

Network Intrusion Detection System Using Machine Learning

Yashika Mahesh Kukreja¹ and Dr. Kiran Tikar²

¹Student, Master of Computer Application

²Assistant Professor, Master of Computer Application

Sadhu Vaswani Institute of Management Studies for Girls, Pune

Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract: Now- a-days , almost every organization depends on computer networks to store information, communication and for many more things. Because of which the chances of cyberattacks are increasing, so for this protecting network from cyberattacks has become very important. Attackers continuously develop new techniques to interrupt network services, steal or access information without any permission. In traditional intrusion detection system, it can detect only known attacks, it cannot perform well or detect if a new or modified attack occurs.

To overcome this problem, Network Intrusion Detection System(NIDS) using Machine Learning was developed. The dataset used here is UNSW-NB15 to train and test the system. The network traffic is divided into ten categories. These categories are Analysis, Backdoor, DoS, Exploits, Fuzzers, Generic, Normal, Reconnaissance, Shellcode and Worms.

Four different machine learning algorithms were tested. These algorithms are Random Forest, Decision Tree, Logistic Regression and XGBoost. Each model was evaluated using accuracy, precision, recall and F1-score. Among the four algorithms XGBoost performed best with an accuracy of 87.60%. Random Forest had an accuracy of 87.50%. Decision Tree had an accuracy 86.36% and for Logistic Regression had an accuracy of 81.25%. Feature analysis showed `ct_dst_sport_ltm` and `sttl` were the most important features for XGBoost model.

Keywords: Network Intrusion Detection System, Machine Learning, Cyber security, Network security, Multiclass Classification, UNSW-NB15, XGBoost.

I. INTRODUCTION

Almost every organization uses networks for communication, to store data, provide services or perform business activities, for this the internet and computer networks have become the important part. These networks provide many benefits, but they also create opportunities for attackers. Cyberattacks can result in unauthorized access, financial loss, interruption of networks and stolen information. Some common network attacks are Denil of Service(DoS), Exploits, Fuzzers, Reconnaissance, Backdoors, Shellcode and Worms.

A Network Intrusion Detection System (NIDS) is designed to monitor network traffic and identify activities. It acts like a security guard, for a computer network and tries to determine whether the traffic is normal or an attack. Traditional intrusion detection system uses predefined rules or patterns. For example, the system can identify the pattern which is already known, but if attackers change their techniques, it makes difficult to identify new attacks. Machine Learning provides a flexible approach, It study's the previously collected traffic, learns the pattern for different attacks and used to classify new traffic.

In this project, the UNSW-NB15 dataset is used to develop multiclass intrusion detection system, for this four machine learning models are compared: XGBoost, Random Forest, Decision Tree and Logistic Regression. The main aim is to determine which model performs best for identifying different categories of network traffic and attacks.

II. LITERATURE REVIEW

Many researches have studied the use of machine learning for network intrusion detection. The dataset UNSW-NB15 dataset was developed by Moustafa and Slay, this dataset contains normal network traffic and also different types of



modern attacks, it provides researchers with a useful dataset for testing intrusion detection techniques. Earlier KDD99 dataset was used, which was difficult to represent the modern network environment. Therefore, newer datasets like UNSW-NB15 are useful for analysing current machine learning approaches.

Different machine learning algorithms have been applied for the intrusion detection. Decision Trees are popular because their decisions are easy to understand. Random Forest improves decision tree by combining many trees. Logistic Regression is commonly used, as it is fast and easy to implement, but it may not be able to show complicated relationships between network features. XGBoost has become most popular for classification problems, it builds multiple decision tree sequentially and tries to improve the mistakes made by previous trees. It shows that ML can effectively help identify suspicious network traffic. These studies provide a strong base for developing and comparing the machine learning models for NIDS.

III. RESEARCH GAP

Existing studies have used different machine learning models but still there is a need for a simple comparison for these models. Many studies mainly focused on accuracy and give less attention to rare attacks because the dataset is imbalance, which makes some attacks harder to detect. There is also need to check precision, recall and f1-score along with accuracy for better evaluation. It is also important to identify which features that can detect attacks effectively. Therefore, this project compares different machine learning models and study the performance of different types of network attacks.

IV. METHODOLOGY

The methodology consists of following main steps : Dataset collection, Data preprocessing, Feature encoding, Label encoding, Model training, Prediction, Model evaluation.

Dataset

The UNSW-NB15 dataset is used in this project, it contains both normal and malicious network traffic and also ten traffic categories.

The model uses:

175,341 training records,

82332 testing records,

194 final features.

Data Preprocessing

The preprocessing steps are:

- Data Loading - The training and testing datasets are loaded using Python and pandas.
- Feature and Target Separation – The input network features are separated from the target attack category.
- One-Hot Encoding – Categorical features are converted into numerical binary columns (0/1).
- Label Encoding – The attack categories are converted into numerical labels:

Analysis =0

Backdoor =1

DoS= 2

Exploits=3

Fuzzers=4

Generic=5

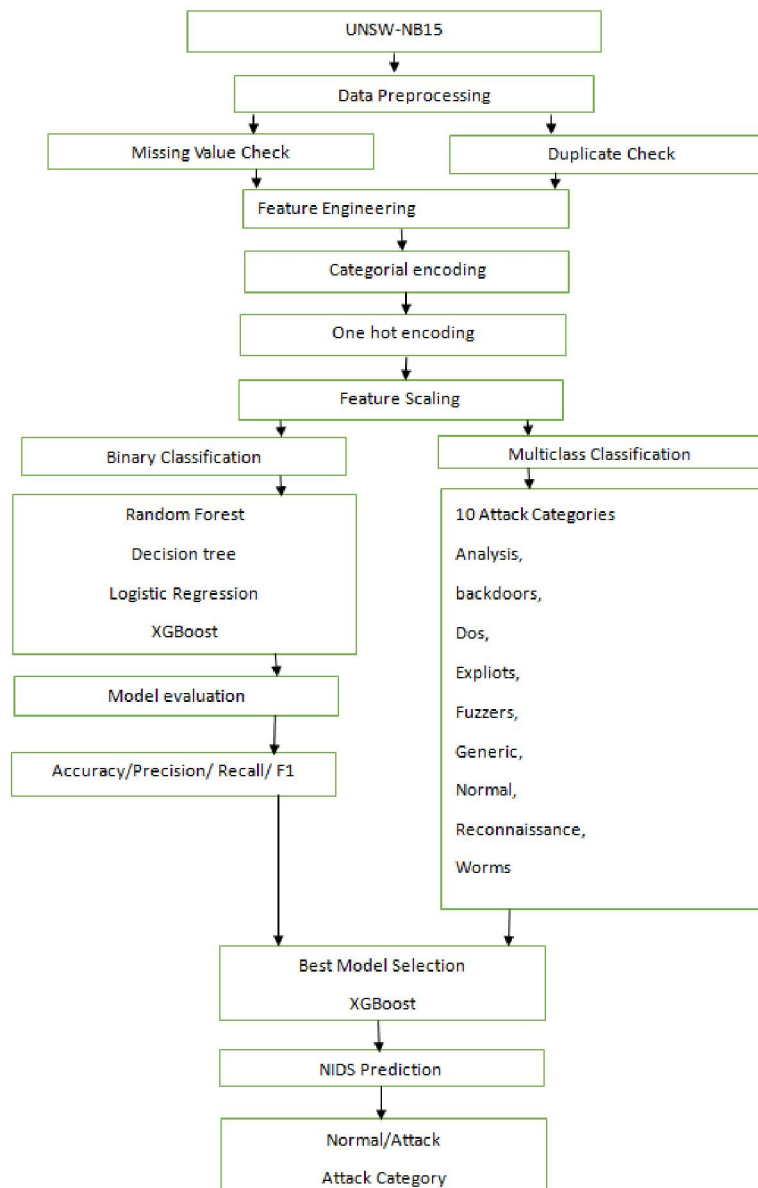
Normal=6

Reconnaissance=7

Shellcode=8



Worms=9



Machine Learning Models

Four different machine learning algorithms are selected for this research:

Random Forest – Random Forest is a machine learning algorithm that uses many decision trees to make final prediction, instead of depending on one tree it combines the results of multiple trees. It can handle a large number of network features and also complex data. This makes the model reduce wrong prediction.

Decision Tree – Decision tree is a algorithm that makes decision step by step. It can classify traffic as normal or different types of attack.



Logistic Regression – Logistic Regression is a simple machine learning algorithm used for classification. It checks the input features and calculates probability. It is easy to use and requires less computing power.

XGBoost – XGBoost is powerful machine learning algorithm used for classification. It creates many decision trees one after another, the new tree corrects the mistakes of previous trees. This helps it find complex patterns in network traffic. XGBoost achieved the highest accuracy, so it is the best performing model in NIDS project.

Algorithm

1. Start
2. Load UNSW-NB15 dataset
3. Clean the data and prepare it
4. Convert text data into numbers
5. Train four machine learning models
6. Check model performance
7. Compare all models
8. Select best model (XGBoost)
9. Show whether the traffic is normal or attack
10. Show the category of attack identified.

Model Evaluation

The models are evaluated using:

Accuracy

Accuracy shows the overall percentage that model classified correctly

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN})$$

For multiclass classification:

$$\text{Accuracy} = (\text{Number of Correct Predictions}) / (\text{Total Number of Predictions})$$

Precision

Precision shows how many of the traffic records predicted as attacks were actually attacks. Higher Precision means there are less false alarms.

$$\text{Precision} = \text{Precision} = \text{TP} / (\text{TP} + \text{FP})$$

Recall

Recall tells how many actual attacks were successfully detected. Higher recall is important in intrusion detection.

$$\text{Recall} = \text{Recall} = \text{TP} / (\text{TP} + \text{FN})$$

F1-Score

F1-score helps us see how good the NIDS is spotting attacks while keeping alarms low.

$$\text{F1-Score} = 2 \times (\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall})$$

V. FINDING AND RESULTS

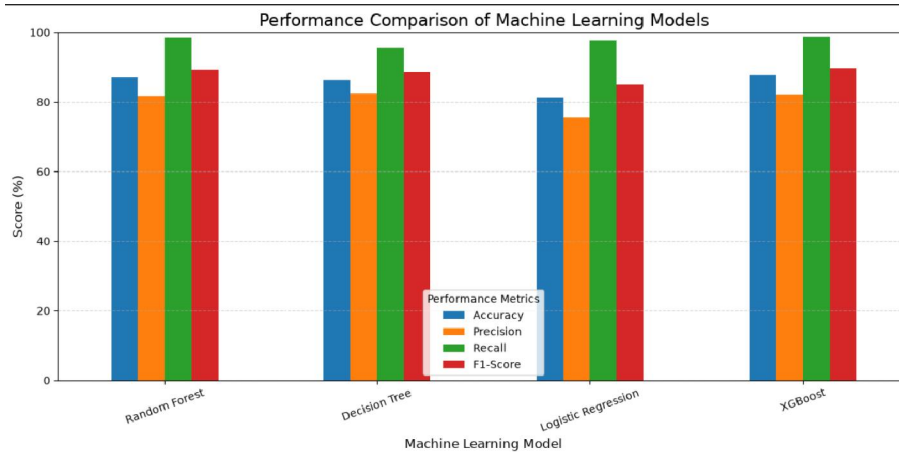
Model Performance

After training and testing the four models, the output/results were:



	Model	Accuracy	Precision	Recall	F1-Score
0	Random Forest	87.05	81.74	98.49	89.33
1	Decision Tree	86.36	82.38	95.68	88.53
2	Logistic Regression	81.25	75.49	97.66	85.15
3	XGBoost	87.60	82.26	98.77	89.76

The result shows, XGBoost has the highest Accuracy and F1-score among four evaluated models.



Macro-Average Results

```

===== MACRO METRICS COMPARISON =====

Random Forest
Macro Precision: 0.5332
Macro Recall   : 0.4828
Macro F1       : 0.4585

Decision Tree
Macro Precision: 0.4990
Macro Recall   : 0.5270
Macro F1       : 0.4988

Logistic Regression
Macro Precision: 0.3769
Macro Recall   : 0.3849
Macro F1       : 0.3354

XGBoost
Macro Precision: 0.5333
Macro Recall   : 0.5487
Macro F1       : 0.5045

Weighted XGBoost
Macro Precision: 0.5081
Macro Recall   : 0.6618
Macro F1       : 0.4943
  
```



XGBoost has highest macro recall and macro F1-score, among the four models. This indicates XGBoost provides better performance across different classes.

Feature Importance

Feature	Importance
ct_dst_sport_ltm	0.277199
sttl	0.162092
service_dns	0.045495
proto_unas	0.044111
state_FIN	0.040086

VI. MAJOR FINDINGS

The result for this project shows that machine learning can be used to classify different types of network traffic. Among the four models tested, XGBoost gave the best performance achieving the highest accuracy of 87.60% and the highest F1-score of 89.76%. Random Forest was the second best model and it also provides strong classification performance for classifying network traffic.

The study also found that the dataset contains significant class imbalance, where rare attacks such as worms have very few training samples, which is difficult to classify and also difficult to identify the models correctly. ct_dst_sport_ltm was the most important feature in XGBoost model. Macro-average precision, recall and F1-score provides additional information about the performance across different attack classes especially minority classes.

The finding shows that XGBoost is a suitable model for this project, but improving the detection of rare attacks remains an important part for future work.

VII. LIMITATION

The project has some limitations like, the system was tested using UNSW-NB15 dataset, if real network data is used the results may be different. The dataset has an unequal number of records for different attacks, which makes rare attacks difficult to detect. Attack such as worms have very few samples, so model is not able to learn them properly. The system was tested on existing data and was not connected to real-time network. Some wrong predictions and false alarms may occur during attack detection. The project does not block or remove detected attacks automatically.

VIII. CONCLUSION

This research developed and evaluated a Network Intrusion Detection System using Machine Learning with UNSW-NB15 dataset. The main purpose was to determine whether machine learning can do classification of network traffic into ten categories.

Tested four machine learning models XGBoost gave best performance reaching the accuracy of 87.60% and F1-score of 89.76%. Random Forest also gave good results while Logistic Regression gave the lowest accuracy. The most important features are ct_dst_sport_ltm and sttl for making predictions. This helps to understand the network feature and identify different types of traffic.

The research also highlighted an important problem like class imbalance as some attack categories contain large number of records, but rare attacks like Worms contain very few samples, this makes it difficult for a model to learn rare attack patterns.

In future this project can also be developed into a real-time NIDS, where the network traffic is continuously monitored and suspicious activity is detected immediately. This can help identify attacks earlier and improve network security.

Overall the study shows machine learning can provide a useful foundation for building intelligent Network Intrusion Detection System, with XGBoost giving the strongest performance among models tested also capable of identifying multiple types of cyberattacks.



REFERENCES

1. Moustafa & Slay (2015) UNSW-NB15: A comprehensive dataset for Network Intrusion Detection System.
2. Moustafa & Slay (2021): Intrusion Detection in Internet of Things Using Supervised Machine Learning on UNSW-NB15.
3. Zonghi, M (2024) Building an Intrusion Detection System on UNSW-NB15: Reducing the Margin of Error to Deal with Data Overlap and Imbalance,
4. Olorunfemi, O. (2024) Intrusion Detection: A Comparison Study of Machine Learning Models Using Unbalanced Dataset.
5. Neeli, V.S.R.P.K, & Nallagattla, V.R.G.(2025) Leveraging Machine Learning Techniques for Intrusion Detection System Using UNSW-NB15 Dataset.
6. Mohale, V.Z & Obangbuwa, I.C (2025) evaluating Machine Learning-Based Intrusion Detection System with Explainable AI.
7. Gabriski, D. (2026) Random Forest-Based Network Intrusion Detection with Feature Selection and Class Balancing on UNSW-NB15 Traffic.
8. Algarni, S. (2026) Supervised Intrusion Detection on UNSW-NB15: A Comparative Study of Classical Machine Learning Models.

