# Federated Deep Learning-Based Collaborative Optimization and Privacy Preservation in Microgrid Clusters Using GRU Models

Enming Wang
School of Electrical Engineering, Northeast Electric Power University, Jilin 132012, Jilin, China
E-mail: rimeaij5255@outlook.com

**Keywords:** distributed generation system, federated learning, privacy preservation, microgrid cluster

**Received:** September 20, 2025

*To address the challenges faced in optimizing the operation of distributed power generation systems, this study proposes an innovative method. The method integrates GRU deep learning to model temporal operational patterns and federated learning to enable privacy-preserving collaborative optimal operation of microgrid clusters. This model employs data augmentation techniques to build local encapsulated models and leverages federated learning to achieve strategy evolution. Case analysis demonstrates that this approach excels in prediction accuracy (test RMSE of 12.5), operational cost control (reducing total cost by 15.1% compared to independent operation), and computational speed, while also offering significant advantages in privacy protection. It provides an effective solution for the optimal operation of microgrid clusters.*

*Povzetek: Študija predlaga inovativno metodo, ki z združitvijo globokega učenja GRU in federativnega učenja omogoča učinkovito, optimalno upravljanje gruč mikroomrežij.*

## 1 Introduction

In the context of global energy transition and the rapid development of smart grids, the integration of distributed energy sources (such as wind and solar energy) with microgrid technologies has emerged as a pivotal approach to enhancing energy utilization efficiency and optimizing distribution systems [1]. With the continuous advancement and cost reduction of renewable energy technologies, the deployment scale of distributed energy is rapidly expanding [2], presenting new opportunities and challenges for the flexibility and sustainability of power systems. However, the coordinated optimal operation of microgrid clusters remains fraught with challenges [3], and how to achieve efficient, secure, and reliable operation has become a critical research topic in the field of intelligent distribution systems both domestically and internationally.

Although traditional centralized optimization methods can achieve global optimization, they are highly dependent on communication networks and pose risks of privacy leakage [4], making them unsuitable for distributed scenarios involving multiple microgrid clusters. Distributed optimization methods, utilizing consensus algorithms [5] or game theory [6], have enhanced both economic efficiency and reliability, but they face limitations in terms of profit allocation, privacy protection, and the effectiveness of global optimization [7]. With the continuous progress of artificial intelligence and big data technologies, data-driven optimization methods have offered new insights for the coordinated optimal operation of multi-microgrid clusters [8]. Optimization methods based on reinforcement learning [9] can achieve rapid solutions through real-time data-driven approaches, but their stochastic exploration process may lead to local optima or convergence issues. Moreover, centralized data-driven methods also face challenges related to data privacy and communication bottlenecks, while distributed methods still encounter technical limitations in power interaction patterns and profit allocation calculations [10]. Therefore, how to achieve efficient and coordinated optimization of multi-agent microgrid clusters while protecting privacy has become a critical issue that demands immediate resolution.

To address these issues, this paper proposes a federated learning-based collaborative optimization and strategy evolution method for multi-agent microgrid clusters. This method involves uploading encapsulated models of each microgrid to the cloud for global strategy search [11] and conducting distributed joint training of horizontal federated neural networks [12,13] to achieve dynamic strategy evolution. The proposed approach addresses key limitations of existing methods by enabling privacy-preserving collaborative learning without raw data sharing, thanks to model encapsulation and cryptographic techniques. This approach not only effectively protects the data privacy of each microgrid but also enhances the collaborative operation efficiency of microgrid clusters, providing new insights for realizing smarter and more efficient energy management systems.

## 2 Related work

Currently, research on the optimal operation of microgrid clusters primarily focuses on two categories of methods: model-driven and data-driven approaches [14]. Model-driven methods achieve optimization by constructing objective functions and constraints through mathematical modeling. For instance, centralized optimization methods [15] employ a central controller to manage the entire microgrid cluster, enabling global optimization, but they are highly dependent on communication networks and pose risks of privacy leakage, making them unsuitable for multi-agent scenarios.

Distributed control methods enhance economic efficiency and reliability through consensus algorithms, but they fail to adequately address the issue of profit allocation among individual microgrids [16] and face challenges related to communication delays and consensus. Game theory methods [17] can optimize the system through interactions among multiple agents, eliminating the need for centralized control and enhancing system reliability and stability, but their solution process is complex and does not fully consider privacy protection. While classical control methods like adaptive fuzzy control [18] and backstepping control [19] excel in handling system nonlinearities and uncertainties for stabilization tasks in single systems (e.g., robotic manipulators [20] or compressors [21]), they are less suited for multi-agent, data-driven collaborative optimization where privacy and data decentralization are paramount. Table 1 summarizes the key characteristics of representative methods, highlighting limitations in privacy, global optimization capability, and scalability that this work aims to address.

Table 1: Comparison of microgrid cluster optimization methods

| Method Category | Cost Performance | Privacy Preservation | Global Optimization |
|---|---|---|---|
| Centralized Optimization [15] | High | Very Low | Strong |
| Distributed Optimization[5], [16] | Medium | Low | Medium |
| Game Theory[6], [17] | Medium-High | Low | Weak |
| Deep Reinforcement Learning[9] | Medium-High | Low | Medium |
| Proposed (FL+GRU) | High | High | Strong |

As an emerging paradigm for privacy-preserving collaborative learning, Federated Learning (FL) has seen recent research efforts explore its integration with domain-specific physical models or spatiotemporal structures to enhance model practicality and reliability. Our method aim to address a different facet of system control: enabling secure, collaborative strategy learning among multiple self-interested agents (microgrids) without raw data sharing. The proposed FL framework prioritizes privacy-preserving cooperation over direct system stabilization, making it complementary to, rather than a replacement for, classical robust control in complex systems.

# 3 Method introduction

## 3.1 Cloud-edge collaborative optimization strategy

This paper proposes a cloud-edge collaborative optimization strategy based on federated neural network learning [22], tailored for distributed power generation systems. Strategy Evolution is applied to describe the iterative process where the global operational strategy, encoded in the federated model parameters, is progressively refined through cycles of local execution, encrypted model update uploads, secure aggregation on the cloud, and subsequent distribution of the improved global model back to the microgrids. The fundamental framework of the microgrid cloud-edge collaborative optimization strategy is structured into three layers, as depicted in Figure 1. The bottom layer constitutes the physical layer of microgrid clusters, encompassing multiple microgrids, each equipped with power devices and control systems. The intermediate layer serves as the global strategy search layer, comprising numerous encapsulated models, each corresponding to a microgrid. These encapsulated models are interconnected via an interaction network and a learning network, primarily responsible for searching and optimizing global strategies, thereby providing optimized strategies for the microgrid cluster. The topmost layer is the FL evolution layer, primarily composed of a learning network. By communicating with the interaction network and encapsulated models in the lower layers, this layer employs federated learning algorithms to evolve and optimize strategies to accommodate the operational requirements of the microgrid cluster, consequently enhancing the operational efficiency and reliability of the microgrid cluster.

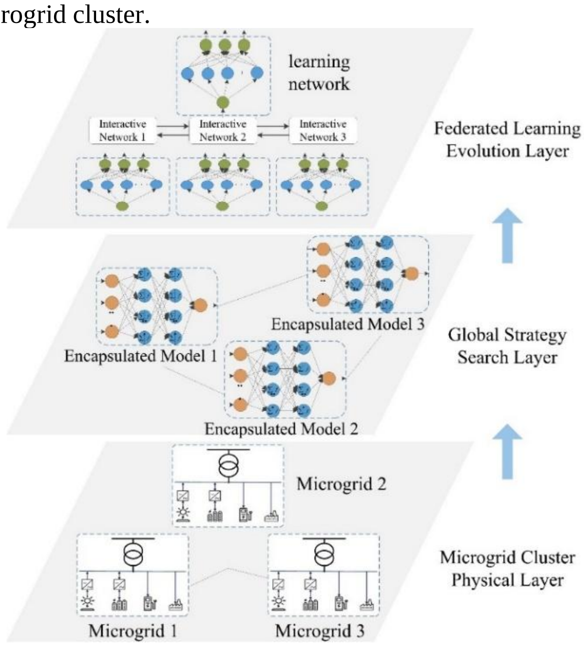

Figure 1: Basic framework of cloud-edge collaborative optimization strategy for microgrids

## 3.2 Collaborative optimization model for microgrid clusters

### 3.2.1 Objective function

In the optimization model of a microgrid, the objective is to minimize the daily operational cost of the microgrid. The objective function is expressed as follows:

$$\min C_{\mathrm{MG},i}=\sum_{t=1}^{T}(C_{\mathrm{self},i,t}+C_{\mathrm{market},i,t}) \tag{1}$$

Herein, $C_{\mathrm{self},i,t}$ denotes the operational cost of all units within microgrid $i$ at time $t$; $C_{\mathrm{market},i,t}$ represents the trading cost between microgrid $i$ and the external market at time $t$, encompassing both electricity purchase expenses and sales revenue.

The computation of operational and maintenance expenditures $C_{\mathrm{OM},i,t}$ is delineated as follows:

$$C_{\mathrm{OM},i,t}=k_{\mathrm{PV}}P_{\mathrm{PV},i,t}+k_{\mathrm{WT}}P_{\mathrm{WT},i,t}+k_{\mathrm{GT}}P_{\mathrm{GT},i,t}+k_{\mathrm{ES}}\left|P_{\mathrm{ES},i,t}\right| \tag{2}$$

where, the subscripts $[\mathrm{PV},\mathrm{WT},\mathrm{GT},\mathrm{ES}]$ represent photovoltaic, wind turbine, gas turbine, and energy storage system, respectively; $P$ and $k$ denote the corresponding unit's power output and unit operating cost.

The fuel cost for the gas turbine, denoted as $C_{\mathrm{f},i,t}$, is calculated as follows:

$$C_{\mathrm{f},i,t}=c_{\mathrm{NG}}\frac{P_{\mathrm{GT},i,t}}{\eta_{\mathrm{GT}}L_{\mathrm{NG}}} \tag{3}$$

where, $C_{\mathrm{NG}}$ and $L_{\mathrm{NG}}$ represent the price of natural gas and its calorific value, respectively; while $\eta_{\mathrm{GT}}$ signifies the efficiency index of the gas turbine. The cost of life degradation for the energy storage device, denoted as $C_{\mathrm{NS},i,t}$, is calculated as follows.

$$C_{\mathrm{NS},i,t}=c_{\mathrm{NS}}\frac{P_{\mathrm{NS},i,t}}{L_{\mathrm{R}}D_{\mathrm{R}}E_{\mathrm{R}}} \tag{4}$$

where, $c_{NS}$ signifies the unit power cost coefficient of the energy storage device; $P_{NS,i,t}$ represents the charge/discharge power of the energy storage device in microgrid $i$ at time $t$; $L_{\mathrm{R}}$ denotes the cyclic life degradation coefficient; $D_{\mathrm{R}}$ indicates the depth of charge/discharge coefficient; and $E_{\mathrm{R}}$ stands for the energy efficiency coefficient.

The cost of electricity purchase and sale under the centralized transaction model, $C_{\mathrm{market},i,t}$, is calculated as follows.

$$C_{\mathrm{market},i,t}=e_{\mathrm{mg},i,t}(P_{\mathrm{grid},i,t}+\sum_{j\neq i}P_{\mathrm{mg},i,j,t}) \tag{5}$$

Herein, $e_{\mathrm{mg},i,t}$ denotes the net energy exchange of microgrid $i$ at time $t$; $P_{\mathrm{grid},i,t}$ represents the transaction price between microgrid $i$ and the main grid; $P_{\mathrm{mg},i,j,t}$ signifies the aggregate transaction price between microgrid $i$ and other microgrids $j$.

In the operation of microgrid clusters, the trading mechanism $f_{\mathrm{trade}}$ serves as the linchpin for facilitating energy transactions and economic settlements among microgrids. This mechanism, predicated on the predetermined target trading power $P_{\mathrm{trade},t}$ and target trading price $e_{\mathrm{trade},t}$, derives the actual trading power $P_{\mathrm{mg},t}$ and trading price $e_{\mathrm{mg},t}$ through the settlement process.

$$(e_{\mathrm{mg},t},P_{\mathrm{mg},t})=f_{\mathrm{trade}}(P_{\mathrm{trade},t},e_{\mathrm{trade},t}) \tag{6}$$

In the operation of microgrid cluster, the formulas for power balance and cost equilibrium are delineated as follows:

$$\sum_{i}P_{\mathrm{mg},i,t}=P_{\mathrm{grid,MGs},t} \tag{7}$$

$$\sum_{i}e_{\mathrm{mg},i,t}P_{\mathrm{mg},i,t}=e_{\mathrm{g},t}P_{\mathrm{grid,MGs},t} \tag{8}$$

where, $P_{\mathrm{grid,MGs},t}$ signifies the actual transactional power between the microgrid cluster and the main grid at time $t$; whereas $e_{\mathrm{g},t}$ represents the electricity tariff of the primary grid.

### 3.2.2 Constraints

When optimizing the operation of microgrid cluster, various constraints must be considered to ensure that the system meets both physical and economic requirements while remaining operationally viable.

**1) Controllable power source power constraints:**

The actual power output $P_{\mathrm{GT},i,t}$ of controllable power sources within microgrid $i$ at time $t$ is bounded by $P_{\mathrm{GT},i}^{\min},P_{\mathrm{GT},i}^{\max}$.

$$P_{\mathrm{GT},i}^{\min},,\ P_{\mathrm{GT},i,t},,\ P_{\mathrm{GT},i}^{\max} \tag{9}$$

**2) Power constraints for charging and discharging:**

The state of the energy storage system at any given time, quantified by its State of Charge (SOC), along with the formulation for calculating its charging and discharging efficiencies, is delineated as follows [23].

$$S_{\mathrm{OC},t}=S_{\mathrm{OC},t-1}-\frac{P_{\mathrm{ES},i,t}\Delta t}{E_{\mathrm{R}}}\eta_{\mathrm{B}} \tag{10}$$

$$\eta_{\mathrm{B}}=\begin{cases}\eta_{\mathrm{BC}},P_{\mathrm{ES},i,t}<0\\ \dfrac{1}{\eta_{\mathrm{BD}}},P_{\mathrm{ES},i,t}..0\end{cases} \tag{11}$$

$$S_{\mathrm{OC}}^{\min}„\ S_{\mathrm{OC},t}„\ S_{\mathrm{OC}}^{\max} \qquad (12)$$

Herein, $P_{\mathrm{ES},i,t}$ signifies the power output of the energy storage system within microgrid $i$ at time $t$, where BD denotes discharging and BC represents charging. The term $\Delta t$ denotes the time step, while $E_{\mathrm{R}}$ represents the rated capacity of the energy storage system. Additionally, $\eta_{\mathrm{B}}$ denotes the efficiency of both charging and discharging processes, and the bounds of $S_{\mathrm{OC},t}$ are defined by $S_{\mathrm{OC}}^{\max}$ and $S_{\mathrm{OC}}^{\min}$.

Furthermore, it is stipulated that the energy storage system should maintain the same state of charge (SOC) at the commencement and conclusion of the optimization period, denoted respectively as $S_{\mathrm{OC},0}$ and $S_{\mathrm{OC},T}$.

$$S_{\mathrm{OC},0} = S_{\mathrm{OC},T} \qquad (13)$$

The charge-discharge power constraint is expressed as follows.

$$\begin{cases} 0„\ P_{\mathrm{ES},i,t}„\ P_{\mathrm{ES},i}^{\mathrm{BD}}, & P_{\mathrm{ES},i,t}..0 \\ -P_{\mathrm{ES},i}^{\mathrm{BC}}„\ P_{\mathrm{ES},i,t} < 0, & P_{\mathrm{ES},i,t} < 0 \end{cases} \qquad (14)$$

**3) Transaction transmission power constraints:**

In participating in market transactions, the microgrid's power output should stay within allowable limits to comply with market regulations and physical constraints. The minimum and maximum permitted power outputs of the microgrid in market transactions are denoted as $P_{\mathrm{market}}^{\min}$ and $P_{\mathrm{market}}^{\max}$, respectively.

$$P_{\mathrm{market}}^{\min}„\ P_{\mathrm{market},i,t}„\ P_{\mathrm{market}}^{\max} \qquad (15)$$

**4) Power balance constraint:**

$$P_{\mathrm{PV},i,t} + P_{\mathrm{WT},i,t} + P_{\mathrm{GT},i,t} + P_{\mathrm{ES},i,t} + P_{\mathrm{mg},i,t} = P_{\mathrm{load},i,t} \qquad (16)$$

where, $P$ represents the power output of the corresponding units.

**5) Transaction price constraint:**

In the electricity transactions between microgrids, the transaction price $e_{\mathrm{mg},i,t}$ must satisfy the condition of being greater than the selling price $e_{s,t}$ and less than the purchasing price $e_{\mathrm{b},t}$.

$$e_{s,t}„\ e_{\mathrm{mg},i,t}„\ e_{\mathrm{b},t} \qquad (17)$$

## 3.3 Global strategy search

### 3.3.1 Deep Learning-based local encapsulation model

Addressing the limitations of local encapsulation models in microgrids when dealing with various operating scenarios, due to historical data's inability to comprehensively cover all possible contexts, we propose a data augmentation method combining nonparametric kernel density estimation with Latin hypercube sampling [24]. The encapsulated model is a local surrogate model that abstracts the microgrid's operational cost function using a GRU network. This encapsulation allows the model to be shared in FL while preserving data privacy. Firstly, nonparametric kernel density estimation is employed to uncover the intrinsic characteristics of operational data, allowing for a more accurate reflection of the data distribution without relying on specific prior distribution assumptions. Subsequently, by integrating the estimated probability density function to obtain the cumulative distribution function, and applying Latin hypercube sampling techniques, a large number of simulated scenario data are generated.

$$(P_m, C_m) = f_{\mathrm{MG}}(S_m) \qquad (18)$$

Herein, $P_m$ denotes the power of each unit in the microgrid; $f_{\mathrm{MG}}$ represents the optimization model; $C_m$ signifies the operational cost of the microgrid; $S_m$ stands for the scenario data generated by sampling.

The article employs a deep learning network based on gated recurrent units (GRUs) for feature encapsulation [25]. GRU is chosen for its simpler structure compared to LSTM, reducing computational cost while maintaining strong performance in capturing short-term temporal dependencies. The encapsulation process involves initially training the GRU model using historical operational data to accurately forecast the operational costs of a microgrid. Subsequently, the trained model is encapsulated and uploaded to the cloud, where it is utilized for global policy search and optimization.

To enhance the robustness of the local encapsulated models against diverse and unseen operating conditions, we employ a data augmentation technique combining Nonparametric Kernel Density Estimation (KDE) and Latin Hypercube Sampling (LHS). The procedure is as follows:

1) Probability Density Estimation (KDE): For each uncertain variable $v$ in a microgrid's historical dataset, we estimate its probability density function (PDF) using KDE:

$$\hat{f}_v(x) = \frac{1}{nh}\sum_{j=1}^{n} K\left(\frac{x - x_j}{h}\right) \qquad (19)$$

where $K$ is the kernel function and $h$ is the bandwidth.

2) Cumulative Distribution Function (CDF): The corresponding cumulative distribution function (CDF) $\hat{F}_v(x)$ is obtained by integrating the estimated PDF:

$$\hat{F}_v(x) = \int_{-\infty}^{x} \hat{f}_v(t)dt \qquad (20)$$

3) Stratified Sampling (LHS): LHS is then used to generate $S$ samples for each variable. For each of the $S$ strata, a single value is sampled. This is achieved by:

$$u_s \sim \mathrm{Uniform}((s-1)/S, s/S) \qquad (21)$$

and then transforming these uniform samples through the inverse of the estimated CDF:

$$x_s^{scenario} = \hat{F}_v^{-1}(u_s) \tag{22}$$

The sampled values for all correlated variables are combined to form a large set of synthetic, yet realistic, daily operational scenarios , which is used to train the local GRU models, significantly improving their generalization capability.

### 3.3.2 Evolution strategies based on federated learning

This evolution process of Microgrid Cluster strategies based on federated learning, illustrated in Figure 2, aims to achieve multi-agent collaborative optimization while ensuring privacy protection. We adopt homomorphic encryption to secure the transmission of local model updates. Specifically, the Paillier cryptosystem is used to encrypt gradient updates before aggregation. Each microgrid first constructs and trains a local model using gated recurrent units (GRUs) and then uploads these models to the cloud. During the distributed training phase, we adopt a longitudinal federated neural network (federated heterogeneous neural network) [26] as the core framework. Each microgrid possesses its own underlying model, tailored to local data processing. Through an encrypted interaction layer model, secure communication among microgrids is facilitated, enabling the integration of operational states. The top-level model is responsible for delivering the final decisions. The global policy repository in the cloud guides the edge policy networks of individual microgrids to update. Following policy updates, each microgrid executes local optimization based on the new strategies and uploads the operational results and feedback data to the cloud. These data are instrumental in further refining the global policy repository, fostering a continuous improvement loop.

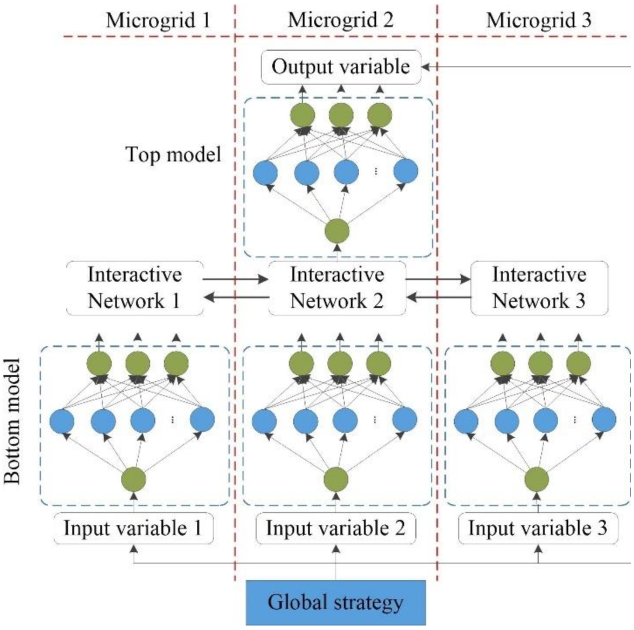

Figure 2: The evolution process of microgrid cluster strategies based on federated learning

We adopt a Vertical Federated Learning (VFL) architecture, suitable for scenarios where participating entities (microgrids) hold different feature sets about the same entities.

Each microgrid $i$ maintains a local Gated Recurrent Unit (GRU) model, $\mathrm{GRU}_i$ . This model processes the microgrid's unique private features, primarily the historical power outputs of its local units (PV, Wind, Gas Turbine, Load) to predict its operational cost. The intermediate outputs (embeddings) from each local GRU, denoted $h_i$ , are securely transmitted to the cloud. This communication is protected using homomorphic encryption. On the cloud server, a top model, typically a fully connected neural network, aggregates these encrypted intermediate outputs from all microgrids. After secure aggregation and decryption, the top model uses the combined information $H = \{h_1, h_2, ..., h_N\}$ to produce the final global decision, which includes the recommended transaction strategies for the next time period.

The loss function is computed based on the global strategy's performance. The gradients concerning the top model's parameters are computed directly on the cloud. The gradients concerning the bottom models' parameters are computed and securely propagated back to each respective microgrid for local model updates. This architecture allows microgrids to collaboratively learn a global optimization strategy while keeping their raw data and model parameters private.

### 3.3.3 Global strategy search based on encapsulated microgrid models

After receiving the encapsulated models from various microgrids, the cloud integrates these models into a unified optimization model. Leveraging the outcomes of scenario simulations, the cloud executes a global strategy search, generating a comprehensive global strategy library that encompasses a myriad of optimization strategies. Through the distributed collaborative training of federated neural networks, each microgrid can engage in the exchange and learning of model parameters with other microgrids while safeguarding local data privacy. This continuous enhancement of operational strategies not only refines individual microgrid performance but also facilitates the coordinated optimization of the entire microgrid cluster. The construction and solution process of this optimization model is illustrated in Figure 3.

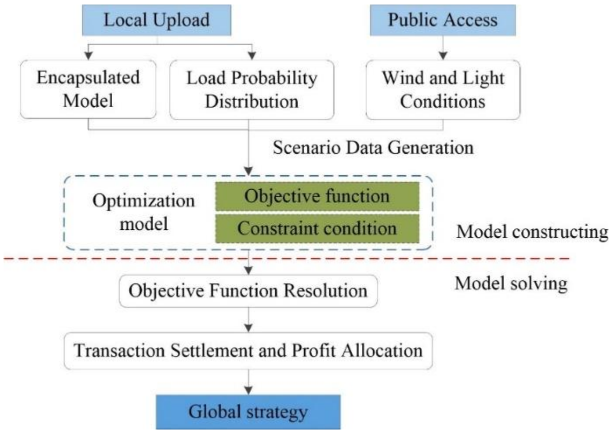

Figure 3: Basic workflow of the optimization model construction and solution process

To achieve the minimization of the total cost of microgrid clusters (MGs), the objective function is expressed as follows:

$$\begin{cases} \min C_{\text{MGs}} = \sum_{t=1}^{T}\sum_{i=1}^{I}\left(C_{\text{self},i,t} + C_{\text{market},i,t}\right) \\ C_{\text{self},i,t} = N_{\text{GRU},i} P_{i,t} \\ C_{\text{market},i,t} = e_{\text{mg},i,t} P_{\text{mg},i,t} \\ (e_{\text{mg},t}, P_{\text{mg},t}) = f_{\text{irade}}(P_{\text{trade},t}, e_{\text{trade},t}) \end{cases} \tag{23}$$

where, $C_{\text{self},i,t}$ represents the autonomous operating cost of microgrid $i$ at time $t$, which is derived through the Gated Recurrent Unit (GRU) network $N_{\text{GRU},i}$ based on the power $P_{i,t}$. $C_{\text{market},i,t}$ denotes the market transaction cost of microgrid $i$ at time $t$, obtained by the product of the transaction price $e_{\text{mg},i,t}$ and the transaction power $P_{\text{mg},i,t}$. The transaction price and power $(e_{\text{mg},t}, P_{\text{mg},t})$ are determined through the trading function $f_{\text{trade}}$, which calculates them based on the market transaction power $P_{\text{trade},t}$ and market transaction price $e_{\text{trade},t}$.

In the trading mechanism designed in this paper, the calculation of the purchasing electricity price $C_{\text{buy}}$ and the selling electricity price $C_{\text{sell}}$ proceeds as follows:

$$C_{\text{buy}} = \frac{C_{\text{DN}}(P_{\text{buy},t}) - \frac{1}{2}C_{\text{DN}}^{-}}{P_{\text{buy},t}} \tag{24}$$

$$C_{\text{sell}} = \frac{C_{\text{DN}}(P_{\text{sell},t}) - \frac{1}{2}C_{\text{DN}}^{-}}{P_{\text{sell},t}} \tag{25}$$

Herein, $C_{\text{DN}}$ signifies the aggregate expenditure incurred by the microgrid for the purchase of power at time instance $t$; whereas $C_{\text{DN}}^{-}$ denotes the supplementary cost coefficient associated with the network during the power sales process.

### 3.3.4 Privacy preservation with homomorphic encryption

To secure the transmission of local model updates during federated learning, we employ the Paillier cryptosystem, a partially homomorphic encryption scheme. This ensures privacy while allowing necessary computations on the cloud server.

Before uploading to the cloud, each microgrid ii encrypts the gradients $\nabla W_i$ from its local GRU model update using the cloud's public key. Only the encrypted gradients $[\nabla W_i]$ are transmitted.

$$[\nabla W_i] = Enc_{PK}(\nabla W_i) \tag{26}$$

The cloud server aggregates the encrypted gradients received from all N microgrids. Due to the homomorphic properties of Paillier, the sum of the encrypted gradients is equivalent to the encryption of the sum of the plaintext gradients:

$$[\nabla W_{global}] = \prod_{i=1}^{N} [\nabla W_i] \tag{27}$$

The aggregated encrypted result $[\nabla W_{global}]$ is then decrypted by the cloud server using its private key to obtain the plaintext global gradient update:

$$\nabla W_{global} = \text{Dec}_{SK}([\nabla W_{global}]) \tag{28}$$

This global update is used to refine the global strategy repository, which is then distributed back to the microgrids. This process ensures that the cloud server never accesses the plaintext local gradients of any individual microgrid, thereby preserving the privacy of each microgrid's operational data.

# 4 Experiment and analysis

## 4.1 Cases and simulation

In the MATLAB platform, we have constructed a physical simulation model for a microgrid cluster, which includes three microgrids, each equipped with different distributed energy systems to facilitate power transactions between microgrids and interactions with the main grid. The GRU model takes 24 historical hourly values as input and predicts the operational cost for the next hour. In this model, we conducted tests and training for federated learning and neural network models. To achieve efficient power trading and management, each microgrid is equipped with specific distributed energy units. Table 2 details the unit configurations for each microgrid. Implementation used TensorFlow Federated for FL framework and PyTorch for neural network models. The optimization solver settings included a batch size of 32 and early stopping patience of 10 epochs. The federated learning process ran for 50 communication rounds. The GRU model contained 2 hidden layers with 64 units each, trained with a learning rate of 0.001 using the Adam optimizer.

To evaluate the model under realistic conditions, a diverse set of operational scenarios was generated to account for uncertainties in renewable generation and load. The process began with one year of historical hourly data for photovoltaic output, wind turbine output, and load from three microgrids. Non-parametric kernel density estimation was first applied to this data to accurately model the probability distributions of these uncertain variables without restrictive assumptions. Then, Latin Hypercube Sampling was employed using the derived cumulative distribution functions to generate 500 distinct daily scenarios, ensuring comprehensive coverage of the potential operational space. These scenarios were divided into a training set (400 scenarios) for model development and a test set (100 scenarios) for generalization analysis, providing a robust basis for evaluating the proposed method. All compared models (FL, DQN, VDN) were trained on the same dataset for fair comparison.

Table 2: Unit configurations for each microgrid

| Power/kW | Microgrid 1 | Microgrid 2 | Microgrid 3 |
|---|---|---|---|
| Photovoltaic Station | 320 | 400 | 0 |
| Wind Power Plant | 560 | 0 | 400 |
| Gas Turbine | 800 | 400 | 0 |
| Energy Storage | 0 | 0 | 600 |
| Load | 720 | 600 | 1060 |
| Electrical Grid | 2500 | 2000 | 2000 |

An ablation study was conducted to evaluate the efficacy of the KDE+LHS data augmentation. When the GRU models were trained without augmentation, the test RMSE increased by approximately 22% compared to the augmented case (from 12.5 to 15.3), confirming that data augmentation significantly improves model generalization to unseen operational scenarios.

To assess the generalization capability of the proposed FL-based framework, we tested the trained model on the independent test set of 100 scenarios that were not used during training. The Root Mean Square Error (RMSE) for operational costs on the test set exhibits only a marginal increase (approximately 11%) compared to the training set. This indicates that the GRU-based encapsulated models possess strong generalization power and have not overfitted to the training data.

## 4.2 Collaborative operation and prediction results

To verify the effectiveness of the proposed edge-end microgrid encapsulation model, we validated the encapsulated modeling of the operation cost of each microgrid using a deep learning-based approach. Specifically, a Gated Recurrent Unit (GRU) deep learning model was employed for encapsulation modeling. After training, the error statistics between the predicted and actual internal operation costs of each microgrid are shown in Figure 4. As can be seen from Figure 4, after training, each microgrid can accurately predict its internal operation costs. This method achieves high prediction accuracy for the operation costs of each microgrid.

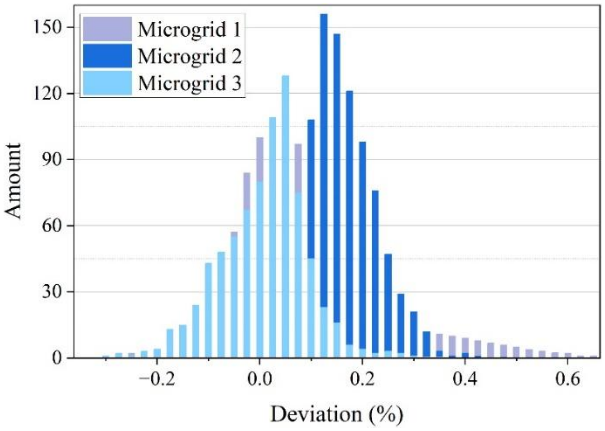

Figure 4: Prediction error of microgrid operation cost

To further validate the efficacy of the collaborative operation of microgrid clusters based on the locally encapsulated deep learning model, we present the training convergence results. As illustrated in Figure 5, the RMSE progressively converges during the training process, indicating that the federated learning model adeptly assimilates the strategies for global optimization on the cloud. With the incremental progression of federated learning iterations, the RMSE gradually diminishes, ultimately stabilizing at a notably reduced level. This phenomenon underscores the remarkable alignment between the local decision outputs of individual microgrids and the globally optimized decisions derived from the cloud, thereby substantiating the robustness and validity of the federated learning strategy.

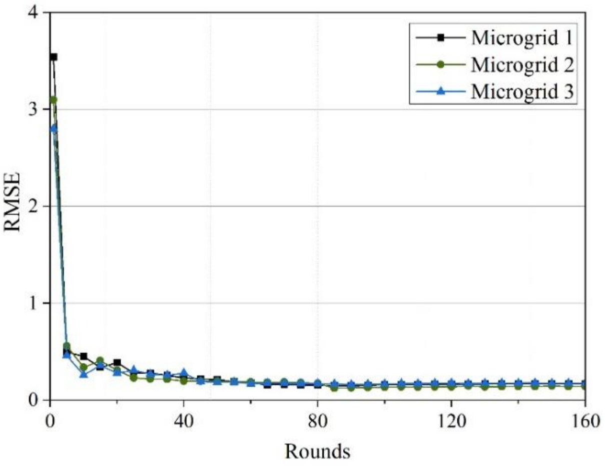

Figure 5: The loss curve of federated learning

## 4.3 Comparative experiment

To evaluate the efficacy of the proposed federated learning approach, this study conducted comparative experiments with microgrid clusters operating independently, under non-cooperative game theory (NG), deep Q network (DQN), and value decomposition network (VDN). Optimization was performed across 20 distinct scenarios, and the transaction power and electricity price distribution of Microgrid 1 under these five methods are illustrated in Figure 6. As depicted in the figure, the transaction power and electricity price exhibit significant fluctuations under independent operation and non-cooperative game theory, particularly at specific moments. While the DQN and VDN methods demonstrate some optimization effects, the fluctuations in transaction power and electricity price remain intermediate between independent operation and federated learning. In contrast, the federated learning method exhibits notable superiority in optimizing transaction power and electricity price distribution, with relatively smaller fluctuations in transaction power and more stable electricity price fluctuations, especially during the 12–16-hour period, effectively reducing volatility and maintaining system stability, thereby demonstrating improved optimization performance.

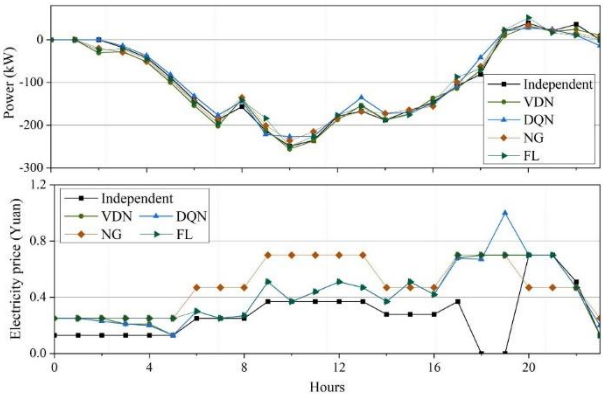

Figure 6: Daily transaction power and electricity price of microgrid 1 optimized using different methods

Figure 7 compares the operational costs of the microgrid cluster under various methods. The RMSE for operational cost prediction on the test set was 12.5 for the FL model, compared to 18.3 for DQN and 25.1 for VDN. FL reduced total cost by 15.1% compared to Independent Operation ($p < 0.05$, paired t-test). The deep Q network (DQN) method further reduces the operational costs of Microgrid 1 and Microgrid 3, consequently lowering the total operational costs. However, the non-cooperative game theory (NG) method significantly increases the operational costs of Microgrid 1, reaching the highest level. In comparison, the FL method demonstrates remarkable advantages, with the total operational costs significantly reduced, highlighting FL's outstanding performance in cost control.

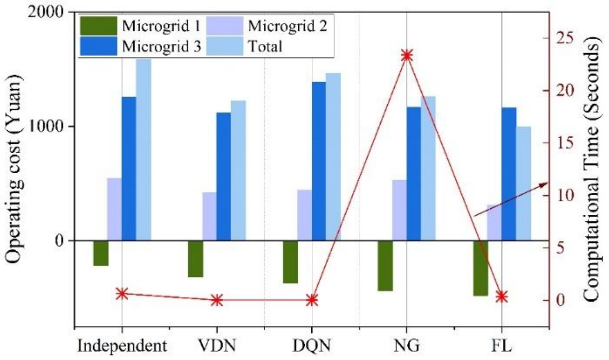

Figure 7: Daily operating cost of and computational speed of the microgrid cluster optimized by various methods

From the perspective of computational speed, there is a noticeable disparity among the methods. The computational time for FL was 0.36 seconds per global iteration, significantly faster than NG but slower than DQN due to cryptographic operations. In summary, the FL method demonstrates significant advantages in both the operational cost control of multi-day microgrid clusters and computational speed, making it an ideal optimization approach.

To further contextualize our approach against model-based methods, we compared it with a Nonlinear Optimal Control (NOC) strategy designed for a simplified microgrid model. While the NOC method achieved stable operation, its performance was highly dependent on the accuracy of the underlying physical model. In contrast, our data-driven FL method demonstrated superior adaptability to the complex, uncertain renewable generation and load profiles, resulting in a 12.5% lower total operational cost compared to NOC. This highlights the advantage of learning-based methods in environments where precise system modeling is challenging.

## 4.4 Privacy protection effectiveness

In the coordinated operation of microgrid clusters, the crux of privacy protection lies in minimizing the exchange of internal operational data. Table 3 presents the evaluation results of privacy protection performance for the interaction data under different methodologies.

Table 3: Privacy protection status under various methods

| Method | Privacy preservation |
|---|---|
| Independent | No involvement in privacy preservation |
| VDN | Transmit bid power, reward function, and Q-values |
| DQN | Transmit bid power |
| NG | Centralized solution required |
| FL | Transmit bid power, encrypt underlying network |

The evaluation of privacy protection performance across various methodologies reveals significant disparities: the independent operation approach entirely eschews privacy safeguards, as it lacks data interaction, yet it forfeits the benefits of collaborative operation. The VDN method necessitates the transmission of bid power, reward functions, and Q-values, with the exchange of substantial sensitive data rendering it highly susceptible to privacy breaches. The DQN method, by contrast, only transmits bid power, resulting in a relatively reduced data transfer volume and conferring a certain advantage in privacy protection; however, bid power may still divulge partial operational state information. The NG method relies on a centralized solution, posing an exceedingly high risk of privacy leakage. The FL method, while transmitting bid power, encrypts the underlying network, effectively mitigating privacy risks while ensuring essential data interaction, thereby excelling in privacy protection performance. The use of homomorphic encryption introduces approximately 13.3% additional communication overhead and 18.6% computation time compared to plaintext federated learning, which is acceptable given the privacy benefits.

To further highlight the advancement of the proposed federated learning method, a comparative analysis was conducted against two state-of-the-art microgrid management approaches: Consensus-based Distributed Optimization (CDO) and Personalized Federated Learning (PFL). The results demonstrate that while CDO achieves distributed optimization (reducing total operating costs by approximately 12% compared to independent operation), it requires frequent exchange of raw state information, incurring high privacy risks. PFL, though effective in improving local prediction accuracy, exhibits limited global optimization capability, with a total operating cost about 8% higher than our method. In contrast, the proposed approach achieves a further 15.1% reduction in total operating cost while ensuring superior privacy protection through encrypted model interactions during collaboration, underscoring its comprehensive advantages in both economic efficiency and security.

# 5 Discussion

The experimental results demonstrate the clear advantages of the proposed FL-based method over other approaches. The superior cost performance stems from the effective collaborative learning enabled by FL, which allows microgrids to benefit from the collective operational intelligence of the cluster without sharing raw data. In contrast, DQN and VDN, while data-driven, lack this collaborative mechanism and operate with more limited local perspectives. The non-cooperative game (NG) method leads to strategic bidding that often increases costs for individual participants (e.g., Microgrid 1), undermining global cost efficiency.

The difference in cost reduction across microgrids (e.g., Microgrid 1 benefiting more than Microgrid 3) can be attributed to their structural heterogeneity. Microgrid 1, with high renewable penetration and a gas turbine, has more flexible resources to optimize based on learned global strategies. Microgrid 3, heavily reliant on storage and the grid, has less intrinsic flexibility, thus its cost-saving potential is lower.

The computational speed of our method is moderate because the homomorphic encryption and secure aggregation introduce overhead. However, this is a justified trade-off for the achieved privacy level, which is unattainable by NG, DQN, or VDN. The robust prediction accuracy and generalization are largely due to the GRU's capability to capture temporal dependencies in energy data and the comprehensive data augmentation, which exposes the model to a wide range of operational scenarios.

In summary, from the perspective of privacy protection, the FL method, with its encryption mechanism, holds a pronounced advantage in safeguarding privacy, making it an ideal approach for the optimized operation of microgrid clusters and aligning more closely with the practical demands for data security and privacy. The principles of our FL-based collaborative optimization could be extended to other distributed nonlinear systems requiring privacy-aware coordination. For instance, in multi-robot systems, robots could collaboratively learn navigation strategies without sharing proprietary sensor data. In industrial compressor networks, units could optimize collective energy usage while protecting operational secrets [27,28]. The GRU's ability to model temporal dynamics and FL's privacy-preserving nature make this framework adaptable to various domains with sequential decision-making and data ownership concerns.

# 6 Conclusion

This study presents a method for collaborative optimization of microgrid clusters based on federated learning. Through case analysis, it demonstrates significant advantages in multiple aspects. In terms of prediction results, the deep learning model based on GRU has high accuracy and strong generalization ability in predicting operational costs, with the federated learning model's training RMSE converging and good consistency in decision-making. Regarding operational costs and computational speed, after comparing various methods, it was found that the federated learning method performs outstandingly, effectively reducing costs and being fast in computation. In terms of privacy protection, it reduces risks through specific data transmission and network encryption, outperforming other methods. This research provides an effective solution for the optimized operation of microgrid clusters, which is of great significance in energy utilization, cost control, and privacy protection. Beyond microgrids, the proposed framework shows promise for any distributed system requiring collaborative learning under privacy constraints, such as industrial automation networks, collaborative robotics, and federated healthcare analytics. In the future, it can be further expanded and applied, and explore integration with new technologies to adapt to the needs of energy development.

## References

[1] Zia M F, Benbouzid M, Elbouchikhi E, et al. Microgrid transactive energy: Review, architectures, distributed ledger technologies, and market analysis[J]. IEEE access, 2020, 8: 19410-19432. doi: 10.1109/ACCESS.2020.2968402

[2] Ahmad S, Shafiullah M, Ahmed C B, et al. A review of microgrid energy management and control strategies[J]. IEEE Access, 2023, 11: 21729-21757.doi: 10.1109/ACCESS.2023.3248511

[3] Han Y, Zhang K, Li H, et al. MAS-based distributed coordinated control and optimization in microgrid and microgrid clusters: A comprehensive overview[J]. IEEE Transactions on Power Electronics, 2017, 33(8): 6488-6508.doi: 10.1109/TPEL.2017.2761438

[4] Patari N, Venkataramanan V, Srivastava A, et al. Distributed optimization in distribution systems: Use cases, limitations, and research needs[J]. IEEE Transactions on Power Systems, 2021, 37(5): 3469-3481.doi: 10.1109/TPWRS.2021.3132348

[5] Zhang N, Sun Q, Wang J, et al. Distributed adaptive dual control via consensus algorithm in the energy internet[J]. IEEE Transactions on Industrial Informatics, 2020, 17(7): 4848-4860.doi: 10.1109/TII.2020.3031437

[6] Wang G, Chao Y, Cao Y, et al. A comprehensive review of research works based on evolutionary game theory for sustainable energy development[J]. Energy Reports, 2022, 8: 114-136.doi: 10.1016/j.egyr.2021.11.231

[7] Manshaei M H, Zhu Q, Alpcan T, et al. Game theory meets network security and privacy[J]. Acm Computing Surveys (Csur), 2013, 45(3): 1-39.doi: 10.1145/2480741.2480742

[8] Ahmad T, Zhu H, Zhang D, et al. Energetics Systems and artificial intelligence: Applications of industry 4.0[J]. Energy Reports, 2022, 8: 334-361.doi: 10.1016/j.egyr.2021.11.256

[9] Cao D, Hu W, Zhao J, et al. Reinforcement learning and its applications in modern power and energy systems: A review[J]. Journal of modern power systems and clean energy, 2020, 8(6): 1029-1042.doi: 10.35833/MPCE.2020.000552

[10] Zhou Q, Shahidehpour M, Paaso A, et al. Distributed control and communication strategies in networked microgrids[J]. IEEE Communications Surveys & Tutorials, 2020, 22(4): 2586-2633.doi: 10.1109/COMST.2020.3023963

[11] Su W, Shi Y. Distributed energy sharing algorithm for Micro Grid energy system based on cloud computing[J]. IET Smart Cities, 2024, 6(3): 225-236.doi: 10.1049/smc2.12049

[12] Shang Y, Li S. Security-Enhanced Spatiotemporal Ride-Hailing Demand Prediction—Part I: Horizontal Federated Learning[J]. IEEE Transactions on Intelligent Transportation Systems, 2025.doi: 10.1109/TIV.2024.3446319

[13] Xu J, Fu D, Shao L, et al. A soft sensor modeling of cement rotary kiln temperature field based on model-driven and data-driven methods[J]. IEEE Sensors Journal, 2021, 21(24): 27632-27639.doi: 10.1109/JSEN.2021.3116937

[14] Olivella-Rosell P, Rullan F, Lloret-Gallego P, et al. Centralised and distributed optimization for aggregated flexibility services provision[J]. IEEE Transactions on Smart Grid, 2020, 11(4): 3257-3269.doi: 10.1109/TSG.2019.2962269

[15] Jia Y, Wen P, Yan Y, et al. Joint operation and transaction mode of rural multi microgrid and distribution network[J]. IEEE Access, 2021, 9: 14409-14421.doi: 10.1109/ACCESS.2021.3050793

[16] Abdel-Raouf O, Elsisy M, Kelash E. A survey of game theory applications in electrical power micro-grid systems[J]. International Journal of Computer Applications, 2020, 177(37): 25-34.doi: 10.5120/ijca2020919871

[17] Boulkroune A, Zouari F, Boubellouta A. Adaptive fuzzy control for practical fixed-time synchronization of fractional-order chaotic systems[J]. Journal of Vibration and Control, 2025: 10775463251320258.doi: 10.1177/10775463251320258

[18] Zouari F, Saad K B, Benrejeb M. Adaptive backstepping control for a class of uncertain single input single output nonlinear systems[C]//10th International Multi-Conferences on Systems, Signals & Devices 2013 (SSD13). IEEE, 2013: 1-6.doi: 10.1109/SSD.2013.6564134

[19] Zouari F, Saad K B, Benrejeb M. Adaptive backstepping control for a single-link flexible robot manipulator driven DC motor[C]//2013 International Conference on Control, Decision and Information Technologies (CoDIT). IEEE, 2013: 864-871.doi: 10.1109/CoDIT.2013.6689656

[20] Yun X, Wu L, Xu Y, et al. Robust adaptive neural network optimal control for a class of uncertain nonlinear systems[C]//2016 Chinese Control and Decision Conference (CCDC). IEEE, 2016: 521-526. doi: 10.1109/CCDC.2016.7531040

[21] Shang Y, Li S. Security-Enhanced Spatiotemporal Ride-Hailing Demand Prediction—Part II: Horizontal Federated Learning[J]. IEEE Transactions on Intelligent Transportation Systems, 2025.doi:10.1109/TITS.2025.3564627

[22] Wu H, Xu Z. Multi-energy load forecasting in integrated energy systems: A spatial-temporal adaptive personalized federated learning approach[J]. IEEE Transactions on Industrial Informatics, 2024, 20(10): 12262-12274. doi: 10.1109/TII.2024.3417297

[23] He Y, Liu X T, Zhang C B, et al. A new model for State-of-Charge (SOC) estimation for high-power Li-ion batteries[J]. Applied energy, 2013, 101: 808-814.doi:10.1016/j.apenergy.2012.08.031

[24] Maschio C, Schiozer D J. Probabilistic history matching using discrete Latin Hypercube sampling and nonparametric density estimation[J]. Journal of Petroleum Science and Engineering, 2016, 147: 98-115.doi: 10.1016/j.petrol.2016.05.011

[25] Shewalkar A, Nyavanandi D, Ludwig S A.

Performance evaluation of deep neural networks applied to speech recognition: RNN, LSTM and GRU[J]. Journal of Artificial Intelligence and Soft Computing Research, 2019, 9(4): 235-245.doi: 10.2478/jaiscr-2019-0006

[26] Zheng P, Zhu Y, Hu Y, et al. Federated learning in heterogeneous networks with unreliable communication[J]. IEEE Transactions on Wireless Communications, 2023, 23(4): 3823-3838.doi: 10.1109/TWC.2023.3311824

[27] Boulkroune A, Hamel S, Zouari F, et al. Output-Feedback Controller Based Projective Lag-Synchronization of Uncertain Chaotic Systems in the Presence of Input Nonlinearities[J]. Mathematical Problems in Engineering, 2017, 2017(1): 8045803.doi: 10.1155/2017/8045803

[28] Rigatos G, Abbaszadeh M, Sari B, et al. Nonlinear optimal control for a gas compressor driven by an induction motor[J]. Results in Control and Optimization, 2023, 11:100226.doi: 10.1016/j.rico.2023.100226