KLE Technological University

Creating Value
Leveraging Knowledge

School of
Electronics and Communication Engineering

Minor Project Report

on

Real-Time Network Intrusion Detection System using Machine Learning

By:

1. SAMIT PATIL USN:01FE22BEC410
2. PAVAN SHIVALLI USN:01FE22BEC411
3. SARVESH K USN:01FE22BEC412
4. NITIN SAVVASE USN:01FE22BEC413
5. MAHAMADSHIRAJ B USN:01FE22BEC432

Semester: VI, 2023-2024

Under the Guidance of

Dr.Suneeta V Budihal

K.L.E SOCIETY'S
KLE Technological University,
HUBBALLI-580031
2023-2024

SCHOOL OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that project entitled **"Real-Time Network Intrusion Detection System using Machine Learning"**is a bonafide work carried out by the student team of **"Samit Patil - 01FE22BEC410 , Pavan Shivalli - 01FE22BEC411 , Sarvesh K - 01FE22BEC412 , Nitin Savvase - 01FE22BEC413 , Mahamadshiraj B - 01FE22BEC432"**. The project report has been approved as it satisfies the requirements with respect to the minor project work prescribed by the university curriculum for BE (VI Semester) in School of Electronics and Communication Engineering of KLE Technological University for the academic year 2023-2024.

Dr.Suneeta V Budihal	**Dr.Suneeta V Budihal**	**Dr.B.S.Anami**
Guide	**Head of School**	**Registrar**

External Viva:

Name of Examiners **Signature with date**

1.

2.

ACKNOWLEDGEMENT

We extend our gratitude to Dr. Ashok Shettar, Vice-Chancellor of KLE Technological University, Hubballi, and Dr. P. G. Tewari, Dean Academics of KLE Technological University, for providing us with the opportunity to conduct our research and for their unwavering support throughout the CIM Mini Project. Special thanks to Dr. Suneeta V.B., our head of school, for her leadership and support. We are also thankful to Prof. Rajeshwari K. for her invaluable help and guidance during our work. Additionally, we acknowledge the contributions of all teaching and non-teaching staff for their assistance and encouragement.

-The project team

ABSTRACT

The increasing complexity and frequency of cyber threats have highlighted the critical necessity for efficient Network Intrusion Detection Systems (NIDS) to protect computer networks. This study examines the use of various machine learning algorithms to detect intrusions, employing the UNSW-NB15 dataset, which realistically represents modern network traffic and attacks. We analyze and compare the performance of several classifiers, including Random Forest, Logistic Regression, and Support Vector Machine, in identifying malicious activities. Our evaluation is based on multiple performance metrics such as precision, recall, F1-score, and accuracy. The results show that the Random Forest classifier consistently achieves higher accuracy and reliability in detecting intrusions than the other models. This research underscores the significance of using comprehensive datasets and advanced machine learning techniques to improve the detection and prevention of network intrusions, thus contributing to the development of more robust cybersecurity measures.

Contents

List of Figures

Chapter 1

Introduction

The increasing integration of digital technologies into organizational operations has heightened the importance of securing computer networks from cyber threats. As networks become more critical to daily functions, they are increasingly vulnerable to a variety of cyber attacks, which can lead to substantial financial losses, data breaches, and operational disruptions. Intrusion Detection Systems (IDS) play a crucial role in identifying and mitigating these threats by continuously monitoring network and system activities.

The growing integration of digital technologies in organizational operations has significantly increased the need for robust network security to protect against cyber threats. As networks become integral to daily functions, they are increasingly susceptible to various cyber attacks, which can result in substantial financial losses, data breaches, and operational disruptions. Intrusion Detection Systems (IDS) are essential for identifying and mitigating these threats by continuously monitoring network and system activities.

Traditional IDS methods primarily use signature-based detection, which involves matching incoming network traffic against a database of known attack signatures. Although effective for recognized threats, these systems struggle to keep up with the ever-evolving nature of new and sophisticated cyber attacks, such as zero-day exploits and advanced persistent threats (APTs). To address these limitations, anomaly-based detection methods have been developed, which identify unusual activities by comparing them to established norms. However, these methods often suffer from high false positive rates, making it challenging to accurately distinguish between normal and malicious activities.

Recently, machine learning has emerged as a powerful tool to enhance IDS capabilities. Machine learning algorithms can analyze large volumes of network data to detect complex patterns and anomalies that traditional methods may miss. This ability allows IDS to adapt to new threats more effectively, reducing the reliance on predefined attack signatures.

This research evaluates the performance of various machine learning models for intrusion detection using the UNSW-NB15 dataset. The UNSW-NB15 dataset offers a comprehensive and realistic framework for testing IDS performance, addressing the limitations of older datasets like KDDCUP99 by incorporating modern attack vectors and a diverse range of features. By assessing different classifiers, including Random Forest, Logistic Regression, and Support Vector Machine, this study aims to identify the most effective model for real-time intrusion detection.

The objective of this research is to demonstrate how machine learning can enhance IDS effectiveness, thereby strengthening the security of modern network environments. Through a detailed analysis of the performance of various machine learning approaches, this study provides valuable insights into developing more advanced and adaptive cybersecurity solutions.

1.1 Motivation

The push to create an advanced real-time Network Intrusion Detection System (NIDS) using machine learning stems from the critical need to safeguard organizational networks against increasingly sophisticated cyber threats. Traditional security measures, while essential, often fall short in addressing the dynamic and evolving nature of contemporary cyber attacks, highlighting the necessity for more intelligent and adaptable security solutions.

1. Overcoming Traditional IDS Limitations : Traditional Intrusion Detection Systems (IDS) primarily use signature-based detection methods, which depend on known attack signatures. While these systems are effective for detecting known threats, they are not equipped to handle new or evolving attack patterns, leaving networks susceptible to zero-day exploits and advanced persistent threats. Anomaly-based detection methods attempt to fill this gap by identifying deviations from normal behavior. However, these methods can produce a high number of false positives, complicating the task of accurately identifying genuine threats and potentially overwhelming security analysts.

2. Harnessing Machine Learning for Improved Detection : Machine learning offers a promising solution to these challenges by enabling IDS to learn from historical data and adapt to new and emerging threats. Machine learning models can analyze large volumes of network traffic data to detect subtle patterns and anomalies that may signify malicious activity. This capability improves the IDS's ability to identify both known and unknown threats, offering a substantial enhancement over traditional detection methods.

3. Enhancing Detection Speed and Accuracy : The capacity of machine learning models to analyze large datasets in real-time significantly improves the speed and accuracy of threat detection. This rapid detection and response capability is vital for minimizing the impact of cyber attacks. By automating the detection process and reducing the need for manual intervention, machine learning-driven IDS can offer more consistent and reliable security monitoring.

4. Adapting to Modern Network Complexities : Modern network environments feature diverse traffic patterns and numerous connected devices, creating complex challenges for intrusion detection. The UNSW-NB15 dataset, used in this study, reflects this complexity, offering a realistic benchmark for evaluating IDS performance. By developing and testing machine learning models with this dataset, our goal is to create an IDS that is effective in today's network environments and capable of defending against a wide range of threats.

5. Strengthening Cybersecurity Posture : The ultimate aim of this research is to contribute to the development of advanced and effective cybersecurity tools. By utilizing machine learning, we seek to improve the detection capabilities of IDS, offering organizations robust tools to safeguard their networks. This research aspires to promote future advancements in network security, ensuring that organizations are better equipped to defend against the ever-evolving landscape of cyber threats.

1.2 Objectives

The main goal of this research is to assess the effectiveness of different machine learning models in detecting network intrusions using the UNSW-NB15 dataset. This evaluation aims to improve the understanding and application of machine learning techniques in enhancing Network Intrusion Detection Systems (NIDS). The specific objectives of the study include:

1. Assess Machine Learning Models:

    - Implement and compare various machine learning algorithms, such as Random Forest, Logistic Regression, and Support Vector Machine, to evaluate their effectiveness in detecting intrusions.

2. Performance Evaluation:

    - Assess the performance of each model using metrics such as precision, recall, F1-score, and accuracy. This thorough evaluation will highlight the strengths and weaknesses of each method.

3. Real-World Applicability:

    - Utilize the UNSW-NB15 dataset, which provides a realistic and diverse representation of modern network traffic and attack patterns, to ensure that the findings are applicable to contemporary network environments.

4. Identify Best Practices:

    - Determine the best practices for configuring and optimizing machine learning models for intrusion detection. This includes selecting appropriate features, tuning hyperparameters, and implementing robust training and testing protocols.

5. Enhance Detection Capabilities:

    - Develop insights into how machine learning can be leveraged to improve the detection capabilities of NIDS, thereby providing more accurate and timely identification of network intrusions.

6. Reduce False Positives:

    - Aim to minimize the rate of false positives in intrusion detection, which is critical for the practical deployment of IDS in real-world scenarios. High false positive rates can lead to alert fatigue and reduced effectiveness of security operations.

7. Support Continuous Improvement:

    - Provide a foundation for continuous improvement in the field of intrusion detection by highlighting areas where further research and development can enhance the performance of machine learning-based IDS.

1.3 Literature survey

1. Intrusion Detection Systems Based on Machine Learning Algorithms (2021):

This study investigates the creation of Intrusion Detection Systems (IDS) using machine learning and deep learning algorithms. The authors introduce a taxonomy of IDS grounded in deep learning and assess the performance of various machine learning algorithms on the KDD Cup 99 dataset. The tested algorithms include Bayes Net, Random Forest, Neural Networks, and advanced deep learning methods like Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks. The evaluation uses WEKA software to determine the accuracy of these algorithms.[2]

Key Findings:

- The study suggests that deep learning techniques can significantly enhance the performance of IDS.
- The utilization of the KDD Cup 99 dataset serves as a standardized benchmark for evaluating the efficacy of various algorithms.

Limitations:

- The study does not demonstrate the performance of learning algorithms for minority attack types, which is critical for comprehensive intrusion detection.
- There is a lack of detailed analysis of the characteristics of the attacks, which could provide deeper insights into how these algorithms can be further optimized for specific types of threats.

2. IntruDtree: A Machine Learning Based Cyber Security Intrusion Detection Model (2020):

This paper presents the IntruDTree model, an innovative machine learning-driven technique for cyber security intrusion detection. The methodology entails prioritizing security features according to their significance using the IntruDTree model and then designing a tree-based intrusion detection system accordingly. The objective is to enhance detection accuracy by concentrating on the most pivotal features influencing security breaches.[1]

Key Findings:

- The IntruDTree model demonstrates the potential for enhancing intrusion detection by prioritizing important security features.
- The efficacy of the model in prioritizing and leveraging these features for constructing an IDS suggests a promising avenue for further exploration and research within the domain.

Limitations:

- The study's focus on a specific dataset limits the generalizability of its findings. Validation on other datasets is necessary to confirm the robustness of the model.
- The evaluation based solely on cybersecurity datasets does not account for real-world variability and the evolving nature of cyber threats, which could affect the model's performance in practical applications.

3. Machine Learning Approach for Anomaly-based Intrusion Detection Systems using Isolation Forest Model and SVM (2023):

The research delves into employing the Isolation Forest model and Support Vector Machine (SVM) for anomaly-based intrusion detection. Emphasizing data collection from the target environment and numerical conversion of features for compatibility with the chosen algorithms, the study explores various feature transformation techniques to enhance the accuracy of the detection models.[3]

Key Findings:

- The Isolation Forest model is effective in identifying anomalies, while SVM aids in the precise classification of these anomalies.

- The methodology prioritizes the collection and processing of real-world data, thereby augmenting the practical relevance and applicability of the models.

Limitations:

- The research underscores prevalent challenges in IDS, including a heightened false alarm rate, imbalanced datasets, and sluggish response times.
- Encrypted packets pose a significant challenge as they are not visible to the IDS, potentially allowing intruders to bypass detection.
- The IDS lacks immediate response capabilities to stop ongoing attacks, which is a critical limitation in dynamic threat environments.

4. Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches: A Review (2022):

Methodology:

The paper conducts a comprehensive survey on machine learning (ML) and deep learning (DL) strategies utilized in network intrusion detection and prevention systems. It evaluates the efficacy of different ML classification techniques using the DARPA dataset, employing algorithms such as AdaBoost, Extra Trees, Gradient Boost, Linear Regression, Multilayer Perceptron, and Random Forest. Additionally, it introduces a novel detection system through an API.[4]

Key Findings:

- Examination of Machine Learning (ML) and Deep Learning (DL) Approaches for Network Intrusion Detection and Prevention Systems.
- Evaluating the Performance of Various ML Classification Techniques on the DARPA Dataset.
- Utilization of classification algorithms to identify and classify intrusive attacks.

Limitations:

- Some ML algorithms exhibit low accuracy levels.
- Future research directions should explore DL methods or hybrid approaches for improved performance.
- Limitations of the DARPA dataset encompass its failure to adequately represent real-world network activity, absence of false-positive instances, and anomalies in attack data. Hence, there arises a necessity to substitute it with datasets such as KDDCup99 or NSL KDD.

1.4 Problem statement

The escalating prevalence of cyber threats, encompassing viruses and hackers, poses a substantial challenge for conventional security systems, which often lag behind in adapting to evolving attack techniques. This underscores the imperative for developing more sophisticated and adaptable solutions. The UNSW-NB15 dataset presents a realistic and intricate environment for assessing network intrusion detection systems (NIDS), serving as a robust foundation for evaluating diverse machine learning algorithms. This research endeavors to gauge the efficacy of various machine learning models in detecting network intrusions utilizing the UNSW-NB15 dataset, addressing limitations observed in existing datasets and augmenting the accuracy and efficiency of NIDS. Through the application of machine learning, the objective is to enhance real-time detection and response capabilities, thereby safeguarding organizational data from intricate cyber attacks.

1.5 Organization of the Report

This report comprises five chapters, each dedicated to distinct aspects of the Real-Time Network Intrusion Detection System employing Machine Learning. Here's a succinct overview of each chapter:

- Chapter 1: Introduction - This section provides an overview of the escalating cybersecurity threats, underlining the necessity for advanced intrusion detection systems. It introduces the UNSW-NB15 dataset and delineates the study's objectives, which center on assessing diverse machine learning models for detecting network intrusions.

- Chapter 2: System Design - Here, the structural framework of the intrusion detection system is outlined. This encompasses data preprocessing steps such as cleaning, encoding, and normalization, along with the partitioning of the dataset into training and testing sets. Additionally, the section discusses the selection of machine learning models utilized in the study.

- Chapter 3: Implementation Details - This section delves into the particulars of implementing the machine learning models on the preprocessed dataset. It covers the algorithms employed, the training process, and the parameters adjusted for optimal performance. Moreover, it describes the tools and programming languages utilized in the implementation.

- Chapter 4: Results and Discussion - In this segment, the performance of the various machine learning models is showcased. Metrics such as accuracy, precision, recall, and F1-score are employed to evaluate the models. The results are scrutinized and compared to underscore the strengths and weaknesses of each approach.

- Chapter 5: Conclusion and Future Scope - The concluding section summarizes the key findings of the study, emphasizing the most effective machine learning models for intrusion detection based on the UNSW-NB15 dataset. It also deliberates on potential enhancements and suggests avenues for future research, including exploring deep learning methods and hybrid approaches to augment detection capabilities.

Chapter 2

Implementation Details

2.1 Specifications and system architecture

2.1.1 Specifications

The primary objective of this system is to construct a resilient Intrusion Detection System (IDS) leveraging machine learning models capable of efficiently detecting diverse cyber attacks utilizing the UNSW-NB15 dataset. The system specifications are outlined as follows:

1. Dataset:
    - UNSW-NB15, which includes various types of network traffic and multiple attack scenarios.
2. Data Preprocessing:
    - Data cleaning, normalization, and feature selection to ensure high-quality input for the machine learning models.
3. Machine Learning Models:
    - Multiple models, such as Support Vector Machine (SVM), Decision Trees (DT), Random Forest (RF), and Neural Networks (NN), will be implemented and assessed.
4. Evaluation Metrics:
    - Performance evaluation will encompass metrics including accuracy, precision, recall, F1-score, and confusion matrix to ensure a thorough assessment.
5. Implementation Tools:
    - Python will serve as the primary programming language, leveraging libraries such as Scikit-learn, TensorFlow, and Keras for implementation.

2.1.2 System Architecture

The system architecture consists of several key components, designed to work together seamlessly to detect intrusions effectively:

1. Data Acquisition:
    - The UNSW-NB15 dataset serves as the primary source of input data, encompassing diverse types of network traffic data, comprising both normal and malicious activities.
2. Data Preprocessing:
    - Cleaning: The process involves eliminating any missing or inconsistent data to maintain the quality of the dataset.
    - Normalization: Features are scaled to a specific range to enhance the performance of machine learning algorithms.
    - Feature Selection: This step involves identifying and selecting the most pertinent features to diminish dimensionality and improve model performance.
3. Model Training:
    - The preprocessed dataset undergoes division into training and testing sets, with 80% allocated for training and 20% for testing.
    - Diverse machine learning models such as SVM, DT, RF, and NN undergo training on the designated training set.
4. Model Evaluation:
    - Trained models undergo evaluation using the test set, where metrics including accuracy, precision, recall, and F1-score are computed to gauge performance.
    - The confusion matrix is employed to visually represent the performance of the classification models.
5. Deployment:
    - The most effective model is deployed within a simulated real-time environment, enabling it to monitor and analyze network traffic for intrusion detection purposes.
6. Feedback Loop:
    - Continuous monitoring and evaluation allow for periodic updates and retraining of the models with new data to maintain high detection accuracy.

2.2 Algorithm

To develop an effective Intrusion Detection System (IDS) using machine learning, a structured algorithm is followed encompassing several crucial steps. Initially, data is gathered from the UNSW-NB15 dataset, which contains diverse network traffic types and intrusion scenarios. The data undergoes preprocessing, involving cleaning to eliminate incomplete or inconsistent entries, normalization to scale features uniformly, and selection of the most pertinent features for classification.

Subsequently, a variety of machine learning algorithms are selected for comparison, including Support Vector Machine (SVM), Linear Regression, Logistic Regression, Decision Tree Classifier, Random Forest Classifier, K-Nearest Neighbors (KNN), and Multi-Layer Perceptron (MLP). The dataset is then partitioned into training and testing sets, and each model is trained on the training set to learn patterns indicative of normal and intrusive behavior.

The performance of each model is assessed using the testing set, employing metrics such as accuracy, precision, recall, and F1-score to gauge effectiveness. In our investigation, the Random Forest classifier achieved the highest accuracy for binary classification, while the MLP classifier excelled in multi-class classification. Following evaluation, hyperparameter tuning is conducted to optimize model performance, fine-tuning parameters specific to each algorithm to enhance accuracy.

Upon identifying the best-performing model, it is implemented in a real-time intrusion detection system. This system continually monitors network traffic, classifying it as either normal or intrusive based on the trained model. By adhering to this meticulous algorithm, the IDS is engineered to be robust, efficient, and capable of detecting a wide spectrum of network intrusions with high accuracy.

2.3 Flowchart

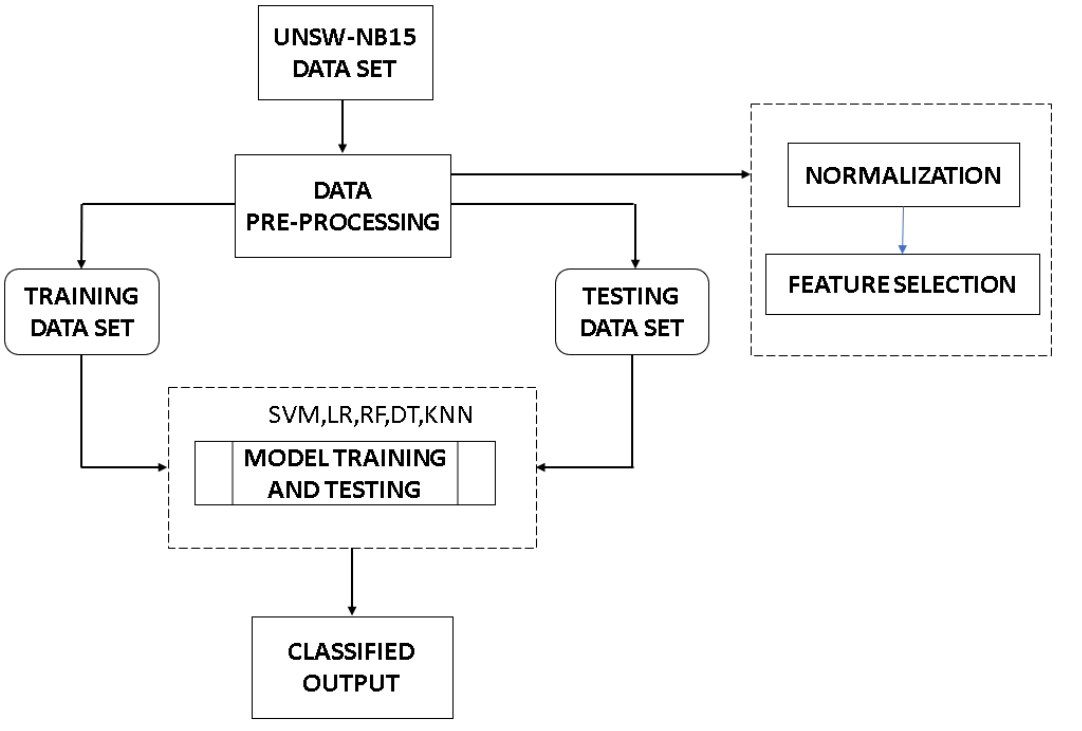

Figure 2.1: Flowchart of the System Architecture

The system's architectural layout is depicted in Figure 3.1. The initial emphasis lies on Data Preprocessing, also known as data engineering, which constitutes a pivotal phase in the learning

process. Subsequent to Data Preprocessing, the dataset undergoes division into training and testing sets, with 80% of the data allocated for training and the remaining 20% for testing. Machine Learning models are subsequently applied to the dataset.

- Preprocessing

  When dealing with raw datasets, it is imperative to inspect and visualize the data. Identical rows may result in overfitting problems, while some columns could contain unclean values such as blanks or nulls. To mitigate these issues, preprocessing the selected dataset is indispensable. This stage encompasses data cleaning, involving the handling of missing values, encoding non-numeric values, and normalizing the data to ensure the dataset is devoid of any flaws that could impact the results of subsequent steps.

  1. Data Cleaning: Rectifying imperfections in the dataset entails standardizing textual values by converting all instances to a consistent case. Null values and spaces are addressed, and numbers stored as text are converted to numeric types.
  2. One-Hot Encoding: Prior to fitting machine learning models, nominal attributes necessitate conversion to numerical values, typically accomplished through one-hot encoding. This process addresses categorical columns by generating new columns for each unique value in the original column, assigning ones to the relevant positions and zeros to others.
  3. Normalization: Large numerical values can impede the learning process in machine learning algorithms, while high-dimensional datasets can be computationally intensive to train. Techniques like Min-Max scaling, Decimal scaling, Z-score standardization, and Max normalization are commonly employed to mitigate these issues. The selection of method often hinges on the specific task at hand. In our data analysis, we utilize Min-Max scaling.

$$F_{norm} = \frac{F - F_{min}}{F_{max} - F_{min}}$$

- Machine Learning Models

  1. Random Forest (RF): Random Forest is an ensemble learning technique that constructs multiple decision trees and aggregates their outcomes for more precise and stable predictions. Within NIDS, it excels in binary classification tasks by distinguishing normal from anomalous traffic. Its proficiency extends to handling large, high-dimensional datasets adeptly, mitigating overfitting through the amalgamation of numerous trees. With a commendable accuracy rate of 98.63%, Random Forest proves highly effective in detecting network intrusions.
  2. Multi-Layer Perceptron (MLP): A Multi-Layer Perceptron (MLP) denotes a neural network comprising multiple layers of nodes. In the realm of NIDS, MLPs are leveraged for multi-class classification tasks owing to their capability to discern intricate, non-linear data relationships. They exhibit efficacy in categorizing diverse cyber attacks, attaining an accuracy rate of 89.93%, thereby rendering them suitable for identifying various intrusion patterns.

3. Support Vector Machine (SVM): Support Vector Machine (SVM) emerges as a supervised learning model that determines the hyperplane optimally separating classes within the feature space. In NIDS applications, SVM proves beneficial for both binary and multi-class classification, particularly in scenarios involving high-dimensional data. Its robustness aids in pinpointing subtle anomalies in network traffic indicative of intrusions.
4. Logistic Regression (LR): Logistic Regression serves as a statistical model employed for binary classification tasks. It gauges the probability of an input belonging to a specific class through a logistic function. Within NIDS, it garners appreciation for its simplicity and efficiency, rendering it apt for real-time detection scenarios characterized by linear feature relationships. Logistic Regression expedites the identification of normal or anomalous network traffic.
5. Decision Tree (DT): A Decision Tree constitutes a model delineated by a tree-like structure of decisions and their prospective outcomes. In NIDS settings, it segments data into subsets grounded on feature values, crafting a framework that prognosticates class labels (e.g., normal or anomalous traffic). Decision Trees are noted for their ease of interpretation and visualization, furnishing lucid insights into the decision-making mechanism underpinning intrusion detection.
6. K-Nearest Neighbors (KNN): K-Nearest Neighbors (KNN) represents an instance-based learning algorithm tasked with classifying data points contingent on the majority class of their nearest neighbors. In NIDS contexts, KNN finds utility owing to its simplicity and efficiency in small dataset scenarios. It juxtaposes novel network traffic data against known instances of normal and anomalous behavior, effectively discerning intrusions through similarity metrics.
7. Linear Regression (LR) : Within the National Institute for Defense Studies (NIDS), linear regression plays a vital role in leveraging machine learning (ML) for analyzing relationships between variables crucial to defense and security. It constructs a predictive model by fitting a line that minimizes the differences between observed and predicted values, facilitating strategic planning, threat assessments, and policy formulation. This method allows NIDS analysts to quantitatively evaluate correlations, providing insights into trends and dependencies essential for enhancing national security and defense strategies.

- Evaluation Metrics

Precision: Precision gauges the accuracy of a model's positive predictions. It represents the ratio of true positive results to the total predicted positives, thereby indicating the proportion of correctly identified positive instances.

$$\text{Precision} = \frac{True\ Postive}{True\ Postive + False\ Postive}$$

Recall: Also referred to as sensitivity, recall evaluates the effectiveness of a classification model in identifying all relevant instances within a dataset. It is calculated as the ratio of true positive results to the total actual positives, demonstrating the model's capability to accurately detect positive cases.

$$\text{Recall} = \frac{\text{True Postive}}{\text{True Postive+False Negative}}$$

F1-score: The F1-score offers a comprehensive performance metric for a classification model. It is computed as the harmonic mean of precision and recall, striking a balance between the necessity for accuracy in positive predictions and completeness in identifying relevant instances.

$$\text{F} - \text{ Measure } = 2\frac{\text{Precision}*\text{Recall}}{\text{Precision+Recall}}$$

- Regression Evaluation Metrics

Mean Absolute Error (MAE): MAE quantifies the average absolute disparity between predicted and actual values. It denotes how closely the predictions align with the actual outcomes on average. However, MAE does not delineate the direction of errors, thus failing to indicate whether the model predominantly over-predicts or under-predicts.

$$\text{MAE} = \frac{1}{\text{N}} \sum_{\text{j}=1}^{\text{N}} |\text{y}_\text{j} - \hat{\text{y}}_\text{j}|$$

Mean Squared Error (MSE): MSE, akin to MAE, calculates the average difference between predicted and actual values. However, it squares these differences before averaging, thereby magnifying larger errors more than smaller ones. MSE is often favored in optimization algorithms due to its computationally simpler gradient calculation, facilitating streamlined programming and model training.

Root Mean Squared Error (RMSE): RMSE is the square root of MSE, furnishing a metric in the same units as the original data. Analogous to MSE, RMSE accords greater significance to larger errors, rendering it sensitive to outliers. It serves as a valuable metric for comprehending the magnitude of prediction errors on the same scale as the data being predicted.

$$\mathrm{MSE} = \frac{1}{\mathrm{N}} \sum_{\mathrm{j}=1}^{\mathrm{N}} \left(\mathrm{y_j} - \hat{\mathrm{y}}_\mathrm{j}\right)^2$$

$$\mathrm{RMSE} = \sqrt{\frac{\sum_{\mathrm{j}=1}^{\mathrm{N}} \left(\mathrm{y_j} - \hat{\mathrm{y}}_\mathrm{j}\right)^2}{\mathrm{N}}}$$

2.4 DATASET

The UNSW-NB15 dataset, devised by the Cyber Range Lab at the Australian Centre for Cyber Security (ACCS) within the University of New South Wales (UNSW), was conceived to rectify the deficiencies of older datasets utilized for the evaluation of intrusion detection systems (IDS), such as KDD99 and NSL-KDD. It functions as a contemporary and comprehensive benchmark for IDS, encompassing an extensive array of network attack types and simulating a realistic and intricate attack environment.

Dataset Content :

- Total Records: 257,673
- Training Records: 175,341
- Testing Records: 82,332
- Features: 44 features per data record, grouped into six categories:
    1. Flow: Integrated information from packets (Features 1-30)
    2. Basic: Connection features (Features 31-37)
    3. Content: General-purpose features (Features 38-42)
    4. Time & Additional Generated Features
    5. Tagged Labels: Features 43-44

Attack Types :

The dataset includes a variety of network attacks categorized into nine types, plus normal traffic:

1. Normal
2. Backdoor
3. Fuzzers
4. Reconnaissance
5. Exploits
6. Analysis
7. DoS
8. Worms
9. Generic

2.5 Classifications

2.5.1 Binary Classifications

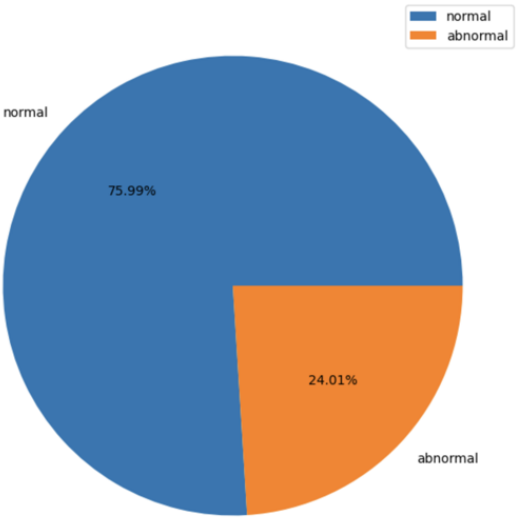

Figure 2.2: Pie chart distribution of normal and abnormal labels

The pie chart depicts the distribution of normal and abnormal labels within the dataset. This graphical depiction aids in comprehending the proportion of each label relative to the entire dataset.

1. Normal Labels (Blue Segment):
    - The larger blue segment represents the normal labels.
    - It constitutes 75.99% of the dataset, indicating that the majority of the data points are labeled as normal.
2. Abnormal Labels (Orange Segment):
    - The smaller orange segment represents the abnormal labels.
    - It constitutes 24.01% of the dataset, indicating that a quarter of the data points are labeled as abnormal.

2.5.2 Multi-Class Classification

A thorough view of the different classes and their proportions within the dataset is provided by the pie chart, which displays the distribution of multi-class labels in the dataset.

1. Normal Labels (Blue Segment):
    - Represent 48.66% of the dataset, indicating that nearly half of the data points are labeled as normal.
2. Backdoor (Orange Segment):

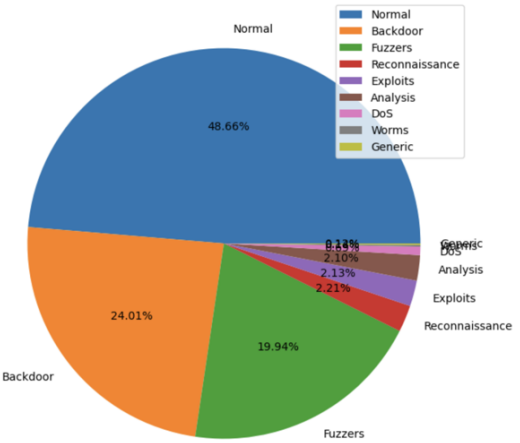

Figure 2.3: The pie chart showcases the distribution of multi-class labels within the dataset.

- Comprises 24.01% of the dataset, making it the second most common label.

3. Fuzzers (Green Segment):

   - Accounts for 19.94% of the dataset, showing significant representation.

4. Other Labels:

   - Reconnaissance: 2.21%
   - Exploits: 2.13%
   - Analysis: 2.10%
   - DoS: 0.13%
   - Worms: Negligible percentage
   - Generic: Negligible percentage

Chapter 3

Results and discussions

3.1 Result Analysis

Binary Classification :

SI.NO	ALGORITHMS	ACCURACY
1	SUPPORT VECTOR MACHINE	97.85%
2	LINEAR REGRESSION	97.86%
3	LOGISTIC REGRESSION	97.84%
4	DECISION TREE CLASSIFIER	98.10%
5	RANDOM FOREST CLASSIFIER	98.63%
6	KNEIGHBOR CLASSIFIER	98.30%
7	MLP CLASSIFIER(Multi Layer Perceptron)	98.38%

Figure 3.1:

The above table shows the result of all algorithms with respect to Binary classification and Random forest classifier has the highest accuracy with 98.63%

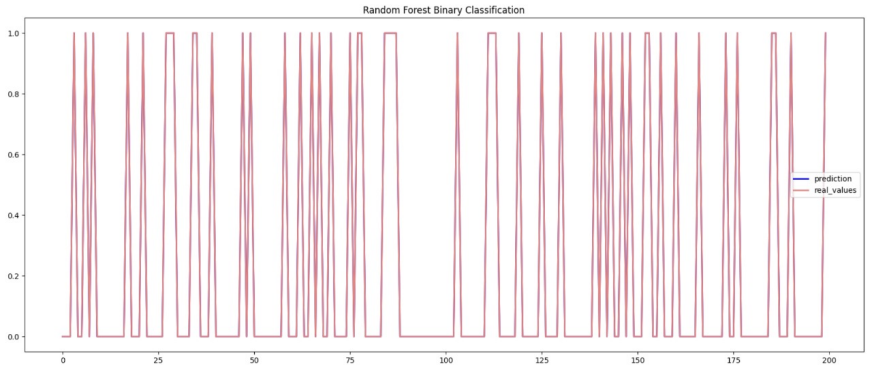

Figure 3.2:

In the Fig 3.1 Showcases the exceptional performance of Random Forest in binary classification, achieving a high accuracy of 98.63% in distinguishing between normal and anomalous network behavior.

Multi-Class Classification :

SI.NO	ALGORITHMS	ACCURACY	R2-SCORE
1	SUPPORT VECTOR MACHINE	89.88%	53.99%
2	LINEAR REGRESSION	81.3%	21.97%
3	LOGISTIC REGRESSION	89.81%	53.88%
4	DECISION TREE CLASSIFIER	85.45%	24.14%
5	RANDOM FOREST CLASSIFIER	89.06%	47.83%
6	KNEIGHBOR CLASSIFIER	88.54%	46.77%
7	**MLP CLASSIFIER(Multi Layer Perceptron)**	**89.93%**	**54.59%**

Figure 3.3:

The above table shows the result of all algorithms with respect to Multi-class classification and MLP Classifier has the highest accuracy with 89.93%

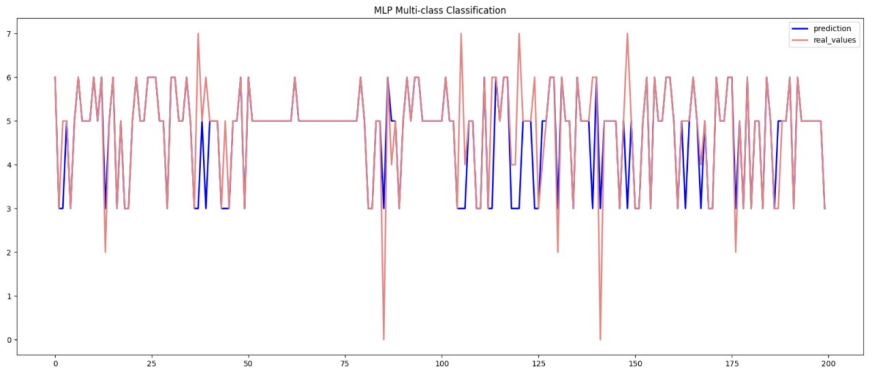

Figure 3.4:

In the Fig 3.2 Highlights the effectiveness of the MLP (Multi-Layer Perceptron) Classifier in multi-class classification, with an accuracy of 89.93% in accurately categorizing various types of cyber attacks.

Using the UNSW-NB15 dataset, the effectiveness of various machine learning methods was assessed for binary and multi-class classifications. The Random Forest classifier outperformed other models, including Support Vector Machine (97.85%), Linear Regression (97.86%), Logistic Regression (97.84%), Decision Tree Classifier (98.10%), K-Nearest Neighbors (98.30%), and Multi-Layer Perceptron (98.38%), in binary classification, with the highest accuracy of 98.63%. This suggests that the Random Forest classifier has a very high degree of success in differentiating between legitimate and invasive network activity. When it came to multi-class classification,

the Multi-Layer Perceptron (MLP) classifier performed best with an accuracy of 89.93%. Support Vector Machine (89.88%) and Logistic Regression (89.81%) were next in line with similar accuracy. Other algorithms with significantly lower performance were Random Forest (89.06%), K-Nearest Neighbors (88.54%), and Decision Tree (85.45%).

The evaluation metrics used for assessing the models included accuracy, precision, recall, and F1-score, ensuring a comprehensive understanding of each model's performance. The high accuracy of the Random Forest classifier in binary classification and the MLP in multi-class classification demonstrates their robustness in detecting intrusions with varying levels of complexity and types. By employing these machine learning models, the intrusion detection system can effectively identify and mitigate a wide range of network threats.

Chapter 4

Conclusions and future scope

4.1 Conclusion

The UNSW-NB15 dataset was used in the study on different machine learning models for intrusion detection, which shows how well these methods operate to recognize binary and multi-class network intrusions. The outcomes show that the Random Forest classifier performs exceptionally well in binary classification, achieving an astounding 98.63% accuracy. This makes it an excellent choice for differentiating between benign and malevolent activity within a network. The Multi-Layer Perceptron (MLP) demonstrated the highest efficacy in multi-class categorization, achieving an accuracy rate of 89.93%, indicating its capacity to manage intricate and diverse forms of intrusions. The thorough evaluation measures employed in this study—accuracy, precision, recall, and F1-score—allow a clear grasp of the advantages and disadvantages of each model. The Random Forest and MLP classifiers' excellent performance highlights their potential in

Future research can build upon these findings by exploring deep learning models and hybrid approaches to further improve detection accuracy and response times. Additionally, testing these models on other datasets and real-world scenarios will help validate their robustness and adaptability. Implementing such advanced models in practical intrusion detection systems will significantly contribute to safeguarding networks against evolving cyber threats.

4.2 Future scope

Machine learning-based intrusion detection systems (IDS) have a bright future ahead of them, largely due to the need to improve cybersecurity in linked and increasingly complex environments. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs), two deep learning models that have demonstrated promise in processing high-dimensional data and identifying complex patterns, should be the main focus of future study. These models can be especially useful for spotting new and advanced assaults that more conventional machine learning models could overlook. The creation of hybrid models, which combine the advantages of several machine learning and deep learning methods to increase detection accuracy, is another exciting avenue.

An additional promising avenue involves the creation of hybrid models amalgamating the advantages of diverse machine learning and deep learning algorithms to enhance detection accuracy and mitigate false positives. Furthermore, real-time intrusion detection systems leveraging streaming data analytics hold promise in delivering prompt responses to threats, thereby bolstering the overall security stance of networks.

Expanding the evaluation of IDS models on diverse and more realistic datasets beyond UNSW-NB15 can provide a more comprehensive assessment of their robustness and adaptability in different network environments. This includes incorporating emerging threats and attack vectors to ensure the IDS can effectively respond to the latest security challenges.

Finally, the integration of machine learning-based IDS with other cybersecurity tools and platforms can create a more holistic and coordinated defense mechanism, enhancing the ability to detect, analyze, and mitigate attacks. This collaborative approach can lead to more resilient and adaptive security systems capable of protecting against an ever-evolving threat landscape.

4.2.1 Application in the societal context

In the societal context, the use of machine learning-based intrusion detection systems (IDS) is crucial since it directly affects people's and organizations' security and privacy. With the growing reliance of society on digital infrastructure, there is an increased chance of cyber dangers including malware, hacking, and data leaks. Machine learning-based intrusion detection systems (IDS) can provide strong security solutions that adjust to fresh and changing threats, acting as a preventative measure. These technologies can be used in the public services sector to protect vital infrastructures against cyberattacks, including transportation networks, water supply systems, and power grids. The IDS contributes to the maintenance of public safety and confidence by guaranteeing the integrity and dependability of these crucial services.

Moreover, in the healthcare sector, where sensitive patient data is stored and transmitted, machine learning-based IDS can protect against unauthorized access and data theft, ensuring compliance with data protection regulations and preserving patient confidentiality. This not only protects individual privacy but also upholds the integrity of the healthcare system.

In the business sector, the implementation of IDS can help companies protect their intellectual property, financial data, and customer information from cybercriminals. This protection is crucial for maintaining competitive advantage, financial stability, and customer trust. Additionally, the presence of robust security measures can enhance a company's reputation and reliability, potentially leading to increased business opportunities and growth.

In general, machine learning-based intrusion detection systems are used in society to improve digital environment security in a variety of industries, ultimately leading to a more secure and safe digital civilization. These systems are essential for protecting private, business, and public data by averting and lessening the effects of cyberattacks. This helps to ensure the safe and orderly operation of contemporary civilization.

Bibliography

[1] **Iqbal H. Sarker, Yoosef B. Abushark, Fawaz Alsolami and Asif Irshad Khan, "IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model",Received: 31 March 2020; Accepted: 15 April 2020; Published: 6 May 2020.**

[2] **Sandy Victor Amanoul, Adnan Mohsin Abdulazeez, Diyar Qader Zeebare, Falah Y. H. Ahmed,"Intrusion Detection Systems Based on Machine Learning Algorithms", 2021 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS 2021), 26 June 2021, Shah Alam, Malaysia.**

[3] **K.Shanthi, R.Maruthi, "Machine learning Approach for Anomaly-based Intrusion Detection Systems using Isolation Forest Model and Support Vector Machine",©2023 IEEE**

[4] **C.Kaushik, T.Ram, Ritvik.C, T.Lakshman, "Network Security with Network Intrusion Detection System using Machine Learning Deployed in a Cloud Infrastructure",©2022 IEEE**

[5] **Uday chandra Akuthota, Lava Bhargava, "Evaluation of Machine Learning Models for Intrusion Detection with the UNSW-NB15 Dataset",©2023 IEEE**

[6] **Aezeden Mohamed, Janne Heilala, Nelson Sizwe Madonsela, "Machine Learning-Based Intrusion Detection Systems for Enhancing Cybersecurity",©2023 IEEE**

[7] **Pooja Vaibhav Potnurwar, Ayush Ainchwar, Rahul Neware,and Vrushali Bongirwar,"Intrusion Detection System for Big Data Environment Using Deep Learning ", 15 January 2024.**