809 [==============================] - 18s 5ms/step - loss: 0.2072 - accuracy: 0.9357 - val_loss: 0.2016 - val_accuracy: 0.9356
Epoch 2/20
2809/2809 [==============================] - 17s 6ms/step - loss: 0.1991 - accuracy: 0.9366 - val_loss: 0.2016 - val_accuracy: 0.9356
Epoch 3/20
2809/2809 [==============================] - 15s 5ms/step - loss: 0.1989 - accuracy: 0.9365 - val_loss: 0.2016 - val_accuracy: 0.9356
Epoch 4/20
2809/2809 [==============================] - 21s 7ms/step - loss: 0.1988 - accuracy: 0.9366 - val_loss: 0.2013 - val_accuracy: 0.9357
Epoch 5/20
2809/2809 [==============================] - 16s 6ms/step - loss: 0.1988 - accuracy: 0.9366 - val_loss: 0.2013 - val_accuracy: 0.9356
Epoch 6/20
2809/2809 [==============================] - 17s 6ms/step - loss: 0.1987 - accuracy: 0.9366 - val_loss: 0.2011 - val_accuracy: 0.9356
Epoch 7/20
2809/2809 [==============================] - 18s 6ms/step - loss: 0.1988 - accuracy: 0.9365 - val_loss: 0.2018 - val_accuracy: 0.9357
Epoch 8/20
2809/2809 [==============================] - 18s 6ms/step - loss: 0.1988 - accuracy: 0.9366 - val_loss: 0.2010 - val_accuracy: 0.9357
Epoch 9/20
2809/2809 [==============================] - 15s 5ms/step - loss: 0.1987 - accuracy: 0.9366 - val_loss: 0.2011 - val_accuracy: 0.9356

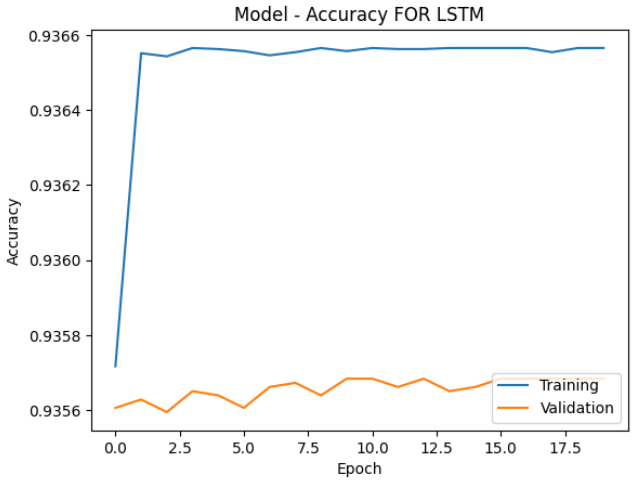


Figure 6: Accuracy for both training and validation

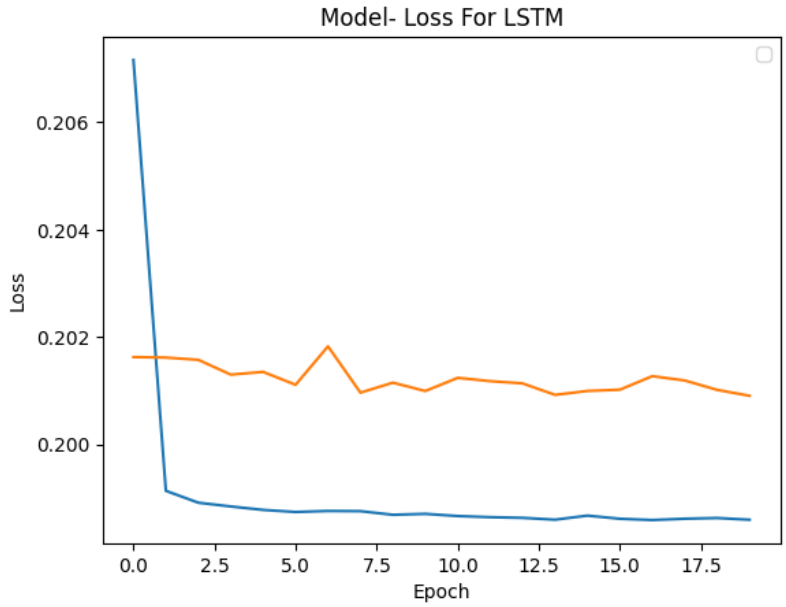


Figure 7: loss for both training and validation

Classification_Report For LSTM

	precision	recall	f1-score	support
Normal	1.00	0.87	0.93	44833
DDoS	0.89	1.00	0.94	45051
accuracy			0.94	89884
macro avg	0.94	0.94	0.94	89884
weighted avg	0.94	0.94	0.94	89884

Figure 8: Classification Report of The LSTM Model

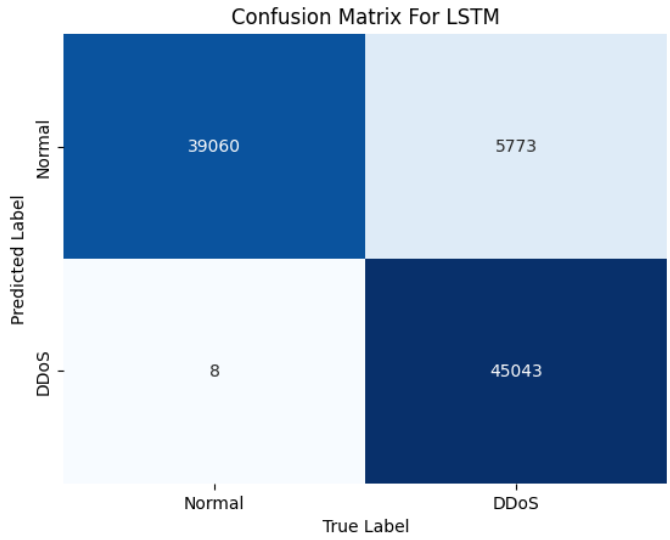


Figure 9: Confusion Matrix of The LSTM Model

4.3 Implementation of the CNN-ANN using the weight of the LSTM Mode

The application of transfer learning for Denial of Service (DoS) attacks involves utilising a pretrained Long Short-Term Memory (LSTM) model as a feature extractor to capture temporal dependencies in the input data. The LSTM model design comprises two LSTM layers, followed by a dense layer employing softmax activation for

classification. The weights of the pretrained LSTM model are imported from a preexisting file. A CNN-ANN model was subsequently constructed, utilising input from the pretrained LSTM model along with additional data inputs. The CNN-ANN model consists of a convolutional layer, a max-pooling layer, and a dense layer. The features derived from the LSTM model and the CNN-ANN model are amalgamated and processed through a classification layer, which comprises a dense layer utilising sigmoid activation. The transfer learning model is developed using the Adam optimiser and the categorical crossentropy loss function. The model is subsequently trained on the training data with a batch size of 32 for 10 epochs. The model employs LSTM alongside supplementary input data to effectively identify DoS assaults. The outcomes of the transfer learning model's training are presented in Table 3. The LSTM model was assessed by accuracy, loss, classification report, and confusion matrix. These are illustrated in Figures 10, 11, 12, and 13.

Table 3: Training Result of the transfer Learning model on the second dataset

```
Epoch 1/10
2534/2534 [==============================] - 23s 6ms/step - loss: 0.0961 - accuracy: 0.9628 - val_lo
ss: 0.0457 - val_accuracy: 0.9829
Epoch 2/10
2534/2534 [==============================] - 15s 6ms/step - loss: 0.0398 - accuracy: 0.9851 - val_lo
ss: 0.0303 - val_accuracy: 0.9892
Epoch 3/10
2534/2534 [==============================] - 16s 6ms/step - loss: 0.0282 - accuracy: 0.9894 - val_lo
ss: 0.0308 - val_accuracy: 0.9879
Epoch 4/10
2534/2534 [==============================] - 17s 7ms/step - loss: 0.0207 - accuracy: 0.9920 - val_lo
ss: 0.0138 - val_accuracy: 0.9950
Epoch 5/10
2534/2534 [==============================] - 15s 6ms/step - loss: 0.0178 - accuracy: 0.9928 - val_lo
ss: 0.0137 - val_accuracy: 0.9947
Epoch 6/10
2534/2534 [==============================] - 13s 5ms/step - loss: 0.0139 - accuracy: 0.9945 - val_lo
ss: 0.0233 - val_accuracy: 0.9904
Epoch 7/10
2534/2534 [==============================] - 14s 6ms/step - loss: 0.0124 - accuracy: 0.9953 - val_lo
ss: 0.0100 - val_accuracy: 0.9960
Epoch 8/10
2534/2534 [==============================] - 13s 5ms/step - loss: 0.0105 - accuracy: 0.9962 - val_lo
ss: 0.0099 - val_accuracy: 0.9968
Epoch 9/10
2534/2534 [==============================] - 13s 5ms/step - loss: 0.0096 - accuracy: 0.9963 - val_lo
ss: 0.0160 - val_accuracy: 0.9930
Epoch 10/10
2534/2534 [==============================] - 15s 6ms/step - loss: 0.0089 - accuracy: 0.9968 - val_lo
ss: 0.0059 - val_accuracy: 0.9979
```

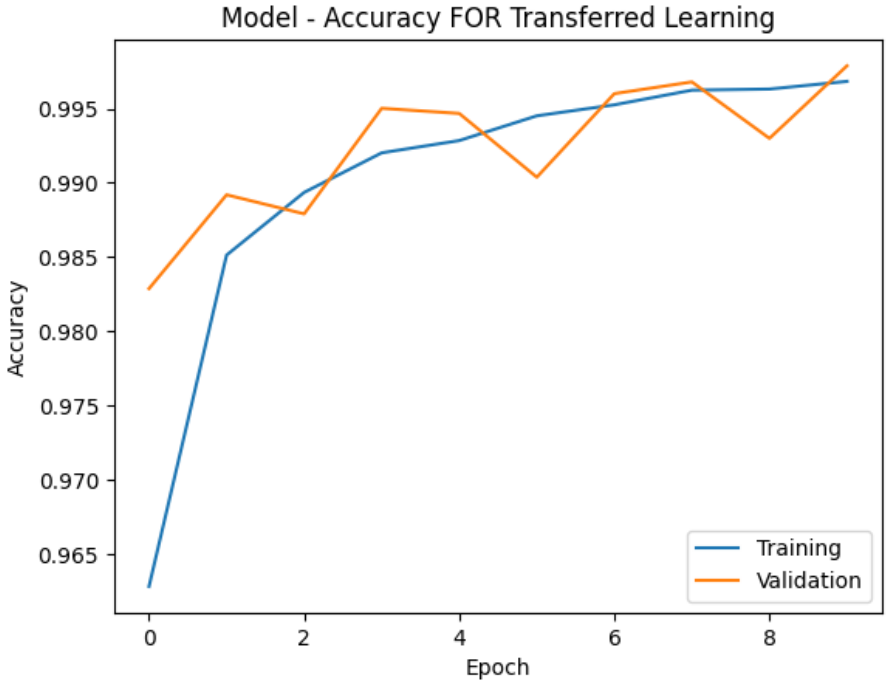


Figure 10: Accuracy for both training and validation

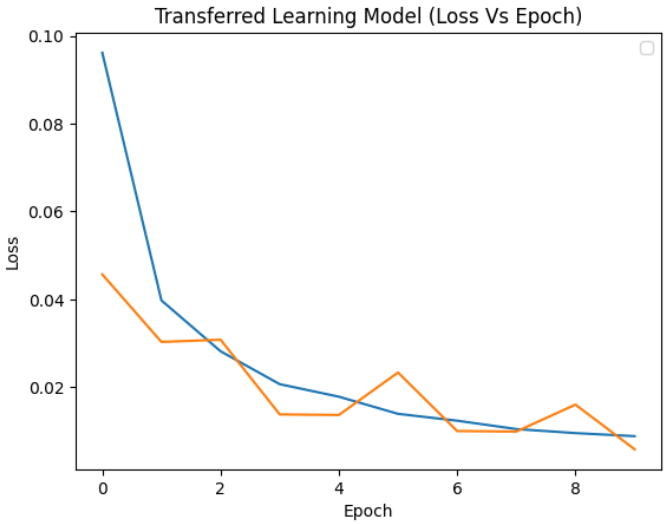


Figure 11: Model Loss for both training and validation

Classification_Report For Transfer Learning Model

	precision	recall	f1-score	support
Normal	1.00	1.00	1.00	12688
DDoS	1.00	1.00	1.00	12646
accuracy			1.00	25334
macro avg	1.00	1.00	1.00	25334
weighted avg	1.00	1.00	1.00	25334

Figure 12: Classification Report

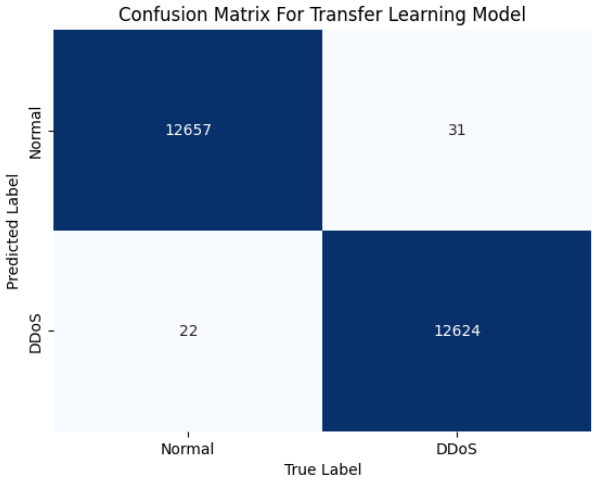


Figure 13: Confusion Matri

V. Simulation Testing

The final model was deployed to web for continuous detection of DDoS attacks. A simulation was carried out to replicate the packets that flows into the network system. The model filters the packets and categorizes the packets into normal packets and further types of DDoS attacks. Figure 14, and 15.

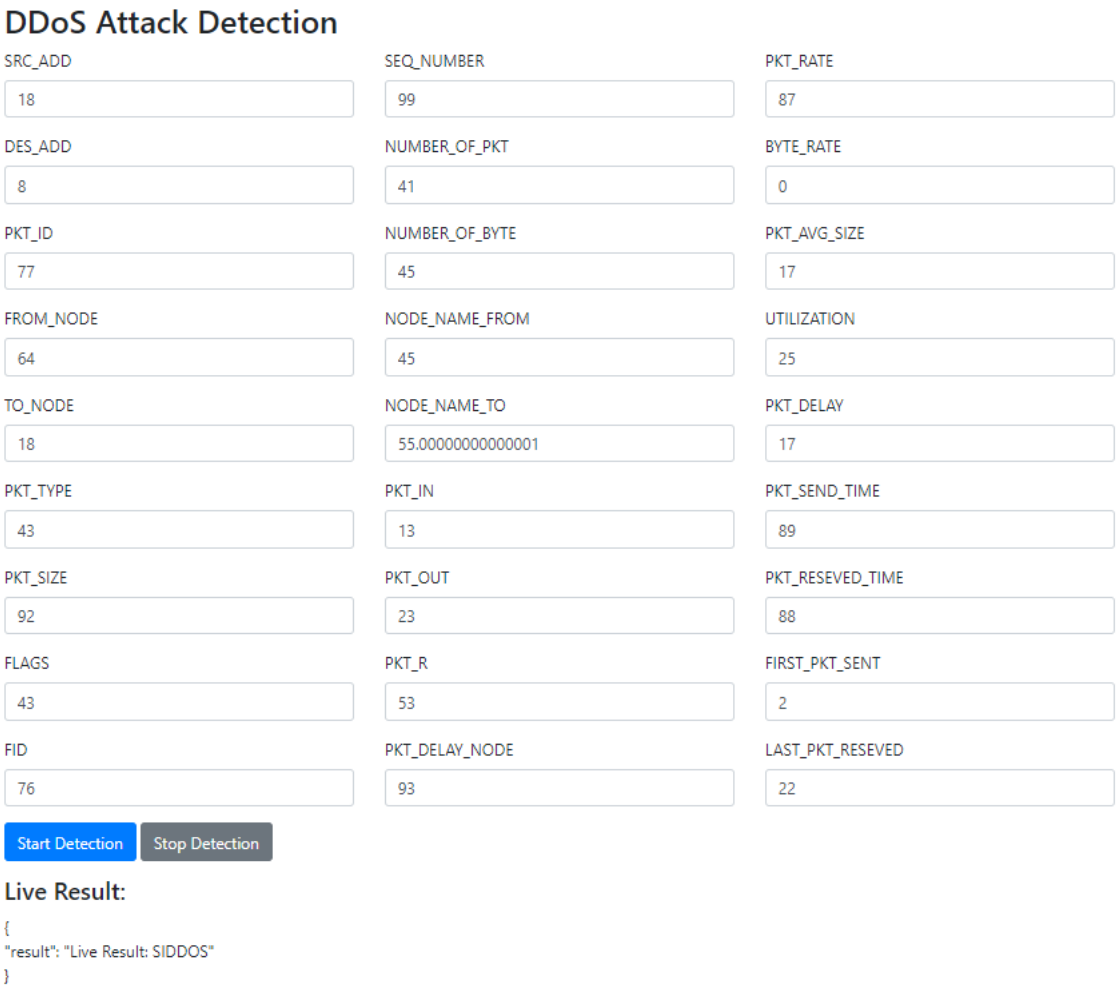


Figure 14: SIDDOS attack detected.

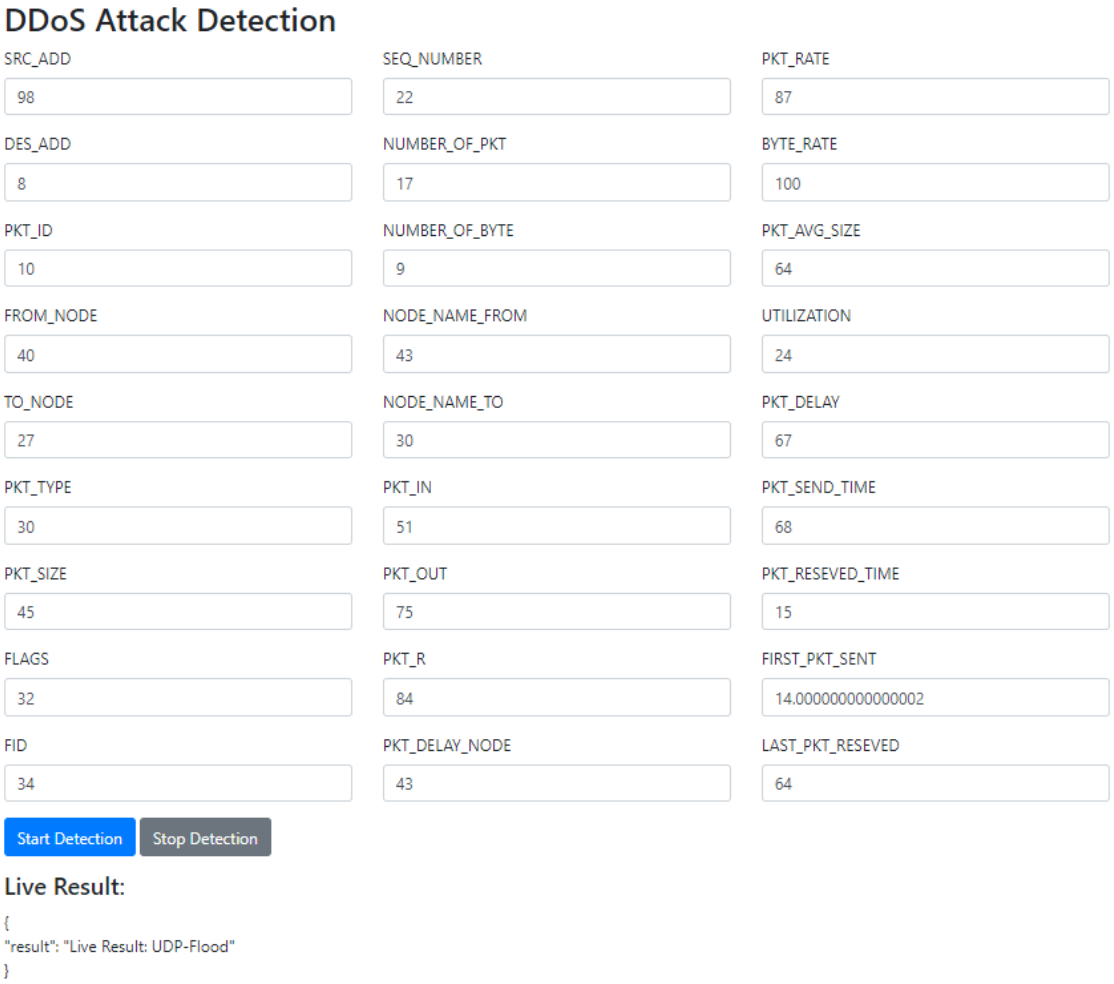


Figure 15: UDP-Flood DDoS attack detected.

VI. Conclusion

The application of the LSTM model on the original dataset, consisting of 28 features and 2,160,667 instances, has demonstrated promising results in detecting Denial of Service (DoS) attacks. The LSTM model architecture, comprising two LSTM layers and a Dense layer, achieved optimal performance during the fourth training session utilising TensorFlow's Keras API. The model has robust performance, achieving an accuracy of 93.66% in training and 93.57% in validation, accompanied with moderate loss values. The model's efficacy is additionally demonstrated by graphical representations of accuracy and loss. Additionally, the classification report and confusion matrix provide critical insights into the model's precision, recall, and overall effectiveness in accurately classifying network traffic as either "Normal" or "DdoS".

Furthermore, the application of transfer learning for DoS attacks entails employing a pretrained LSTM model as a feature extractor, succeeded by a CNN-ANN model. This method yields remarkable results on the second dataset. The transfer learning model achieved a training accuracy of 99.68% and a validation accuracy of 99.79%, accompanied by negligible loss values. The classification report exhibits exceptional precision, recall, and F1-score metrics for both the "Normal" and "DdoS" classes, indicating the model's excellent accuracy in categorising network traffic incidents. Furthermore, the confusion matrix delineates the precise predictions executed by the model for each class, offering additional validation of its dependability.

REFERENCES

[1] J. Almaraz-Rivera, "Enhancing iot network security: unveiling the power of self-supervised learning against ddos attacks", Sensors, vol. 23, no. 21, p. 8701, 2023. https://doi.org/10.3390/s23218701
[2] K. Wang, J. Li, & W. Wu, "An efficient intrusion detection method based on federated transfer learning and an extreme learning machine with privacy preservation", Security and Communication Networks, vol. 2022, p. 1-13, 2022. https://doi.org/10.1155/2022/2913293
[3] S. Mehedi, "Dependable intrusion detection system for iot: a deep transfer learning-based approach",, 2022. https://doi.org/10.48550/arxiv.2204.04837
[4] X. Sun, W. Meng, W. Chiu, & B. Lampe, "Tdl-ids: towards a transfer deep learning based intrusion detection system",, 2022. https://doi.org/10.1109/globecom48099.2022.10001267

[5] M. Xu, X. Li, Y. Wang, B. Luo, & J. Guo, "Privacy-preserving multisource transfer learning in intrusion detection system", Transactions on Emerging Telecommunications Technologies, vol. 32, no. 5, 2020. https://doi.org/10.1002/ett.3957
[6] S. Garg, K. Kaur, G. Kaddoum, P. Garigipati, & G. Aujla, "Security in iot-driven mobile edge computing: new paradigms, challenges, and opportunities", Ieee Network, vol. 35, no. 5, p. 298-305, 2021. https://doi.org/10.1109/mnet.211.2000526
[7] O. Ajayi and A. Gangopadhyay, "Dahid: domain adaptive host-based intrusion detection",, 2021. https://doi.org/10.1109/csr51186.2021.9527966
[8] H. Wang and P. Liu, "Tackling imbalanced data in cybersecurity with transfer learning: a case with rop payload detection",, 2021. https://doi.org/10.48550/arxiv.2105.02996
[9] Y. Ganin, E. Ustinova, H. Ajakan, P. Germain, H. Larochelle, F. Lavioletteet al., "Domain-adversarial training of neural networks",, p. 189-209, 2017. https://doi.org/10.1007/978-3-319-58347-1_10
[10] M. Musa, "A framework for the detection of distributed denial of service attacks on network logs using ml and dl classifiers", Scientia Africana, vol. 22, no. 3, p. 153-164, 2024. https://doi.org/10.4314/sa.v22i3.14
[11] A. Churcher, R. Ullah, J. Ahmad, S. Rehman, F. Masood, M. Gogateet al., "An experimental analysis of attack classification using machine learning in iot networks", Sensors, vol. 21, no. 2, p. 446, 2021. https://doi.org/10.3390/s21020446
[12] L. Bagdadi, "Distributed denial of service attacks classification system using features selection and ensemble techniques", Indonesian Journal of Electrical Engineering and Computer Science, vol. 34, no. 3, p. 1868, 2024. https://doi.org/10.11591/ijeecs.v34.i3.pp1868-1878
[13] S. Qasim, "Advancements in time series-based detection systems for distributed denial-of-service (ddos) attacks: a comprehensive review", BJN, vol. 2024, p. 9-17, 2024. https://doi.org/10.58496/bjn/2024/002
[14] Y. Wu, "Ddos attack detection method based on machine learning", Applied and Computational Engineering, vol. 18, no. 1, p. 88-95, 2023. https://doi.org/10.54254/2755-2721/18/20230968
[15] D. Sharma, "A review paper on ddos detection using machine learning", Asian Journal of Convergence in Technology, vol. 9, no. 2, p. 75-78, 2023. https://doi.org/10.33130/ajct.2023v09i02.013
[16] F. Talpur, "Ml-based detection of ddos attacks using evolutionary algo-rithms optimization",, 2024. https://doi.org/10.20944/preprints202401.1099.v1
[17] B. Alabsi, M. Anbar, & S. Rihan, "Conditional tabular generative adversarial based intrusion detection system for detecting ddos and dos attacks on the internet of things networks", Sensors, vol. 23, no. 12, p. 5644, 2023. https://doi.org/10.3390/s23125644
[18] B. Goparaju and B. Rao, "A ddos attack detection using pca dimensionality reduction and support vector machine", International Journal of Communication Networks and Information Security (Ijcnis), vol. 14, no. 1s, p. 01-08, 2023. https://doi.org/10.17762/ijcnis.v14i1s.5586
[19] K. Dasari and N. Devarakonda, "Detection of ddos attacks using machine learning classification algorithms", International Journal of Computer Network and Information Security, vol. 14, no. 6, p. 89-97, 2022. https://doi.org/10.5815/ijcnis.2022.06.07
[20] A. Silivery, R. Kovvur, & L. Kumar, "An effective deep learning based multi-class classification of dos and ddos attack detection", International Journal of Electrical and Computer Engineering Systems, vol. 14, no. 4, p. 421-431, 2023. https://doi.org/10.32985/ijeces.14.4.6
[21] P. John and R. Nagappasetty, "An intelligent system to detect slow denial of service attacks in software-defined networks", International Journal of Electrical and Computer Engineering (Ijece), vol. 13, no. 3, p. 3099, 2023. https://doi.org/10.11591/ijece.v13i3.pp3099-3110