Minimax Theory and its Applications
Volume 11 (2026), No. 4s, 952-958

Integrated CNN-LSTM Deep Learning Technique for Identifying DDoS Attacks on Distributed Network

K. Jeevan Pradeep [1], P. Raja Rajeswari [2]

[1]Research Scholar,Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. Email: jeevanpradeepsappi@gmail.com, ORCID:0000-0001-9388-2396
[2]Professor,Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. Email: rajilikhitha@kluniversity.in, ORCID:0000-0001-7383-2615

Abstract
One of the most catastrophic vulnerabilities to network security is a distributed denial-of-service (DDoS) assault. Among all network attacks, DDoS assaults are one of the most prevalent. Users who request services from those servers are inconvenienced as a result of these assaults, which bring about server failure. Because of this, an effective approach for detecting DDoS assaults was needed. Researchers have successfully employed deep learning and machine learning for recognizing DDoS assaults. Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM)are two popular deep learning algorithms, to create a novel deep learning classification approach in this work. The model was evaluated using the ISCX-IDS-2012 dataset. In comparison to earlier studies, the suggested model obtained the best accuracy of 98.39%.

Keywords: DDoS assaults, Deep learning, CNN, LSTM, ISCX-IDS-2012

1. Introduction

Networks are essential at this point because they perform a wide range of tasks, the most significant of which is resource sharing. Any connection between two or more nodes is referred to as a network, regardless of whether those nodes are computers, servers, mobile phones, etc. The world's computer networks have merged to create essential technology known as the Internet. However, the Internet is now more susceptible to various types of assaults, with Distributed Denial of Service (DDoS) attacks being the most dangerous cyber-attacks [1] [Bharot, N. et al. 2019]. In the Event of DoS and DDoS, the attacker attempts to overwhelm the host's service, rendering it unreachable to authorized users [2] [Baykara, M., Das, R. 2017]. DoS attacks often originate from a single infected device or virtual machine, whereas while DDoS attacks use several compromised computers or simulated machines to overload the intended systems [3] [Ahmed Sardar Ahmed, and Zafer ALBAYRAK, 2021]. Defending against a DDoS assault becomes exceedingly challenging even with a standard security system in place due to the high volume of simultaneous strikes and the rapid advancement of the attack [4] [Özalp, A. N et al., 2022]. DDoS assaults attempt to mimic regular traffic, which has contributed to their rapid rise. The major causes of this rise are the ease and simplicity with which they can be implemented, the low technical knowledge required on the attacker's side, and the availability of several platforms and attack coordination software [5] [Lima Filho, F. S. De et al., 2019].

An essential tool for protecting networks from malicious attacks is an intrusion detection system (IDS). IDS has embraced two popular techniques: anomaly-based approaches and signature-based detection. Zero-day attacks cannot be detected by signature-based detection, despite its high detection rates and low false alarm rates. On the other hand, anomaly-based detection has the potential to identify brand-new assaults that have never been observed before, but it continues to generate a lot of false positives. Consequently, further development of anomaly-based detection methods is necessary to improve network security. Fig.1 Depicts the DDoS Attack Scenario.

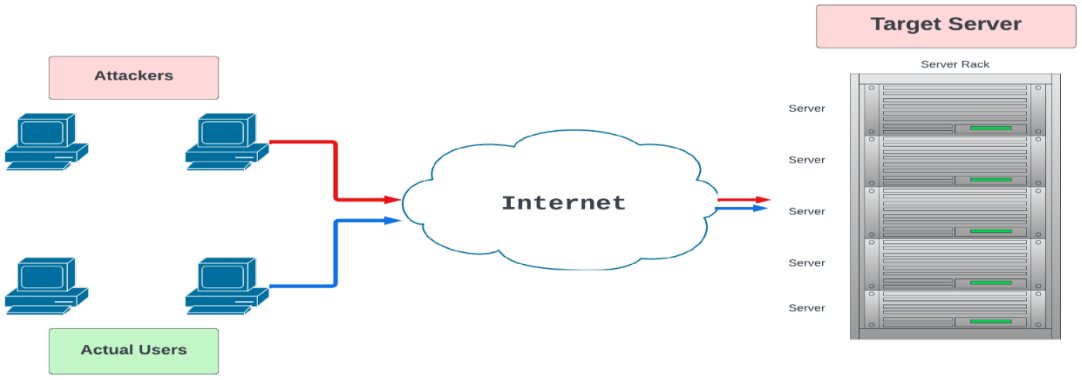

Fig 1. DDoS Attack Scenario

DDoS assaults can be divided into two categories: the application layer and the network layer [6] [Seifousadati et al. 2021]. Security hackers are constantly developing new methods to bypass defenses and detection. Recently, deep learning models have been employed to identify and detect security issues, significantly enhancing their likelihood of success [7][AhmedIssaAlbayrak, 2023]. A novel discipline called deep learning (DL) has just arisen, inspired by neural networks that mimic the human brain [8] [Aytaç, T. et al. 2020]. In this research, we propose a novel DL model that combines the Long Short-Term Memory (LSTM) neural network for sequence prediction with the Convolutional Neural Network (CNN) layers for feature extraction from input data [9] [Tasdelen, A., Sen, B., 2021]. The suggested model's performance in comparison to CNN and LSTM was evaluated using four metrics: accuracy, precision, recall, and F1 score. The model outperformed other state-of-the-art models in terms of accuracy on the same dataset, known as ISCX-IDS-2012.
The following sections of the paper will be covered and finished as follows: Section 2: completion of the pertinent tasks and discussion. Section 3 discusses the study's methods and the ISCX-IDS-2012 dataset. Section 4 contains information on the evaluation criteria. Section 5 provides an explanation of the paper's conclusions and its investigations. Section 6 concludes the paper and discusses future directions.

2. Related Work

Predicting DDoS assaults has advanced remarkably with the advent of new machine learning and deep learning approaches. Yusof et al. [10] developed a feature selection method that combined Consistency Subset Evaluation (CSE) with DDoS Characteristic Features (DCF) in 2017, resulting in an effective machine learning-based intrusion detection system.In the same year, Kushwah and Ali [11] used an artificial neural network (ANN) with black hole optimization to identify DoS assaults in cloud computing. In 2018, Derakhsh et al. [12] proposed a genetic algorithm (GA)-based technique for DDoS attack identification in cloud platforms. They improved the performance of theNaives classifier using GA and evaluated the algorithms with the open-source Artificial Intelligence platform. Hoon, K. S,et al.[13].
In 2019, Anjum and Shreedhara [14] suggested a semi-supervised machine learning system that combined supervised and unsupervised learning methods to enhance DDoS attack detection performance compared to existing algorithms.Neural networks have also been explored as a promising choice for DDoS detection. Mukhametzyanov et al. [15] conducted research in this area. Afsaneh et al. [16] proposed a new method for DDoS attack identification in the context of Software-Defined Networking (SDN). They can be divided into three steps: collector, entropy-based, and classification. They used three sets of data to obtain better results. Panda et al. [17] proposed a Naïve Bayes (NB) solution for the KDD Cup and demonstrated that it can be implemented to obtain a lower false alarm rate, faster calculation, and that it is also cheaper than some of the current IDS solutions.Vanlalruata Hnamte and Jamal Hussain [18] have introduced a deep convolutional neural network (DCNN) framework trained on massive amounts of data in 2023 for the effective classification of the normal and anomalous behavior in network traffic.
Rami J. Alzahrani and Ahmed Alzahrani [19] experimented with six different types of ML algorithms and achieved the best accuracy using Decision Tree (DT) and Random Forest (RF) algorithms.In 2021, Gopal Singh Kushwah and Virender Ranga [20] introduced a hybrid machine learning-based technique by combining the extreme learning machine (ELM) model with the black hole optimization algorithm. They demonstrated its performance superiority over other techniques.
Muhammad Ashfaq Khan and Yangwoo Kim [21] utilized Long Short-TermMemoryto find temporal features, and AE to find worldwide characteristics. They evaluated their approach on the publicly existing ISCX-UNB dataset.In 2021, P Rajesh Kanna and P Santhi [22] proposed an optimized CNN (OCNN) and Hierarchical Multi-scale LSTM (HMLSTM) unified model, enabling effective extraction and learning of spatial-temporal features for DDoS attack classification.

3. Methodology

3.1. Dataset

The ISCX-IDS-2012 dataset, created by the University of New Brunswick's Information Security Centre of Excellence [Shiravi, A.; Shiravi, H.; Tavallaee, M.; Ghorbani, A.A, 2012][23], encompasses both types of assaults. It includes application layer DoS assaults, which are more challenging to identify, in addition to network layer DoS attacks, which are simpler to identify. The data set includes several attack scenarios, such as DDoS attacks using IRC botnets and HTTP DoS attacks. Researchers can access labeled network traces with full packet payloads in pcap and matching profiles. The seven-day data collection period records both good and bad traffic on the network, providing a useful set of data to test and improve intrusion detection systems.Fig.2. Depicts the CNN-LSTM Process.

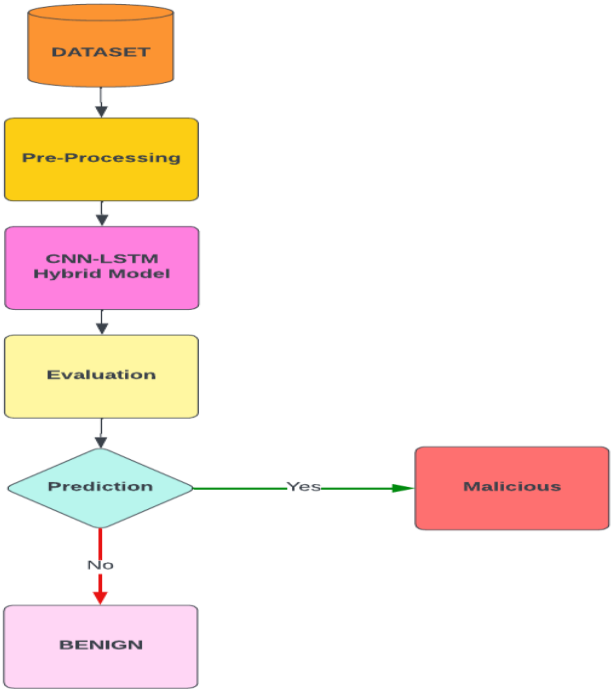

Fig.2. CNN-LSTM Process

3.2. Experimental Setup

In the data loading and preparation phase, the code loads the network traffic data sets from CSV files, comprising both normal and attack data sets. The inputs (X) and outputs (Y) are separated by irrelevant columns, which are dropped.The inputs are then standardized, ensuring they have a zero mean and unit variance, which is a common technique used to normalise the data and improve model performance.

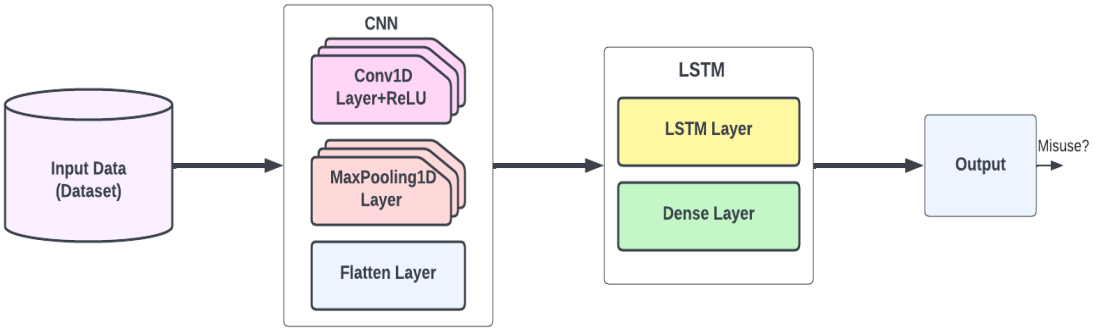

Fig.3 : CNN-LSTM Hybrid Model Architecture

A simple architecture of the CNN-LSTM is depicted in Fig.3. Which comprises two major components CNN and LSTM. The LSTM layers in this architecture are used to create the Sequences at each time setup after the input has first been examined by CNN.

The model architecture is a sequential deep learning network traffic classification model. It has a few layers: Conv1D, MaxPooling1D, Bidirectional LSTM, Flatten and Dense. The Conv1D layer has a kernel size of three, 64 filters, and a ReLU activation function. To capture local patterns in the data, the Conv1D layer is coupled to the data using 64 filters, a kernel size of 3, and an activation function of ReLU. Binary cross-entropy loss and the Adam optimizer are used to train the model. Accuracy and performance of the model is logged during 40 epochs in the training log.

The test set is used to test it, and the model's performance is assessed. The classification accuracy is assessed by creating a confusion matrix that displays the numbers of true positives, true negatives, false positives, and false negatives. The Receiver Operating Characteristic (ROC) curve is the source of the Area Under the Curve (AUC), a metric that evaluates how well the model distinguishes between positive and negative examples. Plots the accuracy and loss to confirm the model's performance during training and to understand the model's stability and convergence. Finally, the trained model is stored for future use allowing for easy access and implementation in real-life applications.

Overall, the code covers important steps such as data preprocessing, model architecture, training, evaluation, and visualization, demonstrating its effectiveness in network traffic classification.
1. Loss: The value of loss is measured when the model is performing during training. As the model shrinks across epochs, it becomes closer and more accurate at predicting the solution and approaches an ideal solution as it shrinks. After 40 epochs, the training set's loss drops from 0.3122 to 0.0673, while the validation set's loss drops from 0.1468 to 0.0836.
2. Accuracy: The accuracy is the ability of the model to correctly classify the data. The training accuracy increases from 94.95% to 98.54% throughout the epoch, and the validation accuracy improves from 96.18% to 98.39%. These findings show that the model is successfully identifying patterns in the simulated data and can generalize new data.
3. Overfitting: An Approach overfits when it fails to generalize to fresh data. Results show no overfitting. Since both the Learning and validation accuracies are similar, the model is not over-optimizing the learning data. The model can also generalize effectively due to the reducing validation loss.
4. Convergence: The model's performance converges after 40 epochs. Training may not enhance loss and accuracy because they are stable. The model learns from training data and performs well when applied to new data, as evidenced by the comparable trends in validation loss and accuracy.
Overall, these observations highlight the model's effective learning and generalization capabilities, absence of significant overfitting, and convergence towards an optimal solution. Fig.4 depicts Accuracy of CNN-LSTM for DDoS attacks Identification on ICSX-IDS 2012 Dataset.

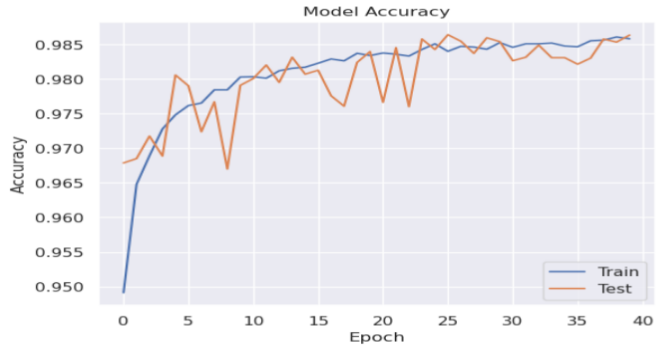

Fig.4: Accuracy of CNN-LSTM for DDoS attacks Identification on ICSX-IDS 2012 Dataset.

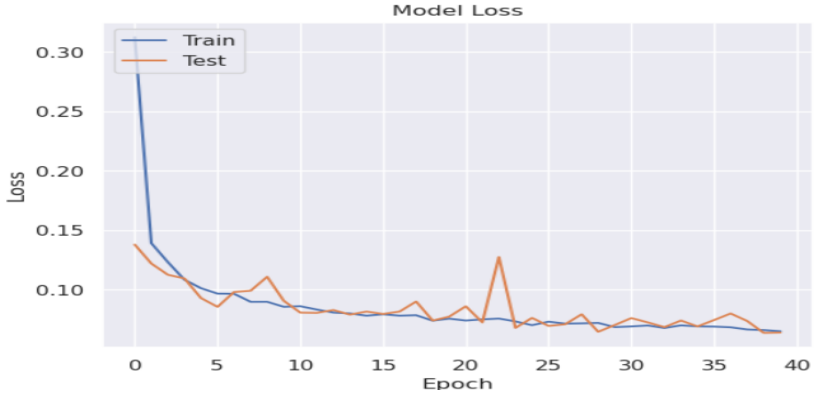

Fig.5: Loss Curve of CNN-LSTM for DDoS attacks Identification on ICSX-IDS 2012 Dataset.

To better visualize the performance of the model, it would be helpful to plot the training and validation loss and accuracy curves over the epochs. This can help identify model learning difficulties like Overfitting and under fitting. Fig.5. depicts Loss Curve of CNN-LSTM for DDoS attacks Identification on ICSX-IDS 2012 Dataset.
By displaying precision, recall, and F1-score for each class (Normal and Attack), together with support counts, the classification report offers a thorough examination of the model's performance. Here is an elaboration of the classification report depicted in Table.1in a table format:

Table 1. Classification Report based on Precision, Recall, F1-Score and Support

Class	**Precision**	**Recall**	**F1-Score**	**Support**
Normal	0.985	0.983	0.984	9932
Attack	0.983	0.985	0.984	10063
Accuracy	–	–	**0.984**	19995
Macro Avg	0.984	0.984	0.984	19995
Weighted Avg	0.984	0.984	0.984	19995

The classification report evaluates the model's "Normal" and "Attack" network traffic categorization performance. The model's accuracy of 0.985 indicates that 98.5 percent of occurrences classed as Normal are True Positives. The model properly identifies 98% of "Normal" cases, according to its recall of 0.983. "Normal" class F1-score is 0.984. The test dataset has 9,932 "Normal" incidences.
The model achieves a precision of 0.983 for the “attack” class, which means that it correctly predicts the “attack” class 98.3% of the time. The model accurately identifies 98.53 % of the real "attack" cases. "Attack" class F1-score is 0.984. There are 10,063 "attack" instances in the test set. The model classifies 98.39 percent of the test dataset with 0.984 accuracy. The macro average shows precision, recall, and F1-scores of 0.984 across both classes. Precision, recall, and F1-scores are 0.984 for the weighted average, which accounts for class support counts. The model classifies network traffic accurately with high accuracy, recall, and F1-scores for both "normal" and "attack" classifications. The model's overall accuracy and consistent performance across classes show its resilience in network traffic categorization tasks.

4. Results and Discussion

4.1 Results

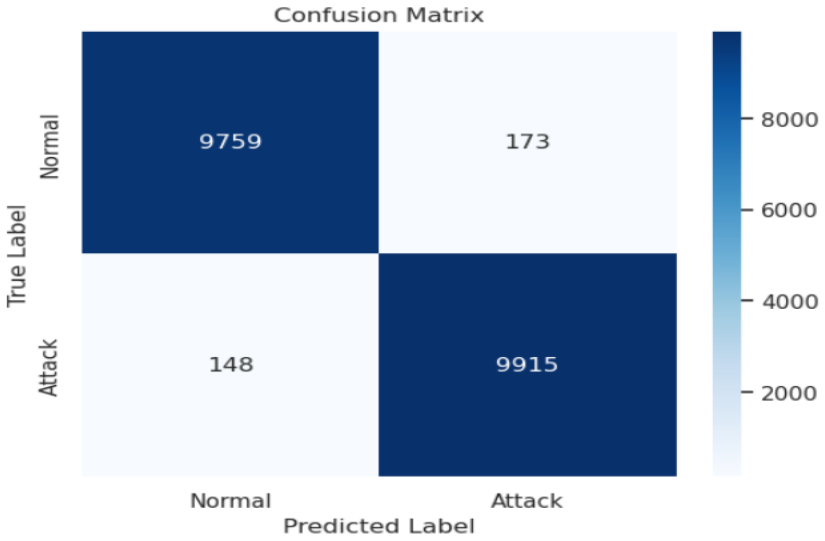

Fig.6 Confusion Matrix Obtained for CNN-LSTM using ISCX-IDS 2012 Dataset

In the proposed study, a GPUT4-x2 GPU was used to execute the code for network traffic categorization. This was done on the Kaggle platform. The procedure for training the model produced some encouraging results in terms of the evaluation of its accuracy and performance. The execution time for each epoch during training was around 19 seconds on average; however, this might have varied greatly depending on the hardware and software combination.
The performance of the classification model was evaluated by using confusion matrix and identifying the strengths to know how well it is performing in the classification of different classes. It displayed the distribution of instances correctly/incorrectly classified that provided a comprehensive picture of the model's predictive capability. The results showed that the classification was high, with 9,915 true positives and 9,759 true negatives, which showed that the model was able to distinguish “Normal” and “Attack” categories. In addition, the relatively low number of false positives (173) and false negatives (148) indicate that the model was able to achieve a high degree of accuracy in its predictions while minimizing classification errors. A complementary measure for the model used outside the confusion matrix was the Area Under the Receiver Operating Characteristic Curve (AUC-ROC) which was used to assess the discrimination between the two classes for different classification thresholds. This model can classify the positive and negative cases well, with an AUC of 0.9776305854138537. This score is for the success of the model in classification problems involving network traffic.

4.2 Discussion

Model performing well. The model has learnt to differentiate between the "Normal" and "Attack" cases as can be observed in the confusion matrix. The model's dependability is enhanced by its low misclassification rate. The AUC value obtained for the model was 0.977, indicating high discrimination ability between the positive and negative cases, which means high discriminating power and capturing of the underlying patterns and characteristics of the data. The model provides good accuracy and AUC value, thus demonstrating its predictive capability of "Normal" or "Attack" network traffic type. These results can be utilized to discover and manage safety issues in networks. It is important to be aware that performance and results from the model can vary

depending on the data set, hardware/software environment and complexity of the classification task. For additional datasets or deployment scenarios, more study could be required to assess the model's performance.

Conclusion

In this research, traffic is classified as "Normal" or "Attack" using a deep learning model. The model performed exceptionally well, correctly identifying both kinds of cases. The attacks included in the dataset, ISCX-IDS-2012, were of many types, allowing this dataset to be tested extensively. The model was impressive in its performance and did not seem to overfit, it seemed to generalize well. The results showed its capability in classification task between “Normal” and “Attack” instances, contributing to bolster network security. The model needs to be further evaluated and tested with different datasets for its effectiveness. In conclusion, the proposed deep learning model has the potential to improve the performance of intrusion detection systems and boost network security.

References

1. Bharot, N., Suraparaju, V., & Gupta, S. (2019). DDoS attack detection and clustering of attacked and non-attacked VMs using SOM in cloud network. In Advances in Computing and Data Sciences: Third International Conference, ICACDS 2019, Ghaziabad, India, April 12–13, 2019, Revised Selected Papers, Part II 3 (pp. 369-378). Springer Singapore.
2. Baykara, M., & Das, R. (2017). A novel hybrid approach for detection of web-based attacks in intrusion detection systems. International Journal of Computer Networks and Applications, 4(2), 62-76.
3. ISSA, A. S. A., & ALBAYRAK, Z. (2021, August). CLSTMNet: A Deep Learning Model for Intrusion Detection. In Journal of Physics: Conference Series (Vol. 1973, No. 1, p. 012244). IOP Publishing.
4. Özalp, A. N., Albayrak, Z., Çakmak, M., & Özdoğan, E. (2022, June). Layer-based examination of cyber-attacks in IoT. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-10). IEEE.
5. Lima Filho, F. S. D., Silveira, F. A., de Medeiros Brito Junior, A., Vargas-Solar, G., & Silveira, L. F. (2019). Smart detection: an online approach for DoS/DDoS attack detection using machine learning. Security and Communication Networks, 2019, 1-15.
6. Seifousadati, A., Ghasemshirazi, S., & Fathian, M. (2021). A Machine Learning approach for DDoS detection on IoT devices. arXiv preprint arXiv:2110.14911.
7. Issa, A. S. A., & Albayrak, Z. (2023). Ddos attack intrusion detection system based on hybridization of cnn and lstm. Acta Polytechnica Hungarica, 20(2), 1-19.
8. Aytaç, T., Aydın, M. A., & Zaim, A. H. (2020). Detection DDOS attacks using machine learning methods.
9. Tasdelen, A., & Sen, B. (2021). A hybrid CNN-LSTM model for pre-miRNA classification. Scientific reports, 11(1), 14125.
10. Yusof, A. R. A., Udzir, N. I., Selamat, A., Hamdan, H., & Abdullah, M. T. (2017, November). Adaptive feature selection for denial of services (DoS) attack. In 2017 IEEE Conference on Application, Information and Network Security (AINS) (pp. 81-84). IEEE.
11. Kushwah, G. S., & Ali, S. T. (2017, August). Detecting DDoS attacks in cloud computing using ANN and black hole optimization. In 2017 2nd International Conference on Telecommunication and Networks (TEL-NET) (pp. 1-5). IEEE.
12. Derakhsh, A. M., Daneshjoo, P., & Delara, C. (2018). Using Genetic Algorithm to Improve Bernoulli Naïve Bayes Algorithm in Order to Detect DDoS Attacks in Cloud Computing Platform. International Journal Of Science And Engineering Investigations, 7.
13. Hoon, K. S., Yeo, K. C., Azam, S., Shunmugam, B., & De Boer, F. (2018, January). Critical review of machine learning approaches to apply big data analytics in DDoS forensics. In 2018 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-5). IEEE.
14. Anjum, M., Shreedhara, K. S.: Performance Analysis of Semi-Supervised Machine Learning Approach for DDoS Detection. Int. J. Innov. Res. Technol., 6 (2), 2019, pp. 144-147
15. Mukhametzyanov, F. F., Katasev, A. S., Akhmetvaleev, A. M., & Kataseva, D. V. (2019). The neural network model of DDoS attacks identification for information management. International Journal of Supply Chain Management, 8(5), 214-218.
16. Banitalebi Dehkordi, Afsaneh & Soltan Aghaei, Mohammad & Zamani Boroujeni, Farsad. (2021). The DDoS attacks detection through machine learning and statistical methods in SDN. The Journal of Supercomputing. 77. 10.1007/s11227-020-03323-w.
17. Panda, Mrutyunjaya & Patra, Manas. (2007). Network intrusion detection using naive bayes. 7.
18. Hnamte, V., & Hussain, J. (2023). Dependable Intrusion Detection System using Deep Convolutional Neural Network: A Novel Framework and Performance Evaluation Approach. Telematics and Informatics Reports, 100077.
19. Alzahrani, R. J., & Alzahrani, A. (2021). Security analysis of ddos attacks using machine learning algorithms in networks traffic. Electronics, 10(23), 2919.

20. Kushwah, G. S., & Ranga, V. (2021). Distributed denial of service attack detection in cloud computing using hybridextreme learning machine. Turkish Journal of Electrical Engineering and Computer Sciences, 29(4), 1852-1870.
21. Khan, M. A., & Kim, Y. (2021). Deep Learning-Based Hybrid Intelligent Intrusion Detection System. Computers, Materials & Continua, 68(1).
22. Kanna, P. R., & Santhi, P. (2021). Unified deep learning approach for efficient intrusion detection system using integrated spatial–temporal features. Knowledge-Based Systems, 226, 107132.
23. Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. computers & security, 31(3), 357-374.