



Enhancing Intrusion Detection Systems

Students: <Dennis Martinez>

Mentor: **Yanzhao Wu**

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

Problem

There are countless attacks around the world that have been emerging the past years and the attacks have been evolving their malware and virus tactics to be able to penetrate any system possible. We will be needing Intrusion Detection Systems in order to compensate for our systems that lack detection and prevention.

Project Overview

The primary objective is to develop a merged IDS solution to improve detection overall.

1. Researching how to combine IDS' and how the architecture should be.
2. Evaluate the performance of the IDS models by using standard metrics like accuracy, recall, precision, and F1 score to see where exactly the system lacks and will be needing improvement.
3. Combining two trained IDS models using techniques such as Weighted Averaging and Voting. The result should be a merge of both models with better results than each individual one.

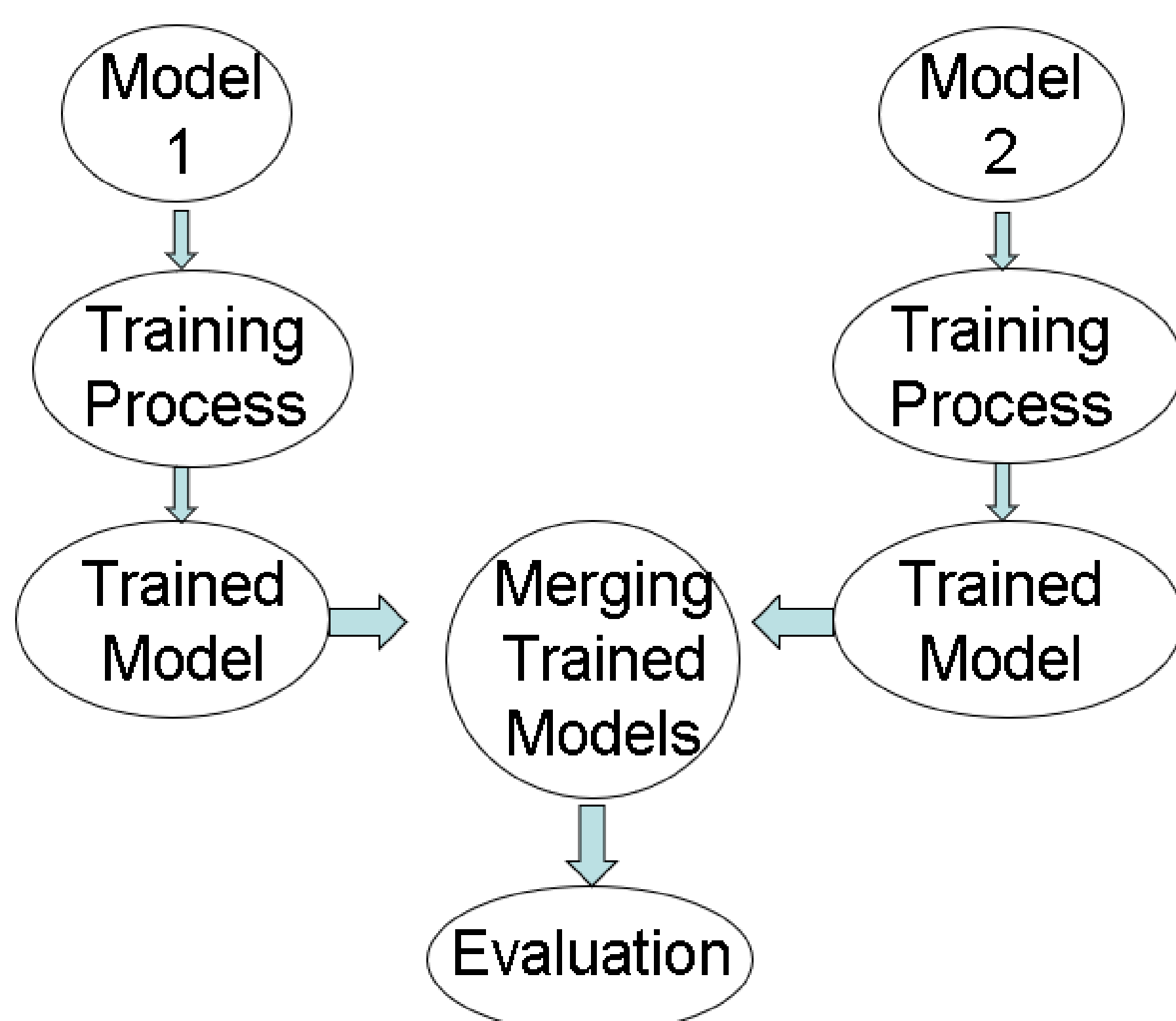
Tools Used

Python 3.11- Was used for most of the project for Data Processing and Visualization using Matplotlib to construct the graphs.

VirtualBox VM (Kali) – Was used to test attacks on the IDS.

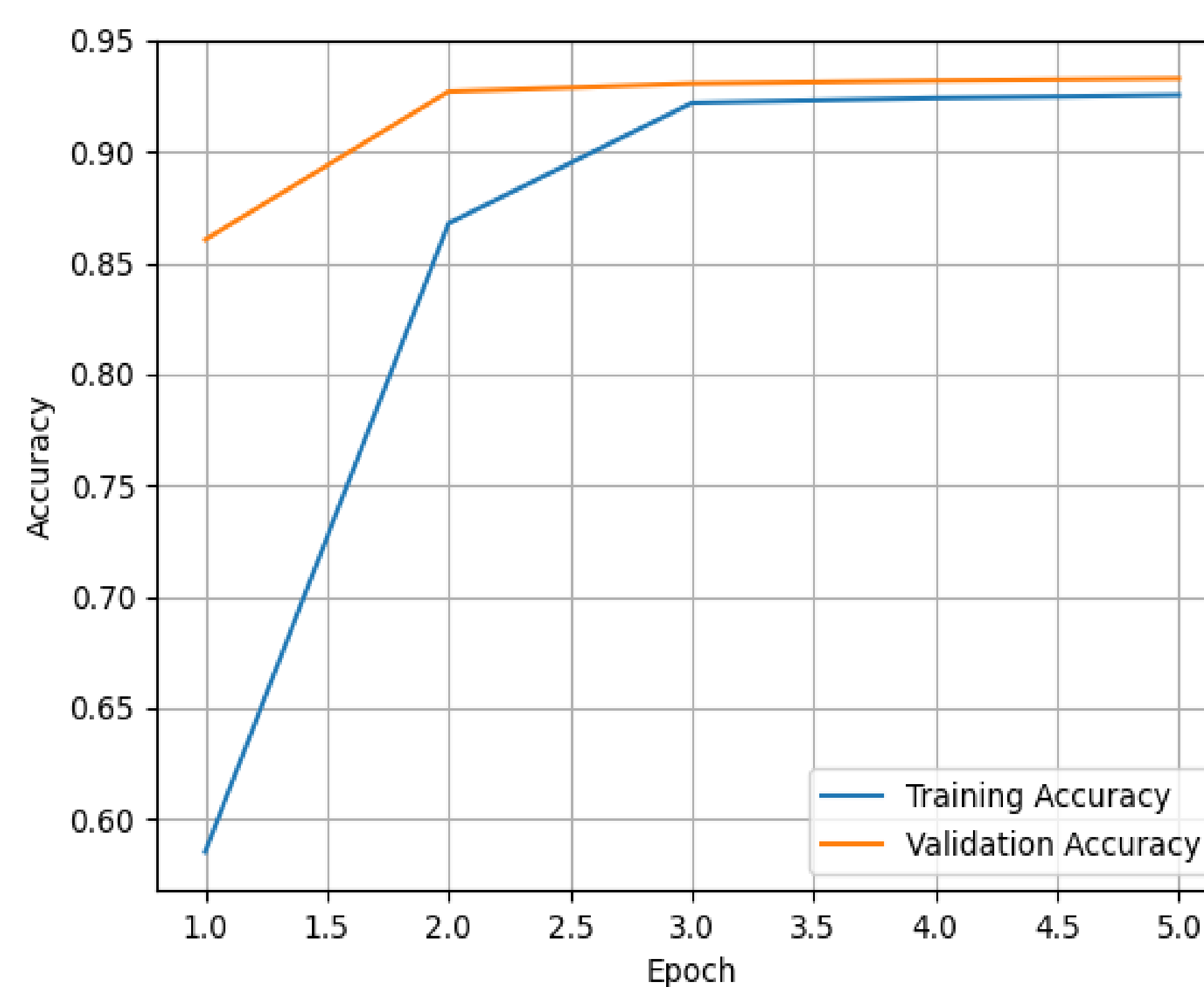
KDD99 Dataset

System Design



System Results

Merged IDS Model Results



Implementation



Individual Contributions

Performed research on open-source Intrusion Detection Systems.

Constructed, troubleshoot, and merged IDS models.

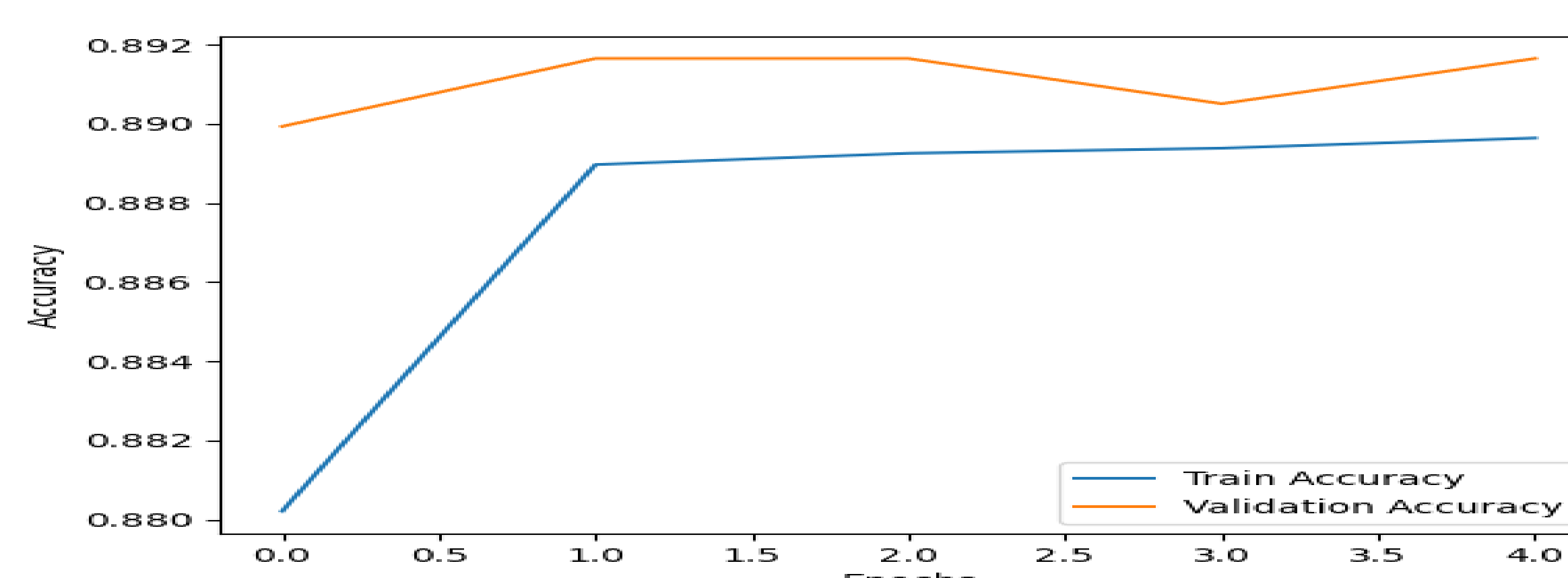
Screenshots

IDS Model 1 Results

```

7701/7720 [=====] - ETA: 0s - loss: 0.5105 - accuracy: 0.8030
Epoch 1: loss improved from inf to 0.51048, saving model to kddresults/dnn3layer/checkpoint-01.hdf5
7720/7720 [=====] - 7s 823us/step - loss: 0.5105 - accuracy: 0.8030
9720/9720 [=====] - 5s 480us/step
-----
accuracy
0.805
recall
1.000
precision
0.805
f1score
0.892
  
```

IDS Model 2 Results



Summary

The Final Results were that the Merged IDS surpassed both models in individual performance. These results contributes to the cybersecurity world by demonstrating the potential of merging two systems to create an even greater security than either system can provide.

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