



Robust Intelligent Intrusion Detection Systems

Students: Alexander Bermeo

Mentor: Yanzhao Wu

Instructor/Faculty: Dr. Masoud Sadjadi, Florida International University

PROBLEM

The problem we are analyzing is the efficacy of detecting network intrusions, such as DDoS attacks and network probes, in modern computer networks. As networks grow in complexity and generate increasingly large amounts of traffic, existing Intrusion Detection Systems (IDS) face challenges in accurately and robustly identifying malicious activities.

The project proposes using robust machine learning techniques, particularly robust ensemble learning methods, to improve the accuracy and resilience of IDS.

PROJECT OVERVIEW

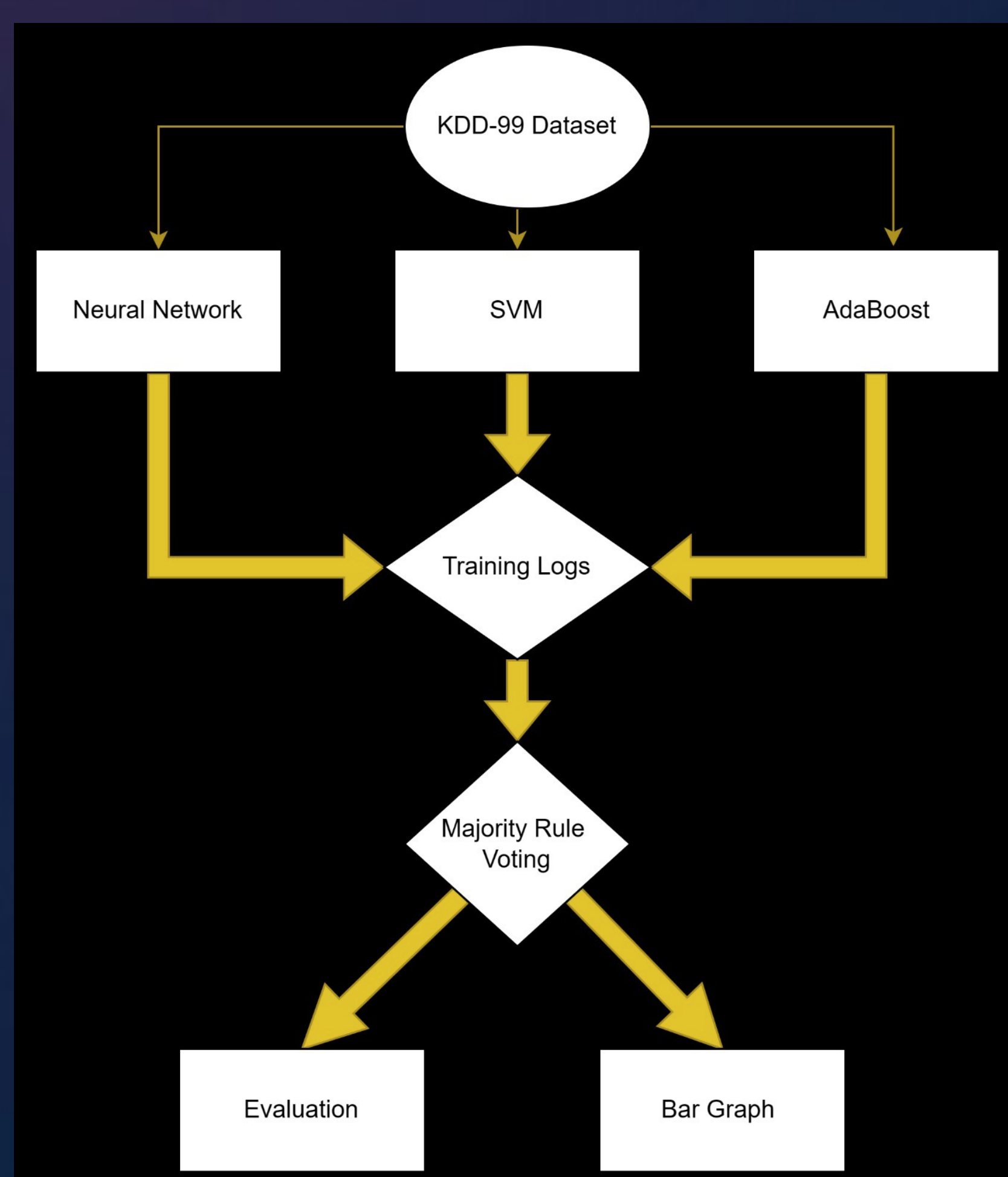
The project aims to address the difficulty of effectively detecting network intrusions, like DDoS attacks, in modern computer networks due to the growing volume of data and evolving network environments. To enhance Intrusion Detection Systems (IDS), the project focuses on using robust machine learning techniques, specifically robust ensemble learning methods. This approach intends to improve the accuracy and resilience of IDS. Additionally, the project offers an opportunity to learn more about Machine Learning, Cybersecurity, and Computer Networks through the research and implementation that was required for this project.

TOOLS USED

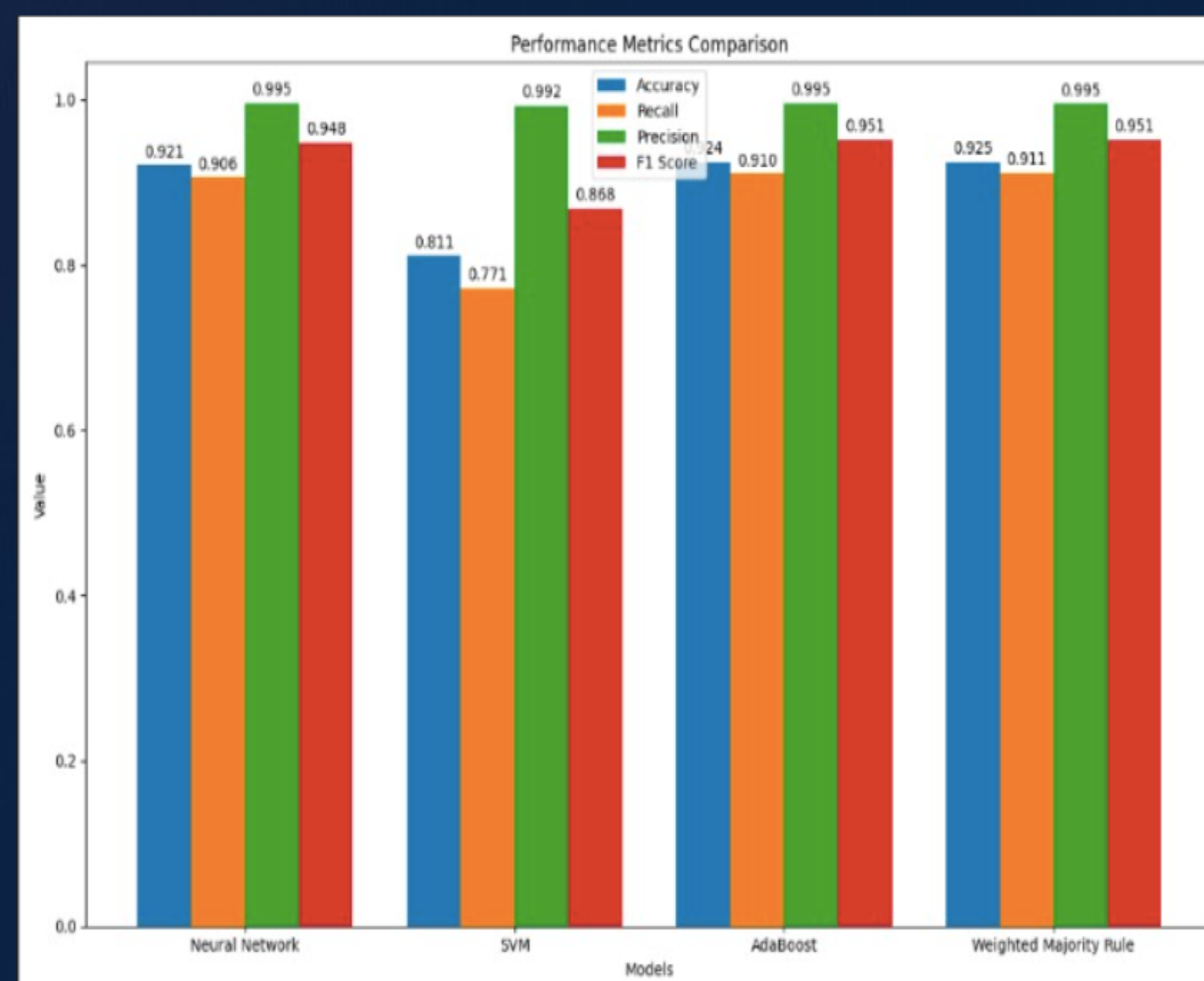
Programming language: Python

Dataset used: KD-99

SYSTEM DESIGN



SYSTEM RESULTS



IMPLEMENTATION

The implementation of this project consisted of:
Dataset: KD-99

Imports: Pandas, NumPy

Models: Neural Network, Support Vector Machine (SVM), and AdaBoost

INDIVIDUAL CONTRIBUTIONS

Throughout the project, my primary focus was on team management and organization on the sprints and required documentation that it required. I was in charge of keeping track of everyone's status on the project and what areas required assistance. With that being said, I also contributed in the creation of the Neural Network model that was required to merge the other models in order to merge them and test them using the Majority Rule test.

SUMMARY

The Python script presented a comprehensive approach to enhancing Intrusion Detection Systems (IDS) using machine learning techniques. It loaded and preprocessed network traffic data, separating it into training and testing sets while normalizing the information for better model performance. Three distinct models, including a Neural Network (NN), Support Vector Machine (SVM), and AdaBoost Classifier, were constructed and trained on the normalized data. These models were individually evaluated using performance metrics like accuracy, recall, precision, and F1-score. Additionally, a combined weighted majority vote method merging predictions from all models was explored for improved intrusion detection. The script produced a visual comparison in the form of a bar graph, showcasing the strengths and weaknesses of each model and the combined approach. All steps, models created, and their respective performance metrics were logged for analysis and record-keeping.

REFERENCES

- <https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7>
- <https://ieeexplore.ieee.org/document/8280825>

ATTENTION: Subheadings shown above is a recommended structure for a research/scientific poster. Main elements of a poster are Introduction, Research and Conclusion. Researchers can customize the section headers based on their projects' needs. REMOVE THIS TEXT ONCE YOU START WORKING ON YOUR POSTER