Efficient Deep CNN-BiLSTM Model for Network Intrusion Detection

Jay Sinha
jay.x.sinha@gmail.com

Manollas M
manollasm1997@gmail.com

***Abstract*—The need for Network Intrusion Detection systems has risen since usage of cloud technologies has become mainstream.With the ever growing network traffic, Network Intrusion Detection is a critical part of network security and a very efficient NIDS is a must, given new variety of attack arises frequently. These Intrusion Detection systems are built on either a pattern matching system or AI/ML based anomaly detection system. Pattern matching methods usually have a high False Positive Rates whereas the AI/ML based method, relies on finding metric/feature or correlation between set of metrics/features to predict the possibility of an attack. The most common of these is KNN, SVM etc., operate on a limited set of features and have less accuracy and still suffer from higher False Positive Rates. In this paper, we propose a deep learning model combining the distinct strengths of a Convolutional Neural Network and a Bi-directional LSTM to incorporate learning of spatial and temporal features of the data. For this paper, we use publicly available datasets NSL-KDD and UNSW-NB15 to train and test the model. The proposed model offers a high detection rate and comparatively lower False Positive Rate. The proposed model performs better than many state-of- the-art Network Intrusion Detection systems leveraging Machine Learning/Deep Learning models.**

Keywords: Intrusion Detection, Deep Learning, Network Traffic, CNN, RNN, Bi-LSTM, LSTM

I. Introduction

With the disruptive adoption of cloud technologies since the start of the mainstream Internet usage, the number of Intrusion incidents has also risen exponentially. Since, one data center maintained by any company like Microsoft, Amazon, Google etc hosts a multitude of on-demand servers, platforms etc to provide services to a vast range of small, medium or large enterprises, the cost associated with network security, firewalls has also seen growth incorporating a wide range of techniques for Prevention and Incident Handling to secure data and prevent disruption of services. These intrusions include Eavesdropping, network viruses, probing attacks etc.

Prediction Models based on network time series data, is one of the techniques being used for Network Intrusion Detection Systems [1]. Majority of time-series data has non-linear characteristics due to various data points that change throughout the time because of irregular fluctuations. Several statistical Machine Learning techniques like k-Nearest Neighbours, Support Vector Machine, Naive Bayes etc [2]–[7] have been used for NIDS as well. These statistical techniques do not include mutual relations between data, and mostly rely on feature engineering or feature selection, which makes them ineffective for real-time usage with even lower Detection Rates. Currently, there has been a widespread usage of deep learning techniques like Convolution Neural Networks (CNN), Recurrent Neural Network etc. These models are still under research for practical usage due to their high False Positive Rate. [8]

Two datasets will be used for Evaluation of the proposed model in this paper: NSL-KDD [9] and UNSW-NB15 [10] dataset. NSL-KDD is a refined version of the original predecessor KDD99 dataset which was released in 1999 [11]. UNSW-NB15 dataset was published by University of New South Wales, Australia in 2015 which marked the limitations of KDD98 and KDD99 data sets including the fact that these datasets do not include modern low footprint attacks. [12]

To perform on both of these very unique datasets, this paper proposes a hierarchical model by combining layers of 1D-CNN and Bi-LSTM. CNN is used to learn the spatial/hgh-level features of a dataset and the Bi-LSTM layers (essentially a sub-category of RNN) to learn the long time-range temporal features of the data and combine these to predict attacks. The predictions are done for Binary Classification of predicting whether or not an attack is happening and Predicting the exact category of the attack. For multi-category attack prediction, in NSL-KDD, the analysis is done on 5 classes - Normal, Denial of Service (DoS), Probe (Probing Attacks), R2L (Root to Local Attacks) and U2R (User to Root Attack). For multicategory attack prediction in UNSW-NB15, 10 classes have been used: Normal, DoS, Exploits, Generic, Reconnaissance, Worms, Shellcode, Analysis, Backdoor and Fuzzers.

II. Related Work

Deep Learning approaches have always been popular with Network Intrusion Detection problems. With the KDD-99 cup data in circulation, the issue has met with proposed deep learning models and the solutions they provide in an incremental fashion. At first, the approaches solving the same, were focused towards pattern recognition, with [13], discussing the approach with a BM pattern matching algorithm which proves to be accelerated in terms of time performance and recognition speed. After pattern recognition algorithms, researchers have used feature selection by leveraging machine learning and deep learning techniques.

A. Machine Learning Techniques:

Traditional machine learning techniques such as Support Vector Machine (SVM) [14], Random Forest [15] and Adaptive Boosting [16] have been often used by researchers for constructing Network Intrusion Detection classifiers. Researchers have also used k-Mean Clustering [17] for efficient classification but they have always turned out to be weak because of high False Positive Rate (FPR), overfitting and with lower accuracy on classes having less percentage of data available as compared to the classes in sufficient numbers. The reason being, the traditional machine learning approaches concentrate upon learning feature importance, feature availability and dimensionality reduction techniques to find the most optimum correlation between data points that seem to have the most amount of influence upon the end-result while completely overlooking the importance of correlation between the features and take into account the time-steps in order to predict the best possible result. This led to the adoption of deep learning approaches in order to resolve the lacking points of the above.

B. Deep Learning Techniques:

There is a large number of research made on Network Intrusion detection leveraging Deep Learning techniques. For this paper, we will be discussing 4 key papers and later on, the results from the proposed model will be benchmarked against the same 4 papers.

1) [18] Using RNN : NSL-KDD and UNSW-NB15 datasets have time step column which makes the use of RNN a default choice. Recurrent neural networks are an extension to Artificial Neural Networks and are mainly used for analysing time series data to learn long range temporal features. RNNs contain an internal feedback loop in order to store time associations and end up forming an acyclic graph as a result. Backpropagation results in a vanishing gradient problem [19](the features learned at the very start of the network start to have the very least amount of effect on the end-result of the model). To solve this problem LSTM (Long Short Term Memory) [20] and GRU (Gated Recurrent Units) are used in order to solve the vanishing gradient problem.

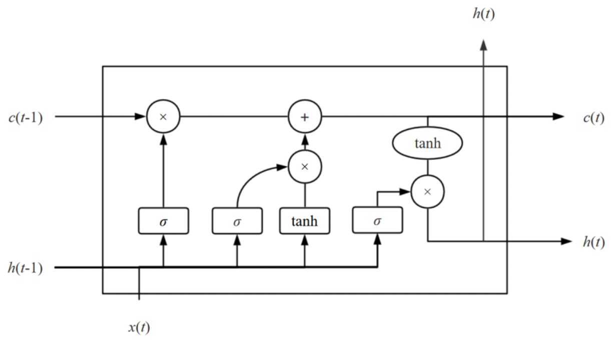


Fig. 1. Structure of a LSTM Cell

$$f_t = (W_f.[h_{t-1}, x_t] + b_f) \quad (1)$$

$$i_t = tanh(W_i[h_{t-1}, x_t] + b_i) \quad (2)$$

$$C_t = tanh(W_C.[h_{t-1}, x_t] + b_C) \quad (3)$$

$$C_t = f_t * C_{t-1} + i_t * \ C_t o_t = (W_o[h_{t-1}, x_t] + b_o \quad (4)$$

$$h_t = o_t * tanh(C_t \quad (5)$$

where f, i, t, o, h, C, W, b denote forget, input, time-step, output layer, hidden layer, cell state, Weight matrix, bias respectively.

In [18], the authors have ran a simulation on a simple RNN, LSTM and GRU and benchmarked them on the KDD'99 Dataset for multi-category predictions and end up achieving accuracy ranging from 94.2% to 96.98% 94.3% to 95.37% on different combination of LSTM layers and GRU layers respectively. On multicategory UNSW-NB15, authors of [18] have reported 64.8% accuracy from a GRU network and 67.5% from a LSTM Network.

2) [21], [22] Using CNN : Convolutional Neural Networks or CNN have been the top performer in Image Recognition for learning boundary regions of different objects in an image which are called spatial features. [23]

In [21], the authors propose a CNN with three hidden layers consisting of a Convolutional Layer along with pooling layer and leverages coarse grained to fine grained learning for deepening the network architecture with more post-convolution kernels resulting in mapping of the features in a high-dimensional space to leverage improved learning. The model mentioned is applied to KDD'99 dataset and gives an accuracy of 99.23%.

In [22], the authors have proposed a 1D-CNN citing that 2-D CNNs are mainly efficient with 2-D Images and 1-D CNN can be used better for learning features on a time-series dataset by by serializing TCP/IP packets in a predetermined time range for effective classification. The dataset used in the papers is UNSW-NB15 and the authors have reported an accuracy of 91.2% with 3 layers of 1-D CNN for binary classification on UNSW dataset.

3) [24] Using CNN and RNN: CNN and RNN are two very different types of neural networks that are being used recently upon time-series data itself. The idea behind combining them is that CNN are used for learning spatial features by increasing the number of kernels which makes learning coarse grained (at the start of the network) and fine-grained (at the end of the network). The RNN in the model learns the temporal features from long range time-series data.

In [24], the authors have proposed such a hierarchical model to leverage spatial and temporal features learning of CNN and RNN respectively. The model consists of multiple CNN layers followed by 2 LSTM layers after preprocessing the dataset. The DARPA and ISCX2012 dataset are very similar to KDD99 Dataset which have attacks combined into 5 upper-level categories and give accuracy of around 50% for DARPA and around 97% for ISCX2012 dataset.

4) [25], [26] Using BiLSTM : A BiLSTM or Bidirectional LSTM is a type of LSTM network in which the learning data is fed from start to end of the model while feeding the information from end to start as well which allows for better learning at every timestep of data. This results in better learning of features per time step. In [25], the authors have proposed a model called BAT which combines Bi-LSTMs with an Attention layer to filter out features that have the least/minimal impact on the end result of the model. The model consists of multiple convolutional layers with a BiLSTM, Attention, Fully Connected Dense Layer. The model is run on NSL-KDD dataset with its 5 five classes resulting in accuracy ranging from 82.97% to 84.24% on multicategory analysis.

In [26], the author has proposed a two Bi-LSTM layered model with sigmoid activation and has performed analysis on UNSW-NB15 dataset with an average F1-Score of 0.86.

III. EXPERIMENT

In this paper, we propose a model combining 1-Dimensional Convolutional Neural Network (1-D CNN) [27] and multiple layers of Bi-directional LSTM (Bi-LSTM) [28]. In this section, the layers of the proposed model's neural network will be discussed along with the Datasets and the preprocessing techniques used on these datasets.

A. Model Architecture

As evident from the block diagram, the proposed model consists of a 1-D CNN Layer along with multiple layers of Bi-LSTM with Reshape and Batch Normalization layers in between. The idea is to leverage the 1-D CNN layer and max pooling layer for it's parameter sharing, spatial arrangement and local perception characteristics. Parameter Sharing allows for a reduced set of parameters and free variables that results in feature extraction with fewer use of processing resources. Spatial arrangement allows for the arrangement in a sparse matrix of features recognised so far to enable better recognition of correlation between features. Lastly, local perception allows for reduced number of parameters and hence, decreases the training duration by a huge amount. Therefore, 1-D CNN allows for fast paced spatial learning for the given time-series data. The 1-D CNN layer is followed by a Max Pooling layer which allows for sample-based discretization of parameters in order to recognise the relevant features resulting reduced training time and preventtion from overfitting. After Max Pooling, comes Batch Normalization layer which enables normalization of parameters between intermediate layers to prevent slower training times. Reshape Layers after batch normalization layers reshape the output of the previous layer for the upcoming pair of Bi-LSTM layers.

Bi-LSTM layers are used to learn from both forward and backward time series data with the hidden layers making use of two units having the same input and connected to the same output. One of the unit processes forward time series and the other processes backward time series. This so called arrangement is said to provide the layers with future data for boosting training time with better learning of features resulting in greater precision for a long spanning time-series data.

The two Bi-LSTM layers in the model are arranged in a manner which doubles it's kernel size in every iteration. As per the block diagram of the model, the first Bi-LSTM layer starts with 64 units and the next and last Bi-LSTM layer 128 number of units. The reason for this choice is to mimic the use of coarse grain to fine grained learning to better understand the correlation of long range time dependent features learnt by the first 1-D CNN Layer which provides for better extraction of features and faster training times. Between each Bi-LSTM layer, there is a Max Pooling layer to dismiss the least relevant features and the Batch Normalization layers to normalize the output data of the previous intermediate layer in order to boost performance and decrease training times.

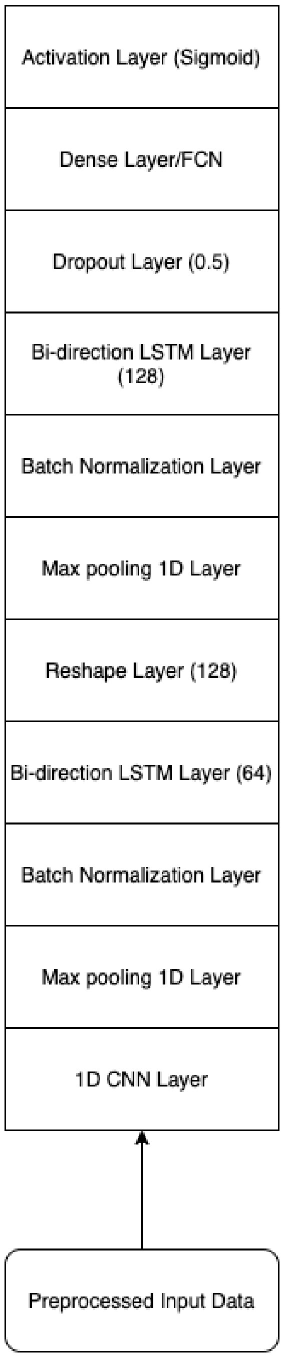

Activation Layer (Sigmoid)
Dense Layer/FCN
Dropout Layer (0.5)
Bi-direction LSTM Layer (128)
Batch Normalization Layer
Max pooling 1D Layer
Reshape Layer (128)
Bi-direction LSTM Layer (64)
Batch Normalization Layer
Max pooling 1D Layer
1D CNN Layer
Preprocessed Input Data

Fig. 2. Block Diagram of the model used

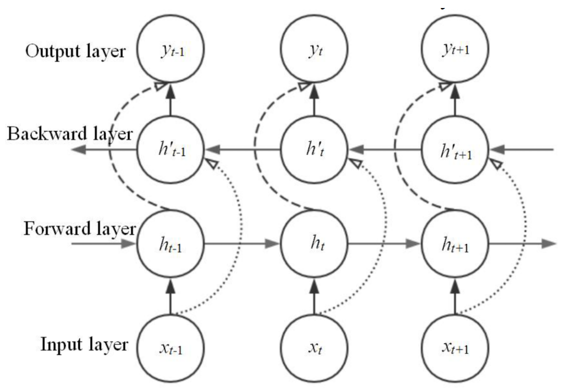


Fig. 3. Structure of a Bidirectional LSTM Cell

Table 1: NSL-KDD Dataset Attack Categories

Category	Count
Normal	77054
DoS	53385
Probe	14077
R2L	3749
U2R	252
Total	148517

The Fully Connected Dense layer comes next which serves as an Output Layer followed by a Dropout Layer. The Dropout Layer is put in place to account for Over Fitting even though the model uses Max Pooling in between every layer. The reason behind this is that, generally, CNN and RNN used in combination have a higher probability of overfitting and perform poorly on the testing set. To keep this in check, the model is evaluated with k-fold cross validation. (More on k-fold cross validation in the following section)

B. Dataset

The proposed model in this paper, is evaluated on two datasets: NSL-KDD and UNSW-NB15.

1) NSL-KDD Dataset: The NSL-KDD dataset was made available by University of New Brunswick. The NSL-KDD Dataset is an improvement on KDDCup'99 Dataset as the latter one has inherent drawbacks revealed by various analyses. NSL-KDD contains the essential records of the complete KDD Dataset and has been one of the most popular dataset for Network Intrusion Detection Systems analysis. NSL-KDD has a lot distinctions from its predecessor including: Removal of redundant records [11], sufficient availability of records in training and testing dataset and number of selected records from each difficulty group inversely proportional to percentage of records in the original KDD Dataset

Table 2: UNSW-NB15 Dataset Attack Categories

Category	Count
Normal	93000
Analysis	2677
Backdoor	2329
DoS	16353
Exploit	44525
Fuzzers	24246
Generic	58871
Reconaissance	13987
Shellcode	1511
Worms	174
Total	257673

2) UNSW-NB15 Dataset: This dataset was published by University of New South Wales in 2015. Since its inception, UNSW dataset has been widely used and gives The UNSW-NB15 dataset includes a wider variety of attacks families, number of features extracted, number of distinct IP addresses used for simulation and collection of data [12]. This data set consists of a hybrid of the real modern normal and the contemporary synthesized attack activities of the network traffic. Table 1 and 2 shows a list of features available in NSL-KDD and UNSW-NB15 Datasets.

C. Pre-Processing

Preprocessing of the datasets is generally handled by Normalization of numeric features and One Hot Encoding of Categorical features for both NSL-KDD and UNSW-NB15 dataset. But as discussed earlier, NSL-KDD Dataset has a refined number of records with every attack category. On the other hand, the UNSW-NB15 dataset has an extremely low number of records for categories like Worms, Fuzzers etc. To solve this issue, Oversampling technique has been used in the training set to make sure every attack category has a comparable number of records.

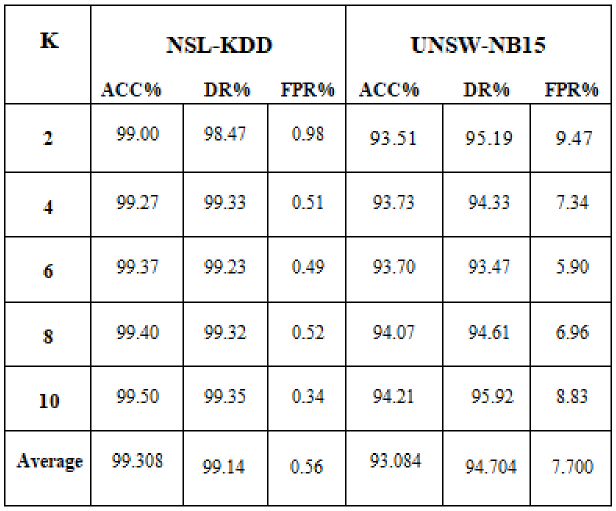
1) One Hot Encoding: There are categorical features in both NSL-KDD and UNSW-NB15 datasets and these should be converted to numerical values for our deep learning model to give out good prediction results.Hence these columns have been converted into numerical values in the pre-processing part using get-dummies function of pandas python library .One-hot encoding is chosen over label encoder since label encoder will produce multiple number in the same column, the model might misunderstand these values to be in a particular order and this will impact the classification.

2) Normalization: Normalization is rescaling the data into a particular range to reduce redundancy and improve training time of the model. Min-Max Normalization is used in the paper and rescales the range of the data to [0,1].

$$X[i] = \frac{X[i] - X_{min}}{X_{max} - X_{min}} \tag{6}$$

3) Stratified K-cross fold validation: Stratification is the process of rearranging the data to ensure each fold is a good representative of the whole. Stratified K-cross fold validation technique splits the dataset into K sets and the model uses

K-1 folds for training and is validated on the Kth fold. This is continued until all the folds are used to validate the model once. Stratification ensures that each fold is a good representation of the whole dataset,this leads to parameter fine-tuning and helps model in classifying the attacks better.K-cross fold method is chosen over other validation methods since it performs better than other methods and requires less computation power [29].



K	NSL-KDD			UNSW-NB15		
	ACC%	DR%	FPR%	ACC%	DR%	FPR%
2	99.00	98.47	0.98	93.51	95.19	9.47
4	99.27	99.33	0.51	93.73	94.33	7.34
6	99.37	99.23	0.49	93.70	93.47	5.90
8	99.40	99.32	0.52	94.07	94.61	6.96
10	99.50	99.35	0.34	94.21	95.92	8.83
Average	99.308	99.14	0.56	93.084	94.704	7.700

Fig. 4. Table of Binary Classification Results

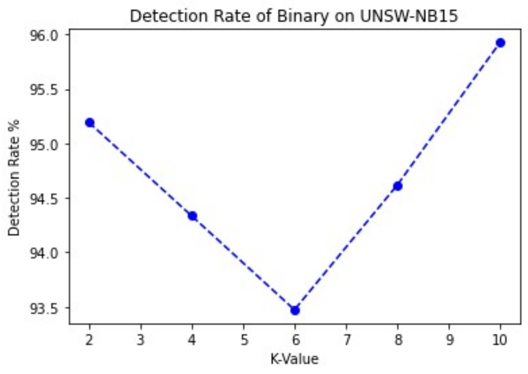


Fig. 5. Detection Rate Plot of Binary Classification for UNSW-NB15 dataset

4) Oversampling: Random Oversampling duplicates data points randomly from the minority class, this reduces the data imbalance and improves prediction accuracy of minority class. RandomOverSampler class of imblearn.oversampling python library is used for oversampling with 'minority' as parameter. The number of samples of minority class Worms in UNSW-NB15 dataset is 173 this is very little compared to the total number of samples 257,673 and this imbalance decreases the prediction accuracy of the minority class [30]. Hence random oversampling technique is applied only on the training set of UNSW-NB15 and there is a significant increase in accuracy, detection rate of the class Worms as you can see in the Fig.12 .

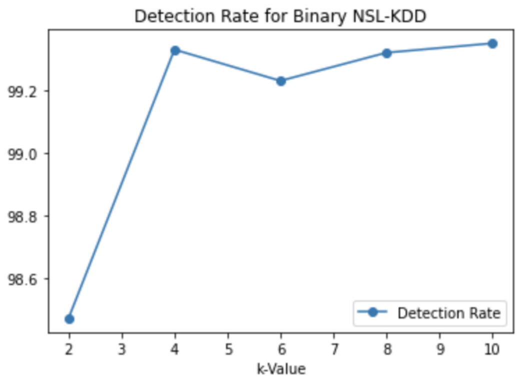


Fig. 6. Detection Rate Plot of Binary Classification for NSL-KDD dataset

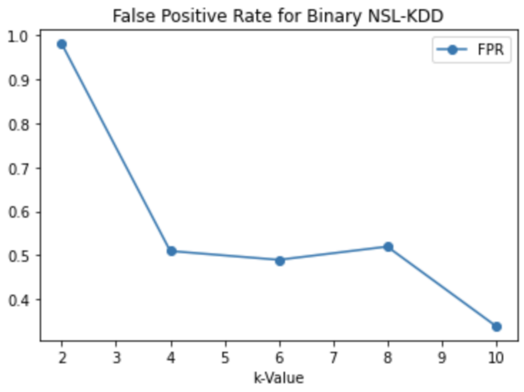


Fig. 7. Flase Positive Rate Plot of Binary Classification for NSL-KDD dataset

IV. Evaluations and Discussion

A. Evaluation Metrics

Some of the metrics that are used to evaluate the performance of the proposed model are Accuracy(ACC),Detection Rate(DR), False Positive Rate(FPR), F1-Score and ROC-AUC curve. Accuracy and DR measures the model's ability to predict all classes and attacks respectively. FPR is the percentage of normal records classified as attacks and this is a very important metric along with DR and ACC. If the FPR is high then the model may not be effective although it has good DR and ACC. F1-score gives more realistic measure of the performance as precision and recall may not give a clear picture of the performance alone. The definition of the above mentioned metrics are given in Equations (7),(8),(9) and (10).

$$Accuracy(ACC) = \frac{TP+TN}{TP+TN+FP+FN} \tag{7}$$

$$DetectionRate = \frac{TP}{TP+FN} \tag{8}$$

Where TP is the number of attacks correctly classified, TN is the number of normal traffic correctly classified,FN is the

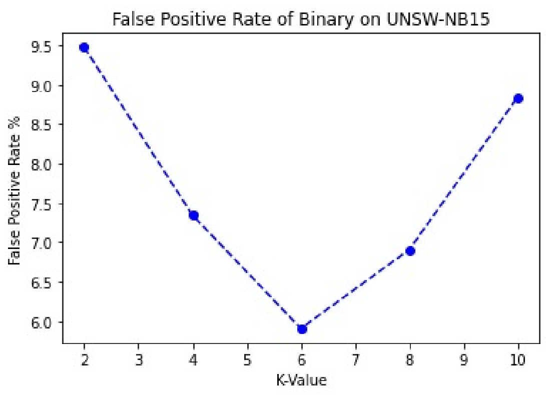
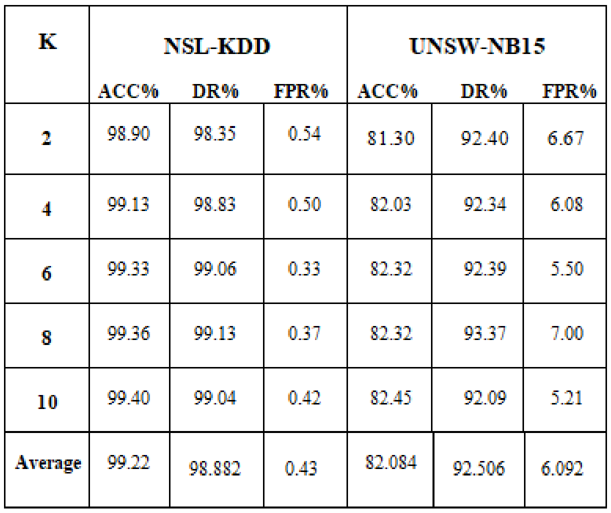


Fig. 8. Flase Positive Rate Plot of Binary Classification for UNSW-NB15 dataset



K	NSL-KDD			UNSW-NB15		
	ACC%	DR%	FPR%	ACC%	DR%	FPR%
2	98.90	98.35	0.54	81.30	92.40	6.67
4	99.13	98.83	0.50	82.03	92.34	6.08
6	99.33	99.06	0.33	82.32	92.39	5.50
8	99.36	99.13	0.37	82.32	93.37	7.00
10	99.40	99.04	0.42	82.45	92.09	5.21
Average	99.22	98.882	0.43	82.084	92.506	6.092

Fig. 9. Table of Multi Class Classification Results

number of attacks misclassified as normal traffic and FP is the number of normal traffic misclassified as attack.

$$FalsePositiveRate = \frac{FP}{FP + TN} \tag{9}$$

$$F1 - score = \frac{2 * Precision * Recall}{Precision + Recall} \tag{10}$$

Finally the ROC-AUC curve measures the model's capability of distinguishing between classes of the dataset when the threshold is varied. AUC (Area Under Curve) is the entire area underneath the ROC curve and it is a value that varies between 0 to 1. Higher the AUC, better the model is at classifying different classes correctly.

B. Model Results

1) Binary Classification: In Binary Classification the model predicts whether the sample is an attack or belongs to normal class. Table in Fig.4 has the results of binary classification by the proposed model under different Stratified K-Fold Cross

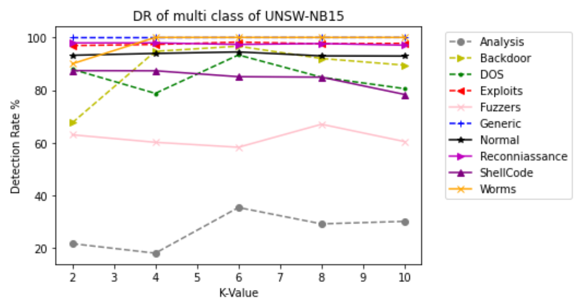


Fig. 10. Detection Rate Plot of all classes for UNSW-NB15

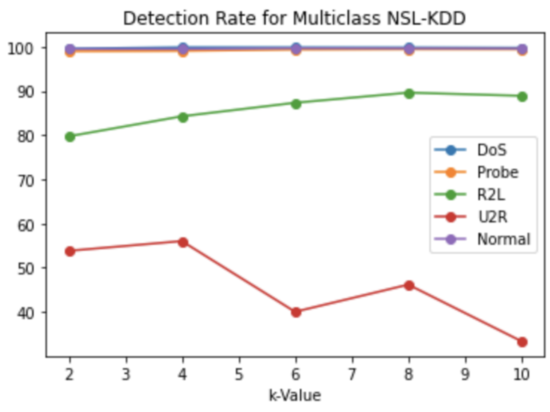


Fig. 11. Detection Rate Plot of all classes for NSL-KDD

Validation for k=2 to 10, the average detection rate (DR%) for UNSW-NB15 dataset is 94.704%, accuracy (ACC) is 93.084% and false positive rate (FPR%) is 7.70%. The model shows high detection rate (DR%) and comparatively low false positive rate (FPR%) and these results for various k-values are plotted in Fig.5, Fig.8 respectively . Fig.13 shows different F1-Scores for k ranging from 2 to 10, the best F1-Score for binary classification is 0.9548 for k=10. The maximum accuracy is 94.21% and detection rate is 95.92% which is obtained when k is 10 and correctly so because as the number of folds increase there will be more sample of each attack/normal class available for the model to train and hence the model will be able to classify them better.

In binary NSL-KDD, the model gives an average accuracy of 99.308% for k-value ranging from 2 to 10 with the best accuracy of 99.5% for k-value=10. The average Detection rate given by model is 99.14%. While the model increases DR from k-value 2 to 4, a decrease in the DR can be seen for k-value = 6. The average FPR% given by the model is 0.0056 with the least FPR received for k-value = 10. The individual metrics and plots as per k-value can be seen in Fig.4, Fig.6 and Fig.7. F1-Score for multiclass NSL-KDD analysis, shows a rise in values from k-value 2 to 10 with the best value of 0.9949 given k-value=10.

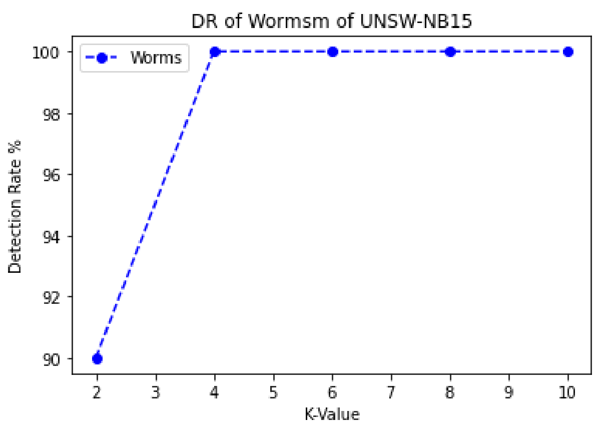


Fig. 12. Detction Rate Plot of Worms attack class for UNSW-NB15

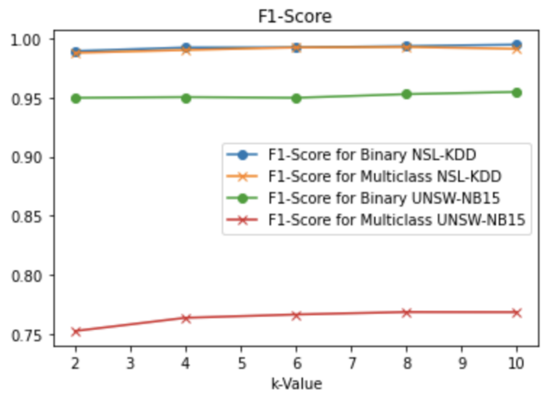


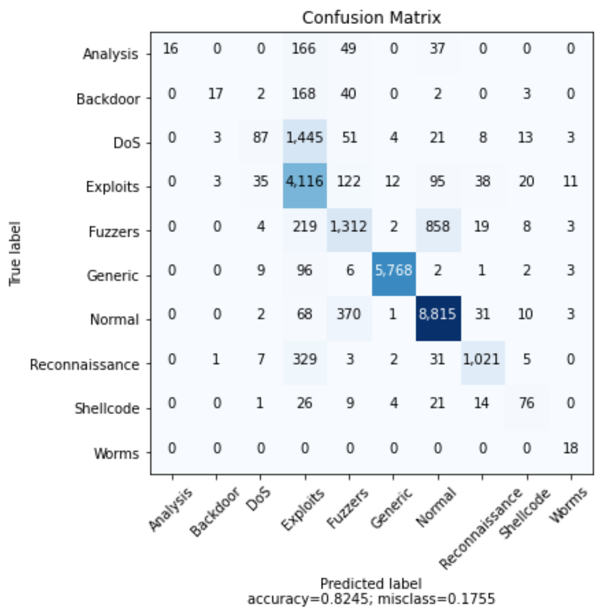
Fig. 13. F1-Score Plot for NSL-KDD and UNSW-NB15 Datasets

.

2) Multi-Class Classification: The results of multi class classification on UNSW-NB15 Dataset for k ranging from 2 to 10 can be seen in Table of Fig.9. The average accuracy is 82.084% (ACC), detection rate (DR%) is 92.506% and false positive rate is 6.092%.The best F1-Score of multi-class classification is 0.7684 for k=8 and F1-Score for different k values is given in Fig.13.

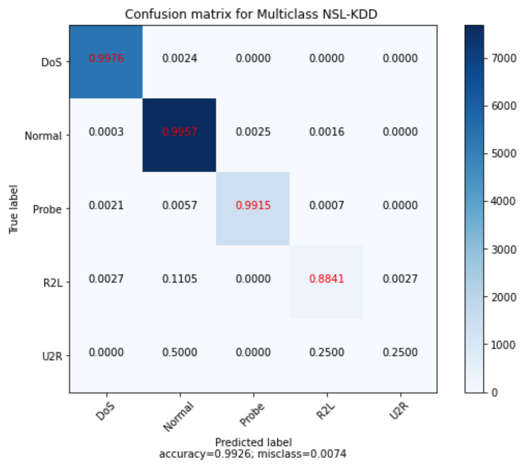
Detection rate of each of the 10 classes is plotted in fig(10) , the model is able to classify Normal,Backdoor,DOS,Exploits, Shellcode, Generic, Reconnaissance and worms very accurately. The model has an average capability to detect the class Fuzzers. The FPR% is comparitavely low and better than any state-of-the-art models and it is seen in Table of Fig.9.

For NSL-KDD dataset in multiclass, the model gives an average Accuracy of 99.22% with the best accuracy of 99.4% for k-value=10. The average Detection Rate is 98.882% with the best result of 99.13% by k-value = 10. The average FPR% is 0.0043 with the best value of 0.0033 by k-value=10. Examining the plot of individual class DR in Fig.11 shows decreasing value of DR for U2R category for k-values greater than 4 which is due to the fact, as k-value increases, the



True label	Analysis	Backdoor	DoS	Exploits	Fuzzers	Generic	Normal	Reconnaissance	Shellcode	Worms
Analysis	16	0	0	166	49	0	37	0	0	0
Backdoor	0	17	2	168	40	0	2	0	3	0
DoS	0	3	87	1,445	51	4	21	8	13	3
Exploits	0	3	35	4,116	122	12	95	38	20	11
Fuzzers	0	0	4	219	1,312	2	858	19	8	3
Generic	0	0	9	96	6	5,768	2	1	2	3
Normal	0	0	2	68	370	1	8,815	31	10	3
Reconnaissance	0	1	7	329	3	2	31	1,021	5	0
Shellcode	0	0	1	26	9	4	21	14	76	0
Worms	0	0	0	0	0	0	0	0	0	18

Fig. 14. Confusion Matrix for UNSW-NB15



True label	DoS	Normal	Probe	R2L	U2R
DoS	0.9976	0.0024	0.0000	0.0000	0.0000
Normal	0.0003	0.9957	0.0025	0.0016	0.0000
Probe	0.0021	0.0057	0.9915	0.0007	0.0000
R2L	0.0027	0.1105	0.0000	0.8841	0.0027
U2R	0.0000	0.5000	0.0000	0.2500	0.2500

Fig. 15. Confusion Matrix for NSL-KDD

number of train sample decreases. Three classes including Normal, DoS, Probe have a high DR. The individual values for Accuracy, DR and FPR along with plots can be checked in Fig.9, Fig.11.

F1-Score for multiclass NSL-KDD analysis, shows a rise in values from k-value 2 to 8 with a slight dip for k-value=10. As discussed, the F1-Score is a very reliable metric for testing a model, which is 0.9929 given by k-value = 8. The plot can be seen in Fig.13.

The class Analysis has very low DR% because this class has 2677 samples in the dataset, this is just 1.03% of the total samples in the dataset and the model does not have enough data to perform better on this class. The class Worms has a lower percentage of records(0.067%) than the class Analysis but the detection rate of the class Worms is reaching 100%

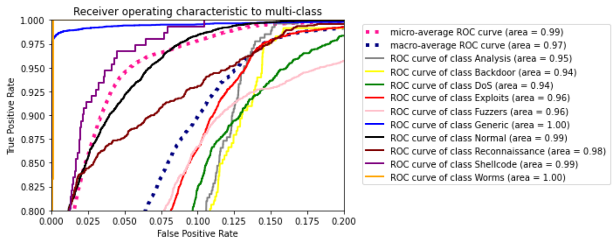


Fig. 16. ROC-AUC Curve for UNSW-NB15

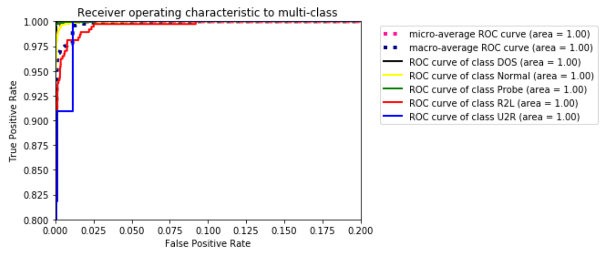


Fig. 17. ROC-AUC Curve for NSL-KDD

as plotted in the Fig.12, this is the result of oversampling. The model was able to train better since more samples were available for training as oversampling was applied on the class Worms. In the confusion matrix Fig.14 all 18 records in the test set were classified as Worms and detection rate is 100% and FPR% is 0.

Fig.16 is ROC-AUC plots on UNSW-NB15, the Area Under Curve (AUC) of all classes are between 0.94-1.0 and the average AUC is 0.971. This is an indicator that the model is very efficient and accurate in distinguishing among various classes of the dataset.

Fig.17 illustrates the AUC for multiclass NSL-KDD which is 1.00 for all classes. As mentioned before, AUC is the measure of model's capability to distinguish between different classes/categories inside a dataset for which the model performs well on NSL-KDD dataset.

C. Comparison with other models

1) NSL-KDD: Comparing the proposed model with other models like: Few-Shot Learning, Bi-LSTM Attention (BAT) model, HAST-IDS and SVM. In comparison, it is clear that the proposed model offers improved performance across metrics specially in Detection Rate. In comparison, the FPR is lower in BAT but still when taking into account all factors including DR and Accuracy, the proposed model becomes the favourable choice. The closest model in overall performance is HAST-IDS model as it provides little lower results.

Table 3: NSL-KDD Multiclass Comparison

Model	DR%	FPR%	Accuracy%
Proposed Model	98.882	0.43	99.22
Few-Shot Learning	92.06	4.22	92.33
BAT-MC Model	83.6	0.34	84.15
HAST-IDS	95.85	-	93.27
SVM	-	-	69.52
1-D CNN	-	-	78.97

2) UNSW-NB15: Comparing the results of proposed model for UNSW-NB15 dataset in multiclass with other models like Adaboost, LSTM, SVM. As evident from table below, the proposed model gives better performance across all metrics including Detection Rate, False Positive Rate and Accuracy. The closest model in this comparison is HAST-IDS as it has a 1.2% higher Detection rate but larger False Positive Ratio along with lower accuracy which makes the proposed model more preferable for use in Intrusion Detection Systems.

Table 4: UNSW-NB15 Multiclass Comparison

Model	DR%	FPR%	Accuracy%
Proposed Model	92.506	6.092	82.084
Adaboost	91.13	22.11	73.19
LSTM	92.06	4.22	92.33
SVM	83.71	7.73	74.8
HAST-IDS	93.65	9.6	80.03

V. Conclusion

This paper proposes a model for analysing network traffic including a multitude of variables like protocol type, service type etc. Oversampling was incorporated in order to account for imbalanced datasets. The combination of using CNN and Bi-directional LSTM layers enabled learning of spatial and temporal features. Result of the proposed model after training and testing on NSL-KDD and UNSW-NB15 datasets gives promising prospective real-time usage for Intrusion Detection systems. As evident from the result, the need to optimize the model for U2R and Worms category of attacks is to be investigated in the future to allow for testing in a honeypot system.

References

[1] H. J. Liao, C. H. R. Lin, Y. C. Lin, and K. Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, p. 16–24, 01 2013.

[2] S. Kishorwagh, V. K. Pachghare, and S. R. Kolhe, "Survey on intrusion detection system using machine learning techniques," *International Journal of Computer Applications*, vol. 78, no. 16, pp. 30–37, September 2013.

[3] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on sdn based network intrusion detection system using machine learning approaches," *Peer-to-Peer Networking and Applications*, vol. 12, pp. 493–501, 2019.

[4] M. Panda, A. Abraham, S. Das, and M. R. Patra, "Network intrusion detection system: A machine learning approach," *Intelligent Decision Technologies*, vol. 5, no. 4, pp. 347–356, 2011.

[5] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A new intrusion detection system based on knn classification algorithm in wireless sensor network," *Journal of Electrical and Computer Engineering*, vol. 2014, June 2014.

[6] S. Garg and S. Batra, "A novel ensembled technique for anomaly detection," *Int. J. Commun. Syst.*, vol. 30, no. 11, pp. 32–48, July 2017.

[7] F. Kuang, W. Xu, and S. Zhang, "A novel hybrid kpca and svm with ga model for intrusion detection," *Applied Soft Computing*, vol. 18, pp. 178–184, May 2014.

[8] N. Hubballi and V. Suryanarayanan, "False alarm minimization techniques in signature-based intrusion detection systems: A survey," *Computer Communications*, vol. 49, pp. 1–17, 08 2014.

[9] [Online]. Available: http://nsl.cs.unb.ca/NSL-KDD/

[10] [Online]. Available: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/

[11] L. Dhanabal and D. S. Shantharajah, "A study on nsl-kdd dataset for intrusion detection system based on classification algorithms," vol. 4, 2015.

[12] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, 2015, pp. 1–6.

[13] C. Yin, "An improved bm pattern matching algorithm in intrusion detection system," *Applied Mechanics and Materials*, vol. 148-149, pp. 1145–1148, 12 2011.

[14] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, "Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection," *IEEE Access*, vol. 6, pp. 33 789–33 795, 2018.

[15] J. Zhang, M. Zulkernine, and A. Haque, "Random-forests-based network intrusion detection systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 38, no. 5, pp. 649–659, 2008.

[16] W. Hu, J. Gao, Y. Wang, O. Wu, and S. Maybank, "Online adaboost-based parameterized methods for dynamic distributed network intrusion detection," *IEEE Transactions on Cybernetics*, vol. 44, no. 1, pp. 66–82, 2014.

[17] Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir, "Intrusion

[26] S. Yang, "Research on network behavior anomaly analysis based on bidirectional lstm," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2019, pp. 798–802.

detection based on k-means clustering and oner classification," in *2011 7th International Conference on Information Assurance and Security (IAS)*, 2011, pp. 192–197.

[18] R. Vinayakumar, K. Soman, and P. Poornachandran, "Evaluation of recurrent neural network and its variants for intrusion detection system (ids)," *International Journal of Information System Modeling and Design*, vol. 8, July-September 2017.

[19] Y. Bengio, P. Simard, and P. Frasconi, "Learning long-term dependencies with gradient descent is difficult," *IEEE Transactions on Neural Networks*, vol. 5, no. 2, pp. 157–166, 1994.

[20] S. Hochreiter and J. Schmidhuber, "Long short-term memory," 1997.

[21] M. Azizjon, A. Jumabek, and W. Kim, "1d cnn based network intrusion detection with normalization on imbalanced data," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 2020, pp. 218–224.

[22] R. U. Khan, X. Zhang, M. Alazab, and R. Kumar, "An improved convolutional neural network model for intrusion detection in networks," in *2019 Cybersecurity and Cyberforensics Conference (CCC)*, 2019, pp. 74–77.

[23] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, vol. 86, no. 11, pp. 2278–2324, 1998.

[24] W. Wang, Y. Sheng, J. Wang, X. Zeng, X. Ye, Y. Huang, and M. Zhu, "Hast-ids: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection," *IEEE Access*, vol. 6, pp. 1792–1806, 2018.

[25] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "Bat: Deep learning methods on network intrusion detection using nsl-kdd dataset," *IEEE Access*, vol. 8, pp. 29 575–29 585, 2020.

[27] A. K. Verma, P. Kaushik, and G. Shrivastava, "A network intrusion detection approach using variant of convolution neural network," in *2019 International Conference on Communication and Electronics Systems (ICCES)*, 2019, pp. 409–416.

[28] M. Schuster and K. K. Paliwal, "Bidirectional recurrent neural networks," *IEEE Transactions on Signal Processing*, vol. 45, no. 11, pp. 2673–2681, 1997.

[29] R. Kohavi, "A study of cross-validation and bootstrap for accuracy estimation and model selection," *IJCAI'95: Proceedings of the 14th international joint conference on Artificial intelligence*, vol. 2, p. 1137–1143, August 1995.

[30] M. Longadge, M. S. S. Dongre, and D. L. Malik, "Class imbalance problem in data mining: Review," *International Journal of Computer Science and Network (IJCSN)*, vol. 2, February 2013.