Machine Learning Based IoT Network Intrusion Detection Classification

Harshil Patel & Yuesheng Chen

Ohio State University, USA

4-2-2020

Motivation

F Forbes

Putin's Secret Intelligence Agency Hacked: Dangerous New 'Cyber Weapons' Now Exposed

This one has exposed "a new weapon ordered by the security service," one that can execute cyber attacks on the Internet of Things (IoT)—the ...

3 days ago

SB SecurityBrief Australia

IoT devices more at risk of cyber attack than ever - report

Increasingly, malware is being used to enable attackers to run malicious code to conduct new attacks. This is becoming the new focus of cyber ...

1 week ago

EC Express Computer (press release) (blog)

3 Ways to Protect IoT Smart Home Appliances from Cyber Attacks

Though prevalent in our lives, securing these devices from cyber-attacks is still a major challenge technologists and manufacturers face.

1 month ago

Traditional Security Solutions

IoT traditional network security solutions may not be directly applicable due to the differences in IoT structure and behavior.

Low Operating Energy

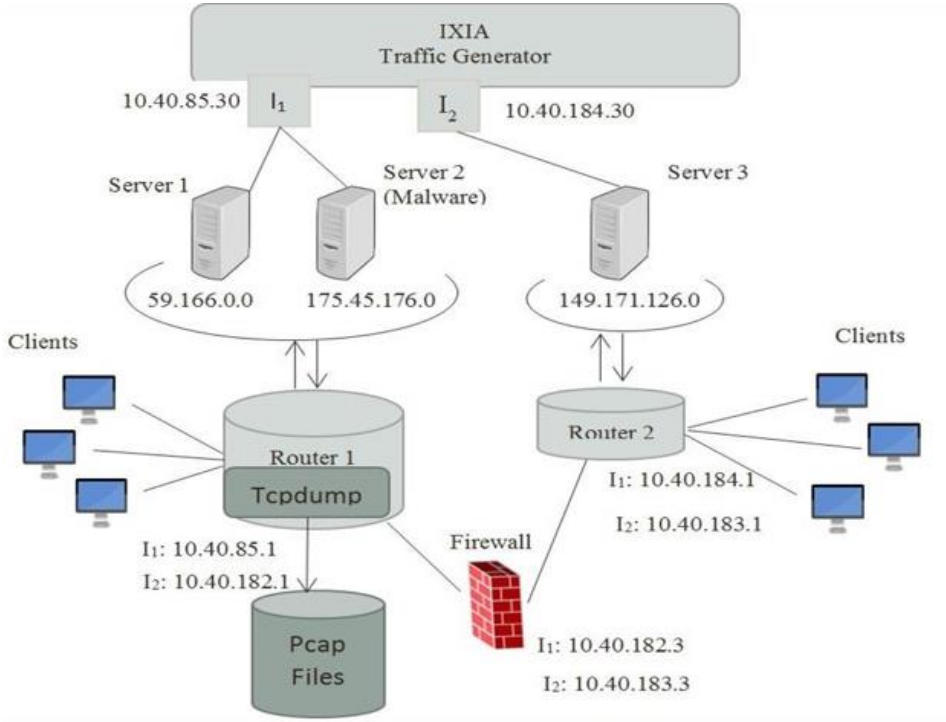
Low operating energy and minimal computational capabilities. Therefore security mechanism such as encryption protocols and authentication can not be directly applied.

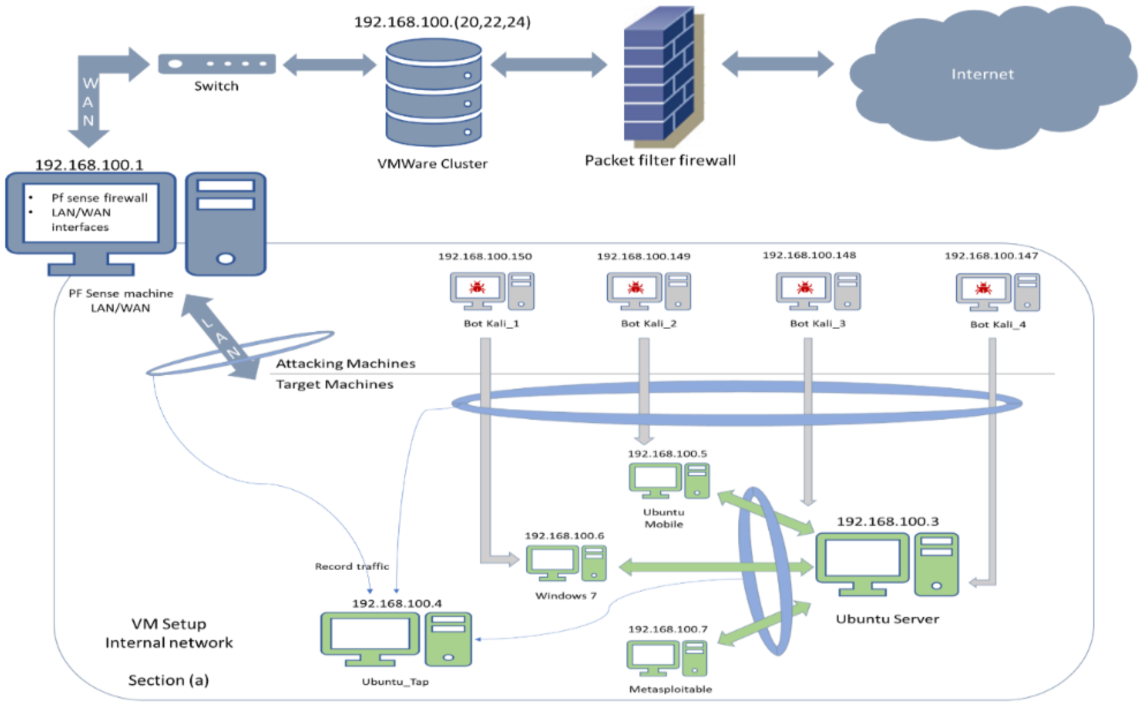
IoT Architecture

The lack of a single standard for IoT architecture.
IoT systems may have different policies, and connectivity domains.

IoT networks have become an increasingly valuable target of malicious attacks due to the increased amount of valuable user data they contain. In response, network intrusion detection systems have been developed to detect suspicious network activity.

UNSW-NB15 DATASET





UNSW-NB15 is an IoT-based network traffic data set with different categories for normal activities and malicious attack behaviors.

Methodology

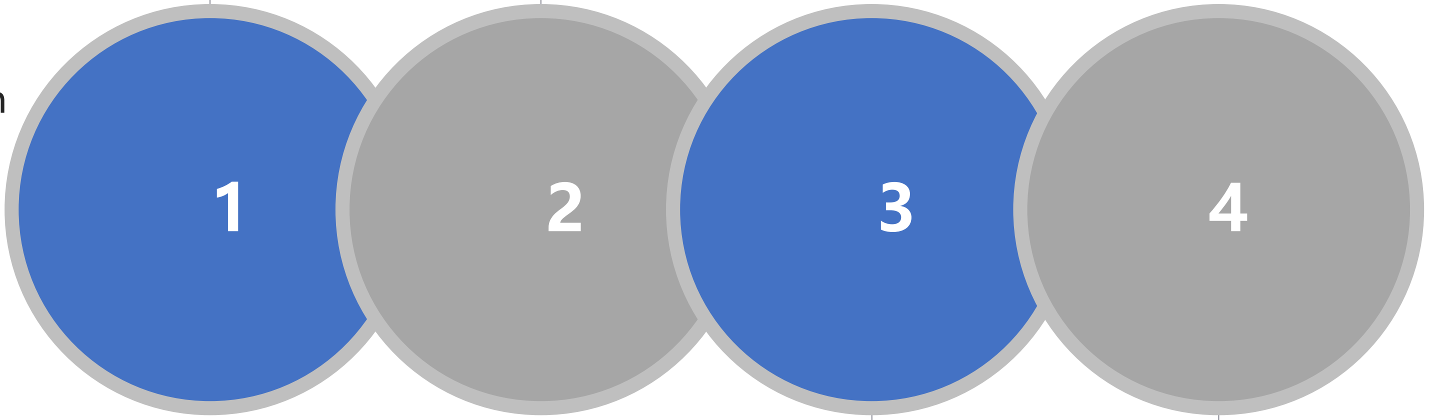
Data Preprocessing

CSV processed with:

1-Pandas, NumPy, skitLearn
2-Remove NaN`s
3-Training & Testing
4-Encoding Transformation

Response Features

1 -Attack or Normal
2 –Attack Classification



Model Selection

ML algorithms:

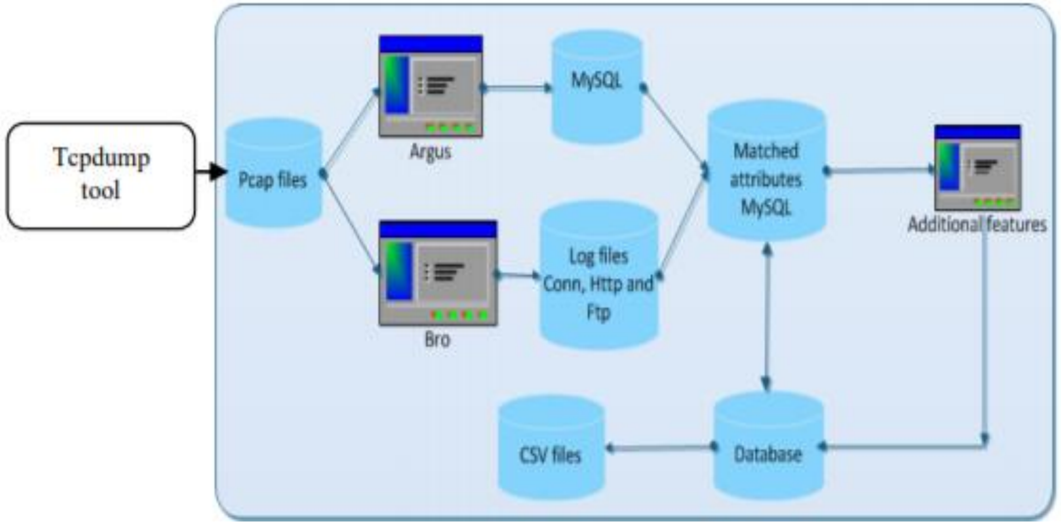
1-Logistic Regression
2-Descion Trees
3-Random Forests
4-Multi-Layer Perceptron Classifier

Model Comparison & Inspection

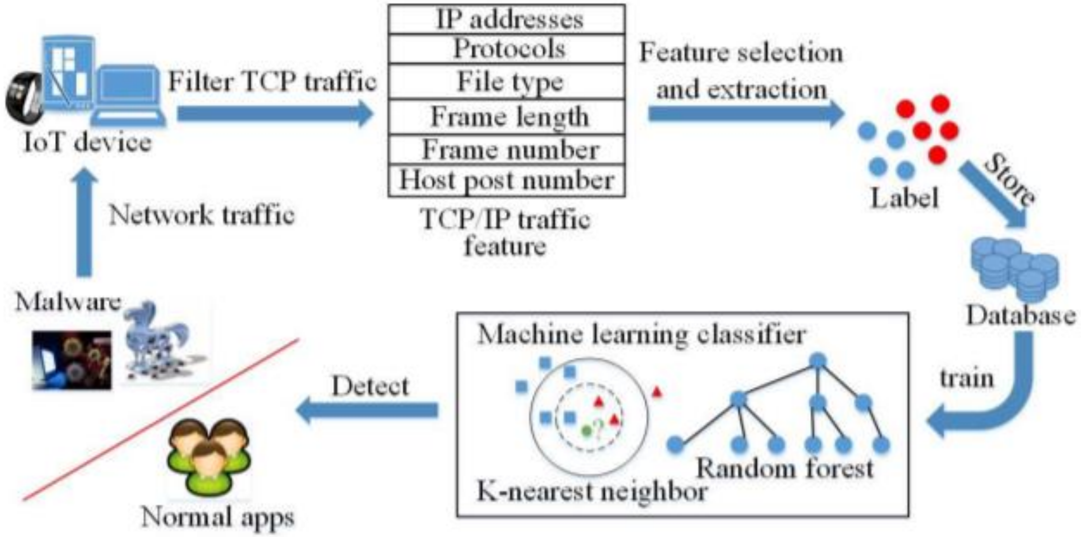
Determine which model should be used to classify category attacks and network intrusions on IoT networks. Also discover relevant features for model inspection.

Overall Architecture

Training Data → Model Hyperparameters → Model Training → Testing Data → Model Evaluation & Metrics → Model Selection



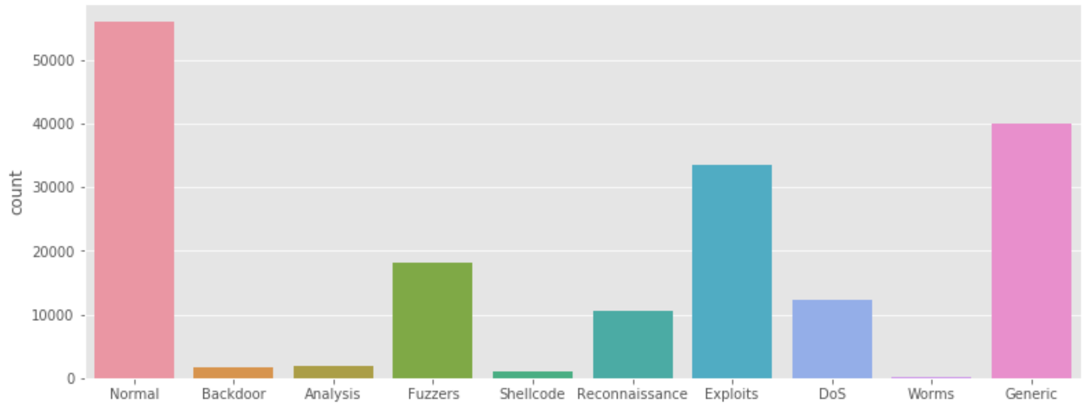
Collecting features of botnet data



Model Comparison

Attack Type Classification

This dataset has nine types of attacks: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms.



	Model Name	CV Fit Time	CV Accuracy mean	CV Precision mean	CV Recall mean	CV F1 mean	Test Accuracy	Test Precision	Test Recall	Test F1
2	RandomForest	30.531478	0.828141	0.828141	0.828141	0.828141	0.756255	0.756255	0.756255	0.756255
1	DecisionTree	2.441377	0.809594	0.809594	0.809594	0.809594	0.738935	0.738935	0.738935	0.738935
0	MultiLayerPerceptron	285.845018	0.809275	0.809275	0.809275	0.809275	0.707125	0.707125	0.707125	0.707125
0	LogisticRegression	81.868670	0.739262	0.739262	0.739262	0.739262	0.633338	0.633338	0.633338	0.633338

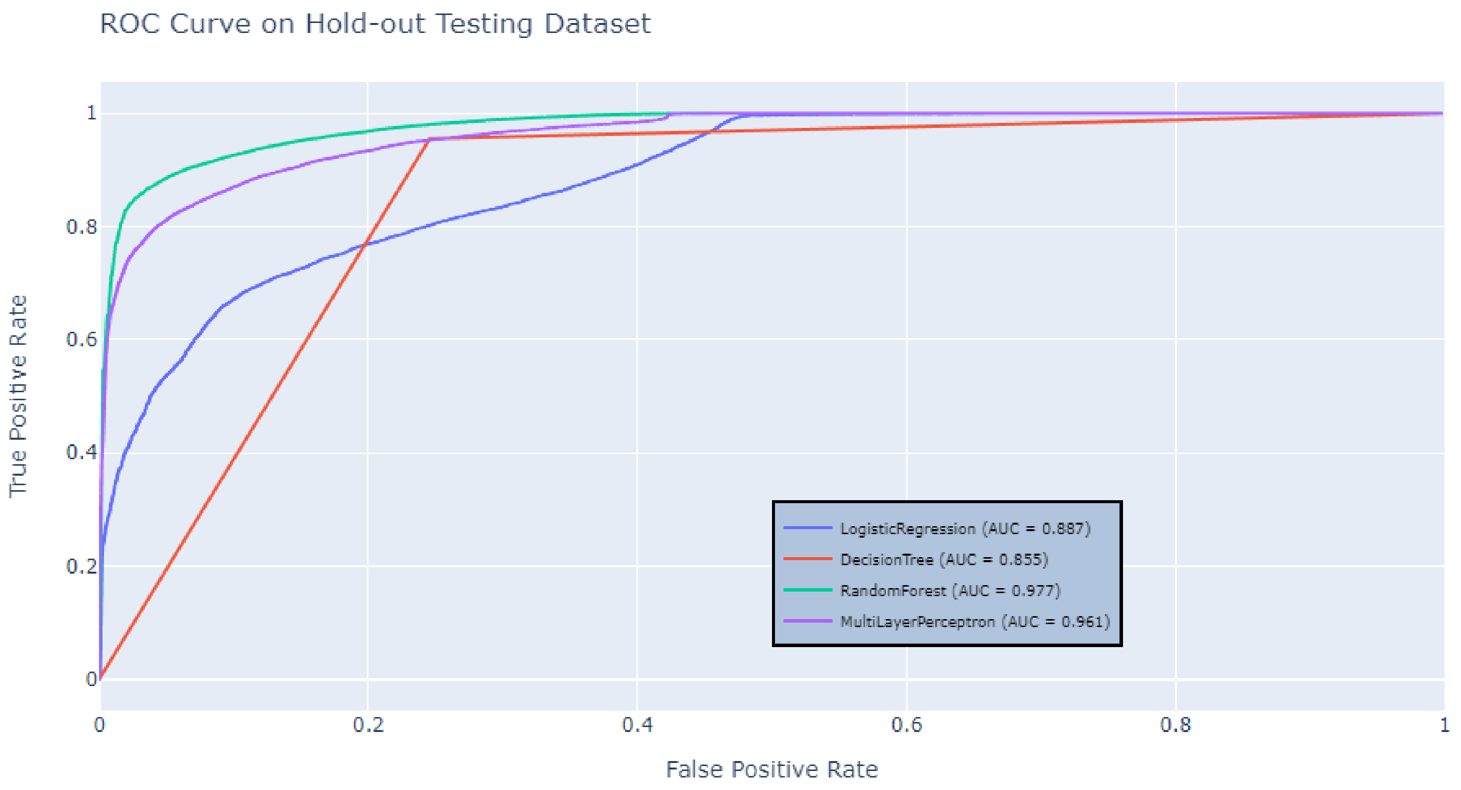
F1 score (weighted average of the precision and recall) is the primary evaluation metric on testing data to show the performance of the trained model. The Random Forest model marginally outperformed the other model.

Additionally, through tuning hyperparameters of Multi-Layer Perceptron and Decision Tree models, they could also perform better.

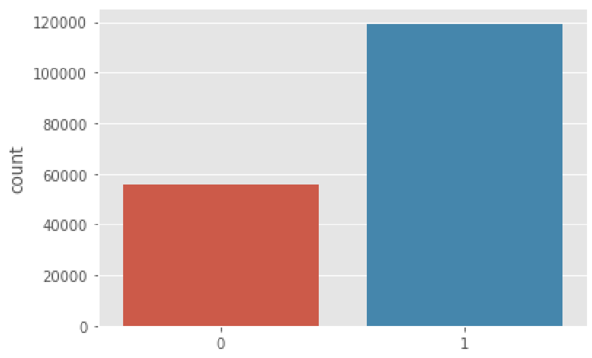
Model Comparison

Attack (1) or Normal (0) Classification (Binary)

	Model Name	CV Fit Time	CV Accuracy mean	CV Precision mean	CV Recall mean	CV F1 mean	CV AUC mean	Test Accuracy	Test Precision	Test Recall	Test F1	Test AUC
2	RandomForest	20.494558	0.959736	0.963049	0.978381	0.970654	0.993565	0.870731	0.818020	0.984161	0.893433	0.977035
1	DecisionTree	1.580191	0.948552	0.962916	0.961438	0.962176	0.942744	0.862605	0.823384	0.955396	0.884491	0.854642
3	MultiLayerPerceptron	131.505321	0.947234	0.955504	0.967664	0.961482	0.990262	0.856228	0.813078	0.959455	0.880223	0.960827
0	LogisticRegression	5.963249	0.927416	0.912978	0.987481	0.948769	0.969047	0.774498	0.728317	0.941741	0.821391	0.886548



The class ratio for the original data: 0.5:1 (56000/119341)

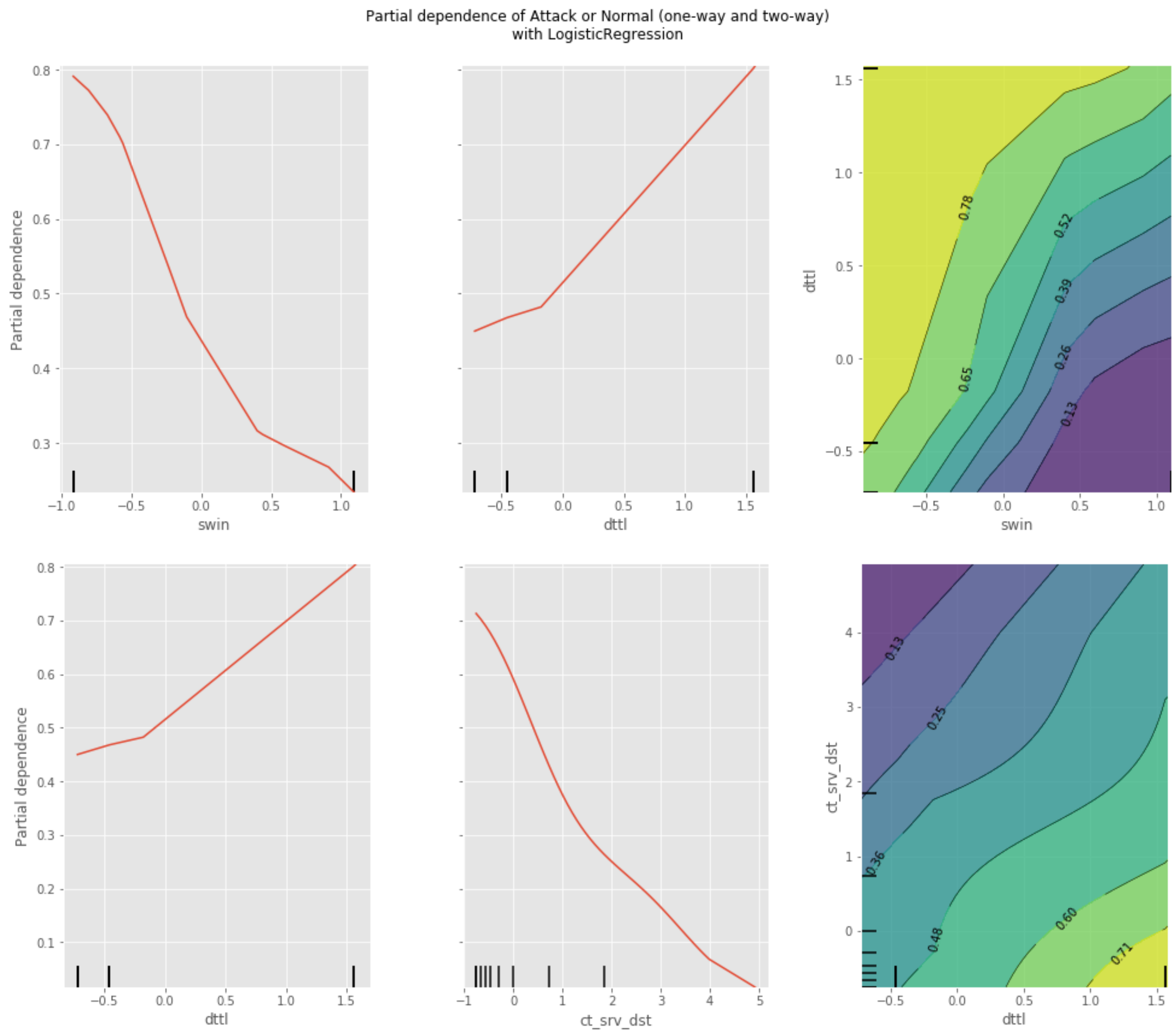


F1 score (weighted average of the precision and recall) is the primary evaluation metric on testing data to show the performance of the trained model.

The Random Forest model marginally outperformed the other model.

Model Inspection

Attack (1) or Normal (0) Classification (Binary)

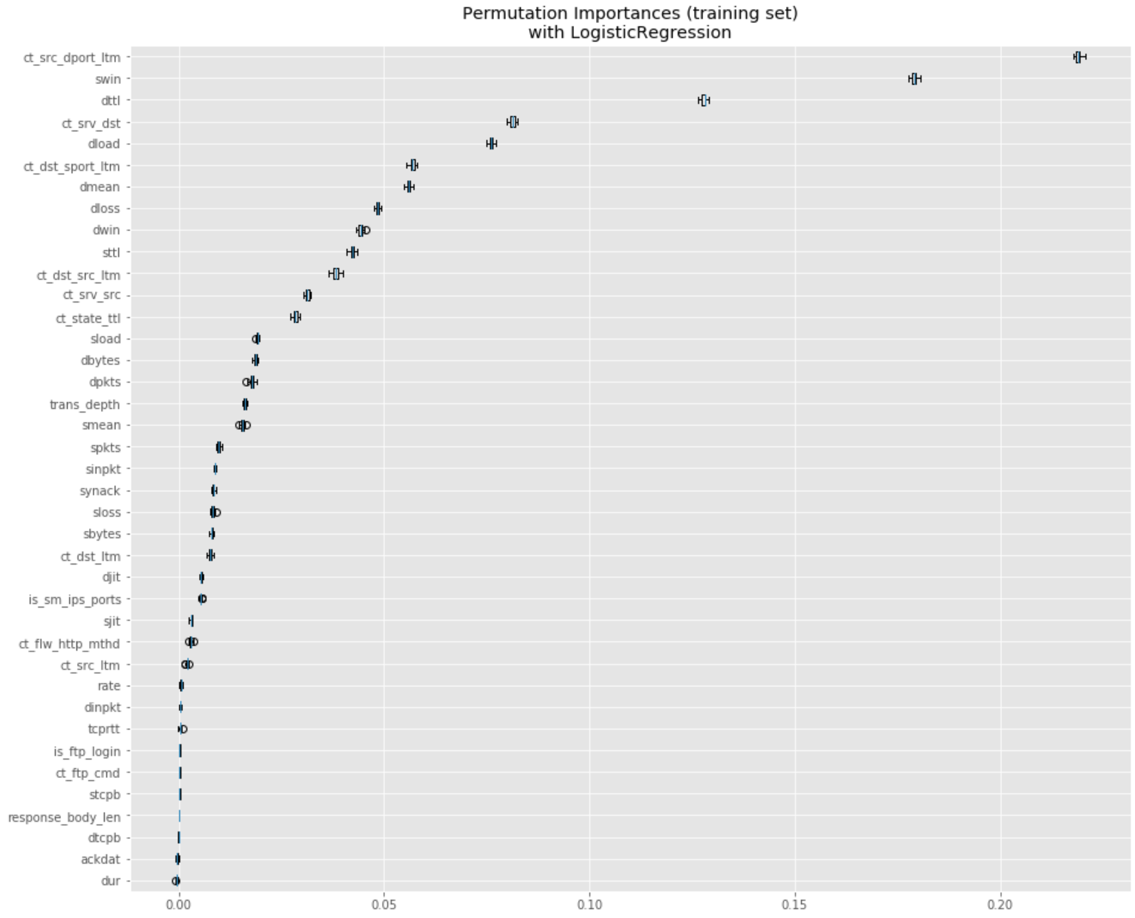


Created partial dependence plots (PDPs) for all 'target' features, that show the dependence between the target response of 1 and target' feature.

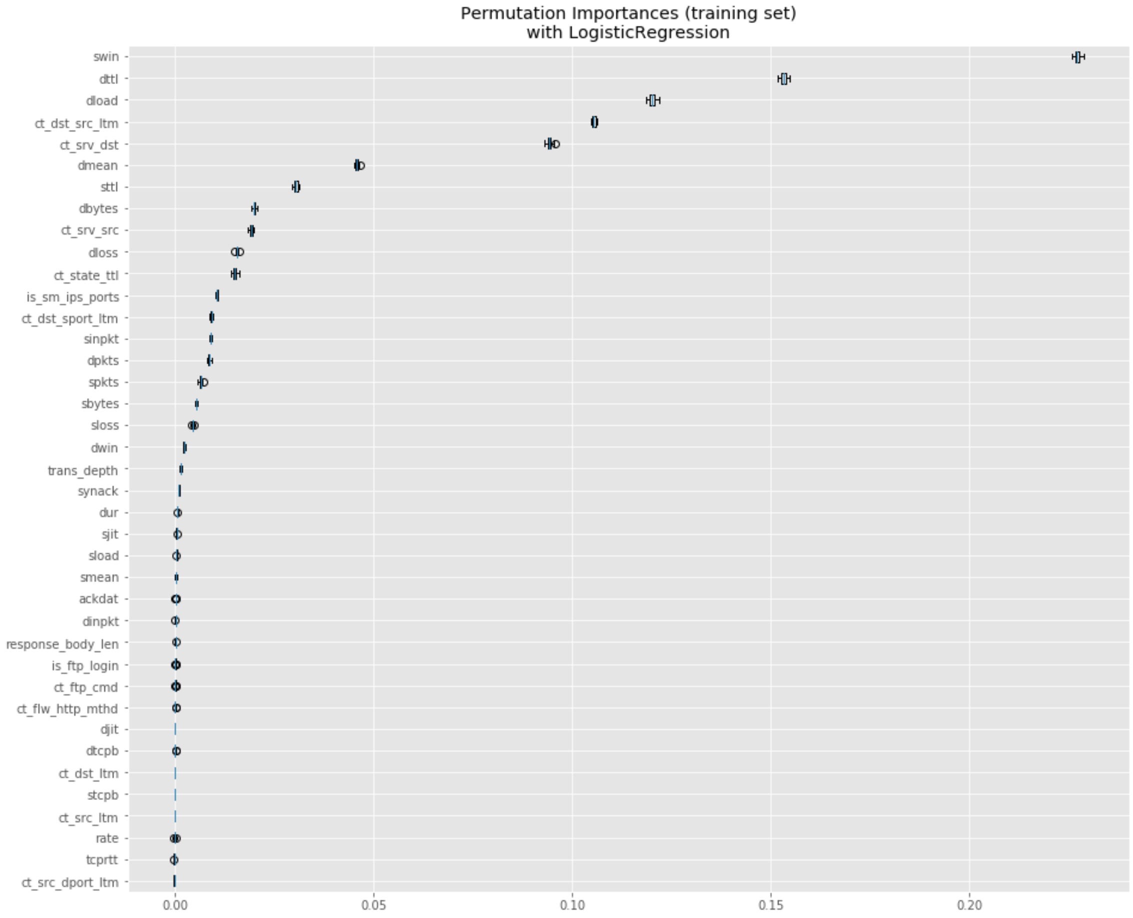
Features including 'swin', 'dttl', and 'ct_srv_dst' were of high dependence. The last set of plots represents paired PDPs that conveys the dependence relationship together among 'target' features.

Feature Importance

Attack Type Classification



Attack (1) or Normal (0) Classification

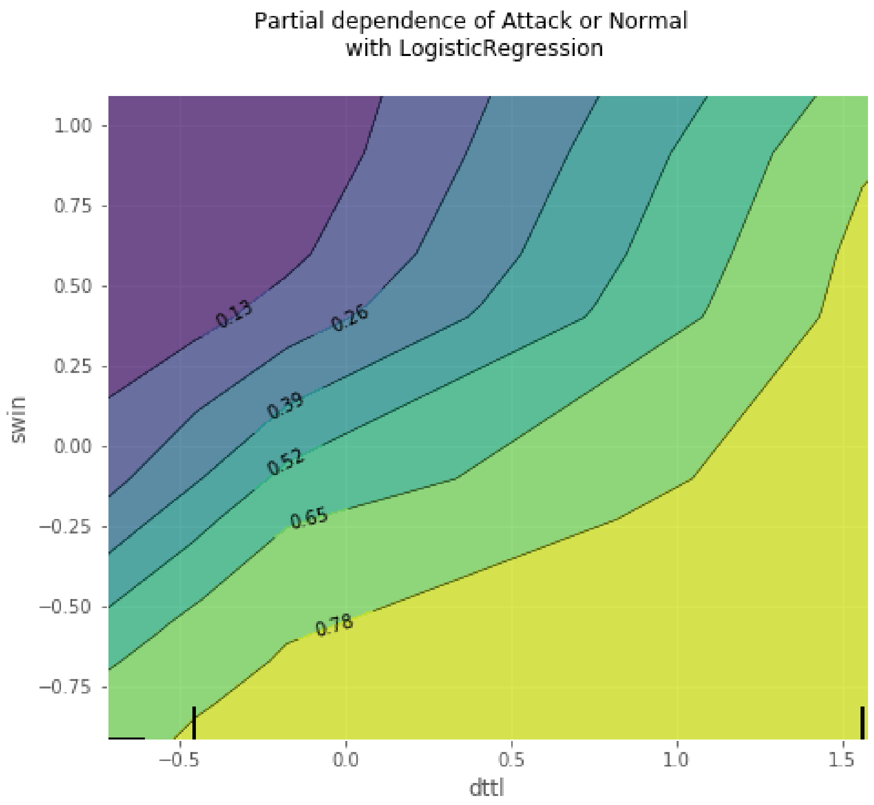


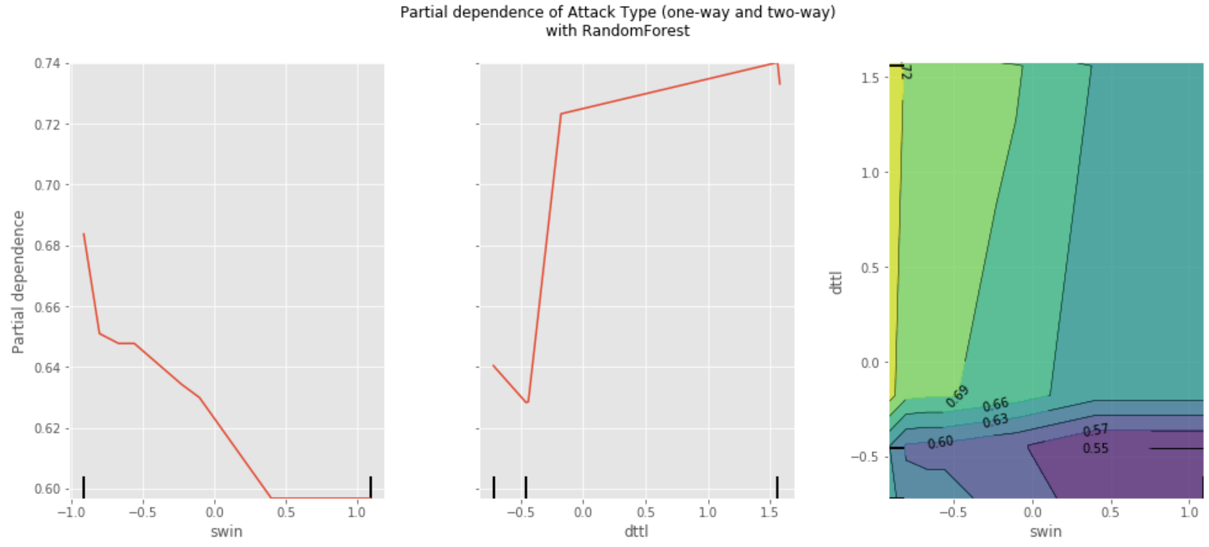
The plot shows that 'swin' and 'ct_src_dport_itm' are very most important feature in the model because once we shuffle the 'swin' and 'ct_src_dport_itm' column of the training data, leaving the target and all other columns in place, the decrease of the accuracy score of predictions is around 0.24 for both, which is a significant finding.

Further Inspection

Attack (1) or Normal (0) Classification (Binary)

Name	Type	Description
swin	integer	Source TCP window advertisement value
dttl	Integer	Destination to source time to live value
ct_src_dport_ltm	integer	No. of connections of the same source address (1) and the destination port (4) in 100 connections according to the last time.
dloss	Integer	Destination packets retransmitted or dropped
ct_dst_sport_ltm	integer	No. of connections of the same destination address (3) and the source port (2) in 100 connections according to the last time.
ct_dst_src_ltm	integer	No. of connections of the same source (1) and the destination (3) address in in 100 connections according to the last time.
ct_srv_dst	integer	No. of connections that contain the same service (14) and destination address (3) in 100 connections according to the last time.





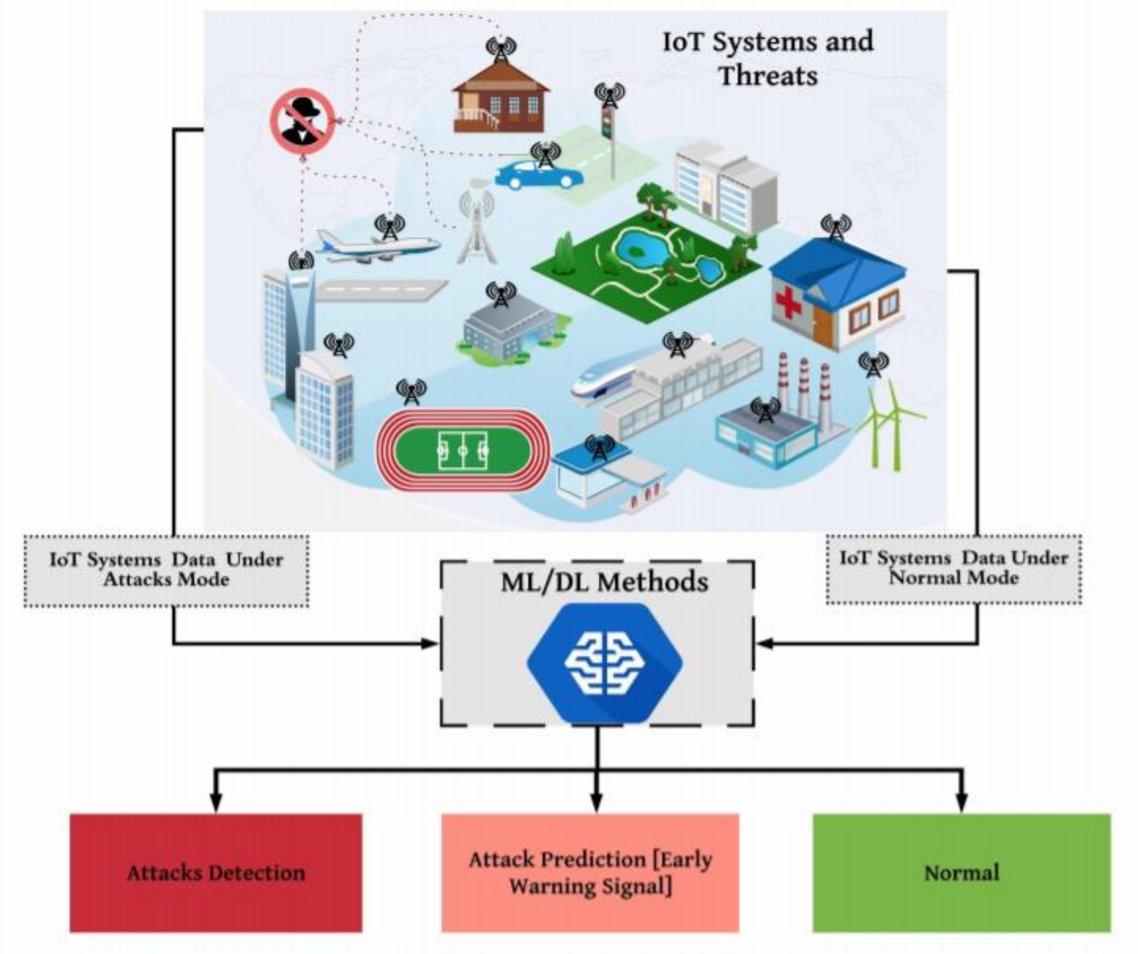
Discussion

- UNSW-NB15 botnet datasets with IoT sensors' data are used to obtain results that show that the proposed features have the potential characteristics of identifying and classifying normal and malicious activity .

- Role of ML algorithms is for developing a network forensic system based on network flow identifiers and features that can track suspicious activities of botnets is possible.

- Furthermore, Random Forests provides a higher detection rate, accuracy and a lower false positive rate compared with both classification responses.

- The ML model metrics using the UNSW-NB15 dataset revealed that ML techniques with flow identifiers can effectively and efficiently detect botnets’ attacks and their tracks.



References

Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015.

Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset." Information Security Journal: A Global Perspective (2016): 1-14.

Moustafa, Nour, et al. . "Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks." IEEE Transactions on Big Data (2017).

Moustafa, Nour, et al. "Big data analytics for intrusion detection system: statistical decision-making using finite dirichlet mixture models." Data Analytics and Decision Support for Cybersecurity. Springer, Cham, 2017. 127-156.