Detecting Cyberattacks in SMART Grids with Machine Learning

New Mexico SMART Grid Center

S. Platero, Southwestern Indian Polytechnic Institute ; A. Langen, Central New Mexico Community College

New Mexico EPSCoR

Introduction

As Power Grids become more intertwined with the Internet of Things the threat of cyberattacks increases.

Researchers are turning to Machine Learning in order to identify and better respond to these new threats by testing the accuracy of different algorithms.

Methodology & Approach

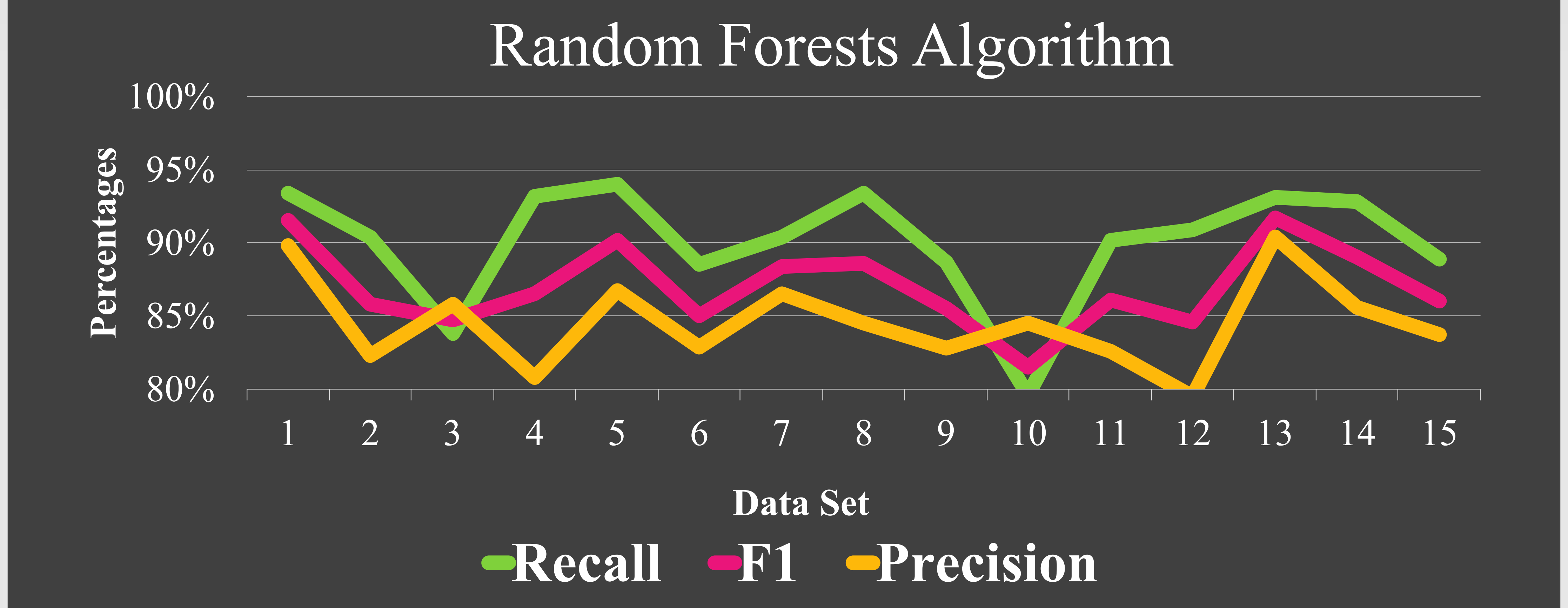
We began our research by learning about Machine Learning and familiarizing ourselves with the many available algorithms. Once familiar we were tasked with using sample code, provided by Ruobin Qi, and Data Sets, compiled by U. Adhikari et al., to test the various algorithms and record the results to compare their Precision, Recall, and F1.

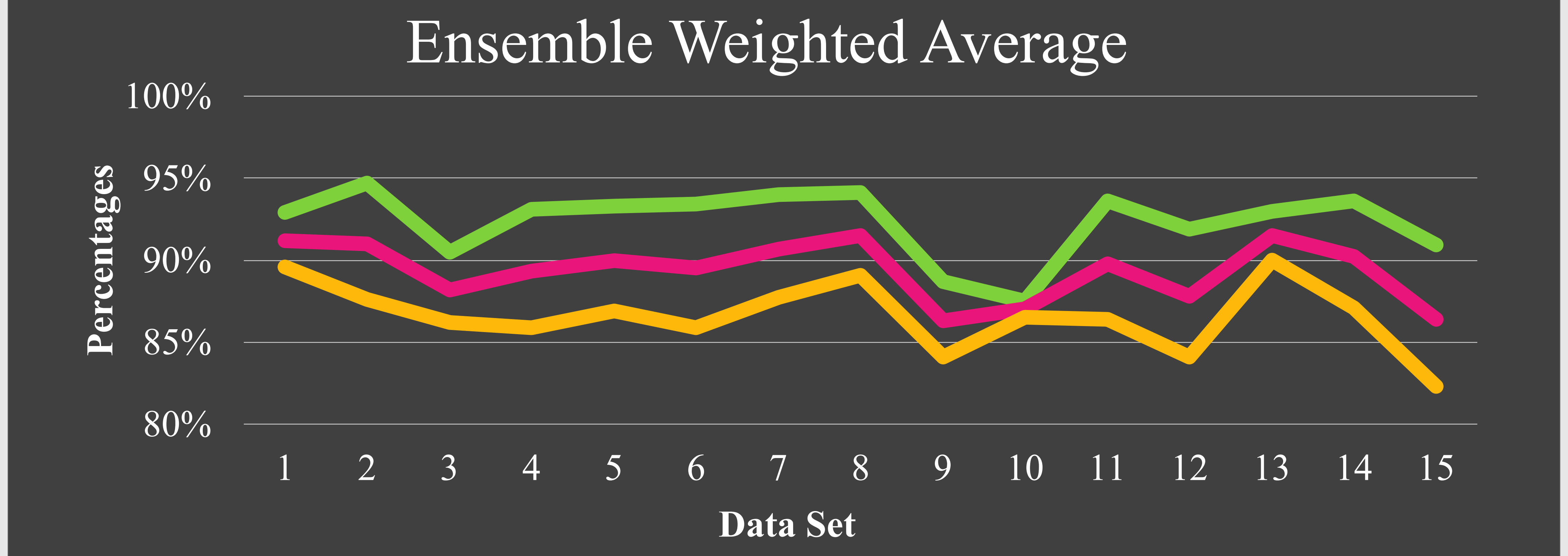
Each algorithm was run through all 15 data sets and recorded to compile the percentage rate of each algorithm's Recall, Precision, and F1.

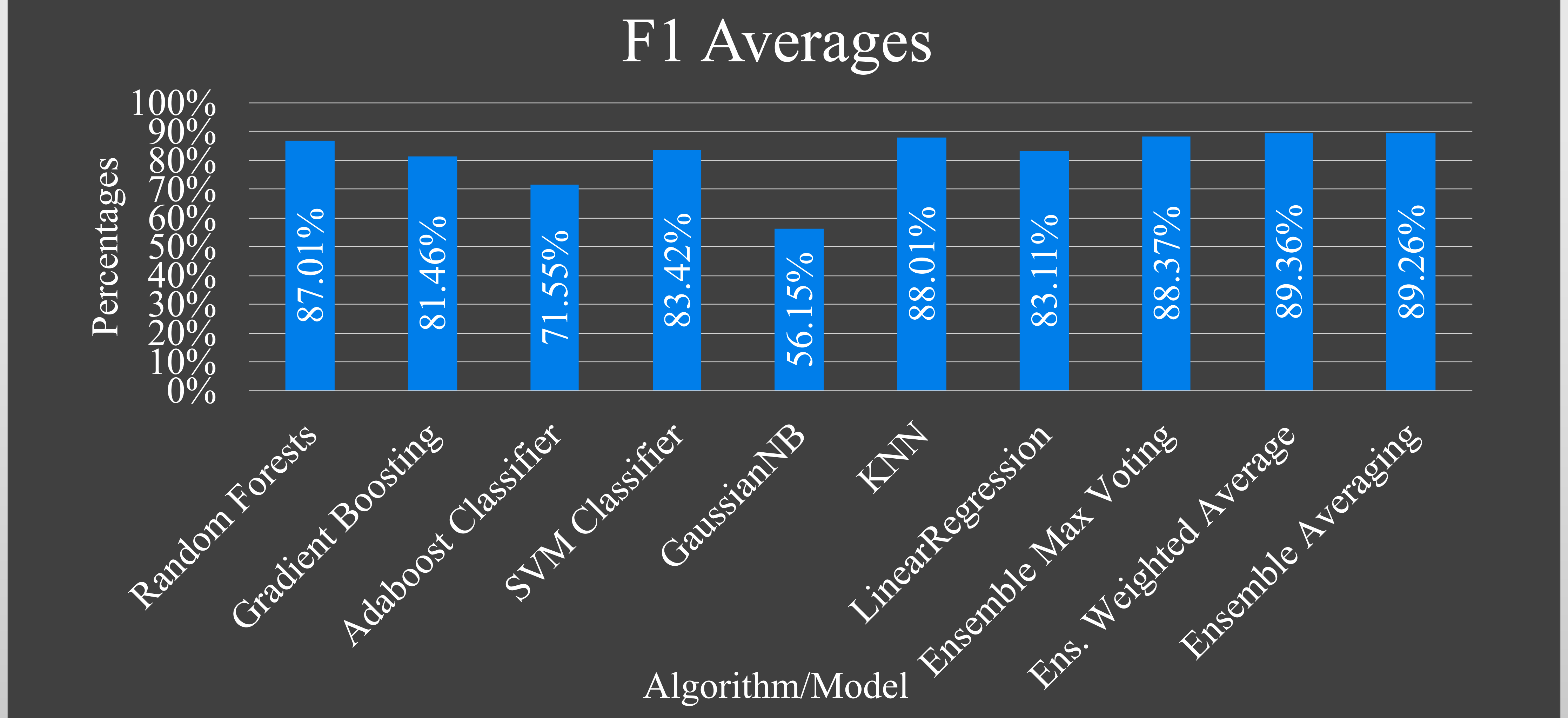
Results

The results varied per algorithm and each showed different strengths and weaknesses. Random Forests was our highest performing individual algorithm. The ensemble model was created using Random Forests, KNN, and SVM, the highest three performing algorithms, and showed more consistency than any individual machine learning algorithm.

Which Algorithm Performs best when identifying Cyberattacks?







This work is funded by the National Science Foundation (NSF) award #OIA-1757207. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Conclusions

We tested the performance of machine learning algorithms for detecting cyber-attacks in smart grids. Three algorithms: Random Forest, SVM and KNN showed the best results. We then built and ensemble model using the three best algorithms and used three different ensemble techniques. The results show that ensemble models perform better in detecting cyberattacks than individual machine learning algorithms.

Future Activities

For the future, this research project has opened our minds to the possibilities of malicious and non-malicious attacks and how they can be detected with machine learning.

- We both want to continue our education in computer science
- Continue to practice and learn more about opportunities that involve this type of research
- Take more programming classes

Acknowledgements

We would like to thank the NSF, NM SMART Grid Center and EPSCoR for providing a successful research program. Including DR Zheng, Ruobin Qi, the EPSCoR Faculty, and Students.