A Deep Learning Model for Network Intrusion Detection with Imbalanced Data

Aysha Bibi *211856 MSCYS-II*

Hidayat-ur-Rehman *211833 MSCYS-II*

DATASET:

The NSL-KDD dataset is used in the experiments in this study. There are 42 dimensional features in the NSL-KDD dataset, one of which is a categorization tag, and the other are feature tags. The classification variables for binary classification are classified into two categories: normal and abnormal. The classification labels are separated into five categories for multiclassification: normal, Dos, R2L, U2R, and probe.

DATA PREPROCESSING:

- **One hot encoding**

  In dataset, there are 3 categorical elements *service, flag,* and *protocol type*. Using the one-hot-encoding approach, we converted these category data into numerical features. Each category characteristic is represented by a binary value. The z2 feature has three properties. The one hot encoding approach was used to convert them to binary data: [1,0,0], [0,1,0],[0,0,1], respectively. Also transformed into one-hot-encoding matrices were z3 and z4 attributes (service and flag).

- **Data Augmentation:**

  Because the amount of U2R and R2L samples in the NSL-KDD testing set is so much larger than that in the training data set, so only a small proportion of such tests are in the training data set, the trained model has trouble differentiating these sample data; as a result, we used the above said ADASYN algorithm to enlarge the information and broaden the sample data (such as U2R and R2L) that contribute for a relatively small percentage of the total amount training set, attempting to balance the percentage of the most of This can help to fix the data transmission imbalance problem to some extent and improve the model's generalization capabilities.

- **Normalization**

The numeric feature values were mapped into the numeric range 0 and 1 using the conventional scalar normalizing approach.

A sample's standard score is computed as arises:

$z = (x - m) / d$

CLASSIFICATION

The dataset that we utilized in our work is NSL KDD dataset containing two class categories normal class label and abnormal class. We have used two deep learning classifiers such as LSTM and Autoencoder (AE), and three other conventional for the five class labels as Denial of service (DOS), Normal, R2L, and U2R.

- **Binary Classification**

  In binary classification we have changed the attack labels into two categories such as ‘NORMAL’ and ‘ABNORMAL’. First, create the data frame with binary labels ‘NORMAL’ and ‘ABNORMAL’ and then encode the labels into 0 and 1. Pie-chart for the binary classification is shown in figure. As shown in the figure we have 53% normal data and 47% abnormal labels in the NSL KDD dataset in case of binary classification. In abnormal label we have four types of attacks.

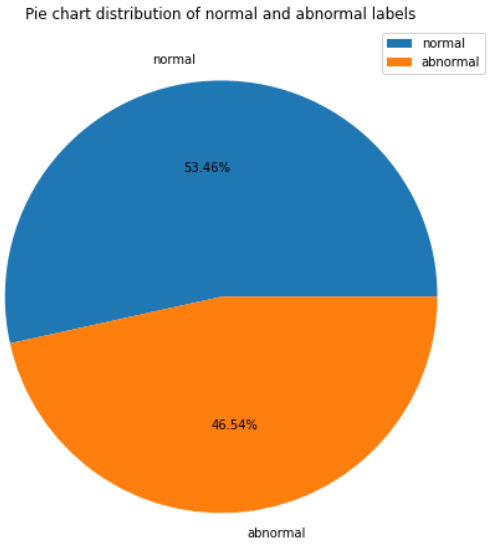


Fig 1: Pie Chart Distribution for Binary Classification

- **Multi-Classification**

In multi-classification, we have 5 class tags such as Normal, Denial of service (DoS), Probe, R2L, and U2R. first, we create data frame for multi-class labels and then performed label encoding for multi-class such as 0,1,2,3,4. Pie-chart for the multi-class classification is shown in figure. As shown in the figure we have 53% normal data and 47% abnormal labels in the dataset in case of binary classification.

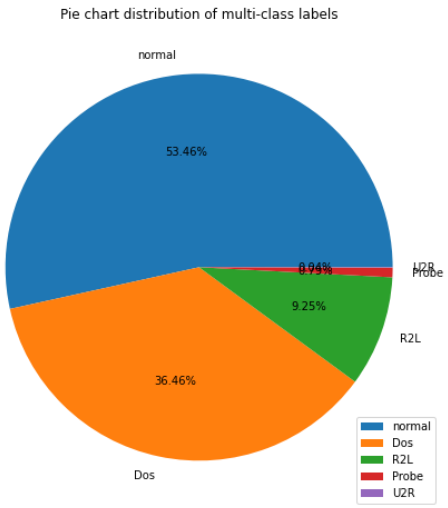


Fig 2: Pie Chart Distribution for Multi Classification

Performance Metrics:

Different system of measurement are used to measure the implementation of the proposed work such as precision, F-measure, recall and accuracy:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$Precision = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

RESULT ANALYSIS:

The research looked at how well the presented approach performed in binary and multiclassification studies using normal, Dos, R2L, U2R, and probe. First, we apply one hot encoding on our dataset after that we performed data augmentation and then performed data normalization. Then we used ADASYN algorithm for data augmentation.

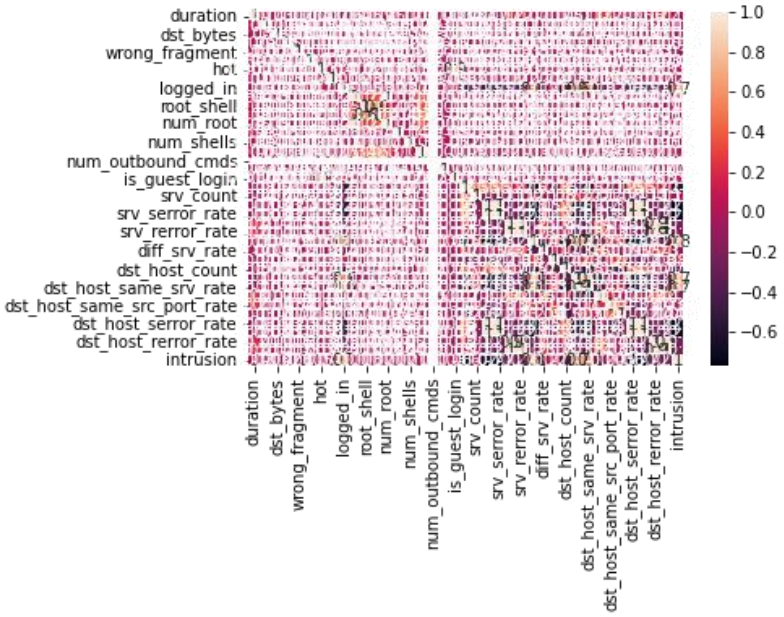


Fig 3: Pearson Correlation Matrix

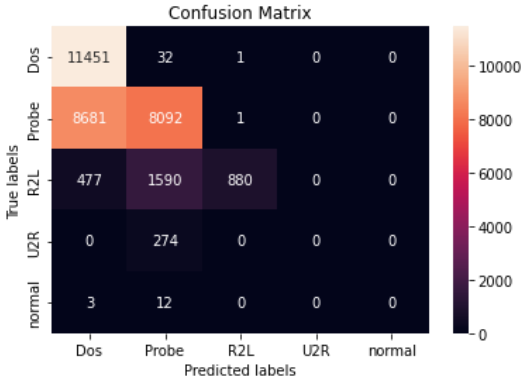


Fig 4: Confusion Matrix of Multi Classification

First, we apply LSTM on the binary classified data and Multi classified data. The accuracy of LSTM on multi classification labels is high as compared to binary classification. Then we apply BiLSTM on both binary and multi classification. BiLSTM also outperformed in case of Multi classification with the accuracy of 97.4%

	Binary Classification	Multi Classification
LSTM	90%	94%
BiLSTM	96.8%	97.4%

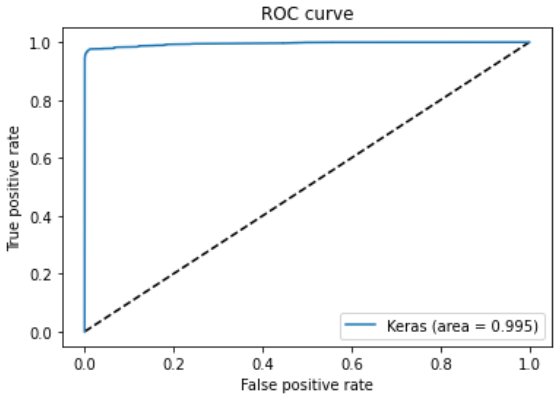
Table 1: Accuracies of Binary & Multi Classification

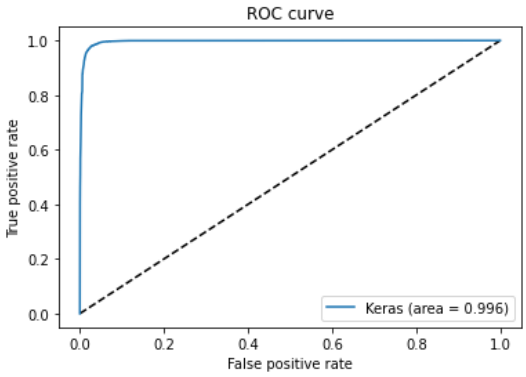
For the multi classification we check accuracy against each class label as shown in the given table. In case of Normal class accuracy of the classifier is 96%, for DoS class 98%, and for Probe class 97%, respectively.

The result shows that both the techniques, LSTM and BiLSTM outperformed in Multi classification labels. The ROC curves of each multi class type are given.

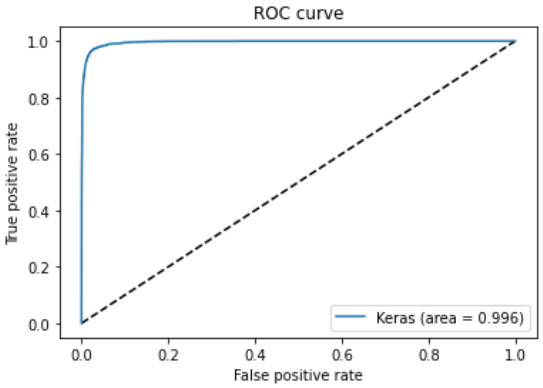
TYPE	ACCURACY
Normal	96%
DoS	98%
Probe	97%
R2L	82%
U2R	80%

Table 2: Accuracies of different labels in Multi Classification

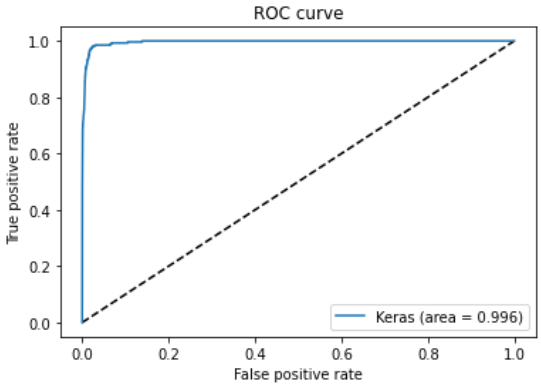




Roc Curve for Normal Type

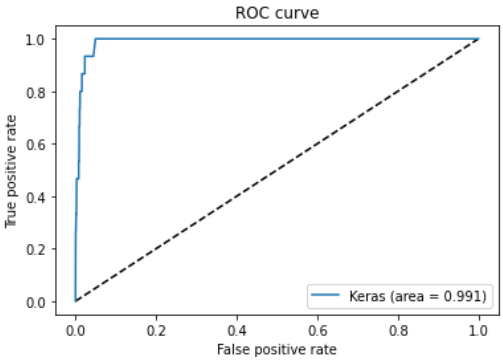


Roc Curve for DoS Type



Roc Curve for Probe Type

Roc Curve for R2L Type



Roc Curve for U2R Type