A Synopsis Report

On

SMART GRID PROTECTION FROM CYBER THREATS USING MACHINE LEARNING ALGORITHMS

A Project Report Submitted
In Partial Fulfillment of the Requirements
for the Degree of

BACHELOR OF TECHNOLOGY

in

Electrical Engineering

(Session: 2025-26)

by

Vaibhav Chaudhary (2207340200061)
Rahul Kumar (2207340200034)
Richa Singh (2207340200038)
Stuti Singh (2207340200057)

Under the Supervision of
Dr. Pushpendra Singh

RAJKIYA ENGINEERING COLLEGE BANDA
Affiliated to
Dr. APJ ABDUL KALAM TECHNICAL UNIVERSITY, LUCKNOW

1. Introduction

With the increasing integration of advanced communication infrastructure, real-time monitoring, and automation, modern electrical networks have evolved into **Cyber-Physical Smart Grids (CPSG)**. While this digital transformation enhances flexibility and efficiency, it simultaneously exposes power systems to a broad range of **cyberattacks**, especially at critical control and measurement points such as AGC loops, substations, PLCs, and SCADA systems.

Cyberattacks such as **False Data Injection (FDI)**, **Denial of Service (DoS)**, **Replay Attacks**, and **Coordinated Multiclass Attacks** aim to mislead the control center or degrade stability. Traditional rule-based protection schemes are inadequate against these intelligent, dynamic threats.

To address these challenges, this project proposes a **Machine Learning–based Intrusion Detection and Protection Framework** for smart grids. A **MATLAB Simulink-based 9-Bus Power System** is integrated with **AI/ML algorithms** such as Spatio-Temporal Graph Neural Networks (ST-GNN), Deep Learning classifiers, and multiclass detection models. The model identifies cyber anomalies in real time and initiates protection actions (e.g., breaker tripping) through a simulated **Modbus–SCADA communication layer**.

Objectives

1. To design a MATLAB Simulink-based **9-Bus Cyber-Physical Smart Grid Testbed** for generating voltage-current time-series data.
2. To simulate **cyberattacks** including FDI, DoS, and Replay through MATLAB Function-based attack injection.
3. To perform **multi-class attack detection** using advanced Machine Learning algorithms.
4. To develop a **graph-based feature extraction model** for capturing spatial and temporal dependencies of power system measurements.
5. To integrate a **SCADA–Modbus layer** for real-time model communication and automatic protection control.
6. To implement a **virtual protection mechanism** (breaker operation) triggered by machine learning–based anomaly alerts.
7. To evaluate model performance using accuracy, confusion matrix, and response time.

2. Literature Review

2.1 Cyber-Physical Fusion for GNN-Based Attack Detection

The paper *"Cyber-Physical Fusion for GNN-Based Attack Detection in Smart Power Grids"* presents a hybrid GNN-based approach to model both electrical topology and cyber dependencies. It highlights the importance of **graph representation learning** for attack detection and shows that GNNs outperform traditional ML models in detecting complex cyber-physical intrusions. This study supports our choice of using **graph-based machine learning** for anomaly detection in smart grids.

2.2 Cyber-Physical Power System: Modeling and Cyber Security Applications

The paper provides a detailed review on modeling and simulation techniques for CPSG systems. It emphasizes the need for integrated testbeds that combine **power system simulation, cyber network emulation, and control logic**. The authors highlight vulnerabilities in SCADA, PLCs, and communication channels. This paper validates our approach of creating a **Simulink–SCADA integrated testbed** for cyberattack experimentation.

2.3 Deep Learning-Based Multiclass Attacks Detection in AGC Systems

The paper proposes a deep learning model for detecting multiple attack types in Automatic Generation Control (AGC). It introduces the idea of **multiclass classification**, where attacks like FDI, DoS, load alteration, and ramp attacks are detected simultaneously using deep neural networks.
This supports our implementation of **multiclass ML models** to detect multiple types of cyberattacks in real time.

3. System Design and Methodology

The proposed system consists of three integrated layers:

3.1 Smart Grid Simulation Layer (MATLAB Simulink)

A **3-Bus transmission system** with generators, transmission lines, loads, and measurement blocks is implemented in MATLAB Simulink.
Key features include:

- Three-phase Voltage and Current measurement using Vabc/Iabc blocks
- powergui for discrete simulation

- MATLAB Function blocks for cyberattack injection
- Controlled Breaker for protection actions
- Workspace logging of real-time data

Simulated cyberattacks:

- **False Data Injection (FDI)** → modifies measurements using biased offsets
- **DoS** → sensor data blocking or freezing
- **Replay Attack** → substitutes live data with stored historical values

3.2 Machine Learning Detection Layer (Python)

The dataset exported from MATLAB is preprocessed using:

- Sliding window segmentation
- Normalization
- Graph-based feature grouping

Machine Learning models used:

1. **Spatio-Temporal Graph Neural Network (ST-GNN)**
2. **Deep Learning Multiclass Classifier**
3. **Graph Attention Network (GAT)** for topology learning

These models classify grid conditions as:

- Normal
- FDI Attack
- DoS Attack
- Replay Attack

3.3 SCADA–Modbus Communication Layer

A virtual communication channel is implemented to simulate real SCADA behavior.

- AI model writes attack detection signals through **MATLAB Engine API** or virtual **Modbus registers**
- Simulink reads “AI_Alert” and “attack_type”

- If attack detected → breaker is tripped (protection action)
- Protection logs are stored in workspace

3.4 Working Principle

The working principle of the proposed Smart Grid Cyberattack Detection and Protection System is based on the integrated functioning of a Power System Simulation Layer (MATLAB Simulink), a Machine Learning Attack Detection Layer (Python), and a SCADA–Modbus Protection Layer. The interaction between these layers enables real-time anomaly detection and automated protection response against cyberattacks.

The working principle can be understood in the following detailed stages:

<u>Stage 1: Smart Grid Simulation and Data Generation (Simulink Layer)</u>

1. A 3-Bus power system is designed in MATLAB Simulink, consisting of:
    - Three-phase transmission lines
    - Loads
    - Generators
    - Circuit breakers
    - Measurement units (Vabc and Iabc)
2. The Simulink model continuously generates three-phase voltage and current data for each bus.
3. This output represents the physical layer of the cyber-physical smart grid.
4. These signals are captured using "To Workspace" blocks and stored as:
    - Bus1_Vabc, Bus2_Vabc, Bus3_Vabc
    - Bus1_Iabc, Bus2_Iabc, Bus3_Iabc
5. This data is exported into CSV/NumPy format to be processed by Python.

<u>Stage 2: Cyberattack Injection Mechanism (MATLAB Function Block)</u>

Cyberattacks are simulated inside Simulink using "MATLAB Function" blocks that modify measurement signals.

Types of attacks simulated:

1. False Data Injection (FDI)

- A biased offset is added to the Vabc or Iabc signals.
- Example:
  Vabc_modified = Vabc_original + offset

2. Denial of Service (DoS)

- Measurement data is frozen, blocked, or replaced by zeros.
- Example:
  Iabc_modified = [0 0 0]

3. Replay Attack

- Old stored data is played back instead of live measurements.

Attack variables such as:

- attack_on
- attack_type
- fdi_offset
- replay_buffer
- attack_target_bus

are controlled from Python or MATLAB workspace.

These attacks represent the cyber layer of the smart grid.

<u>Stage 3: Data Preprocessing (Python Layer)</u>

Once the data is exported from Simulink:

1. The dataset is normalized for ML compatibility.
2. A sliding window technique creates sequences of 10 time steps at a time.
3. Each window is flattened into a feature vector.
4. These windows capture temporal trends in bus voltages and currents.
5. The dataset is labeled for:
   - Normal
   - FDI

  - DoS
  - Replay attacks

This prepares the data for training the AI/ML models.

<u>Stage 4: Machine Learning Detection (ST-GNN Model)</u>

The core of the detection system is a Spatio-Temporal Graph Neural Network (ST-GNN).

How ST-GNN works:

1. Spatial Modeling (Graph Neural Network – GAT layer)
   - Each bus is considered a node in a graph.
   - Transmission lines are the edges.
   - The GAT layer learns interactions and dependencies between buses.
2. Temporal Modeling (1D Convolution Layer / Temporal Blocks)
   - Voltage-current data across time steps is used.
   - The CNN layer extracts temporal features to detect trends and anomalies.
3. Classification
   - The output layer predicts:
     - 0 → Normal
     - 1 → FDI
     - 2 → DoS
     - 3 → Replay

The ML model continuously evaluates incoming data from the MATLAB simulation.

<u>Stage 5: SCADA–Modbus Virtual Communication Layer</u>

Once the AI model detects an attack, it must notify the power system.

Process:

1. When predicted_label != 0, the AI activates: AI_Alert = 1
2. Python sets this flag in MATLAB using:
   - MATLAB Engine API, or

    - Virtual Modbus holding registers

3. Simulink continuously reads:
    - AI_Alert
    - attack_type

This layer simulates real SCADA communication between control center and substations.

Stage 6: Protection Mechanism (Breaker Operation)

When Simulink receives AI_Alert = 1:

1. The breaker connected to the targeted bus or line is triggered.
2. The breaker:
    - Isolates the compromised bus
    - Disconnects the load
    - Prevents further propagation of the cyberattack

Example:

If an FDI attack is detected at Bus-1:

- Breaker between Bus1 & Bus2 opens
- Bus1 is isolated
- Load or generator is disconnected

This prevents false measurements from destabilizing the grid.

Simulink logs the protection event:

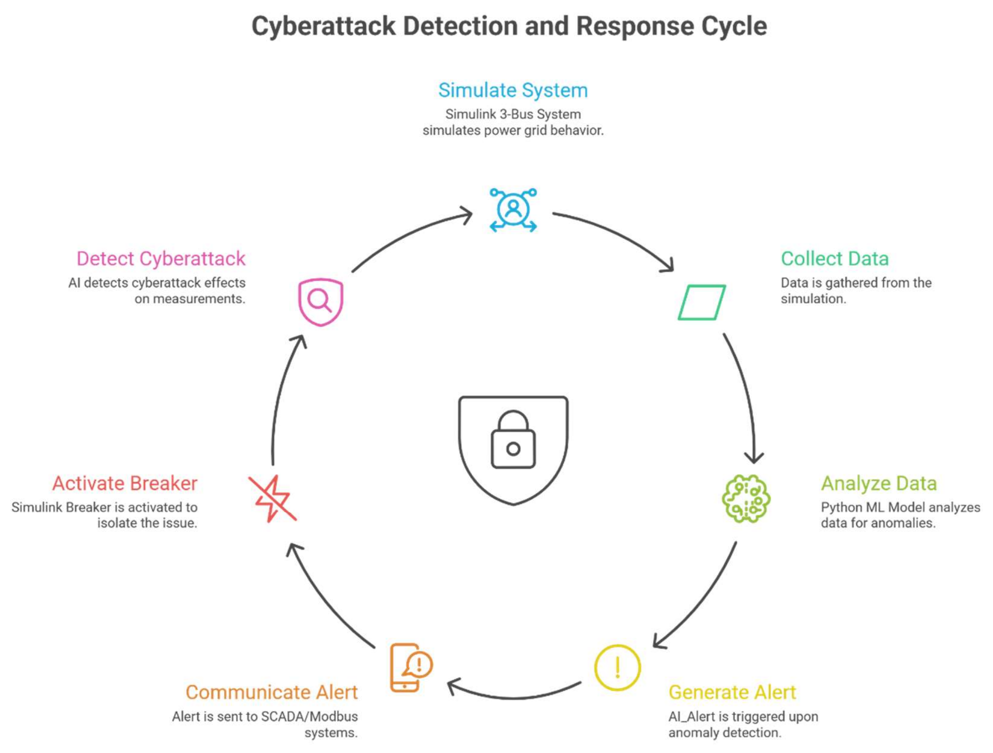
- Protection_Action = [time, bus_id, action_type]

The system includes real-time visualization via Python:

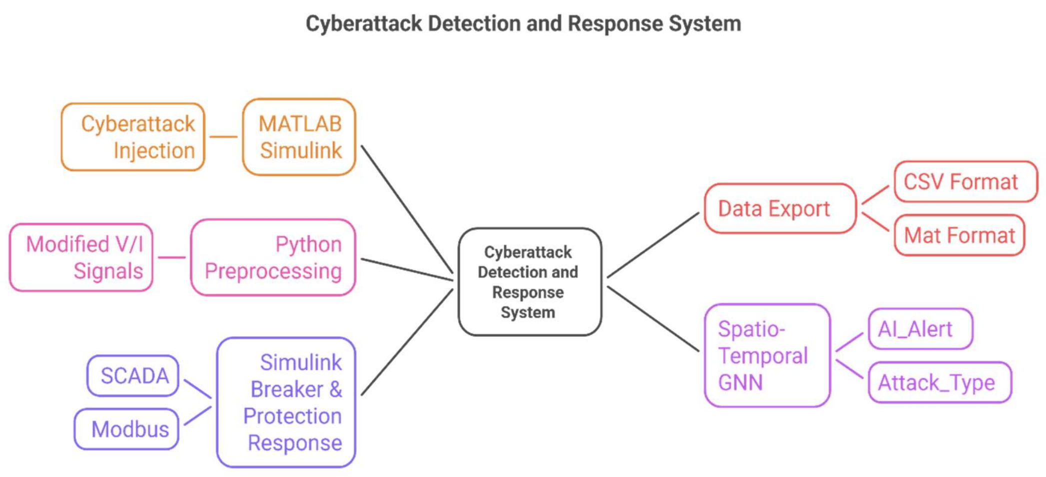
1. Live SCADA Dashboard
    - Animated voltage/current waveforms
    - Shows attack-induced disturbances
2. AI Decision Console
    - Prints prediction results in real time

3. Simulink Scopes
    - Shows physical response (breaker trip, waveform changes)

This demonstrates the complete cyber–physical interaction of the system.


Cyberattack Detection and Response Cycle
Simulate System
Simulink 3-Bus System simulates power grid behavior.
Collect Data
Data is gathered from the simulation.
Analyze Data
Python ML Model analyzes data for anomalies.
Generate Alert
AI_Alert is triggered upon anomaly detection.
Communicate Alert
Alert is sent to SCADA/Modbus systems.
Activate Breaker
Simulink Breaker is activated to isolate the issue.
Detect Cyberattack
AI detects cyberattack effects on measurements.

3.5 Block Diagram



4. Hardware / Software Used

Software

- MATLAB 2021+ (Simulink, powergui, Simscape)
- Python (VS Code)
- NumPy, Pandas, PyTorch, PyTorch Geometric
- MATLAB Engine API for Python
- Modbus-TCP (virtual)
- Matplotlib, Seaborn
- Anaconda Environment

Hardware

No physical hardware—fully software-based simulation.

5. Progress Made

1. 3-Bus Simulink smart grid model designed successfully.
2. V-I measurement and workspace data logging implemented.
3. Cyberattack injection (FDI, DoS, Replay) tested and validated.
4. Data preprocessing and sliding window segmentation completed.
5. ST-GNN model trained on synthetic and real Simulink data.
6. Integration of Python AI alerts with Simulink protection logic completed.
7. Real-time dashboard (SCADA-style visualization) implemented in Python.
8. Initial results show successful detection of attacks with high accuracy.

6. Outcomes

- Accurate multiclass detection of cyberattacks in smart grids.
- Development of an integrated cyber-physical testbed for research.
- Implementation of AI-based real-time protection (breaker trip).
- High classification performance validated with confusion matrix.
- Demonstrated end-to-end smart grid cybersecurity workflow.

7. References (IEEE Standard Format)

1. W. Xue, J. Zhao, and Z. Chakraborty, “Cyber-Physical Fusion for GNN-Based Attack Detection in Smart Power Grids,” *IEEE Transactions on Smart Grid*, 2022. DOI: 10.1109/OAJPE.2025.3594625

2. S. Ahmed, A. Hooshyar, and V. Dinavahi, “Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications,” *IEEE Access*, vol. 9, pp. 126192–126218, 2021. DOI: 10.1109/ACCESS.2020.3016826

3. J. Gupta, M. Abdelmalek, and S. Singh, “Deep Learning-Based Multiclass Attacks Detection and Classification in Automatic Generation Control,” *Electric Power Components and Systems*, vol. 51, no. 4, pp. 368–381, 2023. DOI: 10.1109/TII.2025.3575806