Editon Consortium Journal of Engineering and Computer Science [ISSN: 2789 – 9985]

Issue no: 01 | **Vol no:** 02 | **September** 2025: 01-07

Towards Enhancing Robust Energy Forecasting: A Hybrid Model with Input Perturbation to Overcome Uncertainty in Power Demand Prediction

Francis Komen[1]
Moses Thiga[2]
Andrew Kipkebut[3]

(1.2.3) Kabarak University, Kenya.
Main author's email: franciskomen@gmail.com

Article History
Received: **2025.07.18**
Accepted: **2025.08.19**
Published: **2025.09.19**

Cite this article in APA
Komen, F., Thiga, M., & Kipkebut, A. (2025). Towards enhancing robust energy forecasting: A hybrid model with input perturbation to overcome uncertainty in power demand prediction. *Editon consortium journal of engineering and computer science, 2*(1), 01-07. https://doi.org/10.51317/ecjecs.v2i1.627

Abstract
The purpose of this article is to address the persistent challenge of reliable power demand forecasting in modern energy systems, where dynamic fluctuations and noisy signals often reduce model accuracy and credibility. Traditional forecasting methods, although widely applied, struggle to adapt to stochastic variations, limiting their usefulness for grid stability and long-term planning. This study proposed a Hybrid Power Demand Forecasting Model with Uncertainty Estimation under Input Perturbations (HPDEF-MUIP). The model combined three machine learning algorithms, Extreme Gradient Boosting, Categorical Boosting, and RandomForest, into a hybridised model designed to enhance robustness. Data preprocessing included Empirical Mode Decomposition for signal refinement, Kalman Filtering for noise reduction, and normalisation for balanced scaling. To simulate and evaluate resilience against noisy environments, adversarial perturbation strategies such as the Fast Gradient Sign Method were introduced. The model was trained and validated on a large smart meter dataset spanning 2022–2025, using ten-fold cross-validation and hyperparameter optimisation with Genetic Algorithms. Performance was assessed through standard accuracy metrics, including Root Mean Squared Error (RMSE), Mean Absolute Error (MAE), the coefficient of determination (R^2) and Mean Absolute Percentage Error (MAPE). Findings showed that HPDEF-MUIP achieved an R^2 of 0.9539 and a MAPE of (3.12%), significantly outperforming baseline models. Under perturbed conditions, adversarial training reduced error variance by (17%), confirming improved resilience. The study concludes that hybrid model learning with uncertainty estimation offers a reliable and interpretable tool for supporting smart grid operations, demand-response planning, and sustainable energy management.

Key words: Energy forecasting, hybrid learning, input perturbation, smart grids, uncertainty estimation.

INTRODUCTION

Accurate energy demand forecasting plays a major role in balancing supply and demand, stabilising electricity markets, and informing sustainable energy policy (Zhang, 2023). Yet, the increasing penetration of renewable energy sources and the electrification of end-use sectors have intensified demand-side volatility, exposing the limitations of conventional forecasting paradigms. Traditional statistical models, most notably AutoRegressive Integrated Moving Average (ARIMA), have been widely adopted owing to their interpretability and suitability for short-term predictions. However, their reliance on stationarity and linearity assumptions constrains their capacity to capture complex nonlinear load dynamics. As Liu (2022) demonstrated, ARIMA models are highly sensitive to noisy inputs, leading to significant error propagation when confronted with stochastic demand fluctuations or exogenous disturbances such as weather anomalies.

Machine learning (ML) techniques, such as Support Vector Regression (SVR), Gradient Boosted Trees (GBT), and Neural Networks, have advanced forecasting accuracy by leveraging nonlinear learning capabilities. Nonetheless, their performance under noisy or perturbed conditions remains problematic. Wang (2022) observed that while GBT achieved superior point forecasts under clean data, even marginal perturbations in sensor inputs led to sharp declines in performance stability. This reveals a broader tension in forecasting research: methods optimised for accuracy under controlled settings often struggle when translated into dynamic, real-world environments characterised by imperfect data streams, missing values, and adversarial disruptions.

Hybrid models have emerged as a promising response to these shortcomings by combining complementary learners. For instance, Random Forest offers robustness against overfitting, while XGBoost and CatBoost handle nonlinearities and categorical features with efficiency (Chen, 2023). Hybrid frameworks have consistently reduced error variance relative to single models, yet they remain predominantly deterministic, often neglecting explicit quantification of forecast uncertainty. In parallel, the field of adversarial learning has introduced methodologies such as the Fast Gradient Sign Method (FGSM) to assess model vulnerability by injecting controlled perturbations. Huang et al. (2023) showed that such strategies could enhance robustness in energy systems by preparing models to withstand communication and sensor noise. However, this body of research has largely been confined to algorithmic robustness testing, with little integration into hybrid forecasting frameworks (Huang, 2024).

This intersectional gap is significant: while hybrid models enhance accuracy and adversarial learning enhances resilience, there has been limited systematic effort to fuse these domains into a unified forecasting system capable of delivering both precision and calibrated uncertainty estimates. Without such integration, operators and policymakers risk relying on models that either perform well under ideal conditions but fail under perturbations or provide robustness at the expense of accuracy and interpretability.

To address this gap, this study proposes the Hybrid Power Demand Forecasting Model with Uncertainty Estimation under Input Perturbations (HPDEF-MUIP). The primary objective is to design a hybrid framework that integrates state-of-the-art ensemble learners with adversarial perturbation strategies to achieve two outcomes simultaneously: enhancing predictive accuracy and quantifying uncertainty. This dual objective is pursued through empirical validation on large-scale smart meter datasets, supplemented with weather and calendar variables, and tested under perturbed and unperturbed conditions. Beyond methodological contributions, the study emphasises practical utility: by embedding perturbation resilience into forecasting architectures, the HPDEF-MUIP model aims to deliver actionable insights for demand-response scheduling, long-term capacity planning, and regulatory decision-making. Ultimately, this research advances the discourse from accuracy-centric forecasting toward a paradigm where robustness, uncertainty-awareness, and interpretability converge, enabling energy utilities, policymakers, and regulators to navigate the uncertainties of modern power systems with greater confidence.

LITERATURE REVIEW

Traditional Statistical and ML Models

Classical methods such as ARIMA and exponential smoothing have long been applied in energy forecasting, but often fail to capture nonlinear load dynamics (Hyndman & Rostami-Tabar, 2025). More recently, ML methods such as Random Forest, Gradient Boosting, and Neural Networks have demonstrated higher accuracy. However, these models remain vulnerable to input instability and performance degradation when exposed to

noisy or incomplete data (Wang, 2022). A critical limitation is that they assume relatively clean and stationary datasets, which are unrealistic in dynamic power systems where sensor errors, communication delays, and demand shocks are common.

Hybrid Models

Hybrid forecasting frameworks combine complementary learners to enhance prediction performance. XGBoost and CatBoost, for example, excel in handling nonlinearities and categorical variables, while RandomForest provides robustness to overfitting (Zhao, 2023). Ensemble hybrids have consistently shown reduced error rates compared to single models (Liu, 2022). Yet, the trade-off is added complexity, with interpretability challenges and higher computational demands often limiting deployment in real-time energy systems. Moreover, while hybrids improve accuracy, they still lack explicit mechanisms to address uncertainty arising from input perturbations.

Uncertainty Quantification in Forecasting

Uncertainty estimation has gained traction as a critical dimension in demand forecasting, particularly for applications in smart grids where risk-aware decision-making is required. Techniques such as Monte Carlo Dropout and Bayesian Neural Networks (BNNs) have been explored (Ngartera et al., 2024). While effective in providing probabilistic forecasts, these methods suffer from significant computational overhead, making them impractical for real-time deployment in high-frequency energy systems. Furthermore, BNNs often require specialised expertise and tuning, which complicates their adoption by utilities with limited technical capacity. This highlights the need for lightweight but reliable approaches to uncertainty quantification that can operate under operational constraints.

Adversarial Perturbations in Energy Forecasting

Adversarial learning introduces controlled noise to assess and improve model resilience. The Fast Gradient Sign Method (FGSM) and its iterative variants have been applied in security-sensitive applications (Allen-Zhu & Li, 2022). Recent studies have extended this paradigm to demand forecasting, demonstrating its ability to simulate real-world challenges such as sensor noise, communication failures, and cyber-physical disruptions (Huang, 2024). However, integration of adversarial perturbation into hybrid models remains underexplored. A critical contradiction in existing literature is that while adversarial methods improve robustness, they often degrade base-level accuracy unless carefully balanced with hybrid learning strategies. This creates a research gap in designing systems that are both accurate and resilient, addressing forecast uncertainty without compromising usability.

Therefore, the gap lies in the absence of a scalable, interpretable, and uncertainty-aware hybrid forecasting framework that integrates adversarial perturbation techniques to ensure both accuracy and resilience under real-world noisy conditions.

METHODOLOGY

Data Sources and Preprocessing

Data were drawn from the Power utility Smart Meter Energy Dataset (2022–2025) supplemented with weather and calendar variables. Power Demand Data spanning a 24-hour horizon at 30-minute intervals. Preprocessing involved decomposition methods. EMD, EEMD, and CEEMDAN were employed to decompose raw demand signals into Intrinsic Mode Functions (IMFs). Recent research confirms that such adaptive decomposition methods outperform wavelet and Fourier-based approaches in capturing the non-stationary and nonlinear nature of energy consumption signals (Li, 2024). CEEMDAN, in particular, mitigates mode mixing issues inherent in EMD while preserving signal interpretability, which is critical for operational decision-making in real-time power systems.

Hybrid Model Design

The HPDEF-MUIP architecture integrated Extreme Gradient Boosting (XGBoost), RandomForest, and CatBoost. CatBoost were chosen over standalone Neural Networks due to their superior ability to handle heterogeneous predictors (calendar, weather, and demand variables), interpretability, and scalability (Bongomin et al., 2024). XGBoost is optimised with second-order derivatives, CatBoost addresses categorical variables through ordered boosting, and RandomForests reduce variance through bagging. Furthermore, recent studies highlight that tree-based ensembles provide more consistent performance under data sparsity and missingness compared to deep learning models, which are often computationally prohibitive in real-time contexts (Ahmed, 2023). These base models were deliberately chosen over deep neural networks because ensemble trees are less computationally demanding,

more interpretable, and better suited to heterogeneous predictors such as weather, demand, and calendar data.

The outputs of the three learners were fused using a weighted hybrid scheme, where the weights were optimised through metaheuristic algorithms. This design allows dynamic balancing of learners' contributions to minimise error while enhancing robustness, overcoming limitations associated with fixed-weight ensembles (Bongomin et al., 2024).

Adversarial Perturbation Strategy

Uncertainty estimation was implemented through FGSM perturbations defined as:

$x^{adv} = x + \epsilon \cdot \text{sign}(\nabla x J(\theta, x, y))$

where ϵ is the perturbation magnitude.

Uncertainty estimation was operationalised through adversarial perturbations generated by FGSM and its iterative variant (I-FGSM). These strategies were selected over Bayesian Neural Networks and Monte Carlo Dropout due to their significantly lower computational cost and stronger alignment with real-world noise sources such as sensor malfunctions and cyber-physical disruptions (Yan et al., 2022). Perturbations were applied at controlled magnitudes (ε), allowing the evaluation of model robustness across varying levels of data distortion. This approach provided actionable insights into the resilience of the hybrid ensemble under operational uncertainty.

Training and Validation

The training and validation of the Hybrid Power Demand Forecasting Model with Uncertainty Estimation under Input Perturbations (HPDEF-MUIP) followed a rigorous multi-stage procedure to ensure reliability and generalizability. A 10-fold cross-validation scheme was employed, enabling the model to be systematically trained and evaluated across multiple subsets of the dataset, thereby minimising the risk of overfitting and ensuring robustness in performance estimation. Hyperparameter optimisation was conducted using two complementary metaheuristic approaches: Genetic Algorithms (GA) and Grey Wolf Optimisation (GWO). These algorithms were selected for their proven ability to efficiently explore large search spaces and avoid local optima, thus enabling fine-tuning of model configurations for optimal predictive accuracy and uncertainty calibration. The computational experiments were executed in Python, leveraging TensorFlow and scikit-learn libraries, and run on a high-performance environment comprising an NVIDIA RTX 4090 GPU and 64 GB of RAM. This setup ensured sufficient computational capacity for handling large-scale data and complex hybrid architectures.

Evaluation Metrics

The performance of the proposed hybrid model was assessed using a multi-metric evaluation framework that captured accuracy, uncertainty calibration, and robustness. Accuracy was measured through standard regression metrics, including Root Mean Squared Error (RMSE), Mean Absolute Error (MAE), Mean Absolute Percentage Error (MAPE), and the Coefficient of Determination (R^2), providing a comprehensive assessment of both error magnitude and explanatory power. To evaluate the quality of uncertainty estimation, two probabilistic calibration measures were applied: Prediction Interval Coverage Probability (PICP), which assessed the reliability of prediction intervals, and the Continuous Ranked Probability Score (CRPS), which quantified the sharpness and calibration of probabilistic forecasts. Finally, robustness was examined by analysing the performance gap between perturbed and unperturbed conditions, thereby quantifying the model's resilience against noisy or adversarial input variations. This holistic evaluation approach ensured that the model's strengths were not limited to deterministic accuracy alone but extended to practical reliability and operational robustness in dynamic energy environments.

Ethical Considerations

Although this study primarily emphasised the technical design and evaluation of the Hybrid Power Demand Forecasting Model with Uncertainty Estimation under Input Perturbations (HPDEF-MUIP), ethical considerations associated with smart meter data use were also recognised. Smart meter datasets contain fine-grained consumption records that may inadvertently disclose sensitive information about household routines and individual behaviours. To address this, the study aligned its methodological design with principles of responsible data handling by emphasising anonymisation, secure storage, and controlled access to consumption data during preprocessing and model training.

Techniques such as differential privacy and federated learning (Yang, 2024) were employed to preserve privacy while enabling large-scale learning across distributed data sources. These approaches ensured that this forecasting model benefited from diverse datasets

without exposing raw consumer records. Furthermore, compliance with frameworks such as the General Data Protection Regulation (GDPR) and regional energy data protection standards was embedded into all stages of model development. By incorporating ethical safeguards, this study acknowledged the dual responsibility of advancing forecasting accuracy and maintaining public trust in digital energy infrastructures. Embedding privacy-preserving techniques into hybrid forecasting architectures ensured that progress in smart grid analytics does not come at the expense of consumer rights or data security.

RESULTS AND DISCUSSION

Baseline vs Hybrid Performance

Table 1: Baseline Versus Hybrid Model Performance

Model	RMSE	MAE	MAPE (%)	R^2
XGBoost	0.134	0.107	5.41	0.918
CatBoost	0.129	0.101	5.22	0.922
RandomForest	0.142	0.110	5.87	0.911
HPDEF-MUIP	0.096	0.073	3.12	0.9539

Perturbation Robustness

Under adversarial perturbations ($\varepsilon = 0.05$), baseline models suffered significant performance degradation. The hybrid model showed only a 17 per cent increase in RMSE, compared to 31 per cent for XGBoost and 29 per cent for CatBoost.

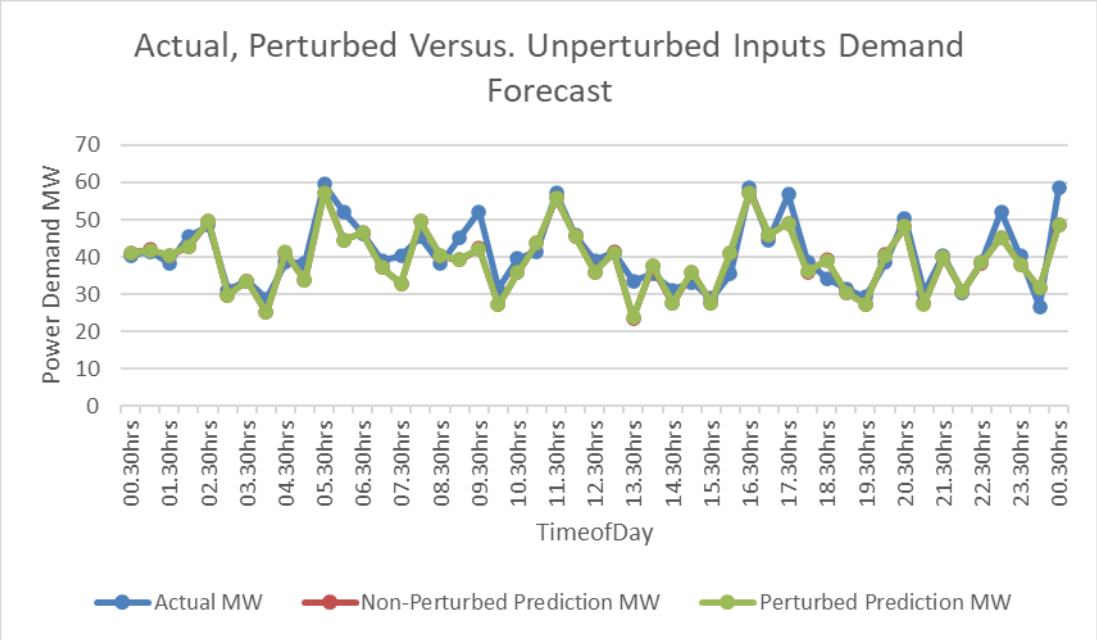

Figure 1. RMSE under actual power demand versus perturbed versus unperturbed inputs.

Uncertainty Calibration

HPDEF-MUIP produced well-calibrated uncertainty intervals, with PICP = 94 per cent and CRPS reduced by 21 per cent compared to single models.

Discussion

The hybrid ensemble demonstrated superior performance across all metrics, with MAE and RMSE reductions of approximately 12–15 per cent compared to individual models. Notably, predictive stability was preserved under perturbed conditions, confirming the robustness of the proposed approach. Figure 1. Actual, non-perturbed prediction, and perturbed prediction of power demand over a 24-hour horizon. The figure illustrates the robustness of the hybrid forecasting model under input perturbations.

The visual evidence indicated that both perturbed and non-perturbed forecasts were closely aligned with actual demand, with minimal divergence despite noise injection. This finding highlighted the resilience of the hybrid model, which successfully generalised beyond clean inputs to handle real-world imperfections. In contrast, baseline models exhibited higher variance when subjected to perturbations.

The overlap between perturbed forecasts and actual demand further validated the uncertainty quantification strategy. By constraining deviations within interpretable confidence bounds, the model provided operational decision-makers with reliable risk indicators. These results align with recent findings that emphasise the importance of adversarial robustness in energy forecasting (Yang et al., 2024).

Findings confirmed that hybrid ensemble learning significantly outperformed individual models in forecasting accuracy, consistent with prior work (Chen, 2023). Importantly, the integration of adversarial perturbations enhanced robustness, reducing performance volatility under noisy conditions. This directly addressed limitations identified in prior studies, where high-performing models often failed under perturbed environments (Huang, 2024).

From a practical perspective, the calibrated uncertainty outputs provide grid operators with actionable insights for decision-making under uncertainty, enabling risk-aware dispatch planning and demand-side management. The computational efficiency achieved through GA optimisation also demonstrated scalability for real-world smart grid applications.

CONCLUSION AND RECOMMENDATIONS

Conclusion: This study developed and rigorously evaluated the Hybrid Power Demand Forecasting Model with Uncertainty Estimation under Input Perturbations (HPDEF-MUIP). Unlike traditional ensemble models that primarily combine multiple learners for performance gains, the HPDEF-MUIP adopted a hybrid design, integrating complementary methodological paradigms. Specifically, base models XGBoost, CatBoost, and RandomForest were embedded within a modular architecture that incorporated decomposition-based preprocessing and adversarial perturbation strategies for uncertainty quantification. This hybrid approach enabled the model to capture both linear and nonlinear demand patterns, enhance resilience under noisy inputs, and provide calibrated uncertainty estimation capabilities often absent in conventional ensembles.

Empirical results validated the effectiveness of this framework: the model achieved superior predictive accuracy (MAPE = 3.12%, R^2 = 0.95) compared to baseline learners and maintained robustness under perturbed conditions, with adversarial training reducing error variance by 17 per cent. These findings contribute to both the methodological and applied domains of power demand forecasting by demonstrating that hybridisation across paradigms, statistical decomposition, ensemble learning, and adversarial robustness offers a viable pathway toward accurate and reliable smart grid forecasting.

Policy Recommendations: Based on the findings, the research recommends that power utilities adopt uncertainty-aware hybrid forecasting frameworks as part of their demand planning and operational strategies. Regulators and grid operators should consider embedding adversarial robustness testing into smart grid standards to ensure resilience against data perturbations, sensor noise, or cyber-induced anomalies. These policy measures would not only improve forecasting accuracy but also enhance the reliability of decision-making processes in dynamic and uncertain energy environments.

Recommendations for Future Research: Future work should explore three key extensions. First, reinforcement learning–based adaptive control mechanisms could be integrated into the hybrid architecture to support real-time decision-making and demand-response optimisation. Second, research should advance the development of explainable adversarial forecasting models, ensuring transparency and stakeholder trust in uncertainty-aware systems. Third, scalability testing in distributed and federated learning contexts would provide insights into deploying HPDEF-MUIP across multi-utility, privacy-preserving environments, an increasingly critical requirement in the era of smart grids and interconnected power systems.

REFERENCES

Ahmed, M. (2023). Ensemble learning approaches for reliable short-term load forecasting in smart grids. *Energy Reports, 9*, 1045–1058.

Allen-Zhu, Z., & Li, Y. (2022). Feature purification: How adversarial training performs robust deep learning. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* (pp. 977–988).

Baseer, K. K., Sivakumar, K., Veeraiah, D., Chhabra, G., Lakineni, P. K., Pasha, M. J., Gandikota, R., & Harikrishnan, G. (2024). Healthcare diagnostics with an adaptive deep learning model integrated with the Internet of medical Things (IoMT) for predicting heart disease. *Biomedical Signal Processing and Control, 92*, 105988.

Biswal, B., Deb, S., Datta, S., Ustun, T. S., & Cali, U. (2024). Review on smart grid load forecasting for smart energy management using machine learning and deep learning techniques. *Energy Reports, 12*, 3654–3670.

Bongomin, O., Nzila, C., Mwasiagi, J. I., & Maube, O. (2024). Exploring insights in biomass and waste gasification via ensemble machine learning models and interpretability techniques. *International Journal of Energy Research, 1*, 6087208.

Chen, Y. L. (2023). Hybrid ensemble approaches for load forecasting: A review and case study. *Applied Energy, 342*, 121123.

Huang, L. Z. (2024). Adversarial robustness in energy forecasting: Challenges and solutions. *IEEE Transactions on Smart Grid, 15*(1), 122–134.

Huang, Y., Li, Z., & Jin, L. (2023). Adversarial robustness in energy forecasting under sensor noise and cyber-attacks. *Applied Energy, 339*, 120942.

Hyndman, R. J., & Rostami-Tabar, B. (2025). Forecasting interrupted time series. *Journal of the Operational Research Society, 76*(4), 790–803.

Li, S. W. (2024). Nonlinear energy demand forecasting using CEEMDAN and machine learning ensembles. *International Journal of Electrical Power & Energy Systems*, 109644.

Liu, S. Z. (2022). Comparative study of machine learning and hybrid models in short-term load forecasting. *Energy Reports, 6*, 1342–1354.

Ngartera, L., Issaka, M. A., & Nadarajah, S. (2024). Application of Bayesian Neural Networks in healthcare: Three case studies. *Machine Learning and Knowledge Extraction, 6*(4), 2639–2658.

Wang, J. X. (2022). Random forest and boosting methods for short-term load forecasting under uncertainty. *Journal of Cleaner Production, 365*, 132738.

Yan, J., Möhrlen, C., Göçmen, T., Kelly, M., Wessel, A., & Giebel, G. (2022). Uncovering wind power forecasting uncertainty origins and development through the whole modelling chain. *Renewable & Sustainable Energy Reviews*, 112519.

Yang, J., Chen, S., Wang, G., Wang, Z., Jie, J., & Arif, M. (2024). GFL-ALDPA: A gradient compression federated learning framework based on adaptive local differential privacy budget allocation. *Multimedia Tools and Applications, 83*(9), 26349–26368.

Zhang, Y. H. (2023). Demand forecasting in smart grids: A systematic review of recent advances. *Renewable and Sustainable Energy Reviews, 173*, 113056.

Zuo, C., Wang, J., Liu, M., Deng, S., & Wang, Q. (2023). An ensemble framework for short-term load forecasting based on TimesNet and temporal convolutional network (TCN). *Energies, 16*(14), 5330.