International Journal of Informatics and Computation (IJICOM)
Vol. 7, No.1, 2025
ISSN: 2685-8711, E-ISSN: 2714-5263 DOI: 10.35842/ijicom

TransDDoS: Transformer-Based Model for Intelligent Detection of DDoS Attacks

M. Hizbul Wathan[1], Indra Irawan[2], Better Swengky[3] ,M.Syafrizal Zain[4] , Ardi Ramadani[5], Selamet Riadi[6]

Abstract
Distributed Denial of Service (DDoS) attacks pose a critical threat to the stability and availability of modern network infrastructures. This study proposes the application of a pure Transformer architecture for the effective detection of DDoS attacks, utilizing the CICDDoS2019 dataset. The research workflow includes data preprocessing (cleaning, normalization, and one-hot encoding), feature selection using the Random Forest algorithm, data splitting (80% training and 20% testing), model training, and performance evaluation. The results show that the Transformer model achieves an accuracy of 99.82%, precision of 99.80%, recall of 99.83%, and F1-score of 99.82%. This approach outperforms previous methods such as CNN, Deep Neural Networks, Deep Q-Networks, and ensemble models, which typically reach accuracy levels between 90% and 99%. The superior performance of the Transformer is attributed to its self-attention mechanism, which effectively captures complex patterns in network traffic data. The key contributions of this study include the novel implementation of a Transformer model in the field of network intrusion detection, the integration of RF feature selection to enhance model efficiency, and a comprehensive empirical evaluation demonstrating improved results over traditional approaches. The findings indicate that the Transformer is a highly promising approach for developing intelligent, early-warning systems to counter large-scale cyberattacks. Future work may explore real-time deployment and adaptive learning capabilities to respond to emerging threats.

Keywords:
Transformer, DDoS, Deep Learning, Network Intrusion Detection

1. Introduction

In today's interconnected digital environment, Distributed Denial of Service (DDoS) attacks continue to pose a critical threat to the availability and reliability of online services. These attacks flood a target server or network with massive traffic, thereby overwhelming its resources and rendering legitimate access nearly impossible. The growing sophistication and frequency of DDoS attacks have necessitated the development of more intelligent and adaptive Intrusion Detection Systems (IDS), especially those capable of real-time analysis and rapid response. Machine learning (ML) and deep learning (DL) techniques have become prominent tools in the development of DDoS detection mechanisms. Several studies have implemented classical machine learning classifiers such as Random Forest, Naïve Bayes, K-Nearest Neighbors (KNN), and Support Vector Machine (SVM) with promising results [1], [2].

Corresponding Author: Indra Irawan(indraa@polman-babel.ac.id)
1 M.Hizbul Wathan, Politeknik Manufaktur Negeri Bangka Belitung, mhizbul@polman-babel.ac.id
2 Indra Irawan , Politeknik Manufaktur Negeri Bangka Belitung, indraa@polman-babel.ac.id
3 Better Swengky, Politeknik Manufaktur Negeri Bangka Belitung, better@polman-babel.ac.id
4 M.Syafrizal Zain, Politeknik Manufaktur Negeri Bangka Belitung, msyafrizalz@polman-babel.ac.id
5 Ardi Ramadani, Politeknik Manufaktur Negeri Bangka Belitung, ardiramadani@gmail.com
6 Selamet Riadi, Universitas Teknologi Mataram, selametriadi.1897@gmail.com

Ensemble learning strategies, such as those used by Bagdadi & Messabih (2024) [3], have also demonstrated improvements in performance through feature selection and classifier fusion. Deep learning-based models like Convolutional Neural Networks (CNN), Autoencoders, and Deep Q-Networks (DQN) have shown competitive results by learning high-level representations of network traffic data [4][5][6].

However, despite these advances, limited attention has been paid to the Transformer architecture, a model originally designed for natural language processing but recently gaining traction in other sequence modeling tasks. Transformers, through their self-attention mechanism, are capable of capturing long-range dependencies and contextual relationships in sequential data, making them particularly suitable for the temporal and high-dimensional nature of network traffic analysis. Ouhssini et al. emphasized the growing relevance of deep learning approaches but acknowledged that more extensive experimentation with attention-based models is still needed [7]. Furthermore, Tymoshchuk et al. demonstrated high classification accuracy using neural networks for identifying DDoS attack types, reinforcing the potential of more expressive deep learning architectures [8].

This study proposes a Transformer-based deep learning framework for DDoS attack detection using the CICDDoS2019 dataset. The specific contributions are as follows:

1. Development of a Transformer-based detection model that leverages the self-attention mechanism to capture intricate patterns in network traffic for effective DDoS classification.
2. Incorporation of feature selection using the Random Forest algorithm, which reduces feature dimensionality and enhances learning performance by removing irrelevant or redundant features.
3. Comprehensive comparative evaluation against state-of-the-art machine learning and deep learning models, including Random Forest, CNN, and hybrid approaches, on various performance metrics such as accuracy, precision, recall, and F1-score.

As DDoS attacks grow in scale and sophistication, there is an urgent need to explore architectures beyond conventional neural networks. This study makes a timely and meaningful contribution by applying the Transformer model to a domain where sequential pattern recognition is crucial yet underexplored. The results not only validate the model's efficacy but also open new avenues for its application in cybersecurity. The integration of advanced feature selection and a robust evaluation framework further strengthens the scientific and practical value of this work, positioning it as a strong candidate for adoption in real-time intrusion detection systems.

2. Related Works

In the digital age, cyberattacks—particularly Distributed Denial of Service (DDoS) attacks—have become increasingly sophisticated, posing severe risks to the stability and integrity of network infrastructures. As online systems grow in complexity and criticality, there is a heightened need for intelligent and adaptive intrusion detection systems (IDS). This literature review critically examines recent studies and innovations in DDoS detection, focusing on the progression from traditional machine learning methods to more advanced deep learning and Transformer-based models.

An article evaluated classical classifiers such as Neural Networks, Naïve Bayes, Random Forest, KNN, and SVM, achieving the best accuracy (98.70%) with Random Forest [9]. Similarly, Salunke et al. explored KNN, Decision Tree, and Random Forest algorithms, demonstrating competitive results on the KDD dataset [10]. However, these approaches often struggle with high-dimensional data and generalization across diverse attack types. Boonchai et al. implemented Deep Neural Networks and Convolutional

Autoencoders to classify multi-class DDoS attacks using the CICDDoS2019 dataset, achieving 91.9% accuracy [4]. Satmoko et al. enhanced detection accuracy to 99.68% using ensemble methods combining KNN, Naïve Bayes, and Random Forest, along with Chi-Square-based feature selection [11].

To improve model precision, another paper integrated autoencoders with Bayesian optimization, reaching up to 90% accuracy [12]. Tymoshchuk et al. further validated the robustness of neural networks in classifying SYN, ACK, HTTP, and UDP flood attacks, achieving 99.35% accuracy and 95.05% in near real-world conditions [8]. Prima et al. benchmarked 14 machine learning models, with Random Forest achieving 100% accuracy, though overfitting risks were not deeply addressed [13]. In a novel CNN-based approach, Najar et al. achieved 99.99% binary classification accuracy and 98.44% for multi-class detection, addressing class imbalance through random sampling and optimal feature reduction [14]. Bagdadi and Messabih reached 99.90% binary accuracy using ensemble methods and feature selection to manage 12 and 7-class DDoS scenarios [3].

Cheng et al. proposed a modified PointNet (mPointNet) architecture for classifying and segmenting DDoS attacks in blockchain networks, reaching 99.65% and 85.47% accuracy, respectively, using the CIC-DDoS2019 dataset [15]. Indra Kumar and Ishigaki introduced a meta-learner-based ensemble combining LSTM, RF, and KNN, improving classification accuracy to 96%, outperforming simpler models [16]. In the context of misinformation detection, Mulyani et al. utilized BERT, a Transformer-based model, for fake news detection in the health domain, significantly outperforming traditional models, highlighting the adaptability of Transformer architectures beyond NLP tasks [17]. Similarly, Cheng et al. and Sinha & Degadwala reviewed the effectiveness of deep learning for multi-class DDoS detection in IoT, highlighting gaps in real-time adaptability [18][19].

Wathan and Aziz provided a comparative study of CNN and several machine learning algorithms (SVM, KNN, GNB, Decision Trees, GBoost), using a large Kaggle dataset [20]. While CNN showed excellent accuracy, KNN emerged as the most stable performer, challenging assumptions about deep learning dominance in all contexts. On a different front, Sugiyatno proposed a defense strategy combining Software-Defined Networking (SDN) and honeypot systems to dynamically redirect and analyze malicious traffic, showcasing how intelligent architecture integration enhances detection and mitigation in modern networks [21].

Recent developments in intrusion detection have increasingly adopted hybrid and Transformer-based models. Aljawarneh et al. proposed a hybrid intrusion detection system combining CNN and RNN architectures, which improved multiclass attack classification while mitigating class imbalance issues [22]. Similarly, Vinayakumar et al. designed a deep learning model using stacked LSTM layers, which demonstrated high detection accuracy and generalization across datasets such as NSL-KDD and UNSW-NB15 [23]. Nguyen et al. further advanced this field by implementing a bidirectional LSTM for anomaly-based DDoS detection in SDN environments, emphasizing the role of temporal pattern recognition in traffic analysis [24].

In lightweight network environments, Roy et al. introduced efficient CNN models optimized for IoT-based intrusion detection, focusing on minimizing computational overhead while maintaining performance [25]. Additionally, Lin et al. explored Vision Transformer (ViT) architectures for intrusion detection tasks, demonstrating that attention-based mechanisms originally designed for image processing can effectively model complex patterns in network traffic data [26]. These studies support the growing relevance of attention and sequence modeling techniques in the field of intelligent intrusion detection.

Overall, the reviewed studies illustrate the dynamic evolution of DDoS detection techniques from conventional classifiers to ensemble and deep learning methods. While many models have achieved near-perfect accuracy, their limitations lie in generalization,

real-time performance, and adaptability to novel attacks. Transformer models, with their ability to model contextual dependencies through self-attention mechanisms, remain underutilized in this domain. Therefore, this study contributes by exploring the application of the Transformer model in DDoS detection, addressing the gap, and setting a foundation for more intelligent, adaptive, and scalable intrusion detection systems in the future.

3. Proposed Method

This study addresses the case of detecting Distributed Denial of Service (DDoS) attacks in computer networks using a deep learning approach based on the Transformer architecture. The dataset employed is CICDDoS2019, developed by the Canadian Institute for Cybersecurity (CIC), which reflects various types of DDoS attacks occurring in real network traffic [27]. The objective of this study is to develop a classification system capable of distinguishing between benign traffic and DDoS attacks with high accuracy and computational efficiency.

3.1 Research Design

This research is conducted through five main stages: (1) data preprocessing, (2) feature selection, (3) data splitting, (4) Transformer model training, and (5) model evaluation. The methodological workflow design is illustrated in Fig. 1.

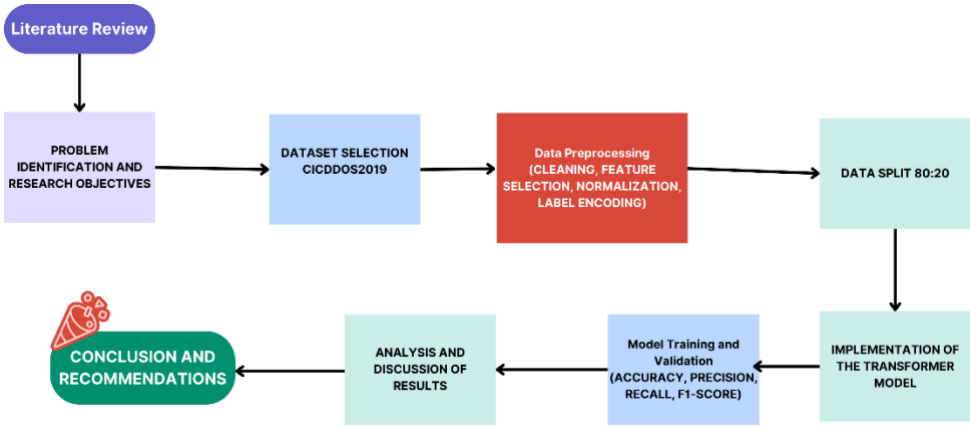

Fig.1 Research Flow Diagram

3.2 Data Pre-processing

This stage comprises several essential processes to prepare the data for use by the learning model:

a. Data Cleaning

This process involves the removal of duplicate entries, null values, and incomplete data. The goal is to ensure the quality and integrity of the dataset [5].

b. Normalization

Normalization is used to scale feature values to a uniform range (typically 0 to 1), using the Min-Max Normalization formula [12]:

$$X_{\text{norm}} = \frac{X - X_{\text{min}}}{X_{\text{max}} - X_{\text{min}}}$$

(1)

c. One-Hot Encoding

This process converts categorical labels into binary numerical representations. For example, if the labels are Normal and DDoS, the encoding result would be: Normal → [1, 0, 0], and DDoS → [0, 1, 0].

d. Feature Selection

Feature selection is performed using the Random Forest algorithm, based on each feature's impact on the reduction of Gini Impurity [13], [14]. The formula for Gini Impurity is:

$$G = 1 - \sum_{i=1}^{n} p_i^2 \tag{2}$$

Features that contribute significantly to classification are retained, while less relevant features are eliminated. In this stage, the Random Forest Feature Importance approach is used to identify the most contributive attributes for attack detection. From a total of 80 features in the CICDDoS2019 dataset, the top 20 most important features are selected based on their average Gini Importance scores.

e. Data Splitting

The dataset is split into two parts: 80% for training data and 20% for testing data. The training data is used to train the model, while the testing data is used to evaluate model performance [5].

3.3 Deep Learning

Deep Learning is a subset of machine learning that utilizes artificial neural networks with multiple layers to extract and understand complex patterns from data [15]. These networks are capable of learning from data in an end-to-end manner. Activation functions such as ReLU and optimization algorithms like Adam are standard practices in modern deep learning implementations [28].

3.4 Transformer

The Transformer is an architecture based on self-attention mechanisms and is particularly effective in processing sequential data. Introduced by Vaswani et al., this architecture has since been widely adopted in intrusion detection and cybersecurity analysis [15], [16]. Key components include Multi-Head Attention, Positional Encoding, and Feedforward Layers.

Scaled Dot-Product Attention Formula:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{3}$$

3.5 Evaluation Metrics

Table 1. Evaluation Metrics

Metric	Formula	Explanation
Accuracy	$\frac{TP + TN}{TP + TN + FP + FN}$	Proportion of correct predictions out of all data
Precision	$\frac{TP}{TP + FP}$	How accurate is the model when predicting positives
Recall	$\frac{TP}{TP + FN}$	The model's ability to detect all actual positive cases
F1-Score	$\frac{2 \times (Precision \times Recall)}{Precision + Recall}$	Harmonic mean of precision and recall

4. Results and Analysis

4.1 Model Training Results

The Transformer model proposed in this study was trained using the CICDDoS2019 dataset. The training process was conducted over 10 epochs, during which the loss value demonstrated a significant downward trend. This indicates that the model successfully achieved stable learning from the training data. Details of the loss and accuracy values throughout the training process are illustrated in Fig. 2.

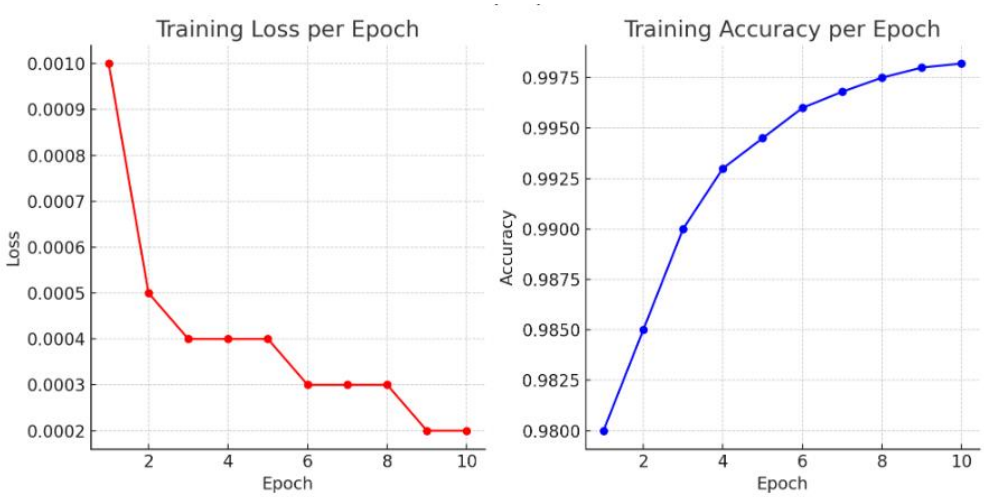

Fig. 2 Model Training Results

The following graph presents the training results based on the provided data: the left

graph shows a consistent decrease in the loss value at each epoch, indicating that the model increasingly minimized the prediction error. The right graph shows an upward trend in accuracy, approaching a maximum value of 0.9982 at the 10th epoch. This trend suggests that the Transformer model was effectively trained without signs of overfitting within the 10-epoch training period. After training was completed, the model was evaluated using the testing dataset. Evaluation was conducted by calculating commonly used classification metrics in the domain of cyberattack detection, including accuracy, precision, recall, and F1-score. The evaluation results are presented in Table 2.

Table 2. Evaluation results

Metric	Value
Accuracy	0.9982
Precision	0.9980
Recall	0.9983
F1-Score	0.9982

The metric values above indicate that the Transformer model demonstrates exceptionally high performance in classifying network traffic as either benign or DDoS attacks. With an accuracy of 99.82%, the model is capable of detecting attacks with remarkable precision and minimal error.

4.2 Feature Selection Results

The results of the feature selection process are presented in Figure 3, which displays the top 20 features based on their importance scores. Features such as Flow Duration, Fwd Packet Length Max, and Total Backward Packets exhibit high correlation with DDoS detection. The use of these selected features effectively reduced the model's complexity without significantly compromising classification accuracy, as shown in Fig. 3.

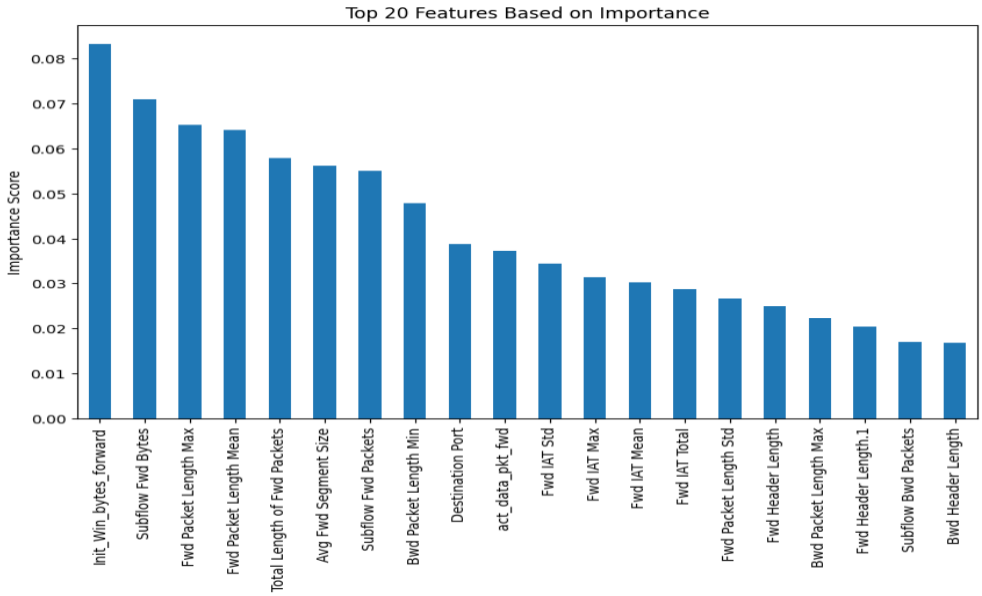

Fig. 3 Visualization of the Top 20 Most Important Features Based on Random Forest Importance

4.3 Confusion Matrix Analysis

To assess the model's performance in greater detail, a **confusion matrix** was used, as shown in Fig. 4.

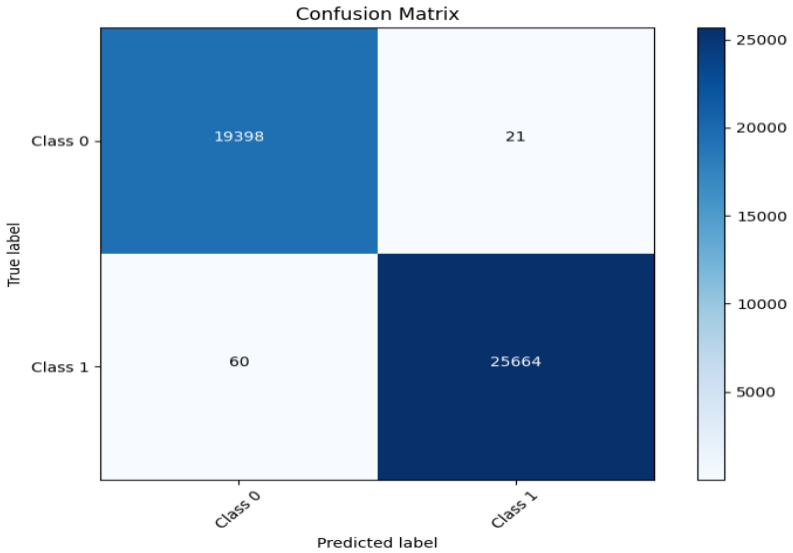

Fig. 4 Confusion Matrix of the Classification Results

Based on the confusion matrix above, TP 25,664 instances of DDoS traffic were correctly classified, and TN 19,398 benign traffic instances were correctly identified. FP obtained 21 benign instances that were misclassified as DDoS, indicating a very low false alarm rate. FN has 60 DDoS instances that were not detected by the model. These low misclassification values reinforce the reliability of the Transformer model in the task of intrusion detection.

4.4 Comparison with Previous Studies

The performance of the Transformer model is compared with several approaches proposed in previous studies. Table 3 presents the comparison results. Between the proposed method and other approaches.

Table 3. Performance Comparison with Previous Studies

Method	Accuracy	F1-Score	Reference
Random Forest + Adaboost	~94%	~93%	[1]
Deep Q-Network (DQN)	96%	-	[2]
LSTM-CNN Hybrid	97.1%	97.0%	[3]
Transformer	**99.82%**	**99.82%**	Proposed Study

The performance of the Transformer model has been proven to significantly surpass that of previous approaches. This indicates that the self-attention mechanism in the Transformer architecture is highly effective in identifying the complex and diverse patterns

characteristic of DDoS attacks.

4.5 Implications and Limitations

The findings of this study suggest that the Transformer architecture holds substantial potential for application in machine learning-based network attack detection systems. Nevertheless, the study presents certain limitations. Firstly, the dataset used comprises simulated data and has not yet been tested in a real-time production network environment. Secondly, the complexity of the Transformer model may introduce computational overhead if not properly optimized. Future research can focus on inference time optimization and validating the model in real-world network settings.

5. Conclusion

This study presented a Transformer-based model for detecting DDoS attacks using the CICDDoS2019 dataset with several stages, including data preprocessing (comprising data cleaning, normalization, and one-hot encoding), feature selection using the Random Forest algorithm, data splitting (80% for training and 20% for testing), Transformer model training, and performance evaluation. The evaluation results demonstrate that the Transformer model achieved an accuracy of 99.82%, a precision of 99.80%, a recall of 99.83%, and an F1-score of 99.82%.

These outcomes indicate outstanding performance and significantly outperform prior methods such as Random Forest, DQN, and hybrid LSTM-CNN models. The self-attention mechanism within the Transformer architecture has proven effective in capturing the complex patterns inherent in network traffic data. Furthermore, the preprocessing and feature selection stages played a critical role in improving detection efficiency and accuracy by reducing data dimensionality and eliminating irrelevant features. This underscores the importance of input data quality in the success of deep learning models for anomaly detection in networks. Therefore, the Transformer presents a highly promising approach for implementation in AI-based intrusion detection systems, particularly in addressing large-scale cyber threats such as DDoS attacks.

Future studies can be extended to real-time environments to assess the model's robustness and efficiency under dynamic network conditions. Additionally, further research may focus on integrating the model with adaptive detection systems capable of automatically adjusting to emerging threats in an ever-evolving cybersecurity landscape.

References

[1] M. F. Saiyedand and I. Al-Anbagi, "Deep Ensemble Learning With Pruning for DDoS Attack Detection in IoT Networks," in IEEE Transactions on Machine Learning in Communications and Networking, vol. 2, pp. 596-616, 2024, doi: 10.1109/TMLCN.2024.3395419

[2] S. Haribalaji and P. Ranjana, "Distributed Denial of Service (DDOS) Attack Detection Using Classification Algorithm," 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ADICS58448.2024.10533510.

[3] L. Bagdadi and B. Messabih, "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, pp. 1868–1878, Dec. 2024. http://doi.org/10.11591/ijeecs.v34.i3.pp1868-1878.

[4] J. Boonchai, K. Kitchat and S. Nonsiri, "The Classification of DDoS Attacks Using Deep Learning Techniques," 2022 7th International Conference on Business and Industrial Research (ICBIR), Bangkok, Thailand, 2022, pp. 544-550, doi: 10.1109/ICBIR54589.2022.9786394.

[5] W. S. Lestari, "Deteksi serangan DDoS menggunakan Q-Learning," JATISI (Jurnal Teknik Informatika dan Sistem Informasi), vol. 9, no. 1, pp. 648–658, Mar. 2022. https://doi.org/10.35957/jatisi.v9i1.1473
[6] M. N. Faiz, O. Somantri, and A. W. Muhammad, "Rekayasa fitur berbasis machine learning untuk mendeteksi serangan DDoS," Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI), vol. 11, no. 3, pp. 176–182, Aug. 2022. [Online]. Available: https://doi.org/10.22146/jnteti.v11i3.3423
[7] M. Ouhssini, A. Karim, E. Agherrabi, and M. Akouhar, "DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing," Journal of King Saud University - Computer and Information Sciences, vol. 36, no. 2, p. 101938, Feb. 2024. [Online]. Available: https://doi.org/10.1016/j.jksuci.2024.101938.
[8] D. Tymoshchuk et al., "Detection and Classification of DDoS Flooding Attacks by Machine Learning," arXiv preprint, arXiv:2412.18990, 2024.
[9] Maslan, A,. et al., "Feature selection for DDoS detection using classification machine learning techniques," IAES International Journal of Artificial Intelligence (IJ-AI), 2020.
[10] M. Salunke, et al., "A Prediction and Classification Process for DDoS Attacks Using Machine Learning," International Conference on Computing Communication Control and Automation, 2023.
[11] D. B. Satmoko, et al., "Peningkatan Akurasi Pendeteksian Serangan DDoS Menggunakan Multiclassifier Ensemble Learning dan Chi-Square," 2018.
[12] R. G. Gunawan, et al., "Pendekatan Machine Learning Dengan Menggunakan Algoritma Xgboost (Extreme Gradient Boosting) Untuk Peningkatan Kinerja Klasifikasi Serangan Syn," Jurnal CoSciTech (Computer Science and Information Technology), 2022.
[13] Prima, F., Dylan, L., & Gunawan, A. A. S. (2023). Comparison of Machine Learning Models for Classification of DDoS Attacks. 1–6. https://doi.org/10.1109/icoris60118.2023.10352232
[14] Najar, A. A., Naik, S. M., Lone, F. R., & Nazir, A. (2024). A novel CNN-based approach for detection and classification of DDoS attacks. Concurrency and Computation: Practice and Experience. https://doi.org/10.1002/cpe.8157
[15] Cheng, J. R., Li, X., Xu, X., Tang, X., & Sheng, V. S. (2023). A Modified PointNet-Based DDoS Attack Classification and Segmentation in Blockchain. Computer Systems: Science & Engineering, 47(1), 975–992. https://doi.org/10.32604/csse.2023.039280
[16] Kumar, A. I., & Ishigaki, G. (2024). Advanced DDoS Attack Classification using Ensemble Model with Meta-Learner. 1–2. https://doi.org/10.1109/icccn61486.2024.10637575
[17] Mulyani, S. H., Suwarto, Hamzah, Wijaya, R., Rodiyah, & Adelia, W. (2024). Fake News Detection in Health Domain Using Transformer Models. International Journal of Informatics and Computation, 6(2), 56–63. https://doi.org/10.35842/ijicom.v6i2.89
[18] Cheng, J. R., Li, X., Xu, X., Tang, X., & Sheng, V. S. (2023). A Modified PointNet-Based DDoS Attack Classification and Segmentation in Blockchain. Computer Systems: Science & Engineering, 47(1), 975–992. https://doi.org/10.32604/csse.2023.039280
[19] Sinha, S., & Degadwala, S. (2023). A Comprehensive Review on Multi-Class DDoS Attack Classification in IoT. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 313–318. https://doi.org/10.32628/cseit2361053
[20] Wathan, M. H., & Aziz, M. (2024). Establising CNN for Network Intrusion Detection: A Comparative Approach. International Journal of Informatics and Computation, 6(1), 40–43. https://doi.org/10.35842/ijicom.v6i1.69
[21] Sugiyatno. (2025). Honeypot Integration with Software-Defined Networking (SDN) for DDoS Attack Mitigation. International Journal of Informatics and Computation, 7(1), 40–50. https://doi.org/10.35842/ijicom.v7i1.101
[22] H. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," Journal of Computational Science, vol. 25, pp. 152–160, Jan. 2018, doi: https://10.1016/j.jocs.2017.03.006.
[23] R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Applying Deep Learning Approaches for Network Traffic Prediction," in Proc. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 2353–2358, doi: https://10.1109/ICACCI.2017.8126164.

[24] T. T. Nguyen, M. H. Phan, and M. Park, "A deep learning-based approach for intrusion detection using bidirectional LSTM in software-defined networking," Electronics, vol. 9, no. 6, pp. 1–18, 2020, doi: https://10.3390/electronics9060905.
[25] R. Roy, T. Chatterjee, and S. Das, "Lightweight CNN Models for Real-Time Intrusion Detection in IoT Networks," in 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2021, pp. 68–73, doi: https://10.1109/Confluence51648.2021.9377052.
[26] W. Lin, J. Wang, and Z. Zhang, "ViTranIDS: A Transformer-Based Network Intrusion Detection System Using Vision Transformer," Computers, vol. 11, no. 4, pp. 58–75, Apr. 2022, doi: https://10.3390/computers11040058.
[27] Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 602-622, Firstquarter 2016, doi: https://10.1109/COMST.2015.2487361.
[28] Mienye ID, Swart TG. A Comprehensive Review of Deep Learning: Architectures, Recent Advances, and Applications. Information. 2024; 15(12):755. https://doi.org/10.3390/info15120755.