Performance Analysis of Intrusion Detection System using CNN, ANN and DNN

[1]Jeyavim Sherin R C
School of Computer Science and Engineering
Vellore Institute of Technology
Chennai, India
jeyavimsherin.rc2021@vitstudent.ac.in

[2]Dr. Parkavi K
School of Computer Science and Engineering
Vellore Institute of Technology
Chennai, India
parkavi.k@vit.ac.in

***Abstract*—The Network Intrusion Detection System (NIDS) is a crucial aspect of safeguarding against cyber threats in the domain of cybersecurity. The major drawback of conservative approaches like Machine Learning (ML) that involve manual feature selection is their dependency on human involvement, which can hinder their efficacy. Deep learning (DL) is one of the technologies widely used in intrusion detection systems, it increases the performance of the model and securing the networks and classify the attacks. The primary concern regarding both convergence and speed along with the uneven values of the input-hidden layer were addressed as a gap in NIDS. This research compares the Convolutional Neural Network (CNN), Deep Neural Network (DNN), and Artificial Neural Network (ANN) are all related to the field of neural networks. The Performance is evaluated using the following metrics like Accuracy, Precision, Recall and true positive rate. For evaluating the effectiveness of the proposed model in both binary and multiclass classifications, the benchmark dataset CSE-CIC-IDS2018 is utilized. As per the experimental findings, the CNN model demonstrated exceptional performance, achieving an impressive accuracy rate of 99.72%.**

***Keywords*—NIDS (Network Intrusion Detection System), CNN, DNN, ANN, DL, Cyber Security**

I. Introduction

Security has become an essential component of modern civilization as technology has advanced. The main concern is on the effectiveness to identify network intrusion and assure with higher security, dependability, and secrecy [1]. An intrusion detection system's primary purpose is to detect fraudulent traffic and prevent entering the network. It is becoming extremely difficult to monitor and detect network traffic because of the high system traffic, which is increasing vastly, and suspicious and regular traffic are easily combined in the flow, makes it difficult to detect for the threats communication network security. Malicious traffic can target servers, website and even individual users. It can perform malicious operations such as stealing personal information of people and attempt to steal, which poses a serious threat to cybersecurity [17]. The primary purpose of an IDS is to promptly detect attacks in real-time, restrict network access, and notify the network administrator to facilitate timely implementation of security measures. Machine Learning approaches are becoming commonly used methods for detecting network intrusion, some of the ML approaches are Signature based approaches, Fuzzy logic approaches and so on. The common methods in NIDS techniques are K-Means, Random Forest, Decision Tree (DT), Support Vector Machine (SVM) [2] which helps to detect malicious attacks. Researchers work to improve the detection of network attacks by combining Bayes, Decision trees and SVM, or SVM and K-means [3]. DL algorithms address the gap of manual selection of features in Traditional ML methods and show better results than traditional ML algorithms.

Intrusion detection is classified into two types based on the behavior - host-based intrusion detection systems (HIDS) detects by monitoring system activity and network-based intrusion detection systems (NIDS) [4]. captures the network activity. IDS can be divided into signature, anomaly and combination of anomaly-based and signature-based techniques called hybrid. This research compares the performance of three deep learning algorithms Artificial Neural Network, Convolutional, and Deep Neural Network in an intrusion detection system. CSE-CIC-IDS2018 is used as dataset for the comparison study, with the selection of 80 features from this dataset [20]. Accuracy, Precision and Recall are the metrics used to evaluate performance.

II. Literature Review

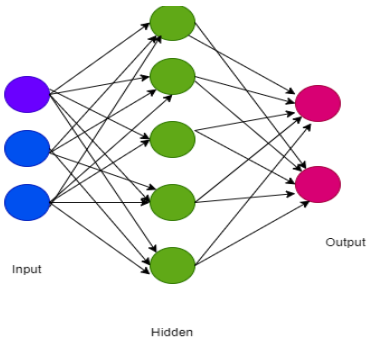
Intrusion detection concept was proposed by Anderson in 1980. Several researchers have used machine learning algorithms such as SVM, Random Forest, KNN, etc [11] [14]. When unauthorized and unlawful access is made, it can cause instability and, in extreme cases, the destruction of the system. To identify such intrusions in a network, the process of collecting all data packets from a specific network segment is known as Network Intrusion Detection System (NIDS) [5]. Network intrusion detection system is an important of network security. This paper proposed Gated Recurrent Unit (GRU) this model has achieved the accuracy of 89% [12]. In [13], authors applied hybrid framework of deep learning models and they achieved good performance. In the past, the artificial intelligence paradigm used machine learning approaches to deal with the problem of network intrusion. Furthermore, in this paper [15], "A Deep Auto encoder-based Approach for Intrusion Detection System" they attempted and approach the issue of NIDS from a DL perspective.

With the increasing complexity of modern attacks, conventional IDS methods are proving inadequate, prompting researchers to explore more innovative and efficient approaches. Some of these methods involve the use of artificial intelligence techniques to predict the type of attack before it happens. The researchers noted a problem for most ANN-based approaches [5]: Reducing the FNR and FPR rates significantly poses a significant challenge, with FP referring to an output with an incorrect positive class prediction and FN indicating an incorrect negative class prediction [18].

A. K. Visvam Devadoss et al. (eds.), *Proceedings of the 6th International Conference on Intelligent Computing (ICIC-6 2023)*, Advances in Computer Science Research 107,
https://doi.org/10.2991/978-94-6463-250-7_23

A. Artificial Neural Network (ANN)

Artificial Neural Network (ANN) is a machine learning model that takes inspiration from the human brain's structure and functioning. It mimics both its structure and its function. ANN is made up of many artificial neurons that are linked together using weighted links. Adjusting the weights and biases of an ANN is a common technique to improve its performance [7]. ANN is made up of perceptron units. An Artificial Neural Network (ANN) can be composed of multiple layers, with the most common architecture consisting of three types of layers: input, hidden, and output layers. The number of input layer neurons is determined by the number of data features [16]. The output layer in the binary classification into two types: attacks or normal traffic. Back propagation is the common technique for weights update. During the classification process, the input will read each set of data from the testing dataset.



FIGUEE 1.Training using ANN

B. Recurrent Neural Network (RNN)

RNNs are designed to handle sequences of inputs by maintaining a hidden state that captures information about the sequence so far. It is mainly used in the development of models that mimic the human brain activity [8] [9]. It acts like a chain.

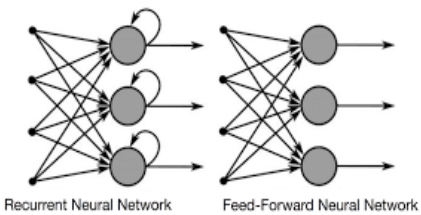


FIGURE 2. Training using RNN

C. Deep Neural Network (DNN)

DNN is one of the DL model which consists of two or more hidden layers. It is used to solve the real world problems [19]. It helps to detect and classify the unpredictable network attacks [6] [10]. DNN which is having 5 layers it is used to training the model and predicted the attacks and produce the results. We have built a model using DNN and got the accuracy is 97.6%. Fig. 8. Depicts the accuracy of DNN. The detection model can be structured below Table I. DNN Sequential model

TABLE 1. Dnn Sequential Model

Layer Type	Output Shape	Param #
dense (Dense)	(None, 64)	7872
dropout (Dropout)	(None, 64)	0
dense_1 (Dense)	(None, 128)	8320
dropout_1 (Dropout)	(None, 128)	0
dense_2 (Dense)	(None,512)	66048
dropout_2 (Dropout)	(None, 512)	0
dense_3 (Dense)	(None, 128)	65664
dropout_3 (Dropout)	(None, 128)	0
dense_4 (Dense)	(None, 1)	129

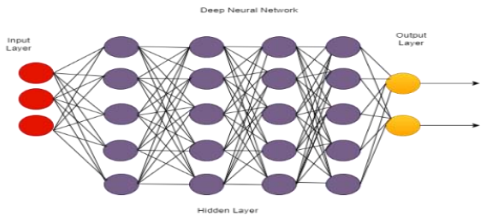


FIGURE 3. Training using DNN

III. SYSTEM DESIGN & IMPLEMENTATION

A. System Design

We have used CNN with the activation function ReLU and a Softmax classifier to proposed an IDS model. CNN is a DL technique that is widely used in many fields. However, the long-term dependency that can be addressed by ReLU, as discussed. As a result, we used Softmax to effectively classify the attacks. The following flow diagram depicts our proposed work. It consists of two parts: a selection of important features and a CNN model. The mentioned two methods that comprise the entire work depicted in Fig.4. are data preprocessing and classification.

B. Methodology

An essential benefit of Convolutional Neural Networks (CNNs) is their capability to automatically extract significant features from raw data, without requiring any manual feature engineering. This is accomplished through the use of convolutional layers that apply filters to the input data and learn to detect patterns and features in the data. The convolutional layers in a CNN can learn to detect patterns in the data that are indicative of normal or malicious network activity, and the network can then use this information to classify incoming traffic as either normal or suspicious.

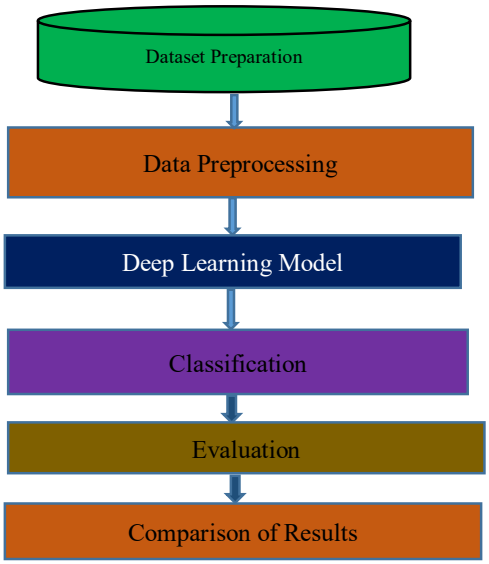


FIGURE 4. Proposed Framework of our Model

C. *Preparation of Dataset*

We used the Python programming language and the pandas library to import the CSE-CIC-IDS2018 dataset. It is the most popular dataset for assessing network intrusion detection systems. Our CSE-CIC-IDS2018 it contains 16,233,002 instances gathered from 10 days of network traffic in the dataset. We have use 6,62,721 samples for our research work. It is having 80 features.

D. *Data Preprocessing*

Data preprocessing is a critical step in machine learning, as it can have a significant impact on the accuracy and effectiveness of the model. Our CSE-CIC-IDS2018 after removing all redundancies, and the model will train and test sets. The CSE-CICIDS 2018 dataset was used to evaluate the effectiveness of our method. This data set having 7 different attack scenarios. Datasets are created using this technique which includes detailed descriptions of intrusions and theoretical models of distribution. The data are further cleaned, converted, and prepared for use as input into the machine learning algorithm once they are in the form of flow data. This stage entails checks for incorrect characters, the elimination of empty fields, the removal or modification of values (other than numbers), and the elimination of duplicate columns. Data preprocessing is necessary mainly because the data collected is often in various formats and sourced from different locations. It also ensures the effectiveness and the accuracy of the model being trained on this dataset. The size of the dataset is more than 6.89 GB which is greater when compare to CSE-CICIDS 2017 dataset. The Table II depicts the attack type of CSE-CICIDS 2018 Dataset.

TABLE 2. Attack type of cse-cicids 2018 dataset

Sl.No	Attack Type
1	Botnet
2	DoS attacks-GoldenEye
3	DoS attacks-Slowloris
4	Heartbleed
5	Web attacks
6	Infiltration
7	Port Scan

E. *Deep Learning Model*

The structure of our model is shown in Fig. 5. To initiate the CNN model, the raw data is fed into the first convolutional layer. Subsequently, the raw data is subjected to pooling, batch normalization, and dropout layers, culminating in the formation of a unified CNN layer that contains densely connected neurons. In order to achieve the best trade-off between detection accuracy and false positive rate, we integrated three CNN layers in our model.

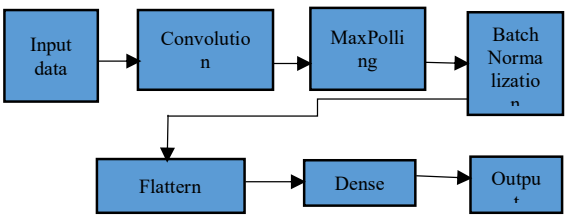


FIGURE 5. CNN Layer Structure

Convolution and pooling are two components of the Convolutional Neural Network (CNN). A series of filters will generate the feature map in convolution. Following that, an activation function will decide whether or not to fire the neuron. $ReLU(z_i) = max(0, z_i)$. The below equation (1) shows the ReLU function.

$$Z = h\left(\sum_i^{p*q} w_i\, v_i + b\right) \tag{1}$$

Max pooling can enhance the learning process and mitigate the risk of overfitting. Covariance shifts will be protected by batch normalization (BN). Batch Normalization is used to training of neural networks faster and stable via normalization of the layers. Deep neural networks experience covariance shifts, which cause input to change from one layer to the next, consequently influencing the efficiency of learning. BN will scale the data transfer from one layer to the next Lastly, dropout refers to the random loss of neurons. This layer is essential for preventing overfitting.

F. *Performance metrics*

Performance metrics are evaluated based on effectiveness, ease of use, cost, speed, CPU and memory needs, and scalability. The ability of IDS evaluation to predict accurate results demonstrates its effectiveness. The confusion matrix, also known as the error matrix, is a common tool used in machine learning to evaluate the performance of a classifier algorithm. It is a table that summarizes the predicted and actual classification results of a dataset, and it provides a quantitative measure of the classifier's performance. It depicts an event's performance in a structured format, with potential results. TP and TN values are used to measure the accuracy of the classifier, and they are essential metrics in evaluating the performance of a binary classifier. However, they do not differentiate between attack and normal behavior, as these terms are typically used in the context of cybersecurity or anomaly detection, where the focus is on identifying malicious behavior or anomalies.

False Positive (FP) occurs when the classifier predicts a positive instance, but it is, in fact, a negative instance. In the context of cybersecurity, this could mean that the classifier wrongly identifies a legitimate user or behavior as a potential attack or anomaly, resulting in false alarms or unnecessary security measures. These false positives can be considered as false alarms, which can cause confusion and potentially reduce the user's trust in the security system.

Therefore, it is essential to balance the trade-off between the FP and FN rates to achieve the optimal performance of the system. The goal is to minimize both the FP and FN rates to ensure that the system can accurately detect potential security risks while avoiding unnecessary false alarms. This can be achieved by continuously monitoring and fine-tuning the classifier's performance and updating the training data to reflect new types of attacks or anomalies that may emerge over time. As a result, a good IDS should have low FN and FP rates and high TN and TP rates. Some equations that can be used as performance measures for predicting accurate IDS based on the confusion matrix:

$$True\ Negative\ Rate\ (TNR) = \frac{TN}{FP+TN} \times 100 \quad (2)$$

$$True\ Positive\ Rate\ (TPR) = \frac{TP}{FN+TP} \times 100 \quad (3)$$

$$False\ Positive\ Rate\ (FPR) = \frac{FP}{TN+FP} \times 100 \quad (4)$$

$$False\ Negative\ Rate\ (FNR) = \frac{FN}{TP+FN} \times 100 \quad (5)$$

$$Precision = \frac{TP}{FP+TP} \times 100 \quad (6)$$

$$Accuracy = \frac{TN+TP}{TP+TN+FN+FP} \times 100 \quad (7)$$

$$F1-Score = 2 \times \frac{Precision \times Recall}{Precision+Recall} \times 100 \quad (8)$$

IV. EXPERRIMENTAL RESULTS

Our model was evaluated using the Pandas, Tensor Flow, and Keras packages were used to create the deep learning model. The model was evaluated based on type of attack type (DoS attacks-Hulk, DoS attacks-SlowHTTPTest, DoS attacks-GoldenEye, DoS attacks-Slowloris, Web attack, Bot). The Table II. shows the classification report of CSE-CICIDS 2018-CNN.

TABLE 3. Classification Report of cse-cicids 2018-cnn

	Precision	Recall	F1-Score	Support
benign	0.81	0.99	0.89	1972
DoS attacks-GoldenEye	0.99	0.99	0.99	2031
DoS attacks-Slowloris	1.00	0.77	0.87	1997
accuracy			0.99	6000
macro avg	0.98	0.99	0.99	6000
weighted avg	0.98	0.99	0.99	6000

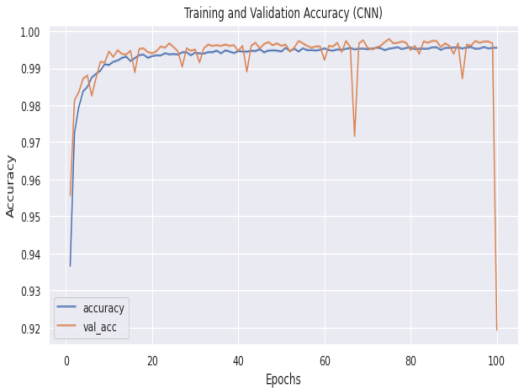


FIGURE 6.Training and Validation Accuracy (CNN)

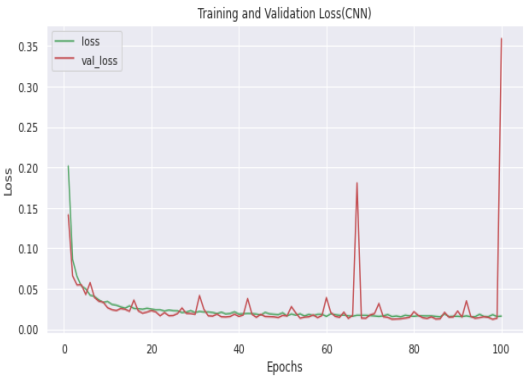


FIGURE 7. Training and Validation Loss (CNN)

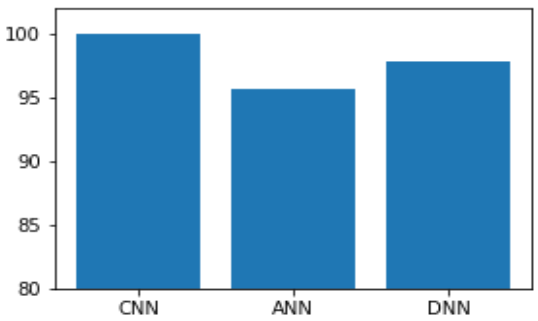
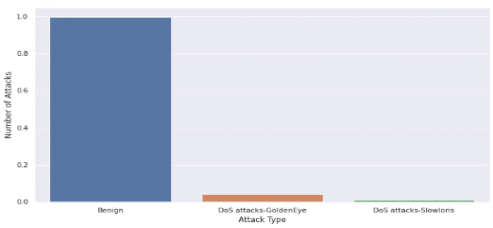


FIGURE 8. Accuracy of ANN, DNN and CNN



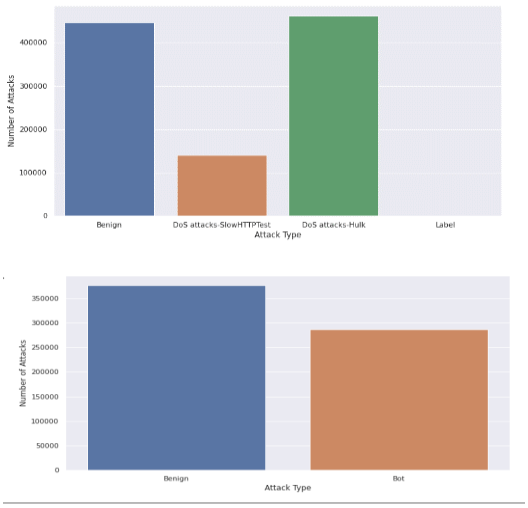


FIGURE 9. Classification of Attacks

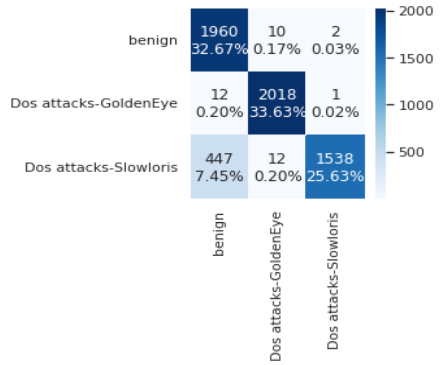


FIGURE 10. Confusion Matrix

V. CONCLUSION AND FUTURE WORKS

The detection and classification of intrusions or cyberattacks in a network infrastructure is essential, and the Intrusion Detection System (IDS) plays a critical role in achieving this in real-time. The IDS is classified based on its ability to detect threats are three types- Signature-based IDS, anomaly-based IDS, and hybrid IDS. This paper focus on the detect network intrusions using systems that uses anomaly-based deep neural networks and convolutional neural algorithms and artificial neural network. The performance evaluation metrics on Accuracy, Precision, and Recall are discussed in the results, it clearly shows CNN performed well in the experiments.

Hence, CNN has outperformed in this research, it opens the room to explore and compare with other deep learning algorithms LSTM, GRU, RNN. Likewise, further examination of performance using different datasets, like UNSW-NB15, CICIDS 2019, useful to evaluate the results.

VI. REFERENCES

[1] Akgun, D., Hizal, S., & Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Computers and Security, 118, 102748.

[2] Al-Emadi, S., Al-Mohannadi, A., & Al-Senaid, F. (2020). Using Deep Learning Techniques for Network Intrusion Detection. 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020, 171–176.

[3] Amutha, S., Kavitha, R., Srinivasan, S., & Kavitha, M. (2022). Secure network intrusion detection system using NID-RNN based Deep Learning. Proceedings - IEEE International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2022, 1–5.

[4] Calisir, S., Atay, R., Pehlivanoglu, M. K., & Duru, N. (2019). Intrusion Detection Using Machine Learning and Deep Learning Techniques. UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering, 656–660.

[5] Choraś, M., & Pawlicki, M. (2021). Intrusion detection approach based on optimised artificial neural network. Neurocomputing, 452, 705–715.

[6] Kasongo, S. M. (2023). A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Computer Communications*, *199*(December 2022), 113–125.

[7] Kim, K., & Aminanto, M. E. (2018). Deep learning in intrusion detection perspective: Overview and further challenges. Proceedings - WBIS 2017: 2017 International Workshop on Big Data and Information Security, 2018-Janua, 5–10.

[8] Kocher, G., & Kumar, G. (2021). Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. Soft Computing, 25(15), 9731–9763.

[9] Peng, K., Leung, V. C. M., Zheng, L., Wang, S., Huang, C., & Lin, T. (2018). Intrusion detection system based on decision tree over big data in fog environment. Wireless Communications and Mobile Computing, 2018.

[10] Qazi, E. ul H., Imran, M., Haider, N., Shoaib, M., & Razzak, I. (2022). An intelligent and efficient network intrusion detection system using deep learning. Computers and Electrical Engineering, 99(February 2021), 107764.

[11] Yang, H., Zeng, R., Xu, G., & Zhang, L. (2021). A network security situation assessment method based on adversarial deep learning. Applied Soft Computing, 102.

[12] Tang, T. A., McLernon, D., Mhamdi, L., Zaidi, S. A. R., & Ghogho, M. (2019). Intrusion detection in sdn-based networks: Deep recurrent neural network approach. Advanced Sciences and Technologies for Security Applications, 175–195.

[13] Akshay Kumaar, M., Samiayya, D., Vincent, P. M. D. R., Srinivasan, K., Chang, C. Y., & Ganesh, H. (2022). A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning. Frontiers in Public Health, 9(January), 1–18.

[14] Swarnalaxmi, S., Elakkiya, I., Thilagavathi, M., Thomas, A., & Raja, G. (2018). User Activity Analysis Driven Anomaly Detection in Cellular Network. 2018 10th International Conference on Advanced Computing, ICoAC 2018, December 2018, 159–163.

[15] Memon, R. A., Qazi, S., & Khan, B. M. (2021). Design and Implementation of a Robust Convolutional Neural Network-Based Traffic Matrix Estimator for Cloud Networks. Wireless Communications and Mobile Computing, 2021.

[16] Sarhan, M., Layeghy, S., Moustafa, N., Gallagher, M., & Portmann, M. (2021). Feature Extraction for Machine Learning-based Intrusion Detection in IoT Networks.

[17] Kocher, G., & Kumar, G. (2021). Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. Soft Computing, 25(15), 9731–9763.

[18] Amutha, S., Kavitha, R., Srinivasan, S., & Kavitha, M. (2022). Secure network intrusion detection system using NID-RNN based Deep Learning. Proceedings - IEEE International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2022, 1–5.

[19] Almomani, O. (2020). SS symmetry Detection System Based on PSO , GWO , FFA and. A Feature Selection Model for Network Intrusion Detection System Based on PSO, GWO, FFA and GA Algorithms, 33(32), 1–22.

[20] Kunang, Y. N., Nurmaini, S., Stiawan, D., & Suprapto, B. Y. (2021). Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. Journal of Information Security and Applications, 58(March), 102804.

[21] Hammad, M., Hewahi, N., & Elmedany, W. (2022). MMM-RF: A novel high accuracy multinomial mixture model for network intrusion detection systems.