IoT Security Analytics Using Packet Capture (PCAP) Files

Ryan Tao
Department of , Cal Poly Pomona
Faculty Advisor: Dr. Mohammad Husain

Problem

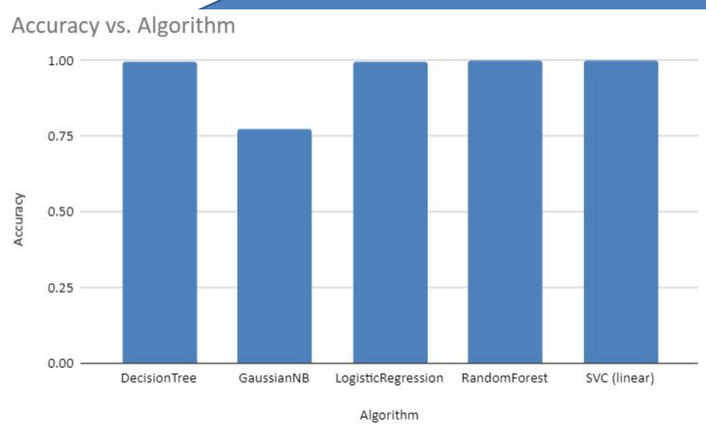
- IoT devices such as Ring Cameras, Alexa, and smart coffee makers are vulnerable to attacks on their network
- IoT Devices are vulnerable due to their weak security protocols along with weak encryption
- Attackers of IoT devices create security concerns as they gain access to data and private information

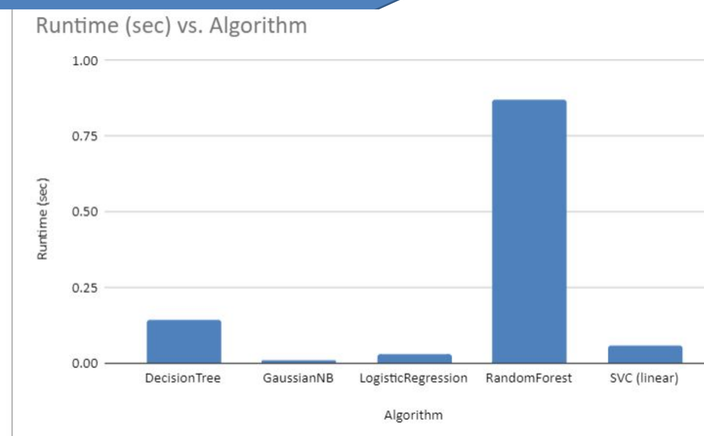
Method

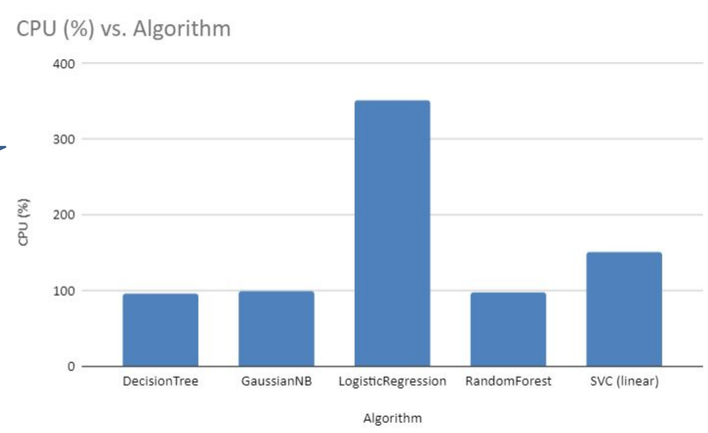
.

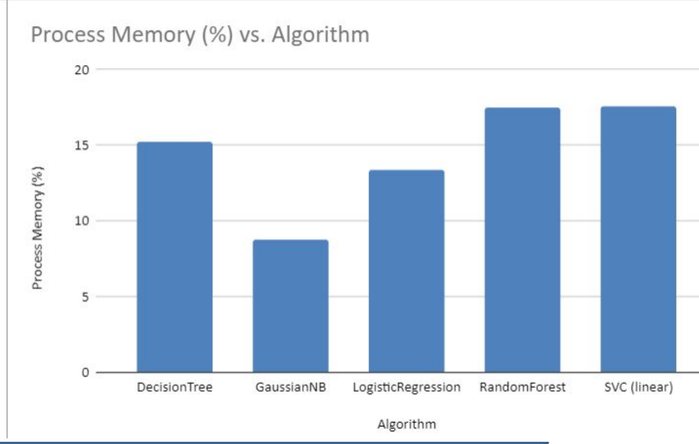
- Prepare the experiment by installing python, sci-kit learn, numpy, pandas, matplotlib, seaborn, psutil, scikit-plot, and pickle
- Set up directories to store experimental, attack, and data results for different types of machine learning to identify the types of malicious attacks
- Extract and sort the data into files for attacks and benign activity on the network
- Shuffle the data to create randomness and a better environment for the machine learning to train
- Run the experiments to train and test the different types of machine learning with the goal of correctly detecting network anomalies

Results









Challenges

- Live sniffing will create a large amount of data that will be stored for analyzing
- Storage could run out fast on the sniffing device
- Heavily taxing on the sniffing device's CPU, memory, and network resources, especially when sniffing multiple IoT devices

Conclusion

- Decision Tree proved to be the most accurate when detecting suspicious network activity followed by Random Forest
  - These however tend to have higher run times when compared with the rest(Logistic Regression, SVC linear, and GaussianNB)
- Logistic Regression and SVC(linear) thrive in medium-sized data sets while GaussianNB struggles with precision, but excels in low runtime