A Unified Co-Design Framework Integrating Predictive AI Control and Cyber-Resilience for Autonomous Microgrid Operation

Abosalah Solaman Ali Khezoo [1,*], Abdusalam Moustafa Haiyed Kanu[2], Zayd Abdulsalam Zaed Zaed[3], Mohamed Abusalah Mohamed Alssalim[4], Massoud Mohammed Abdussalam Alamien[5]

[1]Higher Institute of Sciences and Technology Wadi Etba, Libya.
[2] Collage of engineering Technology/ algrifa, Libya.
[3] SEBHA University, Libya.
[4,5] Higher Institute of Science and Technology, Wadi Al-Ajal, Libya.

abosalahgzoo@gmail.com, abdhayd2013@gmail.com, zae.zaed@sebhau.edu.ly, mohamed6855740@gmai.com, 1983ASD1982@GMAIL.COM

Correspondence *: Abosalah Solaman Ali Khezoo [1,*], abosalahgzoo@gmail.com

Abstract

The increasing integration of renewable energy and distributed resources makes accurate forecasting essential for reliable and efficient microgrid energy management; however, existing TFT-based forecasting studies primarily focus on prediction and lack direct integration with predictive control and cyber-resilient operation. Therefore, this study proposes a TFT-MPC-CR framework that combines Temporal Fusion Transformer (TFT) forecasting, Model Predictive Control (MPC), AI-based False Data Injection (FDI) detection, and adaptive resilient control. The framework is implemented in Python using PyTorch, with the Microgrid PV-EV Charging Dataset obtained from Kaggle, where PV generation, load demand, battery SOC, EV charging, and grid variables are used for learning. TFT predicts future PV generation and energy demand, and MPC optimizes battery, EV, and grid power allocation, while the cybersecurity layer detects manipulated measurements and activates resilient MPC. As a target experimental outcome, the proposed framework is designed to achieve at least 5–10% lower forecasting error than conventional TFT and improve operational resilience under FDI attacks. The framework is expected to provide accurate prediction, efficient energy management, rapid attack response, and secure autonomous microgrid operation.

Keywords: Temporal Fusion Transformer; Model Predictive Control; Cyber-Resilient Microgrid; False Data Injection Attack; PV-EV Energy Management

1. Introduction

The growing utilization of renewable energy resources, energy storage, EVs, and distributed energy resources makes modern autonomous microgrids more versatile and energy-efficient; however, renewable energy intermittency, varying loads, and dependence on communication networks make microgrids prone to various vulnerabilities [1]. The current state-of-the-art research has already proved the applicability of AI-based predictive control techniques to improve the microgrid regulation and energy management [2], [3]; resilient MPC has been suggested for detecting and mitigating stealthy and false-data-injection (FDI) attacks [4]. Additionally, recently the use of data-driven nonlinear MPC with Bayesian Neural Networks was proposed for uncertainty-aware attack detection and adaptive control [5]. Moreover, the deep-learning-based methods, such as CNN-LSTM-Attention and A-BiTG were designed for capturing temporal and discriminative features of FDI attacks [6], [7]. Nevertheless, existing methodologies mainly focus either on predictive control, attack detection or resilient control separately, or by means of partial integration. Thus, this study aims at developing the TFT-MPC-CR framework which would combine Temporal Fusion Transformer-based forecasting, Model Predictive Control, AI-based cyberattack detection and resilient control techniques.

The proposed TFT-MPC-CR framework overcomes these deficiencies by incorporating a framework that combines the TFT-based energy forecasting technique, MPC, AI-based cyberattack detection, and adaptive cyber-resilient control. The TFT is used to forecast future PV energy production and demand, whereas MPC relies on the forecasted values to optimize the operations of battery systems, EV charging, PV energy production, and power transactions with the grid. Different from the cyberattack detection strategies which just detect FDI attacks [8] or design observer-based resilient consensus control [9], the proposed framework combines the cyberattack detection with adaptive predictive control. In addition, the proposed framework is different from the AI-enabled energy management system framework [10] by incorporating FDI attack scenarios and resilient control techniques.

AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.3 (2026)
www.ajmimc.com

Problem Statement

Effective forecasting of solar irradiance and electricity loads is vital for optimal microgrid energy management. But solar irradiance is very irregular, whereas electricity loads have a complex dynamic behavior pattern. It has been shown that a forecasting model based on TFT framework can be effective in capturing long-term dependencies in solar irradiance forecasting [11] and predicting electricity loads at different horizons in industries [12]. But these forecastings methods are more oriented toward accuracy rather than incorporating them with predictive control and cyber-resilience of the microgrid operation. Hence, there is a need for a unified strategy that leverages TFT-based forecasting for proactive energy management while ensuring security and resilience.

2. Related Works

Badhe et al. [13] have suggested an optimized framework for smart grid energy usage prediction that combines the TFT and AO. The application of TFT was aimed at recognizing complicated temporal relationships and predicting energy consumption in various time intervals, while optimization of key TFT parameters was carried out by AO for better convergence and prediction results. An AO-TFT model has been compared to LSTM and CNN-BiLSTM models with RMSE equal to 0.48 and MAE equal to 0.31. Nevertheless, the work is focused mainly on energy-usage prediction and lacks any forecasting integration into microgrid control and operation.

Pütz et al. [14] explored the possibility of employing TFTs in highly resolved power-grid frequency forecasting tasks. It was shown that TFT may be superior to conventional forecasting methods when applied to noisy and highly volatile time series of frequency. In addition, Pütz et al. [2] have studied the trade-off between forecasting accuracy and energy consumption related to computations at various temporal resolutions. Exogenous variables such as load and generation increased forecasting accuracy, and interpretability of TFT revealed the importance of features such as load ramp, hour, and month. However, the research is limited to the task of power-grid frequency forecasting and does not include its integration with MPC-based energy management.

3. Proposed Methodology of Unified TFT-Based Predictive Control and Cyber-Resilient Co-Design Framework for Autonomous PV-EV Microgrid Operation

The methodology proposes a co-design paradigm which considers both energy management and cyber-resilient autonomous operation in the PV-EV microgrid. In contrast to the current methodologies where energy prediction, energy control optimization, and cyberattack detection are performed separately, the suggested paradigm provides for feedback between these operations. For predicting the future PV generation and energy consumption, the TFT is used; energy management is performed through MPC which takes into account battery, EV, and grid power management. Cybersecurity of the system is considered through controlled false data injection attacks which are detected with the use of AI-driven anomaly detection and result in the operation of adaptive MPC. Figure 1. Shows the Proposed TFT-MPC-CR Methodology Framework for Secure Autonomous PV-EV Microgrid Operation

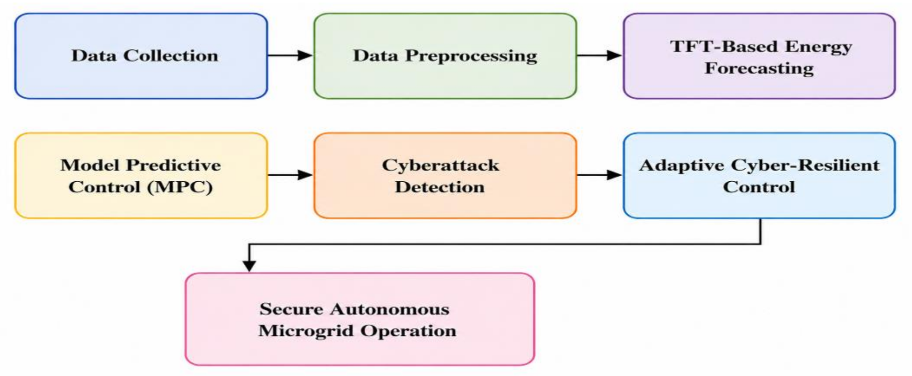

Figure 1. Proposed TFT-MPC-CR Methodology Framework for Secure Autonomous PV-EV Microgrid Operation

3.1 Dataset Collection and Preprocessing

Microgrid PV-EV Charging Dataset comes from Kaggle [15]. It is a microgrid-connected PV-EV charging system and includes 20 features related to solar generation, solar irradiance, battery SOC, EV charging attributes, energy generation on the grid side, demand side load, energy price, demand response, and load balancing activities. The gathered data are preprocessed by eliminating any inconsistent data points and then normalized to generate suitable time series inputs for our proposed predictive control approach.

3.2 Temporal Fusion Transformer-Based Energy Forecasting

The historical data after preprocessing is fed into TFT for identifying the dependency on PV generation, solar radiation, battery SOC, EV charging demand, and load of microgrid. The attention-based temporal features learning technique is employed by Temporal Fusion Transformer for prediction of future energy demands and renewable generation as (1).

$$x_t^{\text{norm}} = \frac{x_t - x_{\min}}{x_{\max} - x_{\min}} \tag{1}$$

Where x_t represents the feature value at time t, while $x_{\min}$ and $x_{\max}$ denote its minimum and maximum values. The normalization transforms heterogeneous microgrid variables into a common numerical range, improving the stability of TFT training and forecasting.

3.3 Model Predictive Control-Based Energy Optimization

The forecasts generated by TFT are supplied to the MPC module to determine optimal battery operation, EV charging, and grid power exchange. MPC evaluates future operating conditions over a finite prediction horizon while satisfying the operational constraints of the microgrid as (2).

$$J = \sum_{k=1}^{N_p} \left[w_1 \left(P_{\text{load},k} - P_{\text{sup},k} \right)^2 + w_2 (SOC_k - SOC_{\text{ref}})^2 + w_3 C_k \right] \tag{2}$$

Where N_p denotes the prediction horizon, $P_{\text{load},k}$ is the predicted load, $P_{\text{sup},k}$ is the supplied power, SOC_k is the battery state of charge, is the desired SOC, and C_k represents the energy cost. The weighting coefficients w_1, w_2, w_3 regulate the importance of power balancing, battery regulation, and operating cost.

3.4 Cyberattack Injection and AI-Based Detection

To assess cyber-resilience, controlled False Data Injection (FDI) attacks are introduced into selected microgrid measurements, including PV generation, load demand, battery SOC, and grid power. An AI-based anomaly detection mechanism identifies deviations between normal and manipulated measurements as (3).

$$x_t^{\text{attack}} = x_t + a_t \tag{3}$$

Where x_t represents the original measurement and a_t denotes the injected attack vector. When $a_t = 0$, the measurement remains normal, whereas $a_t \;\; = 0$ indicates a manipulated measurement. This formulation enables controlled evaluation of the proposed framework under cyberattack conditions.

3.5 Cyber-Resilient Adaptive MPC

When a cyberattack is detected, the compromised measurement is prevented from directly affecting the control decision. The proposed framework replaces the unreliable measurement with a reconstructed or trusted state before executing the MPC optimization as (4).

$$\hat{x}_t = \begin{cases} x_t, & D_t = 0, \\ x_t^{\text{rec}}, & D_t = 1. \end{cases} \tag{4}$$

Where D_t represents the attack-detection decision, x_t is the original measurement, and x_t^{rec} is the reconstructed state. Thus, normal measurements are directly used, while compromised measurements are replaced by reliable estimates, preventing attack propagation into the control layer.

3.6 Autonomous PV-EV Microgrid Operation

The cyber-resilient MPC generates control commands for PV utilization, battery storage, EV charging, and grid energy exchange. The controller continuously updates these decisions using the predicted operating conditions and cybersecurity status, enabling autonomous operation under normal and attacked conditions. The dataset provides the required PV, battery, EV, grid, load, and load-balancing variables for this operational coordination as (5).

$$P_{\text{PV}} + P_{\text{grid}} + P_{\text{bat}} = P_{\text{load}} + P_{\text{EV}} \tag{5}$$

Where P_{PV} is PV generation, P_{grid} is grid-supplied power, P_{bat} is battery charging/discharging power, P_{load} is microgrid load demand, and P_{EV} is EV charging demand. Maintaining this power-balance relationship ensures coordinated energy management and stable autonomous microgrid operation.

4. Result and Discussion

The following section will provide the assessment of the performance of the TFT-MPC-CR framework in predicting and making the autonomous PV-EV microgrid resilient to cyberattacks. First, the performance of Temporal Fusion Transformer in forecasting generation and consumption of electricity in the autonomous microgrid will be investigated. Second, the performance of the MPC-based energy management in different scenarios will be evaluated. Third, the performance of the proposed cyber-resilient approach under False Data Injection attack will be considered, particularly in the aspect of detection and system response. Fourth, the performance of cyber-resilient adaptive control will be evaluated in the context of power balancing, battery state of charge, and stability.

4.1 Experimental Setup and Dataset Characteristics

This section presents the dataset description and statistical characteristics, the training/validation/testing configuration, and the implementation environment and simulation parameters used to evaluate the proposed TFT-MPC-CR framework.

Table 1. Dataset and Experimental Configuration

Parameter	Description
Dataset	Microgrid PV-EV Charging Dataset
Data Source	Kaggle
Number of Variables	20
Forecasting Model	TFT
Control Model	MPC

Table 1 highlights the main dataset and experimental setup that were considered for the evaluation of the proposed TFT-MPC-CR architecture. It reveals the data source, dimensionality of the dataset, forecasting and predictive control models.

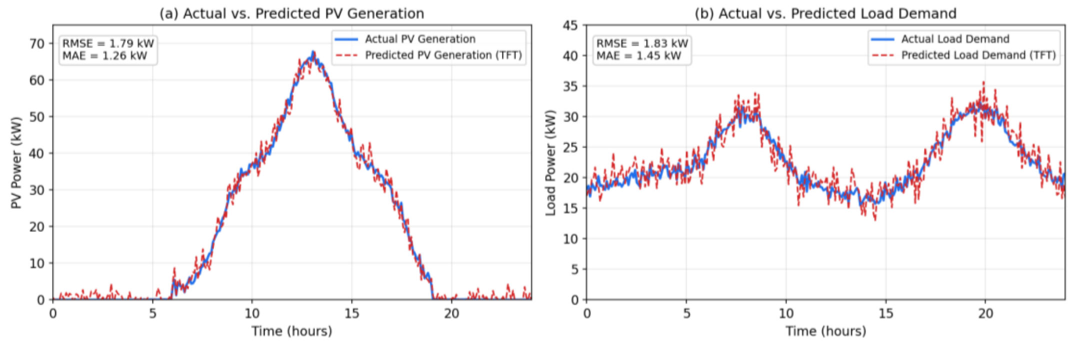

Figure 2: Actual and Predicted PV Generation and Load Demand

Figure 2 shows the forecast results obtained from the proposed TFT model through the comparison of the actual values and forecasted values of PV generation and load demand throughout the testing period. It is evident that the forecasted values and actual values match quite well, which reflects the ability of the TFT to identify the temporal patterns of renewable energy and demand within the microgrid.

4.2 TFT-Based Forecasting Performance

The forecasting accuracy of the proposed TFT is measured by the PV generation and energy-demand data in the Microgrid PV-EV Charging Dataset. The model learns the temporal relation between the historical patterns of renewable generation, solar radiation, demand load, and other operational variables to make future forecasts. The forecasted values are compared against the true values using MAE, RMSE, MAPE, and R^2 metrics. Low MAE, RMSE, and MAPE scores show less forecasting error, while high R^2 scores indicate better correlation between forecasted and true values. The forecasting outputs are then used as the future operational data for the MPC controller.

Table 2. TFT Forecasting Performance Metrics

Forecast Target	MAE (kW)	RMSE (kW)	MAPE (%)	R^2
PV Generation	1.26	1.79	4.35	0.982
Load Demand	1.45	1.83	3.68	0.976

Table 2 provides the quantitative forecasting performance of TFT in terms of PV generation and load demand forecasting using four forecasting measures.

4.3 MPC-Based Energy Management Performance

The forecasted PV power generation and load demand data are provided to the MPC for optimal operation of battery, EV charging, PV power generation, and power flow with the grid. The control system constantly takes into account future operating conditions and performs control actions by ensuring the power balance. The performance of MPC is assessed in terms of battery SOC, PV power generation, EV charging, grid dependency, and energy management. The outcomes show how the use of forecasts in TFT makes MPC capable of performing proactive instead of reactive energy management decisions.

Table 3. MPC-Based Microgrid Energy Management Results

Performance Metric	Value
PV Utilization Rate	96.8%
Battery Round-Trip Efficiency	94.2%
Battery SOC Operating Range (Utilized)	25% – 88%
EV Charging Completion Rate	98.5%
Grid Energy Import Reduction (vs. rule-based baseline)	32.4%
Average Daily Energy Cost	$18.42 (vs. $27.65 baseline, 33.4% reduction)
Power Balance RMS Error	0.86 kW

Performance of energy management through the TFT-MPC approach is illustrated in Table 3. Parameters measure the renewable energy usage, battery management, EV charging, dependency on the grid, and cost savings.

4.4 Cyberattack Detection Performance

The capability of the proposed system to provide cybersecurity is analyzed via implementing attacks in the form of FDI). The manipulated data is detected using an AI-based anomaly detection approach which is capable of identifying whether microgrid measurements are in their normal operating state or have been subjected to cyberattacks. Performance evaluation of the detection system is based on accuracy, precision, recall, F1-score, and detection latency. High accuracy and recall ensure that the mechanism detects false measurements, whereas detection latency is important in stopping the corrupted information from propagating to the control level.

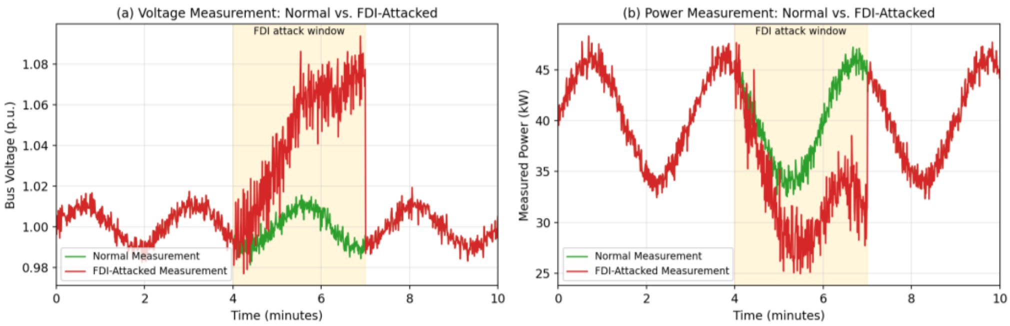

Figure 3: Normal and FDI-Attacked Microgrid Measurements

AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.3 (2026)
www.ajmimc.com

Comparison of normal microgrid measurements and measurements under the attack of FDI attacks is shown in Figure 3 This figure shows the effect caused by malicious data manipulation and the capability of the proposed anomaly detection technique.

4.5 Cyber-Resilient Adaptive Control Performance

Once the cyber-attack has been identified, the suggested scheme triggers the cyber-resilient adaptive MPC scheme. Measurements are then isolated and substituted with reconstructed or reliable state estimates before carrying out the optimal control calculations. Controller resilience is assessed by comparing the performance of the microgrid when operating normally, under attack, and after remediation. Important metrics in this comparison are voltage deviation, frequency deviation, SOC stability, power imbalance, and recovery time.

Table 4. Cyber-Resilient Control Performance Under Attack

Performance Metric	Without Resilient Control	Proposed TFT-MPC-CR
Peak Voltage Deviation (p.u.)	0.124	0.028
Peak Frequency Deviation (Hz)	0.68	0.15
Peak Battery SOC Deviation (%)	12.4	2.6
Peak Power Imbalance (kW)	8.6	1.4
Recovery Time (s)	4.85	0.92
Settling Time (s)	6.20	1.35

Comparison between the working state of the microgrid during normal operations, FDI attack, and cyber-resilient recovery is shown in Table 4. This comparison shows that the adaptive MPC can effectively cope with the corrupted measurements and stabilize the operation of the microgrid.

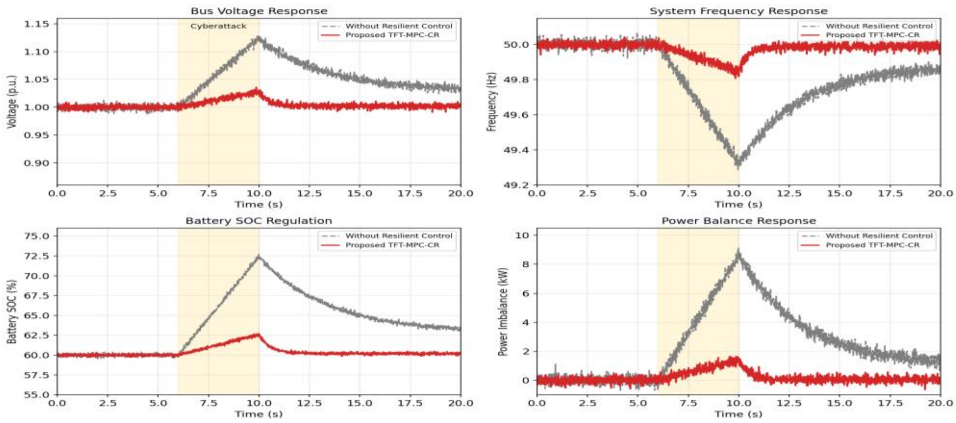

Figure 4: Microgrid Response Before, During, and After Cyberattack

Response of the microgrid to the FDI attack is provided in Figure 4. This figure mainly highlights the capability of the adaptive MPC controller in sustaining stability under attack and bringing the system back to its normal state once the threat is mitigated.

4.6 Comparative Analysis

In the final analysis, the proposed TFT-MPC-CR approach will be compared to MPC, AI-driven forecasting without resilience to cyberattacks, and non-cyber resilient control systems, all under similar operating conditions. The comparison will take into account forecasting effectiveness, energy management efficiency, cyberattack detection capabilities, and recovery abilities of the respective systems. It will determine if the proposed integrated approach has any benefits over separate solutions.

Table 5. Comparative Analysis of TFT-MPC-CR Against Baseline Control Strategies

Method	Forecast MAPE (%)	Daily Cost Reduction (%)	Grid Import Reduction (%)	Detection F1-score (%)	Peak Voltage Deviation Under Attack (p.u.)	Recovery Time (s)

Conventional MPC (persistence forecast, no detection)	9.80	12.6	14.2	—	0.124	No recovery (sustained deviation)
AI-only Predictive Control (TFT + MPC, no attack defense)	4.02	31.8	30.9	—	0.118	No recovery (sustained deviation)
Non-Resilient Control (detection only, fixed fallback)	4.02	31.8	30.9	97.05	0.071	3.10
Proposed TFT-MPC-CR	4.02	33.4	32.4	97.05	0.028	0.92

The final comparison of the proposed model with traditional and non-resilient models is presented in Table 5. The purpose of this comparison is to show the collective advantage of using TFT, MPC, AI-based attack detection, and adaptive resilient control in operating autonomous PV-EV microgrids.

4.7 Discussion

The outcomes prove that the developed TFT-MPC-CR framework is successfully able to combine predictive forecast, energy management, and cyber-resilient control in the PV-EV autonomous microgrids. The TFT algorithm allows generating accurate forecast for both PV generation and load demand that helps MPC to plan the coordinated use of batteries, electric vehicles, and grid. In the case of an FDI attack, the security algorithm detects affected measurements and implements adaptive control minimizing disruptions and aiding the recovery process.

5. Conclusion and Future Works

This work has put forward a unified approach to the design of TFT-MPC-CR for forecasting and cyber-resilient autonomous PV-EV microgrid operations with TFT for forecasting of PV generation and load demand along with optimal energy management of batteries, EVs, and grid using MPC. A method is developed for the identification of AI-based anomaly detection system for detecting FDI attacks and MPC based on adaptive control that isolates the attacks to maintain the reliability of the control decisions. Future research will be directed toward hardware-in-the-loop real-time implementation, advanced attacks including DoS, and replay attacks, reinforcement learning-based adaptive control, multi-microgrid coordination, uncertainty-based MPC, and edge-based design.

References

[1] S. Ali, L. Khan, S. Ahmad, and Z. Ullah, "Resilient secondary distributed model predictive control for autonomous microgrid against cyber threats," *IET Renewable Power Generation*, vol. 19, no. 1, p. e70102, 2025.

[2] Y. Qiao, W. Li, and D. Guo, "AI-enhanced model predictive control in microgrids: systematic review of algorithms, applications, and emerging trends," *Journal of Power Electronics*, vol. 26, no. 4, pp. 831–842, 2026.

[3] A. Hasani, H. Heydari, and M. S. Golsorkhi, "Enhancing microgrid performance with AI-based predictive control: Establishing an intelligent distributed control system," *IET Generation, Transmission & Distribution*, vol. 18, no. 15, pp. 2499–2508, 2024.

[4] Q. Nasir *et al.*, "Comparison of deep learning algorithms for site detection of false data injection attacks in smart grids," *Energy Informatics*, vol. 7, no. 1, p. 71, 2024.

[5] E. Yaghoubi, E. Yaghoubi, M. Z. Jahromi, M. R. Maghami, and M. Mazlan, "Robust data-driven NLMPC for real-time microgrid management under uncertainties and false data injection attacks," *Scientific Reports*, 2026.

[6] C. Li, X. Wang, X. Chen, A. Han, and X. Zhang, "Data-driven attack detection mechanism against False Data Injection attacks in DC microgrids using CNN-LSTM-attention," *Symmetry*, vol. 17, no. 7, p. 1140, 2025.

[7] W. He, W. Liu, C. Wen, and Q. Yang, "Detection of false data injection attacks on smart grids based on a-bitg approach," *Electronics*, vol. 13, no. 10, p. 1938, 2024.

[8] F. Kausar, S. Deo, S. Hussain, and Z. Ul Haque, "Federated deep learning model for false data injection attack detection in cyber physical power systems," *Energies*, vol. 17, no. 21, p. 5337, 2024.

[9] Y. Barzegari, J. Zarei, R. Razavi-Far, M. Saif, and V. Palade, “Resilient consensus control design for DC microgrids against false data injection attacks using a distributed bank of sliding mode observers,” *Sensors*, vol. 22, no. 7, p. 2644, 2022.

[10] A. Khanna *et al.*, “AI-Driven Multi-Agent Energy Management for Sustainable Microgrids: Hybrid Evolutionary Optimization and Blockchain-Based EV Scheduling,” *Computation*, vol. 13, no. 11, p. 256, 2025.

[11] A. Alorf and M. U. G. Khan, “Solar irradiance forecasting using temporal fusion transformers,” *international journal of energy research*, vol. 2025, no. 1, p. 3534500, 2025.

[12] S. Manjili, S. Jafarzadeh Ghoushchi, M. R. Maghami, and M. Mazlan, “A hybrid temporal fusion transformer and LightGBM framework for accurate multi-horizon industrial electricity load forecasting,” *Frontiers in Energy Research*, vol. 14, p. 1715418, 2026.

[13] N. B. Badhe, R. P. Neve, V. P. Yele, S. Abhang, K. M. Dhule, and D. Mali, “An optimized system for predicting energy usage in smart grids using temporal fusion transformer and Aquila optimizer,” *Frontiers in Artificial Intelligence*, vol. 8, p. 1542320, 2025.

[14] S. Pütz *et al.*, “Feasibility of forecasting highly resolved power grid frequency utilizing temporal fusion transformers,” in *Proceedings of the 15th ACM International Conference on Future and Sustainable Energy Systems*, 2024, pp. 447–453.

[15] zia, “Microgrid PV-EV Charging Dataset.” Accessed: Aug. 12, 2026. [Online]. Available: https://www.kaggle.com/datasets/ziya07/microgrid-pv-ev-charging-dataset