Educational Administration: Theory and Practice
2024, 30(5), 6323-6334
ISSN: 2148-2403
https://kuey.net/

Research Article

Advancing Cybersecurity: Leveraging UNSW_NB15 Dataset for Enhanced Detection and Prediction of Diverse Cyber Threats

Swati Gawand[1*], Dr. Meesala Sudhir Kumar[2]

[1*]Research Scholar, Department of Computer Science and Engineering, Sandip University, Mahiravani, Nashik 422213, Maharashtra, India, swatigawand@gmail.com
[2]Professor, Department of Computer Science and Engineering, Sandip University, Mahiravani, Nashik 422213, Maharashtra, India, sudhir.meesala@sandipuniversity.edu.in

Citation: Swati Gawand (2024), Advancing Cybersecurity: Leveraging UNSW_NB15 Dataset for Enhanced Detection and Prediction of Diverse Cyber Threats, *Educational Administration: Theory and Practice, 30(5),* 6323-6334, Doi: 10.53555/kuey.v30i5.3936

ARTICLE INFO **ABSTRACT**

A significant challenge in this domain is the lack of a complete network-based dataset that accurately represents contemporary network traffic patterns, encompasses a wide range of subtle intrusions, and provides detailed, structured information on network activity. Current Intrusion Detection Systems (IDS) struggle with high rates of both false positives and false negatives, leading to reduced accuracy in detecting a wide range of cyber threats. This inconsistency affects the overall effectiveness of these systems in identifying diverse types of attacks. In this paper we discuss the UNSW-NB15 dataset serves as a prominent benchmark for research in network intrusion detection. It was designed to support the advancement and assessment of intrusion detection systems (IDS) and machine learning techniques aimed at identifying and categorizing different forms of network attacks.This study focuses on developing machine learning model that can identify cyber-attacks and and enhance IDS system performance. The UNSW_NB15 dataset contains 9 different types of cyber-attacks namely Fuzzers, analysis, DoS, Backdoor, Exploits, Generic, Reconnaissance, Shellcode, worms. We obtained the dataset from link - http://www.cybersecurity.unsw.adfa.edu.au/ADFA%20NB15%20Datasets/.
The proposed model was executed with different algorithms such as logistics regression Nearest Neighbour, Decision Tree and after analyzing the results, we observed that the Random Forest algorithm achieved remarkable accuracy, precision, recall, and F1 score of 98%, closely followed by the Decision Tree algorithm with an impressive 97% accuracy. However, the Support Vector Machine (SVM) algorithm demonstrated relatively lower accuracy at 54%.

Index Terms – Cyber Attacks, Denial of Service attack (DoS), Wannacry attack, DoS attack, Algorithms.

I. INTRODUCTION

Owing to the escalating frequency and complexity of cyber-attacks spanning various sectors, network security has emerged as a critical realm of research, attracting global attention. Cybercriminals employ diverse tactics to infiltrate users' defenses, gaining unauthorized access to sensitive data and engaging in activities such as eavesdropping [1]. Regrettably, traditional firewalls and antivirus software often prove inadequate in detecting zero-day attacks, denial of service attacks, data breaches, and other sophisticated forms of intrusion. Consequently, cybercrime rates continue to climb due to vulnerabilities in computer systems, ineffective security protocols, and insufficient awareness about cyber threats [2]. In 2021 alone, more than three billion zero-day attacks were documented, highlighting the urgent need for effective solutions to counter these pervasive threats [3].

In this paper we discussed about NSL KDD dataset, an enhanced version of the widely used KDD Cup 99 dataset, serves as a benchmark for evaluating intrusion detection systems (IDS). It was created to address some limitations of the original KDD Cup 99 dataset, such as redundant records and the lack of modern network traffic characteristics. The NSL-KDD dataset contains a comprehensive set of features extracted from network traffic data, categorized into various types of attacks and normal activities. These features encompass network connection attributes like protocol type, service, flags, and packet and byte counts.

On this dataset we apply various machine learning algorithms for identification of cyber-attacks and classification .Also predicting what kind of cyber-attack will happen in future. Machine learning algorithms offer the capability to proactively detect and counter cyber-attacks within applications. By leveraging these algorithms, it becomes possible to train systems to recognize and preempt potential cyber threats. This is typically accomplished through the development of models that analyze datasets containing security events, discerning patterns indicative of malicious activities. By doing so, these algorithms enable real-time monitoring, identification, and response to emerging threats.

The remainder of this paper is organized as follows. Section II is related to literature survey. Section III present the Methodology. Section IV discuss the result analysis. Section V contains the conclusion of this research study and the future direction of works.

II. RELATED WORK

A comparative analysis is conducted utilizing these machine learning algorithms. System performance is evaluated using Cross-Validation score, Recall value, F1 Score, Precision value and Accuracy value metrics. The analysis of system performance demonstrates which algorithm achieves the most accurate results [1]. Machine Learning algorithms can be used to train and detect if there has been a cyber-attack. As soon as the attack is detected, an email notification can be sent to the security engineers or users [4]. Any classification algorithm can be used to categorize if it is a DoS/DDoS attack or not. One example of a classification algorithm is Support Vector Machine (SVM) which is a supervised learning method that analyses data and recognizes patterns. Any system that requires minimal human intervention would be ideal. Machine learning techniques for classification include Logistic Regression, Nearest Neighbours, Support Vector Machine, Nave Bayes, Decision Tree, and Random Forest Classification. Upon the availability of large collection of past data with labels, Deep Learning classification models involving Restricted Boltzmann Machines (RBM), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), or Long-Short Term Memory (LSTMs) cells for feature extraction followed by a densely connected neural network have become more efficient in solving complex tasks Applicability of the above supervisory machine learning techniques is conditioned based on the availability of large collections of labelled data [1]. Mona Alduailijet al. [3] describes a cloud computing mechanism for detecting DDoS attacks. The primary purpose of this article is to reduce misclassification mistakes in DDoS detection. The suggested study employs two feature selection techniques, namely the Mutual Information (MI) and Random Forest Feature Importance (RFFI) methods, to identify the most relevant features. Random Forest (RF), Gradient Boosting (GB), Weighted Voting Ensemble (WVE), K Nearest Neighbour (KNN), and Logistic Regression are applied to selected variables. (LR). The experimental results show that the accuracy of RF, GB, WVE, and KNN with 19 characteristics is 0.99. Cyber Attack Detection Model (CADM) Based on Machine Learning Approach [5], pre-processing is done to remove the missing values, outliers etc. and from the pre-processed data, the significant features are found by applying correct feature selection algorithm. After that, the data with the selected features are classified with the help of classification algorithms. Ensemble method is used for classification because this method produces highly trusted decisions and improves overall accuracy by working together. Cyber Attack Detection Model (CADM) Based on Machine Learning Approach [5] The principal contributions behind building this CADM system are: Build an automated detection mechanism CADM by using DBSCAN to work with multi-dimensional data and LASSO to reduce dimensionality and choosing the effective characteristics of a network for classification of different types of attack. Attack Forecast and Prediction[7]Improving defensive capabilities in cyber-space for improving cyber-security is one of the key challenges that need to be solved to enable re- silient societies and modern life, which is increasingly penetrated by information technology. Understanding the past and predicting the future is an approach being sought in the course of time to develop new security profiles and software to help protect socially sensitive data and critical infrastructure from attackers. Predicting future cyber-attacks can help businesses, individuals and society. Minimizing attacker's first mover advantage therefore need to be a focal point of research. Machine learning formula plays an important role in raising the protection mea- sures in this intrusion detection system. ML algorithms are classified into 2 types: supervised learning and unsupervised learning. They're differentiated by the information (i.e., input) that they settle for. Supervised learning refers to algorithms that are given a group of la- belled training information, with the task of understanding what differentiates the labels. Unsupervised learning refers to algorithms that are given unlabeled training information, with the task of inferring the classes all by itself. Typically, the labelled information is in- credibly rare, or even the task of labelled data is itself terribly exhausting and we may not be able or ready to sight if labels actually exist [8]. The machine learning security corporations typically deploy train methods on giant information sets to ”learn” what to look out for and the way to react to totally different things on networks. Machine learning is much too powerful in its title, though, and approach could be a natural suited antivirus defense and malware scanning: Machine learning approach can facilitate us to stop sensitive information leaks, corporate executive intrusion detection system and malware detection [8]. Modeling Machine Learning for Analyzing Crime News [36] Time series of crime data in San Francisco, Chicago and Philadelphia were used for predicting crimes in the following years. Decision Tree (DT) classification model performed better than K-nearest neighbors (KNN) and Naive Bayes (NB). Crime data were passed through two different data processing procedures in Canada. A crime prediction was made with accuracy between 39 percent and 44 percent using the KNN and DTs. Data such as location, type, date, time, latitude and longitude of the crimes taking place in the USA were used as input. The result of the crime predictions made with KNN Classification, Logistic Regression (LR), DTs, Random Forest (RF), Support Vector Machine (SVM) and Bayesian methods was that the KNN classification was the most successful with an accuracy of 78.9 percent.

The use of SVM with the algorithms increases their accuracy and efficiency with respect to time and results. As SVM is a classification algorithm, it has the capability to classify the points or sets in much precious manner. There are various applications that use SVM for classification purpose. A thorough search has resulted into selecting SVM for the system. Different phases of the system use the SVM differently. But what makes it most reliable is its advantage of redundancy. The use of SVM increases systems accuracy and response time. Although, the configuration of the phone does matter a lot, as this is an android based system. As the world is growing more prone to the technology and smart phones, there are well developed and high configured phones. The majority of them use Android today. So an android based system is developed for compatibility and ease of use to users[27].

In the modern world and fast development of the internet, the connection among people is being very significant than ever, people are looking for new methods to do advance communication between them without any issue, real-time communication is one of this ways. Currently video conference system usually needs to install application software. Therefore software need to be developed for different operating systems (android, windows, and mac) and user data goes through servers. However, web-based video conference system is OS independent so it saves development cost[28].

III. METHODOLOGY

This section provides a detailed explanation of the system methodology. Figure 1 illustrates the Proposed Model, where the dataset serves as the initial input, initiating further operations. Various machine learning algorithms are utilized for model training, considering the heterogeneous nature of the cyber-attack data within the dataset. The framework encompasses the following essential steps:

1. To select which dataset will be used.
2. Data preprocessing methods to deal with irrelevant data from the dataset and data encoding.

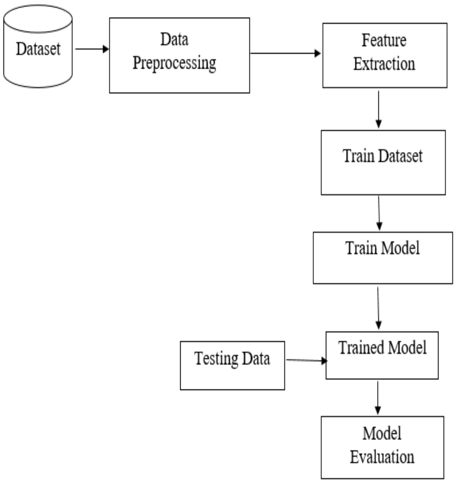

Figure 1: Proposed System Model

3. Feature Extraction to pick up the best attributes from a dataset to construct a model with better detection accuracy and speed.
4. The data is split into a train and test set for the model. In this step, we will construct and train our proposed model.
5. Train the model using machine learning algorithms such as Logistics Regression, Gaussian Naive Bayes, Support Vector Machine, Decision Tress Random Forest, and KNN
6. A test data set is applied to the trained model, and the model's performance is evaluated using the parameters precision, recall, F1 Score, Cross-validation score (CV), accuracy, training score, and testing score.

Collection of Dataset- The UNSW-NB15 dataset is commonly used in cybersecurity research for evaluating intrusion detection systems and other related tasks**.** The official website of the UNSW ADFA (Australian Defense Force Academy) provides access to various cybersecurity datasets, including the UNSW-NB15 dataset. You can download the dataset from the following link: UNSW ADFA Datasets.

- **Data Preprocessing-** Data preprocessing is an essential phase in readying raw data for machine learning models. It stands as the foundational step in model development. Within the datasets utilized, there exist instances of missing and redundant values, referred to as outliers. Consequently, preprocessing involves the elimination of these outliers from the datasets.

- **Feature Extraction-** Feature extraction involves the extraction of key attributes from a dataset to enhance model detection accuracy and efficiency. Within the dataset, comprising a total of 42 columns, 19 features are meticulously selected for training purposes. Recursive Feature Elimination (RFE) modeling is employed for feature selection. Notably, random forest feature importance demonstrates high accuracy compared to alternative techniques. The objective of RFE is to iteratively select features by analyzing progressively smaller feature sets. Initially, the estimator is trained on the complete feature set, followed by the removal of the least important features from the current set. This recursive process continues until the desired number of features is attained..

Machine Learning Algorithms-This model employs various machine learning algorithms, including Logistic Regression, Gaussian Naive Bayes, Support Vector Machine, Decision Tree, Random Forest, and k-Nearest Neighbors (K-NN).

Trained Model- During this phase, a separate test dataset is employed to evaluate the efficacy of the trained model. Evaluation encompasses diverse metrics, including precision, recall, F1 score, cross-validation score (CV), accuracy, training score, and testing score. These metrics collectively provide insights into the model's accuracy and its capability for generalization.

IV. DATA & RESULT ANALYSIS

Data Analysis

The UNSW-NB15 dataset serves as a prevalent resource in cybersecurity research, particularly for evaluating intrusion detection systems and associated endeavors. Originating from the University of New South Wales (UNSW) in Australia, this dataset is openly accessible for academic and research purposes. Interested parties can procure the UNSW-NB15 dataset from the UNSW ADFA-IDS Datasets Website. This official platform, hosted by the UNSW Australian Defense Force Academy (ADFA), offers access to a range of cybersecurity datasets, including the UNSW-NB15 dataset, available for download via the provided link on the UNSW ADFA Datasets website.

The dataset comprises a total of 2,540,044 records, distributed across four CSV files: UNSW-NB15_1.csv, UNSW-NB15_2.csv, UNSW-NB15_3.csv, and UNSW-NB15_4.csv. Additionally, it includes a ground truth table labeled UNSW-NB15_GT.csv and an event list file named UNSW-NB15_LIST_EVENTS.csv.

A subset of this dataset was allocated for training and testing purposes, resulting in two distinct sets: UNSW_NB15_training-set.csv and UNSW_NB15_testing-set.csv. The training set contains 175,341 records, while the testing set comprises 82,332 records. Both sets encompass various types of data, including attack and normal instances.

The Table 4.1 shows this details.

Table 4.1: Classification of Attacks

Attack Class	Attack Type
Fuzzers	An attack that sends malformed or random data to a program, often to trigger unexpected behaviour or vulnerabilities.
Analysis	An attack that involves reconnaissance or probing of a network to gather information about potential targets or vulnerabilities.
DoS	Denial of Service (DoS) attacks attempt to disrupt or overwhelm a target system or network, rendering it unavailable to legitimate users.
Backdoor	An attack that installs unauthorized access points or hidden functionality in a system to allow remote access or control
Exploits	Attacks that take advantage of known vulnerabilities or software bugs to gain unauthorized access to a system or execute arbitrary code.
Generic	Generic attacks that do not fit into specific attack categories, often characterized by unusual or anomalous behaviour
Reconnaissance	An attack that involves actively scanning or probing a network to gather information about its structure, hosts, and services
Shellcode	Attacks that involve injecting malicious code (shellcode) into a target system, typically to gain control or execute commands
Worms	Self-replicating malware that spreads across a network by exploiting vulnerabilities in software or network protocols

● Dataset File Details

The UNSW-NB15 dataset comprises several files, each containing distinct subsets of network traffic data and associated labels. Below are the primary files included in the dataset, along with brief descriptions:

1. UNSW_NB15_training-set.csv:

Contained within this file is the training dataset, utilized to train machine learning models. It encompasses features derived from network traffic data, including protocol types, packet sizes, durations, and payload content. Each instance is accompanied by labels denoting whether it represents normal traffic or a particular type of attack.

2. UNSW_NB15_testing-set.csv:
Much like the training set file, this document comprises the testing dataset, serving to assess the performance of trained models. It mirrors the features and labels present in the training set file, yet represents a distinct collection of instances unseen during the training phase..

3. UNSW_NB15_training-set-a.csv:
This document serves as an alternate training set, featuring a subset of data extracted from the primary training set. It offers a platform for experimentation or aims to alleviate the computational resources demanded during model training.

4. UNSW_NB15_testing-set-a.csv:
Much like the alternative training set, this file acts as an alternative testing set, comprising a subset of data derived from the primary testing set. It provides an avenue for experimentation or aims to mitigate the computational demands associated with testing models.

5.UNSW_NB15_UNSW_NB15testing-set-c.csv: This file encompasses an additional testing set, labeled "testing-set-c." Its purpose may involve further evaluation or validation tasks.

6.UNSW_NB15_features.csv: This file furnishes thorough descriptions of features extracted from network traffic data, comprising details regarding feature names, types, and their respective descriptions.

7. UNSW_NB15_list_of_attacks.csv: Contained within this file is a comprehensive list of attack types featured in the dataset, accompanied by their corresponding descriptions.

Together, these files constitute the UNSW-NB15 dataset, offering researchers and practitioners a robust collection of network traffic data for various purposes, including research, experimentation, and the development of intrusion detection systems and machine learning algorithms.

Following table 4.2 shows the frequency of intrusion in dataset.

Table 4.2: Frequency of Attack in dataset

Type of Data	Frequency
Normal	2054090
Fuzzers	24246
Analysis	2677
Backdoor	2329
DoS	16 535
Exploits	44525
Generic	58861
Reconnaissance	13987
Shellcode	1511
Worms	174
Total Records	2218761

Following Table 4.3 shows frequency of records in the training dataset. Following Figure 4.1 shows graphical representation of Intrusion Category Network Traffic in UNSW-NB15 Dataset

Table 4.2: Frequency of Attack in training dataset

Type of Data	Frequency
Normal	37000
Fuzzers	6062
Analysis	677
Backdoor	583
DoS	4089
Exploits	11132
Generic	18871
Reconnaissance	3496
Shellcode	378
Worms	44
Total Records	82332

Following Table 4.4 shows frequency of records in the testing dataset

Type of Data	Frequency
Normal	56000
Fuzzers	18184
Analysis	2000

Backdoor	1746
DoS	12264
Exploits	33393
Generic	40000
Reconnaissance	10491
Shellcode	1133
Worms	130
Total Records	17,5341

Exploratory Data Analysis

Exploratory Data Analysis (EDA) serves as a crucial initial phase in the data analysis journey, focusing on unraveling the structure, patterns, and interrelations within a dataset. Through the utilization of diverse techniques like data visualization, summary statistics, and exploratory modeling, EDA empowers analysts and data scientists to glean profound insights into the intrinsic nature of the data. This investigative process entails scrutinizing distributions, pinpointing outliers, delving into correlations among variables, and discerning any latent issues or irregularities.

Within machine learning, correlation denotes the statistical connection between two or more variables, gauging the degree to which alterations in one variable coincide with changes in another. The Pearson correlation coefficient, commonly symbolized as 'r,' stands as a prevalent metric utilized to assess the magnitude and orientation of the linear association between two continuous variables. Its scale spans from -1 to 1, capturing the extent of correlation between the variables. where:

- r=1 indicates a perfect positive correlation (as one variable increases, the other variable also increases linearly).
- r=−1 indicates a perfect negative correlation (as one variable increases, the other variable decreases linearly).
- r=0 indicates no linear correlation between the variables

Feature Selection: Correlation analysis plays a pivotal role in identifying redundant or closely related features within a dataset. By eliminating such features, model complexity can be diminished, enhancing interpretability without compromising predictive accuracy. Table 4.5: Correlation Values between two values

Variable 1	***Variable 2***	***Correlation Values***
stime	*Ltime*	*1*
swin	*Dwin*	*0.997174708*
dloss	*Dpkts*	*0.992128631*
dbytes	*Dloss*	*0.991376462*
dbytes	*Dpkts*	*0.970803704*
ct_dst_ltm	*ct_src_dport_ltm*	*0.960191873*
ct_srv_src	*ct_srv_dst*	*0.956759024*
sbytes	*Sloss*	*0.954961115*
ct_srv_dst	*ct_dst_src_ltm*	*0.951066477*
ct_src_ltm	*ct_src_dport_ltm*	*0.945315205*
ct_srv_src	*ct_dst_src_ltm*	*0.942174265*
ct_dst_ltm	*ct_src_ltm*	*0.938506142*
tcprtt	*Synack*	*0.932940833*
ct_src_dport_ltm	*ct_dst_sport_ltm*	*0.921432623*
tcprtt	*Ackdat*	*0.921293044*
ct_src_dport_ltm	*ct_dst_src_ltm*	*0.910904101*
Sttl	*ct_state_ttl*	*0.905564623*
Sttl	*Label*	*0.904224554*

Correlation Heatmap-

A correlation heatmap visually represents the correlation matrix, showcasing pairwise correlation coefficients between variables in a dataset through a color-coded matrix. This visualization offers a swift and intuitive means of discerning correlation patterns among variables. Typically, correlation heatmaps are generated and interpreted to unveil underlying relationships within the data.

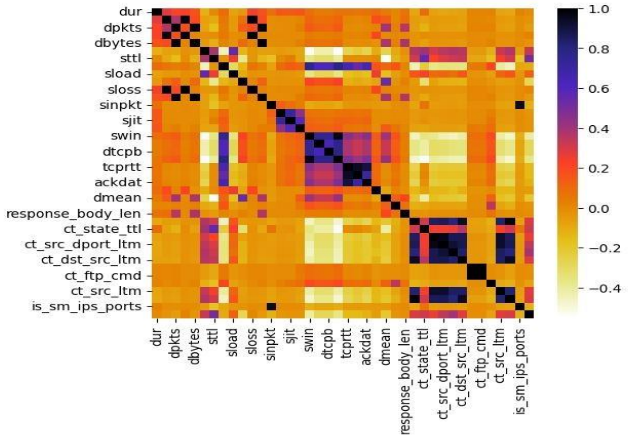

Figure 4.1 Correlation heatmap of UNSW_NB15 Dataset

Result Analysis

Proposed system is executed in two ways i.e. with feature selection (19) features that are highly correlated and without feature selection. Table 4.6 Shows the Performance Evaluation with feature selection on dataset with different machine learning algorithms. The table presents a comparative analysis of various machine learning algorithms based on their accuracy, recall, and precision metrics

Table 4.6: Performance Evaluation on dataset with feature selection

Algorithm	**Accuracy**	**Recall**	**Precision**
Logistic Regression	92.80%	92.80%	92.83%
KNN	91.04%	90.04%	89.09%
Decision Tree	96.38%	96.38%	96.38%
Random Forest	97.68%	97.68%	97.69%
SVM	54.46	72.02	63.17
Gradient Boosting	85.85%	85.85%	85.86%
MLP	94.25%	94.25%	94.26%
MLP(Keras)	94.10%	94.10%	94.10%
GRU(Keras)	93.33%	94.33%	92.33%
LSTM(Keras)	92.48%	92.48%	92.48%

Among the algorithms assessed, Random Forest emerges as the top performer, exhibiting the highest accuracy, recall, and precision rates, indicating its effectiveness in correctly classifying instances and minimizing errors. Decision Tree also demonstrates strong performance, achieving consistently high scores across all metrics. Logistic Regression, MLP, and MLP (Keras) perform comparably well, showing high levels of accuracy, recall, and precision. Additionally, GRU (Keras) and LSTM (Keras) exhibit similar performance, albeit with slightly lower precision scores. Gradient Boosting follows closely behind, showcasing respectable accuracy, recall, and precision rates. However, SVM lags behind the other algorithms, with notably lower accuracy, recall, and precision scores, suggesting limitations in its classification capabilities. Overall, the analysis highlights Random Forest as the standout algorithm for achieving superior classification performance across multiple metrics, while also emphasizing the varying strengths and weaknesses of each algorithm in handling classification tasks. Table 4.7 Shows the Performance Evaluation without feature selection on test dataset with different machine learning algorithms.

Table 4.7:Performance Evaluation without feature selection on test dataset

Algorithm	**Accuracy**	**Recall**	**Precision**
Logistic Regression	75%	76%	65%
KNN	76%	70%	68%
Decision Tree	72%	69%	96.38%
Random Forest	78%	74%	72%
SVM	42%	39%	41%
Gradient Boosting	68%	65%	66%
MLP	74 %	70%	68%
MLP(Keras)	72%	67%	64%
GRU(Keras)	71%	67%	63%
LSTM(Keras)	71%	69%	68%

The table provides a comprehensive overview of the performance metrics of various machine learning algorithms, including Logistic Regression, KNN, Decision Tree, Random Forest, SVM, Gradient Boosting, and different types of neural network models. Each algorithm is evaluated based on its accuracy, recall, and precision metrics, crucial indicators of its classification performance. Overall, Random Forest emerges as the top-performing algorithm, boasting the highest accuracy among the algorithms considered. Notably, Decision Tree exhibits unexpectedly high precision, possibly indicating overfitting to the majority class. In contrast, SVM demonstrates the lowest performance across all metrics, suggesting limitations in its ability to correctly classify instances. Neural network models, including MLP, MLP (Keras), GRU (Keras), and LSTM (Keras), generally perform comparably to traditional algorithms, indicating their effectiveness in handling classification tasks. The analysis underscores the importance of considering multiple performance metrics to comprehensively evaluate the effectiveness of machine learning algorithms for classification tasks.

In summary, the analysis highlights the varying performance of different machine learning algorithms, with Random Forest demonstrating the highest accuracy and precision, followed closely by Decision Tree and MLP. SVM exhibits relatively lower performance, indicating potential limitations in handling the given dataset. The performance of neural network models (MLP, GRU and LSTM) is comparable to traditional algorithms, suggesting their effectiveness in classification tasks.

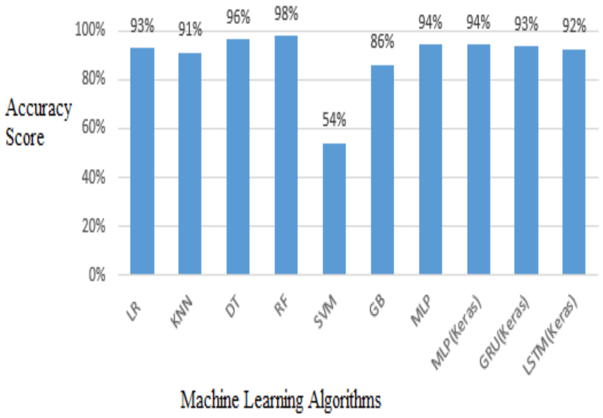

Figure 4.2: Accuracy Comparison of different algorithms

From the Figure 4.2 we can state that Decision Tree (DT), Random Forest (RF) classification accuracy is higher. The "cv score" typically represents the performance of a machine learning model evaluated using cross-validation. Cross-validation is a technique used to assess the generalization ability of a model by partitioning the available data into multiple subsets, often referred to as "folds." Cross-validation provides a more reliable estimate of a model's performance compared to a single train-test split because it leverages multiple iterations of training and evaluation on different subsets of the data. This helps to mitigate the variability in model performance that may arise from the specific random partitioning of the data in a single train-test split.

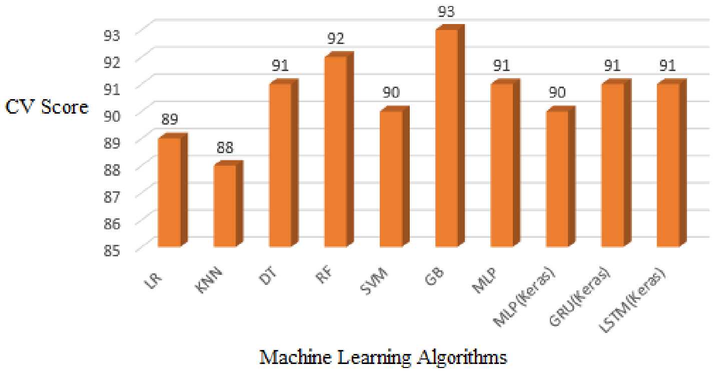

Figure 4.3:CV Score Comparison of different algorithms

From the Figure 4.3 we can state that gradient boosting CV Score is 93, Random Forest (RF) Score is 92. A higher cross-validation (CV) score typically indicates better performance of a machine learning model. In the context of cross-validation, the CV score is an aggregated metric

As experiment Conducted with NSL KDD dataset that has multiple classification data. Decision Tree and Random Forest algorithm achieves higher accuracy than other algorithms. Results may vary depending on the dataset values.

A lower cross-validation (CV) score typically indicates poorer performance of a machine learning model. In the context of cross-validation, the CV score represents the average performance of the model across multiple folds of the dataset. A lower CV score suggests that the model's predictions are less accurate or less reliable when generalized to unseen data.

The F1 score represents the harmonic mean of precision and recall and is a commonly used metric for evaluating the performance of a classification model, particularly when dealing with imbalanced datasets. The F1 score ranges from 0 to 100, with 100 indicating perfect precision and recall, and 0 indicating poor performance. It is a useful metric for evaluating models, especially in scenarios where there is an imbalance between the classes or when both false positives and false negatives are important considerations. Random Forest and Decision Tree achieves higher F1 Score. A higher F1 score represents better overall performance of a classification model. In practical terms, a higher F1 score means that the model strikes a good balance between minimizing false positives (precision) and minimizing false negatives (recall). This is particularly important in scenarios where both types of errors have significant consequences or when there is an imbalance between the classes in the dataset. Following table 4.8 shows CV Score and F1 score

Table 4.8: Represent F1 Score and CV Score

Algorithm	**F1 Score**	**CV Score**
Logistic Regression	92.80%	89.80%
KNN	90.05%	88.02%
Decision Tree	96.38%	91.44%
Random Forest	97.68%	92.68%
SVM	56.02	89.56%
Gradient Boosting	85.55%	92.64%
MLP	94.25%	91.25%
MLP(Keras)	94.10%	90.10%
GRU(Keras)	93.33%	91.33%
LSTM(Keras)	92.48%	90.80%

Following Table 4.9 shows the false alarm rate of different algorithm. The false alarm rate, also known as the false positive rate (FPR), is a metric used to evaluate the performance of a binary classification model. It measures the proportion of negative instances that are incorrectly classified as positive by the model out of all actual negative instances in the dataset

Table 4.9 False Alarm Rate of different algorithms

Algorithm	**FAR**
Logistic Regression	7.20
KNN	8.96
Decision Tree	3.67
Random Forest	2.32
SVM	45.54
Gradient Boosting	14.15
MLP	5.75
MLP(Keras)	5.9
GRU(Keras)	6.67
LSTM(Keras)	7.52

Random Forest exhibits the lowest false alarm rate among the algorithms considered, indicating its effectiveness in minimizing false positive predictions and accurately classifying negative instances. SVM demonstrates the highest false alarm rate among all algorithms, indicating a significant propensity for false positive predictions and highlighting potential limitations in its classification performance. Gradient Boosting, MLP, MLP (Keras), GRU (Keras), LSTM (Keras) these algorithms exhibit false alarm rates ranging from 5.75% to 14.15%, positioning them between the lower rates of Decision Tree and Random Forest and the higher rate of SVM.

Comparative Analysis

In Comparative analysis, UNSW_NB15 Dataset is compared with NSL KDD Dataset. The NSL KDD dataset is a dataset that is used as a comparison for research in the field of intrusion detection. Where in the NSL-KDD dataset there are two dataset NSL-KDD train and NSL-KDD test.

Total Records in Train dataset is 4,898,431 and test dataset contains total 311,027 records. There are 41 attributes available in the NSL-KDD data set. The 42nd attribute contains data about various 5 classes of network connection vectors and they are categorized as one normal class and four attack classes. The 4 attack classes are further grouped as DOS, Probe, R2L and U2R . The specific types of attacks are classified into four major categories. The Table 4.11 shows this details.

Table 4.11: Classification of Attacks in NSL KDD Dataset.

Attack Class	Attack Type
DoS	Back , Land , Neptune , Pod , Smurf , Teardrop, Worm
Probes	Satan , Ipsweep , Nmap , Portsweep , Mscan , Saint
R2L	GuessP assword, Ftp Write, Imap, Phf, Multihop, Warezmastery
U2R	Bufferoverflow, Loadmodule, Rootkit, Perl, Sqlattack, Xterm

Following Figure 4.4 shows the accuracy comparison of NSLKDD & UNSW_NB15 Dataset. This diagram compares the accuracy of different machine learning models or algorithms across various methods. The accuracy is represented on the y-axis as a percentage. The x-axis lists different approaches or algorithms, including LR (Logistic Regression), KNN (k-Nearest Neighbours), Decision Tree, Random Forest, SVM (Support Vector Machine), gradient boosting, and MLP (Multi-Layer Perceptron).

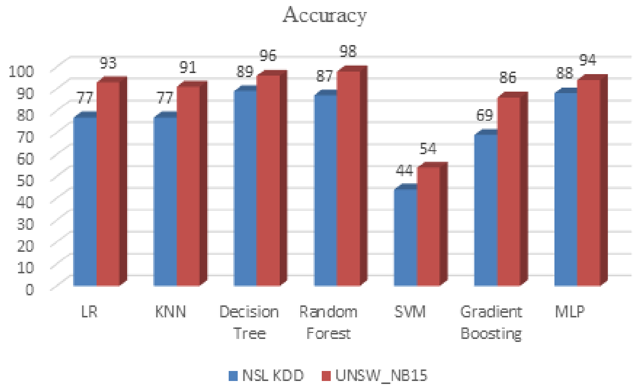

Figure 4.4: Accuracy Comparison of NSLKDD & UNSW_NB15 Dataset

The chart shows that for the LR and KNN models, the accuracy of NSL KDD is lower than UNSW_NB15. However, for Decision Tree, Random Forest, SVM, Gradient Boosting, and MLP, the accuracy of UNSW_NB15 is higher compared to NSL KDD.

The highest accuracy for NSL KDD is achieved with the Decision Tree model (around 89%), while the highest accuracy for UNSW_NB15 is achieved with the RF model (around 98%).

This diagram allows for a visual comparison of the performance of different models or algorithms across different tasks or datasets, as measured by their accuracy. The relative strengths and weaknesses of each model can be evaluated based on the specific task or dataset.

Following figure 4.5 shows: F1 Score Comparison of NSL KDD & UNSW_NB15 Dataset.

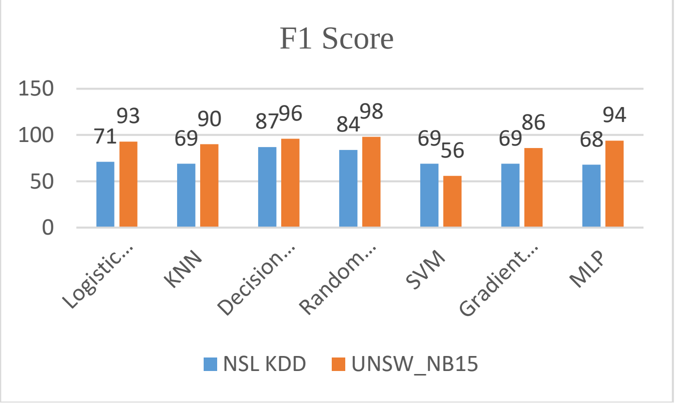

Figure 4.5 F1 Score Comparison of NSLKDD & UNSW_NB15 Dataset

The diagram presents a comparison of the F1 scores achieved by different machine learning models on two datasets, NSL KDD and UNSW_NB15, across various classification tasks or scenarios. The x-axis lists the classification tasks or scenarios, including Logistic Regression, k-Nearest Neighbors (KNN), and Decision Tree, Random Forest, Support Vector Machine (SVM), Gradient Boosting, and Multi-Layer Perceptron (MLP) .The y-axis represents the F1 score, which is a measure of a model's accuracy that combines precision and recall, ranging from 0 to 100.

For Logistic Regression, KNN, and Decision Tree tasks, the models exhibit higher F1 scores on the NSL KDD dataset compared to the UNSW_NB15 dataset, suggesting better performance on the NSL KDD dataset for these tasks. For Random Forest and SVM tasks, the F1 scores are relatively close between the two datasets, indicating comparable performance of these models across both datasets for these specific tasks. For Gradient

Boosting and MLP tasks, the models demonstrate higher F1 scores on the UNSW_NB15 dataset compared to the NSL KDD dataset, implying better performance on the UNSW_NB15 dataset for these particular tasks.
Following Figure 4.6 shows CV Score Comparison of NSLKDD & UNSW_NB15 Dataset. The CV score is a measure of a model's ability to generalize to unseen data and provides an estimate of the model's performance on new, independent data. Higher CV scores typically indicate better generalization and predictive performance of the model.
This graph compares the CV (Cross-Validation) scores of different machine learning models on two datasets: NSL KDD and UNSW_NB15, across various classification tasks or algorithms.
The x-axis represents the different classification algorithms or tasks, such as Logistic Regression, KNN (k-Nearest Neighbors), Decision Tree, Random Forest, SVM (Support Vector Machine), Gradient Boosting, and MLP (Multi-Layer Perceptron).

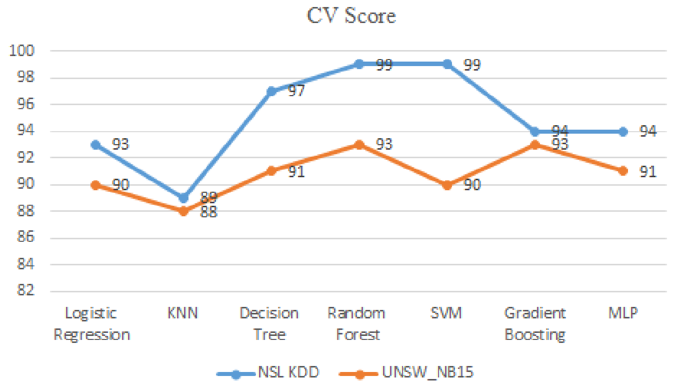

Figure 4.6: CV Score Comparison of NSL KDD & UNSW_NB15 Dataset

V. Conclusions

The rapid pace of technological advancement has made securing systems a formidable challenge. Detecting cyber-attacks has become an increasingly daunting task in today's environment. In this study, we present a comparative approach leveraging machine learning techniques for cyber-attack identification and prediction. Our experimental analysis utilizes the UNSW_NB15 dataset, a comprehensive collection of network traffic data.
The proposed model was executed with different algorithms, and after analyzing the results, we observed that the Random Forest algorithm achieved remarkable accuracy, precision, recall, and F1 score of 98%, closely followed by the Decision Tree algorithm with an impressive 97% accuracy. However, the Support Vector Machine (SVM) algorithm demonstrated relatively lower accuracy at 54%.In future research endeavors, we aim to explore multiclass datasets and assess the system's performance in detecting more complex and diverse cyber-attack types. Additionally, we plan to investigate advanced techniques to further enhance the system's effectiveness in identifying sophisticated cyber threats.

REFERENCES

[1] Gawand, S. ., & Kumar, M. S. (2024). Analytics of Binary Class Detection & Forecasting of Cyber Incident by Machine Learning Methods. International Journal of Intelligent Systems and Applications in Engineering, 12(20s), 100–108. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/5122

[2] Kousik Barik, Sanjay Misra, Karabi Konar, Luis Fernandez-Sanz Murat Koyuncu,” Cy- bersecurity Deep: Approaches, Attacks Dataset, and Comparative Study”, Applied Artificial Intelligence, Published with license by Taylor Francis Group, pp 1-25,2022

[3] Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez- Sanz Vera Pospelova,” The Emerging Threat of Ai-driven Cyber Attacks: A Review”, Applied Artificial Intelligence, Published with license by Taylor Francis Group,1-36, DOI: 10.1080/08839514.2022.2037254,2022

[4] Mona Alduailij, Qazi Waqas Khan, Muhammad Tahir, Muhammad Sardaraz, Mai Aldu- ailij, and Fazila Malik,” Machine-Learning-Based DDoS Attack Detection Using Mutual In- formation and Random Forest Feature Importance Method”, Cloud Computing and Symme- try: Latest Advances and Prospects,1-15, DOI https://doi.org/10.3390/sym14061095,2022

[5] Arpitha. B,Sharan. R , Brunda. B. M,Indrakumar. D. M, Ramesh,”Cyber Attack Detection and notifying system using ML Techniques“, Indian Journal of Computer Science and Engineering (IJCSE) ,pp 28153-28159,2021

[6] Fahima Hossain, Marzana Akter and Mohammed Nasir Uddin ," Cyber Attack Detection Model (CADM) Based on Machine Learning Approach ",2nd International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST) ,pp 567-572,2021

[7] Abdulkadir Bilen and Ahmet Bedri Özer," Cyber-attack method and perpetrator prediction using machine learning algorithms",PeerJ Computer Science,pp 475-496 ,2021

[8] Florian Klaus Kaisera , Tobias Budiga ," Attack Forecast and Prediction ", C&ESAR'21: Computer Electronics Security Application Rendezvous, pp 77-97, 2021

[9] Twinkle Shah, Sagar Parmar , Kishan Panchal ," Cyber Crime Attack Prediction", International Research Journal of Engineering and Technology ,pp 1037–1042. 2020

[10] Kumar,"Cyber-attack prediction using machine learning algorithms", International Conference on Advances in Computing, Communication and Control (ICAC3),pp 1–5,2020

[11] H. Alqahtani, I. Sarker, A. Kalim, S. Minhaz Hossain, S. Ikhlaq and S. Hossain,"Cyber Intrusion Detection Using Machine LearningClassification Techniques," In Proc. International Conference on Communications in Computer and Information Science, pp. 121-131, 2020

[12] A. Ahmim, M. Ferrag, L. Maglaras, M. Derdour and H. Janicke, "A Detailed Analysis of Using Supervised Machine Learning for Intrusion Detection," Strategic Innovative M arketing and Tourism, pp. 629-639, 2020.

[13] W. Zong, Y. Chow and W. Susilo, "Interactive three-dimensional visualization of network intrusion detection data for machine learning," Future Generation Computer Systems, vol. 102, pp. 292-306, 2020

[14] O. Sarumi, A. Adetunmbi and F. Adetoye, "Discovering computer networks intrusion using data analytics and machine intelligence," Scientific African, vol. 9, p. p 1-5, 2020.

[15] A. Nagaraja, B. Uma and R. Gunupudi, "UTTAMA: An Intrusion Detection System Based on Feature Clustering and Feature Transformation," Foundations o f Science, vol. 25, no. 4, pp. 1049-1075,2020.

[16] A. Saleh, F. Talaat and L. Labib, "A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifiers", Artificial Intelligence Review, vol. 51, no. 3, pp. 403-443, 2020.

[17] H. Liu and A. Gegov, "Collaborative Decision Making by Ensemble Rule Based Classification Systems," Studies in B ig Data, pp. 245-264, 2020.

[18] P. Negandhi, Y. Trivedi and R. Mangrulkar, "Intrusion Detection System Using Random Forest on the NSL-KDD Dataset," Emerging Research in Computing, Information, Communication and Applications, pp. 519-531, 2019.

[19] C. Gayathri Harshitha, M. Kameswara Rao and P. Neelesh Kumar, "A Novel Mechanism for Host-Based Intrusion Detection System," In Proc. First International Conference on Sustainable Technologies for Computational Intelligence, pp. 527-536, 2019.

[20] Y. Ever, B. Sekeroglu and K. Dimililer, "Classification Analysis of Intrusion Detection on NSL-KDD Using Machine Learning Algorithms," In Proc. International Conference on Mobile Web and Intelligent Information Systems, pp. 111-122, 2019.

[21] T. Tang, D. McLernon, L. Mhamdi, S. Zaidi and M. Ghogho, "Intrusion Detection in SDN-Based Networks: Deep Recurrent Neural Network Approach," Deep Learning Applications fo r Cyber Security, pp. 175-195, 2019.

[22] A. Gupta, G. Prasad and S. Nayak, "A New and Secure Intrusion Detecting System for Detection of Anomalies Within the Big Data," Studies in Big Data, pp. 177-190, 2018.

[23] A. Saleh, F. Talaat and L. Labib, "A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifiers", Artificial Intelligence Review, vol. 51, no. 3, pp. 403-443, 2017.

[24] M.Ibrahim,"An empirical comparison of random forest-based and other learning-to-rank algorithms,"Pattern Analysis and Applications, vol. 23, no. 3, pp. 1133-1155, 2019.

[25] Mahmudul Hasan, Md. Milon Islam, Md Ishrak Islam Zarif, M.M.A. Hashem,Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,Internet of Things,Volume 7,2019,100059,ISSN25426605,https://doi.org/10.1016/j.iot.2019.100059.

[26] M. G. Raman, N. Somu, S. Jagarapu, T. Manghnani, T. Selvam, K. Krithivasan, V.S. Sriram, An efficient intrusion detection technique based on support vector machine and improved binary gravitational search algorithm, Artificial Intelligence Review (2019) 132

[27] Pushkar Salve, Pranav Mankar, Rohan Kothawade, Hardik Parakh , Prof. Swati Khokale "A NOVEL APPROACH FOR IDENTIFICATION OF UNAIDED PERSON USING FINGER PRINT IMPRESSION OR FACIAL RECOGNITION" Internation Journal for Science and Advance Research In Technology, 4(4)

[28] Prof. Swati R. Khokale, Ruchika R. Borade, Shweta S. Malpure, Pravin H. Pandit, Pitam D. Kumar."A Review on Fake News Detection with Machine Learning", Volume 9, Issue V, International Journal for Research in Applied Science and Engineering Technology (IJRASET) Page No: 960-962, ISSN : 2321-9653, www.ijraset.com IJRAR22A2365.pdf