Library Progress International
Vol.44 No.3, Jul-Dec 2024: P.5564-5572

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Validation of Deep Learning-based Hybridization Model for DDoS Attack Detection with Performance Metrics Comparison

Dhananjay Shripad Rakshe[1], Dr. Sweta Jha[2], Dr. Pawan R. Bhaladhare[3]

[1]School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India, Email: jay.rakshe19@gmail.com
[2]School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India, Email: sweta.jha@sandipuniversity.edu.in
[3]School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India, Email: pawan.bhaladhare@sandipuniversity.edu.in
* jay.rakshe19@gmail.com

How to cite this article: Dhananjay Shripad Rakshe, Sweta Jha, Pawan R. Bhaladhare (2024) Validation of Deep Learning-based Hybridization Model for DDoS Attack Detection with Performance Metrics Comparison. *Library Progress International*, 44(3), 5564-5572.

Abstract
Separating fraudulent from valid traffic is the main difficulty in a Dispersed Denial-of-Service (DDoS) attack. DDoS assaults are deliberate attempts to obstruct any computer, network, or support system from operating normally by flooding the target or nearby resources with an enormous volume of Internet traffic. This type of attack can be a single-source attack or a complicated multi-source attack, among other variations. In this study, a novel deep learning classification method was proposed by hybridizing two common deep learning algorithms; DDoS attack detection using intelligent deep neural unified sequential memory networks (IDNUSMN). The model was tested on the NSL-KDD dataset. Z-score normalization was used as a preprocessing step is used to convert data into standard normal distribution. The proposed method is implemented using Python software. The IDNUSMN is compared to the other traditional algorithms. According to the results, the IDNUSMN outperformed the others in terms of F1-score (98.35%), precision (98.18%), recall (98.5%), and accuracy (98.25%). The study's validation results demonstrate how effective the hybridization model based on deep learning is in detecting DDoS attacks.

Keywords: Attack Detection, Intelligent Deep Neural Unified Sequential Memory Networks (IDNUSMN), Distributed Denial-of-Service (DDoS)

1. Introduction

A malevolent actor initially investigates several susceptible systems via the Internet to take control of and exploit them to produce huge traffic. Afterward, it floods the target system with the created traffic, interfering with its regular functions [1]. Since IoT devices have limited resources, such as CPUs (Central processing units) and backup memory, they are especially vulnerable to DDoS attacks. There's a possibility that this vulnerability will be exploited and compromised as Internet of Things devices to be used in DDoS assaults if it isn't corrected. DDoS assaults are not new. They have existed for an extended period [2]. DDoS assaults fall primarily into two categories: bandwidth depletion, in which an attacker aims to overwhelm the target node with a massive volume of resource depletion, in which an attacker aims to destroy a victim node's vital resources to keep a legitimate user from utilizing them, and traffic to stop valid traffic from reaching the victim node [3]. DDoS attacks are a common kind of cyber attack in which network users' services are created in an unauthorized and disturbed manner. The attackers employ this tactic to prevent legitimate users from accessing services. These DDoS attacks are used by attackers to prevent access for legitimate users. Here, the attackers heavily tax the public network services that the target server offers. A network of several hosts on the Internet is referred as a botnet, and it is used to send traffic to users or victims. [4]. DDoS attacks are thought to be a kind of hostile assault on cloud systems that

causes several serious issues. These attacks produce a lot of network traffic with transmitted packets in it. On the network, frequent users who wish to access services that don't meet their needs are in jeopardy. DDoS defense techniques classify packets as either malicious or benign [5]. When a DDoS attack occurs, a network starts distributing its resources to meet the demands. However, a network will stop serving requests whenever the volume of requests exceeds what it can handle. Any request, even from authorized users, would be turned down, which would interfere with the IoT's ability to deliver services [6]. The management of resources during the attack and the flow of multilayer information are both part of the solution. It provides massive online data storage capabilities and is accessible from anywhere in the world at any time [7]. DDoS attack detection has limitations, such as accuracy issues brought on by false positives and false negatives, continuous challenges in adjusting to new attack and evasion techniques used by attackers, and significant resource requirements for maintaining efficient detection capabilities. Using machine learning to improve detection algorithms for more accuracy, integrating real-time threat intelligence to quickly respond to new attack patterns, and expanding infrastructure to effectively manage demands are all required. This paper proposes the hybrid of two well-known deep learning algorithms to build intelligent deep neural unified sequential memory networks (IDNUSMN), a novel classification method for DDoS attack prediction.

Organization

The work is categorized into related work in section 2, the methodology could be explained in section 3, experimental results explained in section 4, and the conclusion is explained in section 5.

2. Related works

For several online attacks, including phishing, malware, rebate manipulations, spam, and DDoS attacks [8]. They suggested tackling the problem of DDoS attacks with several machine learning techniques, such as Decision Tree (DT), Naïve Bayes (NB), Support Vector Machine (SVM), and Artificial Neural Network (ANN). The fields of computer security and related fields profited immensely from their validation.

They provided a powerful fuzzy and Taylor-elephant herd optimization (FT-EHO) method for DDoS attack detection that draws inspiration from deep belief network (DBN) classifiers [9]. FT-EHO employed a fuzzy classifier, the taylor series, and the elephant heart optimization algorithm to learn rules. The suggested FT-EHO's performance was assessed using accurate computer simulations.

DDoS attacks are routine operations that involve sending an overwhelming amount of Internet traffic to the target or the surrounding infrastructure. They recommended identifying abnormalities, and a contractive autoencoder-based deep learning model was proposed in [10]. After learning the typical traffic pattern from the compacted form of the input data, they utilized a stochastic threshold approach to identify the assault.

DDoS attacks were one of the new security and privacy threats associated with software-defined networking (SDN) [11]. They analyzed the performance of several classification techniques, such as Convolutional Neural Networks (CNN), DT, K-nearest neighbors (KNNs), SVMs and Multilayer Perceptron (MLP). Identified DDoS assaults in SDN systems could be greatly aided by the comparative analysis presented.

Intrusion Detection Models (IDM) were presented in [12] to detect Distributed DDoS attacks in the automotive domain. The suggested method uses the SVM classifier’s Radial Basis Function (RBF) kernel along with an extensive. Experimental simulations were used to validate the suggested architecture and show how well it can identify DDoS intrusions.

A Hybrid Convolutional Neural Network-Long-Short Term Memory (CNN-LSTM) model in SDN-based networks was proposed in [13] to identify slow DDoS attacks. Their hybrid CNN-LSTM model gives better results than typical machine learning models like l-Class Support Vector Machines (l-Class SVM) and other deep learning models like MLP.

Reducing the feature space lowers overfitting and the model's computation time, leading to the development of a new automatic detection methodology [14]. The suggested features and hyperparameters were supplied to several supervised learning techniques, including SVM, GB, DT, LR, and KNN. The right parameters for learning procedures and hyperparameter regulation improve the model.

The Lightweight Universal Communication and Information Device (LUCID) was offered in[15] to predict a practical deep learning DDoS detection system. That takes the advantage of CNN features. CNNs categorize the traffic patterns as either neutral or malignant.Our evaluation findingsdemonstrate that the suggested method was appropriate for efficient DDoS detection in operational contexts with limited resources.

3. Methodology

The dataset was collected from kaggle and preprocessed using z-score normalization. Intelligent deep neural unified sequential memory networks (IDNUSMN), a hybrid of two popular deep learning methods, for DDoS attack detection. Figure 1 shows an overall flow.

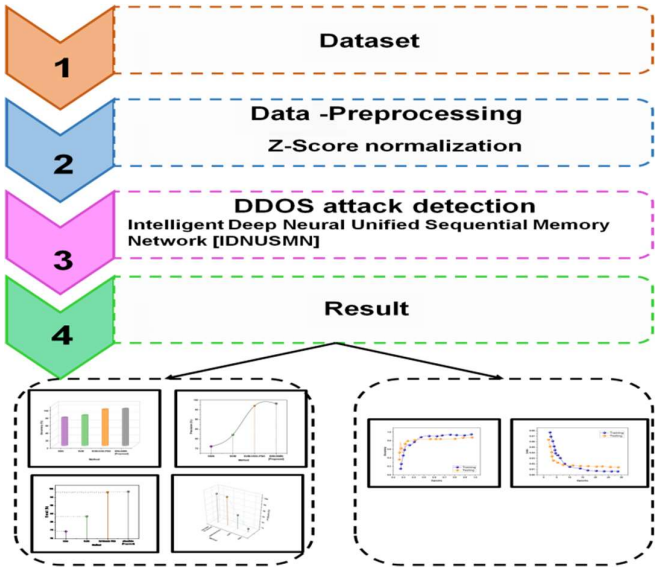


Figure 1: Overall flow

3.1 Data set

The NSL-KDD dataset, which is a streamlined and structured version was used in this work. Several hours of network traffic collection resulted in the creation of the KDD dataset. The NSL-KDD dataset has 52 features and 157,642 samples. This proposed study has been specifically designed to identify malicious or benign traffic during DDoS attacks. Although there are many different kinds of cyber-attacks in the NSL-KDD dataset, our work mainly focuses on determining whether the traffic resulting from DDoS attacks is malicious or benign.

3.2 Data preprocessing

The gathered NSL-KDD dataset was preprocessed using Z-score normalization to convert data into standard normal distribution. Its purpose is to convert numerical data so that it has an SD of 1 and a mean of 0.

3.2.1 Z - Score normalization

The Z-score normalization method bases its normalization on the mean (mean value) and standard deviation (standard deviation) of the data. This process is quite beneficial if the actual lowest and maximum values of the data are unknown.

The following formula (1) is applied:

$$W_{new} = \frac{W-\mu}{\sigma} = \frac{W-Mea\ (W)}{stdDev(W)} \quad (1)$$

$Wnew$ = The new value from the normalized results

W = Old value

μ = Population mean

σ = Standard deviation value

3.3 DDoS Attack using IDNUSMN

IDNUSMN enhances the detection of DDoS attacks. This integrated technique combines the sequential data processing and memory retention of SMN with the advanced pattern recognition capabilities of IDN. Through the integration of these technologies, the system can detect and counteract DDoS attacks in real-time. Improving the correctness and efficiency of detection systems, these unified structural designs provide a strong network defense against altering threats.

3.3.1 Intelligent deep neural (IDN)

By using deep learning to automatically identify complicated attack patterns in network traffic, Intelligent Deep Neural (IDN) networks get better DDoS attack detection while also achieving notable improvements in accuracy. Three layers make up an Improved Deep Neural Network (IDNN): the input layer, hidden layer, and output layer. Every layer consists of several nodes that regularly combine to become a single node in a consequent layer. The

input and output layers are usually one layer each, although there might be more than two hidden layers. Six input levels and seven hidden layers are offered in the suggested work to examine the data. Each cycle of fast current in this IDNN has 64 input neurons and 64 output neurons. Only a minor number of neurons are underfitting while most neurons are overfitting.

The size and quantity of hidden layer neurons are carefully selected for the aforementioned purpose. Practical computations are made for every neuronal layer. Because the buried layer size is controlled by the Tensor flow and set as a hyperparameter. The activation function is the foundation for the IDNN's capacity for fault learning and problem solutions. The IDNN's output layer provides the predicted classes, while the IDNN's input layer receives the coefficient value.

Each node's weight is calculated, and an activation function is used to anticipate the proper values. Repaired linear units, or ReLUs, are employed in the proposed work as an activation function to determine a suitable weight between the nodes and lower system error. Pack propulsion shifts the weight in the opposite direction, from the output layer to the input layer, until the cost function is lowered. The outputs of neurons are defined by(2):

$$z_r^{m+1} = \sigma\left(\sum_{j=1}^{n} \omega_{jr}^m z_j^m + a_r^{m+1}\right) \quad (2)$$

Where$\sigma(y)$represents the activation functionz_r^{m+1}indicates the $m+1$ layers r neuron's output, ω_{jr}^m represents the weight of the m layer's$j$neuron and a_r^{m+1}indicates the bias of linear relationships. The loss function measures the inaccuracies in the repelling process between the estimated coefficient and the real values. The loss function's minor value resolves the variables a and ω. The intelligent DNN's loss function is expressed as follows (3):

$$F(\theta) = -\frac{1}{M}\sum_m \sum_r s_{mr} log z_{mr} \quad (3)$$

Where $z_{mr}$is the projected value of the rthsamplemth element, θ is the parameter of ω and$a$, and N is the number of samples. The actual values of the rth sample mth element are represented by s_{mr}. The equipping of neurons is reduced by the employment of a dropout mechanism, which somehow removes the neurons from the neuron network structure. Furthermore, the suggested approach raises the standard learning rate compared to the conventional gradient descent technique. The best variable for θ can be written as follows (4):

$$\begin{cases} n_s = \beta_1 n_{s-1} + (1-\beta_1) h_s \\ U_s = \beta_2 u_{s-1} + (1-\beta_2) h_s^2 \\ h_s = \nabla_\theta F(\theta_{s-1}) \\ \hat{n}_s = \frac{n_s}{1-\beta_1^s} \\ \widehat{U}_s = \frac{u_s}{1-\beta_2^s} \\ \theta_s = \theta_{s-1} - \alpha \frac{\hat{n}_s}{\sqrt{\hat{u}_s + \varepsilon}} \end{cases} \quad (4)$$

$$\alpha = \alpha_0 \beta_3^{\frac{epoch-num}{M}} \quad (5)$$

WhereU_s indicates the gradient's average movement, $h_s$represents the gradient's parameter, and $n_s$is the gradient's average movement; α_0 is the learning rate's beginning value$\widehat{U}_s$and $\hat{n}_s$are corrected values; and $\beta 1$, $\beta 2$, and $\beta 3$ are the rates of exponential decay that are in use. 0.9, 0.999, and 0.95ep batch size indicate the present training times; and och-num-indicates the batch processing parameter in equation (5).

3.4 Sequential memory network (SMN)

Sequential Memory Networks (SMNs) improve the detection of DDoS attacks by making it possible to accurately identify abnormal network behavior. The adaptive learning features of this model enhance threat identification in real-time, successfully strengthening network resilience against DDoS attacks.

The gating units and memory neurons that are incorporated form the core of the SMN neural network. Memory neurons use the time series chain to pad information by storing the extracted data's regularity and the current data. As a result, data can be moved from the earlier time unit to the later time unit, decreasing the rate of data loss and expanding the amount of data that can be kept. Assuming that the hidden layer state is $(w_1, w_2, \dots, w_s)$and the input sequence is $(g_1, g_2, \dots, g_s)$ at times.

$$e_s = \sigma(X_e \cdot [g_{s-1}, w_s] + a_e) \quad (6)$$

$$j_s = \sigma(X_j \cdot [g_{s-1}, w_s] + a_j) \quad (7)$$

$$P_s = \sigma(X_p \cdot [g_{s-1}, w_s] + a_p) \quad (8)$$

$$\widetilde{D}_s = tang(X_d \cdot [g_{s-1}, w_s] + a_d) \quad (9)$$

$$D_s = e_s . D_{s-1} + j_s . \widetilde{D}_s \quad (10)$$

$$g_s = P_s . tang(D_s) \quad (11)$$

In the formula,e_s, j_s, and P_s stand for the forgetting gate, input gate and output gate, respectively; X_e, X_j, X_p, and X_d indicate the weight of the recursive connection. The input at any given time is represented by w_s while the hidden layer's state at the final instant is represented by $g_{s-1}.D_s$andD_{s-1} indicates the output layers of the hidden layer at each instant, while a_e, a_j, a_p, anda_d reflect the bias of each function.

3.5 IDNUSMN

Intelligent Deep Neural Unified Sequential Memory Networks (IDNUSMN), which make use of intelligent neural network algorithms, suggest a widespread method for detecting DDoS attacks. By combining sequential memory capacity; these networks can competently capture the sequential patterns created in DDoS attacks in network traffic data. IDNUSMNs advance efficiency and accuracy in detecting damaging activity by streamlining the detection process through the use of integrated architectures. To enhance overall detection reliability in constantly shifting and dynamic cyber threat landscapes, IDNUSMNs surpass these alternatives by utilizing deep neural networks' inherent ability to learn challenging features directly from data. This method can help organizations defend against DDoS attacks more precisely and efficiently in a proactive manner.

4. Result

Simulation setup

An Intel i7 core Windows 10 laptop with 8GB RAM and Tensor Flow/Keras was modeled with Python 3.10.1 software and the scikit-learn method. In the section proposed method, IDNUSMNis compared to existing methods such as Support vector machines (SVM), K-Nearest Neighbors (KNN), and Support vector machine (SVM) - PSO (particle swarm optimization) utilizing Harris Hawks' optimization (HHO) (SVM-HHO-PSO)[16]. The following metrics are used: recall, accuracy, precision, and F1 score.

Model is trained accuracy assesses how well it matches actual results, whereas loss quantifies the predicted and true values diverge. Better model performance in machine learning tasks is indicated by higher accuracy and lower loss, which show the model's capacity to minimize errors and produce accurate predictions. Figure 2 shows accuracy and loss.

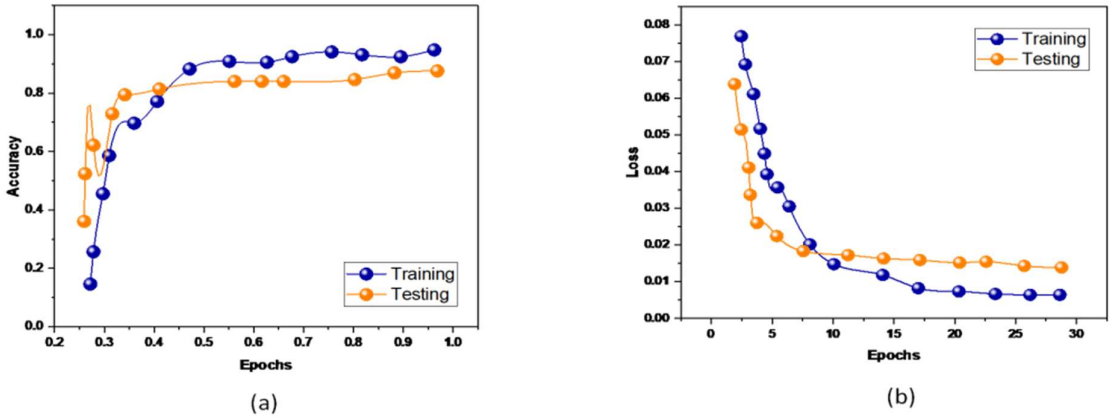
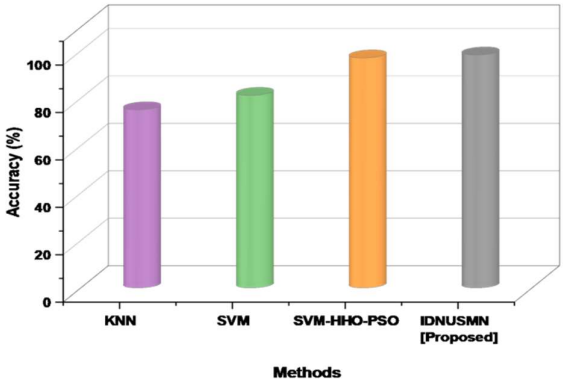


Figure 2: Outcome of Accuracy (a) and Loss (b)

Accuracy in DDoS attack detection is defined as the ratio of successfully identified instances (attacks and ordinary traffic) to the total number of occurrences. It assesses the detection system's ability to discriminate between safe and harmful traffic. Figure 3 and table 1 display the accuracy performance. The accuracy value for proposed (IDNUSMN-98.25%) outperforming the existing systems (KNN-75.12%, SVM-81.20%, and SVM-HHO-PSO-97%) respectively. Our suggested approach is effective in DDoS attack detection.



.

Figure 3: Performance of Accuracy

The ratio of successfully recognized DDoS assaults to all instances classified as DDoS attacks is known as precision in DDoS attack detection. It shows the capacity of the system to prevent false positives with high precision, the majority of alerts marked as attacks are actual attacks. Figure 4 and Table 1 display the precision performance. The precision value for proposed (IDNUSMN-98.18%) outperforms the existing systems such as (KNN-76.11%, SVM-82.14%, and SVM-HHO-PSO-97.06%) respectively. Our proposed method is better than the existing method for DDoS attack detection.

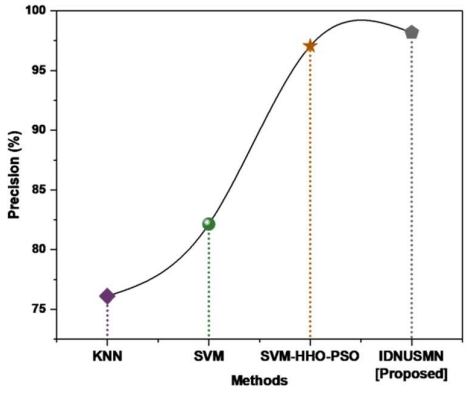


Figure 4: Performance of precision

The ratio of accurately identified DDoS attacks to the total number of actual DDoS attacks is known as recall in DDoS attack detection. It measures how well the system can identify all real attacks. A high recall rate means that the system minimizes false negatives by successfully identifying the majority of actual attacks. Figure 5 and table 1 display the recall performance. The recall value for proposed (IDNUSMN-98.5%) outperforming the existing systems such as (KNN-74.27%, SVM-83.45%, and SVM-HHO-PSO-98%) respectively. Our recommended method is superior to the existing method for DDoS attack detection.

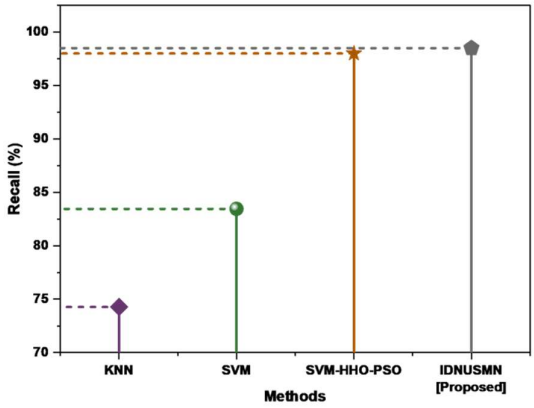


Figure 5: performance of Recall

The F1 score for DDoS attack detection is made up of the average precision and recall. By taking into consideration both false negatives and erroneous positives, it provides a single statistic that strikes a compromise between recall and precision. A robust detection system that correctly identifies attacks with few errors is indicated by high F1 score. Figure 6 and table 1 display the recall performance. The F1 score for the proposed (IDNUSMN-98.35%), outperforms the existing systems such as (KNN-75.47%, SVM-84.95%, and SVM-HHO-PSO-97.90%) respectively. Our suggested method is more effective than an existing method for DDoS attack detection.

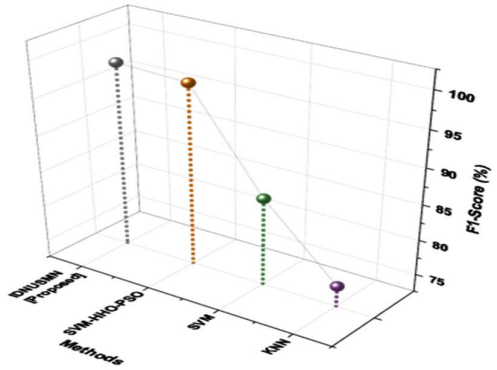


Figure 6: performance of F1 Score

Table 1:Outcome values of Precision, Accuracy, Recall, and F1 score

Method	Accuracy (%)	Precision (%)	Recall (%)	F1score (%)
KNN	75.12	76.11	74.27	75.47
SVM	81.20	82.14	83.45	84.95
SVM-HHO-PSO	97	97.06	98	97.90
IDNUSMN [Proposed]	98.25	98.18	98.5	98.35

5. Discussion

Our proposed IDNUSMNs are to overcome the drawbacks of conventional techniques like SVM, KNN and hybrid models like SVM-HHO-PSO [16]. KNN has trouble processing high-dimensional input and needs a lot of processing high –dimensional input and needs a lot of processing power. SVM has high computational complexity makes it inefficient for handling huge datasets, and data noise can negatively impact classification performance. Combining SVM with optimization techniques, hybrid models such as SVM-HHO-PSO may have difficulties striking a balance between computing efficiency and accuracy (98.25%). To tackle this limitation, we proposed

IDNSUMN which integrates intelligent deep neural and sequential memory networks for DDoS attack detection. IDNUSMNs can potentially outperform standard and hybrid methods in terms of accuracy and adaptability by utilizing these qualities, which makes them appropriate.

6. Conclusion

In this paper, two well-known deep learning algorithms were hybridized to produce intelligent deep neural unified sequential memory networks (IDNUSMN), a unique DDoS attack detection method.The method was validated using the NSL-KDD dataset. Z-score normalization was used as a preprocessing step to convert the data into a standard normal distribution. Python software is used to simulate the suggested approach. The other conventional algorithms and the IDNUSMN are contrasted. The outcome demonstrates that the IDNUSMN has outperformed the other in terms of F1-score-98.35%, accuracy-98.25%, recall-98.5%, and precision-98.18%. Our suggested method for DDoS Attack Detection outperforms the existing method. While intelligent deep neural unified sequential memory networks are more effective at detecting DDoS attacks, they have limitations. Real-time deployment in resource-constrained situations is limited by their high computing resource requirements. To prevent performance hazards like overfitting, they depend on having enough, well-balanced training data. Upcoming advancements in hardware and algorithm performance might make real-time detection possible in a variety of settings. For, longer-lasting efficacy, ongoing research in adaptive learning attempts to keep up with DDoS tactics, while hybrid models and improved explaining ability promise more resilient defenses.

References

1. Peneti, S. and Hemalatha, E., 2021, January. DDOS attack identification using machine learning techniques. In *2021 International Conference on Computer Communication and Informatics (ICI)* (pp. 1-5). IEEE.
2. Khempetch, T. and Wuttidittachotti, P., 2021. DDoS attack detection using deep learning. *IAES International Journal of Artificial Intelligence*, *10*(2), p.382.
3. Khare, M. and Oak, R., 2020. Real-time distributed denial-of-service (DDoS) attack detection using decision trees for server performance maintenance. *Performance Management of Integrated Systems and its Applications in Software Engineering*, pp.1-9.
4. Balasubramaniam, S., Vijesh Joe, C., Sivakumar, T.A., Prasanth, A., Satheesh Kumar, K., Kavitha, V. and Dhanaraj, R.K., 2023. Optimization Enabled Deep Learning-Based DDoS Attack Detection in Cloud Computing. *International Journal of Intelligent Systems*, *2023*(1), p.2039217.
5. Ahuja, N., Singal, G., Mukhopadhyay, D. and Kumar, N., 2021. Automated DDOS attack detection in software-defined networking. *Journal of Network and Computer Applications*, *187*, p.103108.
6. Yousuf, O. and Mir, R.N., 2022. DDoS attack detection in the Internet of Things using recurrent neural network. *Computers and Electrical Engineering*, *101*, p.108034.
7. Sumathi, S., Rajesh, R. and Karthikeyan, N., 2022. DDoS attack detection using hybrid machine learning-based IDS models.
8. Tuan, T.A., Long, H.V., Son, L.H., Kumar, R., Priyadarshini, I. and Son, N.T.K., 2020. Performance evaluation of Botnet DDoS attack detection using machine learning. *Evolutionary Intelligence*, *13*(2), pp.283-294.
9. Velliangiri, S. and Pandey, H.M., 2020. Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-art algorithms. *Future Generation Computer Systems*, *110*, pp.80-90.
10. Aktar, S. and Nur, A.Y., 2023. Towards DDoS attack detection using deep learning approach. *Computers & Security*, *129*, p.103251.
11. Ali, T.E., Chong, Y.W. and Manickam, S., 2023. ML/DL approaches for detecting DDoS attacks in SDN. *Applied Sciences*, *13*(5), p.3033.
12. Anyanwu, G.O., Nwakanma, C.I., Lee, J.M. and Kim, D.S., 2022. Optimization of RBF-SVM kernel using grid search algorithm for DDoS attack detection in SDN-based VANET. *IEEE Internet of Things Journal*, *10*(10), pp.8477-8490.
13. Nugraha, B. and Murthy, R.N., 2020, November. 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.

14. Batchu, R.K. and Seetha, H., 2021. A generalized machine learning model for DDoS attack detection using hybrid feature selection and hyperparameter tuning. *Computer Networks*, *200*, p.108498.
15. 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.
16. Sokkalingam, S. and Ramakrishnan, R., 2022. An intelligent intrusion detection system for distributed denial of service attacks: A support vector machine with hybrid optimization algorithm based approach. *Concurrency and Computation: Practice and Experience*, *34*(27), p.e7334.