# A Deep And Machine Learning Comparative Approach for Networks Intrusion Detection

Ali Raad Sameer
*Institute of Informatics and Communication*
University of Delhi
a.ra.ad.s0777@gmail.com

Osamah Mohammed Jasmim
*Institute of Informatics and Communication,*
University of Delhi
osamahmohammed@south.du.ac.in

Mohamed Omar Mohamed
*Institute of Informatics and Communication,*
University of Delhi
Mohedkhadar60@gmail.com

***Abstract* : Intrusion detection is intergral section of firewalls and other attacks prevention applications that works side by side with the attack pouncing section. The strongest attack prevention application is that of wide range of attack pouncing capability. Recently, data driven models are used for this task which offers the required capability of multiple type of attack detection. In this paper, foucse given to establish an attack detection system that compatible with various datasets and able to draw similar perfromacne in attack flection. Multilayer perception (MLP), Convolutional neural network (CNN). Machine learning algorithms are also deployed such as Random Forest (RF) and Boosting algorithms such as XGBoost, AdaBoost and CatBoost. The MLP algorithm was realized with best intrusion detection performance, it yielded a higher accuracy in both dataset cases. Overall, the classification results on the UNSW-NB15 dataset suggest that machine learning algorithms can be successfully applied to network intrusion detection tasks, with various algorithms demonstrating high levels of accuracy in distinguishing between normal and malicious network traffic.**

***Keywords: MLP, CNN, Intrusion, Boosting, UNSW-NB15, RF.***

## I. Introduction

There are a lot more traffic jams, crashes, and smog in cities where more people drive cars. There should be more cutting edge choices. Smart transportation systems (ITS) help places handle daily traffic, people, and big events better. For these features to work well, there needs to be a strong network that lets cars, sensors, and motors share data easily [1].

This is quick and easy to do with VANETs because they use technologies that let cars talk to each other without any help. There could be a lot of hubs but not many WiFi devices [2]. Things go badly, though, because the cars are going fast. It's tough to get the fastest speed on most home networks. Also, the way we talk to each other now is bad [3]. To do things like move cars from one piece of infrastructure to another, you need a lot of Road Side Units (RSUs). It costs a lot of money and doesn't help with anything. People worry about their safety and privacy when cars talk to each other (V2V) [4]. People can get information and do work at edge nodes that are close to them. You can do more with it and get answers faster [5]. As a stand-alone system, an Intrusion Detection System (IDS) can be set up in a number of different ways. Some people have said that cars could be used as edge nodes. Though there are many ideas for IDS-based VANET systems, there are still some problems [6]. For example, the network has more noise and low detection rates. Also, the False Positive Rates (FPR) are high. IDS that is based on oddities is better than IDS that is based on rules because it can find new threats whose paths haven't been found yet [7]. But safety tips could slow down your network. This research shows a way to find attacks on V2V transmission in ad hoc networks in cars that uses AI. It's meant to help with these problems. There is a fast false positive rate, a better false positive rate, and a low false negative rate in this smart IDS for the Internet of Vehicles. It keeps your information safe. You can pick more than one edge node if you don't want one to be too busy. TOPSIS means for Technique for Order Preference by Similarity to Ideal Solution. This is the name of the method. This makes sure that the network works well even when there are a lot of people around [8]. A lot of people use deep learning to find different kinds of problems in networks. In order to naturally find complex traits and finish hard classification tasks, deep learning models led by AI are much better than shallow learning models. There is deep learning that can be used in intrusion detection systems (IDS) [9]. This is news that AI fans will find interesting. The Generative Adversarial Network (GAN) is used by many to find bugs. There are two types of these ways: those that use an auto-encoder and those that use a GAN [10]. Autoencoders and reconstruction methods are often used together to find a "reconstruction error" that can tell the difference between normal and abnormal behavior. As one way to do this, you can teach an autoencoder with real data. After setting the input to the same, you can use their secret representation distribution to figure out what it is. When these samples have more fix mistakes than other samples, something is not right [11]. A number of studies used random analysis and Denoising Autoencoder (DAE) to get rid of noise that could slow things down. The Variational Autoencoder (VAE) method is said to help you find strange things. To get back the info that was lost, this is how the raw data is spread out. Autoencoders were used at first, but now there are GAN-based ways to find off-sets. These are used a lot in computer vision [12]. AnoGAN and f-AnoGAN were the first models on IDS that used GAN to get ideas. A decoder network was added before the generation network in f-AnoGAN to speed up the process. There are now two encoder networks, one for the new data and one for the old data. Things got even better after that. Pictures and intrusion detection datasets can have strange things in them. A good GAN method, like BiGAN, and inverse learning can help find these things. Adding a training step like an autoencoder to the BiGAN design that was already there was supposed to help the model settle down. IDS systems that look for strange behavior will work better and be more useful with this way [13]. This paper is proposing development of rubst malicious and intrusion detection attack detection. It proposes using deep learning stacks with various nature of attacks with various types of networks to get accurate detection.

This work is licensed under a Creative Commons Attribution-Noncommercial 4.0 International License

## II. Methodology

### *A. Problem Statement*

The development of communication networks imposed challenges related to the accommodation of users and privacy. Adhoc network is representing a simple wireless communication stack with cooperation routing bases. The data transmission in packets form from one node to another might face dropping due to nodes malicious activities. In this type of network, and due to its simple structure, the routing mechanism is merely depending on the node availability within the range of the other node. Thus, any third node can appear as receiver to the data and the sender node has no track to verify the destination node. Literature survey shown various contribution to develop the attack resistivity of the node. The use of artificial intelligence (AI) was one of the paramount concerns to protect the network from the malicious activities. The challenges involved in the AI based methods are represented by the accuracy of detection and the model ability to adapt the varying network environments.

### *B. Intrusion Detection*

An effective intrusion detection system (IDS) should provide several key benefits, including the ability to recognize various types of attacks, detect security incidents, and enforce controls over the network. A robust IDS aids in pinpointing bugs or issues within network device configurations.

MANETs need an intrusion detection system (IDS). IDS is available in two main types: anomaly IDS and misuse IDS. The misuse intrusion detection system (IDS), shown in Figure 2, has the capability to identify patterns of known assaults and therefore detect intrusions. However, it may lack the ability to identify novel or undiscovered attacks. Conversely, Anomaly IDS (illustrated in Fig. 2) operates by assessing normal system behavior, flagging deviations from this baseline as potential anomalies. However, it's worth noting that Anomaly IDS systems are also capable of detecting new attacks.

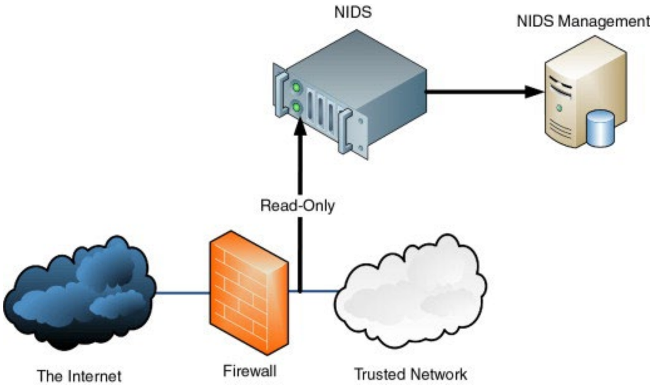

Fig. 1. intrusion attack prevention system consisting of firewall.

An important component of any cybersecurity configuration is an intrusion detection system (IDS), which monitors network or system operations and detects signs of malicious activity or violations of policies. The primary objective is to promptly detect and respond to any instances of misuse, irregularities, or illegal entry that may pose a risk to the security, confidentiality, or accessibility of data and resources. Host-based IDS (HIDS), hybrid IDS, and network-based IDS (NIDS) are only a few examples of the several types of intrusion detection systems (IDS). Network intrusion detection systems (NIDS) analyze network traffic to identify abnormal patterns or signatures, whether they occur inside critical components or at the edges of the network. The hybridization of network is allowing the network to be more combative to the malicious attacks. However, HIDS has a narrower scope since it concentrates on individual hosts or endpoints and detects signs of unauthorized access or intrusion by analyzing system logs, files, and settings. The hybridization of network is allowing the network to be more combative to the malicious attacks. Hybrid intrusion detection systems provide comprehensive security for both host and network configurations by integrating elements from both network-based intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). The hybridization of network is allowing the network to be more combative to the malicious attacks. IDS employs three distinct methods of detection: anomaly-based, behavior-based, and signature-based. Anomaly-based detection establishes a standard level of normal activity and identifies any deviations as potential intrusions, while signature-based detection matches recorded events with a database of recognized attack patterns or rules. Behavior-based detection identifies potentially suspicious activities by studying the actions and patterns shown by people and entities. The hybridization of network is allowing the network to be more combative to the malicious attacks.

Key components of IDS include sensors, analyzers, alerting systems, and response mechanisms. Sensors collect and monitor data from various sources, while analyzers process and analyze this data using detection algorithms. The alerting system generates alerts or notifications upon detecting suspicious activity, and response mechanisms may take automated or manual actions to mitigate threats. The hybridization of network is allowing the network to be more combative to the malicious attacks. Deployment options for IDS include inline IDS, which actively participates in network traffic flow, and passive IDS, which operates non-intrusively by analyzing copies of network traffic or logs. Distributed IDS utilizes multiple sensors or analyzers distributed across different network segments or hosts for comprehensive coverage. The hybridization of network is allowing the network to be more combative to the malicious attacks. However, IDS deployment comes with its own set of challenges, such as false positives, false negatives, scalability issues, and evasion techniques employed by attackers. Despite these challenges, IDS plays a critical role in enhancing visibility and proactive defense capabilities, thereby safeguarding organizations' digital assets and infrastructure against cybersecurity threats.

### *C. Dataset*

The NSL-KDD and UNSW_NB15 datasets were used for this experiment in intrusion detection. Past research suggests that the ISCX NSL-KDD dataset has the capability to address some limitations seen in the KDD'99 dataset [1]. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. Despite significant improvements, the NSL-KDD dataset may still have some issues highlighted by McHugh and may not provide an adequate representation of the complexities seen in actual networks. However, the NSL-KDD dataset remains a valuable resource for researchers seeking to evaluate and compare different intrusion detection techniques. This is crucial since there is a scarcity of publicly accessible datasets especially tailored for network-based intrusion detection systems (IDSs). The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. In addition, the

NSL-KDD dataset offers certain advantages as compared to the original KDD dataset. Significantly, it eliminates duplicate entries from the training set, hence preventing classifiers from exhibiting bias towards often occurring instances. In addition, the recommended test sets do not include any duplicated data, ensuring that the performance of learners will not be affected by strategies that are better at detecting common events. Furthermore, the dataset intentionally selects records from each difficulty level category in a manner that is inversely proportional to their occurrence rate in the original KDD dataset. This approach enhances the evaluation of different learning techniques by boosting the classification rates across many machine learning algorithms, resulting in a more comprehensive and precise assessment. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. Sampling minuscule sections at random is unnecessary given the abundant amount of items included in both the training and test sets of the NSL-KDD dataset. As a result, researchers may choose to conduct tests on the whole dataset, ensuring that the assessment results are reliable and can be compared across other research projects. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. The UNSW-NB15 dataset comprises unprocessed network packets generated by the Cyber Range Lab at UNSW Canberra using the IXIA PerfectStorm software. It mixes authentic contemporary actions with artificially produced sophisticated assault features. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. The tcpdump tool was used to collect this combined information, resulting in a 100 GB raw traffic dataset that was stored in Pcap files. The dataset comprises nine distinct attack techniques, including worms, reconnaissance, shellcode, denial of service (DoS), backdoors, sniffers, and fuzzers. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. Forty-nine characteristics with class labels were generated utilizing twelve algorithms and software tools including Argus and Bro-IDS. The file named UNSW-NB15_features.csv includes the following features. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. The dataset is divided into four CSV files, specifically labeled as UNSW-NB15_1.csv, UNSW-NB15_2.csv, UNSW-NB15_3.csv, and UNSW-NB15_4.csv. The collection has a grand total of 2,540,044 pieces. The file UNSW-NB15_GT.csv includes authentic data, whereas the file UNSW-NB15_LIST_EVENTS.csv documents the specifics of the events. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. The dataset has been partitioned into several training and testing sets for the purpose of conducting experiments. The training set is labeled as UNSW_NB15_training-set.csv, whereas the testing set is labeled as UNSW_NB15_testing-set.csv. The training set comprises 175,341 records, whereas the testing set has 82,332 data points. This dataset include both regular network operations and many types of cyber assaults. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications.

### *D. Preprocessing*

Data preprocessing is a crucial iterative procedure aimed at converting raw data into comprehensible and usable formats. Typically, raw datasets exhibit various shortcomings such as incompleteness, inconsistencies, erroneous entries, and missing values, rendering them unsuitable for direct analysis [37]. Therefore, preprocessing serves as a vital step to rectify these issues, ensuring the resultant dataset is reliable and conducive to effective knowledge discovery. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. In this paper, rigorous data preprocessing was undertaken to mitigate potential challenges inherent in raw datasets. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. Measures were implemented to address missing values, inconsistencies, and redundancies, thereby refining the dataset to a state more amenable for subsequent analysis and modeling. Notably, data gathering efforts were focused on eliminating out-of-range values and handling improbable data combinations, such as instances where demographic attributes like "Sex: Male" and "Pregnant: Yes" coexist. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. Ensuring that data is formatted appropriately for the intended machine-learning task is paramount at the outset of any project. The presence of irrelevant or noisy data can significantly impede model performance and hinder knowledge discovery efforts, underscoring the importance of meticulous data preparation and filtering. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. These preparatory steps, including cleaning, normalization, feature extraction, and selection, constitute a substantial portion of the time invested in a machine learning project, albeit their significance cannot be overstated. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. For instance, in image processing applications, preprocessing is fundamental for enhancing accuracy, especially in satellite imagery analysis where various environmental factors can distort data. Geometric and radiometric correction processes are indispensable for mitigating distortions arising from factors such as sensor variations, atmospheric conditions, and terrain effects [17, 18]. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications.

Furthermore, data transformation and feature extraction techniques play a pivotal role in optimizing classifier performance, ensuring that relevant features are extracted for a given task. This involves selecting pertinent features while filtering out extraneous information, thereby facilitating more meaningful analysis and model development. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications. Unsupervised learning algorithms like Principal Component Analysis (PCA) are commonly employed for feature extraction, enabling the identification of relevant patterns and structures within the data. Ultimately, the efficacy of data preprocessing lays the groundwork for subsequent analysis and modeling, facilitating more accurate and robust machine learning outcomes. The application of data sciences in the world of networking has large impact on the accuracy of malware and security applications.

### *E. Learning models*

Attacks in wireless ad hoc networks can be categorized based on their origin and nature. Internally, attackers may masquerade as normal nodes, manipulating packet delivery or routing paths, posing a significant threat [6]. Externally, attacks are generated by nodes outside the network, causing traffic congestion, spreading incorrect routing information, or even shutting down the network altogether. The attacks on the wireless network can be divided into two types namely passive and active attacks. Active assaults include several types of malicious activities, such as Man-in-the-Middle, black hole, denial of service (DoS), spoofing, eavesdropping, and wormhole attacks, involve direct interference with network protocols, causing significant damage. Passive attacks, on the other hand, involve listening to communication channels to gather information without disrupting protocol operations. The attacks on the wireless network can be divided into two types namely passive and active attacks. To safeguard against cyber-attacks, security techniques like cryptography, firewalls, and intrusion detection systems (IDS) are employed. Among these, intrusion detection is particularly effective in detecting and mitigating complex and dynamic intrusion scenarios [4]. Attack can be detected by monitoring the activates of the data packets, and due to the high density of packs information the task become even complex. The strategy of detection the attack can be established using deep learning algorithms. In this work, multilayer perception (MLP), Convolutional neural network (CNN). Machine learning algorithms are also deployed such as Random Forest (RF) and Boosting algorithms such as XGBoost, AdaBoost and CatBoost.

## III. Results and Discussions

### *A. Results of UNSW_NB15*

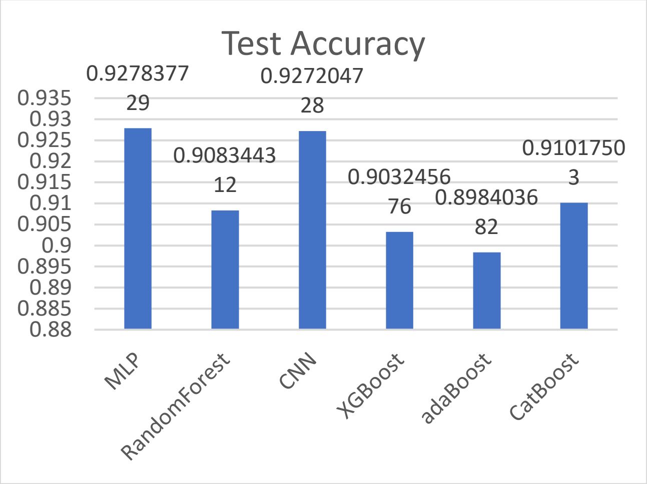

Fig. 2. graphical representation of performance metrics of the UNSW-NB15 dataset.

To discuss the results of the six algorithms used to classify the UNSW_NB15 dataset based on their test accuracy, we can analyze their performance and compare their strengths and weaknesses:

#### *1) MLP (Multilayer Perceptron)*

MLP achieved the highest test accuracy (0.927837729) among the six algorithms. This indicates that it effectively learned the underlying patterns in the dataset and made accurate predictions. MLP is known for its ability to handle complex relationships in data through multiple layers of neurons, which likely contributed to its high performance in this classification task. However, MLP's performance might be sensitive to hyperparameter tuning and dataset characteristics.

#### *2) Random Forest*

Random Forest performed slightly lower than MLP in terms of test accuracy (0.908344312) but still achieved a commendable accuracy score. RandomForest is an ensemble learning method based on decision trees, which are robust and versatile classifiers. Its performance might be attributed to its ability to handle both numerical and categorical data, as well as its capability to capture complex interactions between features.

#### *3) CNN (Convolutional Neural Network)*

CNN achieved a test accuracy (0.927204728) comparable to MLP, indicating its effectiveness in extracting relevant features from the dataset, particularly in image or sequence-based data. CNNs excel in capturing spatial and temporal dependencies in data, which might have been beneficial for this classification task. However, CNNs can be computationally intensive and require large amounts of data for training, which could affect their scalability.

#### *4) XGBoost*

XGBoost is a gradient boosting algorithm known for its efficiency and effectiveness (0.903245676) in handling structured/tabular data. While its test accuracy is slightly lower compared to MLP and CNN, XGBoost still performed well in the classification task. XGBoost's strength lies in its ability to handle missing data, feature interactions, and nonlinear relationships, making it a popular choice for various machine learning tasks.

#### *5) adaBoost*

adaBoost, short for Adaptive Boosting, is an ensemble learning technique that combines multiple weak classifiers to create a strong classifier. While its test accuracy is lower compared to other algorithms in this list, adaBoost is known for its ability to focus on difficult-to-classify instances and improve overall performance iteratively. However, adaBoost might be sensitive to noisy data and outliers. (0.898403682)

#### *6) CatBoost*

Discussion: CatBoost is a gradient boosting algorithm designed to handle categorical features efficiently. It achieved a test accuracy similar to RandomForest and slightly lower than MLP and CNN. CatBoost's strength lies in its ability to handle categorical data without the need for extensive preprocessing, making it suitable for datasets with mixed feature types. However, CatBoost might require longer training times compared to other algorithms. (0.91017503)

All six algorithms demonstrated good performance in classifying the UNSW_NB15 dataset, with MLP and CNN achieving the highest test accuracies. The choice of algorithm depends on various factors such as dataset characteristics, computational resources, interpretability, and specific requirements of the classification task.

### *B. Results of NSL-KDD*

Analyzing the classification performance of the six machine learning algorithms on the NSL-KDD dataset provides insights into their effectiveness in handling this particular dataset:

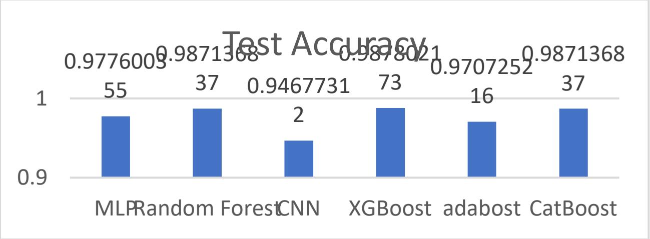

Fig. 3. graphical presentation of performance metrics of the NSL-KDD dataset.

### 1) *MLP (Multilayer Perceptron)*

MLP achieved a high test accuracy (0.977600355), indicating its capability to learn complex patterns within the NSL-KDD dataset. MLPs are known for their ability to handle non-linear relationships in data through multiple layers of neurons. The high test accuracy suggests that MLP effectively captured the underlying structure of the dataset and made accurate predictions. However, MLPs can be sensitive to hyperparameters and may require extensive tuning to achieve optimal performance.

### 2) *Random Forest*

Random Forest achieved the highest test accuracy (0.987136837) among the six algorithms, indicating its robustness and effectiveness in classifying the NSL-KDD dataset. Random Forests are ensemble learning methods based on decision trees, which are capable of handling both numerical and categorical data effectively. The high test accuracy suggests that Random Forest successfully captured the complex relationships and patterns in the dataset, making it a suitable choice for this classification task.

### 3) *CNN (Convolutional Neural Network)*

CNN achieved a slightly lower test accuracy (0.94677312) compared to MLP and Random Forest, but still performed well overall. CNNs are particularly effective for tasks involving image or sequence data, such as in computer vision or natural language processing. The lower test accuracy could be attributed to the complexity of training CNNs and the specific characteristics of the NSL-KDD dataset. However, CNNs are known for their ability to capture spatial and temporal dependencies in data, which could have contributed to their performance.

### 4) *XGBoost*

XGBoost achieved a high test accuracy similar to Random Forest (0.987802173), indicating its effectiveness in handling structured/tabular data like the NSL-KDD dataset. XGBoost is a gradient boosting algorithm known for its efficiency and scalability. The high test accuracy suggests that XGBoost successfully captured the complex relationships between features in the dataset and made accurate predictions. XGBoost's ability to handle missing data and feature interactions could have contributed to its performance.

### 5) *AdaBoost*

AdaBoost achieved a slightly lower test accuracy (0.970725216) compared to Random Forest and XGBoost but still performed well overall. AdaBoost is an ensemble learning technique that combines multiple weak classifiers to create a strong classifier. The lower test accuracy could be attributed to the sensitivity of AdaBoost to noisy data and outliers. However, AdaBoost's ability to focus on difficult-to-classify instances and iteratively improve performance could have contributed to its effectiveness in classifying the NSL-KDD dataset.

### 6) *CatBoost*

CatBoost achieved a high test accuracy (0.98713683) similar to Random Forest and XGBoost, indicating its effectiveness in handling categorical features in the NSL-KDD dataset. CatBoost is a gradient boosting algorithm designed to handle categorical data efficiently without the need for extensive preprocessing. The high test accuracy suggests that CatBoost successfully captured the complex relationships between features and made accurate predictions. However, CatBoost's training time could be longer compared to other algorithms due to its categorical feature handling capabilities.

All six algorithms demonstrated strong classification performance on the NSL-KDD dataset, with Random Forest, XGBoost, and CatBoost achieving the highest test accuracies. The choice of algorithm depends on various factors such as dataset characteristics, computational resources, and specific requirements of the classification task.

## IV. Conclusion

The classification results on the UNSW-NB15 dataset demonstrated that multiple machine learning algorithms, including MLP, RandomForest, CNN, XGBoost, adaBoost, and CatBoost, were able to achieve high test accuracies ranging from approximately 89% to 93%. This indicates that these algorithms are effective in classifying network traffic as normal or malicious with a high degree of accuracy. The classification results on the NSL-KDD dataset revealed that machine learning algorithms such as MLP, RandomForest, CNN, XGBoost, adaBoost, and CatBoost achieved high test accuracies ranging from approximately 94% to 99%. These results indicate the effectiveness of these algorithms in accurately classifying network traffic and detecting intrusions in the NSL-KDD dataset. The MLP algorithm was realized with best intrusion detection performance, it yielded a higher accuracy in both dataset cases. Preprocessing steps, such as handling missing values, addressing inconsistencies, and selecting relevant features, played a crucial role in improving the performance of the machine learning models on the UNSW-NB15 dataset. Additionally, the partitioning of the dataset into training and testing sets facilitated robust evaluation and comparison of different algorithms. Overall, the classification results on the UNSW-NB15 dataset suggest that machine learning algorithms can be successfully applied to network intrusion detection tasks, with various algorithms demonstrating high levels of accuracy in distinguishing between normal and malicious network traffic.

## References

[1] T.J. Nagalakshmi, A.K. Gnanasekar, G. Ramkumar, A. Sabarivani, Machine learning models to detect the blackhole attack in wireless adhoc network, Materials Today: Proceedings, Volume 47, Part 1, 2021

[2] Aimin Yang, Huixiang Liu, Yongjie Chen, Chunying Zhang, Ke Yang, Digital video intrusion intelligent detection method based on narrowband Internet of Things and its application, Image and Vision Computing, Volume 97, 2020

[3] Amritpal Singh, Pushpinder Kaur Chouhan, Gagangeet Singh Aujla, SecureFlow: Knowledge and data-driven ensemble for intrusion detection and dynamic rule configuration in software-defined IoT environment, Ad Hoc Networks, Volume 156, 2024

[4] Dharini N, Jeevaa Katiravan, Sruthi Priya D M, Sakthi Sneghaa V A, Intrusion Detection in Novel WSN-Leach Dos Attack Dataset using

Machine Learning based Boosting Algorithms, Procedia Computer Science, Volume 230, 2023

[5] T Raghavendra, M Anand, M Selvi, K Thangaramya, SVN Santhosh Kumar, A Kannan, An Intelligent RPL attack detection using Machine Learning-Based Intrusion Detection System for Internet of Things, Procedia Computer Science, Volume 215, 2022

[6] Jafar Haadi Jafarian, Amirreza Niakanlahiji, MultiRHM: Defeating multi-staged enterprise intrusion attacks through multi-dimensional and multi-parameter host identity anonymization, Computers & Security, Volume 124, 2023

[7] Snehal Deshmukh-Bhosale, Santosh S. Sonavane, A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things, Procedia Manufacturing, Volume 32, 2019

[8] E. Suresh Babu, C. Nagaraju, M.H.M. Krishna Prasad, Analysis of Secure Routing Protocol for Wireless Adhoc Networks Using Efficient DNA Based Cryptographic Mechanism, Procedia Computer Science, Volume 70, 2015

[9] Putty Srividya, Lavadya Nirmala Devi, A. Nageswar Rao, A trusted effective approach for forecasting the failure of data link and intrusion in wireless sensor networks, Theoretical Computer Science, Volume 941, 2023

[10] M.V.B. Murali Krishna M, C. Anbu Ananth, N. Krishnaraj, Detection of intrusions in clustered vehicle networks using invasive weed optimization using a deep wavelet neural networks, Measurement: Sensors, Volume 28, 2023

[11] Manjula C. Belavagi, Balachandra Muniyal, Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection, Procedia Computer Science, Volume 89, 2016,

[12] C. Edwin Singh, S. Maria Celestin Vigila, Fuzzy based intrusion detection system in MANET, Measurement: Sensors, Volume 26, 2023,

[13] Z. Chiba, N. Abghour, K. Moussaid, O. Lifandali, R. Kinta, A Deep Study of Novel Intrusion Detection Systems and Intrusion Prevention Systems for Internet of Things Networks, Procedia Computer Science, Volume 210, 2022.