International Journal for Modern Trends in Science and Technology, 8(07): 98-101, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0807016
Available online at: http://www.ijmtst.com/vol8issue07.html

Intrusion Detection System using Multi-Layer Perceptron with Grid Search CV

Ankit Kumar[1] | Dr. Deepak Sharma[2]

[1]Student, Department of Computer Engineering, K J Somaiya College of Engineering, Mumbai, Maharashtra, India
[2]Professor, Department of Computer Engineering, K J Somaiya College of Engineering, Mumbai, Maharashtra, India
Email ID: ankit22@somaiya.edu

To Cite this Article
Ankit Kumar and Dr. Deepak Sharma. Intrusion Detection System using Multi-Layer Perceptron with Grid Search CV. International Journal for Modern Trends in Science and Technology 2022, 8(07), pp. 98-101. https://doi.org/10.46501/IJMTST0807016

Article Info
Received: 17 June 2022; Accepted: 16 July 2022; Published: 20 July 2022.

ABSTRACT

In today's life all the organization over the globe are facing a major issue with security's most common challenging issue of intrusion into their network. This intrusion in the network may lead to security concerns hampering the organizations integrity, confidentiality and availability. To solve this issue there are multiple tools in the market which detects the intrusion in a networkby surveillance of network activities and block the unusual activity detected. These tools and technologies monitor the network for sudden change in activity or behavior and processing them further for analyzing if unusual activity is noticed and inform the administrator about the change in behavior of network.Most of these tool uses the traditional machine learning method for intrusion classification into 'good' or 'bad' network.

In this paper we propose a deep learning model whose architecture compromises of Multi-Layer Perceptron used for intrusion classification and uses GridSearchCV to automate the best model selection for the problem. Using deep learning to solve the problem of intrusion detection in an organization by classification of network has numerous advantages as deep learning performs well on large datasets, unstructured data, better self-learning capabilities, cost effective and scalable. In the implementation of the proposed architecture, we have achieved an accuracy of 98.10% for binary classification and 97.62% for multi-class classification.For hyperparameter tuning as we have used GridSearchCV and used five k-fold cross validation for evaluating the best performing model.

KEYWORDS: *Intrusion detection system, deep learning, multi-layer perceptron algorithm, gridsearchcv*

1. INTRODUCTION

Over the past couple of years, we have seen a rapid growth in the field of computer networks. All the organizations who are expanding their businesses into different regional locations have started to virtualize their infrastructure solutions over the internet. Also, during this era of Covid-19 pandemic we have seen that organizations are moving their employees to work from home, instead of the traditional work from office method.Moving the infrastructure solutions to the internet has led to many security threats, vulnerabilities and attack techniques. Having such risks in an organization leads to the concern of integrity, confidentiality and availability of the resources.

To prevent such mishappening in an organizationIntrusion Detection System (IDS)plays a

very crucial role. IDS is a software application that monitors the network traffic in an organization. It is responsible for the detection of unusual network traffic activity. It inspects the behavior pattern of the users, malicious activity and tries to find any anomality and inform the system administrator if detected any. In this research paper we have proposed and implemented a deep learning method to classify the intrusions detected in a network. We have used Multi-Layer Perceptron algorithm to solve the classification problem, and used GridSearchCV as hyperparameter tuning to perform the automation for best model selection.

2. Existing Systems And Their Limitations

Reference [1] shows how author has compared their anomaly-based intrusion detection system which uses SVM with the other traditional machine learning algorithms. The findings from this research are that by not implementing feature selection on the dataset it led to biasing.

The authors in the reference [2] shows how they implemented the NIDS on UNSW-NB15 dataset by using decision tree algorithm and obtained an accuracy of 83.1%. They used label encoding as preprocessing technique. They limitations of this research shows that large number of trees make the algorithm slow and overfitting of data.

From the reference [3] we studied how author implemented KNN algorithm on the BoT-IoT dataset which consists of 64,178 records and 6 features for the intrusion classification. They used Min-Max scaler and gain ratio as the preprocessing techniques. Limitations of this research shows distance computing and feature selection. This experiment shows an accuracy of 83%.

In order to understand the performance of deep learning algorithm in the existing systems, we referred to the research [4] where the author has proposed an architecture of Convolutional Neural Networkwith LSTMon KDD-99 dataset. In the experiment author has achieved an accuracy of 99.78%. Limitations of CNN-LSTM shows with a high false alarm in detecting zero-day attacks as the algorithm was not tested with modern day attacks.

To study the working of LSTM with dimensionality reduction algorithmsuch as Principal Component Analysis and Mutual Information we referred the research paper [5] where the author proposed LSTM-PCA and LSTM-MI algorithms. It was observed that LSTM-PCA using 2 features had the best performance. The future aspects of this research which still needs to be covered as implementation of other variants of LSTM such as Peephole LSTM, Multiplicative LSTM and Weighted LSTM.

3. Block Diagram

A. Proposed Overall Architecture

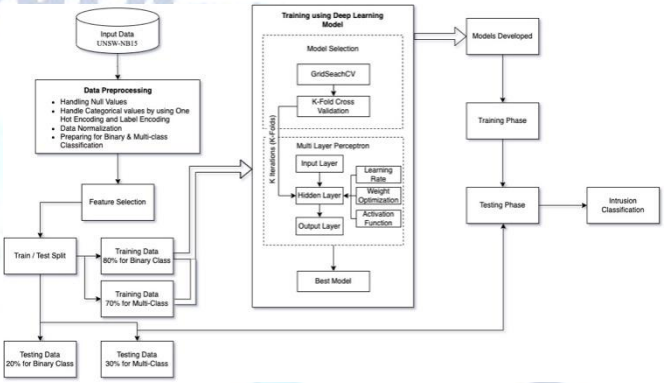

Fig. 1: Proposed Overall Architecture

B. Proposed Model Architecture

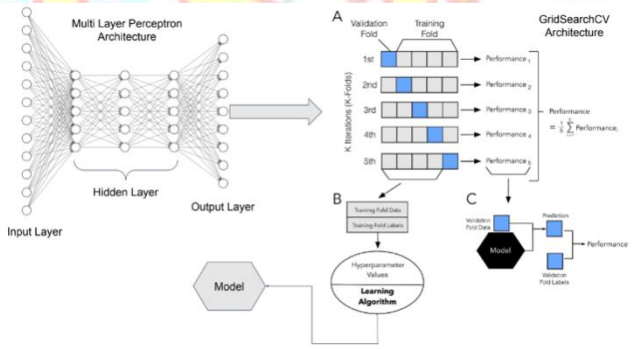

Fig. 2: Proposed Model Architecture

4. Implementation

C. Dataset

In this research experiment to implement the Multi-Layer Perceptron deep learning algorithm for intrusion detection with GridSearchCV as hyperparameter optimizationwe haveused the dataset of UNSW-NB15. [6]

The Pcap files were created at the Cyber Range Lab of the Australian Centre for CyberSecurity (ACCS) using the IXIA PerfectStorm tool.

- UNSW_NB15.csv - Original Dataset
- UNSW_NB15_features.csv - 49 features with the class label. These features are described in thedataset file.

- bin_data.csv, multi_data.csv - Processed CSV dataset file for Binary & Multi-class Classification

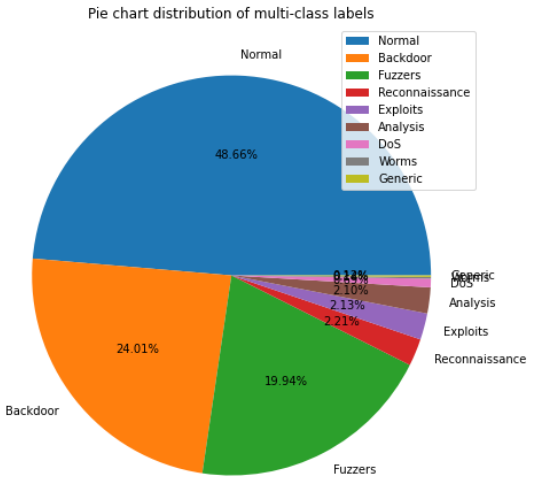

Fig. 3: Pie chart distribution of normal and abnormal labels.

D. Data Preprocessing

Following are the data preprocessing steps that are performed on the dataset:

i. Dataset had 45 attributes and 175341 rows.
ii. After dropping null values Dataset had 45 attributes and 81173 rows.
iii. The data type of attributes is converted using provided data type information from the features dataset.
iv. One-hot Encoding – Converting categorical values into numerical values.
v. Data Normalization–Using Min-Max Scaler to normalize the data in the range of 0 to 1.
vi. Preparing for Binary & Multi-Class Classification – Using LabelEncoder() to encode the 'label' (0,1) for binary classification and 'attack_cat' as (0,1,2,3,4,5,6,7,8) for multi-class classification.
vii. Feature Selection –Using Pearson Correlation Coefficient method for feature extraction where attributes more than 0.3 correlation coefficient were selected.
viii. Splitting Train/Test data – Splitting the data into 80:20 as train:test for binary classification and 70:30 for multi-class classification.

E. Training and Evaluation of Model

During the training MLP is initialized with max iteration. We have tried with differentcombinations of iterations, random state, hidden layers, activation function, solver, alpha andlearning rate. Increasing the size of iterations, wecan get good accuracy but as the number ofiterations increases, after some point, there is a chance for over fitting. So, we haveimplemented up to 100 iterations.

To help us understand and estimate model parameters we have used hyperparameteroptimization. In our case, we used the following values of hyperparameter:

```
parameter_space = {
    'hidden_layer_sizes': [(50,50,50), (50,100,50), (100,)],
    'activation': ['tanh', 'relu'],
    'solver': ['sgd', 'adam'],
    'alpha': [0.0001, 0.05],
    'learning_rate': ['constant','adaptive'],
}
```

Fig. 4: Hyperparameter Tuning

In order to evaluate our the model we have used the procedure of k-fold cross validation. In thisprocedure a single parameter called k that refers to the number of groups that a given data sampleis to be split into. When a specific value for k is chosen, it may be used in place of k in the referenceto the model, such as k=10 becoming 10-fold cross-validation. Here in our experiment we have
used k as 5 with GridSearchCV.

```
clf = GridSearchCV(mlp_multi, parameter_space, n_jobs=-1, cv=5,verbose=2)
clf.fit(X_train, y_train)
print('Best parameters found:\n', clf.best_params_)
```

Fig. 5: Best Model Evaluation

5. RESULTS

A. Binary Classification

Accuracy - 98.1
Mean Absolute Error - 0.02
Mean Squared Error - 0.02
Root Mean Squared Error - 0.14
R2 Score - 89.70

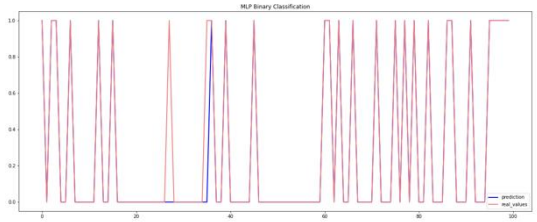

Fig. 6: Binary classification with proposed architecture

B. Multi-class Classification

Accuracy - 97.62
Mean Absolute Error - 0.06
Mean Squared Error - 0.17
Root Mean Squared Error - 0.41
R2 Score - 88.91

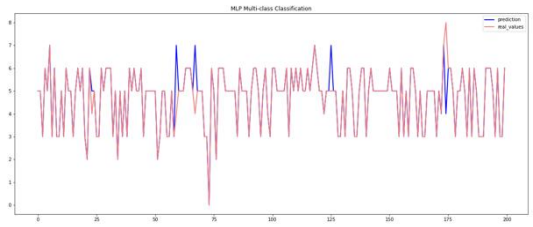

Fig. 7: Multi-class classification with proposed architecture

C. Comparison of ML with proposed DL model

Machine Learning													Deep Learning	
Algorithms	**Linear Regression**		**Logistic Regression**		**Linear SVM**		**KNN**		**Random Forest**		**Decision Tree**		**Multi-Layer Perceptron with GridSearchCV**	
Classification	Binary	Multi-class	Binary	Multi-class	Binary	Multi-class	Binary	Multi-class	Binary	Multi-class	Binary	Multi-class	Binary	Multi-class
Accuracy	97.81	0.81	97.80	97.49	97.85	97.15	97.08	97.08	97.32	97.28	98.09	97.08	98.10	97.62
Mean Absolute Error	0.02	3.77	0.02	0.06	0.02	0.06	0.02	0.06	0.01	0.07	0.02	0.07	0.02	0.08
Mean Squared Error	0.02	15.60	0.02	0.18	0.02	0.18	0.02	0.19	0.01	0.20	0.02	0.21	0.02	0.23
Root Mean Squared Error	0.15	3.95	0.15	0.42	0.15	0.42	0.13	0.44	0.12	0.45	0.14	0.45	0.14	0.48
R2 Score	88.21	3.91	88.18	87.88	88.45	87.93	90.74	86.95	92.60	86.64	89.56	86.18	89.70	85.02

Table I: Comparison of the implemented algorithms

D. Accuracy comparison w.r.t. classification

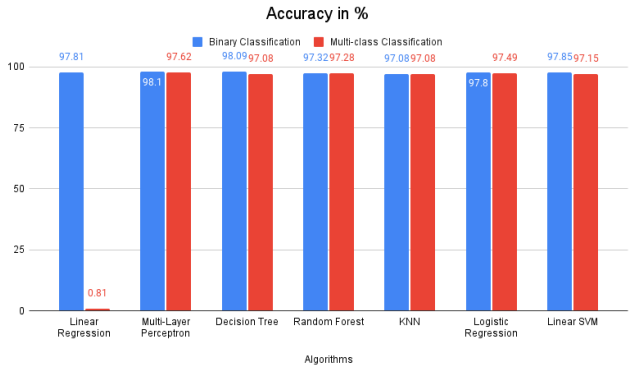

Fig. 8: Bar Graph comparison of algorithms w.r.t accuracy.

6. Conclusion

In this paper, we have proposed andimplemented a new intrusion detection system for identifying the anomalies in the network. We have observed that our proposed architecture ofMulti-Layer Perceptron with using GridSearchCV as hyperparameter optimization performs thebest with the highest accuracy of 98.1% for binary classification and 97.62% for multi-classbasedclassification on the UNSW-NB15 dataset. For feature extraction we had used Pearson CorrelationCoefficient method, so that useless data is removed.

The results can be made more accurate with adding more layers in the multi-layer perceptron andby adding a greater number of hidden neurons. To increase the testing accuracy more, i.e. to avoidmisclassification, we can increase the size of dataset or research for a better and latest dataset withmore number of attacks and input rows or generate for new dataset using the Pcap files using theIXIA PerfectStorm tool. We can even use some weight optimization techniques such as GGA(Greedy Genetic Algorithm) to optimize weight and biases in Multi-layer Perceptron. There aremany areas for improvement based on our MLP-GridSearchCV model. Therefore, how to improvethe classification accuracy and other performance metrics of the model remains to be furtherstudied.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

References

[1] K. Ghanem, F. J. Aparicio-Navarro, K. G. Kyriakopoulos, S. Lambotharan and J. A.Chambers, "Support Vector Machine for Network Intrusion and Cyber-AttackDetection," 2017 Sensor Signal Processing for Defence Conference (SSPD), London,

[2] 2017, on pp. 1-5, doi: 10.1109/SSPD.2017.8233268.

[3] D. R. Janardhana, V. Pavan Kumar, S. R. Lavanya and A. P. Manu, "Detecting Security and Privacy Attacks in IoT Network using Deep Learning Algorithms," 2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), 2021, pp. 35-40, doi: 10.1109/DISCOVER52564.2021.9663586.

[4] S. S. Swarna Sugi and S. R. Ratna, "Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020, pp. 1164-1167, doi: 10.1109/ICISS49785.2020.9315900.

[5] Kottapalle, Prasanna. (2020). A CNN-LSTM Model for Intrusion Detection System from High Dimensional Data. Journal of Information and Computational Science. 10. 1362-1370.

[6] Laghrissi, F., Douzi, S., Douzi, K. et al. Intrusion detection systems using long short-term memory (LSTM). J Big Data 8, 65 (2021). https://doi.org/10.1186/s40537-021-00448-4

[7] https://research.unsw.edu.au/projects/unsw-nb15-dataset