Emerging Trends in Digital Transformation
Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-14***

DEEP LEARNING NN ALGORITHM FOR DDoS ATTACK DETECTION

[1]Dr.P.SATHISH, Assistant Professor, Department of Computer Science & Engineering
Kamala Institute of Technology & Science (KITS(S))
polu.sathish@kitss.edu.in
[2]Dr. Major Ravindra Babu Kallam, Professor & Head, Department of Computer Science & Engineering
Kamala Institute of Technology & Science (KITS(S))
rbkallam2510@kitssingapuram.ac.in.com
[3]Dr. V. Bapuji , Professor, Department of Computer Science, Mohan Babu University Thirupathi, Andhra Pradesh, India
bapuji.vala@gmail.com
[4]Raju Bomma, Asst professor, Department of Computer Science & Engineering
Kamala Institute of Technology and Science(KITS(S))
rajubomma@gmail.com

ABSTRACT: The Deep Learning Neural Network (DLNN) is used for IDS. The architecture of DLNN was developed by Schmid Huber7.2 (2015) and Nielsen (2015). The previous parts of research work presented in this work reported certain limitations such as delayed convergence, poor false prediction performance and unstable output for certain iterations. These limitations are addressed by introducing a deep learning model based on autoencoder and decoder with a gradient descent learning rule. This method was devised using the suggested hybrid HHOPSO optimization, which was employed to alter the bias and weight vectors the NN model.

The efficacy of the studied deep learning model has been confirmed by relating its simulation results with the performance of other models developed in the earlier part of the research work.

Keywords: - DDoS detection- Deep learning- Neural networks- Anomaly detection

1. INTRODUCTION

Deep learning strategies involve using multiple hidden layers in neural network models for training, surpassing the CNN architecture. The work presented utilizes DL strategies as they can achieve superior intrusion classification performance compared to basic learning algorithms.

DOI: https://doi.org/10.5281/zenodo.19016387

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-14***

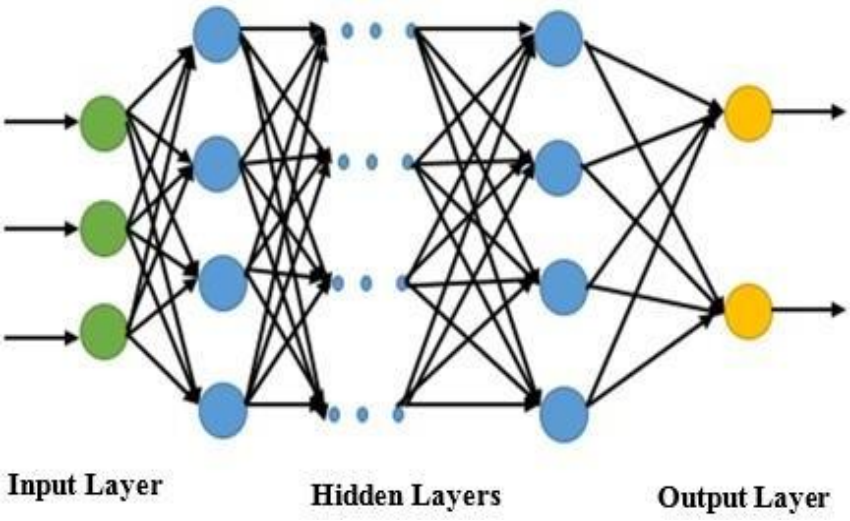

Figure 2.1. Structural design of Deep learning Neural Network

Figure 2.1 illustrates the architecture of the DLNN. It includes multiple hidden layers, each incorporating a non-linear transformation between layers. The DLNN undergoes training using unsupervised learning and a backpropagation NN.This learning procedure employs the autoencoder-decoder principle for network pre-training, followed by fine-tuning using the backpropagation neural network.

In unsupervised learning, the autoencoder utilizes its output as the input data (Ilango et al., 2019).The encoding layerconverts the input samples into a code, moving from high to low dimensional space. Following that, the decoder reverts the input back to its previous form.

2. PROPOSED HYBRID HHOPSO BASED DLNN MODEL

The classic optimizer algorithms like swarm intelligence algorithms, fuzzy rule base or evolutionary algorithms can be applied individually to tune the network modelHowever, these algorithms face limitations such as getting stuck in local optima, experiencing delayed convergence, and encountering global minima.

These limitations have been eliminated by employing hybrid optimization algorithm, which combines the best features of HHO and PSO algorithm. The suggested deep learning model employs a hybrid HHO-PSO optimization algorithm to adjust network parameters, such as weight vectors and bias coefficients, during the training process. During the training of DLNN model, hybrid optimization algorithm is initialized to find the optimal weight values by minimizing the reconstruction error.

The algorithm parameters are detailed in Table 3.1, and the pseudo code for the suggested hybrid deep learning training algorithm.

DOI: https://doi.org/10.5281/zenodo.19016387

Table 3.1. Parameters of the proposed model

Parameters	DLNN
Weights and Bias	Optimally fed by HHO-PSO
Number of input Neurons	Number of selected Features
Number of hidden Layers	Fixed during training
Number of hidden Neurons	(7-12), fixed during training
Number of output neurons	1
Activation Function	Sigmoid Activation Function
Learning rate	0.25(Fixed at end trial)
Learning Rule	Gradient descent rule
Parameters	**Hybrid HHO-PSO**
Population Size	100
Maximum Number of Iterations	Until convergence attained
(u, v)	(0,1)
□	1.5
Initial Energy State E_0	(0,1)

3. RESULT COMPARISON AND DISCUSSION

The efficacy of the proposed IDS models is assessed using the NSL benchmark dataset comprising 41 features. The primary goal of these models is to achieve enhanced accuracy while utilizing fewer features.

Optimal features were chosen through 10-fold cross-validation for every fold, and the selected features are outlined in Table 3.2. The selection of features was carried out with the proposed HHOPSO algorithm.Features were selected based on how frequently they appeared at the conclusion of the 10-fold cross-validation procedure. These chosen features were then input into the NN, and their respective execution was evaluated.

DOI: https://doi.org/10.5281/zenodo.19016387

Table 4.1. Features Chosen by the HHO-PSO Algorithm in the Proposed Approach

No.	Selected Features	No.	Selected Features
1	F4 (flag)	2	F5 (src_bytes)
3	F8 (wrong_fragment)	4	F12 (logged_in)
5	F23 (Count)	6	F25 (serror_rate)
7	F30 (diff_srv_rate)	8	F35 (dst_host_diff_srv_rate)
9	F36 (dst_host_same_src_port_rate)		

The feature selection process involved choosing a subset of features, which was then input into the proposed DL model for grouping of intrusion. Addressing the challenge of managing parameters in DL models, optimal bias and weight were selected for the proposed model.

Initially, several tests were conducted to determine the quantity of hidden layers for constructing the DLNN model. The hidden neurons and layers are crucial factors that impact the network's complexity. Hence, they were determined using a trial-and-error method, and the model efficacyis depicted in Table 4.1

Figure 2.1 illustrates the Accuracy deviation of the presented model over 10 trial runs and respective hidden layers. Effectively managing overfitting is a critical task in DL models, and it can be addressed by analysing the training proficiency of the presented model.

Figure 2.1 illustrates accuracy of the training and testing for several hidden layers, confirming that the network underfits from trial-7 and overfits from trial-9. To overcome problems like overfitting and underfitting, opted for 12 hidden layers

Figure 4.1. Error Rate Across 10 Trial Runs

DOI: https://doi.org/10.5281/zenodo.19016387

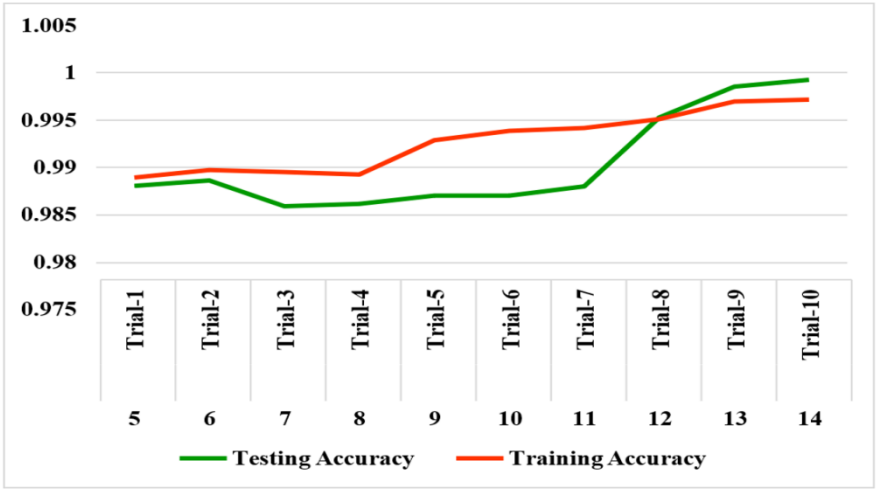

Figure 4.2 Training Performance Across 10 Trial Runs for the Proposed Model

Figure 4.2 compares the performance of various models. The weight and bias vectors of the proposed DLNN model were fine-tuned using PSO, HHO, and the hybrid HHOPSO. The hybrid HHO-PSO-DLNN model performs superiorly than the regular models.

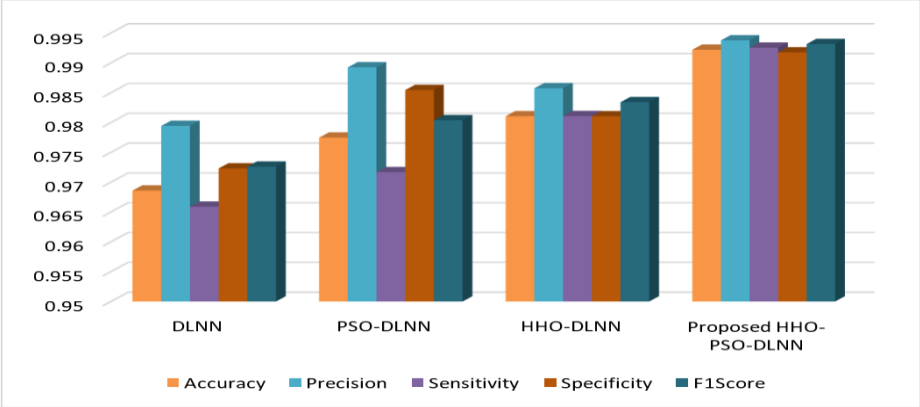

Figure 4.3 Comparative Performance of the Proposed DLNN Model against Other Models

The implementation of the new HHOPSO-DLNN model was compared to all other models from earlier in the research, shown in Figure 4.1, Figure 4.2, and Table 4.3.

Our hybrid HHO-PSO-DLNN model achieved better accuracy in fewer iterations than other models like HHO-PSO-LSTM and HHO-PSO-MLP.

The HHO-PSO-DLNN model achieved superior metric values compared to other models developed in different parts of the research. However, it's important to mention that the proposed model is expected to take more execution time than all other models.

DOI: https://doi.org/10.5281/zenodo.19016387

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-14***

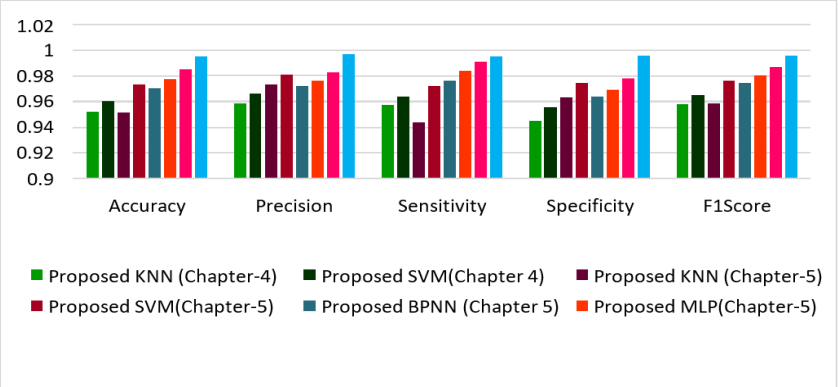

Figure 4.4 Comparative Performance of the Proposed Models against Other Models developed in the research work

4.CONCLUSION& FUTURE SCOPE

This section of the research has designed a deep learning architecture for detecting DDoS attacks using an autoencoder-decoder strategy. The initial structure of the proposed DLNN model is determined through multiple trial ends. Later, the weights of the DLNN model are finely tuned using the hybrid HHO-PSO optimization.The model's performance is evaluated in each trial run.Moreover, the efficacy of the suggested model is assessed by comparing its performance with models from previous research sections and existing approaches. The findings show that the suggested DLNN model is more effective than all other models in spotting intrusions in a cloud computing setting.

Federated Learning: Enabling collaborative model training across multiple devices while preserving data privacy. Explainable AI (XAI): Developing techniques to make deep learning models more interpretable and transparent. Edge AI: Deploying models at the network edge to reduce latency and improve real-time detection. Adversarial Robustness: Creating models resilient to adversarial attacks designed to evade detection. Hybrid Architectures: Combining CNNs, LSTMs, and Autoencoders to capture complex attack patterns. Zero-Day Attack Detection: Developing models capable of detecting previously unseen attack patterns. CNN-LSTM: Capturing spatial and temporal patterns in network traffic-DNN: Detecting low-rate and volumetric DDoS attacks. DBN-LSTM: Identifying complex attack patterns.

REFERENCES

1. Ahmed, AA, Jabbar, WA, Sadiq, AS & Patel, H 2020, 'Deep learning- based classification model for botnet attack detection' 'Journal of Ambient Intelligence and Humanized Computing', pp. 1-10.
2. Chamou, D, Toupas, P, Ketzaki, E, Papadopoulos, S, Giannoutakis, KM, Drosou, A & Tzovaras, D 2019, 'Intrusion Detection System Based on Network Traffic Using Deep Neural Networks', In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, pp. 1-6.
3. Chen, YH, Jan, PT, Lai, CN, Huang, C, Chang, CH & Huang, YC 2020, 'Detecting Linking Flooding Attacks using Deep Convolution Network', In Proceedings of the

DOI: https://doi.org/10.5281/zenodo.19016387

2020 the 3rd International Conference on Computers in Management and Business, pp. 70-74.

4. Doriguzzi-Corin, R, Millar, S, Scott-Hayward, S, Martinez-del-Rincon, J & Siracusa, D 2020, 'LUCID: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection', IEEE Transactions on Network and Service Management.
5. Ghanbari, M & Kinsner, W 2020, 'Detecting DDoS Attacks Using Polyscale Analysis and Deep Learning', International Journal of Cognitive Informatics and Natural Intelligence (IJCINI), vol. 14, no. 1, pp.17-34.
6. Haider, S, Akhunzada, A, Ahmed, G & Raza, M 2019, 'Deep learning based ensemble convolutional neural network solution for distributed denial of service detection in SDNs', In 2019 UK/China Emerging Technologies (UCET), IEEE, pp. 1-4.
7. Hussain, B, Du, Q, Sun, B & Han, Z 2020, 'Deep Learning-Based DDoS-Attack Detection for Cyber-Physical System over 5G network', IEEE Transactions on Industrial Informatics.