A Proposed Ensemble Model of Network Intrusion Detection System for binary and Multiclassification

Amrita Bhatnagar[1], Arun Giri[1], Aditi Sharma[2,*]

[1]Shobhit Institute of Eng. & technology, Meerut, India

[2]Department of Computer Science and Engineering, Symbiosis Institute of Technology, Symbiosis International University, Pune, India

Emails: amritapsaxena@gmail.com; arungiri@shobhitunivesity.ac.in; aditi.sharma@ieee.org

Abstract

A network Intrusion detection system is a system that can find out different types of attacks. ANIDS is used to find out the noble type of attack by using machine learning and deep learning techniques. These techniques are very useful to find out those attacks whose patterns are not stored in the database. Therefore, these types of systems need more research to improve their accuracy and reduce the false alarm rate. In this paper, we are going to propose an ensemble framework for NIDS using different ML and DL techniques. In this paper, we have used the XGBOOST algorithm for feature extraction and for classification, CNN and RNN deep learning techniques are used. This ensemble model is used for the binary and multiclassification of attacks. Our model was checked on the dataset CICIDS-2018 which gives a better accuracy and low false alarm rate.

Keywords: Network Intrusion detection system; Denial of service attack; CNN; RNN; XGOBoost

1. Introduction

An intrusion detection system, often known as a NIDS, is a cybersecurity technology used to identify unwanted access or unusual activities on a network. IDS can be classified in two categories Host based IDS and network-based IDS. In the Host based IDS, IDS is installed on the individual host. It can check all the activities of host if there is any malicious activity is captured then it will generate an alarm. However, it cannot check the activities of network. Monitoring network traffic for unusual behavior and notifying network managers of any possible security breaches are the primary objectives of a network intrusion detection system (NIDS). A Network Intrusion Detection System (NIDS) is made to find anomalous behavior or unwanted access on a network. A NIDS's primary objective is to keep an eye on network traffic for unusual behavior and notify network managers of any possible security breaches [1]. Intrusion Detection Systems (IDS) employ various detection techniques to identify malicious activities and unauthorized access. These are a few methods that IDS uses to find intrusions. These methods may be divided roughly into two primary categories: Anomaly-Based and Signature-Based Detection [2]. Using a signature-based strategy, intrusions are found by searching for patterns or indicators of recognized risks. Every signature is a pattern that links to a known harmful action or attack. Using anomaly-based detection, one may create a baseline of typical network activity and track any changes from it. Hybrid approaches combine multiple detection techniques to leverage the strengths of each. By the help, this approach decreases false positives and increases accuracy by combining many machine-learning methods. In this paper, we are going to use CNN and RNN neural networks for classification and for feature extraction XGBOOST machine learning technique. Deep learning techniques are very useful techniques to detecting cyberattacks. We have used a dataset CICIDS-2018 dataset, developed by the Canadian Institute for Cybersecurity. Our proposed model is worked for binary as well as multiclass classification

DOI: https://doi.org/10.54216/FPA.170105
Received: June 19, 2024 Revised: September 20, 2024 Accepted: October 30, 2024

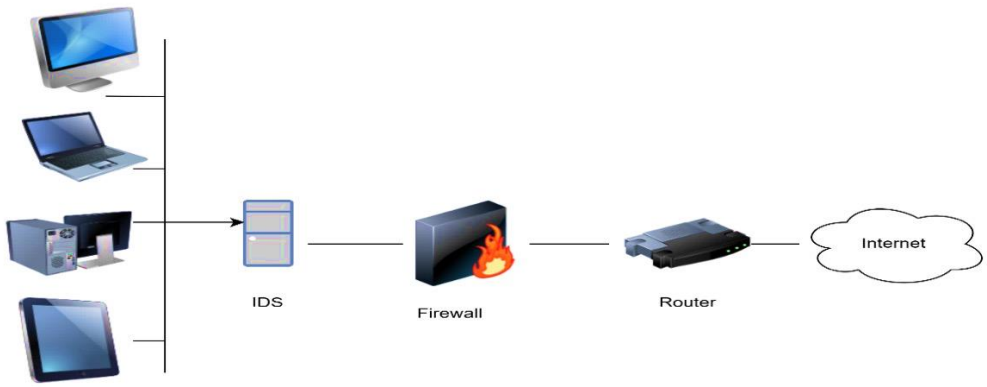

Figure1. Intrusion Detection System

2. Types of attacks

A. Denial of Service (Dos) attack

A Denial of Service (DoS) attack attempts to permanently or temporarily interfere with the operations of a host that is connected to the internet in order to render a computer or network resource inaccessible to its intended users. Usually, this kind of attack consists of flooding the target system with too much traffic or taking use of security holes to bring about a system breakdown. The details of denial-of-service (DoS) attacks, such as their mechanisms, effects, and countermeasures, are provided here.

B. Distributed Denial of attack (DDOS)

A DDoS assault uses several hacked systems to overwhelm the target, hence amplifying the effect of a DoS attack. Oftentimes, an attacker's network of infected devices, or botnet, includes these compromised computers.

C. BOTNET Attack

An assault using a botnet entails a network of hacked computers, also called "bots" or "zombies," that are under the direction of an attacker, sometimes known as a "botmaster." These bots may be used to send spam emails, execute distributed denial-of-service (DDoS) assaults, steal confidential data, and carry out other malevolent tasks. This is a thorough examination of botnet assaults, including their elements, modes of operation, effects, and countermeasures.

D. Brute Force attack

A brute force attack is a method used to gain unauthorized access to systems, networks, or accounts by systematically trying all possible combinations of passwords, encryption keys, or other credentials until the correct one is found. This type of attack relies on the computational power to exhaustively search through the possibilities and is often automated using software tools.

3. Convolution Neural Network

A subclass of deep neural networks called convolutional neural networks, or CNNs, are frequently employed to analyse visual input [3]. For tasks like object identification, categorization, and picture recognition, they work very well. A typical CNN design is made up of several layers, each of which has a distinct function in the processing pipeline. A typical CNN architecture is provided below:

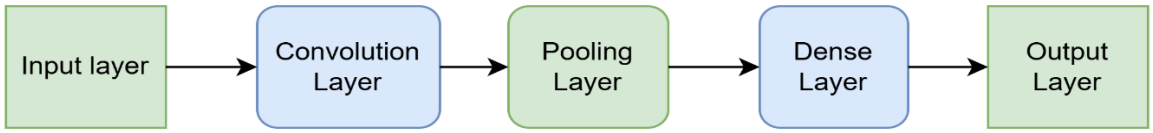

Figure 2. Convolution Neural Network Architecture

DOI: https://doi.org/10.54216/FPA.170105
Received: June 19, 2024 Revised: September 20, 2024 Accepted: October 30, 2024

4. Recurrent Neural Network

A kind of neural networks called recurrent neural networks (RNNs) is made to identify patterns in data sequences like time series, text, or audio. RNNs, in contrast to feedforward neural networks, feature connections that create directed cycles, which enable them to preserve a state and use knowledge from earlier time steps to affect the state and output at that point. Because of this, RNNs work especially well for jobs requiring sequential or context information.

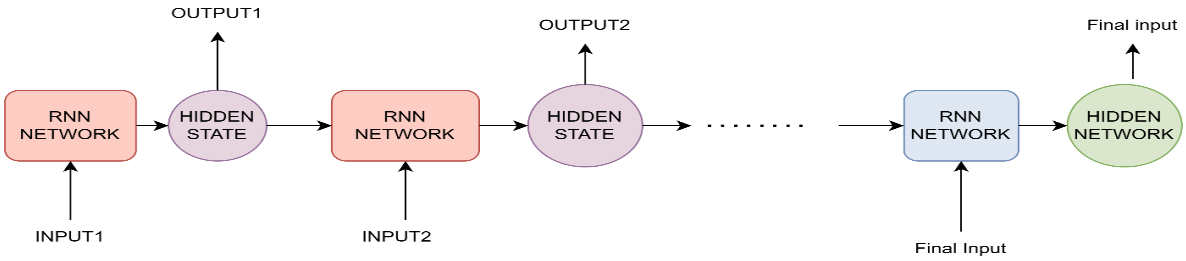

Figure 3. RNN Architecture

5. Dataset

The CICIDS-2018 dataset, developed by the Canadian Institute for Cybersecurity, is a comprehensive dataset for evaluating intrusion detection systems. It addresses various limitations found in previous datasets and provides a detailed representation of modern network traffic and diverse attack scenarios. The dataset includes a wide range of attack types, reflecting real-world cybersecurity threats, making it a valuable resource for research and development in the field of cybersecurity. It captures normal and malicious traffic in a simulated network environment that includes different subnets and devices. It covers a wide range of attack scenarios, including DoS (Denial of Service), DDoS (Distributed Denial of Service), Brute Force, Botnet, Web Attacks, Infiltration, Heartbleed, and more. It has 80 features It provides extensive features extracted from network flows, including packet-level and flow-level data. It includes detailed labels indicating the type of attack or normal traffic, which is crucial for training supervised machine learning models. A wealth of information gleaned from network traffic are included in the CICIDS-2018 dataset to help with the recognition and categorization of different kinds of assaults. For every network flow, the dataset offers 80 features in particular.

Table 1: CICIDS-2018 Dataset

1.Flow Identification Features:
Source IP
Source Port
Destination IP
Destination Port
Protocol
2.Basic Features:
low Duration
Total Fwd Packets
Total Backward Packets
Total Length of Fwd Packets
Total Length of Bwd Packets
Fwd Packet Length Max
Fwd Packet Length Min
Fwd Packet Length Mean
Fwd Packet Length Std
Bwd Packet Length Max
Bwd Packet Length Min
Bwd Packet Length Mean
Bwd Packet Length Std

DOI: https://doi.org/10.54216/FPA.170105
Received: June 19, 2024 Revised: September 20, 2024 Accepted: October 30, 2024

3.Time-based Features:
Flow Bytes/s
Flow Packets/s
Flow IAT Mean
Flow IAT Std
Flow IAT Max
Flow IAT Min
Fwd IAT Total
Fwd IAT Mean
Fwd IAT Std
Fwd IAT Max
Fwd IAT Min
Bwd IAT Total
Bwd IAT Mean
Bwd IAT Std
Bwd IAT Max
Bwd IAT Min
4.Packet-based Features:
Fwd PSH Flag
Bwd PSH Flags
Fwd URG Flags
Bwd URG Flags
Fwd Header Length
Bwd Header Length
Fwd Packets/s
Bwd Packets/s
Min Packet Length
Max Packet Length
Packet Length Mean
Packet Length Std
Packet Length Variance
5.Header Features:
FIN Flag Count
SYN Flag Count
RST Flag Count
PSH Flag Count
ACK Flag Count
URG Flag Count
CWE Flag Count
ECE Flag Count
Down/Up Ratio
Average Packet Size
Fwd Segment Size Avg
Bwd Segment Size Avg
Fwd Bytes/bulk Avg
Fwd Packets/bulk Avg
Fwd Bulk Rate Avg
Bwd Bytes/bulk Avg
Bwd Packets/bulk Avg
Bwd Bulk Rate Avg
6.Flag Features:
Subflow Fwd Packets
Subflow Fwd Bytes
Subflow Bwd Packets

DOI: https://doi.org/10.54216/FPA.170105
Received: June 19, 2024 Revised: September 20, 2024 Accepted: October 30, 2024

Subflow Bwd Bytes
7.Miscellaneous Features:
Init_Win_bytes_forward
Init_Win_bytes_backward
act_data_pkt_fwd
min_seg_size_forward
Active Mean
Active Std
Active Max
Active Min
Idle Mean
Idle Std
Idle Max
Idle Min

6. Literature Survey

In this paper, Authors proposed (CNN) deep learning method to solving the problem of identifying intrusion in a network. UNSW NB15 public dataset was used to train the CNN algorithm [5]. In this paper, Authors examines NIDS using a Convolutional Neural Network (CNN) and LSTM. Authors used KDD99 dataset to train the proposed model, which shows the increase in performance of intrusion detection system [6]. In this paper, Authors develops the novel hybrid intrusion (attack) detection model using DL techniques, Convolutional neural network (CNN) and Long short-term memory (LSTM) to achieve better attack detection accuracy. The model is examined using two different datasets namely UNSW-NB151 and NSL- BOT [7]. In this paper authors introduces novel deep-learning Techniques. This paper aims to develop a reliable intrusion detection mechanism to help identify different attacks. In this method, Long-Short Term Memory Recurrent Neural Network (LSTM-RNN) with seven optimizer functions such as adamax, SGD, adagrad, adam, RMSprop, nadam and adadelta are used. This proposed model is examined on the NSL-KDD dataset and classified as a multi-attack classification [8]. This paper proposes SPIDER, a network anomaly detection model. Four modernized Recurrent Neural Networks (RNNs)–Bi-LSTM (Bidirectional Long Short Term Memory), LSTM (Long ShortTerm Memory), Bi-GRU (Bidirectional Gated Recurrent Unit), and GRU (Gated Recurrent Unit)–are used to prepare the SPIDER model. Principal Component Analysis (PCA) has been used to decrease the dimensions of the data in order to address the dimensionality issues. The widely recognized NSL-KDD and UNSW-NB15 datasets have been used to examine the performance of the suggested SPIDER model to ensure robustness [9]. In this paper, the LSTM DL method is used for NIDS to get high accuracy and low false positive rates, to improve the performance of IDS. [10]. In this paper proposed IDS model shows best performance, evidenced by its high accuracy, elevated detection rates, and minimal false alarm rates. Principal Component Analysis (PCA) and Mutual Information (MI) methodologies are used for feature selection and dimensionality reduction [11]. In this paper author gives a a solution to enhance detection accuracy in traffic anomaly detection by proposing a DL model named DLNID, which merges an attention mechanism with a bidirectional LSTM (Bi-LSTM) network [12]. With the use of a specialized computing unit, this study shows an improvement in the effectiveness of intrusion detection systems (IDS) for spotting unusual network traffic. Specifically, it creates an IDS that combines an RNN that makes use of gated recurrent units (GRUs) with an improved version of LSTM units, known as Cu-LSTMGRU [13]. The RNN-IDS model exhibits exceptional accuracy and robust intrusion detection capabilities in binary and multiclass categorization tasks. Comparing this model to more traditional classification methods such as J48, naive Bayes, and random forest, it performs better in terms of accuracy and detection rates while maintaining a low number of false positives. This is particularly true for jobs involving multiclass classification utilizing the NSL-KDD dataset. [14] To solve the IDS issues, the authors of this research use a hybrid Convolution Neural Network and Deep Watershed Auto-encoder (CNN-DWA) technique. The KDD CUP 1999 dataset is used to train and assess the proposed network. The advantages of the proposed model are illustrated by contrasting the outcomes of the Convolution Neural Network (CNN) method with the CNN-DWA approach [15]. In this paper, Authors offer a Convolutional Neural Network (CNN) based intrusion detection model. In order to balance network traffic prior to CNN training, the Synthetic Minority Oversampling Technique and the Edited Nearest Neighbors (SMOTE-ENN) method are used. The authors assess the model using the NSL-KDD dataset [16]. More precise and reliable intrusion detection is made possible by the suggested framework, which uses deep learning to automatically extract relevant elements from network traffic data. To effectively distinguish between normal and anomalous activity, a deep convolutional neural network (DCNN) has been trained on extensive datasets that include both malicious and benign network traffic [17]. The authors of this paper outline a method for building an IDS using CNN. The technique is taught using known attack

DOI: https://doi.org/10.54216/FPA.170105
Received: June 19, 2024 Revised: September 20, 2024 Accepted: October 30, 2024

signatures, and network traffic is displayed according to TCP/IP connection properties. Authors assess this method on the publicly accessible NSLKDD dataset. The writers are able to get 98.92% accuracy, 99.82% precision, 92.34% recall, and 96.34% F1-score, in that order [18]. In this study, a machine learning (ML)-based IDS framework is put into practice. This system makes use of three distinct kinds of recurrent neural networks, or RNNs: simple RNN, gated RRU, and long-short-term memory (LSTM). In evaluating the effectiveness of the suggested IDS framework, the NSL-KDD and UNSW-NB15 benchmark datasets are taken into account [19]. In this study, the author developed a hybrid intrusion detection system model by utilizing the spatial feature extraction capabilities of convolutional neural networks and the temporal feature extraction capabilities of long short-term memory networks. To make the model work better, we included dropout layers and batch normalization. Three datasets—CIC-IDS 2017, UNSW-NB15, and WSN-DS—were used to train the model based on binary and multiclass classification. The confusion matrix, which incorporates assessment criteria including accuracy, precision, detection rate, F1-score, and false alarm rate (FAR), establishes the efficacy of the system [20-27].

7. Proposed Methodology

In the proposed methodology, we have used a hybrid method of two deep learning techniques. This method are used to classify different type of attacks or it can be used for binary and multiclassification.

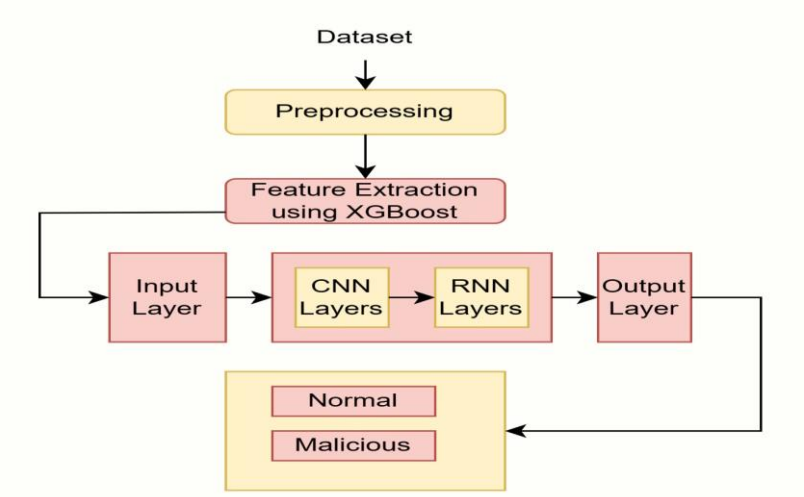

Figure 4. Proposed Methodology for Binary classification

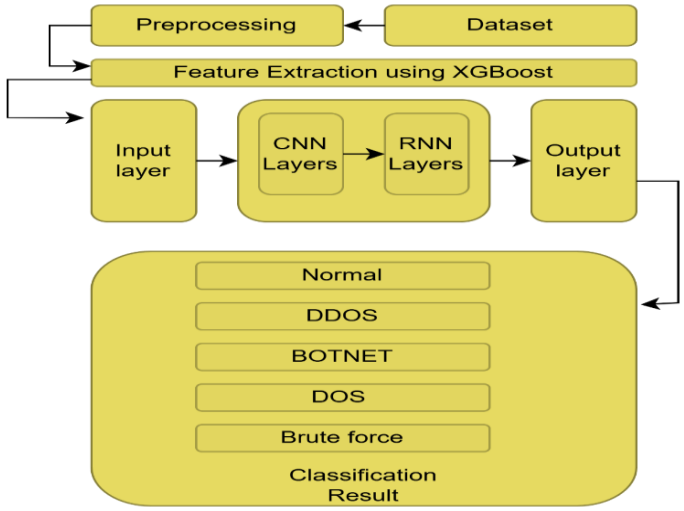

Figure 5. Proposed Methodology for Multiclassification

DOI: https://doi.org/10.54216/FPA.170105
Received: June 19, 2024 Revised: September 20, 2024 Accepted: October 30, 2024

8. Algorithm

These are the steps for the proposed methodology

1. Firstly, collect the dataset CICIDS-2018.
2. Data visualization will be done using graphs, diagrams, PPTs
3. Preprocess the dataset using data cleaning and data normalization techniques.
4. Feature extraction using the XG-Boost technique.
5. Data splitting will be done to divide the training and testing data
6. Apply the dataset to the CNN layer i.e convolution layer and pooling layer
7. Resultant of CNN Layers applied on RNN layers i.e RNN network and hidden layer
8. Output layers give the binary or multiclass classification of attack.

9. Performance Evaluation

A confusion matrix is a tabular representation of the number of accurate and inaccurate guesses (or actual and expected values) that a classifier (or classification model) produces for jobs involving binary classification.

Table 2: Confusion Matrix

	PREDICTED		
TRUE		Positive	Negative
	Positive	True Positive (TP)	False Negative (FN)
	Negative	False Positive (FP)	True Negative

The metrics in Table 1's confusion matrix are used to assess how well IDS is working. TP stands for benign records that have been mistakenly classed as harmful, FP for benign recordings that have been mistakenly classified as malicious, TN for malicious documents that have been mistakenly classified as benign, and FN for malicious records that have been mistakenly classified as benign. We can determine accuracy (ACC), detection rate (DR), precision (Pr), and false alarm rate (FAR) from the confusion matrix indicators. The ratio of accurate record forecasts is referred to as ACC. The capacity to forecast only complete positive records is known as data reliability (DR). FAR is the ratio of typical traffic misclassifications, whereas Pr is the capacity to prevent mislabeling negative data as positive.

ACC = (TP+ TN)/(TP+TN+FP+FN)

Detection Rate (DR) =TP/TP+FN

False Alarm Rate (FAR)= FP/FP+TP

Precision (PR) =TP/TP+FP

F1-Score =TP/[TP+1/2(FP+FN))

Table 3: Experimental Scenario

Dataset	**Classification**			
	Binary		**Multiclassification**	
	No. of Records	**Types of Records**	**No. of Records**	**Types of Records**
CICIDS-2018.	2	Normal & Abnormal	7	Normal Brute force, Botnet, DoS, DDoS,

DOI: https://doi.org/10.54216/FPA.170105
Received: June 19, 2024 Revised: September 20, 2024 Accepted: October 30, 2024

10. Experimental Result & Discussion

We constructed our model on an evaluation platform com rised of an hp with an Intel Core (i7) processor running at 2.80 GHz and 5 GB of RAM. The model for deep learning was implemented using the Pandas, Keras, and Tensorflow libraries .Two techniques of classification have been used to evaluate the models: binary and multiclass. For binary classification, the datasets were split into two classes: normal and assault. We have used five classes for multiclassification Normal DDoS, Botnet, Dos, Brute Force.

A.CNN-RNN based on selected features

Firstly, we have done our experiment with selected features 24, 40,50,60,80. We get the highest accuracy 99.70 with 60 features. We got the highest detection rate 99.64 with 78 features and we found the lowest false alarm 0.11 with 50 features.

Table 4: Feature Selection based on binary CIC-IDS 2018

CIC-IDS2018 Binary classification					
No of Features	ACC	DR	PR	F1-score	FAR
24	97.33	95.85	99.1	95.80	0.84
40	99.42	99.62	99.32	99.63	0.44
50	99.66	99.60	99.56	99.64	**0.11**
60	99.70	99.32	99.00	99.31	0.40
78	99.66	**99.64**	99.55	99.55	0.13

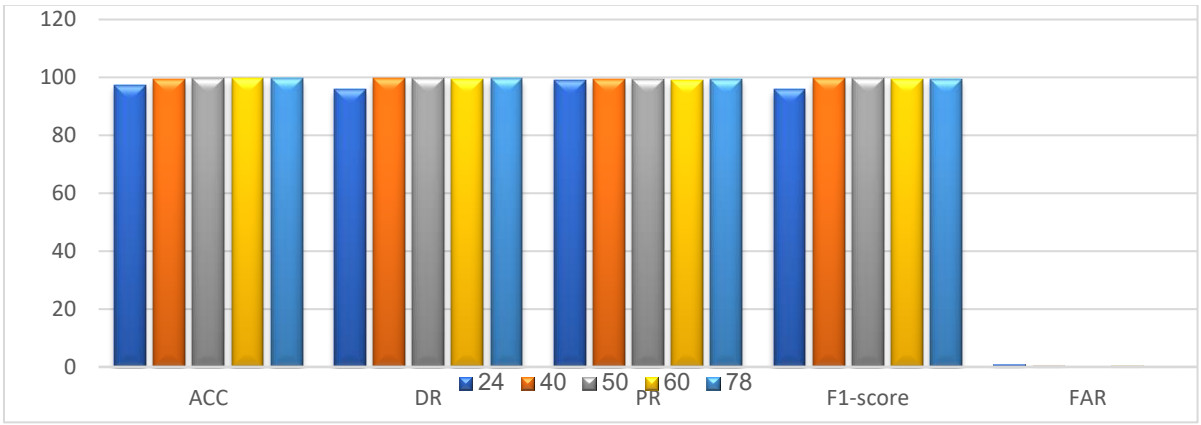

Figure 6. Graphical Representation of Feature Selection based classification

B. CNN-RNN based on stratified K- fold cross

In the next step, we have used K fold cross-validation. One resampling method for assessing a machine-learning model's performance is K-fold cross-validation. First, the dataset is divided into K equal-sized subsets, or "folds." After that, the model is trained and verified K times, with the training set consisting of the remaining K-1 folds and the validation set consisting of a different fold each time. By utilizing each data point for training and validation, this technique guarantees a more reliable assessment of the model's performance.

Because all data points are included for both training and validation, it offers a more precise estimation of model performance. With multiple fold averages, the performance metric's variation is reduced. It can effective use of the whole dataset for validation and training.

Table 5: K Fold Cross For binary classification

CICIDS-2018					
Binary Classification					
K	ACC	DR	PR	F1-Score	FAR
2	99.61	99.67	99.52	99.6	0.11
4	99.65	99.68	99.61	99.5	0.34

DOI: https://doi.org/10.54216/FPA.170105
Received: June 19, 2024 Revised: September 20, 2024 Accepted: October 30, 2024

6	99.64	99.69	99.58	99.7	0.35
8	99.65	99.70	99.57	99.6	0.10
10	99.49	99.69	99.26	99.4	0.5

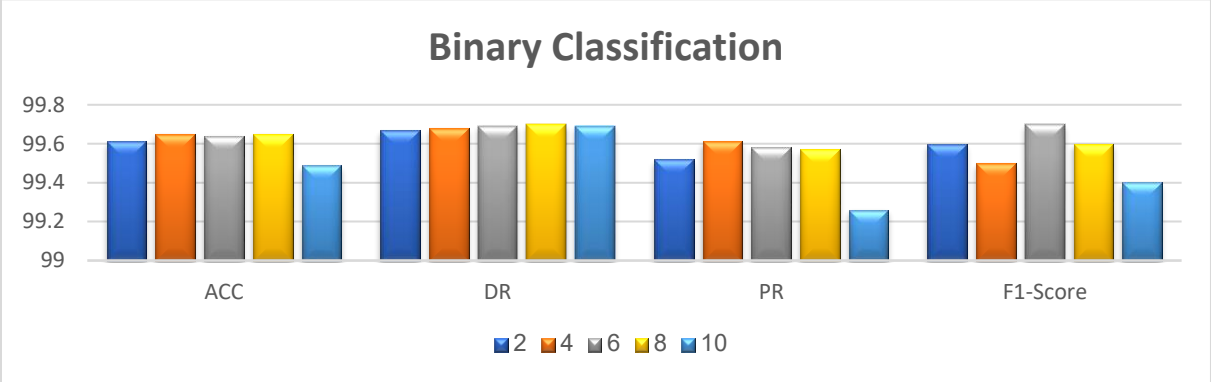

Figure 7. Graphical Representation of binary classification

Table 6: K Fold Cross for Multiclass classification

CICIDS-2018					
Multiclass Classification					
K	ACC	DR	PR	F1-Score	FAR
2	99.60	99.64	99.79	99.90	0.11
4	99.56	99.86	99.61	99.92	0.12
6	99.18	98.58	98.22	98.75	0.20
8	99.62	99.94	99.83	99.97	0.12
10	99.53	99.64	99.41	99.22	0.10

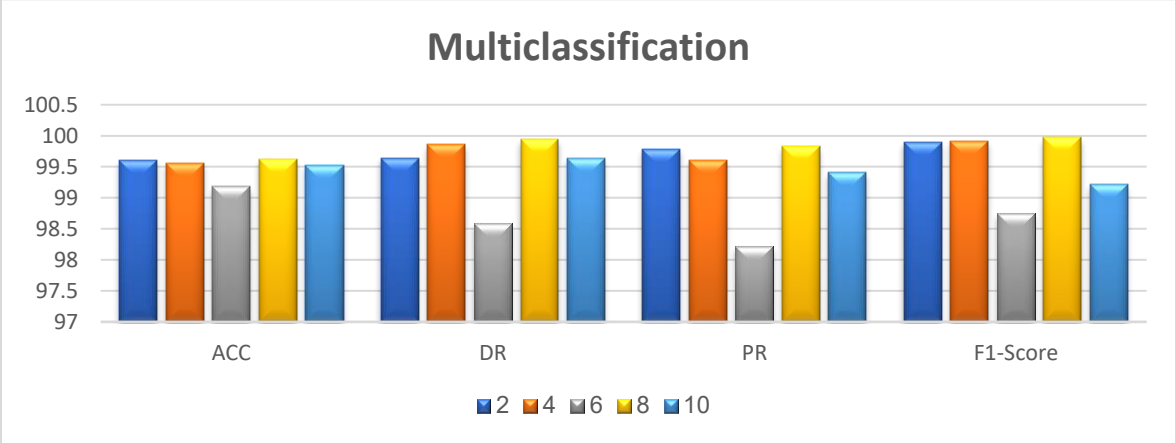

Figure 8. Graphical Repesentation for Multiclassification

10. Conclusion & Future work

In this proposed model, we have used CNN and RNN hybrid model for classification and XGBoost is used for feature extraction. This approach is used for binary and multi-class classification. CNN is used to find out spatial features and RNN is used for temporal features. The hybrid model shows a good result on the CICIDS-2018 dataset. This model shows good accuracy, detection rate and low false alarm rate. Our model will be very useful for NIDS because it can remove the problem of previous IDS. Our model focus on the low false alarm and high Accuracy, which can improve NIDS. We have used K-fold validation to remove imbalance classification.In the future, we can work on IDS in cloud environment and IOT environment. Cloud and IOT environment need to secure with an efficient NIDS.

DOI: https://doi.org/10.54216/FPA.170105
Received: June 19, 2024 Revised: September 20, 2024 Accepted: October 30, 2024

References

[1] Manimaran, A., Chandramohan, D., Shrinivas, S., & Arulkumar, N. (2020). A comprehensive novel model for network speech anomaly detection system using deep learning approach. International Journal of Speech Technology, 23, 305-313. https://doi.org/10.1007/s10772-020-09693-z.

[2] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2. https://doi.org/10.1186/s42400-019-0038-7.

[3] Rawat, W., & Wang, Z. (2017). Deep Convolutional Neural Networks for Image Classification: A Comprehensive Review. Neural Computation, 29, 2352-2449. https://doi.org/10.1162/neco_a_00990.

[4] Leevy, J., & Khoshgoftaar, T. (2020). A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data. J. Big Data, 7, 104. https://doi.org/10.1186/s40537-020-00382-x.

[5] Mohammed, Mohssen. , Abdalla, Mohamed. , Elhoseny, Mohamed. Detecting Zero-day Polymorphic Worms Using Honeywall. Journal of Journal of Cybersecurity and Information Management, vol. 15, no. 1, 2025, pp. 34-49. DOI: https://doi.org/10.54216/JCIM.150104

[6] Gopalakrishnan, Mahalakshmi & Elangovan, Uma & M, Aroosiya & M, Vinitha. (2021). Intrusion Detection System Using Convolutional Neural Network on UNSW NB15 Dataset. 10.3233/APC210116.

[7] Kottapalle, Prasanna. (2020). A CNN-LSTM Model for Intrusion Detection System from High Dimensional Data. 10. 1362-1370. 10.5281/zenodo.7911821.

[8] Shreeya Jain, Pranav M. Pawar, Raja Muthalagu,Hybrid intelligent intrusion detection system for internet of things,Telematics and Informatics Reports,Volume 8,2022,100030,ISSN 2772-5030, https://doi.org/10.1016/j.teler.2022.100030.

[9] Arun Kumar Silivery, Ram Mohan Rao Kovvur, Ramana Solleti, LK Suresh Kumar, Bhukya Madhu,A model for multi-attack classification to improve intrusion detection performance using deep learning approaches, Measurement: Sensors, Volume 30,2023,100924,ISSN 2665-9174, https://doi.org/10.1016/j.measen.2023.100924.

[10] Pritom Biswas Udas, Md. Ebtidaul Karim, Kowshik Sankar Roy,SPIDER: A shallow PCA based network intrusion detection system with enhanced recurrent neural networks,Journal of King Saud University - Computer and Information Sciences,Volume 34, Issue 10, Part B,2022, Pages 10246-10272,ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2022.10.019.

[11] Bhatnagar, Amrita. , Giri, Arun. , Sharma, Aditi. A Hybrid Intrusion Detection Approach for Cyber Attacks. Journal of Journal of Cybersecurity and Information Management, vol. 13, no. 2, 2024, pp. 08-18. DOI: https://doi.org/10.54216/JCIM.130201

[12] B., Jorge. , Mauricio, Kevin. , Marks, Adam. Fusion of Forensic Analysis of Mobile Devices: Integrating Multi-Criteria Decision Methods and Case Study Insights. Journal of Fusion: Practice and Applications, vol. 16, no. 2, 2024, pp. 32-42. DOI: https://doi.org/10.54216/FPA.160203

[13] Boukhalfa, A., Abdellaoui, A., Hmina, N., & Chaoui, H. (2019) LSTM deep learning method for network intrusion detection system. International Journal of Electrical and Computer Engineering (IJECE). https://doi.org/10.36478/jeasci.2020.227.232.

[14] Laghrissi, F., Douzi, S., Douzi, K., & Hssina, B. (2021). Intrusion detection systems using long short-term memory (LSTM). Journal of Big Data, 8(1), 65. https://doi.org/10.1186/s40537-021-00448-4

[15] Dixit, Ashish. , P., R.. , K., B.. , Sharma, Aditi. Safeguarding Digital Essence: A Sub-band DCT Neural Watermarking Paradigm Leveraging GRNN and CNN for Unyielding Image Protection and Identification. Journal of Journal of Intelligent Systems and Internet of Things, vol. 10, no. 1, 2023, pp. 33-47. DOI: https://doi.org/10.54216/JISIoT.100103

[16] Fu, Yanfang & Du, Yishuai & Cao, Zijian & Li, Qiang & Xiang, Wei. (2022). A Deep Learning Model for Network Intrusion Detection with Imbalanced Data. Electronics. 11. 898. 10.3390/electronics11060898.

[17] Aldallal A. Toward Efficient Intrusion Detection System Using Hybrid Deep Learning Approach. Symmetry.. 2022; 14(9):1916 https://doi.org/10.3390/sym14091916

[18] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," in IEEE Access, vol-5.pp. 21954-21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[19] Samha, A.K., Malik, N., Sharma, D. et al. Intrusion Detection System Using Hybrid Convolutional Neural Network. Mobile Netw Appl (2023). https://doi.org/10.1007/s11036-023-02223-6

DOI: https://doi.org/10.54216/FPA.170105
Received: June 19, 2024 Revised: September 20, 2024 Accepted: October 30, 2024

[20] J. K. Samriya, C. Chakraborty, A. Sharma, M. Kumar and S. K. Ramakuri, "Adversarial ML-Based Secured Cloud Architecture for Consumer Internet of Things of Smart Healthcare," in IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 2058-2065, Feb. 2024, doi: 10.1109/TCE.2023.3341696.

[21] X. Zhang, J. Ran and J. Mi, "An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic," 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 2019, pp. 456-460, doi: 10.1109/ICCSNT47585.2019.8962490.

[22] G. Sonowal, A. Sharma and L. Kharb, "Spear-phishing emails verification method based on verifiable secret sharing scheme", Journal of Information Assurance & Security, vol. 16, no. 3, pp. 117-124, 2021.

[23] Vanlalruata Hnamte, Jamal Hussain, Dependable intrusion detection system using deep convolutional neural network: A Novel framework and performance evaluation approach,Telematics and Informatics , Reports,Volume 11,2023,100077,ISSN 2772-5030 https://doi.org/10.1016/j.teler.2023.100077.

[24] Anand, Nishant. , Parwekar, Pritee. , Sharma, Aditi. Optimized LoRaWAN Architectures: Enhancing Energy Efficiency and Long-Range Connectivity in IoT Networks for Sustainable, Low-Power Solutions and Future Integrations with Edge Computing and 5G. Journal of Journal of Intelligent Systems and Internet of Things, vol. 13, no. 2, 2024, pp. 78-90. DOI: https://doi.org/10.54216/JISIoT.130206

[25] L. Heng and T. Weise, "Intrusion Detection System Using Convolutional Neuronal Networks: A Cognitive Computing Approach For Anomaly Detection based on Deep Learning," 2019 IEEE 18th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC), Milan, Italy, 2019, pp. 34-40, doi:10.1109/ICCICC46617.2019.9146088.

[26] Sydney Mambwe Kasongo,A deep learning technique for intrusion detection system using a Recurrent Neural Networks-based framework Computer Communications, Volume 199,2023, Pages 113-125, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2022.12.010.

[27] Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). CNN-LSTM: hybrid deep neural network for network intrusion detection system. IEEE Access, 10, 99837-99849.

DOI: https://doi.org/10.54216/FPA.170105
Received: June 19, 2024 Revised: September 20, 2024 Accepted: October 30, 2024