COLLEGE OF ENGINEERING
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

CPE496/498 Capstone Design Course

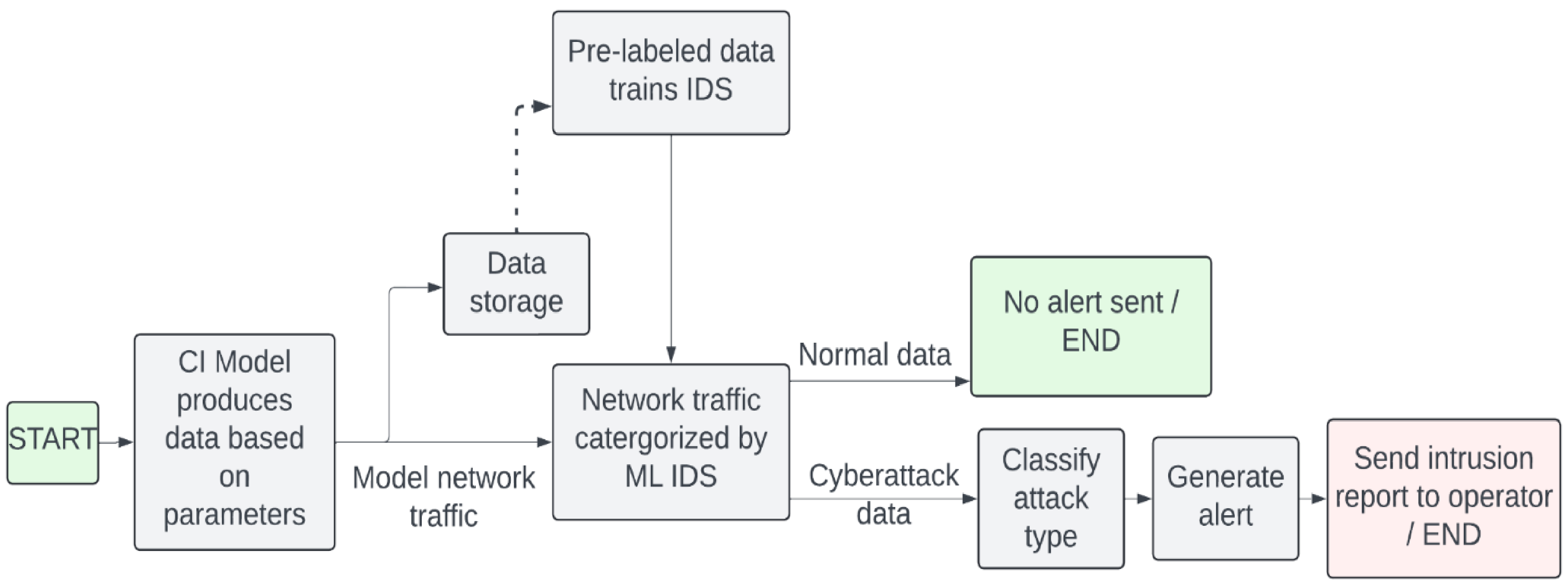
Intrusion Detection System for Critical Infrastructure

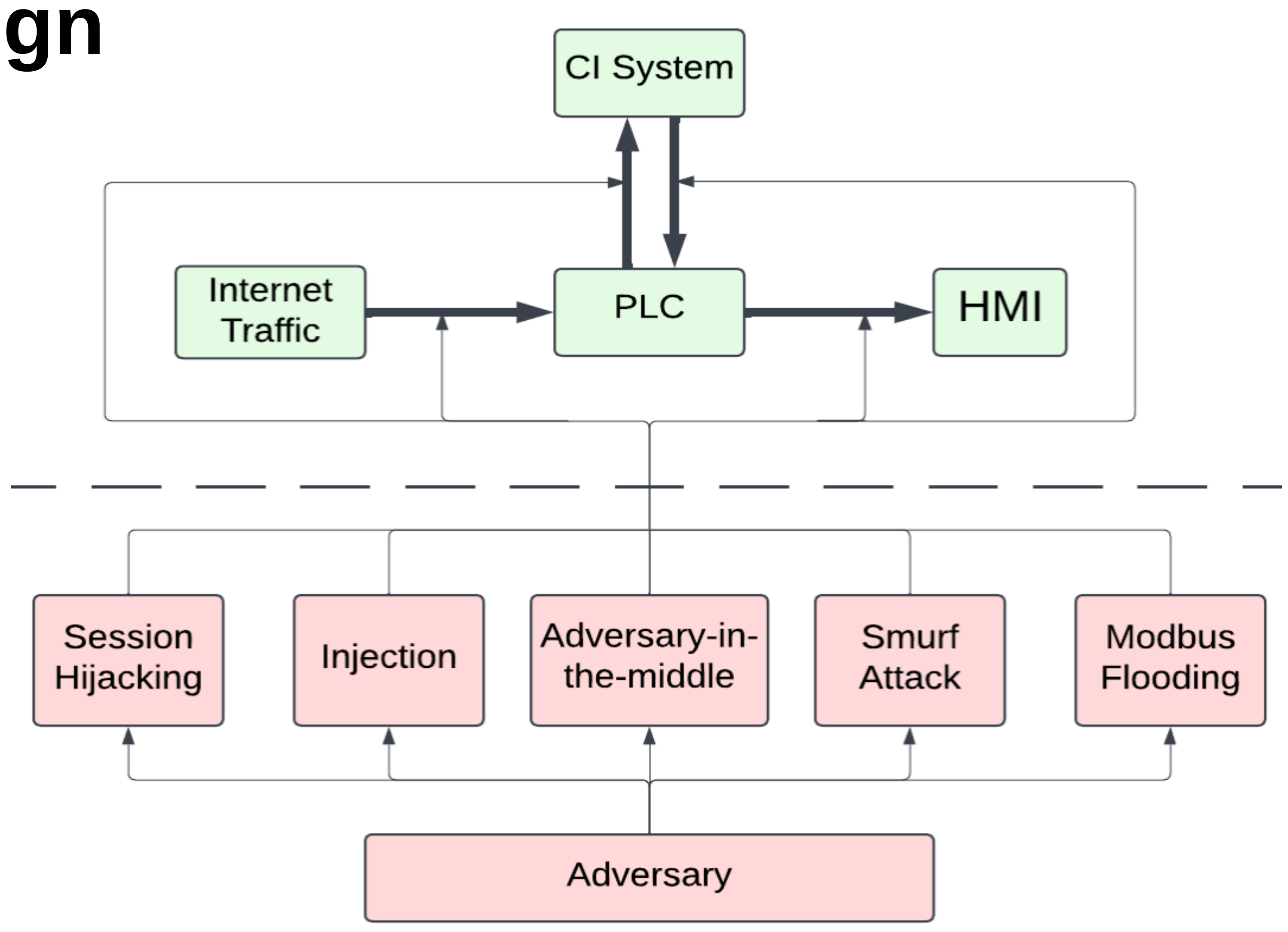
Department of Electrical and Computer Engineering
Team: Justina Edwards, Subhankar Baidya, and Jonathan Biffle
Mentor: M. E. Alim, UAH Center for Cybersecurity Research and Education

Project Overview

Critical infrastructure (CI) impacts several essential infrastructure sectors, such as energy, food, and water industries. However, critical infrastructure remains vulnerable to cyber attacks, putting these critical industries at risk. Our team proposes a machine learning model trained on the network traffic collected from three digital twin testbeds based on critical infrastructure, during normal operations and cyber attack scenarios. The machine learning model will be used to classify the network traffic of the digital twins for the intrusion detection system (IDS).

System Design


START
CI Model produces data based on parameters
Model network traffic
Data storage
Pre-labeled data trains IDS
Network traffic catergorized by ML IDS
Normal data
No alert sent / END
Cyberattack data
Classify attack type
Generate alert
Send intrusion report to operator / END



Background

- This paper [1] implemented SCADA systems as a digital twins and demonstrated how cyber attacks and normal conditions could be simulated on the testbeds.
- This paper [1] discusses how future work could utilize these datasets to train an IDS using machine learning.

Results

- **Data Collection:** Verified data can be accurately collected at a rate 10 times the speed of a real-time rate from the digital twin testbeds.
- **Machine Learning:** The combined classifier has achieved an accuracy of 99.82% with a F1-score of 98% using temporary placeholder data.

Future Work

- Building a more robust intrusion prevention system that will intercept and prevent cyber attacks from causing critical damage.
- Utilizing a greater comparison of algorithms, more testbed data with greater variance, and more cyber attacks to build a more robust intrusion prevention system.

Proposed Solution

- Digital twin testbeds of CI were used to collect instances of network traffic under normal conditions and cyber attacks for accurate and faster-than-real-time data collection.
- The 5 cyber attacks against the models were selected to represent a broad spectrum of vulnerabilities within industrial control systems.
- The machine learning algorithm uses 3 classifiers (SVM, Random Forest, and Naive Bayes) and will use the majority vote of the classifiers to classify network traffic.

Conclusions

- CI is vital for essential infrastructure sectors, and there is a need for an open-source IDS to detect these cyber attacks against CI accurately.
- This project will further contribute to research on CI by providing researcher up-to-date and accurate datasets on CI which will benefit operators, government agencies, and public safety.

Acknowledgements and References

Special thanks to our mentor M. Einaam Alim and the UAH Center for Cybersecurity Research and Education.

[1] M. E. Alim, J. Smalligan and T. H. Morris, "A Collection of Datasets and Simulation Frameworks for Industrial Control System Research," SoutheastCon 2023, Orlando, FL, USA, 2023, pp. 96-103, doi: 10.1109/SoutheastCon51012.2023.10115122.

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION