Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Enhanced Detection of DDoS Attacks through Deep Neural Networks and Machine Learning Techniques

Savita Devi, Taran Singh Bharti

Dept. of Computer Science, Jamia Millia Islamia University, Delhi- India
Email: savita4992dahiya@gmail.com

DDoS attacks represent a significant threat to cybersecurity, inflicting significant damage on individuals and organizations alike. These attacks compromise network performance, deplete system resources, and disrupt service availability. To mitigate this risk, this study employs supervised learning algorithms to distinguish between legitimate and malicious network traffic. Leveraging the CIC-DDoS2019 and DDoS SDN datasets, the research evaluates the performance of Deep Neural Networks (DNN), XGBoost (Extreme Gradient Boosting), Restricted Boltzmann Machine with Supervised Fine-tuning (RBM_SVF), Naive Bayes, K-Nearest Neighbors (KNN), Decision Tree, SGD (Stochastic Gradient Descent), Quadratic classifiers and Logistic Regression. The dataset was divided, with 75% designated for training and 25% reserved for testing. To improve model performance, feature scaling was performed using the StandardScaler. Among the tested algorithms, The Deep Neural Networks (DNN) algorithm demonstrated superior accuracy 99.6 % in identifying DDoS attacks in comparison to XGBoost (98.3%), RBM_SVF (97.2%) and KNN (96.5%). The results indicate that Deep Neural Networks (DNN) proved to be the most effective model for detecting DDoS attacks in this experimental setup.

Keywords: Supervised learning, DDoS attack, KNN, Logistic Regression.

1. Introduction

DDoS attacks happen when a target's service is overwhelmed and disrupted by a massive influx of traffic originating from multiple sources. These attacks pose a significant risk to the Global network. Cybercriminals use DDoS attacks as formidable tools, overwhelming the target's network with a massive influx of packets. This depletes resources, hinders service performance, and blocks legitimate ussers from gaining access. As the number of internet users continues to rise, the frequency of these attacks has escalated, leading to significant financial losses. DDoS attacks, which leverage IP spoofing to hinder request processing and interfere

with normal operations for legitimate users, are the most prevalent type of distributed network attack. Applications based on web and e-commerce sites often become prime targets, serving various malicious purposes. The limitations of traditional networking devices contribute to the occurrence of DDoS attacks. The constantly expanding range of tools and techniques has turned DDoS attacks into one of the biggest challenges for recognition and verification. To effectively counter DDoS attacks, it is essential to establish a thorough security framework, implement intrusion detection systems, and use firewalls [1].

In a typical DDoS attack scenario, a malicious actor overwhelms a victim server with a flood of traffic originating from a botnet, leading to network interruptions. The proliferation of digital platforms for activities such as online shopping, banking, and data exchange has accelerated the shift from physical to digital realms, driven by technological advancements [2-5]. DDoS attacks represent a serious risk to cybersecurity, capable of inflicting substantial damage on individuals and organizations. These attacks overwhelm target systems with excessive traffic, leading to network congestion, resource exhaustion, and service disruptions. To address this critical issue, this research suggests a supervised machine structure as a defense mechanism.

2. Literature Review and Analysis

A range of research studies focused on the detection and classification of DDoS attacks is reviewed in this section. To reduce the effects of these attacks, researchers have designed an algorithmic system derived from C4.5 decision trees, which, when combined with signature-based detection, effectively identifies DDoS attack patterns. Further studies have explored the application of additional machine learning approaches, including recurrent deep neural networks, demonstrating superior performance compared to traditional methods. For instance, one study reported a significant reduction in error rate from 7.517% to 2.103% when using deep learning on a larger dataset [12]. This research explores several innovative approaches to combating DDoS attacks. ArOMA is an autonomous DDoS defense system that leverages the programmability and centralized control of Software-Defined Networking (SDN) to facilitate traffic monitoring, detect anomalies, and implement mitigation measures automatically. Security functions are distributed across the network, ArOMA enables Internet Service Providers (ISPs) to effectively manage DDoS traffic while prioritizing customer needs.

Experimental results demonstrate ArOMA's ability to maintain video stream quality during DDoS attacks [13]. A separate study examines the Mirai botnet, analyzing its rapid expansion, victim profiles, and evolution over a seven-month period. The research highlights the vulnerabilities within the IoT ecosystem and proposes potential mitigation strategies. DBod is an innovative system designed to detect botnets based on Domain Generation Algorithms (DGA) by analyzing DNS query behavior. By exploiting the consistent querying patterns of infected hosts, DBod effectively identifies both known and unknown DGA-based botnets[14]. Finally, the concept of Zombie Coin introduces a Bitcoin-based botnet command-and-control infrastructure. This approach offers increased resilience to takedown efforts and regulatory actions by leveraging the Bitcoin network's decentralized nature and advanced features. The authors anticipate a growing trend towards Bitcoin-based command-and-control systems among botnet operators. This research aims to facilitate the development of effective

countermeasures against this emerging threat[15]. These studies collectively contribute to the advancement of DDoS defense strategies by exploring novel approaches and demonstrating their effectiveness in mitigating these complex attacks.

3. Design and Implementation of the Proposed Model

This study seeks to create a machine learning technique for the classification and prediction of DDoS attacks. The proposed framework encompasses several key stages: dataset selection, data preprocessing, feature scaling, data visualization, data splitting, model building, and model evaluation. To discriminate between DDoS attacks and benign network traffic, the framework employs Logistic Regression, K-Nearest Neighbors and Random Forest methods [3]. This study employs a dataset comprising a subset of CIC-DDoS2019 and DDoS SDN. These datasets are widely used in network security research for intrusion detection and traffic analysis. The resulting dataset contains 500,000 instances with seven attributes, including Timestamp, Mean Forward Packet Length, Average Forward Segment Size, Initial Forward Window Bytes, Forward Segment Size, and a label denoting the presence of a DDoS attack. The dataset exhibits an 80:20 ratio of benign to DDoS traffic [4]. The raw network traffic data was subjected to a preprocessing phase to convert it into a suitable format for machine learning analysis [5]. The dataset was assessed for any missing values. The missing no library was utilized to evaluate the dataset for missing values. The visualization confirms the absence of missing data points. The dataset was chronologically ordered based on the Timestamp attribute. To ensure that features contribute equally to the machine learning model, feature scaling was applied using Min-Max normalization [6]. To facilitate data exploration and understanding, visual representations were generated using the Seaborn library. A heatmap was created to visualize correlations between attributes. Heatmaps employ color gradients to represent relationships between variables. Heatmap depicts the correlation matrix, where color intensity represents the strength of the correlation between each pair of attributes. A strong positive correlation is indicated by warm colors, whereas a weak or negative correlation is represented by cool colors. Distribution Plot illustrates the distribution of data points for each class (DDoS and Benign) in the dataset. It reveals that the dataset is imbalanced, with 80% of the traffic being benign and 20% being DDoS attacks. Pie Chart provides a visual representation of the class distribution within the dataset, confirming the 80:20 ratio of benign to DDoS traffic [7].

3.1. Handling Class Disparity

The dataset exhibits a significant class imbalance, with DDoS instances constituting only 20% of the data. To mitigate the potential bias introduced by this imbalance and enhance model performance, a down sampling method was implemented. Down sampling involves reducing the number of instances in the majority class (benign traffic) to achieve a more balanced class distribution. This approach aims to enhance the model's effectiveness to accurately classify the minority class (DDoS attacks) while maintaining overall performance [8]. The dataset was partitioned into independent and dependent variables, with the latter representing the target class (DDoS or benign). To support model training and assessment, the dataset was split into training (80%) and testing (20%) subsets.

Nine machine learning algorithms - Deep Neural Networks (DNN), XGBoost (Extreme Gradient Boosting), Restricted Boltzmann Machine with Logistic Regression, Supervised Fine-tuning (RBM_SVF), Naive Bayes , K-Nearest Neighbors (KNN), Decision Tree, Stochastic Gradient Descent (SGD) and Quadratic classifiers were employed for classification [9].

4. Experimental Results and Interpretation

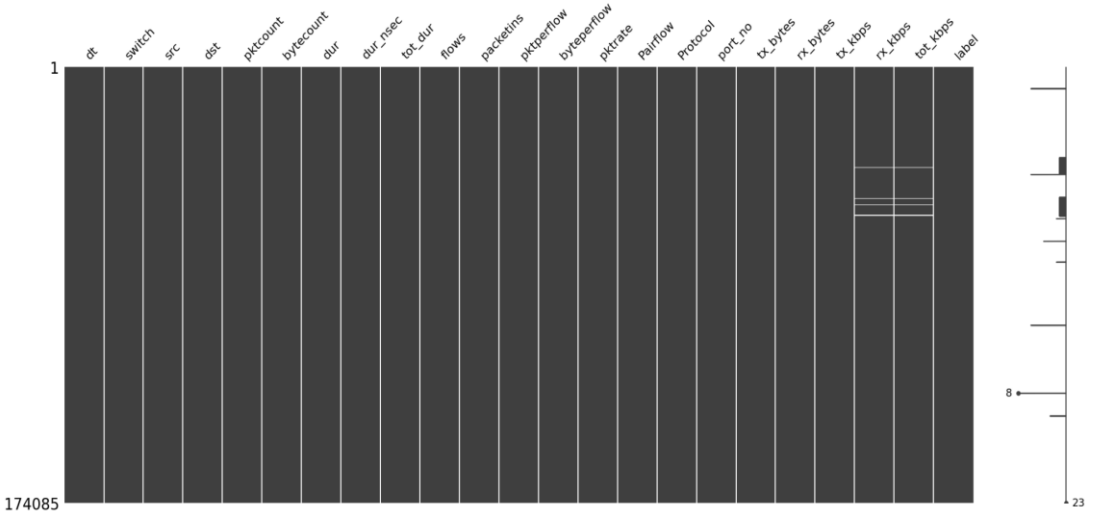

Fig 1: Heatmap of missing values

Figure 1 presents a heatmap illustrating the distribution of missing values across various features in the dataset, which consists of 174,085 entries. Each column represents a specific feature, while each row corresponds to an individual entry. The majority of the features (columns) exhibit no missing values, as indicated by the consistent dark shading across these columns[19].

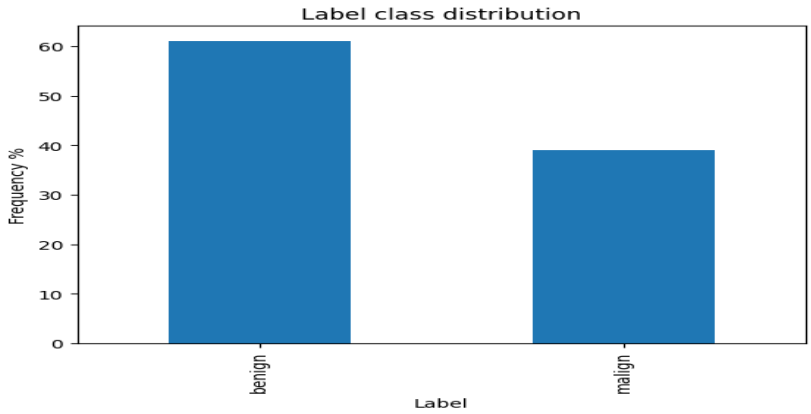

Fig.2: Label class distribution

Figure 2 presents the distribution of the two classes within the dataset: benign and malign. The bar chart shows that the benign class constitutes approximately 60% of the dataset, while the malign class makes up about 40%. Benign: The benign class is represented by the taller bar, indicating that it occurs more frequently within the dataset. Malign: The malign class, represented by the shorter bar, occurs less frequently than the benign class [20].

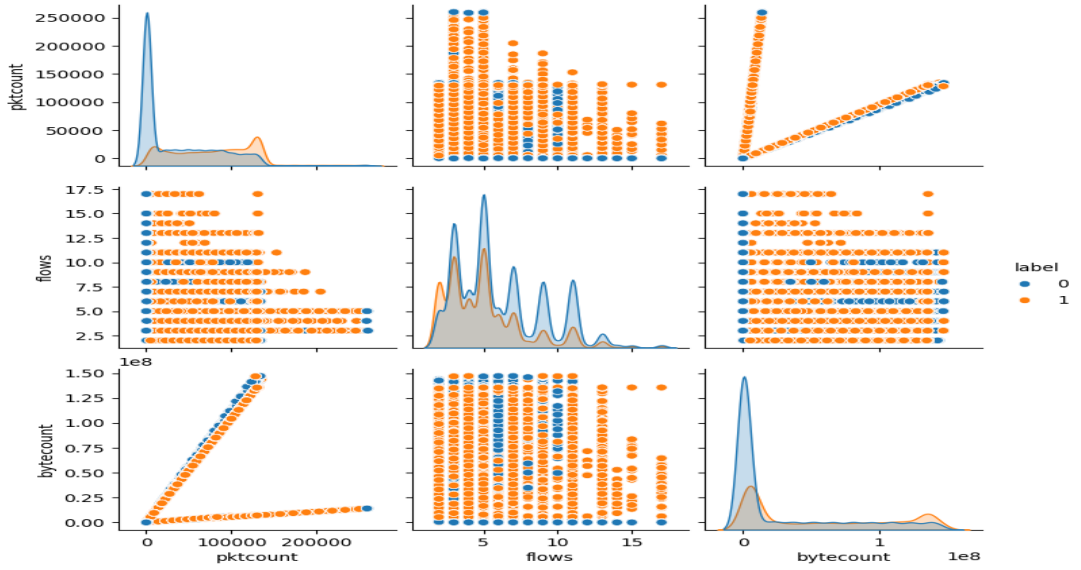

Fig 3. Pairplot of selected features

Figure 3 displays a pair plot of the selected features, where the features on the x-axis are plotted against those on the y-axis, and the color of each point reflects the value of a third feature.

For example, the top left plot shows the relationship between pktcount and bytecount, where the color of each point represents the value of the flow feature. The labels on the axes of the plots are difficult to read in the image you sent, but they appear to be pktcount, bytecount, and flows. These features are likely associated with network traffic, including the packet count, the total bytes transferred, and the number of flows.

The caption below the figure says "250000", "200000", ..., "0" on the left and "17.5", "15.0", ..., "0.00" on the bottom. Overall, the pair plot in the figure is showing the relationships between features that are relevant to predicting DDoS attacks in building management systems [21].

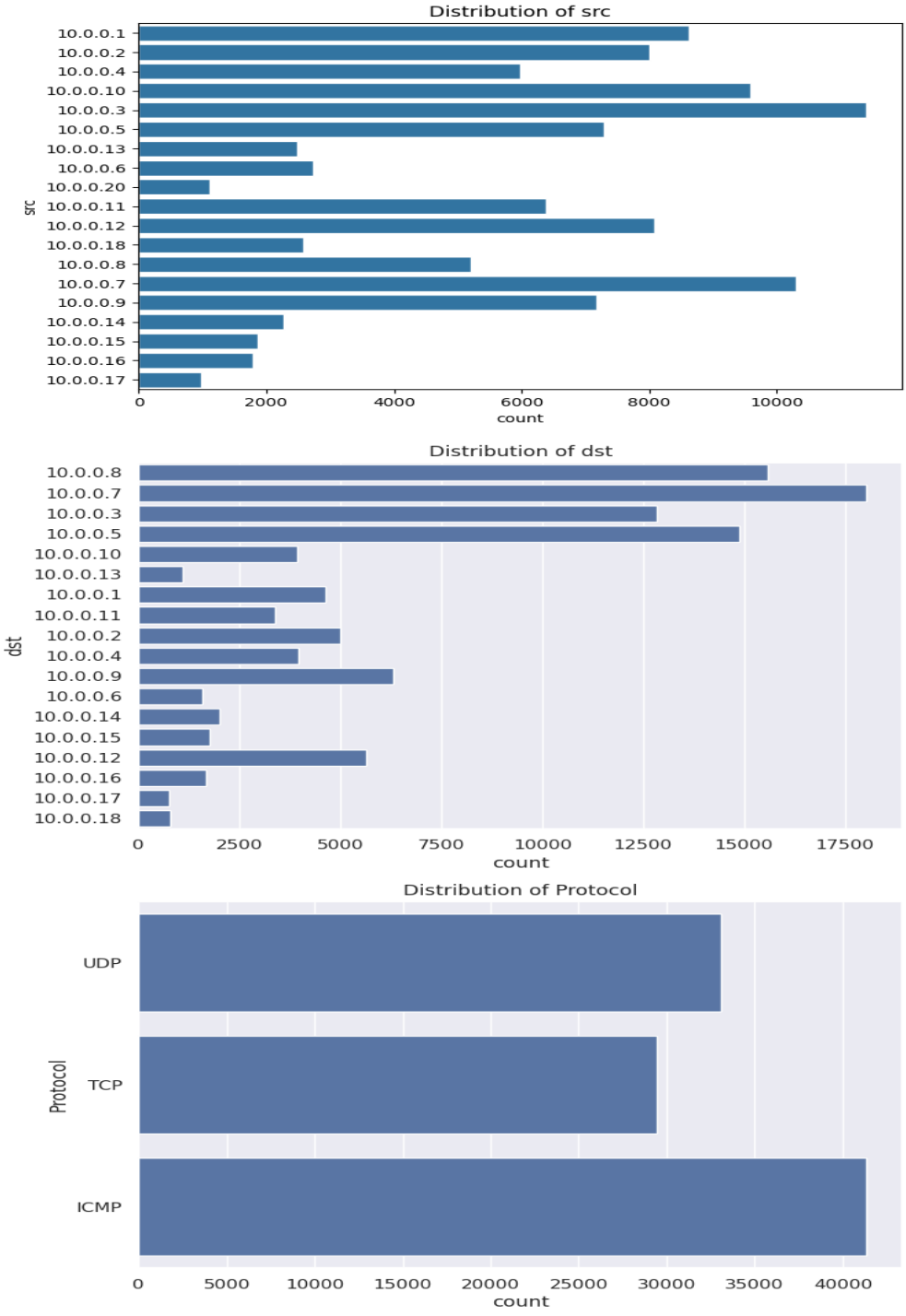

Fig.4 Distribution of Categorical features

Figure 4 illustrates the distribution of categorical features in the dataset. Understanding the

distribution of these features is essential for preprocessing and feature engineering in machine learning tasks. Categories: Commonly includes values like TCP, UDP, ICMP. Distribution: Shows the proportion of each protocol type within the dataset. For example, TCP might be the most frequent protocol, followed by UDP and ICMP [22].

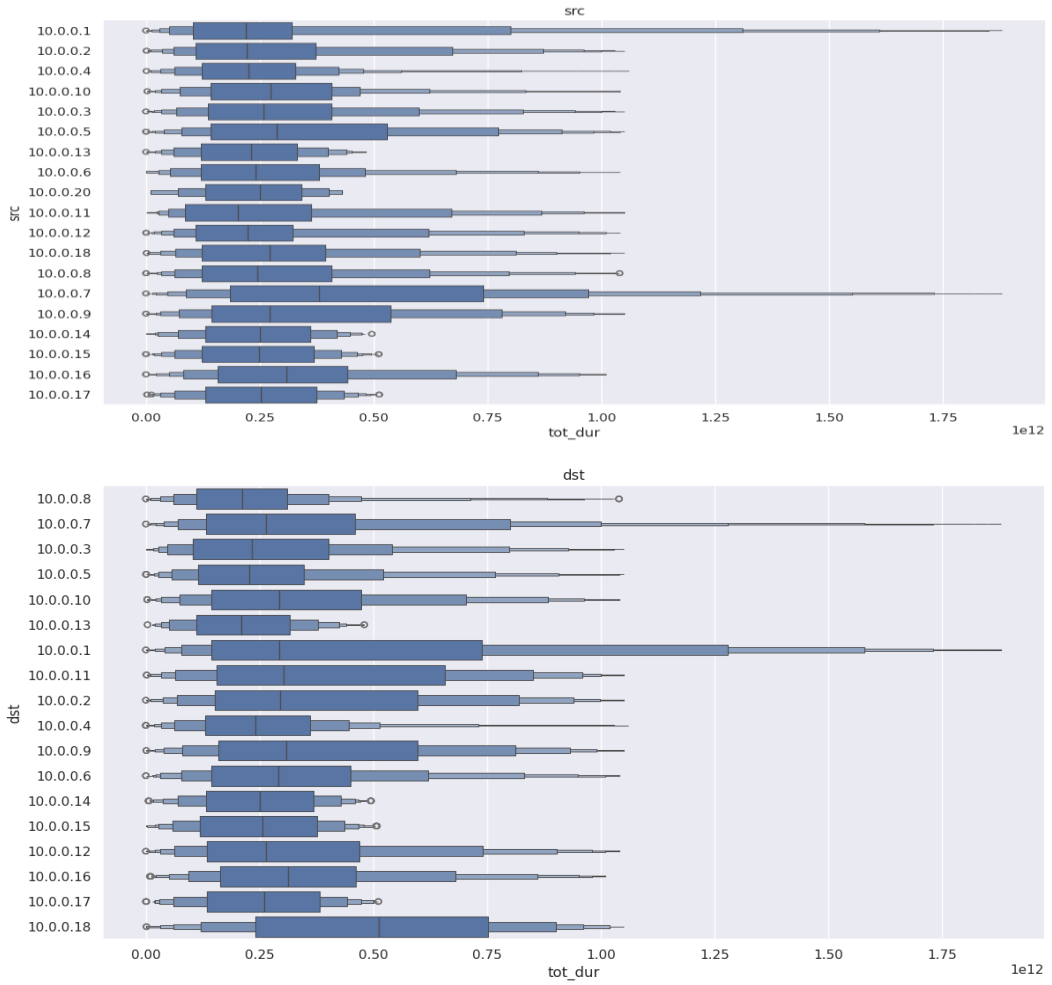

Fig. 5: quartiles of categorical features w.r.t total duration

Figure 5 provides an analysis of the quartiles of various categorical features concerning the total duration. This visualization helps to understand how different categories of each feature distribute over the total duration of events or records in the dataset.

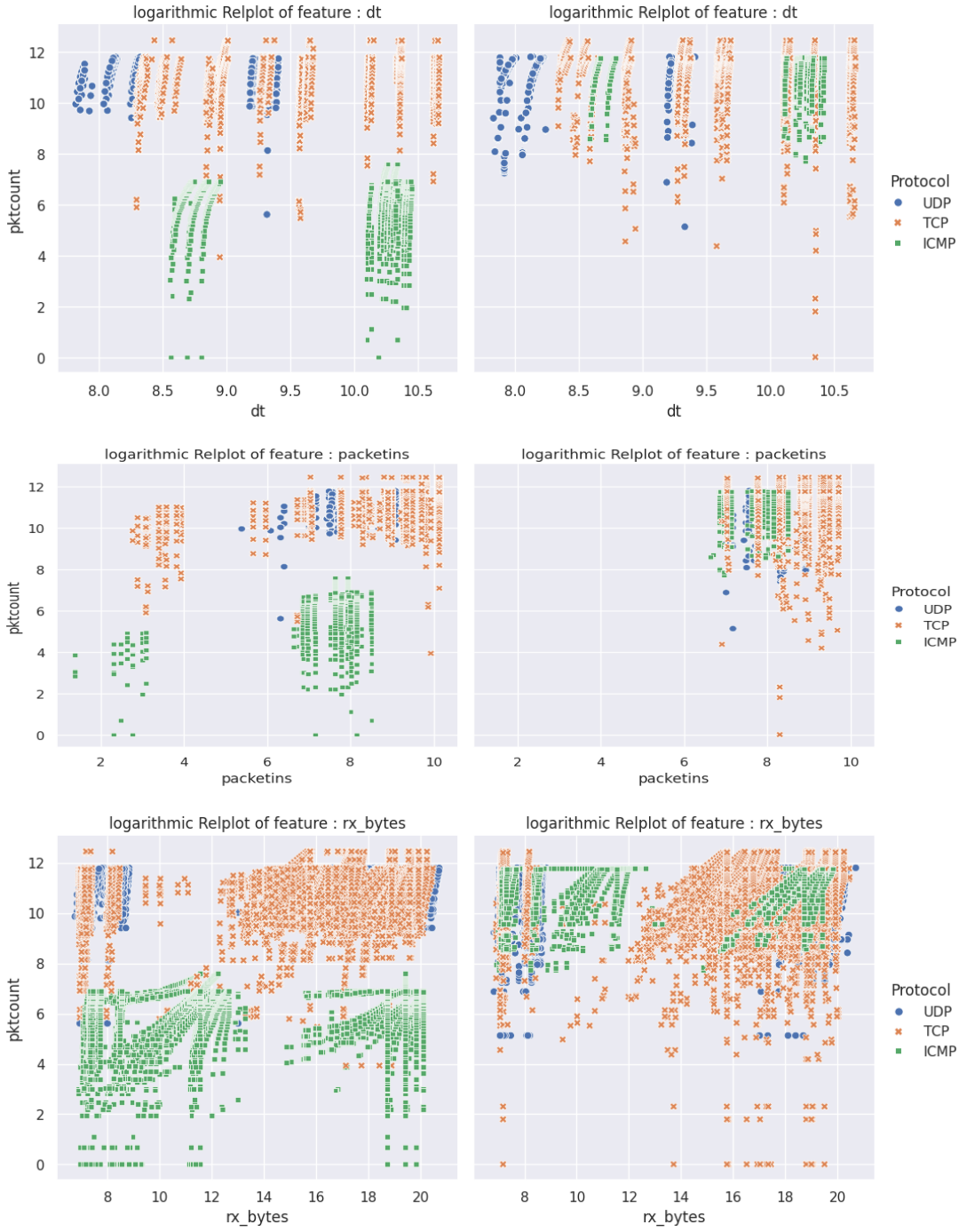

Fig. 6: Distribution of features w.r.t packet count, protocol and type of attack

Figure 6 presents a comprehensive analysis of the distribution of various features in the dataset, focusing on how these distributions vary concerning packet count, protocol, and type of attack.

This detailed visualization helps to understand the interplay between these features and their relevance in identifying different types of network attacks [24].

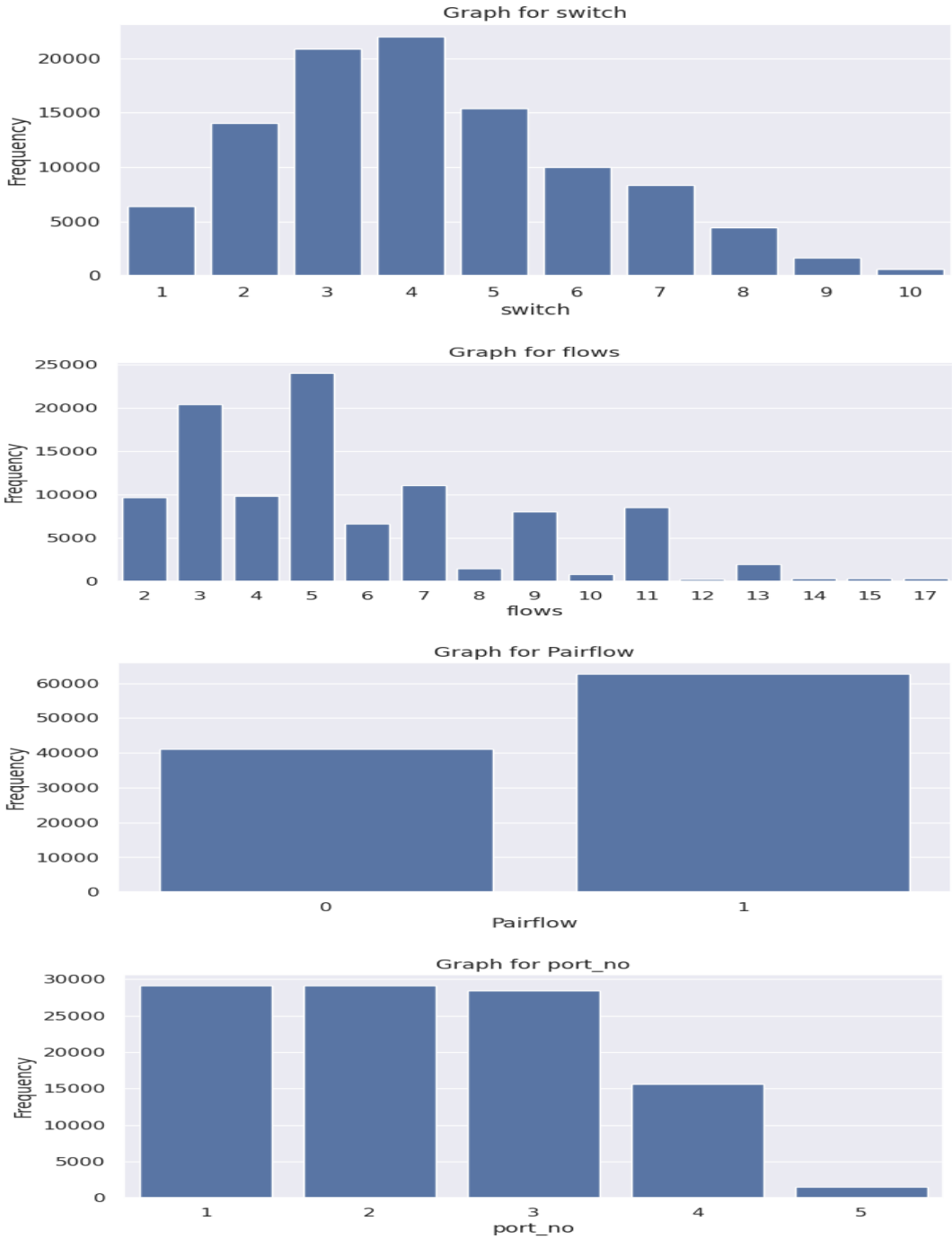

Fig. 7: Distribution of numerical discrete features

Figure 7 provides a detailed visualization of the distribution of numerical discrete features within the dataset. Understanding these distributions is essential for data analysis, preprocessing, and feature engineering in machine learning tasks. Numerical Discrete Features: The figure analyzes several numerical discrete features, showcasing their distribution through histograms. Visual Representation: Each subplot represents the distribution of a specific numerical discrete feature, illustrating the frequency of data points across different values. In conclusion, Figure 8 effectively illustrates the distribution of numerical discrete features within the dataset, providing valuable insights into their central tendency, spread, and shape.This knowledge is essential for making well-informed choices during data preprocessing, feature engineering, and model selection, which ultimately leads to the creation of more strong and dependable machine learning models [25].

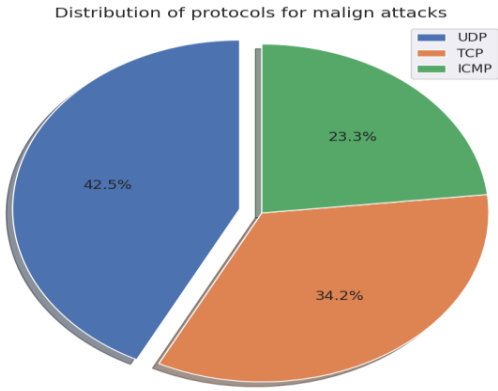

Fig 8: Distribution of Malign attacks

The distribution of malign attacks as shown in Figure 8 provides crucial insights into their frequency and patterns across different categories. Recognizing these patterns can aid in identifying high-risk areas, optimizing resource allocation, and creating targeted interventions to reduce the effects of malicious attacks.

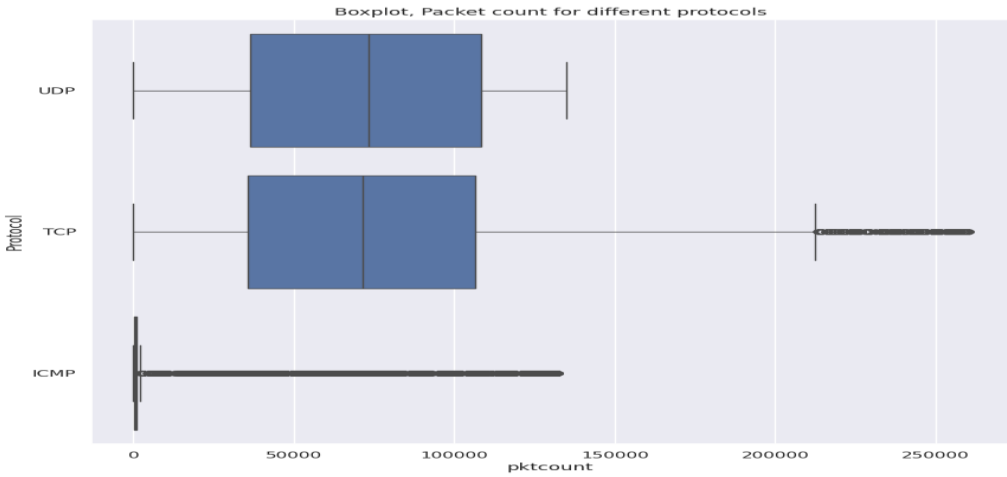

Fig 9: Packet count for different protocols

Figure 9 presents the distribution of packet counts across various network protocols, offering a quantitative assessment of network traffic for each protocol type. The figure aims to depict how different protocols contribute to the total network traffic and highlights their relative usage or importance.

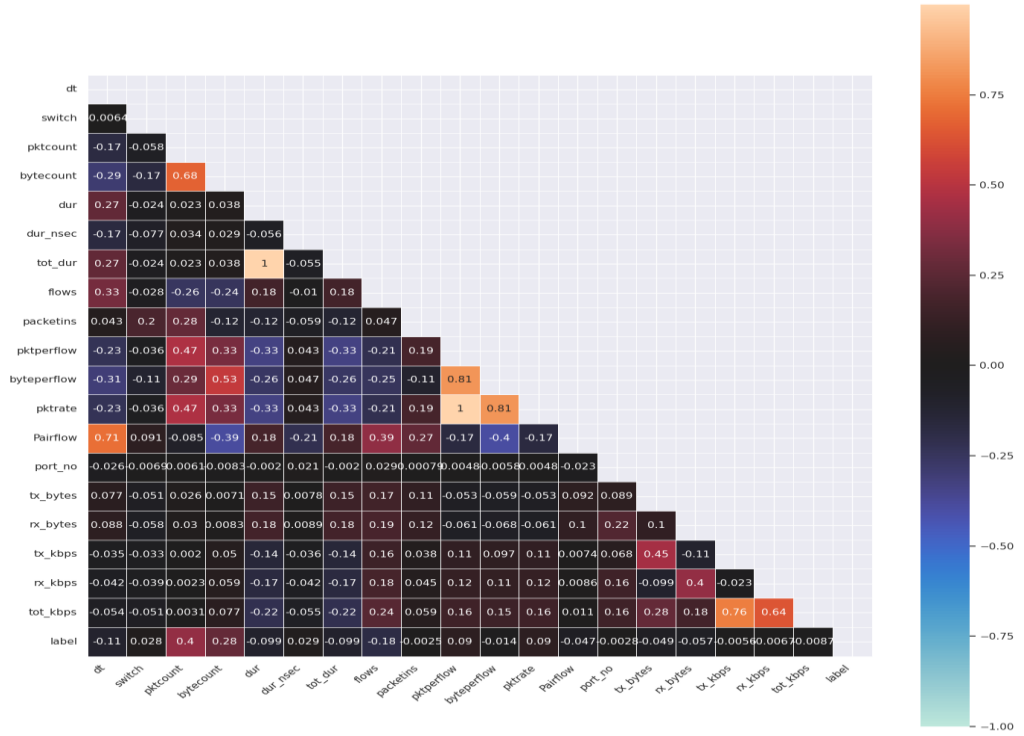

Fig 10: Heatmap of the correlation features

Figure 10 shows the heatmap which visualizes the correlation matrix for various network traffic features. The features are listed both along the left side and across the top of the matrix. Color intensity represents the strength of correlation: blue for positive, red for negative, and white for no correlation. The values within the squares show the correlation coefficients between pairs of features. For example, the correlation between "switch" and "ktcount" is 0.0064, while the correlation between "tot_dur" and "flows" is 0.33. Diagonal values are 1, indicating perfect correlation between a feature and itself. This visualization highlights how certain features move together, either positively or negatively.

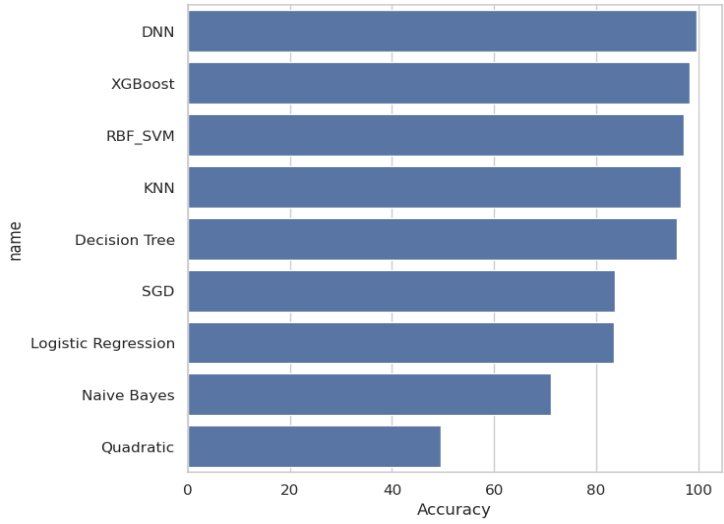

Fig 11: Accuracy comparison of the Models applied.

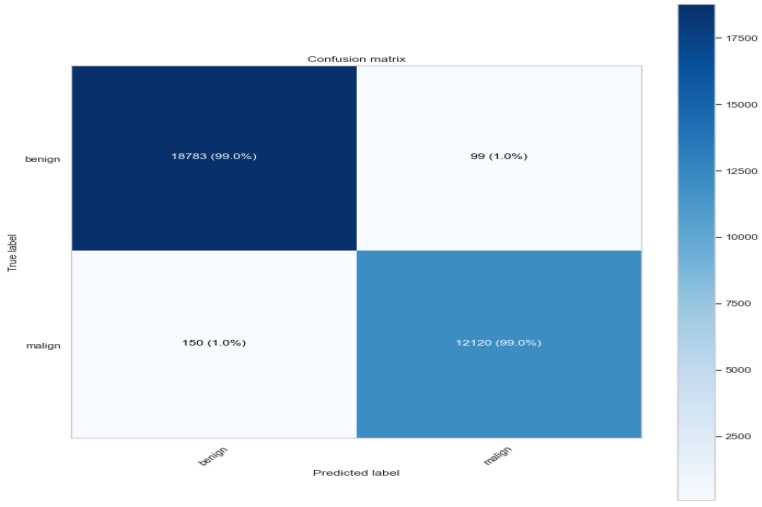

Fig. 12. Confusion matrix of Deep Neural Network

Figure 12 displays the confusion matrix for the Deep Neural Network. A confusion matrix is utilized to assess the performance of a classification model, such as a deep neural network, on a set of test data with known true labels. The rows indicate the actual labels of the data. In this case, it shows two classes: benign and malignant. Columns represent the labels predicted by the DNN model. Values within the squares represent the number of data points in each category. For instance, 18783 benign cases were correctly classified (true positive), 99 benign cases were mistakenly identified as malignant, resulting in false positives. True positives (TP): 18783 (99.0%) - These are the benign cases that were correctly classified by the model. False positives (FP): 99 (1.0%). The model misclassified these benign cases as malignant. These benign cases were wrongly identified as malignant by the model. False negatives (FN): 150 (1.0%) - These malignant cases were misclassified as benign by the model. True negatives

(TN): 12120 (99.0%) - These malignant cases were accurately identified by the model. Looking at these values, we can see that the deep neural network model performed well in classifying both benign and malignant cases. The vast majority of cases (over 99% for both classes) were classified correctly.

Performance Review of the Model

The performance was evaluated using a comprehensive set of evaluation metrics.

Table 1: Performance Metrics of Different Models

Model	Accuracy	Precision	Recall	F1 Score
DNN	99.608374	96.6	94.7	95.6
CNN+FC [26]	0.9926	0.9933	0.9919	0.9925
CNN-LSTM IDS[27]	0.979	0.983	0.979	0.981
CNN-IDS [8]	0.76	0.683	0.827	0.748
RNN-IDS [19]	0.794	0.807	0.811	0.809
LSTM-IDS [1]	0.832	0.841	0.853	0.847
LigthGBM-IDS [13]	0.838	0.828	0.867	0.847
XGBoost	98.311505	96.4	98.9	97.6
RBF_SVM	97.213662	96.5	96.8	96.6
KNN	96.510657	96.6	94.7	95.6
Decision Tree	95.820493	94.1	97.3	95.7
SGD	83.628659	85.1	71.0	77.4
Logistic Regression	83.490627	82.0	75.2	78.4
Naive Bayes	71.221751	66.6	58.6	62.1
Quadratic	49.637262	44.3	99.6	61.4

Table 1 presents the Accuracy, Precision, Recall, and F1 Score of various machine learning models used for the classification task. This table summarizes the performance of seven machine learning models, which include: DNN, XGBoost, RBF_SVM, KNN, Decision Tree, SGD, Logistic Regression, Naive Bayes, and Quadratic Discriminant

Four metrics, namely Accuracy, Precision, Recall, and F1 Score, were used to evaluate the performance of the models. DNN: Achieved the highest accuracy (99.61%), precision (96.6%) and F1 score (95.6%) . In contrast, its recall (94.7%) is slightly lower than XGBoost. XGBoost: Demonstrated accuracy (98.31%), precision (96.4%), recall (98.9%) and F1 score (97.6%) that are very competitive with DNN. It achieved the highest recall among all models. RBF_SVM: Showed accuracy (97.21%), precision (96.5%), recall (96.8%) and F1 score (96.6%) that are all comparable to each other. KNN: Achieved similar accuracy (96.51%) and precision (96.6%) to RBF_SVM, but its recall (94.7%) and F1 score (95.6%) are slightly lower. Decision Tree: Had lower accuracy (95.82%) and F1 score (95.7%) compared to the top performing models. It also has a lower precision (94.1%) but achieved a high recall (97.3%). SGD: Showed a significant drop in performance compared to the previous models, with accuracy (83.63%), precision (85.1%), recall (71.0%) and F1 score (77.4%) all being considerably lower. Logistic Regression: Achieved similar performance to SGD, with accuracy (83.49%), precision (82.0%), recall (75.2%) and F1 score (78.4%) all falling within a similar range. Naive Bayes: Had the lowest accuracy (71.22%) and F1 score (62.1%) among all models. Its precision (66.6%) and recall (58.6%) were also considerably lower than other models. Quadratic Discriminant Analysis: Showed the worst performance overall, with accuracy (49.64%), precision (44.3%), recall (99.6%) and F1 score (61.4%) all significantly lower than the other models. It's interesting to note that while it has a high recall, this is likely due to random chance as the overall accuracy is very low.

5. Summary and Future Directions

This research explores the identification of DDoS attacks, which pose a significant challenge in cybersecurity. To tackle this problem, a supervised machine learning framework was created to differentiate among regular and harmful network traffic. Leveraging datasets such as CIC-DDoS2019 and DDoS SDN, the study employed Deep Neural Networks (DNN), XGBoost (Extreme Gradient Boosting), Restricted Boltzmann Machine with Supervised Fine-tuning (RBM_SVF), Logistic Regression, K-Nearest Neighbors (KNN), Decision Tree, SGD, Naive Bayes and Quadratic classifiers. Rigorous data preprocessing, including handling missing values and feature scaling, was conducted to enhance model performance. The Deep Neural Networks (DNN) algorithm demonstrated superior accuracy 99.6 % in recognizing DDoS attacks when contrasted with XGBoost (98.3%), RBM_SVF (97.2%) and KNN (96.5%).

References

1. Y. Imrana, Y. Xiang, L. Ali and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for [61] intrusion detection," Expert Systems with Applications, vol. 185, no. 11, pp. 115–129, 2021.
2. I. Sharafaldin, A.H. Lashkari, A.A. Ghorbani, Toward generating a new intrusion detection dataset and intrusion traffic characterization, in: 4th International Conference on Information Systems Security and Privacy, Vol. 1, ICISSP, 2018, pp. 108–116.
3. Cheema, M. Tariq, A. Hafiz, M.M. Khan, F. Ahmad, M. Anwar Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review vol. 2022, Security and Communication Networks (May 2022), pp. 1-15, 10.1155/2022/8379532.
4. Agostinello, D., Genovese, A., Piuri, V., 2023. Anomaly-based intrusion detection system for DDoS attack with deep learning techniques. In: Proceedings of the 20th International Conference on Security and Cryptography. 1. SCITEPRESS, pp. 267–275.
5. Sarhan M., Layeghy S., Portmann M. Evaluating standard feature sets towards increased generalisability and explainability of ML-based network intrusion detection Big Data Res., 30 (2022), Article 100359.
6. PolatH. et al. A novel approach for accurate detection of the DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks Expert Syst. Appl. (2022)
7. Mahmoud R., Yousuf T., Aloul F., Zualkernan I. Internet of Things (IoT) security: Current status, challenges and prospective measures 2015 10th International Conference for Internet Technology and Secured Transactions, ICITST (2015), pp. 336-341, 10.1109/ICITST.2015.7412116.
8. M. ElSayed, N. Le-Khac, M. Albahar and A. Jurcut, "A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique," Journal of Network and Computer Applications, vol. 191, no. 3, pp. 103–116, 2021.
9. Bhushan, K., Gupta, B.B. Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. J Ambient Intell Human Comput 10, 1985–1997 (2019). https://doi.org/10.1007/s12652-018-0800-9.
10. Manthan Patel, P.P. Amritha, Vinay B Sudheer, M. Sethumadhavan,
11. DDoS Attack Detection Model using Machine Learning Algorithm in Next Generation Firewall, Procedia Computer Science, Volume 233, 2024, Pages 175-183, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.03.207.
12. B. Indira, K. Valarmathi, D. Devaraj, An approach to enhance packet classification performance of software-defined network using deep learning Soft Computing, 23 (2019), pp. 8609-8619.

13. J. Liu, Y. Gao and F. Hu, "A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM," Computers & Security, vol. 106, no. 11, pp. 102–119, 2021.
14. Jalal Bhayo, Syed Attique Shah, Sufian Hameed, Awais Ahmed, Jamal Nasir, Dirk Draheim, Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks, Engineering Applications of Artificial Intelligence, Volume 123, Part C, 2023, 106432, ISSN 0952-1976, https://doi.org/10.1016/j.engappai.2023.106432.
15. Ali Ihsan, Ahmed Abdelmuttlib Ibrahim Abdalla, Almogren Ahmad, Raza Muhammad Ahsan, Shah Syed Attique, Khan Anwar, Gani Abdullah Systematic literature review on IoT-based botnet attack IEEE Access, 8 (2020), pp. 212220-212232, 10.1109/ACCESS.2020.3039985.
16. Di Mauro M., Galatro G., Fortino G., Liotta A. Supervised feature selection techniques in network intrusion detection: A critical review Eng. Appl. Artif. Intell., 101 (2021), Article 104216.
17. Xie Junfeng, Yu F Richard, Huang Tao, Xie Renchao, Liu Jiang, Wang Chenmeng, Liu Yunjie A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges IEEE Commun. Surv. Tutor., 21 (1) (2018), pp. 393-430.
18. R.A. Calix, S. Rajesh, Feature ranking and support vector machines classification analysis of the NSL-KDD intrusion detection corpus, Proceedings of the Twenty-Sixth International Florida Artificial Intelligence Research Society Conference (May 2013).
19. I. Ullah and Q. Mahmoud, "Design and development of RNN anomaly detection model for IoT networks," IEEE Access, vol. 10, no. 2, pp. 62722–62750, 2022.
20. I. Ko, D. Chambers, E. Barrett, Adaptable feature-selecting and threshold-moving complete autoencoder for ddos flood attack mitigation, J. Inf. Secur. Appl., 55 (2020), Article 102647.
21. K.K. Mishra, S. Tiwari, A.K. Misra, A bio inspired algorithm for solving optimization problems, 2011 2nd Int. Conf. Comput. Commun. Technol. ICCCT-2011 (2011), pp. 653-659.
22. Al-zubidi, A., Farhan, A. & Towfek, S. (2024). Predicting DoS and DDoS attacks in network security scenarios using a hybrid deep learning model. Journal of Intelligent Systems, 33(1), 20230195. https://doi.org/10.1515/jisys-2023-0195.
23. Ferrag MA, Maglaras L, Moschoyiannis S, Janicke H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. J Inf Secur Appl. 2020;50:102419. 10.1016/j.jisa.2019.102419.
24. Yang Li, Li Guo, An active learning based TCM-KNN algorithm for supervised network intrusion detection, Computers & security, 26 (7-8) (2007), pp. 459-467.
25. J. Cheng, J. Yin, Y. Liu, Z. Cai, C. Wu, DDoS attack detection using IP address feature interaction, Proceedings of the IEEE International Conference on Intelligent Networking and Collaborative Systems, IEEE: Piscataway Township, Thessalonika, GreeceNJ, USA (2009), pp. 113-118, 24–26 November 2010.
26. Mohamed et. al, DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing, Journal of King Saud University - Computer and Information Sciences,Volume 36, Issue 2, 2024, 101938, ISSN 1319-1578.
27. Yousef Sanjalawe and Turke Althobaiti, DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning, Computers, Materials and Continua, Volume 75, Issue 2, 2023, Pages 3571-3588, ISSN 1546-2218.
28. Agrawal, N., Tapaswi, S., 2019. Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. IEEE Commun. Surv. Tutor. 21 (4), 3769–3795.