MACHINE LEARNING TO DETECT MALICIOUS NETWORK ACTIVITY

Sadhvi Selvaraj (RA1911043010007), Spandana Shree (RA1911043010010),
Anoushka Singh (RA1911043010027), Dr. A. Ruhan Bevi (Associate Professor)
Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Kattankulathur

INTRODUCTION/ABSTRACT

Analyzing networks has improved in the intrusion detection system (IDS) field. In network intrusion detection malicious research, one popular strategy for finding attacks is monitoring a network's activity for anomalies: deviations from profiles of normality previously learned from benign traffic, typically identified using tools borrowed from the machine learning community. Anomaly detection systems find deviations from expected behavior. Based on a notion of normal activity, they report deviations from that profile as alerts. The basic assumption underlying any anomaly detection system—malicious activity exhibits characteristics not observed in normal usage Furthermore, network traffic nowadays is mainly being encrypted for communication security and privacy, and only very few datasets reflect this situation. The process starts with capturing traffic either as a packet or flow from the internet.

MOTIVATION

- The objective of the project is to classify the network data points as malicious or benign
- Real-world implementation of the IDS will help us prevent from suspicious activity and facilitate safer communication within a network
- Detect and stop attacks on the infrastructure ahead of any serious damage or loss of data

OBJECTIVE

- The objective is to detect such malicious network traffic to alleviate their impact on organizations and provide security administrators with automatic alerts
- This work addresses the issue of malicious network traffic detection using deep convolutional neural network architectures on the modern complex and challenging dataset.
- The system can detect, classify, and generate alarms for abnormal traffic in the network, with a lower false alarm rate. Based on the dataset , we tested the binary classification of network traffic.

REALISTIC CONSTRAINTS

- Flexibility of Internet is essential for the detection
- User information access is required from the user
- High speed should be available.

METHODOLOGY

1. Data Pre-Processing

The dataset needs to undergo a cleaning process to eliminate any duplicate entries. Since the dataset comprises both numerical and non-numerical data, it requires a pre-processing step. Although the classifier in sci-kit-learn works well with numerical inputs, a one-of-K or one-hot encoding approach is used to make the necessary changes.

2. Feature Scaling

Feature scaling is a crucial aspect of machine learning methods. It helps avoid the issue of features with large values that may heavily impact the final results. To address this, for each feature, compute the average, subtract the mean value from the feature value, and divide the outcome by their standard deviation. After scaling, every feature will have a zero average and standard deviation of one.

3. Feature Extraction

The process of feature selection is a smart way to eliminate any redundant or unnecessary data. It involves selecting only the most relevant features that represent the problem effectively while minimizing presentation loss.

4. Split-validation evaluation

This evaluation method breaks down the dataset into two parts - one for testing and the other for training. After fitting the ML model in the memory and training it using another method, the accuracy of the model is determined by computing the confusion matrix, which consists of four values. The True Positive (TP) represents the number of observations that are positive and predicted to be positive, while the True Negative (TN) indicates the number of observations that are positive and predicted to be negative. The False Positive (FP) represents the number of observations that are negative but predicted to be positive, and the False Negative (FN) represents the number of observations that are positive but predicted to be negative.

BLOCK DIAGRAM

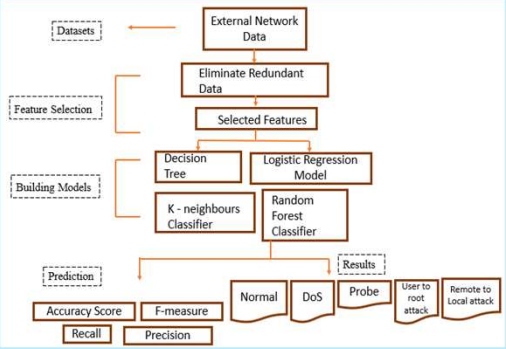


TABLE & METRICS

In terms of measurement, accuracy and precision are two important concepts. Accuracy is the degree of proximity between the measured value and the actual measurement of the object. On the other hand, precision refers to the consistency of multiple measurements of the same object, irrespective of the actual measurement of the object.

$$Accuracy = \frac{(TN + TP)}{(TN + FP + FN + TP)}$$

$$Precision = \frac{TP}{(TP + FP)}$$

$$Recall = \frac{TP}{(TP + FN)}$$

$$F\text{-}measure = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

TABLE I CYBER ATTACK PERFORMANCE MATRIX

Attack	*Accuracy*	*Precision*	*Recall*	*F-Measure*
DoS	99.7	99.6	99.7	99.6
Probe	99.6	99.4	99.3	99.3
R2L	99.8	97.0	99.3	99.3
U2R	97.9	97.1	97.0	97.0

Table 2 presents the important characteristics after a recursive feature removal was conducted on the dataset. Feature retrieval is based on rank.

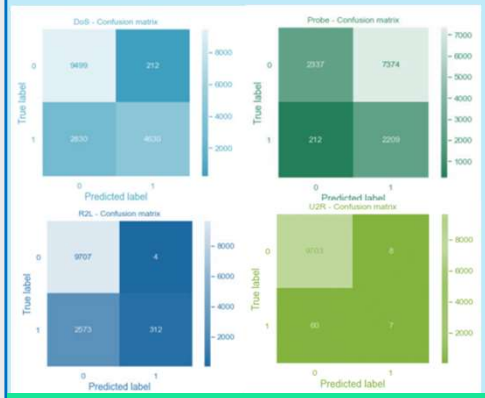
TABLE II REVELANT FEATURES

Target	Features Selected
Denial of Service attack	'log_in', 'count', 'ser_error_rate', 'srv_ser_error_rate', 'same_srv_rate', 'dest_host_count', 'dest_host_srv_count', 'dest_host_same_srv_rate', 'dest_host_ser_error_rate', 'dest_host_srv_ser_error_rate', 'service_http', 'S0_Flag', 'SF_Flag
Probe attack	'log_in', 'rej_error_rate', 'srv_rej_error_rate', 'dest_host_srv_count', 'dest_host_diff_srv_rate', 'dest_host_same_source_port_rate', 'dest_host_srv_diff_host_rate', 'dest_host_rej_error_rate', 'dest_host_srv_rej_error_rate', 'Protocol_icmp', 'service_eco_i', 'service_priv', 'SF_Flag'
Root to Local attack	'source_bytes', 'dest_bytes', 'hot', 'no_of_failed_logins', 'guest_login', 'dest_host_srv_count', 'dest_host_same_source_port_rate', 'dest_host_srv_diff_host_rate', 'ftp_service', 'ftp_service', 'http_service', 'imap4_service', 'RSTO_Flag'
User to Local escalation	'urgent', 'hot', 'root_shell', 'no_of_file_creations', 'no_of_shells', 'srv_diff_host_rate', 'dest_host_count', 'dest_host_srv_count', 'dest_host_same_source_port_rate', 'dest_host_srv_diff_host_rate', 'ftp_service', http_service', telnet_service'

ENGINEERING STANDARDS

- Open CV / Computer Vision- IEEE 2671-2022
- ISO/IEC 23053: Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)

RESULT



CONCLUSION

The purpose of modelling an IDS, demonstrates the significance of utilizing a suitable classification learning algorithm in conjunction with a set of relevant features. Using a decision tree classifier to find important features, a method for selecting features that combine univariate feature selection with recursive feature elimination has been presented and proposed. This procedure repeatedly builds a model by putting the feature aside and then continuing with the other features until all of the features in the dataset are used up. Various classification metric measurements were used to assess the method's efficacy, and it was found that reducing the number of features increased the model's accuracy. The accuracy of the feature selection method proposed in this paper was high, and features were identified using a ranking and information gain technique.

REFERENCES

1. Andrey Ferriyan, Keiji Takeda, Jun Murai. "*Generating Network Intrusion Detection Dataset Based on Real and Encrypted Synthetic Attack Traffic*", August 2021.
2. Robin Sommer, Vern Paxson. "*Outside the Closed World: On Using Machine Learning For Network Intrusion Detection.*"
3. Amirah Alshammari, Abdulaziz Aldribi. "*Apply machine learning techniques to detect malicious network traffic in cloud computing*", July 2021.
4. Xiaoyang Liu, Jiamiao Liu. "*Malicious traffic detection combined deep neural network with hierarchical attention mechanism*". July 2021.

CONFERENCE /JOURNAL PUBLICATION

ICCET 2023

11TH INTERNATIONAL CONFERENCE ON CONTEMPORARY ENGINEERING AND TECHNOLOGY , MAY 1ST -2ND, 2023