An Intelligent Deep Learning Framework For Early Detection Of Distributed Denial-Of-Service Attacks

Sujit Sutradhar[1*], Vinit Grewal[2], Dr. Geetika Parmar[3], Dr. S. Kanchana[4], Manish Shrivastava[5], P.Kavitha[6]

[1*]Deputy Manager. IT Department ICFAI University, Tripura, Mail id: sujitsutradhar87@gmail.com Orcid id- https://orcid.org/0009-0003-4064-6180
[2]Assistant Professor, Department of Engineering and Technology, GNDU REGIONAL CAMPUS, Jalandhar Add:114, University Enclave, Phase 1, Jalandhar Email ID: vinitgrewal19@gmail.com, ORCID O0000-0002-6151-2208
[3]Assistant Professor, Department of Computer Science and Applications, Dr Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India Email ID: geetika.rathod@gmail.com, ORCID iD: 0000-0002-4137-7811
[4]Assistant Professor, Department of Computer Science, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu 603203, India. Email id: kanchans@srmist.edu.in
[5]Associate Professor, Computer Science and Engineering Department, Guru Ghasidas University, Bilaspur, CG Mail id: manbsp@gmail.com Orcid id: 0000-0002-1346-968X
[6]Assistant Professor, Department of Mathematics, Amrita School of Physical Sciences, Coimbatore, Amrita Vishwa Vidyapeetham - 641112 - India. State: Tamil Nadu, India. Email: p_kavitha@cb.amrita.edu

Abstract- Distributed Denial-of-Service (DDoS) attacks remain a critical threat to modern network infrastructures, particularly in cloud and software-defined networking environments. This study proposes a temporal-aware deep learning framework for early detection of DDoS attacks using flow-based traffic features from the CIC-DDoS2019 dataset. A subset of 500,000 traffic flows was utilized, including BENIGN, DrDoS_NetBIOS, and DrDoS_SSDP classes. To ensure realistic evaluation, a strict chronological data-splitting strategy was applied to prevent temporal leakage, and class-weighted optimization was incorporated to address severe imbalance. A feed-forward deep neural network was implemented and evaluated against Logistic Regression and Random Forest baselines. Experimental results demonstrate strong detection performance in the binary configuration, with stable macro F1-scores and high attack recall under imbalance-aware training. Progressive timestamp-based evaluation further confirms that malicious traffic can be reliably detected during early stages of observation, with minimal performance degradation across increasing portions of the traffic timeline. A feature ablation study indicates that static flow-level statistical attributes provide strong discriminative signals. The findings highlight the importance of temporal-aware validation and imbalance-sensitive optimization for realistic and deployment-oriented DDoS detection systems.

Keywords- DDoS detection, deep learning, temporal validation, class imbalance, early-stage detection.

1. INTRODUCTION

DDoS attacks remain a major threat to the contemporary network infrastructure, especially with the fast growth of cloud computing infrastructures, Internet of Things (IoT) systems, and scale enterprise-wide services. The modern DDoS attacks use the high-volume traffic, methods of amplification by reflection, and protocol exploitation to flood the targeted systems in brief time periods, which causes service outage, financial loss, and reputational harm. With complex and heterogeneous network environments that are becoming more and more complex, intelligent, scalable, and reliable detection mechanisms are becoming urgent. The use of deep learning-based DDoS detection

systems has been on the rise because of their capability of automatically learning discriminative traffic representations and operating high-dimensional network features [1-2]. Flow-based detection methods based on aggregated statistical properties derived out of packet streams have been popular because of their efficiency and practicality in large scale deployments, especially in software-defined networking environments [3-4]. Moreover, deployment-friendly and lightweight deep learning systems have shown encouraging detection capabilities in realistic network environments [5]. Nevertheless, the success of these systems is not only determined by the choice of models, but also by the evaluation methodology, imbalance, and time validation strategies.

Although machine learning and deep learning have made significant progress in intrusion detection, there are still a number of challenges. Network traffic datasets are often characterized by high dimensional feature space and extreme class imbalance that may bias the learning algorithms to favor the majority classes and hide the behavior of the minority classes. In general, extensive surveys of deep learning methods underscore the fact that numerous studies focus on general performance of detection and do not pay enough attention to imbalance-aware optimization and realistic evaluation conditions [6]. In addition, a number of current DDoS detection systems in SDN and flow-based systems are based on random traintest splits, which can cause temporal leakage and overstated performance estimates [7-8]. Chronological validation is necessary in operational settings as the detection systems have to examine future, invisible traffic streams. Also, early-stage detection, where malicious behaviour is detected before traffic has been accumulated fully, is not a well-explored area. Even though adaptive traffic sampling and monitoring mechanisms have been suggested to improve real-time DDoS detection, their analysis is usually not provided with progressive time analysis [9]. Absent a strict timeline-based assessment, it is hard to tell whether the detection models in fact extrapolate to changing traffic conditions or are just using fixed statistical separability.

To address these challenges, this study proposes a temporal-aware deep learning framework for DDoS detection using flow-level statistical features and rigorous chronological validation. The objectives of this work are:

- To develop an imbalance-aware deep learning model capable of maintaining stable performance under highly skewed traffic distributions.
- To implement a strict chronological data-splitting strategy that prevents temporal leakage and simulates realistic deployment conditions.
- To design and evaluate a progressive timeline-based early detection protocol that assesses detection stability across increasing portions of observed traffic.

Through comprehensive experimentation and comparative evaluation with traditional machine learning baselines, this study aims to contribute a deployment-oriented and methodologically rigorous approach for flow-based DDoS detection in modern network environments.

2. LITERATURE REVIEW

Detection of Distributed Denial-of-Service (DDoS) attacks has been widely investigated both in conventional machine learning and in deep learning. The initial methods mostly were based on classical machine learning models like Support Vector Machines (SVM), k-Nearest Neighbors (KNN), Decision Trees, Logistic Regression, and Random Forest classifiers. These models are usually run on manually derived statistical characteristics of network traffic streams, such as packet counts, bandwidth rates, and inter-arrival delays. The use of tree-based models, especially Random Forest, has shown great performance because of their capability to deal with nonlinear decision boundaries and non homogeneous distributions of features. Nevertheless, classic machine learning solutions can be very sensitive to feature engineering, and can perform poorly in the face

of high dimensional feature space or changing patterns of attacks. In addition, most previous studies measure performance based on random train-test splits that may result in temporal leakage and excessive generalization ability estimation.

As the large-scale network data sets have become more and more available, deep learning models have been proposed to automatically extract discriminative representations of traffic features. Other deep learning networks such as fully connected neural networks and hybrid networks have shown better detection results compared to traditional means [10- 11]. Structured traffic data have been subjected to Convolutional Neural Networks (CNNs) in order to extract spatial associations between statistical features [12], and hybrid deep learning systems that combine feature selection and neural architecture have increased the robustness of classification [13]. It has also been demonstrated that deep learning based methods are effective in large scale DDoS detection tasks [14]. Moreover, software-defined networking specific deep learning architectures have also been suggested to enhance detection performance in programmable network layouts [15-16]. Hybrid architectures that combine the autoencoder architectures with the multilayer perceptrons have also shown the capability to enhance the classification performance in complex traffic settings [17]. Although these developments have been made, not all deep learning-based studies are concerned with the overall accuracy and do not adequately consider severe class imbalance or realistic chronological validation. The other direction that is emerging in the research on DDoS detection is in regard to early-stage detection mechanisms. Sliding windows and streaming based IDS systems seek to detect malicious activities before traffic passes their entirety. Although this type of methodology is intended to minimize detection latency, the evaluation protocols are frequently restricted to static data, or not specifically simulated to address progressive observation conditions. Therefore, it is not certain that early detection models are stable to changing distributions of traffic.

Another important issue in cybersecurity datasets is the imbalance in classes. SMOTE has been popularly used as an oversampling method but other techniques like undersampling strategies have been used to rebalance datasets but both methods can distort the underlying data distributions or add artificial noise. A different approach is offered by the use of cost-sensitive learning and weighted loss functions that modify the optimization task without modifying the underlying data. Even though some of the studies have recognized the problem of imbalances, detailed analysis based on macro-averaged indicators and precision-recall is relatively under-researched in the literature on DDoS detection.

Although the literature is rather comprehensive, three gaps can still be identified: small application of strict chronological validation to avoid temporal leakage, lack of interest in imbalance-conscious optimization in highly skewed traffic conditions, and lack of evaluation of progressive early-stage detection performance. The current paper fills these gaps by incorporating imbalance-sensitive training, data splitting based on time, and progressive timeline evaluation into a single deep learning model of flow-based DDoS detection.

3. METHODOLOGY

3.1 Dataset Description

The dataset used in this study is the CIC-DDoS2019, which is a publicly available benchmark dataset used to test the performance of distributed denial-of-service detection systems. The data is flow-based network traffic logs, with each flow being described by statistical characteristics derived on the basis of unidirectional packet streams. In order to evaluate it experimentally, 500,000 of the traffic flows were considered to make sure that the computations are feasible and the diversity of attacks is

representative [18]. There are various traffic classes in the dataset, which are BENIGN, DrDoS_NetBIOS, and DrDoS_SSDP. All records have a timestamp attribute, which allows time-sensitive ranking of traffic to evaluate it in a temporal context.

3.2 Data Preprocessing

A preprocessing pipeline was proposed to offer leakage-free and stable model training. The label column was automatically determined by selecting categorical attributes that had a small set of distinct values, which was not hardcoded. Columns whose unique ratio is too large (greater than 95 percent unique values) were eliminated since such identifier-like attributes may introduce artificial separability. Categorical features were transformed into numbers by label encoding. The infinite values were replaced using missing values and then imputed using the median based imputation. In addition, the variables with zero variance (constancy) were eliminated to reduce unnecessary data. Finally, RobustScaler was employed to normalize the numerical features to minimize the impact of extreme outliers that characterize the DDoS traffic statistics.

3.3 Class Imbalance Handling

The dataset is severely imbalanced in terms of classes, with attack traffic being far more numerous than benign samples. To overcome this problem, the dynamically computed class weights based on the training data were done using inverse frequency weighting. These class weights were used in the training of all classification models so that the misclassification of the minority classes was more heavily punished in the optimization process.

3.4 Temporal-Aware Data Splitting

To avoid temporal leakage and to train a model in realistic deployment conditions, the dataset was chronologically sorted with the help of the timestamp attribute before the model training. It was split by time with the first 80% of the traffic flows going to training and the last 20% going to testing. This time division makes sure that the model is tested on future unobservable traffic patterns instead of random shuffled samples.

3.5 Deep Learning Model

The traffic classification was done using a feed-forward deep neural network (DNN) architecture. The model is built of three fully connected hidden layers containing 128, 64 and 32 neurons respectively with ReLU activation functions. The use of batch normalization and dropout regularization was used to enhance training stability and minimize overfitting. The output layer applies the sigmoid activation function when performing binary classification and softmax activation function when performing multi-class classification. Class-weighted optimization was used to train the model to deal with imbalance in the dataset.

3.6 Baseline Models

To test the efficiency of the proposed deep learning framework, two conventional machine learning models have been used as baseline: Logistic Regression and Random Forest. Training of Logistic Regression was done on scaled features with a class-weighted optimization strategy and training of Random Forest was done with the same class-weighting strategy but without feature scaling. These reference models are used to give comparative performance.

3.7 Early Detection Evaluation

A progressive timeline-based evaluation strategy was used to evaluate the ability of early-stage detection. The model performance was evaluated by incrementally adding more and more proportion of observed traffic (10%, 20%, 30%, 50%, 80% and 100 percent) after sorting the test set chronologically. This method models the conditions of real-time monitoring and assesses the possibility to identify malicious behavior at an early stage when the network traffic is developed.

3.8 Evaluation Metrics

Multiple metrics were used to measure model performance to consider the class imbalance. These measures are precision, recall, F1-score, Macro F1-score in case of multi-class analysis, Receiver Operating Characteristic Area Under the Curve (ROC-AUC) and Precision-Recall Area Under the Curve (PR-AUC). PR-AUC and Macro F1-score were given particular focus because they are strong in the presence of highly skewed data distributions.

4. RESULTS

4.1 Statistical Characteristics of the Dataset

The experimental study was done on a subset of 500,000 flows of the CIC-DDoS2019 dataset with three traffic types: BENIGN, DrDoS_NetBIOS, and DrDoS_SSDP. As shown in Table 1, there is a very severe imbalance in the dataset, with the attack traffic significantly outnumbering benign samples. DrDoS_NetBIOS takes up 59.88% of the dataset, DrDoS_SSDP takes up 39.98, and BENIGN traffic is only 0.14% of the total flows. This creates a disproportionate ratio of about 419: 1 of majority attack type and benign traffic. This extreme skewness is the reason why class-weighted optimization and macro-averaged evaluation metrics are used. Following preprocessing (removal of identifiers, categorical encoding, constant features removal, missing value imputation, correction of infinite values, and normalization to RobustScaler) the final feature dimensionality was 72 to 73 features based on experimental setting. Temporal analysis showed that there was a high density of attack types in thin time bands, which played a key role in determining the behavior of chronological split in subsequent experiments.

Table 1. Class Distribution of the 500,000-Flow Subset

Class	Samples	Percentage
DrDoS_NetBIOS	299,401	59.88%
DrDoS_SSDP	199,884	39.98%
BENIGN	715	0.14%
Total	500,000	100%

4.2 Binary Classification Performance (DrDoS_NetBIOS vs BENIGN)

Experiments on binary classification were done with DrDoS_NetBIOS and BENIGN traffic with a strict chronological 80/20 split, providing 160,000 training samples and 40,000 testing samples. The computation of the class weights was performed based on the training data only to solve the imbalance issue without leakage. Table 2 shows that the proposed deep neural network (DNN) was able to perform well in discriminative performance following the optimization of threshold. The model achieved the accuracy of 99.89, ROC-AUC 0.9841, PR-AUC 0.9999, and a macro F1-score of 0.9092. Notably, the confusion matrix indicates that the model was able to correctly identify 104 of 118 benign samples, which is an 88.14 percent benign recall and an attack recall of 99.92. With the imbalance ratio of about 337:1 in the test split, these findings indicate successful

minority-class recovery. Even though ROC-AUC is high, macro F1-score and per-class recall are more accurate indicators of performance in the case of extreme skew.

Table 2. DNN Binary Classification Performance

Metric	Value
Accuracy	0.9989
ROC-AUC	0.9841
PR-AUC	0.9999
Macro F1-score	0.9092
Weighted F1-score	0.9989

4.3 Baseline Model Comparison

To confirm the performance of the suggested framework, the two models Logistic Regression and Random Forest were tested under the same conditions of preprocessing, temporal splitting and class-weighting. Table 3 demonstrates that the F1-score and attack recall of Logistic Regression were 0.9982 and 0.9965, respectively, which implies that there is a great deal of linear separability in this binary setup. Random Forest had an ideal classification performance with F1-score and attack recall value of 1.0. These results indicate that flow-level statistical characteristics of this dataset are highly separable between DrDoS_NetBIOS and BENIGN traffic. Although the DNN does not substantially exceed the Random Forest in the raw predictive metrics, it has more continuous probabilistic outputs, threshold adaptability and stability in imbalance-conscious optimization, which are significant factors when used in real-time deployment settings.

Table 3. Binary Model Comparison

Model	F1-score	Attack Recall	PR-AUC
Logistic Regression	0.9982	0.9965	0.9997
Random Forest	1.0000	1.0000	1.0000
Proposed DNN	0.9989	0.9992	0.9999

4.4 Timestamp-Based Early Detection Evaluation

To determine the potential of early-stage detection, the chronologically sorted test set was tested in progressively increasing timeline proportions, as a simulation of deployment conditions where decisions have to be made before the entire traffic sequence is observed. As shown in Table 4, the performance was very stable in all the stages with F1-score of between 0.9957 and 0.9986 and attack recall of 99.8 and above. It is noteworthy that the model was able to reach an F1-score of 0.9986 and attack recall of 0.9992 even at 10 percent of the timeline (4,000 samples). The fact that the difference between stages (less than 0.3 percent) is minimal shows that even the initial parts of the traffic history already have enough statistical indicators to be able to detect attacks reliably. These results confirm the suggested temporal-conscious assessment plan and suggest high generalization between progressive observation windows.

Table 4. Progressive Timestamp-Based Early Detection Results

Stage (% of Timeline)	Samples	F1-score	Attack Recall	PR-AUC
10%	4,000	0.9986	0.9992	1.0000
20%	8,000	0.9983	0.9990	1.0000
30%	12,000	0.9957	0.9981	0.9999
50%	20,000	0.9974	0.9987	1.0000
100%	40,000	0.9986	0.9993	1.0000

4.5 Feature Ablation Study

To analyze the role of rate-based temporal features, 27 flow-duration, packet-rate and inter-arrival-time features were eliminated, leaving the feature set with 45 dimensions. Random Forest, as evidenced by Table 5, did not lose its perfect classification accuracy even when the features were removed, and the F1-score and attack recall were both 1.0. It means that, only the flow-level statistical characteristics at the static level can be used to give high separability between DrDoS_NetBIOS and BENIGN traffic in this subset. The lack of performance degradation implies that the discriminative patterns are not only conditioned by the properties of rate-based accumulation, but they also emerge due to the structural packet and header statistics inherent to the attack behavior.

Table 5. Random Forest Performance After Removing 27 Rate-Based Features

Metric	Value
F1-score	1.000
Attack Recall	1.000
PR-AUC	1.000

4.6 Multi-Class Temporal Evaluation

Multi-class assessment was conducted at a strict chronological 80/20 split (400,000 training and 100,000 testing samples). Because of the time clustering of attack types in the data, the test window had a majority of DrDoS_SSDP traffic causing underrepresentation of the classes. As Table 6 demonstrates, Logistic Regression had a macro F1-score of 0.3083 and weighted F1-score of 0.9248 whereas random forest had a macro F1-score of 0.6644 and weighted F1-score of 0.9931. The decrease in macro F1-score is due to the unequal distribution of the classes instead of the deficiency of the model per se. These findings indicate a critical dataset property: the attack types are time-segmented, providing a element of distribution shift with the rigid chronological separation and making it difficult to assess the multi-class generalization.

Table 6. Multi-Class Temporal Performance

Model	Macro F1	Weighted F1
Logistic Regression	0.3083	0.9248
Random Forest	0.6644	0.9931

5. DISCUSSION

The experimental findings show that the suggested temporal-mindful deep learning model can be used to achieve high detection rates in case of harsh class imbalance and stringent time-based assessment. The deep neural network in the binary setting was able to differentiate DrDoS-NetBIOS traffic and benign flows with high recall and recall of both majority and minority classes. The macro F1-score proves that the performance did not rely on the prevalent attack type only, which means that the imbalance-aware optimization strategy has been effective to avoid the bias toward the majority traffic. Even though Random Forest demonstrated an ideal performance in the binary case, the proposed DNN offered a similar predictive power but with consistent probabilistic values and threshold flexibility, which is beneficial to the real-time deployment scenarios where the sensitivity needs to be varied. Other deployment-oriented deep learning mechanisms have been highlighted in recent SDN-based detection models, where the significance of flexible and resilient models in operational networks is emphasized [19].

The early detection evaluation is further supported by the timestamp which proves the strength of the framework. The performance of the model was very consistent over progressive segments of the traffic timeline, which proves that even at the initial stages of observation, discriminative features of DDoS traffic can be detected. The fact that the F1-score has not changed significantly and the model has a high attack recall is an indication that the model does not solely rely on late-stage traffic accumulation patterns. This observation is consistent with the recent research on variable-rate and adaptive DDoS detection methods, in which rapid identification of traffic abnormalities is essential in reducing the growth of the attacks [20]. The ability to detect early-stage is especially applicable to real-life mitigation systems where the response latency has a direct effect on the service availability.

The study of feature ablation gives further information about the structural features of the dataset. Deleting the rate-based time-related attributes did not lead to a drop in the classification performance, which means that flow-level statistical characteristics that are not dynamic can give powerful discriminatory indicators between attack and benign traffic in this subset. This implies that separability is not just due to traffic intensity measures, but also due to structural variations of packets and flows. Deep learning models that are hybrids between representation learning and neural architectures have also been reported to be highly separable when using enriched statistical features [21], which makes the point that deep models can identify strong patterns of traffic beyond mere rate measures.

The multi-class time-based assessment demonstrated a significant data property: temporal grouping of types of attacks. When strict chronological splitting was applied, some classes were underrepresented in the test window, and thus their macro-averaged performance was low, even though the overall accuracy was high. This result is a demonstration of distribution shift and not model deficiency. Attack campaigns can also be temporally clustered in realistic network settings, and chronological analysis can thus detect drift in class distributions. Recent multi-class DDoS detection research in SDN settings has also documented issues of ensuring balanced performance across temporally distributed attack classes [22], which has supported the significance of prudent temporal validation design.

Although the deep learning model did not significantly improve on tree-based methods in raw predictive metrics, the main value of the current study is its methodological rigor. Combination of imbalance-conscious optimization, rigid chronological analysis, and gradual early identification analysis creates a realistic and deployment-centered evaluation structure. Comparisons of deep learning architectures have revealed that the superiority of models frequently relies on evaluation strategy and methodology of data partitioning as opposed to architecture itself [23]. Unlike the methods that depend on random data partitioning that can cause temporal leakage, the current study has shown that even with realistic temporal constraints, strong detection can be preserved. Moreover, the methods that integrate deep learning with probabilistic modelling in the detection of unfamiliar or changing DDoS trends highlight the importance of strong validation steps when there is a change in the distribution [24].

Regarding practicality, the findings affirm that flow-based statistical characteristics are very informative in detecting DDoS and can aid in stable early-stage detection of unhealthy activity. Nevertheless, the temporal clustering of the types of attacks observed indicates that generalization claims would be enhanced by generalizing further through cross-session and cross-day validation. Future studies can investigate more varied temporal divisions, experiments on generalization of attacks and experimenting with robustness in different network conditions to increase the applicability of the proposed framework.

Comprehensively, the results confirm the usefulness of the temporal-conscious, imbalance-conscious deep learning model and emphasize key issues to be taken into account when realistically testing DDoS detection systems in practice.

6. CONCLUSION

This study presented a temporal-aware deep learning framework for early detection of distributed denial-of-service attacks using flow-based traffic features from the CIC-DDoS2019 dataset. The suggested methodology combines the imbalance-sensitive optimization strategy, strict chronological data division, and timeline-based progressive evaluation to guarantee realistic and deployment-oriented evaluation. The framework ensures that it has methodological rigor and practical applicability by eliminating identifier-like attributes and avoiding the temporal leakage. As shown by experimental findings, the deep neural network provides high detection rates in the binary setup, successfully separating attack traffic and benign flows and balancing the performance across classes. Imbalanced training is important in highly skewed traffic settings, and the use of class-weighted optimization is shown to be much more effective at detecting minorities. Further development of the use of progressive timestamp-based evaluation proves that malicious behavior can be detected with a high degree of reliability at the initial stages of traffic monitoring, which indicates the possibility of the framework to be used in real-time mitigation systems. The comparison with the Logistic Regression and Random Forest models shows that flow-level statistical features are strongly separable in the subset under consideration. Although tree-based models had competitive performance, the proposed deep learning model has stable probabilistic results and threshold flexibility, which are beneficial in the working environment with varying operational detection sensitivity. On the whole, the results indicate the relevance of temporal-conscious validation and imbalance-sensitive optimization in designing DDoS detection systems. The proposed framework helps in the formulation of more realistic and strong evaluation methods of flow-based intrusion detection in large scaled networks.

REFERENCES

1. Asad, M., Asim, M., Javed, T., Beg, M.O., Mujtaba, H. and Abbas, S., 2020. Deepdetect: detection of distributed denial of service attacks using deep learning. The Computer Journal, 63(7), pp.983-994.
2. Yuan, X., Li, C. and Li, X., 2017. DeepDefense: identifying DDoS attack via deep learning. In 2017 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 1–8. IEEE.
3. Li, C., Wu, Y., Yuan, X., Sun, Z., Wang, W., Li, X. and Gong, L., 2018. Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN. International Journal of Communication Systems, 31(5), e3497.
4. Niyaz, Q., Sun, W. and Javaid, A.Y., 2016. A deep learning based DDoS detection system in software-defined networking (SDN). arXiv preprint, arXiv:1611.07400.
5. Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martinez-del-Rincon, J. and Siracusa, D., 2020. LUCID: A practical, lightweight deep learning solution for DDoS attack detection. IEEE Transactions on Network and Service Management, 17(2), pp.876–889.
6. Mittal, M., Kumar, K. and Behal, S., 2023. Deep learning approaches for detecting DDoS attacks: A systematic review. Soft Computing, 27(18), pp.13039–13075.
7. Elsayed, M.S., Le-Khac, N.A., Dev, S. and Jurcut, A.D., 2020. DDoSNet: A deep-learning model for detecting network attacks. In 2020 IEEE 21st International Symposium on

A World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 391–396. IEEE.
8. Haider, S., Akhunzada, A., Mustafa, I., Patel, T.B., Fernandez, A., Choo, K.K.R. and Iqbal, J., 2020. A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. IEEE Access, 8, pp.53972–53983.
9. Ujjan, R.M.A., Pervez, Z., Dahal, K., Bashir, A.K., Mumtaz, R. and González, J., 2020. Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Generation Computer Systems, 111, pp.763–779.
10. Akgun, D., Hizal, S. and Cavusoglu, U., 2022. A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Computers & Security, 118, 102748.
11. Aktar, S. and Nur, A.Y., 2023. Towards DDoS attack detection using deep learning approach. Computers & Security, 129, 103251.
12. Amma, N.G.B. and Subramanian, S., 2018. Vcdeepfl: Vector convolutional deep feature learning approach for identification of known and unknown denial of service attacks. In TENCON 2018 – 2018 IEEE Region 10 Conference, pp. 0640–0645. IEEE.
13. Alghazzawi, D., Bamasag, O., Ullah, H. and Asghar, M.Z., 2021. Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. Applied Sciences, 11(24), 11634.
14. Kumar, D., Pateriya, R.K., Gupta, R.K., Dehalwar, V. and Sharma, A., 2023. DDoS detection using deep learning. Procedia Computer Science, 218, pp.2420–2429.
15. Elubeyd, H. and Yiltas-Kaplan, D., 2023. Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks. Applied Sciences, 13(6), 3828.
16. Nugraha, B. and Murthy, R.N., 2020. Deep learning-based slow DDoS attack detection in SDN-based networks. In 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 51–56. IEEE.
17. Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W. and Camtepe, S., 2021. Ae-mlp: A hybrid deep learning approach for ddos detection and classification. IEEE Access, 9, pp.146810–146821.
18. Jamwal, A., 2025. CIC-DDoS 2019 dataset combined [dataset]. Kaggle. Available at: https://www.kaggle.com/datasets/anikaitjamwal/cic-ddos-2019-dataset-combined (Accessed: 11 February 2026).
19. Hnamte, V., Najar, A.A., Nhung-Nguyen, H., Hussain, J. and Sugali, M.N., 2024. DDoS attack detection and mitigation using deep neural network in SDN environment. Computers & Security, 138, 103661.
20. Bahashwan, A.A., Anbar, M., Manickam, S., Al-Amiedy, T.A., Aladaileh, M.A. and Bin-Salem, A.A., 2025. A deep learning-based mechanism for detecting variable-rate DDoS attacks in software-defined networks. Mobile Networks and Applications, 30(1), pp.12–41.
21. Pajila, P.J., Robinson, Y.H., Allimuthu, U., Julie, E.G., Jaffrin, L. and Sheena, B.G., 2025. Enhanced autoencoder and deep neural network (AE&DNN) method for ddos attack recognition. Wireless Networks, 31(4), pp.3277–3295.
22. Zaidoun, A.S. and Lachiri, Z., 2025. A hybrid deep learning model for multi-class DDoS detection in SDN networks. Annals of Telecommunications, pp.1–14.
23. Mandela, N. and Etyang, F., 2025. Comparative analysis of deep learning models for effective denial of service (DoS) attack detection in network security. Journal of Electrical Systems and Information Technology, 12(1), 73.
24. Shieh, C.S., Lin, W.W., Nguyen, T.T., Chen, C.H., Horng, M.F. and Miu, D., 2021. Detection of unknown ddos attacks with deep learning and gaussian mixture model. Applied Sciences, 11(11), 5213.