A Reliable Phasor Measurement Framework Using Artificial Intelligence to Prevent False Data Manipulation

Hariprasath Manoharan[1,*], Sasi Kumar K[2]
[1]*Department of Electronics and Communication Engineering, Panimalar Engineering College, Poonamallee - 600123, Chennai, Tamil Nadu, India*
[2]*Department of Electrical and Electronics Engineering, Panimalar Engineering College, Poonamallee - 600123, Chennai, Tamil Nadu, India*
[*]*hari13prasath@gmail.com; sasikumar@panimalar.ac.in*

***Abstract*—This work introduces a novel intelligent security approach to improve the reliability of smart grid operations by protecting measurement data produced by the Phasor Measuring Unit. The increasing demand for power distribution requires continuous and accurate monitoring, which is dependent on reliable measurement data synchronized with strict timing constraints. To address the risks related to inaccurate measurements, unauthorized modification, and malicious disruption, this study develops a self-adaptive security analysis process using an artificial intelligence-based learning strategy. The system evaluates multiple operational factors and converts them into dynamic multivariate states to support accurate decision making. The proposed method integrates a learning mechanism based on nearest neighbor classification to detect abnormal measurement behavior and prevent false data events before operational failure occurs. An experimental evaluation in four scenarios demonstrates that the approach improves security and reliability metrics compared to existing solutions. The results confirm that the proposed method provides an effective pathway for reliable measurement data and resilient smart grid operation.**

***Index Terms*—Artificial intelligence; False data; Phasor measurement unit; Security; Smart grid.**

I. INTRODUCTION

In contemporary power generation and distribution systems, electrical networks increasingly rely on dedicated communication and measurement infrastructures to support reliable and efficient power flow. This transition has led to the evolution of conventional grids into intelligent smart grids, where real-time monitoring and decision-making are essential. However, the rapid growth in the number of connected users and distributed energy resources has made traditional power distribution mechanisms inadequate, necessitating a continuous assessment of line connectivity and operational conditions [1], [2]. Several recent studies [3]–[5] have highlighted that phasor measurement units (PMUs), which provide time-synchronized voltage and current measurements, play a critical role in maintaining grid observability and stability. At the same time, previous research has demonstrated that PMU-based systems are vulnerable to timing manipulation, false data injection, and communication-level attacks, which can significantly compromise grid security if not detected at early stages. These findings underline the importance of protecting both measurement accuracy and synchronization mechanisms in smart grids.

Conventional assessment of line connectivity and device integrity often relies on manual inspection or isolated monitoring approaches [6], [7], which are impractical in large-scale interconnected grids due to manpower limitations and high error probability. Therefore, data-driven and artificial intelligence-based methods have been explored in the literature to improve anomaly detection and security enforcement. Although these methods contribute valuable insights, many existing approaches address individual aspects such as communication attacks, protocol vulnerabilities, or static security assessment, without jointly considering time synchronization, residual measurement behavior, and component-level variations. In practical smart grid environments, power measurements are primarily derived from voltage and current phasors.

Any degradation in observability or synchronization can propagate errors between interconnected units, potentially leading to cascading failures. This requires a unified framework capable of detecting abnormal measurement behavior, identifying false data, and maintaining reliable grid operation under dynamic conditions. Motivated by these challenges, the present work incorporates time-periodic synchronization, artificial intelligence-based learning, and PMU-driven observability analysis to enable early detection and prevention of false data manipulation. Accordingly, a real-time monitoring framework is proposed in which synchronized PMU measurements are analyzed using supervised learning and nearest neighbor classification to detect anomalies across interconnected grid units. The proposed approach is designed to operate under varying system conditions and two-way communication scenarios, thereby enhancing the security and reliability of smart grid operations. The block diagram of the proposed PMU-based security framework is illustrated in Fig. 1.

Manuscript received 21 January, 2026; accepted 27 March, 2026.

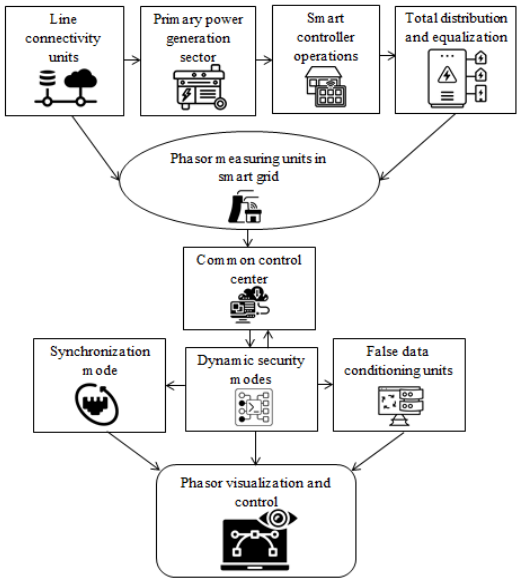


Fig. 1. Block diagram of PMU security in smart grids.

A. Background and Related Works

For the purpose of representing all design characteristics in smart grids, this part identifies the comparison with existing works. It is crucial to examine the devices that address the issue of security in data units, since background work offers crucial information on the grid that is connected at earlier stages where line connectivity is established. Additional grid representations with different levels of observability must be noticed throughout the process of equalization in these systems to minimize the number of fault units. The study conducted by the authors in [1] examines a novel side channel assault and proposes strategies to mitigate the occurrence of such attacks in the context of transient executions, where the phasor measurement unit (PMU) precision measurement unit adjusts all triggering points. During the execution process, only weak points are examined, whereas the potential propagation of attacks at different locations is not considered at any one time. Given the dynamic nature of attack processes, it is imperative to incorporate a threat model into autonomous detection units conducted by PMU at different locations. The paper examines a data-driven strategy derived from global positioning systems (GPS), which involves the transfer of data between different locations, thus providing assistance to future generation systems [2]. The smart grid elements implemented in GPS exhibit significant variances across key infrastructures, prompting an analysis of the interoperability, resilience, and sustainability aspects. A four-state strategy is discovered for the parametric outcomes mentioned above, in which a local area network PMU is attached, resulting in a reduction in security within the overall system. To mitigate the presence of local networks, a reinforcement learning approach is implemented, referred to as a dynamic process [3]. A multi-stage game technique is intended in smart grids to ensure equal full loss across all connected networks, enabling future actions with other grid users. The distributed technique offers insight into defense mechanisms and protection strategies, allowing for an observation of attackers from several perspectives. However, it is important to note that a physical representation is not offered in this particular scenario.

Furthermore, a variety of metrics releated to data integrity assaults are shown as evaluations to facilitate crucial decision-making. Consequently, the data dispatch process, which incorporates many protocols, is offered as supplementary components [4]. The compromise of entire data due to particular protocol peculiarities necessitates the provision of sub-optimal alternatives that offer equal contingencies. The presence of resiliency losses is found when all compromised aspects are obtained when there are changes in the operating points. This is considered a significant drawback that cannot be resolved at any stage. Therefore, a two-layer strategy has been devised to establish a restoration state for the deployment of comprehensive service features. This approach involves making optimal arrangements through the implementation of a rescheduling mechanism [5]. To perform rescheduling activities of this nature, non-dispatchable distributed networks are interconnected. This allows for the resolution of the demand response through low-cost connectivity. The distribution of representations is facilitated by a two-way mathematical model, resulting in the achievement of a standard design. However, the constraints imposed by different scenarios vary, making it impossible to establish ideal planning techniques due to the alteration of complete grid connections prior to restoration. On the other hand, a comprehensive analysis of erroneous data is conducted, encompassing both static and dynamic fluctuations. This analysis involves the identification of power system problems using a phasor measurement unit (PMU), as well as the analysis of overloads induced by dispatch units using micro-grid representations [6]. To address several vulnerabilities, certain countermeasures are implemented to prevent consecutive loading, hence mitigating the risk of misleading data injections. Synchronization is also inadequately provided, resulting in complete destruction of the sequential process in the event of additional attacks. In such cases, a migration is required between neighboring PMU nodes.

In addition, a well-defined implementation strategy is also presented that outlines potential future directions and problems. This strategy aims to address numerous uncertainties by implementing predetermined conditions, which emphasizes the importance of overcoming threat models [7]. However, these issues are prevalent in numerous instances where the modernization of bidirectional communication is necessary to enhance the compatibility of interconnected smart grid units in future states. However, to ensure the security of the PMU, these modernizations can only be implemented if all faults are detected, which is not feasible in real-time scenarios due to the growing interconnection of the grid. The correct adherence to the structure, dynamics, and principles of grid observability is necessary due to the increased dispersal of various load units. This requires a departure from traditional grid connection [8]. When examining individual structures, it is imperative to take into account all economic factors that do not disrupt the growth of potential dynamics. Consequently, significant network connections may fail, necessitating the utilization of external devices for connection. When external devices are connected, the combined data is seen to be

represented, resulting in a higher level of data robustness. This, in turn, disrupts the overall power flow. To effectively manage power flow activities, it is necessary to strategically position a micro PMU. This placement will enhance the visibility of distribution cases at certain points, while also ensuring standard synchronizations [9]. The comparison of the proposed and existing approaches, together with their relevance to the objective functions, is presented in Table I.

TABLE I. EXISTING VS. PROPOSED.

Ref.	Methods/Algorithms	Objectives			
		A	B	C	D
[10]	Advanced metering infrastructure for attack and defense techniques	✓	✓		
[11]	Two stage stochastic optimization for solving uncertainties in smart grid		✓	✓	
[12]	Smart grid monitoring with the Internet of Things (IoT) for security management		✓		✓
[13]	Decision support system for grid resource intensive problems	✓			✓
[14]	Application of machine learning for power system security			✓	✓
[15]	Classification method for analyzing load entropies in smart grid	✓	✓		
[16]	Implementation of cyber-attack model in critical smart grid infrastructure			✓	✓
Proposed	Machine learning for smart grid security with PMU observable units	✓	✓	✓	✓

Note: A: Data measurements and transit time periods; B: Observation of component attacks and equal residual data; C: PMU security violations; D: Accuracy of grid points

B. Research Gap and Motivation

The data presented in Table I indicate that a higher number of analyses are performed in cases where there are challenges in performing parametric assessments. Furthermore, the entire smart grid exhibits significant problematic characteristics due to the increased number of line connections, resulting in unequal power distributions and allotted loads. The security characteristics of the data are reduced as a result of time-synchronization failure, leading to an observed increase in demand and, subsequently, limiting various elements of the smart grid. Furthermore, current methodologies exhibit certain limitations that require resolution through the proposed strategy.

RG1: Can time synchronization be achieved through the collaboration of central units for the purpose of transmitting and receiving data jointly?

RG2: Can false data and the actual condition of device operations in a smart grid be accurately measured for all incremental power flows?

RG3: Is it possible to identify various threats without compromising security features by enhancing location accuracy?

C. Major Contributions

The suggested method incorporates artificial intelligence optimization to address the gap in existing methodologies by identifying bogus data and enhancing the security of the smart grid. Therefore, the objective functions that offer help close the gap between the current and ideal approaches are as follows.

– To minimize transit time and accurate data measurements across all additional power routes, hence balancing different needs.

– To detect residual data and mitigate potential component attacks, it is necessary to monitor sudden changes in contrast to past states.

– The objective is to reduce security breaches in different grid connections, hence enhancing the precision of PMU measurements.

II. PROPOSED SYSTEM MODEL

This section presents a selection of common mathematical representations for smart grid measurements, which are specifically designed to account for variations in different parameters. Given the necessity of maintaining a perpetual representation for all measuring units, it is imperative to enhance security measures to prevent parametric deviations in all instances, including data indicating units. Therefore, in the context of the construction of smart grids using phasor measurement units (PMUs), the information exchange process involves the use of transmitting and receiving units, in which counter measurement values are processed and displayed as follows.

A. Data Transit Time

Given the elevated security risks associated with data terminal units, it is essential to detect attacks that occur during data transmission. The transit time deviation for each PMU data packet is evaluated to identify abnormal delays between transmitting and receiving units. The transit time deviation is defined using (1) as follows

$$\Delta T_i = min\left|C_t\left(R_i\right) - C_t\left(T_i\right)\right|, i = 1, 2, ..., n, \quad (1)$$

where C_t denotes the time stamping function synchronized with the central clock unit, R_i indicates the reception time stamp of the i^{th} PMU data packet at the control center, T_i represents the transmission time stamp of the same i^{th} PMU data packet at the PMU, and n is the total number of PMU data packets observed within a given monitoring interval.

The index i consistently refers to an individual PMU measurement instance on both sides of the equation. The absolute difference between transmission and reception time stamps quantifies the transit delay, while the minimum value is used to detect abnormal deviations caused by communication faults or malicious interference. Equation (1) establishes that synchronizing transmission and reception time stamps through a central clock unit enables consistent alignment of PMU measurements across the grid. In PMU-based systems, even small timing mismatches can result in phase angle errors, incorrect state estimation, and misinterpretation of system dynamics. By computing the transit time deviation between transmitting and receiving units with respect to a common clock reference, abnormal delays caused by communication faults, clock drift, or malicious timing manipulation can be detected at an early stage. Once such deviations are identified, the affected measurements are excluded or corrected before they propagate to higher-level monitoring and control processes.

This prevents the accumulation of timing-induced inconsistencies across interconnected grid components, which is a primary cause of large-scale data failure in smart grids. Therefore, central clock-based adjustment directly contributes to maintaining data reliability and mitigating the risk of complete data failure.

B. False Data Measurements

Due to the high and dynamically varying loading conditions in PMU-enabled smart grid units, it is essential to detect and suppress erroneous measurements arising from false data injection. To evaluate the impact of false data on individual branch flows, a false data impact metric is defined using (2) as follows

$$f_d(b) = min\left(I_p(b) \times V_f(b)\right), b = 1, 2, ..., B, \quad (2)$$

where $I_p(b)$ denotes the incremental power flow magnitude at the i^{th} connected branch, expressed in per-unit, $V_f(b)$ indicates a dimensionless false data weighting factor that indicates the presence and severity of corrupted PMU measurements at the same branch, $f_d(b)$ is a scalar false data impact metric that quantifies the contribution of false measurements to branch-level power flow deviation, and n is the total number of monitored branches or PMU measurement instances.

The operator "·" denotes the scalar multiplication applied to each measurement instance. By minimizing $f_d(b)$, the optimization process suppresses the influence of corrupted data on incremental power flows, thus preventing false measurements from propagating across interconnected grid units.

C. Residual Grid Data

To mitigate the risk of malicious data injection attacks, it is essential to quantify the residual deviation between the expected and received PMU measurements. Residual grid data represent inconsistencies that arise when injected or manipulated data deviate from the normal system state. The residual deviation metric is defined in (3)

$$RD_i = min\sum_{i=1}^{n} \rho_m(i)(\alpha_i - \beta_i), \quad (3)$$

where $\rho_m(i)$ denotes the actual measured PMU state at the i^{th} node, α_i represents the estimated or predicted state vector under normal operation, and β_i indicates the received or observed state vector.

The minimization objective ensures that residual deviations are constrained within acceptable thresholds, allowing abnormal data patterns caused by cyber-attacks to be identified.

D. Component Attacks

Component attacks arise from abrupt changes in grid elements, such as transmission lines, sensors, or PMU-connected components. These attacks often manifest as sudden variations in reactance or connectivity, which directly affect grid observability. The impact of component-level disturbances is quantified using (4)

$$CA_b = min\sum_{i=1}^{n} \omega_r(b) \times \Delta_a(CS_b - PS_b), \quad (4)$$

where $\omega_r(b)$ denotes reactive variation associated with the i^{th} component, $(CS_b - PS_b)$ indicates abrupt changes in current and previous states, and Δ_a captures abrupt deviations between consecutive states.

The minimization objective enforces stability by limiting abnormal reactance changes beyond predefined thresholds. Significant deviations in this metric indicate potential component-level attacks that compromise PMU observability and system reliability.

E. Security Violations

Even when residual deviations are minimized, security violations may occur due to insufficient monitoring or compromised PMU nodes. To address this, a weighted inspection-based security violation metric is defined in (5)

$$V_i = min\sum_{i=1}^{n} \tau_w(i) \aleph_i, \quad (5)$$

where τ_w denotes the inspection weight assigned to the i^{th} PMU based on its criticality and $\aleph_i$ indicates the number of inspection or validation instances.

The minimization objective ensures that security risks are reduced by assigning a higher inspection priority to vulnerable or critical nodes. This formulation enables continuous monitoring of PMU integrity and prevents unauthorized access or data breaches in grid-connected units.

F. Location Accuracy

Accurate spatial representation of PMU measurements is essential for reliable grid monitoring, particularly in densely connected regions. To ensure consistency across locations, a normalized location accuracy metric is defined using (6)

$$d_n = min\sum_{i=1}^{n} nz_i - nz_1, \quad (6)$$

where nz_i, nz_1 denotes the normalized measurement value at the i^{th} grid location and the reference normalized value.

This metric minimizes spatial deviations among densely deployed PMUs while maintaining secure data handling in sparsely connected regions. Normalization improves comparability across locations and reduces the risk of location-based data distortion or loss.

G. Objective Functions

The security-related connectivity factors discussed above are integrated into a single composite objective function using a weighted multi-criteria formulation. Each criterion represents a specific aspect of PMU-based smart grid security, and weighting coefficients are used to control their relative influence. The objective function is defined using (7) as follows

$$f_1(x) = \\ = min\sum_{i=1}^{n}\left(w_1\Delta T_i, w_2 f_d(i), w_3 RD_i, w_4 CA_i, w_5 V_i, w_6 d_n\right), \quad (7)$$

where $w_1, w_2, \ldots, w_6$ denotes non-negative weighting coefficients satisfying $\sum_{k=1}^{6} w_k = 1$.

The composite function indicated above is represented as a universal objective function with different parametric

scenarios, where optimization is performed for all units of the smart grid using an artificial intelligence system

$$obj_t = f_1(x). \tag{8}$$

III. ARTIFICIAL INTELLIGENCE ALGORITHM

To obtain precise data on ageing and other relevant elements, such as grid deployment and connectivity issues, the suggested system integrates a PMU artificial intelligence algorithm. The proposed framework follows a layered architecture designed to address cyber-physical threats in PMU enabled smart grids. The first layer performs data acquisition by collecting synchronized voltage, current, frequency, and time stamp measurements from distributed PMUs. The second layer handles data preprocessing, where missing samples are removed, time alignment is ensured, and normalization is applied to improve robustness against measurement noise and communication delays. In the third layer, discriminative features such as transit time deviation, false data impact, residual deviation, and component attack indicators are extracted to represent the cyber-physical state of the grid. The fourth layer performs optimization and classification using the proposed objective function and the k-nearest neighbors (KNN) algorithm to identify abnormal patterns. Finally, the decision layer flags cyber-attack events and supports mitigation-oriented monitoring by distinguishing between normal and compromised grid states. The effectiveness of the proposed framework depends on the availability of representative training data that capture both normal grid operation and cyber-attack scenarios. The training dataset consists of labeled PMU measurements generated under various load conditions and simulated attack intensities to ensure sufficient coverage of operating states. Data quality is ensured through preprocessing and feature normalization, while robustness against data imbalance and noise is achieved by using distance-based classification rather than model-dependent learning. As the framework does not rely on strict statistical assumptions, it remains adaptable to evolving attack patterns with incremental updates to the training dataset.

A. Supervised Learning

In the proposed framework, supervised learning is adopted as the overall learning paradigm to distinguish between normal and compromised smart grid states using labeled PMU data. Within this supervised learning framework, KNN is used as a classification technique due to its simplicity, robustness, and suitability for real-time PMU-based applications. The supervised learning stage focuses on preparing labeled training data and extracting discriminative features from PMU measurements, while the KNN performs distance-based classification using these labeled features to identify abnormal or false data patterns. The identification of errors in smart grid units is conducted using historical state information, which allows for the identification of complex circumstances that cannot be prevented in the future due to unequal load conditions. Therefore, it is possible to identify all potential close error values during this phase, as illustrated in (9)

$$error_i = \sum_{i=1}^{n} \xi_i (GD_i), \tag{9}$$

where ξ_i denotes labeled set and GD_i represents grid data.

According to (9), the measurement of total error is performed using appropriate labels in previous measurements. Consequently, in subsequent states, the grid data will be modified, and only normalized data will be selected to minimize error.

In the context of smart grid units, it is imperative to identify loss functions to mitigate overall power loss. This involves determining the weightage functions associated with each grid connectivity. The regression approach can be applied to this sort of representations, allowing the identification of neighborhood grids by incorporating descriptive variables, as specified in (10)

$$NG_i = \sum_{i=1}^{n} \Upsilon_i \times wt_i, \tag{10}$$

where Υ_i denotes the number of the descriptive features and wt_i indicates the weight of the grid connectivity.

The relationship between the descriptive features and the total number of weights is described by (10), which requires the use of linear progression units with current-state signals. Additionally, it is possible to make multivariable judgments by using diverse descriptive qualities while ensuring that the weight of current-state transmissions is not maximized.

To mitigate the occurrence of superfluous grid connectivity across diverse regions, it is imperative to minimize the risk associated with distinct interconnection units. Therefore, the establishment of risk reduction is achieved by using labeled identifications, which incorporate a penalty element as denoted in (11)

$$GR_i = \sum_{i=1}^{n} \mathfrak{O}_i RS_i \tag{11}$$

where $\mathfrak{O}_i$ indicates the number of penalties and RS_i represents the risks minimized.

According to (11), the severity of fines is directly proportional to the total number of risk factors, therefore, requiring the establishment of effective grid communication. The supervised classification framework employs the KNN algorithm with normalized Euclidean distance as the similarity metric. The number of nearest neighbors k is empirically selected to balance robustness and sensitivity, and all features are normalized prior to classification to ensure fair distance computation. The complete learning workflow, including data preprocessing, feature extraction, optimization, and classification, is described using algorithmic steps and pseudocode as follows (Algorithm 1).

Algorithm 1. Supervised learning.

Input
$y_1, y_2, .., y_n$: Labeled operational states
$x_1, x_2, .., x_n$: PMU measurement data
Output
Trained model M
1.Compute baseline statistics of error values from normal operating data
2. Initialize error threshold
3. For each PMU measurement instance $i = 1$ *to* n do
4. Compute 〖error〗_i using historical unequal load conditions
5. Extract feature vector $NG_i = \{\Delta T_i, RD_i, CA_i, V_i\}$
6. End for
7. Minimize total risk by updating model parameters:
$M = arg\ min\ \sum error_i$
8. Return trained model M

B. Classification Using KNN

In the proposed smart grid security framework, KNN algorithm is implemented as a supervised classifier to identify false data measurements in PMU-enabled systems. The PMU measurement streams are first preprocessed and converted into feature vectors comprising transit time deviation, false data impact factor, residual data deviation, component attack index, and voltage variation. Historical PMU data with known operating conditions are used to form the labeled training dataset, where each feature vector is categorized as normal or false data. For each incoming PMU measurement, the Euclidean distance between its feature vector and all training samples is computed after feature normalization to prevent scale dominance. The k nearest samples with minimum distance values are selected and a weighted voting scheme is applied in which the closer neighbors have a greater influence on the final decision. If the majority of the weighted neighbors indicate abnormal behavior, the measurement is classified as false data; otherwise, it is treated as valid. The value of k is empirically chosen to ensure robustness against noise while maintaining real-time computational efficiency, making the KNN implementation suitable for practical smart grid security monitoring. The Euclidian distance is described using (12)

$$d\left(F_i, F_j\right) = \sqrt{\sum_{l=1}^{6}\left(F_{i,l} - F_{j,l}\right)}, \tag{12}$$

where F_i denotes the feature vector of PMU node i and l represents the feature index.

Equation (12) demonstrates the feasibility of managing power distribution fluctuations throughout a whole grid by taking into account two distinct grids. Nevertheless, the disparity between the two units can enhance processing at different stages, thus preventing total data disruption. Feature vectors were constructed by aggregating synchronized PMU measurements and derived security indicators over fixed observation windows. For each PMU node, raw voltage magnitude, voltage phase angle, current magnitude, and system frequency samples were first extracted from the time-aligned data streams. From these signals, higher-level features were computed, including transit time deviation, false data magnitude, residual grid deviation, component variation index, inspection weight, and normalized location deviation. Each feature vector therefore represents the cyber-physical state of a PMU at a given time window and is where all components are normalized to ensure comparable scaling. These feature vectors serve as structured input to the KNN classifier to distinguish between normal and attack conditions.

The optimization process within the proposed framework operates directly on feature variables extracted from synchronized PMU measurements. Specifically, the variables optimized during classification are the feature component data transit-time deviation, false data impact, residual grid deviation, component attack indicator, security violation weight, and normalized location deviation. These variables jointly form the feature vector, which represents the cyber-physical state of each PMU node. The KNN classifier does not perform parameter learning, but instead optimizes classification decisions by minimizing the distance between feature vectors in the multidimensional feature space, thereby identifying abnormal operating states based on similarity to labeled training samples. Figure 2 depicts the proposed AI-driven security framework.

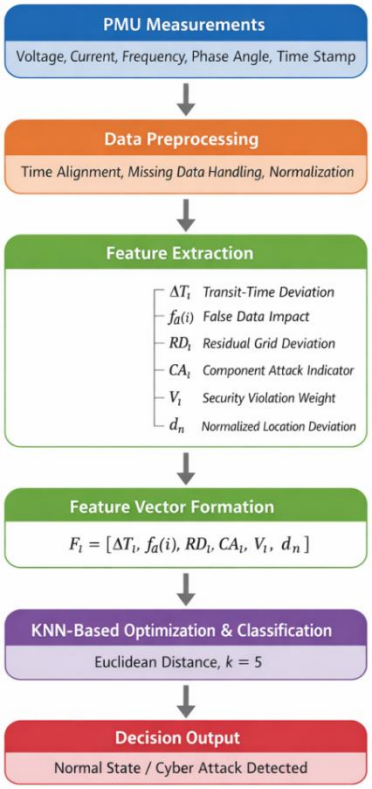


Fig. 2. Proposed AI-driven PMU security framework.

Data correctness can be implemented in KNN by adjusting the grid connectivity to immediate connections with interconnected line representations, hence altering the overall observability. Therefore, it is necessary to ensure the accuracy of the data by incorporating homomorphism with the data content, as specified in (13)

$$\pi_i = \sum_{i=1}^{n} ey_i\left(CC_d(i)\right), \tag{13}$$

where ey_i denotes the encrypted data and $CC_d(i)$ indicates the data correctness.

Equation (13) demonstrates the need to encrypt data prior to its transmission to the nearest neighbors to rectify specific data. If the nearest neighbors are not mapped with accurate encryption, it will be necessary to update the control units in the future, which should be avoided.

To mitigate the potential repercussions of connectivity failure in subsequent instances, it is imperative to ascertain the specific weights assigned to grid connections in situations where a shared way of establishment is required. Equation (14) can be utilized to describe the analytical representation of the weighted neighbors in the following manner

$$MP_i = \sum_{i=1}^{n} \varpi_i \times fail_i, \tag{14}$$

where ϖ_i denotes the weighted units and $fail_i$ indicates the total number of grid failures.

In the failure node scenario, (14) is used to account for the inclusion of supplementary weight factors for the

respective grids. The KNN algorithm is selected due to its non-parametric nature, minimal training overhead, and suitability for small-to-moderate PMU datasets where labeled cyber-attack samples are limited [17]–[21]. KNN directly exploits distance-based similarity in feature space, which aligns well with the physical interpretation of PMU measurements such as time deviation, residual variation, and component state changes. Although advanced classifiers such as support vector machines, random forests, and graph neural networks can achieve high detection accuracy, they require extensive hyperparameter tuning, larger labeled datasets, and increased computational complexity. The proposed framework prioritizes real-time applicability and interpretability for smart grid environments, where rapid detection and deployment feasibility are critical. Unlike existing PMU safety approaches that apply KNN solely as a generic classifier, the proposed method integrates KNN within a cyber–physical optimization framework that jointly models time-synchronization deviation, false data impact, residual grid data, component-level disturbances, and security violations. The framework introduces a unified objective function that fuses these heterogeneous indicators into a single decision process, enabling early detection of coordinated cyber-physical attacks. In contrast to conventional KNN-based methods that rely only on statistical similarity, the proposed approach embeds power system operational constraints and PMU observability characteristics, improving interpretability and practical relevance for smart grid security monitoring. The algorithmic flow of the k-nearest neighbors (KNN) method for smart grids is given in Algorithm 2 and the procedural flow of false data detection is illustrated in Procedure 1.

Procedure 1. AI-Based False Data Detection Using PMU Measurements.

Begin PROCEDURE
- Step 1: Acquire synchronized PMU data (V, I, time stamps, location).
- Step 2: Preprocess data and compute feature vectors using (1)–(6).
- Step 3: Construct labeled datasets from historical normal and attack states.
- Step 4: Train supervised learning model using labeled grid states.
- Step 5: Apply KNN classification to identify nearest operational neighbors.
- Step 6: Compute residual deviation RD_i and KNN distance $d(F_i, F_j)$.
- Step 7: Initialize adaptive thresholds.
- Step 8: Detect false data events based on residual and distance thresholds.
- Step 9: Validate results under four security scenarios.

end PROCEDURE

Algorithm 2. K-Nearest Neighbors-based False Data Detection.

Input
- $z_1, z_2, .., z_i$: Test PMU data
- Training dataset GD
- Number of neighbors k
- Output
- Classification decision for false data detection

1. For each test instance z_i do
2. Compute distance $dist(z_i, x_n)$ to all training samples x_n using normalized Euclidean distance
3. Select k nearest neighbors based on minimum distance
4. Apply weighted voting to determine class label
5. If classified as abnormal, then
6. Flag z_i as false data
7. Else
8. Accept z_i as valid PMU measurement
9. End if
10. End for

IV. RESULTS

The experimental evaluation presented in this section is directly derived from the theoretical parameters and formulations introduced earlier in the manuscript. Specifically, transit time deviation, false data impact, residual data deviation, component attack indicators, and voltage variation metrics are computed from PMU measurements and used as feature inputs to the proposed AI-driven framework. These parameters, defined analytically in the theoretical section, form the basis for the optimization objective and the k-nearest neighbors (KNN) classification process. Consequently, the results reported in this section reflect the practical effectiveness of the theoretical formulation under different operating and attack scenarios, ensuring consistency between the analytical model and experimental validation. The experimental evaluation of the proposed method was carried out using PMU measurement data generated from a standard test power system modeled in MATLAB/Simulink. The power network, including buses, transmission lines, and loads, was simulated using conventional power system blocks, and synchronized phasor measurement units were placed in selected buses to collect time-synchronized voltage, current, and frequency measurements under both normal operating conditions and simulated false data injection scenarios. The PMU data were exported from the Simulink environment and imported into MATLAB using built-in data handling functions, where they were organized into structured matrices corresponding to individual PMU nodes and time instances. Prior to analysis, the data were preprocessed to remove missing samples and normalized to ensure uniform scaling across features. The feature vectors were then constructed by extracting transit time deviation, false data impact, residual data deviation, component attack indicators, and voltage variation parameters from the raw PMU measurements. The proposed optimization framework and KNN classifier were implemented in MATLAB, where labeled historical data were used for training and unseen PMU measurements were used for testing. Multiple simulation scenarios were executed by varying load conditions, communication delays, and attack intensities, and performance metrics such as detection accuracy, false alarm rate, and response time were computed from the classification outcomes to obtain the results presented in this section. Table II presents the significance of the different scenarios examined for particular test systems to analyse the impact of security with PMUs in smart grids.

The performance evaluation presented in this section is based on the theoretical metrics introduced earlier, including transit time deviation, false data impact, and residual data deviation. These metrics are directly computed from PMU measurements and used as input features for the proposed classification framework. Therefore, the results reflect the practical effectiveness of the theoretical formulation in different operating and attack scenarios.

TABLE II. IMPORTANCE OF SCENARIOS.

Scenarios	Significance
Synchronization of time-periodic measurements	To identify variations in time-periodic measurements, false data measurements are controlled
Total number of component attacks	To identify complete risk factors in PMU associated components

Scenarios	Significance
Control of security violations	To inspect individual grid point data with security standards to avoid violation risks
Grid point accuracy	To normalize grid data points, security of associated units are assured

Discussions. The proposed AI-driven cyber-attack analysis framework was implemented using MATLAB. The PMU measurement data were generated using standard benchmark systems modeled in Simulink. PMUs were placed on generator buses and critical load buses to ensure full system observability. Each PMU recorded voltage magnitude, phase angle, frequency, and time stamp measurements at a reporting rate of 30 samples per second. Cyber-attack scenarios were emulated by injecting false data, time-delay disturbances, and component parameter variations into the PMU measurement streams. The dataset consisted of approximately 12,000 labeled samples, with 70 % used for training and 30 % for testing. Data preprocessing included time alignment using a common GPS clock reference, normalization to the unit scale, and removal of missing samples.

Feature vectors were constructed using transit-time deviation, false data magnitude, residual grid deviation, component variation index, inspection weight, and normalized location parameters. These features formed the input to the KNN classifier. The KNN model was configured with $k = 5$, Euclidean distance metric, and uniform weighting.

The input to the artificial intelligence core consists of time-synchronized measurement data obtained from distributed phasor measurement units deployed across the smart grid. Primary data sources include voltage magnitude, current magnitude, system frequency, phase angle, and time stamp information collected under both normal operating conditions and simulated cyber-attack scenarios using a standard test system. These raw PMU measurements are imported into the analysis environment and transformed into discriminative feature vectors that serve as input to the supervised classification process. The extracted features include transit time deviation, false data impact factor, residual data deviation, component attack indicators, and voltage variation indices, which collectively capture temporal inconsistencies, electrical anomalies, and data integrity violations caused by cyber-physical attacks. To ensure high feature quality, preprocessing steps such as time alignment, noise filtering, and normalization are applied, reducing redundancy and improving class separability. Since the performance of the KNN classifier directly depends on the quality and discriminative power of the input features, careful feature construction and preprocessing play a critical role in achieving robust and accurate attack detection. Table III presents comprehensive information on the simulation environment that is taken into account for the suggested strategy.

Before applying the proposed analysis framework, the PMU measurement data underwent a structured preprocessing stage to ensure data consistency and uniform feature scaling. First, missing samples caused by communication delays or packet loss were identified using time stamp continuity checks; isolated missing values were removed, while short gaps were handled by linear interpolation to preserve temporal coherence. Next, all PMU data streams were time-aligned using GPS-synchronized time stamps to ensure sample-level synchronization across measurement units. To allow a uniform contribution of voltage, current, frequency, and security indicators derived during classification, normalization was performed using min-max scaling, mapping each feature to the range [0, 1]. This preprocessing step prevents bias toward parameters with larger numerical ranges and improves the robustness of the subsequent KNN-based classification.

TABLE III. SIMULATION PARAMETERS.

Bounds	Requirement
Operating systems	Windows 8 and above
Platform	MATLAB and PMU security tool
Version (MATLAB)	2015 and above
Version (PMU security tool)	3.2 and above
Applications	Smart grid applications with PMU device installation
Implemented data sets	Number of line connections, observable state indications and nearest neighbors

The proposed framework is evaluated based on its ability to distinguish between normal and compromised grid states using PMU-derived features under varying load and communication conditions. The evaluation focuses on detection accuracy, robustness to data variations, and consistency of classification outcomes across multiple simulation scenarios. By applying the same theoretical metrics across all experiments, the performance of the framework is assessed in a unified and systematic manner, demonstrating its suitability for the detection of the cyber-physical attacks in smart grid environments. The proposed framework relies on representative labeled PMU data to model normal and attack scenarios; therefore, detection performance may degrade when previously unseen or adaptive attack patterns occur. The requirement for labeled data introduces additional labeling costs during deployment. Furthermore, although the framework is validated using standard test systems, simulated environments may not fully capture real-world grid complexities. Adversarial robustness against coordinated multi-point attacks and scalability to very large PMU deployments remain important directions for future investigation.

The comprehensive depiction of all enumerated instances and their juxtaposition with established methodologies are as follows.

Scenario 1: Synchronization of time-periodic measurements

In this situation, measurements are performed at regular intervals of time, and it is necessary to synchronize the whole data with different power units. Given that each grid unit has independent clock sections and the state of observable units undergoes changes, it becomes imperative to achieve synchronization between the transmitter and receiving units. Additional data flow is necessary to account for individual state changes, which requires a transit time period. In the event of a breakdown during the transmission phase, complete repair is required. In the event of corrections, the data measurement undergoes modifications, resulting in the regulation of incremental power flows.

Consequently, an individual branch configuration is implemented in this scenario. The inclusion of second-degree freedom in measurements enhances the chance of accurate measurements, hence minimizing the occurrence of erroneous measurements in all relevant scenarios. On the other hand, by using labeled information, it is feasible to minimize the presence of incorrect information that may occur at earlier stages, hence preventing branch failures.

Figure 3 depicts the coordination of intermittent measurements and inaccurate data measurements for the suggested and current methods. Figure 3 clearly demonstrates that the suggested approach effectively manages incremental power flows, which are indicative of inaccurate data observations, for each particular clock segment. The occurrence of inaccurate data reductions can be attributed to the existence of a central clock controller, which ensures synchronization among all PMU data units. The outcome of this scenario is verified by considering the number of state transmissions as 4, 12, 27, 30, and 64. The proportion of incremental flows observed is 18 %, 33 %, 54 %, 59 %, and 61 %. Therefore, the percentage of erroneous data associated with the indicated incremental flows in the existing technique is 26, 24, 21, 17, and 13. In contrast, the projected model shows a reduction in false data to 15 %, 12 %, 9 %, 5 %, and 3% due to the proper synchronization of time measurements in various states.

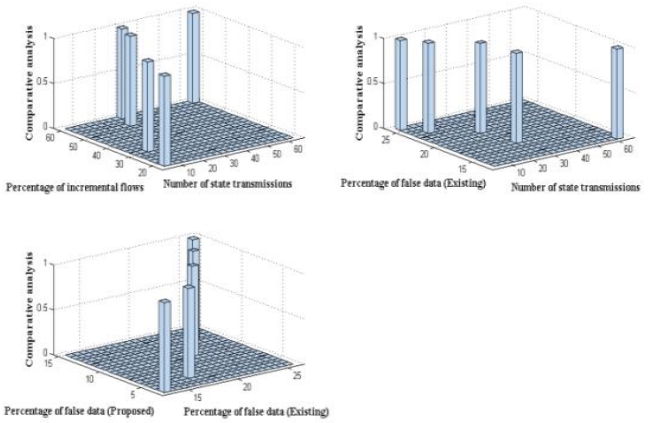


Fig. 3. Comparative analysis of the impact of false data under false data injection intensity of 5 % to 20 %, PMU reporting rate of 30 samples/s, and branch loading levels of 0.6 p.u.–1.0 p.u.

Scenario 2: Total number of component attacks

Given the presence of PMUs in the overall grid connection, it becomes imperative to assess the cumulative count of component attacks across different time intervals. Therefore, in this particular circumstance, a decrease in the occurrence of component attacks upon synchronization is observed, resulting in a reduction of entire erroneous data measurements caused by errors in dormant devices. In this situation, additional state functions are found for each connected component, resulting in the observation of injected bad data in grids and the subsequent processing of methods to remove such data. Furthermore, to enhance the precision of inaccurate data in interconnected PMUs, a comparison is conducted between the present and prior states. This ensures that the entire system remains immune to various types of attacks. Consequently, the current measurement conditions can also experience sudden changes. If this is not detected early on, there will be a greater amount of inaccurate data, necessitating further improvements in line connectivity. Therefore, the suggested method uses supervised learning and KNN to identify a comprehensive solution for these alterations.

The comparison of component assaults between the proposed and existing approaches is depicted in Fig. 4.

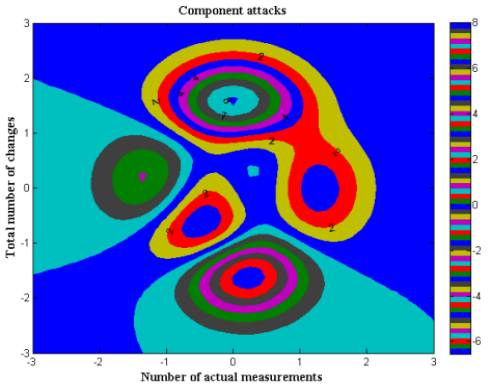


Fig. 4. Component state variations with reactance perturbations of ±10 %, synchronized GPS time stamping, and nominal system frequency of 50 Hz.

Figure 4 clearly demonstrates that the suggested strategy reduces the amount of component assaults and residual grid data compared to the previous methodology [7]. One of the main factors contributing to the decrease in attacks is the consistent presence of reactive components in grids, which prevents sudden changes from occurring in the early stages. To assess the results of residual grid and component attacks, a total of 41, 56, 68, 81, and 94 actual measurements were recorded, with corresponding variations of 8, 11, 16, 23, and 29. The aforementioned measurements and alterations indicate that the percentage of component attacks observed in the existing approach is 23 %, 20 %, 18 %, 14 %, and 11 %. Nevertheless, by implementing the same number of modifications, the suggested approach successfully reduced the overall occurrence of component assaults to 12.8 %, 7.7 %, 4 %, and 2 % accordingly. The reduction of linked residual data with poor data is observed in the grid, whereas the current-state representations of smart grid systems maintain threshold limits. The proposed framework considers a cyber-physical threat model in which an attacker has limited but targeted access to PMU measurement streams and associated communication links. The attacker is assumed to be capable of injecting false data, introducing time-synchronization delays, and manipulating component-level measurements without having direct control over the physical power generation units.

The attack scenarios addressed include false data injection attacks on voltage and current measurements, time stamp manipulation attacks that affect PMU synchronization, residual data corruption during transmission, and component-level attacks that cause abrupt changes in the system reactance. The attacker does not possess global system knowledge and cannot simultaneously compromise all PMU nodes, reflecting realistic constraints in operational smart grids.

Scenario 3: Control of security violations

Most of smart grid operations involve the use of data transmission capabilities, in which information is obtained from GPS systems. It is imperative to adhere to security requirements to minimise the occurrence of violations in

each connectivity unit with PMU. Therefore, in this situation, the potential for security breaches is evident through ongoing inspections carried out on the line connecting the places where PMUs are linked. If any of the security measures implemented in the observability connecting lines are altered, the entire smart grid will experience a decrease in security. This will lead to data loss in the subsequent steps, resulting in uneven load distributions. By retaining a minimal amount of weights, it is feasible to regulate the entire smart grid in real time without violating security regulations, thus achieving electricity in the required units. However, the weights of these types are contingent upon the specific location of the PMU. Consequently, a labelled connection is established to ascertain a set of rule factors that align with the security restriction.

The comparison of control for security violations in the proposed and existing approach is depicted in Fig. 5 [7].

Figure 5 demonstrates that the suggested approach effectively manages security violations compared to the previous paradigm by conducting continuous inspections at the locations of the PMU installation. One of the primary factors contributing to the decrease in security breaches is the provision of minimal weights for each line connectivity in observable states, which therefore leads to the implementation of secure monitoring systems. Verification of the outcome of the control process involves considering a total of 28, 39, 44, 47, and 51 unique weights. The inspection rates for these weights fall within specific ranges of 129, 157, 188, 209, and 243, respectively. Therefore, the existing approach reduces the proportion of violations to 32 %, 29 %, 26 %, 23 %, and 20 % for the mentioned weights and inspections. Similarly, with the same number of constraints, the percentage of violations is reduced to 9 %, 6 %, 5 %, 4 %, and 2 %.

Scenario 4: Grid point accuracy

Once the synchronization and identification of component attacks and security violations have been completed, it becomes imperative to analyze the accuracy % at interconnected grid points. Thus, in this situation, the accuracy of the grid points is assessed using normalized data measurements, resulting in a total reduction in data losses related to PMU. To assess the precision of grid points, a comparative analysis is performed using a smart grid system that has observable line connections. This analysis involves examining both the prior and current states of the grid. Moreover, the accuracy in this particular scenario is not solely linked to data, but also to device measurements, thus mitigating the overall risks connected with grids. The enhancement of smart grid connectivity accuracy can lead to the establishment of a trade-off, wherein the correctness of grid point data can be influenced by the incorporation of KNN. Figure 6 presents an analysis of the comparative results pertaining to the accuracy of the grid points for both the proposed and existing methodologies.

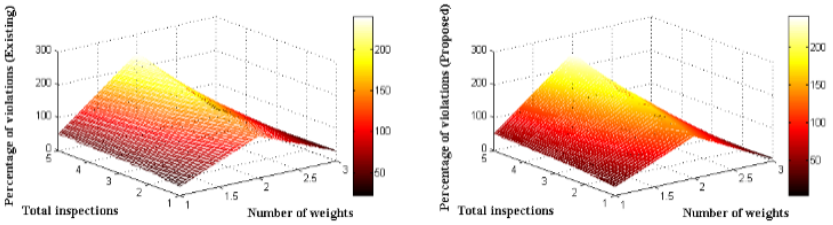


Fig. 5. Security violation assessment based on varying PMU data weights (0.2–0.8) and successive inspection cycles (ℵ = 1–10) in simulated node compromise scenarios.

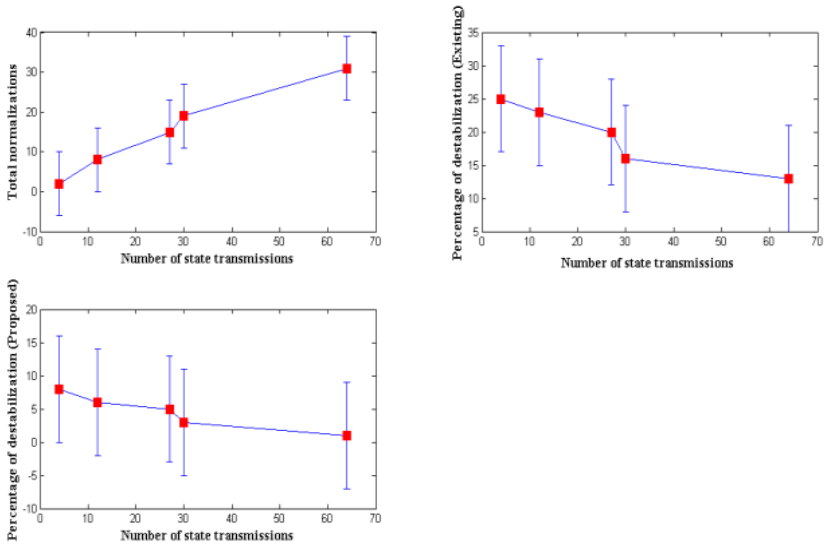


Fig. 6. Normalized PMU data representation using min-max normalization, six-dimensional feature vectors, and mixed normal and attack operating conditions.

The analysis of Fig. 6 reveals that the projected model exhibits a higher level of grid point accuracy compared to the existing approach [7]. The reduction in data normalization, when compared to earlier state measurements, leads to an increase in grid point precision. Consequently, a minimal level of data correctness is

required. The enhanced precision leads to a decrease in the number of PMU penalties, resulting in cost savings for each line connectivity while keeping the number of observable states constant. To assess the correctness of grid points, we consider a total of 4, 12, 27, 30, and 64 state transmissions. Additionally, we apply normalizations of 2, 8, 15, 19, and 31 to each transmission unit. Thus, the existing technique restricts the proportion of destabilizations to 25 %, 23 %, 20 %, 16 %, and 13 % for the aforementioned normalizations. In contrast, the proposed model reduces the destabilizations to 8 %, 6 %, 5 %, 3 %, and 1 % for the same normalization factor.

V. CONCLUSIONS

The implementation of security measures in smart grids is imperative due to the significant reliance on data communication for load distribution in accordance with generation requirements. Therefore, the PMU devices that have been implemented are examined once they have achieved full observability within the same line connectivity units. Transit time intervals for synchronization are commonly observed during this operation to accurately adjust the overall time span between the transmitting and receiving units. In the context of smart grid connectivity, it is imperative to not only provide observability, but also implement ongoing maintenance to avoid unauthorized entry of false data into the system. Given that comprehensive data are collected using GPS units, it is imperative that data transmission is accompanied by secure units. In the proposed framework, GPS is used to provide accurate time synchronization for PMU measurements, ensuring consistent time stamping of voltage, current, and frequency data across distributed grid nodes. This synchronization enables the detection of time-based anomalies such as delays and time stamp manipulation attacks through transit-time deviation analysis. Encryption is assumed at the communication layer to protect PMU data confidentiality during transmission; however, cryptographic mechanisms are not explicitly modeled in the optimization process. Instead, the framework focuses on detecting cyber-physical inconsistencies that may arise even in encrypted channels, such as false data injection, residual deviation, and component-level attacks.

Consequently, the load connection is limited to the central units. The proposed method incorporates artificial intelligence optimization to prevent incremental flows by watching specific limiting parameters, in addition to ensuring the security of information. To ensure effective control for PMUs in smart grid connectivity, it is necessary to have labeled information that accurately identifies false data. This labeled information helps prevent residual data from entering individual line connections. To mitigate the risk of erroneous component installation in the smart grid, it is important to conduct a thorough examination of any modifications by comparing them with the current- and prior-state representations. This process is typically carried out using a planned approach.

The suggested system model with artificial intelligence optimization is analyzed in real time using four scenarios and two case studies. In these situations, the proportion of erroneous data is reduced to 3 % when the state transmissions change, compared to the previous technique, which has a 13 % increase in false data. As a result, the simulation results indicate a reduction in component attacks and violations to 2 %, leading to a decrease in destabilization to 1 %. The proposed framework relies on representative labeled PMU data to model normal and attack scenarios; therefore, detection performance may degrade when previously unseen or adaptive attack patterns occur. The requirement for labeled data introduces additional labeling costs during deployment. Furthermore, although the framework is validated using standard test systems, simulated environments may not fully capture real-world grid complexities. Adversarial robustness against coordinated multi-point attacks and scalability to very large PMU deployments remain important directions for future investigation.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interests.

REFERENCES

[1] P. Qiu, Q. Gao, C. Liu, D. Wang, Y. Lyu, X. Li, C. Wang, and G. Qu, "PMU-spill: A new side channel for transient execution attacks", *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 70, no. 12, pp. 5048–5059, 2023. DOI: 10.1109/TCSI.2023.3298913.

[2] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach", *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, 2017. DOI: 10.1109/COMST.2016.2616442.

[3] Z. Ni and S. Paul, "A multistage game in smart grid security: A reinforcement learning solution", *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 9, pp. 2684–2695, 2019. DOI: 10.1109/TNNLS.2018.2885530.

[4] A. Giani, R. Bent, M. Hinrichs, M. McQueen, and K. Poolla, "Metrics for assessment of smart grid data integrity attacks", in *Proc. of IEEE Power and Energy Society General Meeting*, 2012, pp. 1–8. DOI: 10.1109/PESGM.2012.6345468.

[5] H. Keshavarz Ziarani, S. H. Hosseinian, and A. Fakharian, "Providing a new multiobjective two-layer approach for developing service restoration of a smart distribution system by islanding of faulty area", *International Transactions on Electrical Energy Systems*, 2024. DOI: 10.1155/2024/9687002.

[6] Y. Xu, "A review of cyber security risks of power systems: From static to dynamic false data attacks", *Protection and Control of Modern Power Systems*, vol. 5, no. 3, pp. 1–12, 2020. DOI: 10.1186/s41601-020-00164-w.

[7] S. Dorji, A. A. Stonier, G. Peter, R. Kuppusamy, and Y. Teekaraman, "An extensive critique on smart grid technologies: Recent advancements, key challenges, and future directions", *Technologies*, vol. 11, no. 3, p. 81, 2023. DOI: 10.3390/technologies11030081.

[8] O. M. Butt, M. Zulqarnain, and T. M. Butt, "Recent advancement in smart grid technology: Future prospects in the electrical power network", *Ain Shams Engineering Journal*, vol. 12, no. 1, pp. 687–695, 2021. DOI: 10.1016/j.asej.2020.05.004.

[9] A. Ravi, M. Saranathan, P. H. K. Achuthan, M. C. Lavanya, and V. Rajini, "A comprehensive review on the current trends in micro-phasor measurement units", *IOP Conference Series: Materials Science and Engineering*, vol. 1258, art. 012045, 2022. DOI: 10.1088/1757-899X/1258/1/012045.

[10] Y. Kim, S. Hakak, and A. Ghorbani, "Smart grid security: Attacks and defence techniques", *IET Smart Grid*, vol. 6, no. 2, pp. 103–123, 2023. DOI: 10.1049/stg2.12090.

[11] S. M. Armaghan, F. Asgharzadeh, B. Yousefi-Khanghah, and H. R. Ashrafi, "Resilient operation of electric vehicles considering grid resiliency and uncertainties", *International Transactions on Electrical Energy Systems*, vol. 2023, art. 5320002, pp. 1–15, 2023. DOI: 10.1155/2023/5320002.

[12] T. D. Le *et al.*, "GridAttackAnalyzer: A cyber attack analysis framework for smart grids", *Sensors*, vol. 22, no. 13, p. 4795, 2022. DOI: 10.3390/s22134795.

[13] V. V. Tynchenko *et al.*, "Mathematical models for the design of

GRID systems to solve resource-intensive problems", *Mathematics*, vol. 12, no. 2, p. 276, 2024. DOI: 10.3390/math12020276.

[14] V. P. and N. Visali, "Evaluation and improvement of power system security with the application of machine learning", *El-Cezerî Journal of Science and Engineering (ECJSE)*, vol. 11, no. 1, pp. 48–57, 2024. DOI: 10.31202/ecjse.1316748.

[15] Z. Lu, L. He, D. Zhang, B. Zhao, J. Zhang, and H. Zhao, "A security level classification method for power systems under $N-1$ contingency", *Energies*, vol. 10, no. 12, p. 2055, 2017. DOI: 10.3390/en10122055.

[16] N. K. Singh and V. Mahajan, "Mathematical model of cyber intrusion in smart grid", in *Proc. of 2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia)*, 2019, pp. 965–969. DOI: 10.1109/GTDAsia.2019.8715946.

[17] M. K. Paramathma, D. Devaraj, and B. S. Reddy, "Artificial neural network based static security assessment module using PMU measurements for smart grid application", in *Proc. of 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, 2016, pp. 1–5. DOI: 10.1109/ICETETS.2016.7603086.

[18] S. D'Antonio, L. Coppolino, I. A. Elia, and V. Formicola, "Security issues of a phasor data concentrator for smart grid infrastructure", in *Proc. of the 13th European Workshop on Dependable Computing*, 2011, pp. 3–8. DOI: 10.1145/1978582.1978584.

[19] M. Varan, A. Akgul, F. Kurugollu, A. Sansli, and K. Smith, "A novel security methodology for smart grids: A case study of microcomputer-based encryption for PMU devices", *Complexity*, 2021. DOI: 10.1155/2021/2798534.

[20] D. Dzafic, I. Dzafic, and A. Akagic, "Anomaly detection in smart grid time-series data using Graph Deviation Networks", *Engineering Applications of Artificial Intelligence*, vol. 165, part B, art. 113512, 2026. DOI: 10.1016/j.engappai.2025.113512.

[21] N. Li, J. Zhang, D. M. Ma, and J. Ding, "Enhancing detection of false data injection attacks in smart grid using spectral graph neural network", *IEEE Transactions on Industrial Informatics*, vol. 21, no. 6, pp. 4543–4553, 2025. DOI: 10.1109/TII.2025.3545044.



This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 (CC BY 4.0) license (http://creativecommons.org/licenses/by/4.0/).