RV College of Engineering®
Mysore Road, RV Vidyaniketan Post,
Bengaluru - 560059, Karnataka, India

Report on Experiential Learning / Project Based Learning

ACY 2025-26

THEME:

SDG 11: Sustainable Cities and Communities

Title of the Project:

Power Grid Anomaly Detection and Prediction of Physical and Cyber Attacks

Sl. No.	Program	USN	Name	Email Id
1.	ET	1RV23ET039	Sanjay CM	sanjaycm.et23@rvce.in
2.	ET	1RV23ET069	Satkrit Samyaan	satkritsamyaan.et23@rvce.edu.in
3.	EC	1RV23EC005	Abu Arshian	abuarshian.ec23@rvce.edu.in
4.	EC	1RV23EC042	Dhruvi Bhandari	dhruvibhandari.ec23@rvce.edu.in
5.	EI	1RV23EI066	Siddhant Shah	siddhantshah.ec23@rvce.edu.in

Sl. No.	Evaluators
1.	Dr. Mohana
2.	Dr. Jayanthi P N

ABSTRACT

The increasing digitalization of power systems has transformed traditional electrical grids into smart grids that integrate advanced sensing, communication, and automation technologies. While this transformation improves efficiency and reliability, it also exposes the grid to complex cyber-physical threats, including cyber-attacks and subtle physical faults. Conventional threshold-based monitoring systems are insufficient to detect such anomalies due to the dynamic, time-dependent nature of smart grid data.

This project presents an **AI-based anomaly and cyber-attack detection framework** that jointly analyzes **power grid sensor data** and **network traffic data** to identify abnormal behavior. The proposed system employs **machine learning and deep learning models**, including **Random Forest and LSTM**, to model normal system behavior and detect deviations indicative of physical anomalies or cyber intrusions. Ensemble decision-making, temporal learning, and zone-wise modeling are used to improve detection reliability. A web-based interface enables real-time monitoring, visualization, and severity-aware alerts. Experimental results demonstrate that the proposed framework effectively detects both cyber and physical anomalies, improving robustness, interpretability, and operational usefulness in smart grid environments.

TABLE OF CONTENTS

INTRODUCTION

Smart grids signify a significant improvement over conventional power systems by combining electrical infrastructure with information and communication technologies (ICT). These systems depend on distributed sensors, smart electronic devices (IEDs), and communication networks to facilitate real-time monitoring, management, and enhancement of power generation, transmission, and distribution. The implementation of smart grids is essential for facilitating renewable energy incorporation, demand response, and smart city projects.

Even with these benefits, the growing dependence on digital communication and automation has greatly enlarged the vulnerability of power grids. Cyber-attacks like false data injection, denial-of-service, command injection, and unauthorized access can undermine grid stability, trigger power outages, and result in significant economic and social repercussions. Simultaneously, physical issues like equipment wear, line problems, and voltage fluctuations can appear as slight variations in sensor readings that are hard to identify with traditional monitoring methods.Conventional grid monitoring systems often depend on set thresholds and established rules, which are inadequate in changing operating conditions. These methods create false alerts amid harmless variations and frequently overlook gradually emerging or subtle anomalies. Additionally, many current systems consider cyber and physical anomaly detection as distinct issues, overlooking the interconnectedness between cyber and physical realms in today's smart grids.

AI-based systems helps to detect anomalies without relying on prior knowledge of attack signatures. This project focuses on developing an integrated, data-driven, cyber-physical anomaly detection framework that leverages AI models to improve the security, reliability, and resilience of smart grid systems.

Literature Review

Title: A Comprehensive Review of Machine Learning and Deep Learning-Based Intrusion Detection Systems

Authors: Divya M K, V. Ebenezer

Year of Publication: 2025

Inference:

This paper surveys intrusion detection systems using machine learning and deep learning techniques. It categorizes IDS into signature-based and anomaly-based approaches and discusses models such as Random Forest, SVM, CNN, and LSTM. The study highlights the effectiveness of ensemble and temporal models in detecting unknown and zero-day attacks while addressing challenges such as high false positives and data imbalance.

Title: Enhancing Smart Grid Security: A Data-Driven Anomaly Detection Framework

Authors: Nguyen Khanh Son, Arun Kumar Sangaiah, Darshan Vishwasrao Medhane, Mohammed J. F. Alenazi, Salman A. AlQahtani

Year of Publication: 2024
Inference:

This work presents an unsupervised anomaly detection framework using Gaussian Mixture Models (GMM) to detect anomalies in smart grids without labeled data. Detected anomalies are classified into cyber-attacks or natural events using supervised machine learning models, with Random Forest achieving high accuracy. SHAP is used for explainability, improving system transparency and trust.

Title: A Learning-Based Framework for Detecting Cyber-Attacks Against Line Current Differential Relays

Authors: Amir Ameli, Abdelrahman Ayad, Ehab F. El-Saadany, Magdy M. A. Salama, Amr Youssef

Year of Publication: 2021
Inference:

This paper proposes a learning-based framework using a multilayer perceptron to detect False Data Injection Attacks (FDIA) and Time Synchronization Attacks (TSA) on protection relays. The model differentiates cyber-attacks from physical faults using selected electrical features and is validated on the IEEE 39-bus system, demonstrating high robustness and accuracy.

Title: Cyber-Physical Anomaly Detection in Microgrids Using Time-Frequency Logic Formalism

Authors: Omar Ali Beg, Luan Viet Nguyen, Taylor T. Johnson, Ali Davoudi
Year of Publication: 2021
Inference:

This study introduces a cyber-physical anomaly detection framework using parametric time-frequency logic (PTFL). By analyzing voltage and current signals in both time and frequency domains, the approach detects cyber-attacks and physical faults without requiring detailed system models. The method is effective in identifying subtle and stealthy anomalies in microgrid environments.

Title: A Review of False Data Injection Attacks Against Modern Power Systems

Authors: Gaoqi Liang, Junhua Zhao, Fengji Luo, Steven R. Weller, Zhao Yang Dong
Year of Publication: 2017
Inference:

This paper provides a comprehensive review of False Data Injection Attacks in modern power systems. It discusses theoretical foundations, attack construction techniques, physical and economic impacts, and defense strategies. The study emphasizes the limitations of traditional bad data detection methods and highlights the need for advanced AI-based detection techniques.

Title: A Review of Cyber Security Risks of Power Systems: From Static to Dynamic False Data Attacks

Authors: Yan Xu
Year of Publication: 2020
Inference:

This paper analyzes the impact of static and dynamic false data injection attacks on economic dispatch, state estimation, and power system stability. It highlights how dynamic attacks can evade traditional detection techniques and stresses the

importance of time-aware and adaptive detection models for improving smart grid resilience.

Title: Advancing Cyber-Attack Detection in Power Systems: A Comparative Study of Machine Learning and Graph Neural Network Approaches

Authors: Tianzhixi Yin, Syed Ahsan Raza Naqvi, Sai Pushpak Nandanoori, Soumya Kundu
Year of Publication: 2024
Inference:

This paper compares conventional machine learning methods, deep learning models, and graph neural networks (GNNs) for cyber-attack detection in power systems. The results show that GNN-based approaches outperform traditional models in detecting and localizing attacks, highlighting the importance of spatial relationships in smart grid security.

Title: Adaptive Cyber Attack Detection in Distribution Systems Using Machine Learning and Spatiotemporal Patterns

Authors: S. Shakila Bhanu, Vadla Sujith Kumar, Kodi Hari Krishna et al.
Year of Publication: 2025
Inference:

This study proposes a hybrid GNN–LSTM framework for cyber-attack detection in power distribution systems. GNNs capture spatial grid relationships, while LSTMs model temporal attack patterns. The system achieves high detection accuracy with low latency and incorporates explainable AI using SHAP for improved interpretability.

Title: Hybrid AI Anomaly Detection for Smart-Grid Electricity Theft

Authors: Taejun Choi, Yifei Wu, Ryan K. L. Ko
Year of Publication: 2025
Inference:

This paper presents a hybrid anomaly detection approach combining CNN–LSTM models with unsupervised outlier detection techniques to identify electricity theft in smart grids. The framework effectively captures temporal consumption patterns and improves detection accuracy through feature selection, supporting scalable and adaptive smart grid security solutions.

Title: Enhancing Smart Grid Security with Machine Learning: A Comparative Study of Supervised and Unsupervised Techniques

Authors: Abdirizak Abdullahi Khalif, Abubakar Abdi Warsame, Jafar Ismail Mohamed et al.
Year of Publication: 2025
Inference:

This study compares supervised and unsupervised machine learning techniques for smart grid cybersecurity. It evaluates models based on accuracy, complexity, and scalability, identifying strengths and limitations of each approach. The paper highlights the need for adaptive and hybrid ML models to handle evolving cyber threats in smart grids.

Title: Telling Apart: ML Framework Towards Cyber Attack and Fault Differentiation in Microgrids

Authors: Tapadhir Das, Suman Rath, Shamik Sengupta
Year of Publication: 2024
Inference:

This paper proposes a multi-stage machine learning framework to differentiate between malicious cyber anomalies and malfunction anomalies in microgrids. The framework uses supervised ML models along with Explainable AI (XAI) techniques to identify influential features responsible for each anomaly type. By distinguishing cyber-attacks from physical faults, the system improves response accuracy, transparency, and operational reliability.

Title: Dynamic Graph-Based Anomaly Detection in the Electrical Grid

Authors: Shimiao Li, Amritanshu Pandey, Bryan Hooi, Christos Faloutsos, Larry Pileggi
Year of Publication: 2022
Inference:

This work introduces DYNWATCH, a topology-aware anomaly detection algorithm that models the electrical grid as a dynamic graph. The method incorporates graph distances based on Line Outage Distribution Factors (LODF) to capture power flow changes caused by topology variations. By combining temporal weighting and statistical anomaly detection, the approach effectively detects natural faults and cyber-attacks while accommodating regular topology changes.

Title: A Method of Abnormal Detection for Power Grid Control System Metrics Based on AI Platform

Authors: Shen Jialing, Ji Xuechun, Gao Shang, Kong Yanru, Li Hao, Lao Yingying
Year of Publication: 2024
Inference:

This paper presents an AI-based real-time anomaly detection method for power grid control system metrics using sliding windows and ensemble learning. Slow-climbing anomalies are detected using the Mann–Kendall trend test, while sudden metric mutations are identified through multi-algorithm ensemble techniques. Dynamic thresholds generated via short-term time-series prediction enable adaptive and early anomaly detection, significantly outperforming traditional fixed-threshold approaches.

Problem Statement:

Modern smart grids generate large volumes of time-series data from both physical sensors and communication networks. Current monitoring and security systems struggle to reliably distinguish between normal operational variations, physical faults, and malicious cyber behavior in such data. Static threshold-based methods are prone to false alarms and missed detections, while rule-based systems lack adaptability to evolving attack patterns and changing grid conditions. Additionally, many existing approaches treat cyber and physical anomaly detection independently, failing to capture their interdependence in cyber-physical systems. As a result, anomalies often go undetected or are detected too late, leading to potential grid instability, equipment damage, and service disruptions.

Objectives:

The main objectives of this project are as follows:

1. To design an AI-based framework capable of detecting both physical anomalies and cyber-attacks in smart grid environments.

2. To model normal operational behavior of power grid sensors using machine learning techniques and identify deviations as physical anomalies.

3. To analyze network traffic data using time-series learning to detect cyber intrusions and abnormal communication patterns.

4. To improve detection accuracy and robustness through ensemble learning and temporal modeling using Random Forest and LSTM.

5. To provide real-time monitoring, visualization, and logging of detected anomalies through a web-based interface.

6. To generate actionable insights that assist grid operators in timely decision-making.

System Overview and Architecture

The proposed system is designed as a cyber-physical anomaly detection framework consisting of the following major components:

- Data acquisition and preprocessing
- Physical anomaly detection module
- Cyber-attack detection module
- Machine learning and deep learning models
- Data storage and logging
- Visualization and monitoring interface

1. Physical Dataset

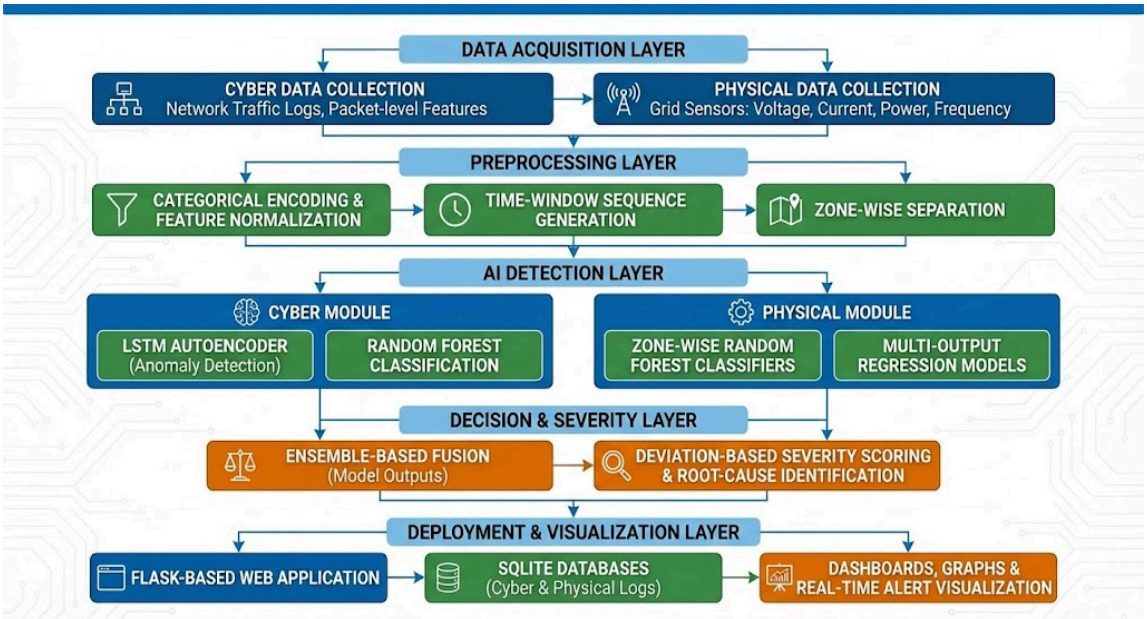
The physical dataset consists of power grid sensor measurements collected over time. The key features include:

- Timestamp
- Sensor ID
- Location or zone
- Voltage (V)
- Current (A)
- Power (kW)
- Frequency (Hz)
- Power factor

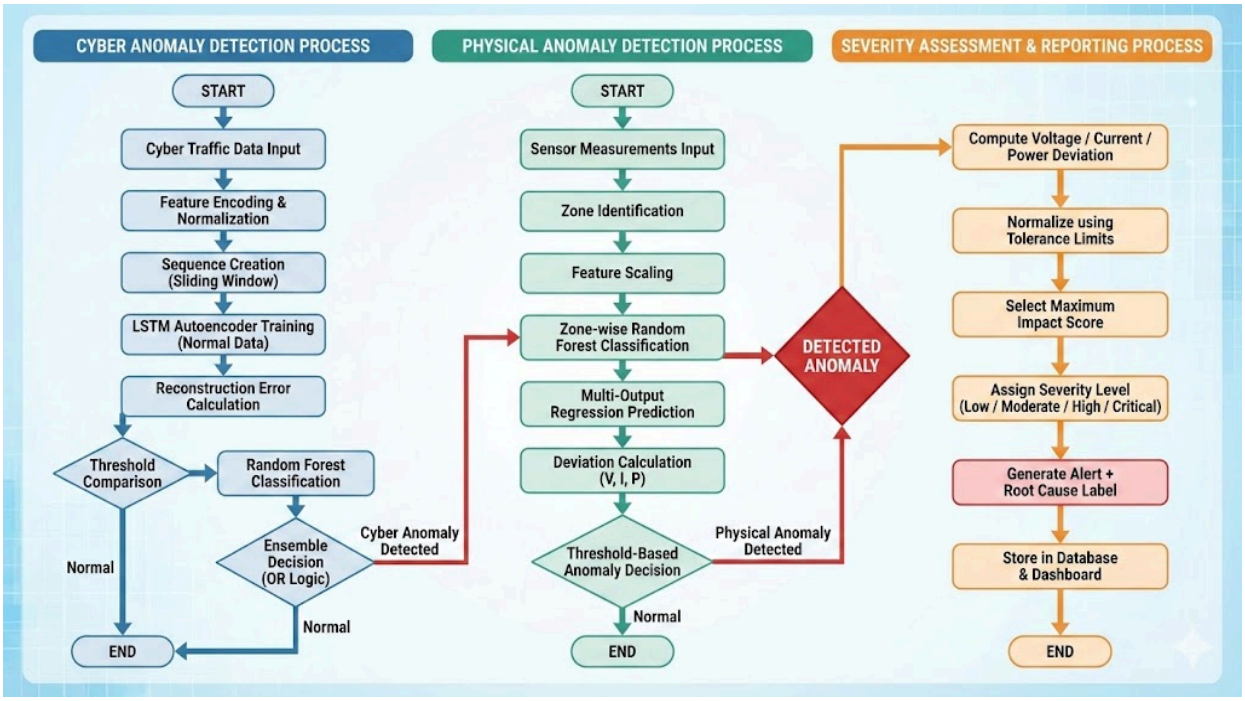
2. Cyber Dataset

The cyber dataset consists of network traffic measurements representing communication between grid components. The features include:

- Timestamp
- Source IP and destination IP
- Port number
- Protocol
- Packet size
- Latency, throughput, jitter
- Authentication failure indicators



FLOWCHART:



Methodology:

1. Data Preprocessing

Data preprocessing involves cleaning missing or invalid values, normalization, and feature scaling. For physical data, zone-wise normalization is applied to account for variations in operating conditions across different grid locations. For cyber data, relevant traffic features are extracted and standardized.

2. Physical Anomaly Detection

The physical anomaly detection module uses zone-wise Random Forest models trained on normal operational data. Each zone has its own model and scaler, reflecting the heterogeneous behavior of grid segments. The model learns normal sensor patterns and flags deviations as anomalies. This approach significantly reduces false alarms compared to global thresholding.

3. Cyber-Attack Detection

Cyber-attack detection is performed by analyzing network traffic patterns. The system employs a hybrid approach combining machine learning models and interpretable heuristic rules to detect suspicious behavior such as abnormal packet sizes, protocol misuse, and traffic spikes. The framework is designed to be easily extendable to fully ML-based or LSTM-based cyber detection.

4. Temporal Learning Using LSTM

LSTM models are used to capture temporal dependencies in both physical and cyber data. By learning time-series patterns, LSTM networks help distinguish between transient fluctuations and genuine anomalies. This temporal modeling improves detection accuracy and reduces false positives.

5. Ensemble Decision-Making

Ensemble learning using Random Forest combines multiple decision trees to improve robustness and generalization. The ensemble approach helps handle noisy data and diverse anomaly patterns, making the system more reliable under real-world conditions.

6. Web-Based Deployment

The entire framework is implemented as a Flask-based web application that provides:

- Real-time anomaly detection
- Visualization dashboards
- Historical anomaly logs
- Severity-based alerts

Detected events are stored in SQLite databases for physical and cyber domains separately.

Results and Discussion:

1. Physical Anomaly Detection Results

The physical anomaly detection module successfully identifies abnormal sensor behavior across different grid zones. Zone-wise modeling significantly reduces false positives caused by normal operational variations. The results demonstrate high consistency and reliability.

2. Cyber-Attack Detection Results

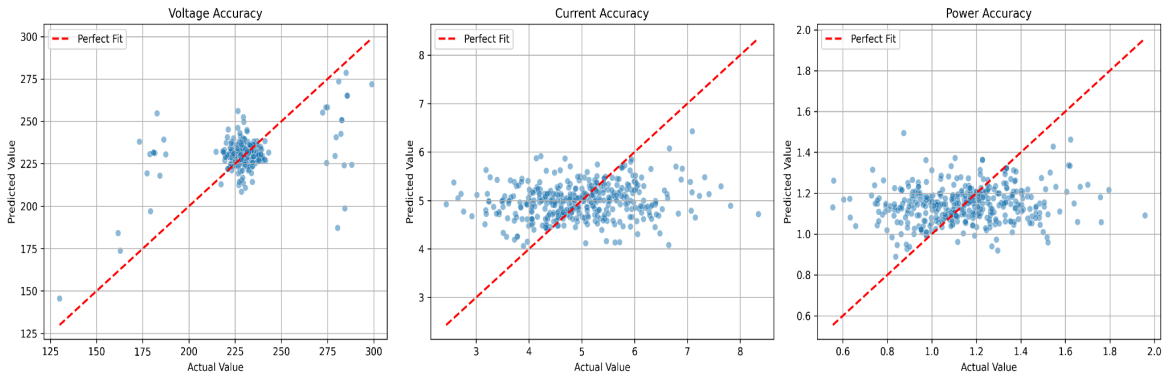
The cyber detection module effectively flags suspicious network traffic patterns. The hybrid detection approach ensures interpretability and stability while maintaining detection performance.

3. Overall System Performance

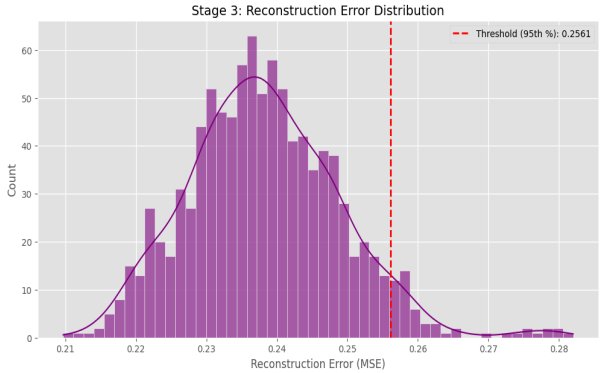
The combined cyber-physical framework outperforms single-domain detection approaches. Temporal learning and ensemble decision-making significantly improve detection reliability and operational usefulness.

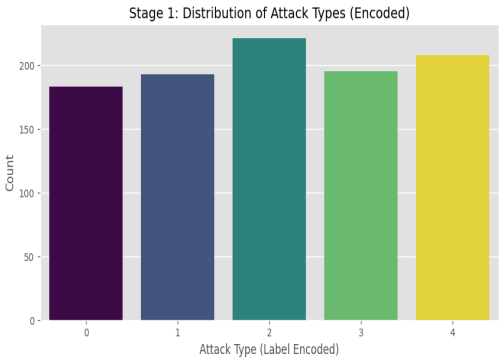
```
Accuracy: 0.960727969348659

Classification Report:
              precision    recall  f1-score   support

           0       0.96      0.99      0.98      1750
           1       0.95      0.80      0.87       338

    accuracy                           0.96      2088
   macro avg       0.96      0.89      0.92      2088
weighted avg       0.96      0.96      0.96      2088


Confusion Matrix:
[[1737   13]
 [  69  269]]
```

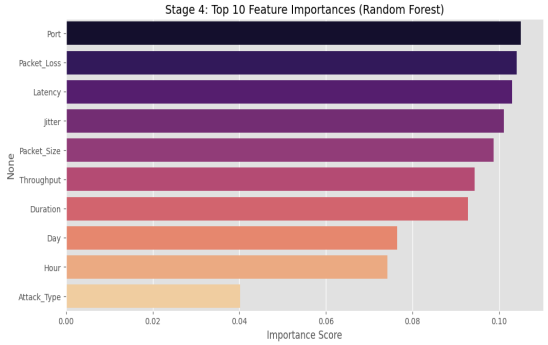
	precision	recall	f1-score
0	1.00	0.95	0.97
1	0.84	1.00	0.91
accuracy			0.96
macro avg	0.92	0.98	0.94
weighted avg	0.97	0.96	0.96

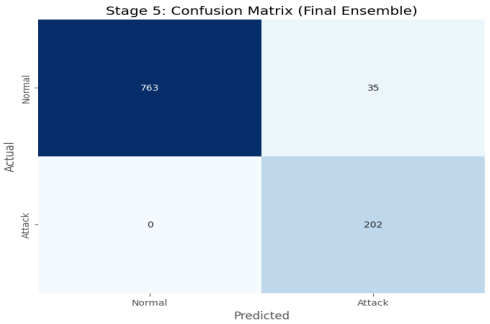


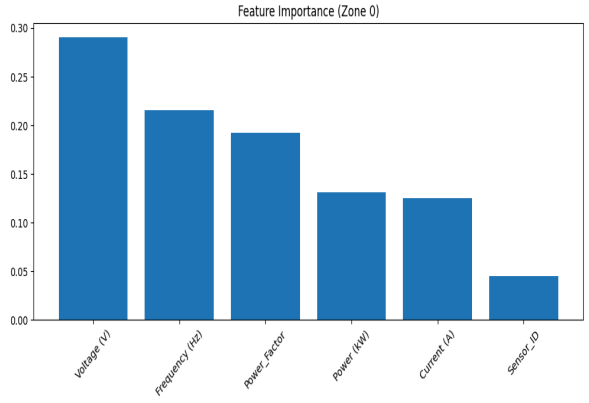
The graphs and matrices obtained are shown below and the explanations and observations are also given:

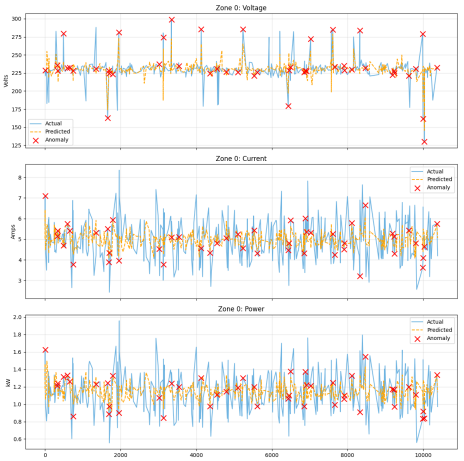












bar chart represents the distribution of different cyber-attack categories in the dataset after label encoding. Each bar corresponds to a specific attack type encoded numerically, and the height indicates the number of samples belonging to that category.

This histogram displays the distribution of reconstruction errors (MSE) produced by the trained LSTM autoencoder. A red dashed line marks the anomaly detection threshold, typically set at the 95th percentile.

This horizontal bar chart ranks the top ten most influential features used by the Random Forest classifier in cyber-attack detection. Features include protocol, packet loss, latency, jitter, packet size, throughput, and time-based features.

This confusion matrix compares actual labels (normal/anomaly) with predicted labels obtained using reconstruction-error-based anomaly detection. It quantitatively evaluates detection performance in terms of true positives, true negatives, false positives, and false negatives.

Conclusion:

This project presents a detailed and comprehensive AI-based anomaly and cyber-attack detection framework for smart grid environments. By jointly analyzing physical sensor data and cyber network traffic, the proposed system effectively addresses the limitations of traditional monitoring approaches. The integration of Random Forest and LSTM models enables robust, adaptive, and time-aware anomaly detection. The end-to-end implementation demonstrates practical feasibility and provides a foundation for future smart grid security solutions.

Future Scope:

1. Integration of Graph Neural Networks for topology-aware detection
2. Online and adaptive learning for evolving threats
3. Deployment on real-time SCADA systems
4. Enhanced explainable AI for operator trust
5. Integration with edge and fog computing

References:

- S. Jialing, J. Xuechun, G. Shang, K. Yanru, L. Hao and L. Yingying, "A Method of Abnormal Detection for Power Grid Control System Metrics Based on AI Platform," 2024 IEEE 8th Conference on Energy Internet and Energy System Integration (EI2), Shenyang, China, 2024,
- S. Li, A. Pandey, B. Hooi, C. Faloutsos and L. Pileggi, "Dynamic Graph-Based Anomaly Detection in the Electrical Grid," in IEEE Transactions on Power Systems, vol. 37, no. 5, pp. 3408-3422, Sept. 2022
- T. Das, S. Rath and S. Sengupta, "Telling Apart: ML Framework Towards Cyber Attack and Fault Differentiation in Microgrids," 2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS), St. Louis, MO, USA, 2024,
- A. A. Khalif et al., "Enhancing Smart Grid Security with Machine Learning: A Comparative Study of Supervised and Unsupervised Techniques," 2025 International Conference on New Trends in Computing Sciences (ICTCS), Amman, Jordan, 2025
- T. Choi, Y. Wu and R. K. L. Ko, "Hybrid AI Anomaly Detection for Smart-Grid Electricity Theft," 2025 IEEE PES 35th Australasian Universities Power Engineering Conference (AUPEC), Brisbane, Australia, 2025
- S. S. Bhanu, V. S. Kumar, K. H. Krishna, A. R. Reddy, B. V. S. Reddy and P. M. Khan, "Adaptive Cyber Attack Detection in Distribution Systems using Machine Learning and Spatiotemporal Patterns," 2025 International Conference on Intelligent Computing and Control Systems (ICICCS), Erode, India, 2025
- T. Ige, C. Kiekintveld and A. Piplai, "An Investigation into the Performances of the State-of-the-art Machine Learning Approaches for Various Cyber-attack Detection: A Survey," 2024 IEEE International Conference on Electro Information Technology (eIT), Eau Claire, WI, USA, 2024
- S. Sankar, R. Dutta and S. Karmakar, "Cyber Threat Prediction and Assessment with Machine Learning Approaches," 2024 IEEE 21st India Council International Conference (INDICON), Kharagpur, India, 2024
- Y. R. Bhavyashree, M. K. Kavyashree and K. R. Amrutha, "Systematic Review on Frameworks for Intrusion Detection using Machine Learning and Deep Learning Algorithms," 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON), Bengaluru, India, 2024
- M. Baptiste, F. Julien and S. Franck, "Systematic and Efficient Anomaly Detection Framework using Machine Learning on Public ICS Datasets," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2021,
- D. M K and V. Ebenezer, "A Comprehensive Review of Machine Learning and Deep Learning-Based Intrusion Detection Systems," 2025 First International Conference on Intelligent Computing and Communication Systems (CICCS), Bengaluru, India, 2025
- N. Nelufule, C. Mudau, B. Nkwe, S. Chishiri, L. Mncwango and M. Mutenwa, "Cybersecurity in Smart Grids using Machine Learning: A Systematic Literature

Review," 2025 6th International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS), Bengaluru, India, 2025

- S. Kasturi, U. Chandrashekhar, M. V. Galindo, A. B. M. Valencia, T. C. Manjunath and S. Vashishtha, "Development of an AI-Based Cybersecurity Framework for Reliable Smart Grid Energy Management," 2025 International Conference on Sustainability, Innovation & Technology (ICSIT), Nagpur, India, 2025
- M. N. Kurt, O. Ogundijo, C. Li and X. Wang, "Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach," in IEEE Transactions on Smart Grid, vol. 10, no. 5, pp. 5174-5185, Sept. 2019