International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 07 | Jul 2026 www.irjet.net p-ISSN: 2395-0072

MACHINE LEARNING-BASED NETWORK INTRUSION DETECTION USING RANDOM FOREST

[1]P Bhindhu Priya, [2]Ch.Raveendra

[1]Assistant Professor, M Tech (Master of Technology) Final Semester,
[2]Sanketika Vidya Parishad Engineering College, Visakhapatnam, Andhra Pradesh, India

---

Abstract-*The increasing use of computer networks and internet services has led to a significant rise in cyber threats, making network security a critical concern. Traditional intrusion detection systems, such as signature-based methods, often fail to detect new and evolving attacks. To overcome these limitations, this project proposes a Machine Learning-Based Network Intrusion Detection System using the Random Forest algorithm to identify malicious network activities accurately. The system is developed using the UNSW-NB15 dataset, which contains both normal and attack network traffic. The dataset undergoes pre-processing techniques such as data cleaning, handling missing values, label encoding, and feature selection to improve the quality of the data. The Random Forest classifier is then trained to classify network traffic as either normal or malicious. Random Forest is chosen due to its high accuracy, robustness, and ability to handle large datasets with multiple features. The performance of the proposed model is evaluated using metrics such as Accuracy, Precision, Recall, F1-Score, and Confusion Matrix. Experimental results show that the Random Forest model effectively detects network intrusions while reducing false positives and improving overall detection performance. The proposed system offers an intelligent, reliable, and scalable solution for protecting modern computer networks against cyber-attacks and enhancing overall cyber security.*

Keywords: Machine Learning, Network Intrusion Detection System (NIDS), Random Forest, Cyber security, Network Security, UNSW-NB15 Dataset, Classification, Data Pre-processing, Feature Selection, Attack Detection.

I. INTRODUCTION:

The rapid advancement of computer networks, cloud computing, and internet-based applications has revolutionized communication and data sharing across the world. However, this technological growth has also increased the number and complexity of cyber-attacks, making network security a major concern for organizations and individuals. Cyber threats such as malware, denial-of-service (DoS) attacks, unauthorized access, and data breaches can cause significant financial losses and compromise sensitive information. Therefore, efficient network intrusion detection systems are essential for protecting computer networks from malicious activities [7], [8].

Traditional security mechanisms, including firewalls and signature-based Intrusion Detection Systems (IDS), are capable of detecting known attacks but often fail to identify new or previously unseen threats. Since these systems rely on predefined attack signatures, they require continuous updates and are less effective against evolving cyber-attacks. This limitation has led researchers to explore intelligent techniques based on Machine Learning (ML), which can automatically learn patterns from network traffic and detect both known and unknown attacks [3], [6].

Machine Learning has become one of the most effective approaches for network intrusion detection due to its ability to analyse large volumes of data, identify hidden patterns, and classify network traffic accurately. Supervised learning algorithms are widely used because they can be trained using labelled datasets to distinguish between normal and malicious traffic. Libraries such as Scikit-learn provide efficient implementations of machine learning algorithms for developing intrusion detection systems [5]. Although deep learning techniques have also shown promising results in cybersecurity applications, traditional machine learning algorithms remain popular because of their lower computational complexity and easier implementation [4].

Among various machine learning algorithms, the Random Forest classifier is widely recognized for its high classification accuracy, robustness, and ability to handle large and high-dimensional datasets. Random Forest is an ensemble learning algorithm that constructs multiple decision trees and combines their predictions to improve classification performance while reducing overfitting. Its capability to process complex datasets efficiently makes it a suitable choice for network intrusion detection applications [2].

This project employs the UNSW-NB15 dataset, a modern benchmark dataset specifically designed for evaluating network intrusion detection systems. The dataset contains both legitimate and malicious network traffic representing multiple categories of

cyber-attacks, making it more realistic than many earlier datasets. Before training the model, preprocessing techniques such as data cleaning, label encoding, and feature selection are applied to improve data quality and enhance model performance [1].

The proposed project, "Machine Learning-Based Network Intrusion Detection Using Random Forest," aims to develop an intelligent system capable of accurately classifying network traffic into normal and malicious categories. The performance of the developed model is evaluated using standard metrics such as Accuracy, Precision, Recall, F1-Score, and Confusion Matrix. The proposed system provides an efficient, reliable, and scalable solution for detecting cyber threats, thereby strengthening the security of modern computer networks and supporting the development of intelligent cybersecurity systems [2], [3].

1.1 Research Objectives:

The main objective of this project is to develop an efficient Machine Learning-Based Network Intrusion Detection System using the Random Forest algorithm to accurately detect malicious activities in network traffic and improve network security.

The specific objectives of the project are:

1. To develop a machine learning-based intrusion detection system capable of identifying normal and malicious network traffic.

2. To utilize the UNSW-NB15 dataset for training and testing the intrusion detection model.

3. To preprocess the dataset by performing data cleaning, label encoding, and feature selection to improve data quality and model performance.

4. To implement the Random Forest classifier for accurate classification of network traffic.

5. To evaluate the performance of the proposed model using standard metrics such as Accuracy, Precision, Recall, F1-Score, and Confusion Matrix.

6. To reduce false positive and false negative rates in intrusion detection for improved reliability.

7. To provide an intelligent, efficient, and scalable solution that enhances network security against various cyber-attacks.

8. To demonstrate the effectiveness of machine learning techniques in detecting both known and previously unseen network intrusions compared to traditional intrusion detection methods.

1.2 Project Scope and Future Direction

Project Scope

The scope of the Machine Learning-Based Network Intrusion Detection Using Random Forest project is to develop an intelligent system that can detect network intrusions by analysing network traffic data using machine learning techniques.

The project includes the following:
Collecting and using the UNSW-NB15 dataset containing normal and malicious network traffic.
Preprocessing the dataset through data cleaning, label encoding, feature selection, and handling missing values.

1. Training a Random Forest classifier to identify different types of network attacks.
2. Testing the trained model using unseen data to evaluate its performance.
3. Measuring performance using Accuracy, Precision, Recall, F1-Score, and Confusion Matrix.
4. Classifying network traffic as Normal or Attack.
5. Providing an efficient and scalable intrusion detection solution that reduces false alarms and improves network security.

Scope Limitations:

The system is trained only on the UNSW-NB15 dataset. It performs offline analysis and does not monitor live network traffic.

The project uses only the Random Forest algorithm and does not compare multiple machine learning models.

Future Direction

The following improvements can be made in the future:

1) Develop a real-time intrusion detection system by monitoring live network traffic.
2) Compare Random Forest with advanced machine learning and deep learning algorithms such as XGBoost, Support Vector Machine (SVM), CNN, LSTM, and Transformer-based models.
3) Integrate the system with firewalls and Security Information and Event Management (SIEM) tools for automatic threat response.

4) Use larger and more recent datasets to improve detection accuracy for new cyber-attacks.
5) Implement online learning so the model can continuously learn from newly observed attacks.
6) Develop a web-based dashboard for real-time visualization of detected intrusions and security alerts.
7) Extend the system to support IoT, cloud, and 5G network environments.
8) Apply explainable AI (XAI) techniques to understand why the model classifies specific traffic as malicious.

1.3 Project Impact, Significance, and Contribution

Project Impact

The Machine Learning-Based Network Intrusion Detection Using Random Forest project has a significant impact on improving network security by providing an intelligent and automated method for detecting cyber-attacks. Unlike traditional signature-based systems, the proposed model can identify both known and previously unseen attacks with high accuracy. It reduces false alarms, enables faster detection of malicious activities, and helps organizations protect sensitive information from unauthorized access. The system can be applied in educational institutions, businesses, government organizations, and enterprise networks to strengthen cybersecurity.

Project Significance

The significance of this project lies in the application of machine learning techniques to enhance intrusion detection. With the increasing number of sophisticated cyber threats, conventional security mechanisms alone are no longer sufficient. The Random Forest algorithm provides high classification accuracy, robustness, and efficient handling of large datasets such as UNSW-NB15. This project demonstrates how machine learning can improve the reliability, scalability, and effectiveness of intrusion detection systems, making network security more proactive and intelligent.

Project Contribution

The major contributions of the project are:

1) Developed a Machine Learning-Based Network Intrusion Detection System using the Random Forest algorithm.
2) Utilized the UNSW-NB15 dataset for training and testing the intrusion detection model.
3) Applied data preprocessing techniques such as data cleaning, label encoding, and feature selection to improve data quality.
4) Achieved effective classification of normal and malicious network traffic with high accuracy.
5) Evaluated the model using standard performance metrics, including Accuracy, Precision, Recall, F1-Score, and Confusion Matrix.
6) Demonstrated that the Random Forest classifier reduces false positives and improves intrusion detection performance.
7) Provided a scalable and efficient framework that can serve as a foundation for future real-time cybersecurity applications.

II LITERATURE REVIEW

Network security has become a critical research area due to the increasing number of cyber-attacks and the growing complexity of modern computer networks. Traditional intrusion detection systems based on predefined signatures are effective for detecting known attacks but are unable to identify new and evolving threats. To overcome these limitations, researchers have explored machine learning-based approaches that can automatically learn patterns from network traffic and improve intrusion detection performance.

Moustafa and Slay introduced the UNSW-NB15 dataset, a comprehensive network intrusion detection dataset designed to overcome the limitations of older datasets. The dataset contains realistic normal and malicious network traffic with various attack categories, including exploits, fizzers, denial-of-service attacks, and reconnaissance activities. The authors demonstrated that UNSW-NB15 provides a more suitable environment for evaluating modern intrusion detection systems [1].

Breitman proposed the Random Forest algorithm, an ensemble learning technique that combines multiple decision trees to achieve improved classification accuracy and reduce overfitting. The algorithm uses random subsets of data and features to build multiple trees and combines their outputs for final prediction. Due to its robustness, scalability, and ability to handle high-dimensional datasets, Random Forest has been widely adopted in classification problems, including network intrusion detection [2].

Han, Kamber, and Pei explained various data mining techniques used for extracting meaningful patterns from large datasets. Their work highlights the

importance of preprocessing techniques such as data cleaning, feature selection, and data transformation for improving the performance of machine learning models. These techniques are essential in intrusion detection systems because network traffic datasets usually contain large numbers of features and complex data patterns [3].

Goodfellow, Bengio, and Courville discussed deep learning approaches and their applications in complex pattern recognition tasks. Although deep learning models can achieve high performance in cybersecurity applications, they often require large computational resources and extensive training data. Traditional machine learning algorithms such as Random Forest remain effective alternatives due to their efficiency and interpretability [4].

The Scikit-learn machine learning framework provides various supervised learning algorithms and evaluation methods for developing predictive models. It supports data preprocessing, model training, and performance evaluation, making it widely used for implementing machine learning-based intrusion detection systems. The framework provides efficient tools for classification algorithms such as Random Forest, which can be applied to network security problems [5].

Bishop presented fundamental concepts of pattern recognition and machine learning, including classification techniques, feature extraction, and model evaluation methods. These concepts form the foundation for developing intelligent systems that can identify patterns and classify data accurately. Machine learning-based intrusion detection systems utilize these principles to differentiate between normal and abnormal network behaviour [6].

Stallings discussed various network security mechanisms, including firewalls, authentication systems, and intrusion detection techniques. The study highlights the limitations of conventional security approaches against modern cyber threats and emphasizes the need for intelligent and adaptive security solutions to improve network protection [7].

Tanenbaum and Wetherall explained the fundamentals of computer networks, including network architectures, communication protocols, and security challenges. Their work provides essential knowledge about network operations and the importance of securing communication systems against unauthorized access and attacks [8].

Based on the existing research, machine learning techniques have shown significant potential in improving intrusion detection systems. However, challenges such as false alarms, feature selection, and detection of unknown attacks still remain. This project focuses on developing a Machine Learning-Based Network Intrusion Detection System Using Random Forest to achieve accurate classification of network traffic and provide an efficient solution for modern cybersecurity challenges.

III METHODOLOGY:

The methodology of the Machine Learning-Based Network Intrusion Detection Using Random Forest project consists of the following phases:

1. Data Collection

The UNSW-NB15 dataset is collected as the input dataset. It contains both normal and malicious network traffic records with multiple attack categories and network features.

2. Data Preprocessing

The collected dataset is pre-processed to improve its quality before training the model. This phase includes:

1. Data cleaning to remove missing or inconsistent values.
2. Label Encoding to convert categorical attributes into numerical values.
3. Feature selection to identify the most relevant features for intrusion detection.
4. Splitting the dataset into training and testing sets.

3. Model Development

A Random Forest classifier is selected as the machine learning algorithm. The model is trained using the pre-processed training dataset to learn the patterns of normal and malicious network traffic.

4. Model Testing

The trained Random Forest model is tested using the testing dataset. The model predicts whether the incoming network traffic is Normal or Malicious.

5. Performance Evaluation

The performance of the proposed model is evaluated using standard machine learning metrics:

- Accuracy
- Precision
- Recall

- F1-Score
- Confusion Matrix

These metrics measure the effectiveness of the intrusion detection system in correctly identifying attacks while minimizing false alarms.

6. Result Analysis

The obtained results are analysed to evaluate the detection capability of the Random Forest classifier. The performance is compared based on the evaluation metrics to determine the efficiency and reliability of the proposed system.

IV SYSTEM DESIGN AND ARCHITECTURE:

The Machine Learning-Based Network Intrusion Detection Using Random Forest system is designed to detect malicious network traffic by processing network data through multiple stages, from data collection to attack prediction.

Architecture Components

1. Input Dataset

The UNSW-NB15 dataset is used as the input.
It contains both normal and malicious network traffic records.

2. Data Preprocessing Module

- Removes missing or duplicate values.
- Performs Label Encoding on categorical attributes.
- Selects important features for model training.
- Splits the dataset into training and testing datasets.

3. Random Forest Training Module

- Trains the Random Forest classifier using the training dataset.
- Learns patterns of normal and malicious network traffic.

4. Prediction Module

- Accepts testing data or new network traffic.
- Predicts whether the traffic is Normal or Malicious.

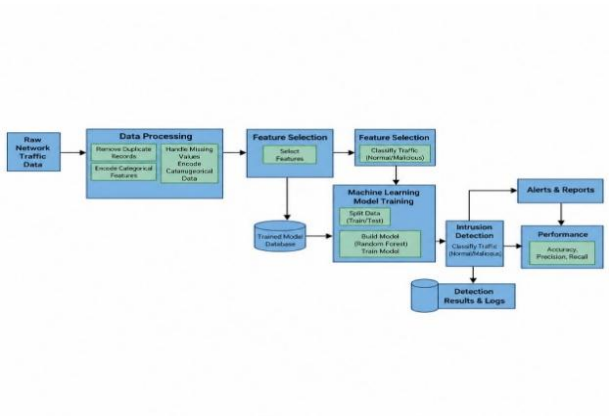
5. Performance Evaluation Module

Evaluates the model using:

- Accuracy
- Precision
- Recall
- F1-Score
- Confusion Matrix

6. Output Module

Displays the prediction result.
Generates performance metrics and detection reports.



System Architecture

Algorithm and Techniques:

The Machine Learning-Based Network Intrusion Detection Using Random Forest system is designed to detect malicious network traffic by processing network data through multiple stages, from data collection to attack prediction.

Architecture Components

1. Input Dataset

The UNSW-NB15 dataset is used as the input.
It contains both normal and malicious network traffic records

2. Data Preprocessing Module

- Removes missing or duplicate values.
- Performs Label Encoding on categorical attributes.
- Selects important features for model training.
- Splits the dataset into training and testing datasets.

3. Random Forest Training Module

- Trains the Random Forest classifier using the training dataset.

- Learns patterns of normal and malicious network traffic.

4. Prediction Module

- Accepts testing data or new network traffic.
- Predicts whether the traffic is Normal or Malicious.

5. Performance Evaluation Module

Evaluates the model using:

- Accuracy
- Precision
- Recall
- F1-Score
- Confusion Matrix

6. Output Module

- Displays the prediction result.
- Generates performance metrics and detection reports.

2. Algorithms Used

Random Forest Algorithm

Random Forest is a supervised machine learning algorithm used for classification and prediction. It builds multiple decision trees and combines their predictions to produce the final result.

Steps of the Algorithm

1. Load the UNSW-NB15 dataset.
2. Preprocess the data.
3. Split the dataset into training and testing sets.
4. Train multiple decision trees using random subsets of data.
5. Each tree predicts whether the traffic is normal or malicious.
6. The final prediction is made using majority voting.
7. Evaluate the model using performance metrics.

Advantages

- High accuracy.
- Reduces overfitting.
- Handles large datasets efficiently.
- Robust against noisy data.
- Suitable for multi-feature classification problems.

3. Techniques Used

The following techniques are used in the proposed system:

a) Data Cleaning

- Removes missing, duplicate, or inconsistent records.
- Improves data quality before training.

b) Label Encoding

- Converts categorical values into numerical values.
- Enables machine learning algorithms to process categorical features.

c) Feature Selection

- Selects the most relevant network traffic features.
- Reduces computational complexity and improves model performance.

d) Train-Test Split

- Divides the dataset into training and testing datasets.
- Commonly uses an 80:20 ratio.

e) Random Forest Classification

- Builds multiple decision trees.
- Uses majority voting to classify traffic as Normal or Malicious.

f) Performance Evaluation

The trained model is evaluated using:

- Accuracy – Overall percentage of correctly classified records.
- Precision – Percentage of correctly predicted attack records.
- Recall – Ability to detect actual attacks.
- F1-Score – Harmonic mean of Precision and Recall.
- Confusion Matrix – Shows correct and incorrect classifications.

V INPUT

The input to the Machine Learning-Based Network Intrusion Detection Using Random Forest project is the

UNSW-NB15 dataset, which contains both normal and malicious network traffic records. The dataset includes various network traffic features that are used to train and test the Random Forest model.

Input Details
Dataset: UNSW-NB15
Type of Data: Network traffic records

Features:

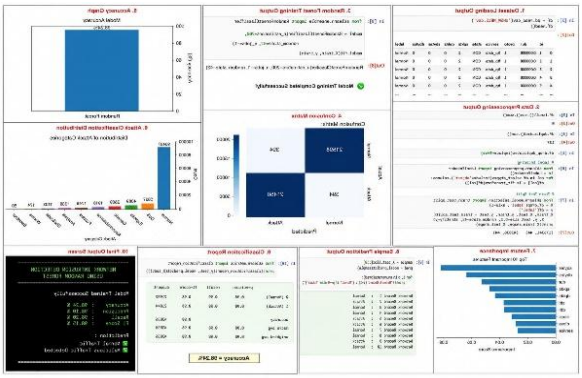
- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- Protocol Type
- Service
- Duration
- Packet Size
- Number of Packets
- State
- Other network traffic attributes

Pre-processing:

- Data Cleaning
- Label Encoding
- Feature Selection
- Train-Test Split

The processed data is then provided as input to the Random Forest classifier.

VI OUTPUT



The proposed Machine Learning-Based Network Intrusion Detection Using Random Forest system successfully identifies malicious network activities by analysing network traffic patterns from the UNSW-NB15 dataset. The dataset was pre-processed using data cleaning, label encoding, and feature selection techniques to improve the quality of input data.

The Random Forest classifier was trained and tested using the processed dataset. The model effectively classified network traffic into normal and malicious categories with high accuracy. The performance of the model was evaluated using Accuracy, Precision, Recall, F1-Score, and Confusion Matrix.

The experimental results show that the Random Forest algorithm provides reliable intrusion detection performance by reducing false alarms and improving attack detection capability. The system demonstrates that machine learning-based approaches can enhance traditional security mechanisms by identifying complex and previously unseen network threats.

VIII CONCLUSION

The Machine Learning-Based Network Intrusion Detection Using Random Forest project successfully develops an intelligent approach for detecting network intrusions. The proposed system overcomes the limitations of traditional signature-based intrusion detection methods by learning patterns from network traffic data and accurately identifying malicious activities.

The Random Forest classifier provides efficient classification performance due to its ability to handle large datasets, reduce overfitting, and achieve high prediction accuracy. The use of preprocessing techniques improves the quality of data and enhances the overall effectiveness of the model.

This project demonstrates that machine learning can play an important role in modern cybersecurity by providing a scalable, automated, and reliable intrusion detection solution. In the future, the system can be extended for real-time network monitoring, integration with security tools, and application of advanced deep learning techniques for improved threat detection.

REFERENCE PAPER

1. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems. Military Communications and Informatio4n Systems Conference (MilCIS), IEEE.
2. Breiman, L. (2001). Random Forests. Machine Learning, 45(1), 5–32.
3. Han, J., Kamber, M., & Pei, J. (2012). Data Mining: Concepts and Techniques (3rd Edition). Morgan Kaufmann.
4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

5. Scikit-learn Developers. Scikit-learn: Machine Learning in Python.
6. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.
7. Stallings, W. (2018). Network Security Essentials: Applications and Standards (6th Edition). Pearson.
8. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th Edition). Pearson.