SecureDash

Advancing Smart Grid Security with an Intrusion Detection Framework

Jayashre

Project Overview and Development

June 17, 2024

Table of Contents

Table of Contents

Project Overview

This project aims to enhance Smart Grid security by developing an advanced intrusion detection system that leverages machine learning to combat cyber threats, such as DDoS attacks. The primary goal is to advance intrusion detection capabilities within smart energy grids, ensuring uninterrupted operation and safety in our increasingly digital world. By integrating real-time monitoring, advanced anomaly detection, and robust threat mitigation strategies, the project seeks to protect critical infrastructure from evolving cyber threats and maintain the reliability and resilience of modern energy grids.

Table of Contents

Smart Grid & Intrusion Detection System

Smart Grid: An advanced electricity network utilizing digital communication technology for efficient and reliable electricity and data management. It enables two-way communication, optimizing resource utilization, incorporating renewable energy sources, and enhancing grid resilience through real-time monitoring and control.

IDS in Smart Grid: Safeguards the communication network against cyber threats by continuously detecting both known and unknown attacks across different layers: Home Area Network (HAN) for individual homes, Neighborhood Area Network (NAN) for aggregating data, and Wide Area Network (WAN) for the larger infrastructure.

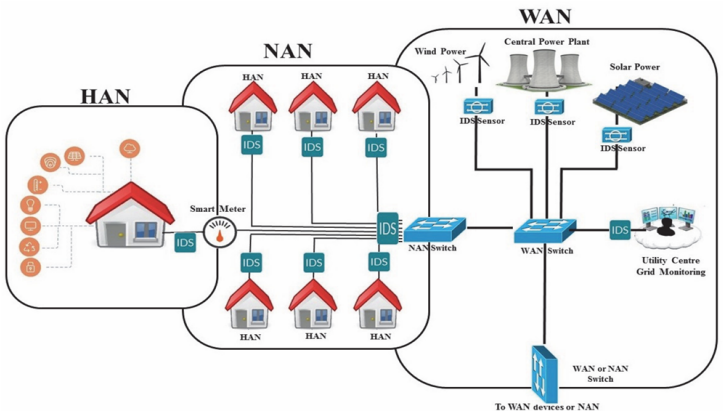

Table of Contents

Tech Stack

Technologies Used

1. **Python**: For implementing machine learning and deep learning models.
2. **Google Colab**: For the development of machine learning models in Python.
3. **Scapy & Numpy**: For capturing and processing network packets.
4. **Standard Scaler & ADASYN**: For data scaling and handling class imbalance.
5. **MySQL**: For backend database management.
6. **Power BI**: For real-time visualization and analytics.
7. **Electron, HTML, CSS & Javascript**: : For developing the desktop application.
8. **Flask**: For running the web server to view the database.

Table of Contents

Machine Learning Model Development

1. **Hybrid Deep Learning Model**: Combines Convolutional Neural Network (CNN) and Gated recurrent unit (GRU) for effective feature extraction and sequence learning.
2. **Data Preprocessing**: Features scaled using Standard Scaler, and class imbalance addressed with ADASYN.
3. **Model Architecture**
   - **CNN** for feature extraction.
   - **GRU** for capturing long-term dependencies
   - **Flattening** CNN Layer for Feature Integration
   - **Concatenation** Layer for Merging Outputs from CNN and GRU
   - Addition of **Fully Connected** Layer
   - **Dropout Layer** to Prevent *Overfitting*
   - **SoftMax Layer** for *Classification*
4. **Training**: The model was trained on the **CIC-DDOS2019** dataset.
5. **Testing**: The model was then evaluated on the testing dataset, achieving an accuracy of 99.7% and a loss of 1.5%.

Table of Contents

Architecture Diagram of the Hybrid Model

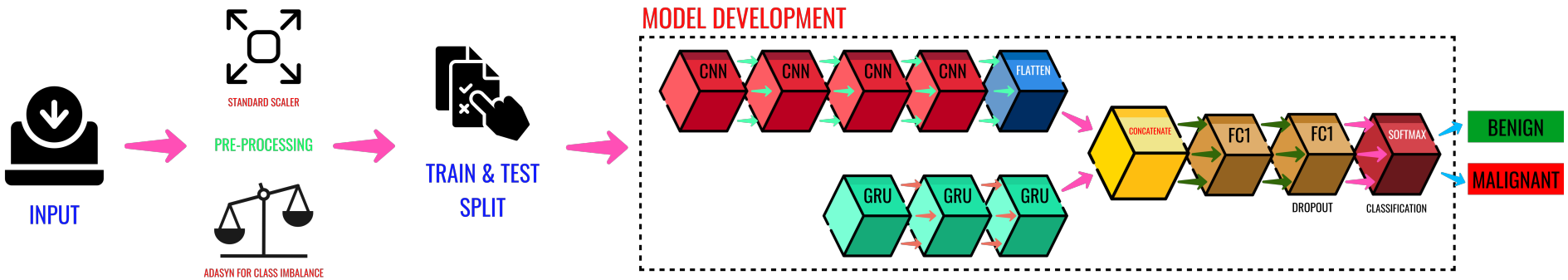

Table of Contents

Product Development

Product Overview:

1. **Packet Capture**: *Network packets* are captured using **Scapy** and *processed* with **Numpy**.
2. **Feature Extraction**: Essential features are *extracted* and *scaled*.
3. **Prediction**: Features are sent to the **trained ML model** for *prediction*.
4. **Visualization**: Predictions are sent to **Power BI** for *real-time visualization*.
5. **Database Storage**: Predictions are also stored in **MySQL** for *future analysis* and *viewing0*.

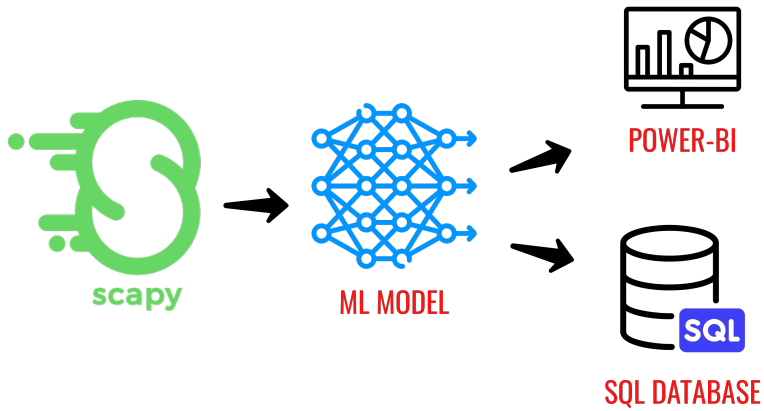

Table of Contents

Outcomes and Challenges

1. Gained expertise in developing deep learning models for cybersecurity.
2. Learned the intricacies of Smart Grid technology and its security challenges.
3. Developed skills in real-time data processing and visualization.
4. Enhanced understanding of integrating ML models with practical applications.

Challenges and Future Scope

Challenges

1. Handling large volumes of network data in real-time.
2. Integrating the system with existing infrastructure (IDS/IPS).
3. Lack of Documentation on Scapy Library.

Future Scope

1. Advancing explainable AI techniques for transparent decision-making.
2. Delving deeper into intrusion detection within SCADA and Smart Grid settings.
3. Enhancing scalability and performance for wider deployment.

Table of Contents

Thank you