JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

Detect Denial of Service Attack using Hybrid Deep Neural Network

Nazanin Najm Abdulla[1]
Informatics Institute for Postgraduate
Studies Iraqi Commission for
Computers & Informatics(IIPS/ICCI)
Nazanin.shafi95@gmail.com

Rajaa K. Hasoun [2]
Department of Information System Management
The University of Information Technology and Communication
Baghdad, Iraq
dr.rajaa@uoitc.edu.iq

Received: 2022 March 15; **Revised:** 2022 April 20; **Accepted:** 2022 May 10

Abstract

Network hacking has become more resource-intensive in recent years, particularly in firms and organizations that rely on the internet, such as Amazon, because the hacker's goal is to prohibit the user from using the network's resources, whether the target is offensive or pecuniary. As a result, there are multiple methods for detecting intrusion and network penetration that use various ways to distinguish between legitimate and unauthorized users, including artificial intelligence systems (AI), deep learning (DL), and machine learning (ML).Organizations' network infrastructure is vulnerable to several threats, including break-ins, security breaches, and system exploitation. A network's Network Intrusion Detection System (NIDS) detects such penetration attacks and intrusions within the network. Pattern matching can easily detect recognized attacks, but new attacks are more difficult to detect.This study used a deep learning technique to build an intrusion detection model.Deep learning can perform better than classical machine learning used in earlier works in extracting features of enormous data while considering the vast cyber traffic in real life. In conclusion, the suggested approach involved training an IDS model using a hybrid deep neural

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

network using the entire NSL-KDD Dataset.The experimental results obtained from the system approved its success within a 100% accuracy value, which is considered a perfect detection rate of four attacks(DoS, Probe, U2R, and R2L), and for detecting DoS, the accuracy was 99% in NSL-KDD.

Keywords: Deep Neural Network, hybrid CNN, NSL-KDD, Denial of Services Attack, Performance Evaluation.

1 Introduction

Many attackers organize the transmission of a large amount of meaningless data to try to overload the target's computing resources or the close network links in a volumetric DOS attack. DOS is the most dangerous attack that causes network traffic problems[1]. Since the Computer Incident Warning Service announced the first attack event in 1999, DoS attacks have been one of the most persistent network security risks. Despite the reality that many defence mechanisms have been suggested in industry and academia, DOS attacks remain a major threat increasing yearly. DoS attacks are an essential security issue in any network architecture. The full network can be damaged by overlapping bandwidth like DOS attacks. The enemy can use various methods to fake packet fields and send huge traffic tables and regular traffic to SDN architecture, leading bandwidth and other resources to be depleted. The controller is flooded with faked flows without an efficient security system, forcing the controller to fail by establishing new flow rules and actions[2].Social network analysis is one of the many applications for machine learning, which has gained popularity over the years,text mining and multimedia concept retrieval. DL, a machine learning technique, is frequently applied in these disciplines. Due to the data's quick growth and availability and the hardware industry's amazing developments, new distribution and hardware computing research have surfaced. Deep learning significantly outperformed its predecessors and was inspired by conventional neural networks. It develops a multi-layered learning model using graph technology and neuronal transformations[3].Deep learning networks incorporate numerous deep layer units with highly optimized algorithms and designs. This study examines several optimization techniques to increase training precision and shorten training duration.This paperwill use a

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

deep learning methodology to create an IDS model for this study. Given the massive amount of cyber traffic activity, Deep learning can outperform classical machine learning, which was used in prior studies to extract features from large datasets. As a result, A suggestion was made for training an IDS model utilizing the entire NSL-KDD Dataset using the proposed hybrid deep learning strategy.

2 Related works

Md Moin Uddin Chowdhury et al. (2017) provided instructions on acquiring some deep learning techniques to improve intrusion detection. They first developed a deep CNN for intrusion detection. They used the results from various deep CNN levels to construct a linear support vector machine and 1-nearest neighbour classifier for a few intrusion detections. Few-shot learning is a cutting-edge approach for dealing with scenarios when the number of training instances for a given class is limited. They tested their method using the KDD99 and NSL-KDD datasets, which simulate penetration in a military network.[4].

Shreekhand Wankhede et al. (2018).this study creates a deep intrusion detection model that is integrated and based on SDAE-ELM. An integrated deep intrusion detection model based on DBN-Softmax is created for host intrusion detection, significantly enhancing the detection accuracy of host intrusion data.The Dataset was split into several splits throughout testing, and the best split for the RF and MLP techniques was found.The Random forest algorithm performs better than MLP when the outcomes of the two methods are compared[5].

Yalei Ding et al. (2018) use a deep learning methodology to develop an IDS model in this paper. Given the enormous amount of cyber traffic that exists in real life, they believe that deep learning, as opposed to traditional machine learning, has the opportunity to be successful when extracting characteristics from big data. As a result, to speed up processing, consume fewer system resources, and maintain accurate detection rates, CNN decreases the data vector dimension. Their learning data sets were pre-classified using a Neural Network in the following step. They contrast the model's performance with multi-class classification to deep learning techniques like Deep Belief Network, LSTM, and traditional machine learning techniques like RF and SVM [6].

Sinh-Ngoc Nguyen et al. (2018),an essential component for seeing and blocking unauthorized traffic before it damages the

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

system is the intrusion detection system (IDS). The protected system will be secured in real-time if this system can gather data from a network system and immediately suggest a solution. However, it is very challenging to detect them due to the enormous amount and complexity of malicious. Additionally, certain detecting systems challenge with the speed of implementation and accuracy. In this study, they present IDS-CNN, a DoS detection tool built on convolutional neural networks (CNN). Our CNN-based DoS detection experiments show that it is highly accurate, with a maximum accuracy of 99.87 percent. There are additional comparisons with other machine learning methods accessible.[7].

XIANWEI GAO et al. (2019) this paper explore recent advancements and lasting issues in intrusion detection technology utilizing the NSL-KDD data set as the research object. It also presents an adaptive ensemble learning methodology. They develop a MultiTree algorithm by altering the proportion of training data and building several decision trees. They select some base classifiers, such as decision trees, random forests, KNNs, and DNNs, and create an ensemble adaptive voting algorithm to enhance the overall detection impact. The adaptive voting technique's overall accuracy is 85.2 percent, whereas the MultiTree algorithm's accuracy is 84.2 percent, according to NSL-KDD [8].

Fatima Zohra Belgrana et al. (2020) Using Databases to Find the New Chosen Having to learn Discovery One of the goals of this study is to identify the crucial elements of the data set the NSL- KDD that influence the outcome of the detection. Therefore, they will absorb the negative aspects of the Dataset. They started by implementing our Network IDS (NIDS) using the Condensed Nearest Neighbors algorithm. Given that it considers sample distribution, it is a particularly good method for classification and regression. CNN decreases the data vector dimension to speed up processing, consume less system resources, and maintain accurate detection rates. Their learning data sets were pre-classified using a Neural Network in a second technique[9].

AANSHI BHARDWAJ et al. (2020) use a Deep Neural Network (DNN) with a well-stacking sparse Autoencoder (AE) for feature learning; this study provides a unique architecture for separating network traffic into DDoS assault traffic and benign traffic. DNN and AE are most effective at detecting DDoS attacks by modifying the settings using appropriately developed procedures. The

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

proposed adjustments result in a more manageable network that avoids exploding and disappearing gradients, minimizes reconstruction errorand guards against overfitting. Performance metrics such as detection F1-Score, accuracy, recall, and precision were utilized to contrast the suggested strategy with ten cutting-edge strategies. Validation tests were conducted on the CICIDS2017 and NSL-KDD benchmark datasets. The proposed approach outperforms current methods and yields outcomes comparable to the CICIDS2017 Dataset on the NSL-KDD[10].

Lokesh Karanam et al. (2020),to deal with the problem of an unbalanced data set this work employs CNN to choose feature characteristics from the input data and then feed these features to LSTM for sequence analysis. The weight given to each example will be determined using the cost function technique depending on each class's overall number of training examples. To further reduce the cost of computing, the raw input data format is transformed into a matrix format (picture). Using a common NSL-KDD, this study assesses the CNN-LSTM model's performance. The test findings revealed that the model trains had a 99.6% accuracy and a 96.75% detection rate[11]

Mahmoud Said ElSayed et al. (2021) suggest a unique hybrid deep learning method built on convolutional neural networks (CNN). A unique regularization technique called SD-Reg has been used to combat overfitting and improve the ability of NIDSs to identify unobserved intrusion events. The weight matrix's standard deviation serves as the foundation for SD-Reg. The evaluation results show that the SD-Reg outperforms the earlier regularized procedures. Additionally, the proposed hybrid technique outperforms single DL models in all evaluation measures[12].

3 NSL_KDD Dataset

The NSL_KDD Dataset, which is an improvement to the KDD'99 D, the NSL_KDD data set was proposed as a solution to some of the KDDCUP'99 data set fundamental issues. The most extensively used data set for anomaly detection is KDDCUP'99[13]. Hundreds of thousands of connection records are included in the collection, each of which defines a normal or abnormal status, as shown in (figure1) the features in the Dataset.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

Fig.1 properties of several NSL-KDD dataset kinds

Type	Features
Nominal	Protocol_type(2), Service(3), Flag(4)
Binary	Land(7), logged_in(12), root_shell(14), su_attempted(15), is_host_login(21),, is_guest_login(22)
Numeric	Duration(1), src_bytes(5), dst_bytes(6), wrong_fragment(8), urgent(9), hot(10), num_failed_logins(11), num_compromised(13), num_root(16), num_file_creations(17), num_shells(18), num_access_files(19), num_outbound_cmds(20), count(23) srv_count(24), serror_rate(25), srv_serror_rate(26), rerror_rate(27), srv_rerror_rate(28), same_srv_rate(29) diff_srv_rate(30), srv_diff_host_rate(31), dst_host_count(32), dst_host_srv_count(33), dst_host_same_srv_rate(34), dst_host_diff_srv_rate(35), dst_host_same_src_port_rate(36), dst_host_srv_diff_host_rate(37), dst_host_serror_rate(38), dst_host_srv_serror_rate(39), dst_host_rerror_rate(40), dst_host_srv_rerror_rate(41)

Feature encoding and data normalization are used to preprocess network data. In the min-max normalization technique, network attribute values were scaled into a similar value range as part of the network feature normalization process. The feature conversion procedure is required to transform feature data that is not numerical into numerical values. The Dataset includes 42 features, as shown in (Table 1) and 125973 records. It contains five classes, one of which is normal and four of which are attacks, including the Probe, Remote to Local (R2L), User to Root (U2R), and Denial of Service (DoS), the latter of which has just 7458 records[14].

Whenever an attacker makes a computer or memory resource too busy or full to respond to legitimate requests, denying access to authorized users, this is referred to as a DoS attack. An effort to learn more about a computer network to evade security measures is known as a probing attack. An attacker who can send packets via a network but does not have access to that system engages in a remote-to-local attack (R2L). The User to Root (U2R) is a type of hacking for which the offender gains access to a system ordinary user account first (password sniffing, perhaps via a dictionary attack,or social engineering), then uses a vulnerability to gain root access[13].

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

4 The Proposed System

This study provides a classification system based on feature selection for detecting DoS assaults; as shown in Fig. 1,the NSL KDD dataset hybrid deep neural network model was utilized to detect attacks. The recommended structure in (Fig. 1) is partitioned into five stages:

- Load Dataset
- Divided Dataset into two-part train and test
- Preprocessing train and test part
- Apply algorithms on data set to detect all attacks type
- Evaluation result

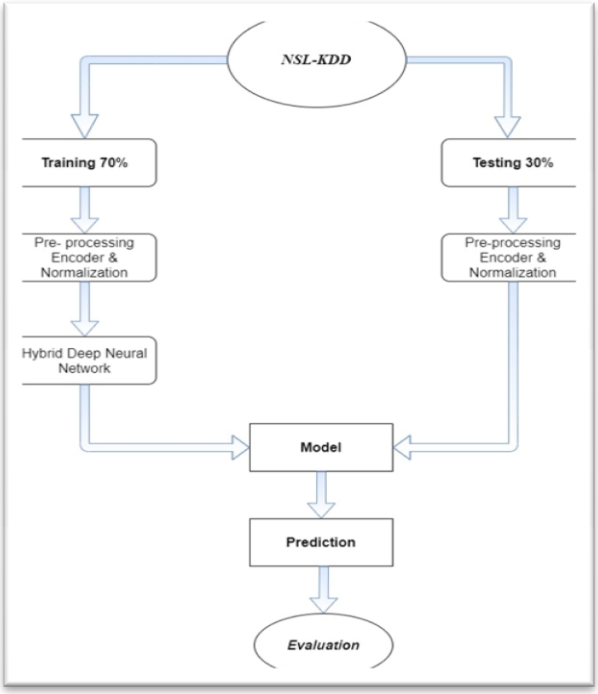


Figure1. The architecture of the proposed system

4.1. **Dataset:**using Dataset is the first step in the proposed system is to load the NSL_KDD Dataset.

4.2. Dataset partition stage

Before preprocessing and applying algorithms, this stage involves partitioning the Dataset into two parts: 70% for training and 30% for testing.

4.3. Preprocessing stage

This is a third stage that deals with data encoding and min-max normalization; supplying uniform and smooth data, this stage

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

makes it easier for classification algorithms to produce effective results in the shortest amount of time. The character values are replaced with numeric values throughout the encoding process. On the other hand, the normalizing procedure handles noisy inputs and keeps feature values within a set range (-1 and 1).

4.4. Detection stage

Techniques of detection in the implementation of IDS, DL and ML techniques are currently being used extensively. The benefit of a deep learning algorithm is its capacity to draw out relevant facts from a dataset. Using a deep hybrid model improves attack detection performancefrom nine layers. In terms of prediction accuracy, this technique outperforms a single model. In this paper, an open-source deep-learning library, Keras, was attained to implement the deep hybrid model and explained how to probe; U2R, R2L, and DoS attacks were detected by using a deep hybrid model; the first step of applying the model to a dataset to detect the four types of attacks and evaluate their performance. After that, apply the same techniques to the Dataset to detect only DoS attacks and measure the performance of the detection process.

4.5Hybrid Deep Neural Network

The proposed deep model includes nine layers: CNN is a one-dimensional kind with nine layers: three 1D conventional layers, three Max pooling layers, one LSTM layer, one Dropout layer, and one dense layer. The model is trained on the Dataset to detect all forms of assaults, and the testing subset is used to evaluate the detection outcomes on the deep hybrid model. The model is then trained on the Dataset to detect DoS in this Dataset exclusively. The activation function, responsible for deciding the outcome from the neural network and used in each layer, is one of the most critical factors in the suggested deep CNN model for success in classification. The most useful activation function in deep learning models for classification and prediction is ReLU (Rectified Linear Units). The Stride is the neural network filtering parameter that regulates the number of moves across the data, and it is equal to 1 in this study, while the Kernel is equal to 3. Padding is in charge of expanding the range of data and ensuring its validity.

5. Evaluated performance: using (accuracy, precision, recall, and f1-score). Performance was assessed using the same methods but exclusively to the Dataset DoS attack detection.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

6. **Result**: It deals with recognizing data instances in the Attack or Normal condition and is the last level of the suggested architecture. This step is thoroughly covered in the following section. This work created a hybrid deep neural network model using ensemble techniques on the NSL-KDD Dataset. The preprocessing was done in Python.

1. Results and discussion

As a result, in this portion of the article, we give the testing results of the proposed method in terms of classification model creation time, accuracy, and false positives. Also, compare it to various machine learning approaches that are currently available. For evaluation purposes, the evaluation of a classifier on a test dataset and Stratified Cross-Validation is seen as more relevant. The training and testing datasets provided by NSL KDD are used to assess the classification accuracy. The suggested approach is contrasted with other widely used deep learning methods. The findings of the suggested framework are discussed in this section. Various accuracy measurements derived from the confusion matrix are used to assess performance. The measurement outcome when ensemble methods are used on the Dataset to find every type of attack in the Dataset.The proposed model techniques have higher accuracy of 100%. When ensemble algorithms are applied to a dataset to detect only DoS attacks in the entire Dataset without employing feature selection approaches, the model has the greatest detection DoS accuracy of 99.9%. As demonstrated by a compare the accuracy of several algorithms in related works on the NSL_KDD Dataset, as shown in Table 2

Table 2 Comparison of the Proposed System with Previous Studies

Ref	**NSL-KDD features**	**AI Direction**		**No. of DL layer**	**Attack Types**	**Performance Measurement**				**Execution Time**
		ML	**DL**			Accuracy	Precision	Recall	F1-measure	
[4]	20	K-NN	CNN	13	U2R	ML 80% DL 94%	-	-	-	-

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

[6]	41	-	CNN	15	DoS R2L	80%	85%	-	-	-
[15]	18 41	Bagging	-	-	Probe DoS R2L U2R	99% 77.5%	99% 83.6%	99% 81.2%	-	 5.7s
[8]	41	Ada Boost	DNN	11	-	ML 76% DL 81%	81% 84%	76% 81%	72% 80%	277.8s
[16]	14	LG NB	-	-	DDoS	LG 88% NB 93%	86% 90.3%	85% 95 %	86% 90%	-
[10]	25	-	AE+ DNN	-	DDoS	98.3%	99.2%	97.1%	98.5%	-
[17]	28	XGB	-	-	7 DoS types	97%	97%	96.8%	-	-
[18]	23	LSTM+ SVM	-	-	DDoS	90%	95%	82 %	88%	-
[19]	18 41	RF	-	-	Probe DoS	99% 98%	-	-	-	-
[20]	41	J48+CAR T	-	-	DoS, probe, U2R, R2L	99%	-	-	-	-

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

Proposed system	**41**	**Bagging**	**Hybrid deep (CNN, LSTM, max-pooling, dropout, dense)**	**9**	**DoS, probe, U2R, R2L**	**ML 99.5% DL 100%**	**99.5 % 100%**	**99.5% 100%**	**99.5% 100%**	**6.4 MS 3.4 S**

Classification Phase Results and Measurement based on the proposed hybrid Deep Learning

Results and Measurement from the Classification Phase Using DL, the results of implementing the proposed hybrid deep learning algorithm for performing the classification procedure to detect four types of attacks in NSL-KDD were demonstrated in this thesis section. The proposed hybrid deep learning consists primarily of multi-layers of the types conventional, LSTM, dense, and max-pooling. Its detailed architecture is shown in table (3), which includes a complete description of each layer's parameters and the output shape.

Table 3Deep learning report for detection 4 types of attack (U2R, Dos, Probe, R2L)

conv_1 (ConvID)	(none, 39, 16)	64
max_poolingId_1 (Max/pooling1)	(none,39,16)	0
conv_2 (ConvID)	(none,37,32)	1568
max_poolingId_2 (Max/pooling1)	(none,37,32)	0
conv_3 (ConvID)	(none,35,64)	6208
max_poolingId_3 (Max/pooling1)	(none,17,64)	0
lstm_1 LSTM	(none,70)	37800
dropout_1 Dropout	(none,70)	0
dense_1 Dense	(None,1)	71
total params: 45,711		
trainable params:45,711		
non-trainable params:0		

Classification Phase Results and Measurement based on the proposed hybrid Deep Learning to detect DoS Attack

Results and Measurements from the Classification Phase Using DL, the results of

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452

implementing the proposed hybrid deep learning algorithm for performing the classification procedure to detect DoS attack types in NSL-KDD were demonstrated in this thesis section. The proposed hybrid deep learning consists primarily of multi-layers of the types conventional, LSTM, dense, and max-pooling. Its detailed architecture is shown in table (4), which includes a complete description of the parameters of each layer and the output shape.

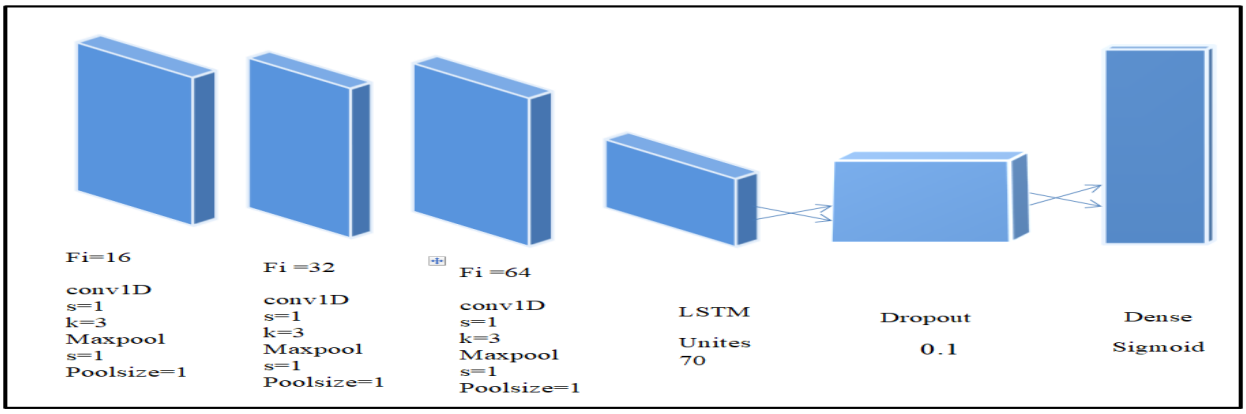
Table 4 Deep learning report for detection only DoS type in NSL-KDD

conv_1 (ConvID)	(none, 39, 16)	64
max_poolingId_1 (Max/pooling1)	(none,39,16)	0
conv_2 (ConvID)	(none,37,32)	1568
max_poolingId_2 (Max/pooling1)	(none,37,32)	0
conv_3 (ConvID)	(none,35,64)	6208
max_poolingId_3 (Max/pooling1)	(none,17,64)	0
lstm_1 LSTM	(none,70)	37800
dropout_1 Dropout	(none,70)	0
dense_1 Dense	(none, 8)	568
total params: 46,208		
trainable params:46,208		
non-trainable params:0		

6 Conclusions

Network Intrusion Detection System (NIDS) detects such penetration attacks and intrusions. Pattern matching can easily detect known forms of attacks, but it is more difficult to detect new attacks. This paperused a deep learning methodology to construct an IDS model in this research. When extracting features from huge data, deep learning has the potential to outperform standard machine learning, taking into account the massive volume of real-world internet traffic. The suggestion was to use a hybrid deep learning approach to build an IDS model on the whole NSL-KDD Dataset that included nine layers of Neural Networks (CNN), a popular deep learning technique.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 3696-3710
https://publishoa.com
ISSN: 1309-3452



References

[1] N. Bindra and M. Sood, "Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset,"*Autom. Control Comput. Sci.*, vol. 53, no. 5, pp. 419–428, 2019, doi: 10.3103/S0146411619050043.

[2] A. A. Aburomman and M. B. I. Reaz, "A survey of intrusion detection systems based on ensemble and hybrid classifiers,"*Comput. Secur.*, vol. 65, pp. 135–152, 2017, doi: https://doi.org/10.1016/j.cose.2016.11.004.

[3] M. E. A. Ibrahim and Q. Abbas, "Current and Future Trends of Deep Learning based Visual Attention,"*Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 1, pp. 155–160, Jan. 2019.

[4] M. M. U. Chowdhury, F. Hammond, G. Konowicz, C. Xin, H. Wu, and J. Li, "A few-shot deep learning approach for improved intrusion detection,"*2017 IEEE 8th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2017*, vol. 2018-Janua, pp. 1–7, 2018, doi: 10.1109/UEMCON.2017.8249084.

[5] S. Wankhede and D. Kshirsagar, "DoS Attack Detection Using Machine Learning and Neural Network," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, Aug. 2018, pp. 1–5, doi: 10.1109/ICCUBEA.2018.8697702.

[6] Y. Ding and Y. Zhai, "Intrusion detection system for NSL-KDD dataset using convolutional neural networks,"*ACM Int. Conf. Proceeding Ser.*, pp. 81–85, 2018, doi: 10.1145/3297156.3297230.

[7] S.-N. Nguyen, V.-Q. Nguyen, J. Choi, and K. Kim, "Design and implementation

of intrusion detection system using convolutional neural network for DoS detection," in *ACM International Conference Proceeding Series*, 2018, pp. 34–38, doi: 10.1145/3184066.3184089.

[8] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, "An Adaptive Ensemble Machine Learning Model for Intrusion Detection,"*IEEE Access*, vol. 7, pp. 82512–82521, 2019, doi: 10.1109/ACCESS.2019.2923640.

[9] F. Z. Belgrana, N. Benamrane, M. A. Hamaida, A. M. Chaabani, and A. Taleb-Ahmed, "Network Intrusion Detection System Using Neural Network and Condensed Nearest Neighbors with Selection of NSL-KDD Influencing Features,"*IoTaIS 2020 - Proc. 2020 IEEE Int. Conf. Internet Things Intell. Syst.*, pp. 23–29, 2021, doi: 10.1109/IoTaIS50849.2021.9359689.

[10] A. Bhardwaj, V. Mangat, and R. Vig, "Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of ddos attacks in cloud,"*IEEE Access*, vol. 8, pp. 181916–181929, 2020, doi: 10.1109/ACCESS.2020.3028690.

[11] L. Karanam, K. K. Pattanaik, and R. Aldmour, "Intrusion Detection Mechanism for Large Scale Networks using CNN-LSTM,"*Proc. - Int. Conf. Dev. eSystems Eng. DeSE*, vol. 2020-Decem, pp. 323–328, 2020, doi: 10.1109/DeSE51703.2020.9450732.

[12] M. S. ElSayed, N.-A. A. Le-Khac, M. A. Albahar, and A. Jurcut, "A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique,"*J. Netw. Comput. Appl.*, vol. 191, p. 103160, Oct. 2021, doi: https://doi.org/10.1016/j.jnca.2021.103160.

[13] H. Chae, B. Jo, S. Choi, and T. Park, "Feature Selection for Intrusion Detection using NSL-KDD,"*Recent Adv. Comput. Sci. 20132*, pp. 184–187, 2013.

[14] C. C. Ugwu, O. O. Obe, O. S. Popoola, and A. O. Adetunmbi, "A distributed denial of service attack detection system using long short term memory with Singular Value Decomposition,"*Proc. 2020 IEEE 2nd Int. Conf. Cyberspace, CYBER Niger. 2020*, pp. 112–118, 2021, doi: 10.1109/CYBERNIGERIA51635.2021.9428870.

[15] S. Liu, L. Wang, J. Qin, Y. Guo, and H. Zuo, "An intrusion detection model based

on IPSO-SVM algorithm in wireless sensor network,"*J. Internet Technol.*, vol. 19, no. 7, pp. 2125–2134, 2018, doi: 10.3966/160792642018121907015.

[16] S. Das, D. Venugopal, and S. Shiva, "A Holistic Approach for Detecting DDoS Attacks by Using Ensemble Unsupervised Machine Learning,"*Adv. Intell. Syst. Comput.*, vol. 1130 AISC, pp. 721–738, 2020, doi: 10.1007/978-3-030-39442-4_53.

[17] J. Liu, B. Kantarci, and C. Adams, "Machine learning-driven intrusion detection for Contiki-NG-based IoT networks exposed to NSL-KDD dataset,"*WiseML 2020 - Proc. 2nd ACM Work. Wirel. Secur. Mach. Learn.*, pp. 25–30, 2020, doi: 10.1145/3395352.3402621.

[18] C. C. Ugwu, O. O. Obe, O. S. Popoọla, and A. O. Adetunmbi, "A Distributed Denial of Service Attack Detection System using Long Short Term Memory with Singular Value Decomposition," in *2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA)*, Feb. 2021, pp. 112–118, doi: 10.1109/CYBERNIGERIA51635.2021.9428870.

[19] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods,"*IEEE Access*, vol. 7, pp. 51691–51713, 2019, doi: 10.1109/ACCESS.2019.2908998.

[20] A. Iqbal, S. Aftab, I. Ullah, M. A. Saeed, and A. Husen, "A Classification Framework to Detect DoS Attacks,"*Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 9, pp. 40–47, 2019, doi: 10.5815/ijcnis.2019.09.05.