Implementation and Comparison of various ML and Deep Learning Techniques for Network Intrusion Detection System

[1]Shreevatsa T P, [2]Radhika K R

[1]Student, [2]Professor
[1] Department of Information Science and Engineering,
[1]BMS College of Engineering, Bangalore, India

ABSTRACT - With the advent of internet to almost every walk of contemporary life, the need for internet security is ever increasing. The threat to the system can be a Denial-of-Service attack or a Worm attack or a Fuzzers attack and causing the integrity of the system to collapse or to compromise. Thus, to monitor the system network, Intrusion Detection System are extensively used in the cybersecurity domain. In order to detect attacks and subsequently thwart such future attacks, the project uses Machine Learning and Deep Learning algorithms to find and detect such attacks. The project is built on UNSW-NB15 (modern substitute to the well-known KDD99 Dataset) to analyze and classify normal and abnormal packets. The paper also sheds some light on few Machine Learning and Deep Learning Algorithms and makes a comparative study on them.

Index terms: Machine Learning Algorithms, Deep Learning, Intrusion Detection System

I. INTRODUCTION:

The word 'internet' has long become part of everyone's domestic and professional life, more so in the past two decades. Along with the dot-com boom, the internet became a basic commodity, initially to tech-companies, followed by private organizations and finally to the common man. It opened up a new front for all the sectors from medical industry to military, , entertainment to education, commercial business to government offices, banking system to gaming industry , agriculture to administration, logistics to infrastructure and so on.

The basic definition of internet is as follows: "The Internet is a vast network that connects computers all over the world". This definition shows that any person with a computer or an electronic device that is capable of computing can be used to connect other computer in the world. By an estimate, there are about 21.5 billion devices connected to the internet.

Unfortunately, internet has also become the medium to conduct attacks called cyber-attacks. Cyber Attack involves damaging or destroying a computer network or system. These attacks are carried out by an individual or by an organized cyber terrorist (local or foreign), simply called hackers. There are alleged instances of one country attacking the network and servers of another country to steal the sensitive data or to damage the reputation or even the very system of the victim country.

As the number and severity of these cyber-attacks increased day by day, the need for extremely sophisticated level of security for both servers and the network has increased tremendously. One such popularly in use security measure is Intrusion Detection System (IDS). As the name synonymous, the system detects the intrusion of the threats and attacks against the system. The traditional signature based IDS has now given way to the advanced derivations such as Machine Learning and Deep Learning algorithms.

The project implements the Machine Learning and Deep Learning algorithms based IDS and compares them in terms of its ability to classify the packet as valid (normal) or malicious (abnormal) packet (Binary Classification) and detect the type of attack (Multi-class Classification).

II. LITERATURE SURVEY:

The NSL-KDD dataset is utilized in one of the articles to implement the IDS utilizing Random Forest, XGBoost, and Decision Tree [2]. The work by Alenazi[1] uses a decision tree-based strategy with recursive feature elimination to choose pertinent and significant characteristics and employs the Local Outlier Factor (LOF) method to identify anomalous or outlier data. The next paper focuses on Collaborative IDS and describes the issue of Probe Response Attacks and how it is carried out. As a result, the author offers a defense against PRA which is termed as Shuffle-based PRA Mitigation (SPM) [6].

The M. H. Kamarudin paper [5] suggests an ensemble classification approach-based anomaly-based intrusion detection system to identify unknown attacks on web servers. To eliminate unnecessary data, a filter and wrapper selection technique is utilized. Then, logit boost is used as a weak classifier together with random forests.
The data sets do not accurately reflect network traffic and contemporary minimal footprint assaults for the current network threat environment. In order to address the lack of network benchmark data set, Jill's research [4] discusses the development of a UNSW-

NB15 data set. IXIA is a tool that can create both benign and harmful packet (Pcap) files. These packets are received and gathered by a server using the tcpdump utility [8]. The standard Kddcup99 dataset is used in the research [6] and is fed into a feedforward neural network method.

In a paper written by Jayant, port scan attempts are identified, and information on the machine from which port scan attempts were made is discovered. Using the distant computer's IP address, the following data is discovered. Operating System Detection, Traceroute Information, IP Address Location, etc. Angry IP, Nmap, and MegaPing were among the tools used to conduct the port scans [10].

III. PROPOSED SYSTEM:

The project's goal is to implement IDS using the fresh UNSW-NB15 dataset. The model is developed using a variety of Machine Learning and Deep Learning methods on the UNSW-NB15 dataset. Additionally, it contrasts the ML and DL algorithms. This project can be used as a springboard in the future to create a comprehensive real-time intrusion detection system and IPS.

In order to identify if a packet is malicious or legitimate, the project uses the concepts of machine learning and deep learning. The type of assault is classified using a multi-class classification model. Accuracy, F1-score, Error, and other metrics are used to compare the performance of the algorithms. The following models are created and compared algorithms: multi-layer perceptron, Restricted Boltzmann Classifier, Random Forest, Logistic Regression, K-Nearest Neighbor, and Long Short-Term Memory (LSTM).

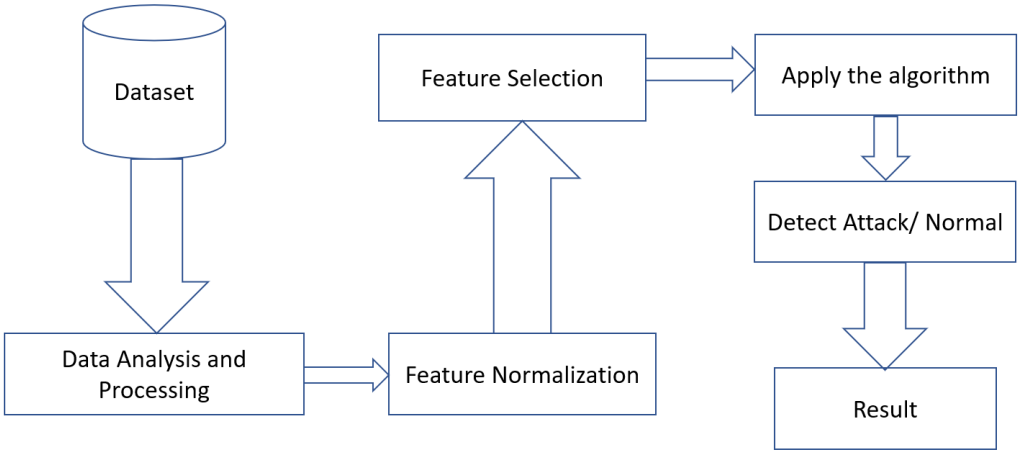

Fig. 1: IDS flow for Binary Classification

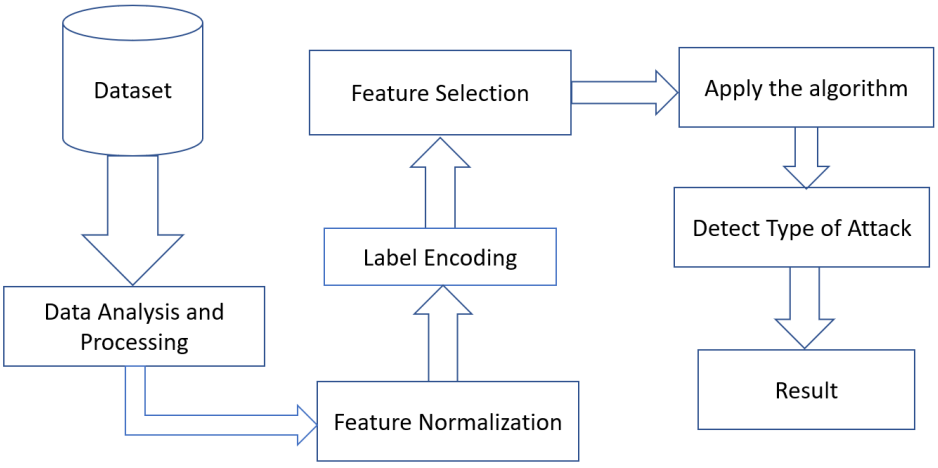

Fig. 2: IDS flow for Multi-class Classification

The dataset is initially analyzed and preprocessed, i.e., Exploratory analysis is performed to understand the data. The data is then normalized and scaled to transform the features into the same dimension. The data is encoded and all the categorical values are converted to numeric values as the machine learning algorithms don't work well with former type of data. Appropriate features with correlation(Pearson Coefficient) more than 0.3 are selected and unwanted features are dropped. The model is built on the cleaned dataset. The model is then saved for future reference as explained in Fig. 1. The model understands whether the given data is attack or not, for binary classification. After the system is trained, it is tested to check for accuracy, f1-score, variance, mean

squared error etc. The Fig. 2. depicts the design of the multi-class classification. The flow here is similar to that of the binary classification model, except in the final step the model classifies the packet according to the class of attack.

IV. IMPLEMENTATION:

The total number of the entries in the UNSW- NB15 dataset are 175341. But it contains considerable amount unknown(garbage) values, especially in service features, which makes the model to learn erratically if not resolved. Thus, those packets are discarded.

Data Visualization and Pre-processing:

After removing the rows of unknown(NaN) values, the dataset contains 48.66% of normal packets and 51.44% of abnormal packets. The abnormal packets are of type DoS, Fuzzers, Worms, Backdoor, Reconnaissance, Exploits, Analysis, Generic. The below pie chart provides the split of the same.

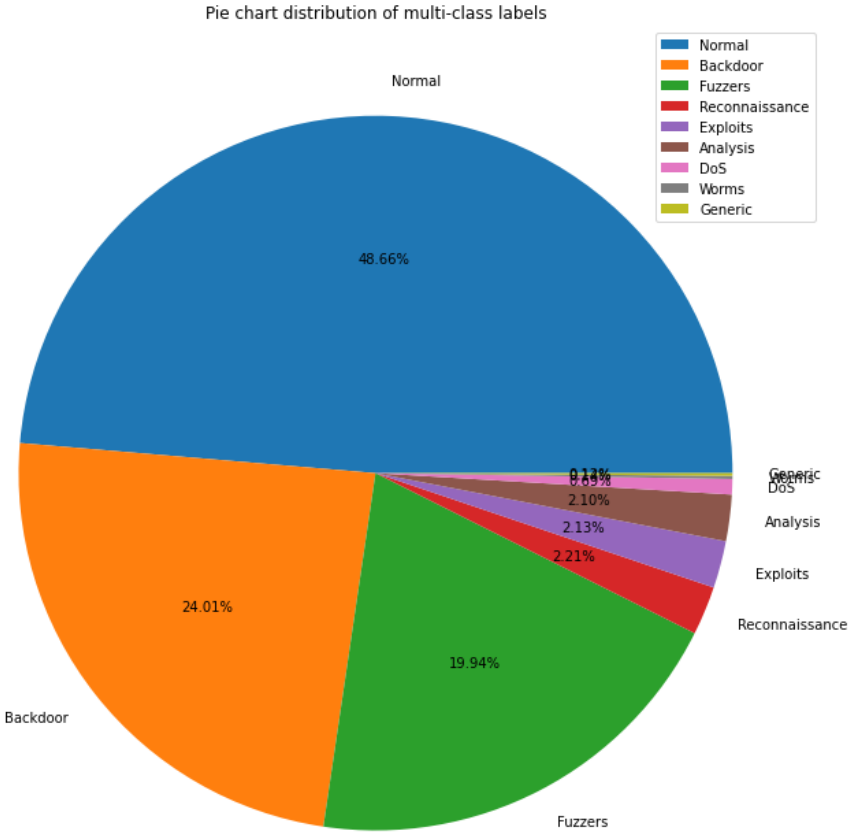

Fig. 4: Distribution of Normal and abnormal packets

One hot encoding:

The columns containing the categorical data is converted to numerical data which is the suitable input for Machine Learning. The columns such as prototype, service and state are converted from categorical data such as tcp, udp, ftp, snmp, FIN etc into binary values. Thus, the number of columns is increased from the initial 45 to 61.

Normalization:

After converting all the categorical data into numeric data, the data is ready to be normalized. MinMaxScaler is used to fit and transform the column values.

Label Encoding:

The label column which signifies, whether the packet is a normal or abnormal, is encoded with 1 and 0 respectively. Similarly, "attack_cat" column too is converted from categorical data to numerical data, i.e., categories like normal, worms, generic, fuzzers etc are assigned with numerical values like 1,2,3, etc.

Correlation Matrix:
The correlation matrix provides the insights of relationship between the features. If the matrix has correlation nearing to 1, then it is said to be called positively related and correlation value nearing -1, then it is said to be negatively related. If the correlation value is near to 0, then it is said that the features have no or very less relation.

Correlation Matrix for Binary Classification:
The heatmap in fig. 5, shows the relation between the features present on the x-axis and y-axis. The black colour shows the negative correlation between the features, indicating that with the increase of value in one feature is inversely proportional to the other features and vice-versa. The whitish colour represents the positive correlation between the features, indicating that with the increase of value in one feature is directly proportional to the other features. The reddish colour represents less correlation value, indicating no relation between them.

Feature Selection:
From the correlation matrix, the features having correlation value more than 0.3 is selected for both binary and multi class classification.

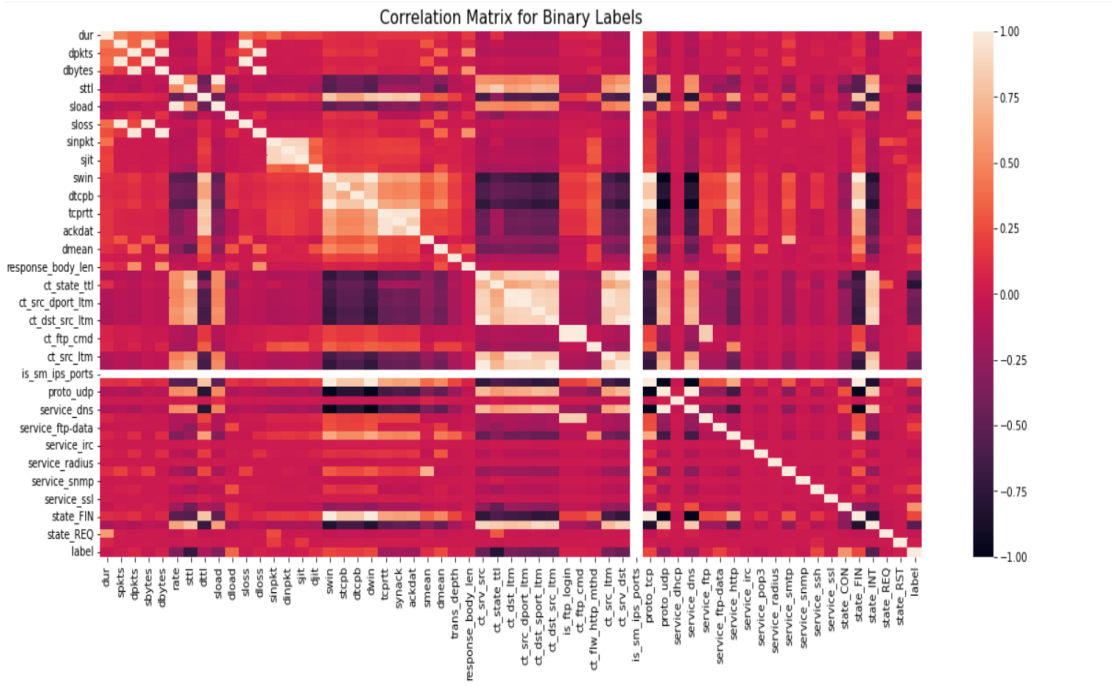

Fig. 5: Correlation Matrix for Binary Labels

Binary Data Classification:
The final dataset that is taken into account when building the model has 15 features, including rate, source time to live, source load, destination load, number for each state, according to a specific range of values for source/destination ttl, number of connections with the same service and same source IP, number of connections with the same source address, and the destination port in 100 connections.

Multi-class classification:
The final dataset that is taken into account when building the model includes 9 features, including the value of the Destination to Source Time to Live, the value of the Source TCP Window, the value of the Destination TCP Window, the round-trip time for TCP connection setup, the time for TCP connection setup, the time between acknowledgment and data packets, DNS services, and the type of protocol, which can be either TCP or UDP.

Oversampling:
Few of the attack classes in the dataset are very less than the required numbers, i.e., the dataset is imbalanced for multi-class classification. Thus, those data points belonging to the minority data class is oversampled to increase their number which ultimately helps to predict the classes properly.

V. RESULTS:

The accuracy and f1-score are used to measure the performance of the models. The accuracy may give wrong metric when the data set is imbalanced. Thus, this paper also measures the performance in terms of f1-score along with accuracy. The accuracy and f1-score are given by:

$$Accuracy = \frac{Number\ of\ correct\ predictions}{Number\ of\ Predictions} \qquad f1 - score = 2 * \frac{Recall * Precision}{Recall + Precision}$$

Table 1: Accuracy and f1-score of ML models for Binary Classification

Sl. No	Algorithms	Accuracy (%)	f1-score (%)
1.	Logistic Regression	97.70	95.06
2.	Support Vector Machine(SVM)	97.74	95.146
3.	Random Forest Classifier	98.52	96.92
4.	K- Nearest Neighbours	98.25	96.33
5.	Decision Tree	98.05	96
6.	Multilayer Perceptron	98.08	95.91
7.	Restricted Boltzmann Classifier	97.58	94.84
8.	LSTM	96.65	94.35

The accuracy and the F1-score of the algorithms for the binary classification are provided in the Table 1. All the algorithms provided excellent accuracy against the testing data. The Random Forest and Decision Tree classifiers provided highest performance, lowest Mean Absolute Error, Mean Squared Error, Root Mean Squared Error loss when compared to the other algorithms.

Table 2: Accuracy and f1-score of ML models for Multi-class Classification

Sl. No	Algorithms	Accuracy (%)	f1-score (%)
1.	Logistic Regression	88.88	86.28
2.	Support Vector Machine(SVM)	90.07	87.36
3.	Random Forest Classifier	89.20	87.69
4.	K- Nearest Neighbours	88.94	87.35
5.	Decision Tree	85.55	85.47
6.	Multilayer Perceptron	90.18	87.61
7.	Restricted Boltzmann Classifier	89.98	87.35
8.	LSTM	89.69	86.93

For the multi-class classification, all the algorithms provided good accuracy against the testing data. The multilayer perceptron and SVM classifiers provided highest performance amongst the deep learning and machine learning algorithms respectively. The time to build the model for multiclass classification is considerably more when compared to its binary counterpart.

VI. CONCLUSION:

The project develops a model to identify and categorise the type of packet and compares method performance metrics for the UNSW-NB15 dataset, including accuracy, f1-score, mean squared error, and others.The machine learning and deep learning algorithms successfully identified and classified the kind of packet after developing the model and testing it. Deep learning algorithms like Multilayer Perceptron, LSTM, and Restricted Boltzmann, as well as machine learning algorithms like Logistic Regression, Linear Support Vector Machine, Random Forest, Decision Tree, and Linear Support Vector Machine, were able to predict with the highest degree of accuracy for Binary classification. A high level of accuracy and f1-score are also provided by the prediction for multi-class classification.

Future Scope: By offering a greater quantum of attack, the performance of the multi-class classification algorithms can continue to improve data. One of the cyber-security areas with enormous potential is NIDS employing machine learning, and this project offers comparison information for the ML models of the algorithms. To further enhance Intrusion Prevention System and create a real-time system, the aforementioned models can be utilised as a benchmark.

References:

1. Alzahrani, A.O.; Alenazi, M.J.F. Designing a Network Intrusion Detection System Based on Machine Learning foSoftware-Defineded Networks. Future Internet 2021, 13, 111. https://doi.org/10.3390/fi 13050111
2. Thomas Rincy N 1 and Roopam Gupta, Design and Development of an Efficient Network Intrusion Detection System Using Machine Learning Techniques, Hindawi Wireless Communications and Mobile Computing Volume 2021, Article ID 9974270, 35 pages https://doi.org/10.1155/2021/9974270
3.Ahmad, Zeeshan; Shahid Khan, Adnan; Wai Shiang, Cheah; Abdullah, Johari; Ahmad, Farhan (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, (), –. doi:10.1002/ett.4150.
4. Liu, Hongyu; Lang, Bo (2019). Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. Applied Sciences, 9(20), 4396–. doi:10.3390/app9204396
5.M. H. Kamarudin, C. Maple, T. Watson and N. S. Safa, "A LogitBoost-Based Algorithm for Detecting Known and Unknown Web Attacks," in IEEE Access, vol. 5, pp. 26190-26200, 2017, doi: 10.1109/ACCESS.2017.2766844.
6. Vasilomanolakis, Emmanouil; Sharief, Noorulla; Muhlhauser, Max (2017). [IEEE 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) - Lisbon, Portugal (2017.5.8-2017.5.12)] 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) - Defending against Probe-Response Attacks. , (), 1046–1051. doi:10.23919/inm.2017.7987436
7. Hamit Erdem, Atilla Özgür, (2017), A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015
8. Moustafa, Nour; Slay, Jill (2015). [IEEE 2015 Military Communications and Information Systems Conference (MilCIS) - Canberra, Australia (2015.11.10-2015.11.12)] 2015 Military Communications and Information Systems Conference (MilCIS) - UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). , (), 1–6. doi:10.1109/MilCIS.2015.7348942
9.Iftikhar Ahmad, Azween B Abdullah Perak, Abdullah S Alghamdi, “Applying Neural Network to U2R Attacks”, 2010 IEEE Symposium on Industrial Electronics and Applications (ISIEA 2010), October 3-5, 2010, Penang, Malaysia
10. Gadge, Jayant; Patil, Anish Anand (2008). [IEEE 2008 16th IEEE International Conference on Networks - New Delhi, India (2008.12.12-2008.12.14)] 2008 16th IEEE International Conference on Networks - Port scan detection. , (), 1–6. doi:10.1109/icon.2008.4772622
11. Douligeris, C.; Mitrokotsa, A. (2004). [IEEE Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology - Darmstadt, Germany (14-17 Dec. 2003)] Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No.03EX795) - DDoS attacks and defense mechanisms: a classification. , (), 190–193. doi:10.1109/isspit.2003.1341