RV College of Engineering, Bengaluru - 560059.

Go, change the world

Title: Power Grid Anomaly Detection and Prediction of Physical and Cyber Attacks

Sanjay CM | Satkrit Samyaan | Abu Arshian| Dhruvi Bhandari | Siddhant Shah

1RV23ET039 | 1RV23ET069 | 1RV23EC005 | 1RV23EC042 | 1RV23EI066

Introduction

Smart grids integrate power systems with digital communication, sensors, and automation to enable efficient and reliable energy management. However, this increased connectivity exposes the grid to cyber-attacks and physical anomalies that are difficult to detect using traditional rule-based monitoring systems. Conventional threshold-based techniques fail to capture the temporal and multivariate behavior of smart grid data. This project proposes an AI-based cyber-physical anomaly detection framework that leverages machine learning and deep learning models to detect abnormal behavior in both physical power systems and cyber communication networks.

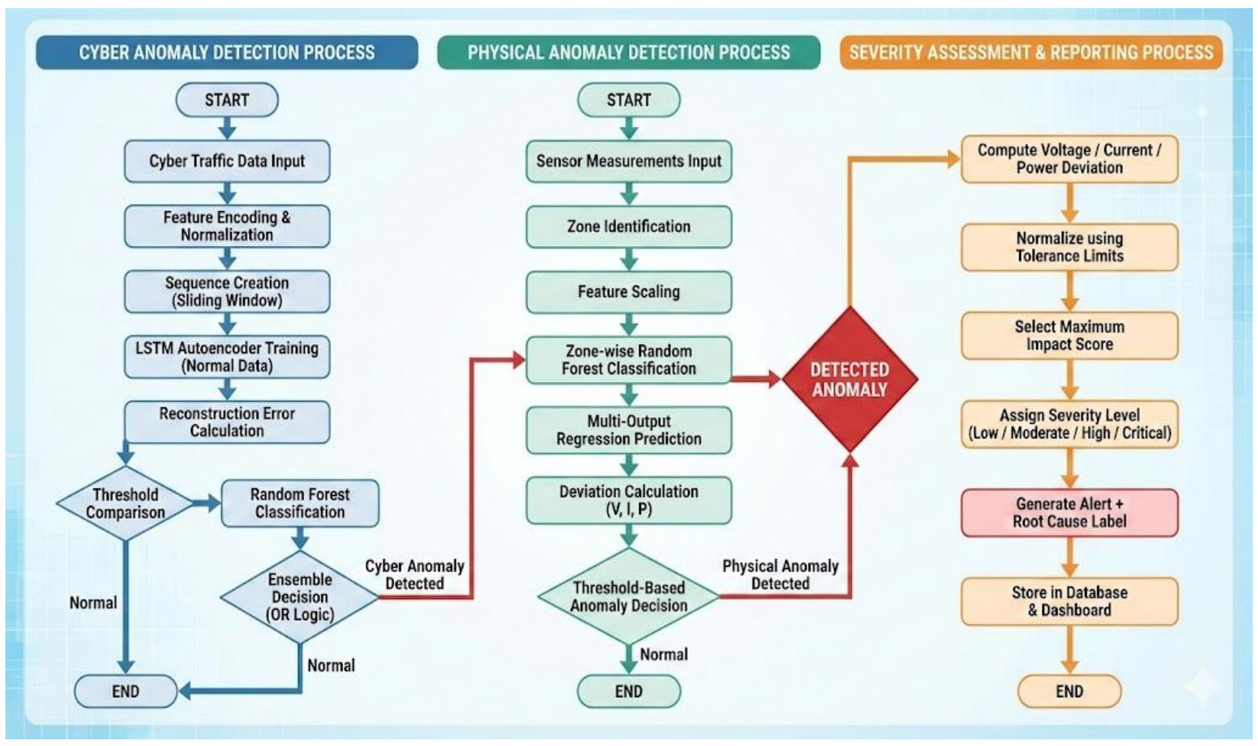
Problem Definition

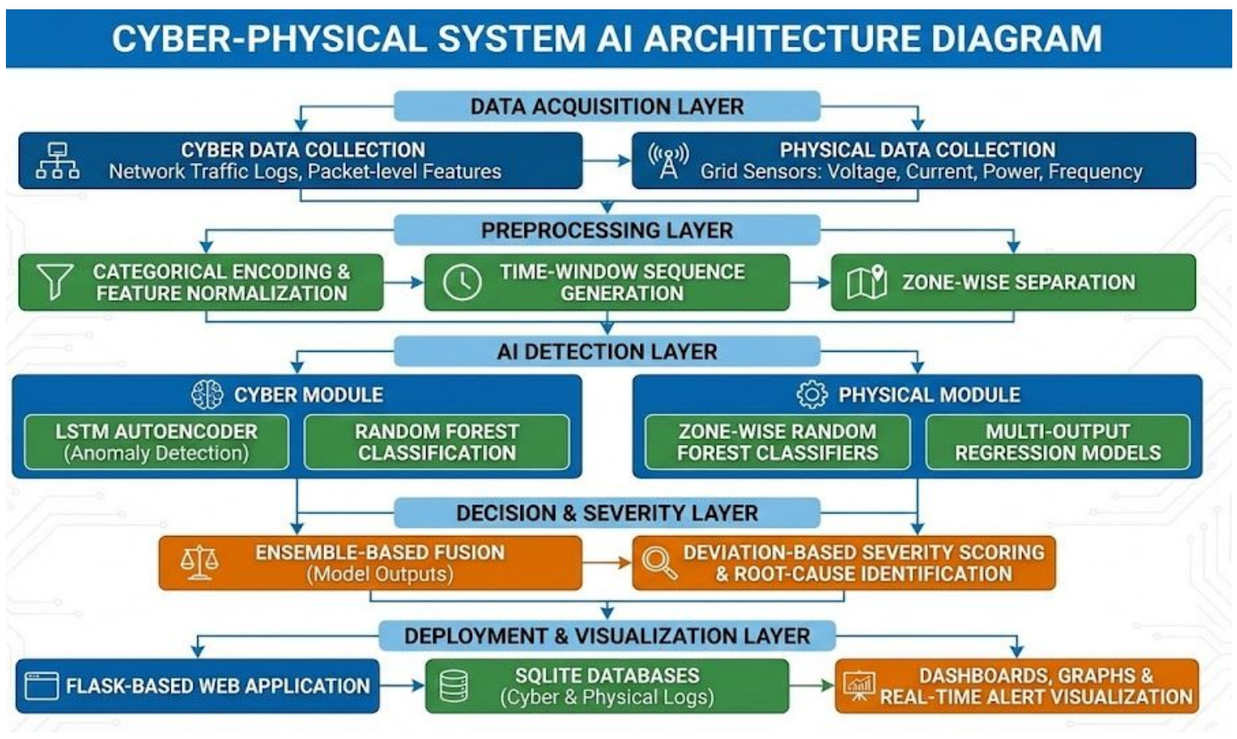
Current monitoring systems struggle to reliably distinguish normal operational variations from malicious or faulty behavior in time-series cyber and power grid data, resulting in false alarms and missed anomalies.

Objectives

- To detect cyber-attacks and physical anomalies in smart grid environments using AI techniques
- To model normal system behavior using time-series learning
- To improve detection accuracy through ensemble learning
- To provide interpretable and reliable anomaly detection
- To enable real-time monitoring and visualization of anomalies

Methodology

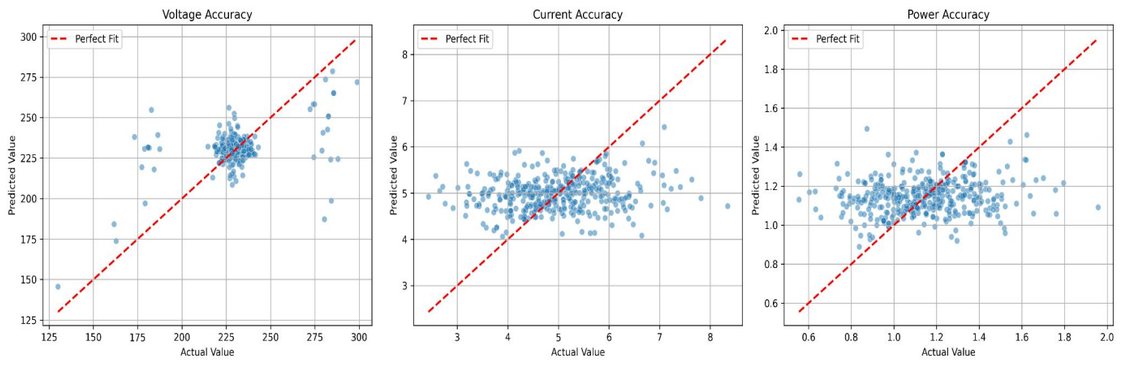




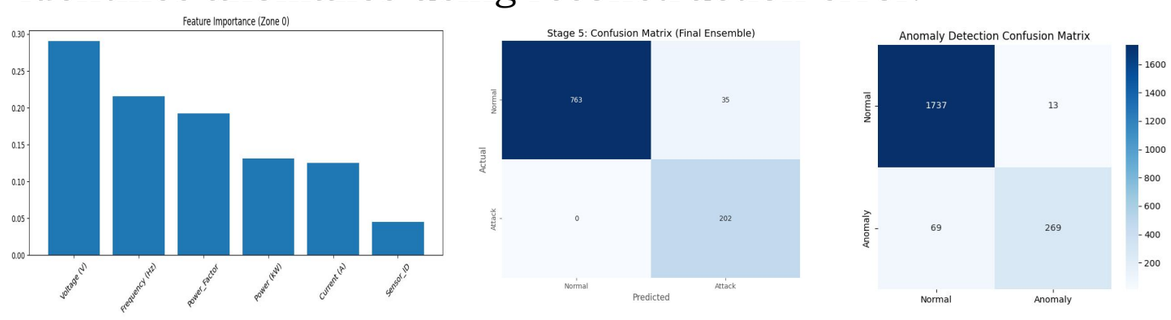
Tools used

- Programming Language: Python
  Deep Learning: LSTM Autoencoder
  Machine Learning: Random Forest Classifier
  Libraries: NumPy, Pandas, Scikit-learn, TensorFlow/Keras, Matplotlib, Seaborn
  Web Framework: Flask
  Database: SQLite
  Visualization: Confusion matrices, feature importance plots, time-series graphs

Results and Discussions



The proposed framework effectively detects both cyber-attacks and physical anomalies with high accuracy and low false alarm rates. The LSTM autoencoder successfully learns normal temporal behavior and identifies anomalies using reconstruction error.



Conclusions

This project presents an AI-based cyber-physical anomaly detection framework for smart grids that combines deep learning and ensemble machine learning models. By integrating temporal modeling, feature-based classification, and zone-wise analysis, the system overcomes the limitations of traditional monitoring methods. The results demonstrate improved detection accuracy, interpretability, and practical applicability, making the framework suitable for real-world smart grid security and monitoring applications.

References

- T. Yin, S. A. R. Naqvi, S. P. Nandanoori and S. Kundu, "Advancing Cyber-Attack Detection in Power Systems: A Comparative Study of Machine Learning and Graph Neural Network Approaches," 2024 Resilience Week (RWS), Austin, TX, USA, 2024
- Y. Xu, "A Review of Cyber Security Risks of Power Systems: From Static to Dynamic False Data Attacks," in Protection and Control of Modern Power Systems, vol. 5, no. 3, pp. 1-12, July 2020
- G. Liang, J. Zhao, F. Luo, S. R. Weller and Z. Y. Dong, "A Review of False Data Injection Attacks Against Modern Power Systems," in IEEE Transactions on Smart Grid, vol. 8, no. 4, pp. 1630-1638, July 2017
- O. A. Beg, L. V. Nguyen, T. T. Johnson and A. Davoudi, "Cyber-Physical Anomaly Detection in Microgrids Using Time-Frequency Logic Formalism," in IEEE Access, vol. 9, pp. 20012-20021, 2021,
- A. Ameli, A. Ayad, E. F. El-Saadany, M. M. A. Salama and A. Youssef, "A Learning-Based Framework for Detecting Cyber-Attacks Against Line Current Differential Relays," in IEEE Transactions on Power Delivery, vol. 36, no. 4, pp. 2274-2286, Aug. 2021