*International Journal of Information Systems and Computer Technologies (IJISCT) Vol. 3, No.2*
*ISSN: 2791-3635(Print), 2791-3643(Online).* DOI: https://doi.org/10.58325/ijisct.003.02.0088

# Classification of Malicious Intrusion through ANN-CNN Sequential Classifier

Humza Rana*[1]

[1]Department of Computer Science, Bahauddin Zakariya University Multan, Pakistan.

Corresponding Author: Humza Rana (Humza.Rana99@gmail.com)

**ABSTRACT**
Network intrusion is an activity that disturbs the normal working of computer systems like stealing important data, destroying useful information, and slow functioning in file systems. In recent years network intrusion has become worse because it gets more advanced day by day and difficult to classify the intrusion. It is now important to prevent future threats from malicious intrusion. The old methods used in the prevention and classification of intrusion now become useless and very slow. The advanced method which is AI is required for this task which also saves time and performs classification accurately. The DL based Hybrid-model is presented in this paper for classification. This paper aims to propose a neural network model named ANN-CNN sequential classifier for classifying network intrusion. This multiclass hybrid deep learning model is trained on the multiclass dataset to check model performance in the multiclass nature of data. The proposed model is highly tuned by its parameter to take the best performance from a combination of both neural networks model Artificial Neural Network and Convolutional Neural Network and with selection of dropout value to prevent overfitting. The proposed approach applies to three multiclass datasets named WSN Dataset in 5 classes, Microsoft Malware Dataset in 9 classes, and Virus Malware Digits in 10 classes after an experiment with 99.6%,99.6%, and 98.1% results. The proposed approach is also compared with a different deep learning model that shows the proposed model's excellence from others. The proposed model achieves up to 99% accuracy on multiclass datasets.

**Keywords:** Deep Learning; Artificial Neural Network; Convolutional Neural Network; Network Intrusion.

## 1. INTRODUCTION

The Intrusion detection system determines the malicious type of behavior in network traffic. It prevents and keeps safe from unauthorized users or steals information of the users. Cyber-criminals use advanced methods to break the security without being unaware of users. Intrusion in networks is now advanced with time and comes in different forms. The intrusion detection method is in two types signature-based and anomaly-based however these old methods now become useless [1]. Malicious intrusion or malicious activity is designed to destroy the normal activity of a computer system and its functions. It may also cause personal information leakage, important file deletion, and different types of fraud to computer users. The malicious intrusion may be of different types like malware, phishing, and injections [2]. The number of internet users increases which will also cause a rise in the chances of intruders taking advantage and demanding money. As the technology becomes advanced it is more difficult to classify the intrusion [3]. Additionally, various kinds of intruders need different detection methods to deal with them. The old methods cannot classify the intrusion type due to their model complexities [4]. Thousands of malicious files are developed every day that disturb computer systems all over the world [5]. The old methods and algorithms have now become lazy and unable to determine the advanced type of malicious pattern. The deep learning algorithms now used by researchers to determine malicious activity for many years classify malicious instances accurately and fast [6]. Several deep learning models were proposed in previous years that classify the malicious activity at best performance but the performance as it single model. The existing model is also time-consuming and lazy performance in multiclass classification. Joshi et al. 2021 [7] presented a feature extraction technique using ANN. Two classes were used in their experiment. The model needs to be trained in multiclass datasets. In this paper, the ANN-CNN sequential classifier is proposed to determine the malicious intrusion for different classes. This model is proposed by combining the two strong deep learning models including the artificial neural network and convolution neural network to make the model perform classification at the highest rate. This hybrid model is trained by the tuned parameters to take the best performance from the model in the classification. The model was applied to the three multiclass datasets to evaluate the model performance in classification.

### *1.1 PROBLEM*

The existing deep learning models of a multiclass nature time time-consuming. The number of multiclass datasets needs to be evaluated by the model for real performance. Comparison of the proposed approach with any existing approach needed and time performance by the model performance. Intrusion types get advanced day by day and break the security easily highly advanced security methods need to detect the intrusion in the network.

### *1.2 CONTRIBUTION*

The hybrid deep learning model is proposed to perform powerful classification in malicious activity. Three multiclass datasets were used for model evaluation. Compute the model time evaluation duration. Compare the proposed model with different deep learning model performance. Optimize the number of neurons and filters in the hybrid model to overcome the model complexity and time and dropout value to reduce overfitting.

## 2. RELATED WORK

Gupta et al. 2022 [8] propose a neural network approach for detecting malicious activity. The Microsoft Big Dataset 2015 was used in their experiment. After the experiment, they show 90.17% and 90.19% accuracy respectively. Their model covers 9 types of malicious classes. A lot of training and model tuning is required for the model's best performance in classification. Kalyan et al. 2022 [9] propose a CNN model for detecting malware. The model works for two classes only and performance-wise the model gives 95% accuracy. The model training is required for work with the multiclass malicious activity. The PE files used in the experiment are malicious and non-malicious types. Akhtar et al. 2022 [10] propose a CNN-LSTM model to determine the malicious activity. The dataset from the Kaggle is used in the experiment of two classes. After an experiment, the model gives 99% detection accuracy. The model is required to be trained on the multiclass dataset for evaluating the model performance and how well performs on the multiclass malicious activity. Khan et al. 2022 [11] propose stack ensemble ANN to detect network intrusion. The dataset named NF-UQ-NIDS was used in the experiment. The dataset contains the 11 types of malicious intrusion. After an experiment, the model performance was up to 98% accuracy performance. The model accuracy needs to be improved for best classification and to determine the unknown intrusion type.

Ahmad et al. 2023 [6] propose an inception V3 model for classifying malicious activity by using machine learning techniques and other transfer learning methods. The BIG dataset challenge across nine malicious families was used in their experiment. After the experiment proposed model inception v3 gives 99.6% accuracy. Jamal et al. 2022 [12] propose an artificial neural network model for classifying malicious attacks. For the experiment, the IoT-based network dataset was used. The dataset contains the eight malicious classes. After the experiment, their proposed model gives 97.08% accuracy. The single dataset used in their experiment the model needs to be trained on different multiclass datasets to evaluate the model performance in different aspects. Cao et al. 2022 [13] presented a CNN-GRU model for network intrusion detection. Three types of datasets were used in their experiment. Their model gives 99.69% performance in three multiclass datasets. The model training takes a lot of time and does not show time performance by the model. Different parameters need to be changed to get the model more efficient performance. Balyan et al. 2022 [14] improve RF model using EGA-PSO. The NSL-KDD dataset was used in the experiment. The proposed HNIDS gives 98.7% accuracy performance. The dataset contains five classes. The model needs to be trained in a high number of classes for multiclass performance by the model. Time performance by model is also required to determine the model efficiency.

Malgwi et al. 2022 [15] presented an ANN model for detecting network-based intrusion. The CICIDS 2017 dataset used in the experiment contains two number of classes. The model needs to be trained in the multiclass nature of intrusions. Their model gives 99.9% accuracy in two classes. Time performance of the model and comparison of the model with different also needs. Talukdar et al. 2024 [16] presented a network intrusion detection ML model using different techniques which are stacking and oversampling for big and unbalanced nature of datasets. After their experiment with their proposed method, their model achieved 99.9% accuracy performance in the CICIDS 2018 dataset. The model performance is excellent in the ML model but this experiment needs to be conducted through the deep learning models to compare the performance in terms of time and efficiency between deep and ML models. Altunay et al. 2021 [17] presented CNN for detect the network intrusion. The CSE-IDS 2018 dataset used in

experiment. The dataset samples passes through SMOTE. Their approach gives 98.7% performance in five malicious class of intrusion. The number of classes and further additional datasets required to be evaluated by this approach to determine the performance in all aspects. The time performance by the model also needs to be calculated for classification.

## 3. METHODOLOGY

This part contains the methodology part of the proposed model. The model combines the two strong deep learning models including the artificial neural network and convolutional neural network. The methodology is designed for work with multiclass classification. The model combines the characteristics of both models to perform best classification.

### *3.1 Proposed Architecture*

```
# Let X is Data
# Let Y be Intrusion Labels
# Perform Label Encoder and Categorical Operation in the Y
labels = Label_Encoder(Y)
Ye = Categorical(labels)
# Perform Scaling on X
Scaled=Min_Max_Scaler(X)
# Splitting The Data, and Labels
X_train, X_test, Y_train, Y_test=Splitting(Scaled, Ye, split_ratio=0.3)
# Initialize the proposed model
model = Sequential([
   Conv1D(50, 3, activation='relu', input_shape=(68, 1)),
   MaxPooling1D(2),
   Conv1D(50, 3, activation='relu'),
   MaxPooling1D(2),
   Flatten(),
   Dense(80, activation='relu'),
   Dropout(0.5),
   Dense(20, activation='relu'),
   Dropout(0.5),
   Dense(10, activation='SoftMax'),
])
# Compile the propose model
model.compile(optimizer=’rmsprop’, loss=’categorical_crossentropy’ metrics=’accuracy’)
# Train the Model
model. fit(X_train, Y_train, epochs=500, validation_split=0.1, batch_size=3000)
```

In the above architecture, there are first one-dimensional convolutional layers with 50 filters and size 3 the activation function of ReLU, and the input shape (68,1) for one-dimensional data in the convolution layer. The second layer of the Max Pool performs max pool operation in the data as for one dimensional its function to overcome the number of dimensions with a size of 2. The flattened layers come which perform operations as they take data from 2D and convert it into 1D-type data. The dense layer fully connected layers with different numbers of neurons contain 80, 20 having activation function relu. The dropout 0.5 is used in the model to reduce the overfitting in the model. The last one SoftMax performs multiclass classification according to multiclass datasets with the number of classes they associate. The model compile process takes the optimizer as RmsProp, loss function as the categorical cross-entropy for multiclass, and metrics accuracy finally the model is trained with epochs 500, and a validation split of 0.1.

### *3.2 Proposed ANN-CNN Hybrid Model*

The proposed ANN-CNN hybrid model is illustrated in Figure 1, mentioning layers and their shapes in the architecture. It contains three dense layers two dropout layers, two conv1d layers, two max pool and one flatten.

Model: "sequential"

| Layer (type) | Output Shape | Param # |
|---|---|---|
| conv1d (Conv1D) | (None, 66, 50) | 200 |
| max_pooling1d (MaxPooling1D) | (None, 33, 50) | 0 |
| conv1d_1 (Conv1D) | (None, 31, 50) | 7,550 |
| max_pooling1d_1 (MaxPooling1D) | (None, 15, 50) | 0 |
| flatten (Flatten) | (None, 750) | 0 |
| dense (Dense) | (None, 80) | 60,080 |
| dropout (Dropout) | (None, 80) | 0 |
| dense_1 (Dense) | (None, 60) | 4,860 |
| dropout_1 (Dropout) | (None, 60) | 0 |
| dense_2 (Dense) | (None, 10) | 610 |

Total params: 73,300 (286.33 KB)
Trainable params: 73,300 (286.33 KB)
Non-trainable params: 0 (0.00 B)

**Figure 1.** Proposed Hybrid ANN-CNN model

## 4. EXPERIMENT

The experiment from the proposed model with multiclass is taken in Core i7, 7th Generation, Intel Graphics card, and 8 GB of RAM system. The experiment from the proposed model is applied to three multiclass datasets as discussed below the experiment. The multiclass datasets are collected from the different malware dataset sources. The three datasets include the Microsoft Malware Dataset [18], WSN-Dataset [19], and the virus digit malware dataset [20].

**Table 1.** Proposed Model Performance and Comparison of different methods on WSN-Dataset

| Architecture | Evaluation-Score | Precisions-Score | Recalls-Score | F1-Score |
|---|---|---|---|---|
| ANN-CNN | 0.996% | 0.99% | 0.99% | 0.99% |
| LSTM | 0.986% | 0.981% | 0.982% | 0.981% |
| GRU | 0.987% | 0.985% | 0.981% | 0.982% |
| RNN | 0.986% | 0.985% | 0.986% | 0.98% |
| MLP | 0.982% | 0.981% | 0.980% | 0.981% |

Table 1 contains an evaluation-value, precisions-value, recalls-value, and f1-values of the presented architecture ANN-CNN classifier in the multiclass WSN dataset. It presents the comparison of proposed approaches with different methods performance.

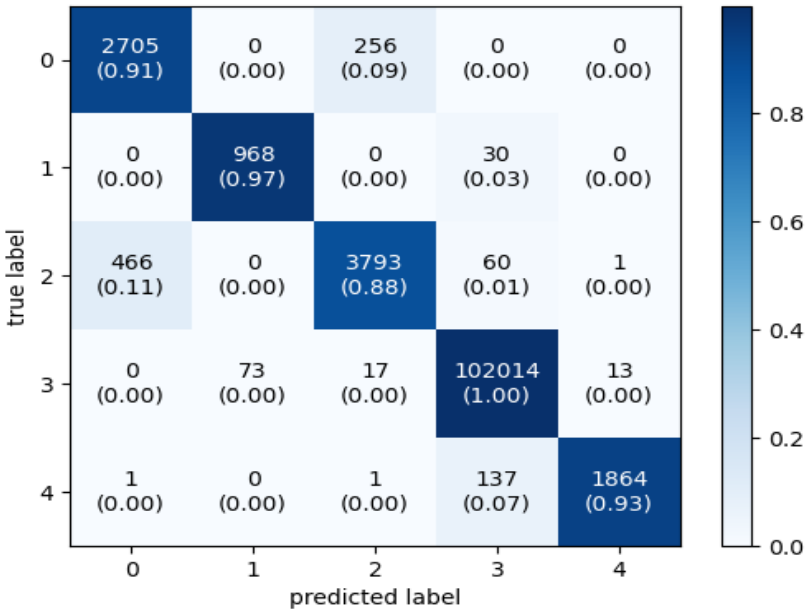


**Figure 2.** Confusion matrix on 5 classes from the proposed model performance on WSN-Dataset

Figure 2 shows per class predicted by the proposed approach. It contains five number of class prediction by the hybrid model.

**Table 2.** Propose Model Performance and Comparison of different methods on Microsoft Malware Dataset

| Architecture | Evaluation-Score | Precisions-Score | Recalls-Score | F1-Scores |
|---|---|---|---|---|
| ANN-CNN | 0.996% | 0.984% | 0.984% | 0.984% |
| LSTM | 0.901% | 0.88% | 0.881% | 0.89% |
| GRU | 0.941% | 0.940% | 0.941% | 0.942% |
| RNN | 0.967% | 0.961% | 0.960% | 0.960% |
| MLP | 0.961% | 0.962% | 0.961% | 0.961% |

Table 2 contains the evaluation-score, precisions, recalls, and f1-scores of the proposed model ANN-CNN classifier in the Microsoft Malware multiclass Dataset. It presents the comparison of proposed approaches with different methods performance.

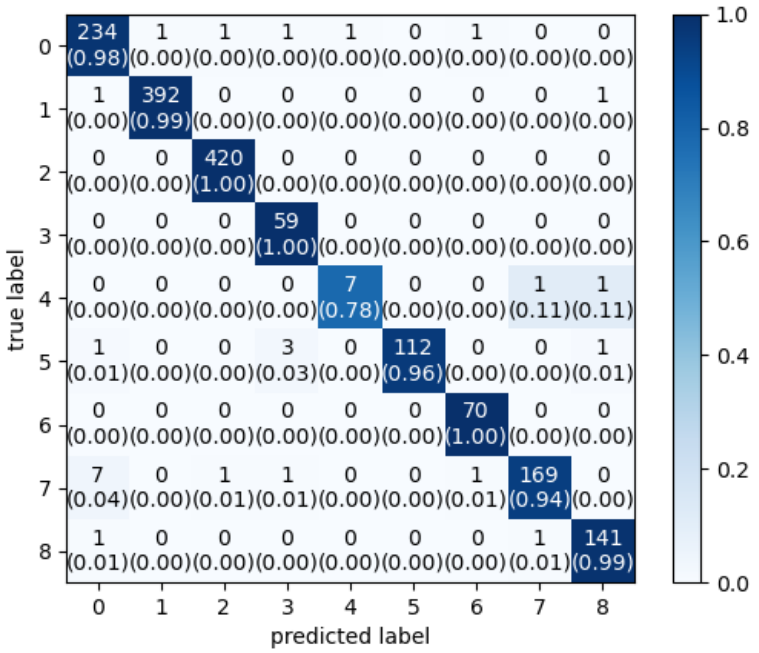


**Figure 3.** Confusion matrix on 9 classes from the proposed model performance on the Microsoft Malware Dataset

Figure 3 shows per class predicted by the proposed approach. It contains nine number of class prediction by the hybrid model.

**Table 3.** Propose Model Performance and Comparison of different methods on Virus Digit Malware Dataset

| Architecture | Evaluation-Score | Precisions-Score | Recalls-Score | F1-Score |
|---|---|---|---|---|
| ANN-CNN | 0.981% | 0.904% | 0.914% | 0.914% |
| LSTM | 0.87% | 0.86% | 0.85% | 0.88% |
| GRU | 0.821% | 0.801% | 0.801% | 0.801% |
| RNN | 0.80% | 0.79% | 0.771% | 0.772% |
| MLP | 0.78% | 0.76% | 0.75% | 0.761% |

Table 3 contains the evaluation-score, precisions-score, recalls-score, and f1-score of the proposed model ANN-CNN classifier in the virus malware multiclass dataset. It presents the comparison of proposed approaches with different methods performance.

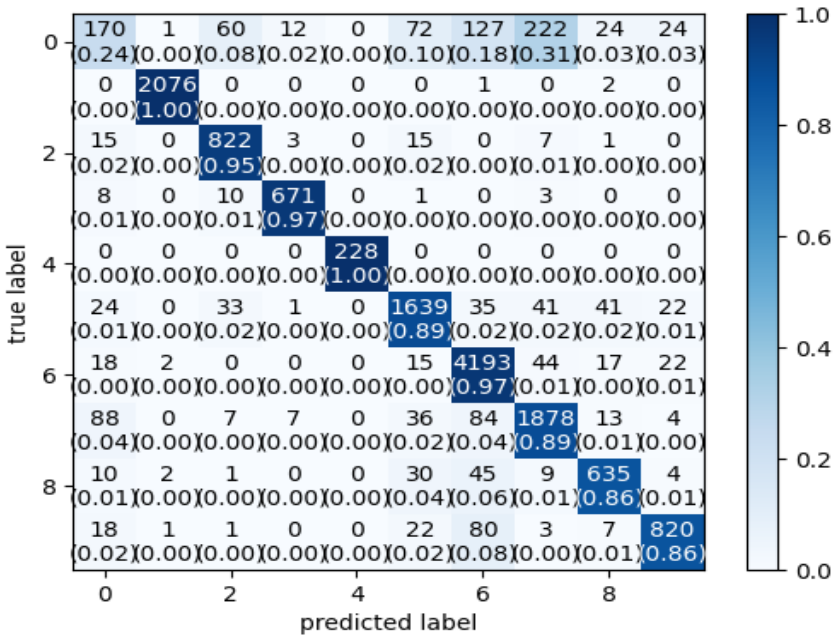


**Figure 4.** Confusion matrix on 10 classes from the proposed model performance on the Virus Digit Malware Dataset

Figure 4 shows per class predicted by the proposed approach. It contains ten number of class prediction by the hybrid model.

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| 1 | 0.97 | 0.96 | 0.96 | 238 |
| 2 | 0.99 | 0.99 | 0.99 | 354 |
| 3 | 1.00 | 0.99 | 1.00 | 437 |
| 4 | 0.98 | 0.99 | 0.98 | 95 |
| 5 | 1.00 | 0.75 | 0.86 | 4 |
| 6 | 0.96 | 1.00 | 0.98 | 103 |
| 7 | 0.95 | 1.00 | 0.97 | 70 |
| 8 | 0.98 | 0.96 | 0.97 | 179 |
| 9 | 0.99 | 0.98 | 0.99 | 150 |
| accuracy | | | 0.98 | 1630 |
| macro avg | 0.98 | 0.96 | 0.97 | 1630 |
| weighted avg | 0.98 | 0.98 | 0.98 | 1630 |

**Figure 5.** Classification report on 10 classes from the Hybrid ANN-CNN model performance on the Microsoft Malware Dataset

Figure 5 presents the classification report of each class with different metrics. It contains the number of classes. It presents the weighted-score and outcome-score in it.

## 5. DISCUSSION

The conducted experiment proposed a model ANN-CNN classifier on three multiclass datasets that performs excellent classification with accuracy. The proposed model performs 99.6% on two datasets which are multiclass and 98% which are also multiclass the confusion matrix shows how the proposed model performs best classification on predicting the class of intrusion. The precision, recall, and f1 score from the proposed model on the multiclass dataset ensure the model excellence in the multiclass approach. To prevent overfitting and reduce the model complexity the model layers specific neurons and dropout values used. The experiment from the proposed model is better than the existing literature in recent years for multiclass classification. The comparison of the proposed model with the LSTM, GRU, RNN, and MLP models shows that ANN-CNN classification is efficient for the multiclass approach. With suitable selection of neuron filters and layers in a hybrid model reduces the computation of the model and time also increases the performance efficiency. The dropout value of 0.5 is also used to prevent the overfitting problem.

## 6. CONCLUSION

The ANN-CNN classifier performs excellently in multiclass datasets. The model is designed by combining both artificial neural networks and convolutional neural networks after the proposed model the model is highly tuned and trained to take the best model performance in a multiclass approach. In the three multiclass datasets used in the experiment which are in multiclass the ANN-CNN classifier performs 99.6% on two datasets and 98% on one dataset which predicts the intrusion type accurately. This hybrid model takes 0.75 s time to perform classification.

## 7. FUTURE

The model needs to be implemented on the image datasets to determine the intrusion. Highly GPU training for the best and fastest prediction by the ANN-CNN classifier on the multiclass images dataset. The Ant colony optimization and particle swarm optimization techniques were applied in the proposed ANN-CNN model to improve the model performance in classification.

## REFERENCES

[1] Geeks intursion, “Intrusion,” 2024, [Online]. Available: https://www.geeksforgeeks.org/intrusion-detection-system-ids/

[2] M. Gopinath and S. C. Sethuraman, “A comprehensive survey on deep learning based malware detection techniques,” *Comput. Sci. Rev.*, vol. 47, p. 100529, 2023, doi: 10.1016/j.cosrev.2022.100529.

[3] S. S. Lad and A. C. Adamuthe, “Malware classification with improved convolutional neural network model,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 12, no. 6, pp. 30–43, 2020, doi: 10.5815/ijcnis.2020.06.03.

[4] Y. Wu, D. Wei, and J. Feng, “Network attacks detection methods based on deep learning techniques: A survey,” *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8872923.

[5] A. Bensaoud, N. Abudawaood, and J. Kalita, “Classifying Malware Images with Convolutional Neural Network Models,” 2020, doi: 10.6633/IJNS.202011_22(6).17.

[6] M. Ahmed, N. Afreen, M. Ahmed, M. Sameer, and J. Ahamed, “An inception V3 approach for malware classification using machine learning and transfer learning,” *Int. J. Intell. Networks*, vol. 4, no. September 2022, pp. 11–18, 2023, doi: 10.1016/j.ijin.2022.11.005.

[7] C. Joshi, R. Kumar, and V. Bharti, “A Fuzzy Logic based feature engineering approach for Botnet detection using ANN,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2021, doi: 10.1016/j.jksuci.2021.06.018.

[8] K. Gupta, N. Jiwani, M. H. U. Sharif, R. Datta, and N. Afreen, “A Neural Network Approach For Malware Classification,” *3rd IEEE 2022 Int. Conf. Comput. Commun. Intell. Syst. ICCCIS 2022*, pp. 681–684, 2022, doi: 10.1109/ICCCIS56430.2022.10037653.

[9] E. Venkata Pawan Kalyan, A. Purushottam Adarsh, S. Sai Likith Reddy, and P. Renjith, “Detection Of Malware Using CNN,” *2022 2nd Int. Conf. Comput. Sci. Eng. Appl. ICCSEA 2022*, 2022, doi: 10.1109/ICCSEA54677.2022.9936225.

[10] M. S. Akhtar and T. Feng, “Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time,” *Symmetry (Basel).*, vol. 14, no. 11, 2022, doi: 10.3390/sym14112308.

[11] S. Ann, “Network Intrusion Detection Using Stack-Ensemble ANN,” pp. 1104–1109, 2022.

[12] A. Jamal, M. Faisal Hayat, and M. Nasir, “Malware Detection and Classification in IoT Network using ANN,” *Mehran Univ. Res. J. Eng. Technol.*, vol. 41, no. 1, pp. 80–91, 2022, doi: 10.22581/muet1982.2201.08.

[13] B. Cao, C. Li, Y. Song, Y. Qin, and C. Chen, “Network Intrusion Detection Model Based on CNN and GRU,” *Appl. Sci.*, vol. 12, no. 9, 2022, doi: 10.3390/app12094184.

[14] A. K. Balyan *et al.*, "A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method," *Sensors*, vol. 22, no. 16, pp. 1–20, 2022, doi: 10.3390/s22165986.
[15] Y. M. Malgwi, I. Goni, and B. M. Ahmad, "Artificial Neural Network Model for Intrusion Detection System," *Mediterr. J. Basic Appl. Sci.*, vol. 06, no. 01, pp. 20–26, 2022, doi: 10.46382/mjbas.2022.6103.
[16] M. A. Talukder *et al.*, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," *J. Big Data*, vol. 11, no. 1, 2024, doi: 10.1186/s40537-024-00886-w.
[17] H. C. ALTUNAY and Z. ALBAYRAK, "Network Intrusion Detection Approach Based on Convolutional Neural Network," *Eur. J. Sci. Technol.*, no. 26, pp. 22–29, 2021, doi: 10.31590/ejosat.954966.
[18] "COW : Malware Classification in an Open World".
[19] "WSN-Dataset", [Online]. Available: https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds/code
[20] D. A. Noever and S. E. M. Noever, "V IRUS -MNIST : A B ENCHMARK M ALWARE D ATASET".