



Engineering
& Computing

School of Computing
& Information Sciences

School of Computing & Information Sciences

Summer 2023 Capstone II Project



Enhancing Intrusion Detection Systems

Students: Josue Camejo

Mentor: **Yanzhao Wu**

Instructor: *Dr. Masoud Sadjadi*, Florida International University

Problem

The number of zero-day attacks around the world has spiked in recent years. This increase has not just been zero-day attacks, but various forms of malware and viruses are being constantly updated and used by threat actors. In a perfect world, we can handle these attacks by using IDS (Intrusion Detection Systems) & IPS (Intrusion Prevention System). However, our systems are falling behind when it comes to detecting and preventing these attacks from affecting their network. Attackers are constantly upgrading and inventing new ways to obfuscate or manipulate data to be able to trick the IDS/IPS software into allowing them through.

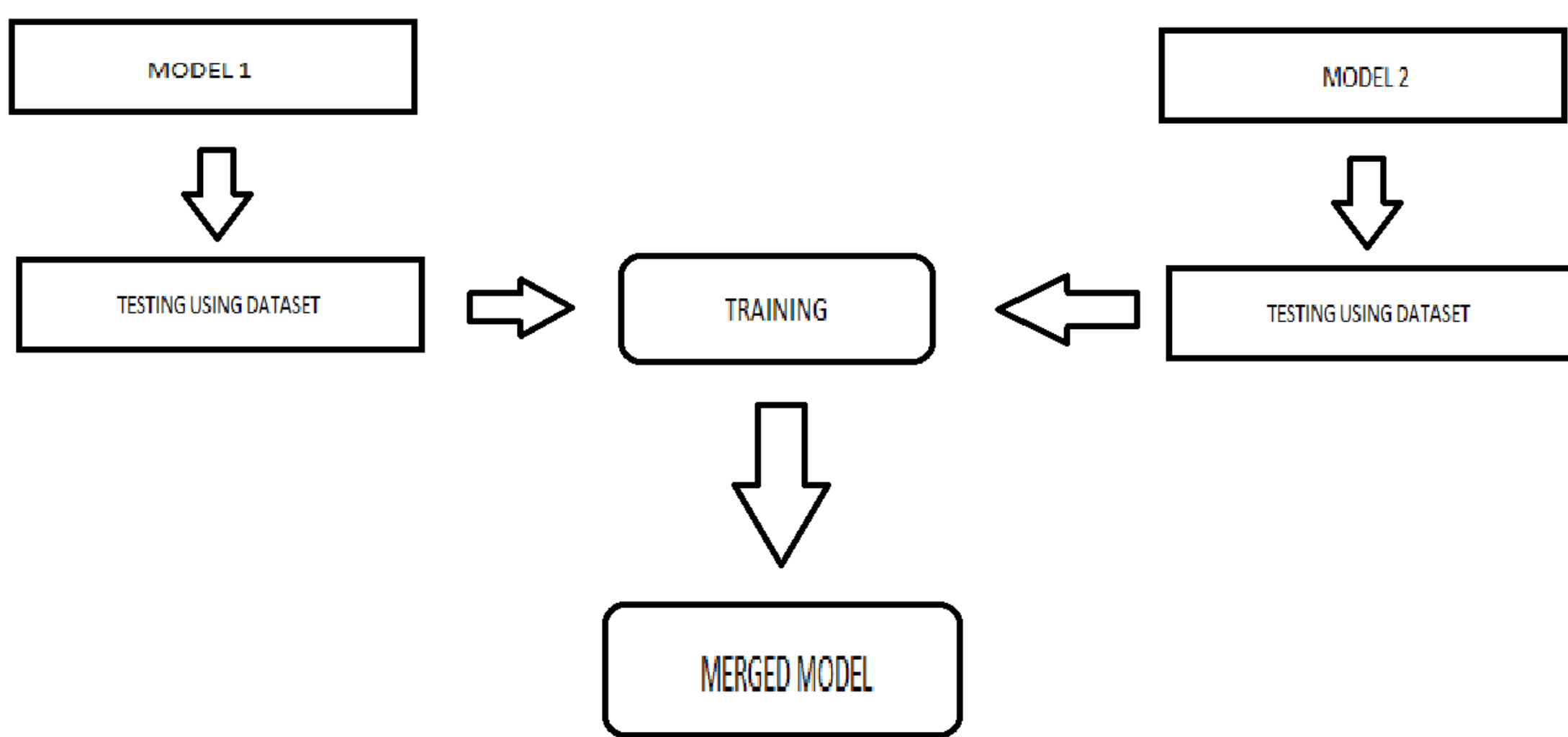
Project Overview

- Our primary objective was to develop a merged IDS solution by integrating multiple open-source models. The specific goals include:
 - Investigate the architecture and compatibility of the open-source models to identify areas for integration and determine the viability of merging these systems.
 - Evaluate the performance of each IDS model individually using standard metrics such as accuracy, recall, precision, and F1 score. This evaluation will provide insights into the strengths and weaknesses of each model in detecting network intrusions.
 - Combine the two pre-trained IDS models using ensemble techniques such as Voting, Stacking, or Weighted Averaging. The aim is to leverage the diverse predictions of both models and create an ensemble IDS that potentially outperforms the individual models in accuracy and precision.

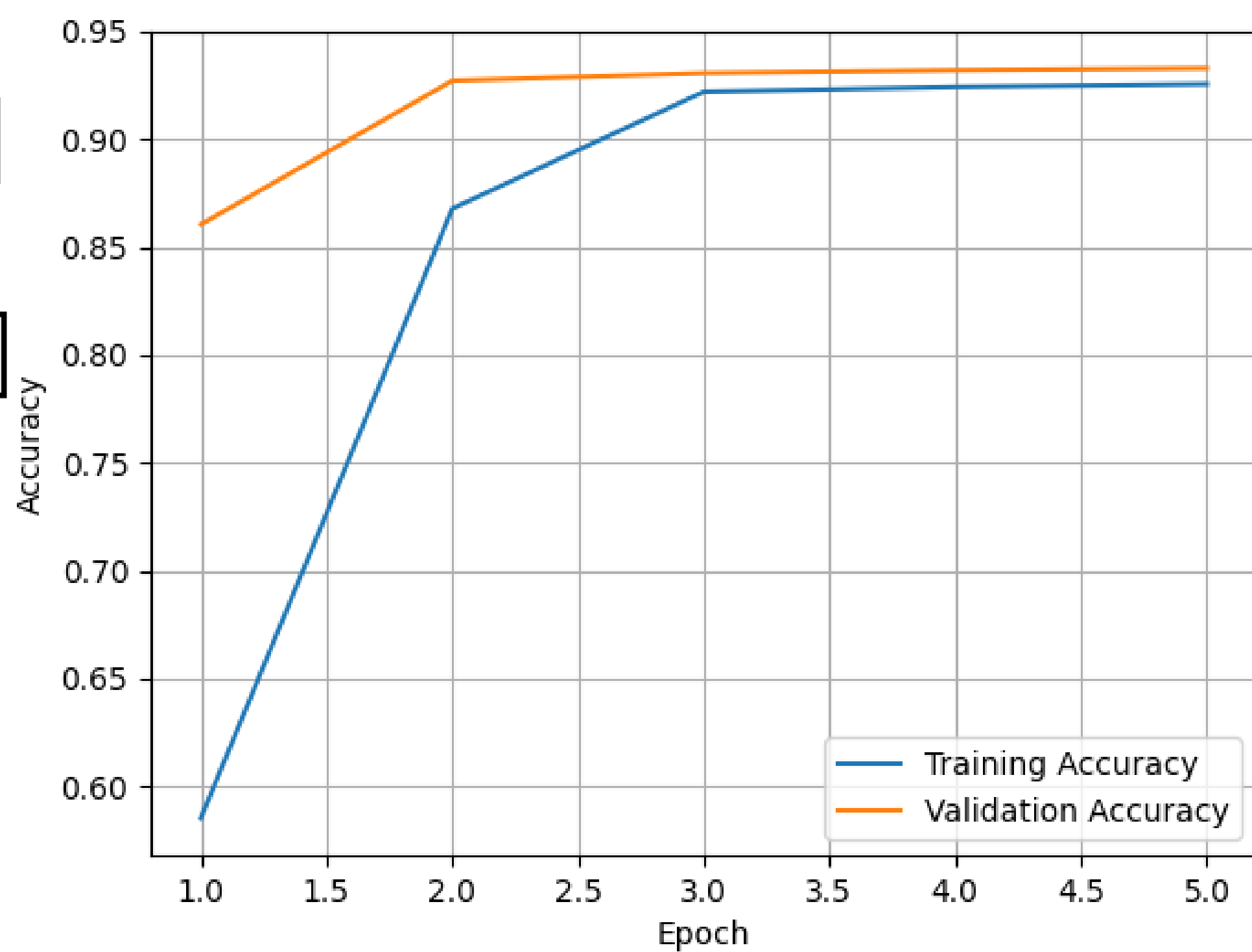
Tools Used

- Python
 - For Data Processing, to preprocess and clean the raw data before training the IDS models. Model Training, allows for straightforward model training using specific algorithms.
 - Visualization, libraries such as Matplotlib and Seaborn, allow for visualization of data, model performance and training history.
- VirtualBox VM
 - Kali Linux Virtual Machines
 - Windows 10 Virtual Machines
- For running tests and analyzing the models during live experiments on a network.
- Open-Source IDS models, Intrusion Detection Systems using KDD99-Dataset

System Design



System Results



Implementation

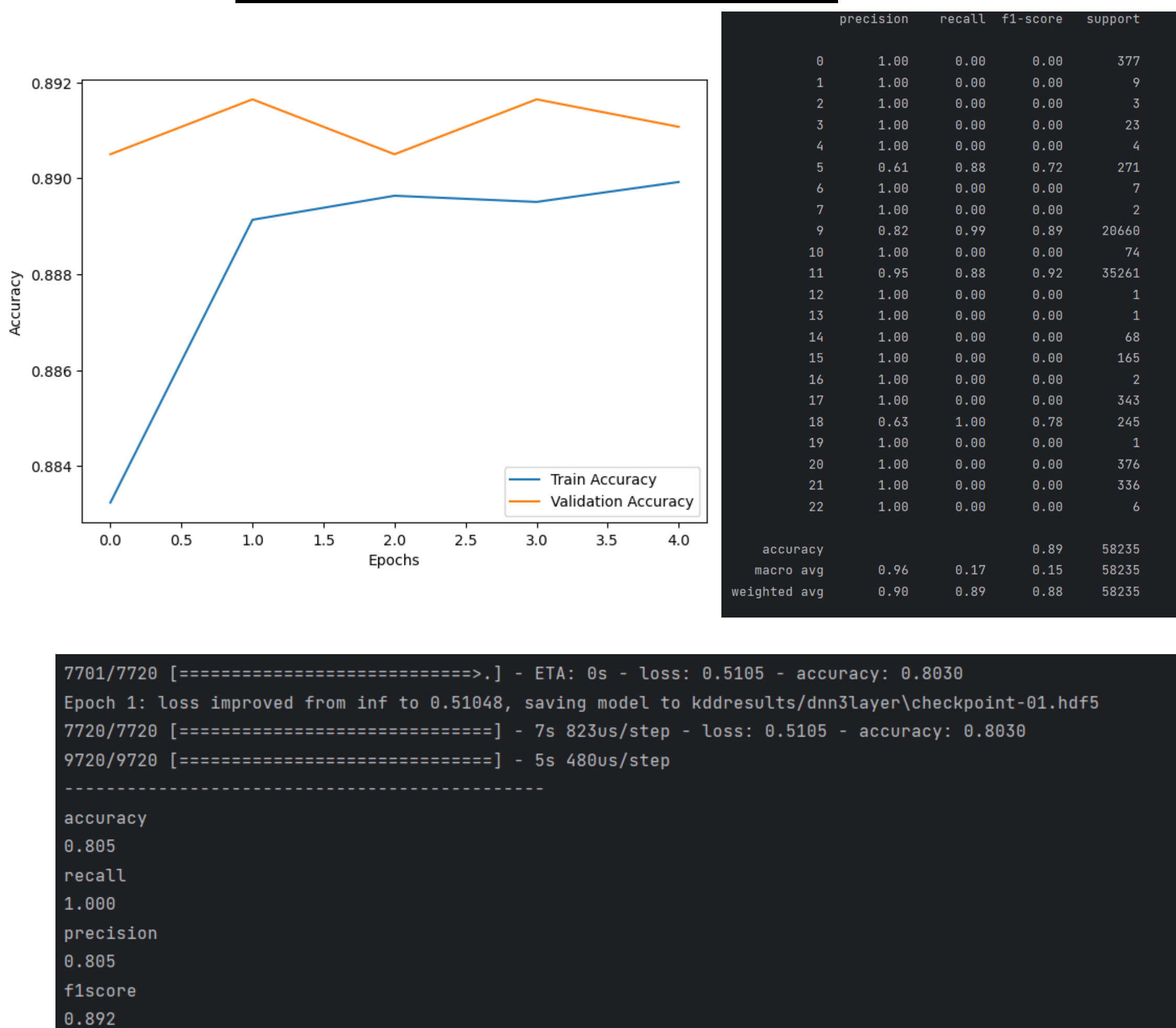


Individual Contributions

Performed research on potential Datasets and open-source Intrusion Detection Systems.

Performed Daily checkups with the team to make sure progress was on track.

Screenshots



Summary

The IDS project demonstrated the effectiveness of merging two IDS models using Python, resulting in a final model that surpassed the performance of the individual models. This achievement contributes significant value to the field of cybersecurity, showcasing the potential of ensemble approaches for improved network security and intrusion detection accuracy.

Acknowledgement

The material presented in this poster is based upon the work supported by **XXXXX (name of the sponsor: federal, state or local, or industry, if applicable)**. We/I thank **XXXX** for assistance, cooperation and mentorship that I/we received throughout this process