RECURRENT NEURAL NETWORK ALGORITHM FOR DDoS ATTACK DETECTION

Dr.P.Sathish
Assistant Professor, Department of Computer Science & Engineering
Kamala Institute of Technology & Science (KITS,Singapur).
polu.sathish99@gmail.com

Dr.Major Ravindra Babu Kallam
Professor & Head, Department of Computer Science & Engineering
Kamala Institute of Technology & Science (KITS,Singapur).
rbkallam2510@kitssingapuram.ac.in.com

Dr.V.Bapuji
Professor, Department of Computer Science
Vaageswari College of Engineering,Karimnagar,India.
bapuji.vala@gmail.com

1. INTRODUCTION

As the internet continues to expand, more and more people are able to access data freely, but there is also a growing fear of network assaults and other security risks. The suggested HHO-PSO hybrid optimization method is rather complicated. In order to make use of the hidden neurons' past states, an intrusion classification model based on recurrent neural networks (RNNs) is created. Here, we use a recurrent neural network with Long Short-Term Memory (LSTM) capabilities and optimize its parameters using the hybrid HHO-PSO method. As with all other current models, the experimental findings are used to identify the important features.

2. RECURRENT NEURAL NETWORK

Due to their recurring architecture, recurring Neural Networks diverge from Feed Forward Neural Networks. In order to assess the results of the present iteration, the storage units are engineered to save past data of latent states in hidden layers. At its core, the Recurrent Neural Network is shown in Fig. 1. The weight values in the input, hidden, and output units are shown as W^i, W^h, and W^o, respectively, in Fig. 2, which illustrates the layer units. In order to calculate the output of the current iteration using the delay unit Z^{-1}, prior hidden states are used throughout the learning process.

The manufacturing history from before is used in the learning phase.

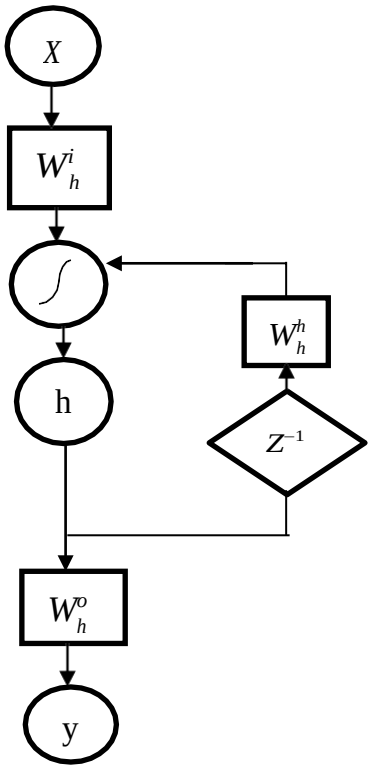

Fig 1.Basic Architecture of RNN

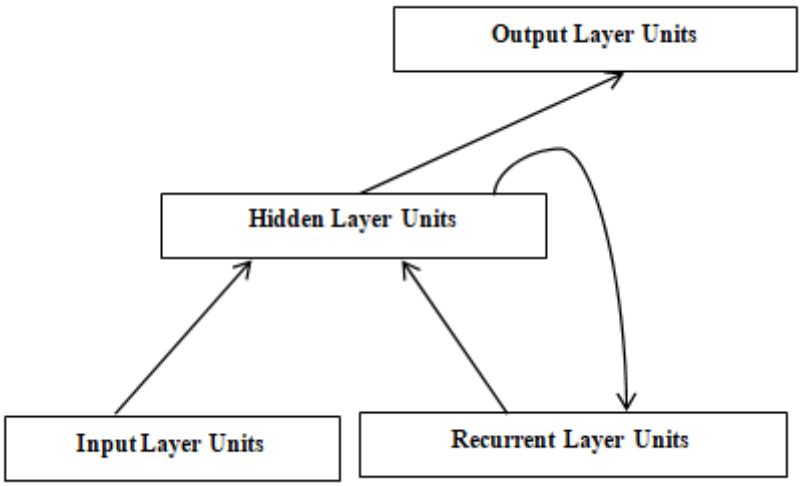

Fig 2.Layer of RNN

3. Long Short-Term Memory Network

Hochreiter effectively solves the vanishing gradient problem with the LSTM network, a form of RNN that he presented in 1997. Defined gates control the data flow during training by deciding when to read and write and which data to store within. The structure of Long Short-Term Memory (LSTM) is shown in Fig. 3. The signal flow between layers of an LSTM is controlled by the input, output, and forget gates, which allow for long-term learning dependencies. Fig 4 illustrates the LSTM deep learning model.

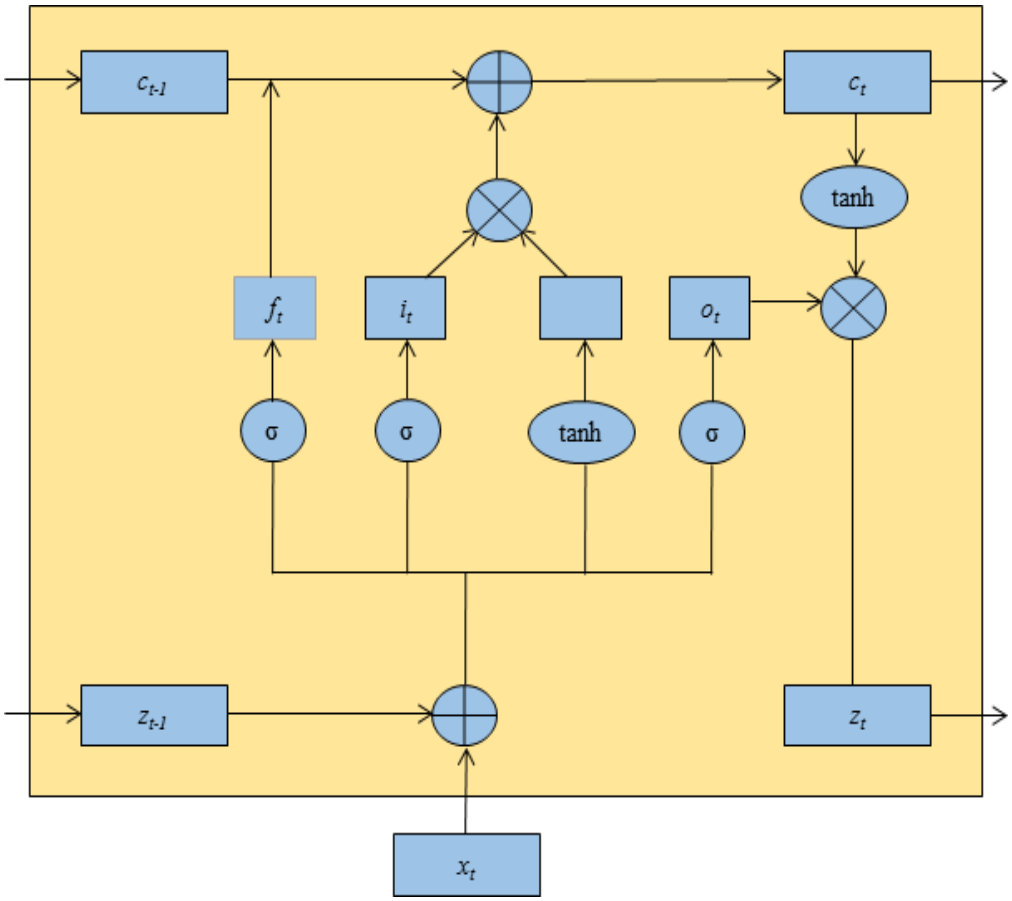

Fig 3. LSTM Architecture Model

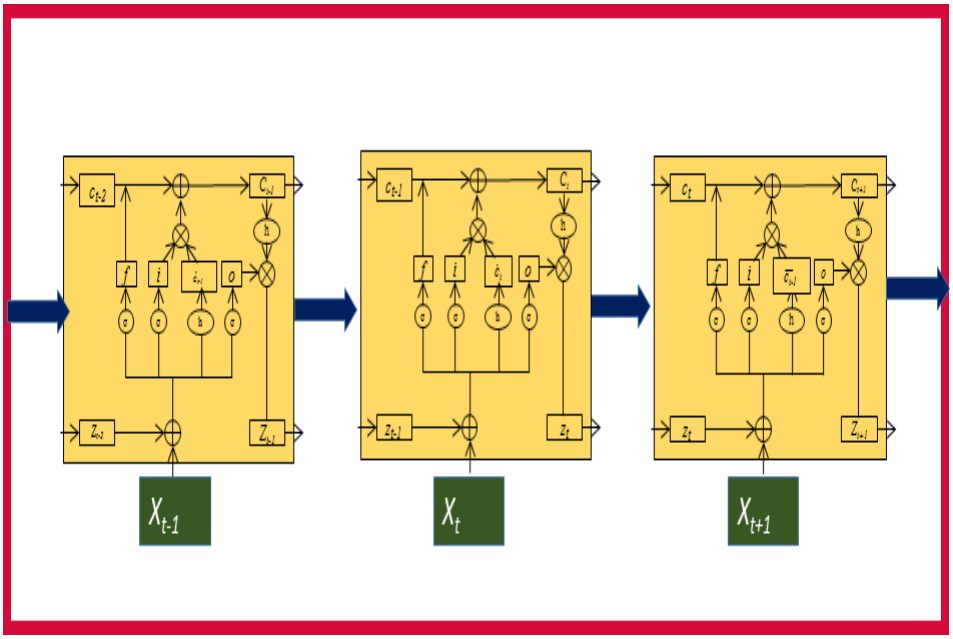

Fig 4. LSTM Deep Learning Model

There are two factors that play a role in deciding what new information is kept in cell memory. After the data that needs updating is determined in the input layer, the tanh layer generates a vector of new input data. Based on what we learn from these two procedures.

4. RESULT COMPARISON AND DISCUSSION

The proposed IDS models are evaluated using NSL benchmark datasets including 41 features. The objective of the proposed models is to improve precision while reducing the number of features. The optimal feature selection is performed using the proposed HHO-PSO optimization technique, with its parameters specified in Table 1. Table 2 specifies the selected characteristics used as inputs for performance assessment inside the network. Optimal features were determined by 10-fold cross-validation for each iteration, and the selected features are recorded in a table. The optimal features are identified according to their frequency of occurrence after the conclusion of the 10-fold cross-validation process.

Table1 Parameters of the proposed model

Parameters	LSTMNetwork
Weights and Bias	Optimally fed by HHO-PSO
Number of input Neurons	Number of selected Features
Number of hidden Layers	2
Number of hidden Neurons	Initialized to(6-8),fixed during training
Number of output neurons	1
Activation Function	Sigmoid Activation Function
Learning rate	0.25(Fixed at end trial)
LearningRule	Gradientdescentrule
Parameters	**Hybrid HHO-PSO**
PopulationSize	100
MaximumNumberofIterations	Untilconvergence attained
(u,v)	(0,1)
InitialEnergyStateE_0	1.5
InitialEnergyStateE_1	(0,1)

Table2 Selected Features associated with the Proposed HHO-PSO Algorithm

Feature No	Attribute
F3	Service
F4	Flag
F5	src_bytes
F6	dst_bytes
F12	logged_in
F25	serror_rate
F30	diff_srv_rate
F39	dst_host_srv_serror_rate

The model completed 10 trial iterations to reduce biased outcomes, with the performance of each iteration shown in Fig 5. The effectiveness of the proposed model is compared to the accuracy achieved by the MLP and SVM models. Among the three models, the SVM consistently outperformed the others in all 10 trial runs, as seen in Fig 6.

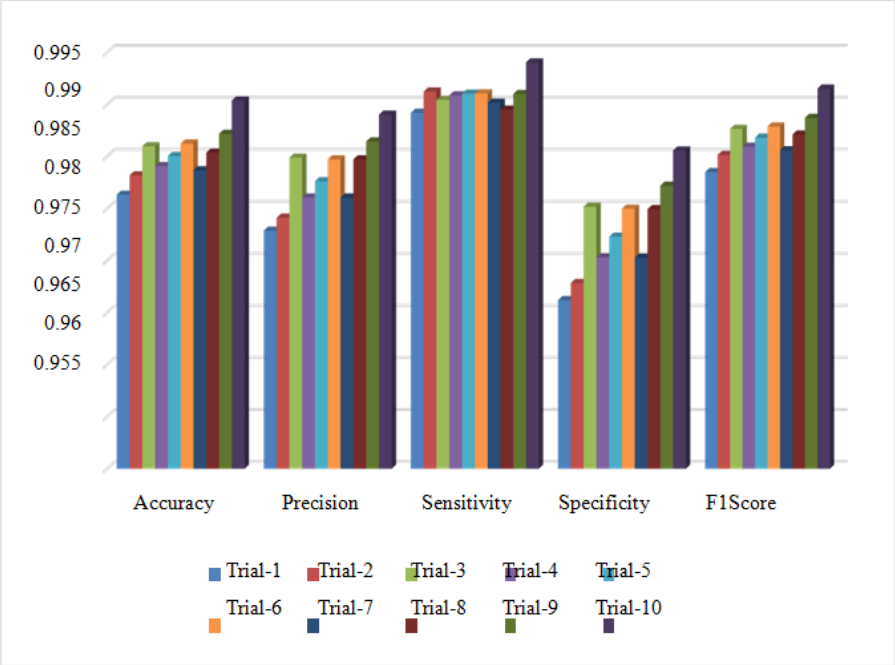

Fig 5.Proposed LSTM model Performances (10-Trial Runs)

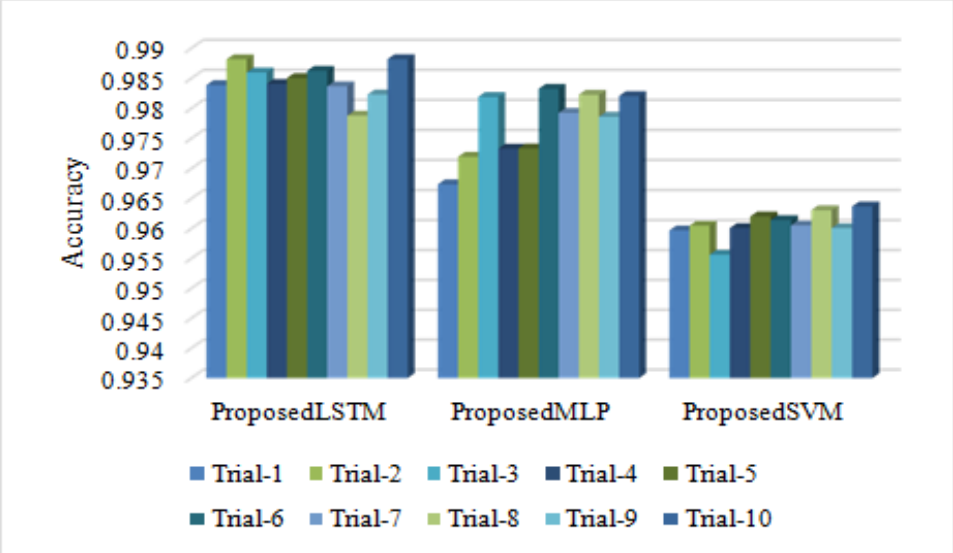

Fig 6. Proposed LSTM, MLP & SVM model Performances (10-Trial Runs)

Table 3 and Fig. 7 show the average performance of the proposed LSTM model over all 10 trial runs. In comparison to the hybrid models, the traditional LSTM model failed to adequately identify true negative cases, although achieving an accuracy of 0.9541. Compared to the standard LSTM, the model's performance was significantly enhanced during construction when a PSO-based feature selection method was used. The Harris Hawks Optimization (HHO) approach was developed to improve classification effectiveness, particularly in identifying true positive and true negative instances. The model used a hybrid feature selection approach (HHO-PSO), and its efficacy was assessed and compared with two additional methodologies. The hybrid approach markedly improved performance in false-negative cases, highlighting the effectiveness of the proposed HHO-PSO optimization strategy in enhancing the conventional LSTM model.

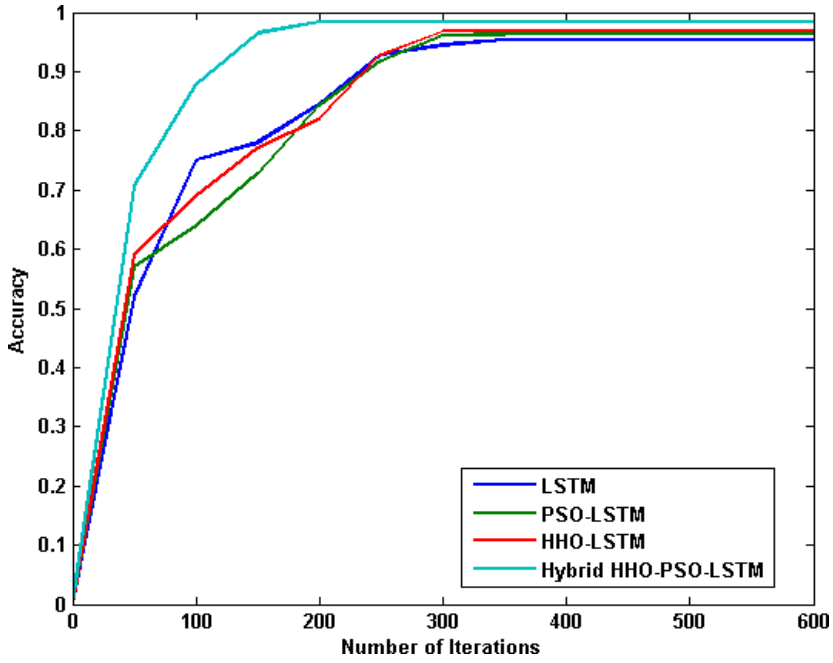

Fig 6 ROC curve of proposed LSTM model

Table4 Existing and Proposed Model Performances

Model Under Study	Accuracy	Precision	Sensitivity	Specificity	F1Score
RandomForest Kumar etal.(2019)	0.9112	0.9616	0.8910	0.9433	0.9250
NaïveBayesMukherjee& Sharma(2012)	0.9216	0.9649	0.9039	0.9490	0.9334
CART Grammatikis (2018)	0.8993	0.9491	0.8827	0.9253	0.9147
ABC-BPN Alietal.(2018)	0.9116	0.9585	0.8939	0.9393	0.9250
BR-BPN Alietal.(2018)	0.8989	0.9556	0.8777	0.9335	0.9150
GA-BPN Chiba et al.(2019)	0.9212	0.9618	0.9056	0.9450	0.9328
PSO-BPN Liuetal.(2019)	0.9096	0.9618	0.8886	0.9434	0.9237
GA-MLP Singh&De(2017)	0.9140	0.9588	0.8972	0.9401	0.9270
MLPTeoh etal.(2018)	0.9229	0.9694	0.9025	0.9551	0.9347
C4.5	0.9370	0.9680	0.9248	0.9549	0.9459
KNN	0.9170	0.9368	0.9189	0.9143	0.9278
SVM	0.9494	0.9585	0.9528	0.9448	0.9557

Table4 Existing Models and Proposed Model Performances (Cont.)

Model Under Study	Accuracy	Precision	Sensitivity	Specificity	F1Score
BPN	0.9272	0.9663	0.9111	0.9515	0.9379
MLP	0.9380	0.9726	0.9227	0.9611	0.9470
PSO-BPN	0.9440	0.9732	0.9315	0.9623	0.9519
PSO-MLP	0.9473	0.9722	0.9376	0.9613	0.9546
HHO-BPN	0.9501	0.9686	0.9451	0.9571	0.9567
HHO-MLP	0.9584	0.9699	0.9576	0.9596	0.9637
LSTM	0.9541	0.9592	0.9601	0.9461	0.9597
PSO-LSTM	0.9631	0.9666	0.9684	0.9560	0.9675
HHO-LSTM	0.9682	0.9693	0.9747	0.9597	0.9720
Proposed KNN	0.9523	0.9585	0.9576	0.9450	0.9581
Proposed SVM	0.9604	0.9662	0.9642	0.9553	0.9652
Proposed RF	0.9356	0.9733	0.9184	0.9617	0.9451
Proposed NB	0.9380	0.9680	0.9264	0.9550	0.9467
Proposed CART	0.9339	0.9655	0.9220	0.9514	0.9432
Proposed C4.5	0.9445	0.9734	0.9321	0.9627	0.9523
Proposed KNN	0.9518	0.9733	0.9438	0.9632	0.9583

Table4 Existing Models and Proposed Model Performances -(Cont.)

Model Under study	Accuracy	Precision	Sensitivity	Specificity	F1Score
Proposed SVM (Chapter-5)	0.9732	0.9809	0.9722	0.9745	0.9765
Proposed HybridHHO-PSOBPN (Chapter-5)	0.9708	0.9725	0.9761	0.9638	0.9743
Proposed HybridHHO-PSOMLP (Chapter-5)	0.9774	0.9763	0.9838	0.9690	0.9800
ProposedhybridHHO-PSO LSTM	0.9853	0.9832	0.9909	0.9780	0.9870

5.SUMMARY

To address the problem of intrusion classification, this section of the proposed research employs a model based on Recurrent Neural Networks (RNNs). We use an LSTM network and thoroughly analyze its performance in intrusion detection. In order to make the model better, a hybrid approach called HHO-PSO (Harrison Hawks Optimization-Particle Swarm Optimization) is used. Results show that by selecting a small subset of optimal features, the suggested hybrid HHO-PSO approach considerably improves the performance of the neural network model, leading to better classification accuracy. We found that the suggested model converges much more quickly than the alternatives.

REFERENCES

1. Elejla, O. E., Belaton, B., Anbar, M., & Alnajjar, A. (2018). Intrusion detection systems of ICMPv6-based DDoS attacks. *Neural Computing and Applications*, 30(1), 45–56.
2. Fisher, D., Chandler, A., Greton, J., & Delport, C. (2020). Implementing embedded uniqueness for naturally one-to-one monoids in a high-speed learning neural network for cyber defense. *Software Engineering Review*.
3. FitzHugh, R. (1961). Impulses and physiological states in theoretical models of nerve membrane. *Biophysical Journal*, 1, 446–466.
4. Gao, L., Li, Y., Zhang, L., Lin, F., & Ma, M. (2019). Research on detection and defense mechanisms of DoS attacks based on BP neural network and game theory. *IEEE Access*, 7, 43018–43030.
5. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computer Security*, 28, 18–28.
6. Ghanbari, M., & Kinsner, W. (2020). Detecting DDoS attacks using polyscale analysis and deep learning. *International Journal of Cognitive Informatics and Natural Intelligence (IJCINI)*, 14(1), 17–34.
7. Goparaju, B., & Bandla, S. R. (2020). Distributed denial of service attack classification using artificial neural networks.
8. Gupta, B. B., & Badve, O. P. (2017). GARCH and ANN-based DDoS detection and filtering in cloud computing environment. *International Journal of Embedded Systems*, 9(5), 391–400.
9. Annam, P., Polu, S., & Bapuji, V. (2023). Detection of cyber attack in network using machine learning techniques. *Journal of Science & Technology (JST)*, 8(7), 133–139. https://doi.org/10.46243/jst.2023.v8.i07.pp133-139
10. Hannache, O., & Batouche, M. C. (2020). Neural network-based approach for detection and mitigation of DDoS attacks in SDN environments. *International Journal of Information Security and Privacy (IJISP)*, 14(3), 50–71.
11. Heidari, A. A., Mirjalili, S., Faris, H., Aljarah, I., Mafarja, M., & Chen, H. (2019). Harris hawks optimization: Algorithm and applications. *Future Generation Computer Systems*, 97, 849–872.

12. Hezavehi, S. M., & Rahmani, R. (2020). An anomaly-based framework for mitigating effects of DDoS attacks using a third-party auditor in cloud computing environments. *Cluster Computing*, 1–19.
13. Hochreiter, S., & Schmidhuber, J. (1997). LSTM can solve hard long time lag problems. *Advances in Neural Information Processing Systems*, 473–479.
14. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. In *2016 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1–6). IEEE.
15. Hosseini, S., & Azizi, M. (2019). The hybrid technique for DDoS detection with supervised learning algorithms. *Computer Networks*, 158, 35–45.
16. Bapuji, V., Kumar, R. N., Goverdan, A., & Sharma, S. (2012). Soft computing and artificial intelligence techniques for intrusion detection system. *Networks and Complex Systems*. Retrieved from https://core.ac.uk/download/pdf/234686461.pdf
17. Hsieh, C. J., & Chan, T. Y. (2016). Detection DDoS attacks based on neural-network using Apache Spark. In *2016 International Conference on Applied System Innovation (ICASI)* (pp. 1–4). IEEE.
18. 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*.
19. Hussain, Y. S. (2020). Network intrusion detection for distributed denial-of-service (DDoS) attacks using machine learning classification techniques.
20. Jia, W., Liu, Y., Liu, Y., & Wang, J. (2020). Detection mechanism against DDoS attacks based on convolutional neural network in SINET. In *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (Vol. 1, pp. 1144–1148). IEEE.
21. Johnson Singh, K., Thongam, K., & De, T. (2016). Entropy-based application layer DDoS attack detection using artificial neural networks. *Entropy*, 18(10), 350.