# EID2CNN: ENHANCING INTRUSION DETECTION WITH DEEP CNN EPOCH-WISE TRAINING INSIGHTS

**Dr. Suresh Babu Chandolu 1**
Head of the Department, Department of CSE(AI&ML), Dhanekula Institute of Engineering & Technology, Ganguru-521139, Vijayawada, Andhra Pradesh.
suresh.chandolu@gmail.com

**Dhanvi Gandrothu 2**
B.Tech Student, Department of CSE(AI&ML), Dhanekula Institute of Engineering & Technology, Ganguru-521139, Vijayawada, Andhra Pradesh.
dhanvi.222459@gmail.com

**Venkata Sowjanya Munganda 3**
B.Tech Student, Department of CSE(AI&ML), Dhanekula Institute of Engineering & Technology, Ganguru-521139, Vijayawada, Andhra Pradesh.
mvsowjanya2005@gmail.com

**Chaitanya Yarramsetti 4**
B.Tech Student, Department of CSE(AI&ML), Dhanekula Institute of Engineering & Technology, Ganguru-521139, Vijayawada, Andhra Pradesh.
chaitanyayarramsetti7@gmail.com

**Charan Sai Molabanti 5**
B.Tech Student, Department of CSE(AI&ML), Dhanekula Institute of Engineering & Technology, Ganguru-521139, Vijayawada, Andhra Pradesh.
charansai.molabanti@gmail.com

**Meghana Sri Santhi Pasupuleti 6**
B.Tech Student, Department of CSE(AI&ML), Dhanekula Institute of Engineering & Technology, Ganguru-521139, Vijayawada, Andhra Pradesh.
meghanasanthi13@gmail.com

**Abstract—** Increased internet users have made cyberattacks a massive threat to network security. The conventional methods of intrusion detection are usually incapable of identifying the contemporary undetected attacks. The CNN and multiclass network traffic classification-based intrusion detection system is developed on CICIDS2017 dataset. The dataset is prepared to be fed to CNN using label encoding, MinMax feature scaling as well as format them into 9x9 matrices. The suggested method evaluates learning by analyzing performance at each epoch and optimization of CNN models during training. According to the findings of the experiment, the accuracy of the system is 99.81 percent in identifying various forms of network attacks. The trained model is put to evaluate the invasions using a Flask-based web interface using the network traffic data supplied to the web interface.
**Index Terms—** Convolutional Neural Network, Deep Learning, IDS, CICIDS2017, Network Security, Multiclass Classification.

## I. INTRODUCTION

The computer networks are prone to attacks like denial-of-service attack because of the surging internet service and electronic communication.

malware, intrusion, denial of service and brute force. These attacks may break into personal information, disrupt the work processes and cause significant losses. Signatures are used by traditional intrusion detection systems (IDS) to recognize known attack patterns. However, they are not applicable in the modern world of cybersecurity since they tend to fail in dealing with ambiguous or evolving threats. To facilitate network security, automatic knowledge acquisition of the intricate traffic pattern will be required of smart detection processes.

Deep learning and machine learning may improve intrusion detection using network traffic data, according to recent study and identifying anomalies in the patterns. Different authors have applied deep learning models to recognize network intrusions with a higher degree of reliability and accuracy; these networks are CNNs, LSTMs, and hybrid networks. The concept of data poisoning on CNN-based intrusion detection systems was examined by Reddy et al, in which safe detection is noted to occur after a well trained model [1]. Rakesh et al. researched intrusion detection on machine learning and deep learning ensemble algorithm on the CICIDS2017 data, and demonstrated that the advanced methods of learning can be applied to network security [2]. Nazarri et al. refined CNN-based classification by converting network traffic data into visual representations with the help of IGTD technique [3]. In their study on the subject of CNN-based anomaly detection of network security, Kalra et al. pointed out the capability of deep learning in identifying sophisticated patterns of network attack [4]. DeepNetDetect is a deep learning system, which Cyril developed to identify abnormalities in network traffic at the initial level [5]. The relevance of AI-based models of IDS is growing.

This study classifies multiclass network traffic using the CNN-based Intrusion Detection System, which is based on CICIDS2017. The model is able to obtain spatial correlations between the network features by preprocessing and organizing the data to feed into CNN. Epoch-wise performance analysis is a study of the dependency between the training time and model convergence and the model accuracy. The experimental results reveal that the system has consistent learning characteristics and good performance in the detection of network intrusion since it is applicable to the research proposal.

## II. LITERATURE SURVEY

Ding et al., suggested a combination method that uses Generative Adversarial Networks (GAN) and KNN to manage the unbalanced data in the network intrusion detection. The GAN model generates synthetic data according to the categories of minority attacks to promote classification and detection. This approach enhances intrusion detection in very skewed information of network traffic [6].

In order to classify network traffic data, Zhang et al. developed an intrusion detection system on CNN. Convolutional layers enhance the cyber threat identification of the system and automatically retrieve meaningful characteristics of network data. According to the findings, deep learning networks are capable of improving the detection of network traffic intrusion of uneven distribution [7].

Liu et al. proposed a rapid intrusion detection model, which used LightGBM and Adaptive Synthetic Oversampling (ADASYN). Although Oversampling offers a trade-off between the artificial classes of minorities and the dataset, LightGBM classifier is superior

in regard to speed recognition and accuracy of the classification. This combination enables the intrusion detection systems to be more effective and reliable [8].

Tama and Rhee put the Gradient Boosted Machine (GBM) approach to detecting anomalies to the test. They discovered that ensemble learning minimized false positives and maximized classification accuracy in as far as network intrusion detection was concerned. The research established that the determination of aberrant network activity can be established by enhancing algorithms [9].

To detect network intrusions, Yang and associates created a regularized supervised adversarial variational autoencoder. Deep learning and adversarial learning boost feature representation and detection in the proposed model. The experiments have indicated that the method can be capable of detecting intricate patterns of network traffic infiltration [10].

Tavallaee et al. discovered old patterns of attacks and duplication of KDD Cup 99 which is a widely used dataset. This research paper has shown the need of more current and realistic cybersecurity data set and has discovered that these loopholes can affect the accuracy of the intrusion detection models [11].

Concerning the investigation of botnet in IoT, Bot-IoT offered by Koroniotis et al. gives accurate network traffic information. The data set can be appropriate in the design and testing of the modern IoT intrusion detection systems because it contains both harmful and normal traffic patterns [12].

Divekar et al. benchmarked the dataset of the intrusion detection system based on anomalies. To enhance the operation of the IDS, the paper compares the alternatives to the KDD Cup 99 dataset and suggests the necessity to possess more recent datasets which represent the behavior of network traffic in a better way [13].

IGAN-IDS, an ad hoc intrusion detection system based on generative adversarial networks, was introduced by Huang and Lei. In order to address the problem of unbalanced datasets and improve the classification and detection of intrusion systems, the model uses GAN to create fake examples of assaults [14].

Elghalhoud et al. studied the response of machine learning models to detect IoT intrusions to the data balance and hyperparameters change. They have discovered that fine-tuned model parameters, balanced dataset, improve the effectiveness, and the accuracy of intrusion detection systems [15].

## III. METHODOLOGY

CNN is used by the suggested intrusion detection to classify network data into fewer sorts of attacks. Its successful processing presupposes that CICIDs2017 has to be collected and grouped in a small number of CSV files. Reformulation of the data, classifying data that is categorical with the use of numbers and MinMax scaling feature data to the zero to one range are all forms of data preparation. When 80 percent of the data are processed, this is used to train and the remaining 20 percent is used to test and 10 percent is used to validate the model. In order to represent spatial relationships among features of network concepts, tabular feature vectors are padded and transformed into 9x9 format, one of the assumptions of CNN-based learning. The CNNs use softmax output layer to provide predictions of multiple classes, fully connected layer to classify and a few convolutional layers to extract features. Adam optimizer with a learning rate of 0.0001 is used for model training. Training convergence and model stability are assessed using accuracy, precision, recall, F1-score, and epoch-wise tests.

### A) Proposed System

The suggested system's CNN-based intrusion detection system (IDS) identifies and classifies network threats. To analyze the network traffic information, the system utilizes the CICIDS2017 dataset site that contains a set of malicious and benign traffic that is the result of cyberattacks that took place recently. The label encoding and MinMax feature scaling help to clean, randomize and transform the dataset to enable the models to be learned. To ensure that the model learns the behavior of the traffic and compares the new information, the processed set is divided into training and test sets.

The padded feature vectors are rearranged into a 9x9 format of a matrix to play a role in enhancing stronger CNN learning of tabular network traffic characteristics. This allows the layers of the brain to understand spatial correlations. Fully connected network will be employed in CNN structure to separate network information into types of attacks and multiple convolution layer will be used to extract features. Epoch-wise performance analysis is performed to study the learning behavior and model convergence after the training of a model with Adam optimizer with a 0.0001 learning rate. Lastly, one will be able to generate real-time predictions of intrusion detection with a confidence rating of network traffic traffic using a Flask based web interface and the trained model.

### B) System Architecture

The deep learning intrusion detection system is recommended based on malicious network traffic. To make processing CICIDS2017 easier, it consists of a multitude of CSV files. The dataset is scaled by eliminating redundancies, and the feature scaling is performed to normalize the network traffic features. The phase also ensures that all input features are included in the training and also increases the effectiveness of model learning.

After pre processing, received network traffic characteristics are subjected to a feature reshaping step to deep learning in the shape of a 9x9 matrix. This arrangement enables the CNN to acquire spatial correlations between features in the course of training. After several epochs, CNN model is obtained to identify the benign and malicious patterns of traffic. The performance of the model is evaluated by use of accuracy, precision and recall after training. It is a CNN model with the best architecture combined with a Flask-based web-app allowing the user to upload CSV network traffic data and get live predictions of traffic classes and ratings of confidence.

### C) MODULES

1. Dataset Collection and Integration

This module has rendered the CICIDS2017 data analysis possible. The set originally contained CSV files of multi-day traffic of the network. The files are then combined into a single dataset to make the processing easier with containment of the examples of the benign and malicious traffic to be evaluated and trained.

2. Data Preprocessing

This module improves the dataset quality in advance before the model is trained. It includes the process of encoding category labels into numbers and cleaning the data set assigned to it with a shuffle in order to minimize bias and MinMax scaling feature values. The deep learning model can learn faster with this preprocessing.

3. Feature Reshaping for CNN

The tabular network traffic statistics are presented as 9x9 matrix because CNN model takes structured input, which in this case is an image. Normalize feature vectors. This modification enables CNN model to learn spatial correlation of features.

4. CNN Model Development and Training

The module is in form of CNN architecture which is utilized in order to categorize network data into different types of attacks. The model involves fully connected layers in the classification and convolution layer in the extraction of features. The model is trained using benign and malevolent network traffic patterns using the processed dataset and the number of epochs.

5. Model Evaluation and Performance Analysis

Data is utilized to assess the CNN model following training. Accuracy, precision, recall, and F1-score are used to assess intrusion detection systems. We also verify the model improvement with the help of epoch-wise performance analysis to see the extent to which the model has been improved throughout the training.

6. Flask Web Application Deployment

Finally, Flask and the learnt CNN model are used in the final module deployments. CSV network traffic is transmitted over this interface. In order to ensure that intrusions are detected as quickly as possible, the system analyzes provided data to estimate networking traffic type and present a score of confidence.

## D) ALGORITHMS

### a) Convolutional Neural Network (CNN)

The primary deep learning model used by the suggested system to recognize and classify network intrusions is CNN. In order to distinguish between harmful and legitimate information, convolutional layers automatically find important patterns in altered network traffic data and create spatial correlations between features. The gathered attributes are then fed through by fully connected layers and a softmax classifier.

## IV. EXPERIMENTAL RESULTS

After preprocessing and training, a CNN-based intrusion detection system was assessed using 2017 CICIDS data. Ten percent of the dataset was used for validation, twenty percent for testing, and eighty percent for training. The CNN model was trained using 150 epochs and 1024 batches by the Adam optimizer. Deep learning can track more complex network traffic pattern that is shown with 0.0081 loss value and test accuracy of 99.81. The model can distinguish between network traffic and cyberattacks using the model's superior F1-score, recall, and accuracy.

The CNN models were evaluated epoch-wisely so that the learning during the training process could be researched. The findings show that values of the loss decreased with the increase of the epochs yet training accuracy and validation accuracy increased. After 150 epochs, the model achieved accuracy of 99.81 and this indicates that there was good convergence and learning. There is no overfitting of this model because there is almost no difference between the accuracy of training and validation. These findings indicate the appropriateness and accuracy of CNN-based multiclass network intrusion detection algorithm.

Accuracy: Compare positive and negative results and decide on test dependability. An explanation based on math:

Precision: Precision is a positive measure of instances. Application of these results in the determination of accuracy:

Recall: If a model's predicted positives are accurate in relation to the total positives, it can identify every instance of a machine learning label.

F1-Score: Correct machine learning models are indicated by high F1 scores. Accuracy and memory enhance model correctness. Accuracy gauges how well a model dataset predicts frequency.

The accuracy of CNN model training and validation by epoch is displayed below. Accuracy increases considerably during the initial epochs and stabilizes at 99.8 with high model generalization and learning.

This plot presents model training and validation loss. The loss decreases considerably as the epochs increase, which means that there is persistent convergence and enhanced model performance.

This figure illustrates the Flask based web interface of the System for detecting intrusions. The interface examines the CSV files of network traffic uploaded by users with the help of the trained CNN model.

In this picture, the intrusion detection system returns the prediction output, uploaded network traffic data is categorized as being DDoS, PortScan, Web Attack, DoS GoldenEye, and Benign with confidences rates.

This table displays CNN model training, validation, loss, and test accuracy at different epochs. Model performance is gradually improved throughout epochs. The model's training accuracy was 91.79 at epoch 1, while its test accuracy was 97.13 with higher loss. Losses decrease as training and validation accuracy quickly increase. With 150 epochs, 99.83 training accuracy, 99.86 validation accuracy, and 99.81 test accuracy with the lowest training and validation loss, the model works optimally. These results demonstrate that the CNN model is a good learner of network traffic patterns that does not overfit.

Table 1. Epoch-wise Performance of CNN Model

| Epochs | Train Acc | Val Acc | Train Loss | Val Loss | Test acc |
|---|---|---|---|---|---|
| 1 | 0.9179 | 0.9734 | 0.286 | 0.0694 | 0.9713 |
| 15 | 0.996 | 0.9968 | 0.0135 | 0.0112 | 0.9849 |
| 25 | 0.997 | 0.9972 | 0.0104 | 0.0103 | 0.9965 |
| 50 | 0.9977 | 0.9977 | 0.0078 | 0.01 | 0.9966 |
| 75 | 0.9981 | 0.9981 | 0.0071 | 0.0071 | 0.9975 |
| 100 | 0.9982 | 0.9983 | 0.0056 | 0.0068 | 0.9976 |
| 150 | 0.9983 | 0.9986 | 0.0053 | 0.0058 | 0.9981 |

This chart compares training, validation, and test accuracy with various epochs. The level of test accuracy also increased to a steady value of 99.81 at 150 epochs.

The training and validation loss changes at different epochs. The CNN model has the ability to minimize loss after discovering the network traffic patterns.

Epoch-wise analysis: The model achieved 91.79 percent training accuracy and 97.13 percent test accuracy at epoch 1 with larger values of loss and limited classes in the minority doing poorly as there were not well represented in the data. The model had learned and worked better after 150 epochs of the training and in all classes such as minority attack categories.

## V. CONCLUSION

The article described an CNN-based IDS as it was needed to classify network traffic into multiclass using the CICIDS2017 dataset. It was possible to perform the CNN input, feature extraction, and network attack classification because the data was processed and organized. Experimental results indicated that the proposed model had reduced training loss and validation loss, 99.81% test accuracy and good detection performance. The epoch analysis depicts the steady learning and convergence of a model without overfitting. With the trained model and the web application, which is founded on Flask, to spot intrusions, traffic may be monitored. Technology has been superb and efficient and complementing the network security and detection of cyber threats.

## REFERENCES

[1] S. M. Reddy, S. P. S. V. Adithya, B. S. Reddy and S. Rajula, "Quantifying the Impact of Data Poisoning: A Case Study on CNN-based Intrusion Detection Systems," 2025 10th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2025, pp. 1053-1057, https://doi: 10.1109/ICCES67310.2025.11337104.

[2] L. Rakesh, L. Upadhyay and P. M. Reddy, "Evaluation of Network Intrusion Detection with Machine Learning and Deep Learning Using Ensemble Methods on CICIDS-2017 Dataset," 2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2023, pp. 1429-1433, https://doi: 10.1109/ICAC3N60023.2023.10541488.

[3] M. N. A. A. Nazarri, M. H. M. Yusof and A. A. Almohammedi, "Generating Network Intrusion Image through IGTD Algorithm for CNN Classification," 2023 3rd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 2023, pp. 172-177, https://doi: 10.1109/ICCIT58132.2023.10273902.

[4] A. Kalra, K. S. Gill, M. Kumar and R. Rawat, "CNN-Enhanced Network Security: A Sustainable Approach to Anomaly Detection," 2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), Faridabad, India, 2024, pp. 828-831, https://doi: 10.1109/ICAICCIT64383.2024.10912303.

[5] H. P. Cyril, "DeepNetDetect: A Deep Learning-Based Approach for Early Anomaly Detection in Network Traffic," 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA, 2026, pp. 1-6, doi: 10.1109/ICAIC67076.2026.11395734.

[6] H. Ding et al., “Imbalanced data classification: A knn and generative adversarial networks-based hybrid approach for intrusion detection,” Future Generation Computer Systems, vol. 131, pp. 240–254, 2022.

[7] X. Zhang, J. Ran, and J. Mi, “An intrusion detection system based on convolutional neural network for imbalanced network traffic,” in IEEE 7th International Conference on Computer Science and Network Tech. (ICCSNT), pp. 456–460, 2019.

[8] J. Liu, Y. Gao, and F. Hu, “A fast network intrusion detection system using adaptive synthetic oversampling and lightgbm,” Computers & Security, vol. 106, p. 102289, 2021.

[9] B. A. Tama and K. H. Rhee, “An in-depth experimental study of anomaly detection using gradient boosted machine,” Neural Computing and Applications, vol. 31, pp. 955–965, 2017.

[10] Y. Yang, K. Zheng, B. Wu, Y. Yang, and X. Wang, “Network intrusion detection based on supervised adversarial variational auto-encoder with regularization,” IEEE Access, vol. 8, pp. 42169–42184, 2020.

[11] M. Tavallaee et al., “A detailed analysis of the kdd cup 99 data set,” in 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1–6, 2009.

[12] N. Koroniotis, N. Moustafa, et al., “Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset,” CoRR, vol. abs/1811.00701, 2018.

[13] A. Divekar et al., “Benchmarking datasets for anomaly-based network intrusion detection: Kdd cup 99 alternatives,” in IEEE 3rd Int. Conf. on Computing, Communication and Security (ICCCS), pp. 1–8, 2018.

[14] S. Huang and K. Lei, “Igan-ids: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks,” Ad Hoc Networks, vol. 105, p. 102177, 2020.

[15] O. Elghalhoud, K. Naik, et al., “Data balancing and hyper-parameter optimization for machine learning algorithms for secure iot networks,” In Proceedings of the 18th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet ’22), 2022.

.