Format for uploading details of completed projects

1. Project details

a. *Title*: Development of a real-time cyber-attack detection module and its hardware-in-loop testing for an integrated power network

b. *Institute*: Indian Institute of Technology (Banaras Hindu University), Varanasi, India, 221005

2.Aim / Objectives:

- . To develop a detection model, which is independent of prior statistical assumptions of the grid parameter, based on a data driven approach
- Hardware-In-the-Loop Validation for Dynamic State Estimation
- To develop the best possible detection scheme working both for steady state and contingency scenarios in the power network
- Real-time detection of the effect of false data intrusions and the respective attack location to apply instant remedial action.
- To validate simulation results with an experimental testbed developed based on Real-Time Digital Simulator (RTDS) through Hardware-In-Loop tests

Following are the primary objectives of the project:

- Smart grid evolution: Fusion of physical infrastructure with information and communication systems.
- Vulnerability: Grid vulnerable to cyber threats
- Impact : Cyber intrusions cause opérationnel disruptions to the grid operators causing the unwanted corrective action, e.g., disconnecting power lines, load shedding, CB tripping etc.
- Requirement: Robust cyber-resilient operation immune to cyber-attack.
- Key step: Development of real-time cyber-attack detection, realization of the same in Hardware-in-loop simulation.

In this project, an effort has been made to develop an FDIA detection module with real time detection capability. The detection strategy has been implemented on secured local servers, enabling operators to ascertain the current grid status. Real-time measurements serve as the primary requirement, feeding into the module for analysis. The FDIA detection algorithm, operating on the secured local server, identifies the presence of false data in the system. It is imperative that the model be implemented on secured local servers to prevent insider attackers from modifying the model parameters. Testing of the FDIA detection model has been conducted under varying noise conditions and fault scenarios in the grid causing fluctuating voltage and power profiles. The model must demonstrate the capability to handle such situations. Extensive simulation and real-time testing have enhanced the training process of the model, ensuring robust performance under diverse grid operation conditions

2. **Executive Summary (*One page*):** Traditionally, power system state estimation (PSSE) has been considered an offline tool utilized to ascertain the state of the power system. In control centers, PSSE is employed to visualize the current status of the power system. Typically, control centers rely on static state estimation (SSE) methods, such as the weighted least squares (WLS) approach, for performing PSSE. These SSE methods are favored for their simplicity, accuracy, and reliability under stable operating conditions. SSE typically estimates the power system's state at regular intervals, typically every 30 to 60 seconds, using measurements collected from remote terminal units (RTUs) that update every 1 to 5 seconds. However, SSE does not take into account the updated measurements received from the RTUs during its execution, causing a lag between its results and the actual system states. This limitation makes it challenging to use SSE for real-time visualization of the power system states.

   In the context of the smart grid, there is a growing demand for online visualization of power system states due to the increasing complexity of power system networks. The emergence of phasor measurement units (PMUs) has significantly increased the reporting rate of measurement data, reaching up to 50 frames per second for 50-Hz systems and 60 frames per second for 60-Hz systems. This reporting rate is much faster compared to that of remote terminal units (RTUs). As a result, PMU measurements hold great potential for real-time visualization of power system states

   However, due to the high cost associated with deploying PMUs, the current practice does not involve online visualization of power system states using only PMUs. Consequently, several dynamic state estimation (DSE) algorithms have been developed to address the power system state estimation problem by utilizing all available field measurements from both RTUs and PMUs. These algorithms aim to enable real-time visualization of power system states. Before implementing these DSE algorithms in control centers, it is crucial to test and validate their performance in a simulated real-time environment. Real-time simulation tools, such as the Real Time Digital Simulator (RTDS), have been introduced to facilitate the testing and validation of power system DSE in a real-time setting. Through these simulations, it is possible to gain confidence in the design of DSE algorithms and validate their performance in a real-time environment.

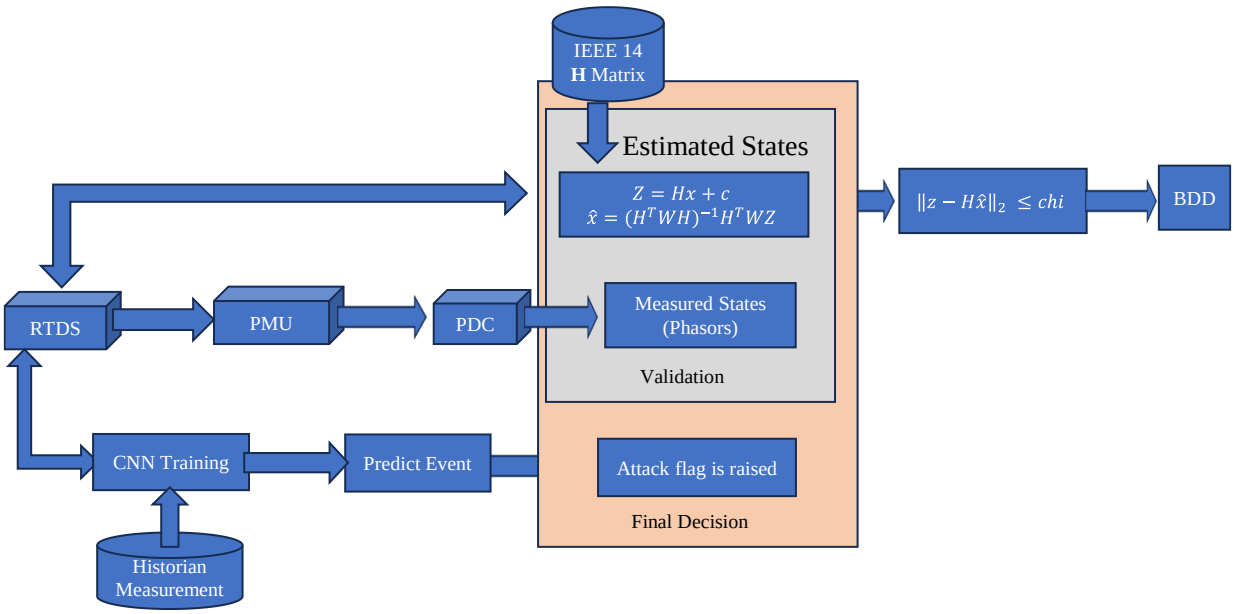


Fig 1:Schemetaic Diagram Of Real Time Detection Scheme

Further with augmentation of communication infrastructure the cyber attack is imminent and worthy to be considered in real time for complex power network. The development of a detection framework for false data injection attacks (FDIA) can be divided into two main components. The initial segment involves the real-time implementation of power system state estimation (PSSE) and its verification using time-stamped phasor time series data, which is concentrated within the software PDC, specifically SEL-5078-2 Synchrowave Central. The experimental setup was established using Real-Time Digital Simulator (RTDS), commercially available Intelligent Electronic Devices (IEDs), and industry-standard components to replicate the configuration. Subsequently, this identical setup was adapted for the real-time execution of a data-driven event classification and identification scheme. The comprehensive elucidation of the implementation and validation procedures can be found in the subsequent section. Figure 4 delineates the schematic representation of the proposed methodology, illustrating the sequential procedures and their respective importance

Cyberattack In Cyber-Physical Systems

In data integrity attacks and False Data Injection Attacks (FDIAs), the objective of the attackers is to manipulate measurement readings and alter the state of the system. The smart grid, as a complex cyber-physical system, consists of interconnected physical and communication components. The physical layer represents the power network, while the cyber layer comprises information and communication technology (ICT) systems and

measurement systems. In such attacks, the vulnerabilities in the system can be exploited by attackers to target the state variables of the system.

The attacker may focus on manipulating measurement devices, the communication network, or the system database to introduce misleading values that confuse the system operator. A data integrity attack can cause the Wide Area Monitoring and Control Center to misinterpret the state variables and generate incorrect control signals. In severe cases, this can lead to system instability or even a complete collapse. By carefully considering system vulnerabilities, an attacker can develop an effective attack vector that triggers cascading failures and disrupts the entire system. Therefore, defending against such attacks is crucial for system operators. To defend against data integrity attacks, there are three broad categories of measures: protection, detection, and mitigation. Detection involves identifying data integrity attacks, and an intrusion detection system (IDS) alerts the system operator when an attack or adversary is detected. Once alerted, the system operator can take mitigation steps to minimize the damage caused by the attack

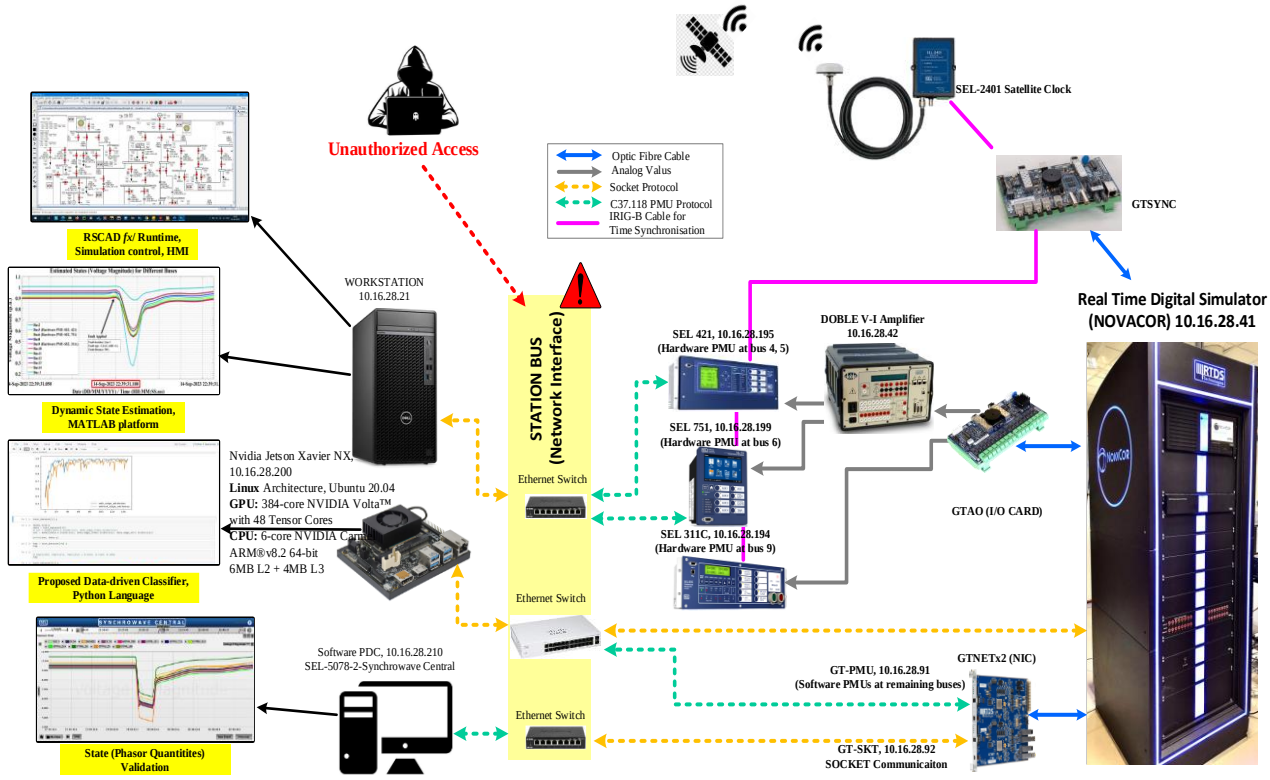
Description of investigation carried out

Lab setup-For the real-time implementation, first we have created a setup of laboratory equipment as shown in Figure 1. We have connected the Satellite Synchronized Clock (SEL-2401) to the GTSYNC card of the Real Time Digital Simulator (RTDS) to synchronize the time. GTNET, GTSYNC and GTAO cards are present inside RTDS Nova Core and are connected via fiber optic cable (FOC). We have used Hardware Phaser Measurement Unit SEL 421 (PMU) to measure RSCAD runtime output which is connected to the GTAO card via the FOC. To collect the data from PMU, we have used Synchro-wave central as Phasor Data Concentrator (PDC).

- The communication of the measurements for dynamic state-estimation relies on Socket protocol
- It supports integer and floating-point single precision (32-bit) numbers compliant to IEEE754
- Unit of data packets:
    - **1 data point (Minimum) = 4 Bytes**
    - **Maximum size = 300 data point / 1200 bytes**
- GTNET-SKT is capable of transmitting 60 data points each time-step (50 microseconds)

Real-time Power System State Estimation, The AI-based NVidia Jetson Development Kit has been used to estimate the states of the IEEE-14 bus systemA Graphics Processor Unit (GPU),

present in the Nvidia Jetson development kit enables state estimation in real time. GTNETSKT protocol has been used to receive real-time data from RTDS.



Experiments in Action

Fig:2**Hardware-In-the-Loop Result Validation for Dynamic State Estimation**

In this project, estimate the real-time state of the IEEE 14 bus system via a high-end workstation is accomplished.. The platform's high accuracy in estimating states for various natural events validates its robustness against changing operating conditions and abnormal data. Moreover, the high computational throughput obtained from the workstation confirms its scalability for real-world applications. To validate our findings, true states in phasor form are transmitted to the software PDC (SEL Synchrowave central) via different hardware PMUs compliant with the PMU protocol C37.118. Below, we present a few supporting results to substantiate this assertion. Figures illustrate the occurrence of a fault event, specifically the LL-G (AB-GS) fault type, which was applied at line-6, situated at a distance of 90% from the upstream bus. In Figure 3, the estimated states, encompassing the magnitudes of bus voltages, are presented. These estimations were obtained through the execution of state estimation using measurement data collected from sensors positioned at various locations. Figure 4 depicts the screenshot of the terminal of SEL-5078-2 Synchrowave Central software PDC. The PDC captures phasor values of the voltages at different buses. These phasor values have been utilized to validate the counterpart values estimated by state estimation and real-time validation of Hardware-In-the-Loop (HIL) is a accomplished.

CASE I: Fault at Bus-6

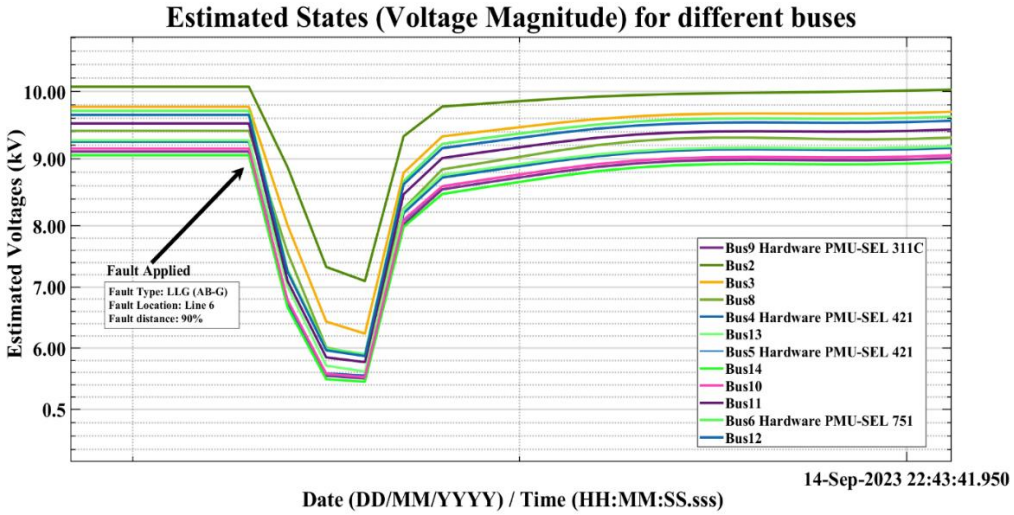


Figure 5: Case 1

Figure 3 depicts the screenshot of the terminal of SEL-5078-2 Synchrowave Central software PDC. The PDC captures phasor values of the voltages at different buses. These phasor values have been utilized to validate the counterpart values estimated by PSSE.

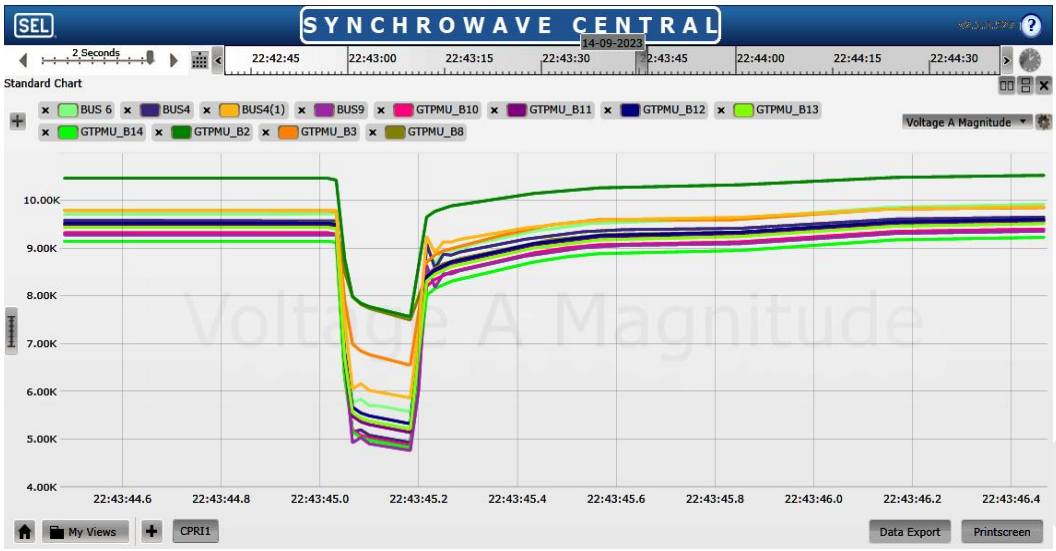


Fig.3 : SEL Synchrowave Central 5078-2

Both images consist of time series datasets that represent voltage magnitudes at various bus locations. These datasets serve the purpose of detecting and identifying various events in power systems, such as faults, steady-state operating conditions, and single line outages (n-1 contingencies). The temporal axis aligns with the moment of determination made by PSSE, whereas, it corresponds to the temporal stamps associated with various phasor values.

CASE II : Fault at Bus-2

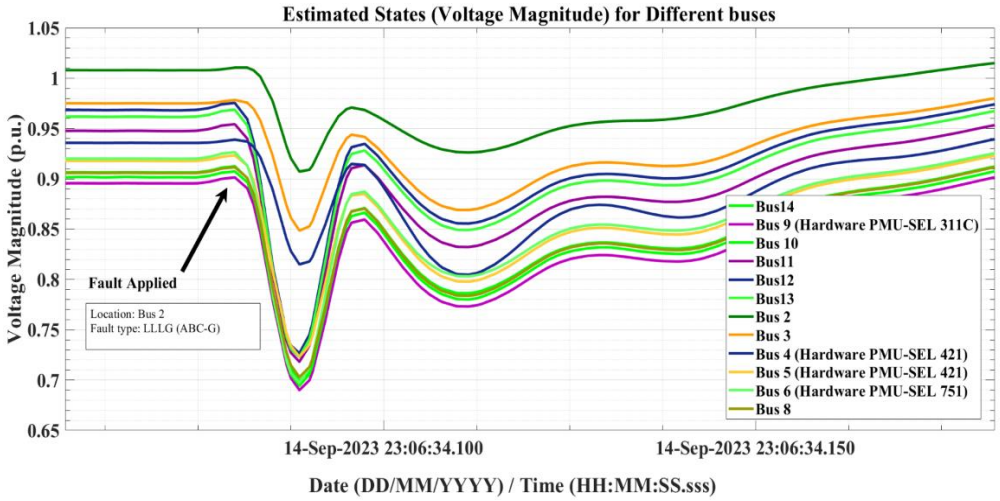


Fig 4: Case 2

Figure 4 displays real-time estimations of state variables, specifically voltage angles (in degrees) at various bus locations, in response to the line-16 outage. This figure 4 is characterized by a time axis and annotations that delineate the timing of the event and convey relevant information.

CASE III : SLG fault at Line-2

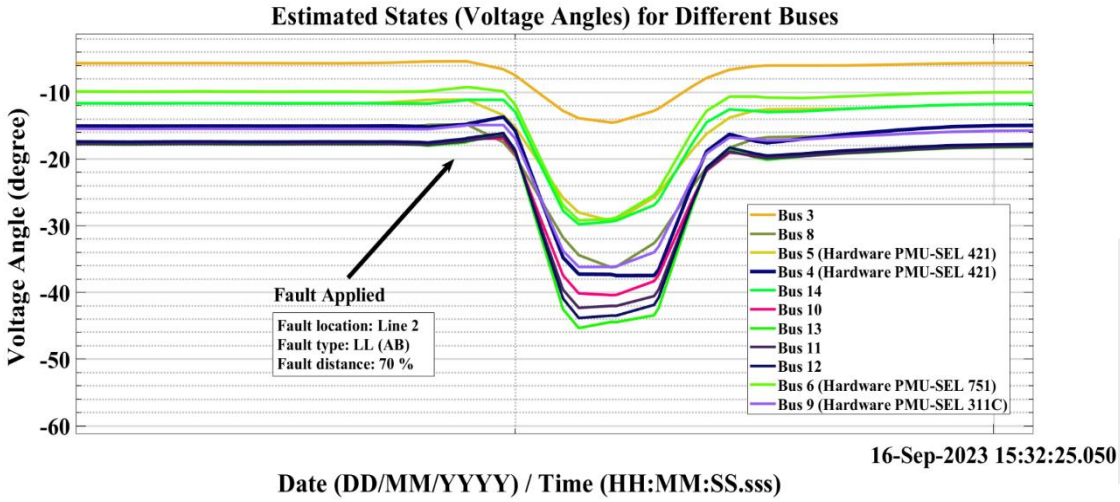


Fig 5: Case 3

Figure 8 illustrates the inferred system states, voltage angles (in degrees) associated with a line-2 fault, characterized as a double-line-to-ground (LL) fault occurring at a location 70% along the distance from the upstream bus.

It is to the pertinent snapshots employed for illustrative purposes in the context of the Hardware-in-the-loop experiment conducted within the established framework. Figures are comprised of two windows. The Window-1 pertains to the RSAC fx Runtime Graphical User Interface (GUI), which facilitates the management of simulations and the imposition of various operational scenarios, such as faults, line outages (n-1 contingency), and the

introduction of anomalies, specifically, false data injection attacks on sensor measurements. In contrast, the second interface, window-2, corresponds to the output terminal of the Nvidia Jetson Xavier Development Kit. This interface primarily exhibits the decisions made by the data-driven framework developed in response to the real-time manipulation of the simulation. Additionally, this display includes timestamps associated with event detection and decisions made by the developed framework.

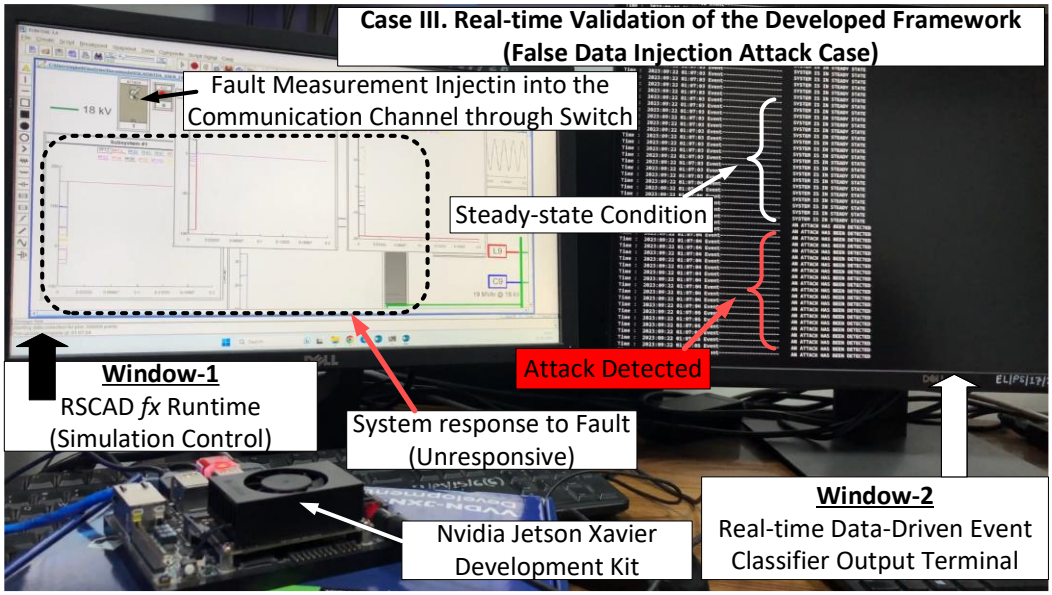


Fig 6 :Methodology in Action (Fault detection)

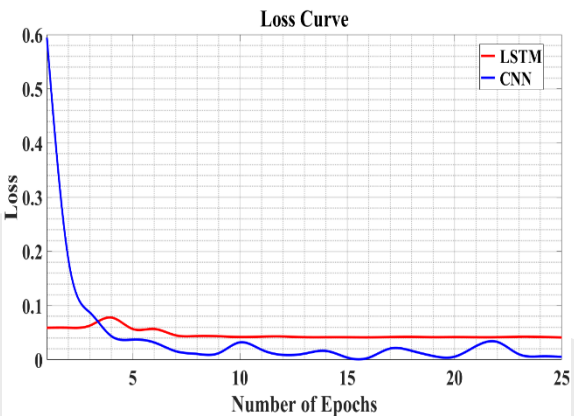
Figures 6 represent the identification of a system fault and Fault Detection, Isolation, and Accommodation (FDIA) detection, respectively. These visual representations include pertinent annotations to facilitate the visualization of the real-time experimental process.

Methodology in Action (Attack detection)

Figure 6 elucidates the intricacies of Window-2, delineating its significant role in the validation of decision-making processes and temporal efficiency within the developed framework, particularly concerning various event-driven scenarios.

Hardware-In-the-Loop Result Validation for Detection Framework

This section validates the performance of the developed CNN-base power system event classification framework by using accuracy curve and loss curve and its comparative analysis with LSTM-based sequence NNs.



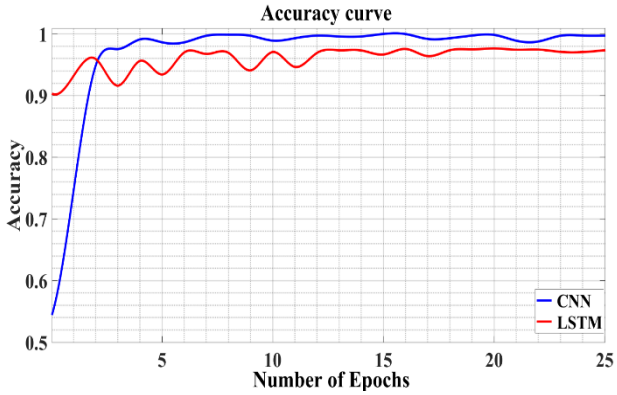


Figure 7: Performance assessment of the NNs

This section validates the performance of the developed CNN-base power system event classification framework by using accuracy curve and loss curve and its comparative analysis with LSTM-based sequence NNs.

3. Scope for further work

1. Early detection of cyber-attacks: The real-time cyber-attack detection module can detect attacks as they occur, allowing system operators to respond quickly and prevent further damage.

2. Reduced downtime: By detecting attacks early, the system can be shut down before significant damage occurs, reducing the downtime required for repairs and maintenance.

3. Improved reliability: The cyber-attack detection module can improve the reliability of the power grid by identifying potential threats before they can cause damage.

4. Enhanced cybersecurity: By continuously monitoring the power grid for cyber threats, the detection module can help to identify and mitigate potential vulnerabilities in the system.

5. Improved response times: The real-time detection module can significantly reduce response times to cyber threats, allowing system operators to quickly implement countermeasures to prevent further damage

4. Benefits visualized

Implementing a real-time cyber-attack detection module for a power system network involves several steps. Once the development of the module is successfully completed, the following steps can be taken to implement the module in the power sector:

1. Testing and Validation: Before implementing the module in the power sector, it is important to test and validate it thoroughly. The module should be tested under various conditions and scenarios to ensure that it can detect cyber-attacks accurately and in realtime. This testing should be done in a controlled environment to avoid any risks to the power system.

2. Integration with Power System Network: Once the module is tested and validated, it can be integrated with the power system network. The integration process will involve connecting the module to the power system network and configuring it to work with the existing systems.
3. Continuous Monitoring and Maintenance: Once the module is implemented, it should be continuously monitored and maintained to ensure that it is functioning properly. This will involve regular updates and upgrades to the module to keep up with the evolving threat landscape

4.The cyber physical test bed developed at the smart grid laboratory is immensely helpful for carrying out the research associated with practical challenge in the complex power network. It is worthy to mention the significant publication and solution of the practical problem in power system both in transmission and distribution level in the due course of time is the major thrust of the developed testbed.

Some of Publications Obtained From the Developed Testbed

1. D Mukherjee, S Ghosh, RK Misra A Novel False Data Injection Attack Formulation Based on CUR Low-Rank Decomposition Method IEEE Transactions on Smart Grid,,vol 13, issue6, pp.4965-4968,2022

2. A Jagan, U Prasad, SR Mohanty, SP Singh "Enhanced Adaptive Overcurrent Protection Scheme for AC Microgrid and Its Real-Time Validation Through Cyber Physical Power System Testbed" International Journal of Circuit Theory and Applications(Willey Publisher) vol.53,issue12, pp., 7325-7346,2024

3. U Prasad, SR Mohanty, S Singh, SP Singh Assessment of protection issues in active distribution networks with cyber attack-induced OLTC operations IEEE Transactions on Industry Applications vol.60 issue.6, pp.8168-8178,2024