Advancing Smart Grid Security with an Intrusion Detection Framework

Jayashre

June 6, 2024

Overview

To enhance Smart Grid security, this project develops an advanced intrusion detection system using machine learning to combat cyber threats like DDoS attacks. Its goal is to advance intrusion detection in smart energy grids, ensuring uninterrupted operation and safety in our increasingly digital world.

Target Audience

Utility Companies

Cybersecurity Professionals

Government Agencies

Technology Providers

Research & Academia

Features

Creation of a real-time monitoring dashboard to track network activity and detect anomalies promptly.

Integration of the developed system with existing intrusion detection systems for enhanced threat detection and mitigation.

Implementation of continuous surveillance techniques to monitor network traffic and identify potential threats in real-time.

Creation of a user-friendly interface for system management and monitoring, facilitating ease of use for grid operators and cybersecurity personnel

Tech Stack

- Python: Used for implementing machine learning and deep learning approaches.
- Datasets: Utilizing the CIC-DDOS2019 dataset.
- Real-Time Monitoring Platforms: Such as Kafka and Pulsar.
- Intrusion Detection and Prevention Systems: Like Suricata and Snort.
- Monitoring and Visualization Tools: Including Grafana, Tableau, and Power BI.
- Google Colab: For the development of machine learning models in Python.

Future Scope

Advancing explainable AI techniques is crucial as deep-learning models gain prevalence in critical systems. Ensuring transparent decision-making enhances practicality in real-world scenarios by unraveling the detection process and providing meaningful insights.

Expanding on this study's foundation to delve deeper into the nuances of intrusion detection within SCADA and Smart Grid settings.

Conclusion & Thank You

I value and appreciate your feedback.