Privacy-Preserving Regulation Capacity Evaluation for HVAC Systems in Heterogeneous Buildings Based on Federated Learning and Transfer Learning

Zhenyi Wang, *Graduate Student Member, IEEE*, Peipei Yu, *Graduate Student Member, IEEE*, and Hongcai Zhang, *Member, IEEE*

***Abstract*—Heating, ventilation, and air conditioning (HVAC) systems in buildings have great potential to provide regulation capacity that is leveraged to maintain the balance of supply and demand in the power system. In order to make full use of HVAC's regulation capacity, it is important to accurately evaluate it ahead of time. Because physical model-based approaches are hard to implement and highly personalized for each building, data-driven approaches are preferable for this capacity evaluation. However, given the insufficient data for individual buildings and buildings' potential unwillingness to share their data because of privacy concerns, it is extremely challenging to build a high-performance data-driven regulation capacity evaluation model. In this paper, we propose a privacy-preserving framework that combines federated learning and transfer learning to evaluate the regulation capacity of HVAC systems in heterogeneous buildings. Specifically, a classified federated learning algorithm is proposed to build capacity evaluation models of HVAC systems for different building types. Each building trains its model locally without sharing data with other buildings to preserve privacy. The algorithm also tackles data insufficiency and achieves high evaluation accuracy. In addition, we design a cross-type transfer learning algorithm to enhance model generalization and further address data deficiency. A protocol is created for the above two algorithms to protect privacy and security. Finally, numerical case studies are conducted to validate the proposed framework.**

***Index Terms*—Demand response, federated learning, HVAC system, privacy-preserving, regulation capacity, transfer learning.**

I. Introduction

With the increasingly high penetration of renewable energy sources (RES), the uncertainty of power system generation has greatly increased owing to the high unpredictability and volatility of RES [1]. Therefore, more flexible regulation capacities are needed to maintain the system supply–demand balance [2]. With the phasing out of conventional flexible generating units (e.g., thermal generators and gas turbines), demand response is gaining more attention for providing regulation capacity in power system operation and has already been adopted by leading countries worldwide [3].

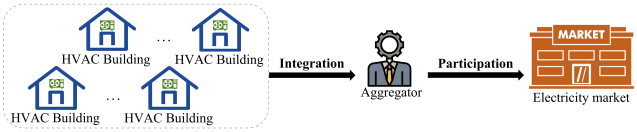


Fig. 1. Diagram of an aggregator coordinating multiple buildings.

Heating, ventilation, and air conditioning (HVAC) systems in buildings have great potential to furnish regulation capacity [4] because they account for a large share of total electricity consumption, (e.g., over 40% in many cities in the world) in addition to having the thermal inertia to keep comfort levels within acceptable limits during regulation [5]. In addition, the automation devices that are already present in the system can be utilized to reduce infrastructure costs and realize intelligent remote control. Furthermore, owing to the large number and wide distribution of HVAC systems, an aggregator is usually exploited to integrate and regulate the capacities of many buildings together, and participates in the electricity market as an agent representing all of the buildings [6], as shown in Fig. 1. In an electricity market, the aggregator usually needs to provide a regulation capacity offer in advance. Then, during real-time operations, if the aggregator fails to provide the regulation services as it promised, it may be penalized or even expelled from the market [7]. Hence, it is critical for the aggregator to accurately evaluate the regulation capacity of all HVAC systems in buildings ahead of time.

However, accurate regulation capacity evaluation can be challenging because precisely modeling HVAC systems is difficult. Fabietti et al. [8] proposed a model-predictive control (MPC) framework to determine the regulation capacity of commercial buildings and provide frequency regulation services for the Swiss electricity market. Pavlak et al. [9] combined the zone temperature setpoint perturbation method with MPC to evaluate the hourly regulation capacity of commercial buildings in the ancillary service market. Ali et al. [10] derived a building thermodynamic model and then proposed a mathematical formula to evaluate the capacity of its HVAC system. Further, Lu [11] applied a simplified equivalent thermal model

Manuscript received 17 June 2022; revised 9 October 2022 and 7 December 2022; accepted 19 December 2022. Date of publication 23 December 2022; date of current version 23 August 2023. This work was supported in part by the Science and Technology Development Fund, Macau, SAR, under Grant SKL-IOTSC(UM)-2021-2023 and Grant 0011/2021/AGJ, and in part by the Guangdong–Hong Kong–Macau Joint Laboratory for Smart Cities under Grant EF008/IOTSC-YKV/2021/GDSTC. Paper no. TSG-00864-2022. *(Corresponding author: Hongcai Zhang.)*

The authors are with the State Key Laboratory of Internet of Things for Smart City and Department of Electrical and Computer Engineering, University of Macau, Macau, China (e-mail: hczhang@um.edu.mo).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2022.3231592.

Digital Object Identifier 10.1109/TSG.2022.3231592

for simulating residential HVAC units. Goddard et al. [12] developed a single-state variable system model for HVAC systems to predict power consumption and evaluate regulation capacity. The above studies relied on precise physical models to determine the regulation capacity of HVAC systems in buildings. These models usually include a large number of parameters, some of which are often difficult or even impossible to estimate. In addition, the building indoor temperature is influenced by various factors, including heat transfers across buildings and heat gains from the environment, which are computationally expensive to model. Thus, it is difficult to apply physical-model-based methods for regulation capacity evaluation of HVAC systems in heterogeneous buildings.

To overcome the aforementioned challenges, recently, researchers have widely used data-driven model-free methods. As such, some researchers have proposed supervised learning approaches. For example, Javed et al. [13] presented a random neural-network-based smart controller to estimate room heat consumption and then control the HVAC system. Kim [14] utilized artificial neural networks for HVAC system modeling in a multi-zone building and then used it to ensure thermal comfort and cost-effective operation. Some other researchers have adopted reinforcement learning (DRL) algorithms. For example, Yu et al. [15] and Li et al. [16] adopted DRL to tackle uncertainties of HVAC system operations and electricity prices, respectively. Yu et al. [17] extended single-agent DRL to multi-agent DRL with an attention mechanism, enabling unified control of multiple HVAC systems. These data-driven approaches require sufficient high-quality historic data for training. However, this can be challenging in practice, especially for new buildings or those without proper metering systems.

To resolve the problem of some buildings not having sufficient data for data-driven regulation capacity evaluation, two possible approaches can be used: 1) sharing the data across different buildings to train a high-performance global model that can be used for all buildings; 2) applying well-trained models from buildings with sufficient data to those without sufficient data. For the first approach, it is common practice to use a central entity to collect data from all buildings and carry out training processes. However, buildings may be unwilling to share their data owing to privacy concerns. To protect privacy, researchers have proposed federated learning, which allows users to collaboratively train a global model without sharing data, only exchanging gradients or model parameters [18]. Several studies have exploited federated learning in power systems for electricity consumer characteristics identification [19], solar generation disaggregation [20], and distributed energy resources forecasting [21]. For the second approach, transfer learning [22] is usually adopted, which transplants knowledge learned from one domain to another domain based on similarities in data, tasks, or models between domains. Therefore, it is possible to obtain a high-performance model with little or even no data in some buildings by exploiting the well-trained model from other buildings. There has been some research utilizing transfer learning in power systems, such as nonintrusive load monitoring, wind power prediction, and power system security assessment [23], [24], [25], [26].

However, the above two approaches can not address our problem well individually. First, owing to the FedAvg algorithm of federated learning, the global model may not reflect the differences between HVAC systems in heterogeneous buildings, which may lead to performance degradation [18], [27]. Second, the prerequisite for transfer learning to be able to transfer knowledge is to have well-trained models from other buildings. However, developing a well-trained model may already face data deficiency and privacy issues.

To fill the aforementioned research gap, we propose a privacy-preserving deep learning framework that combines federated learning and transfer learning to train a data-driven model for regulation capacity evaluation of HVAC systems in heterogeneous buildings. Compared with the published literature, the main contributions of this paper are threefold:

1) A classified federated learning algorithm is designed to build high-performance evaluation models for HVAC system regulation capacity by leveraging data from multiple buildings. According to the designed identification scheme, each model is only trained by data from one type of buildings. Compared with traditional federated learning methods to obtain a global model of all buildings, each type of buildings receive a personalized model through the proposed algorithm. The personalized model avoids performance degradation due to model overgeneralization, which is caused by the use of data from excessively heterogeneous buildings.
2) A cross-type transfer learning algorithm is developed to further improve the performance of models that are trained by the classified federated learning algorithm. For building types that all buildings have the issue of insufficient data, this algorithm enhances their model accuracy by transplanting knowledge from the well-trained models of other building types. Further, it also makes up for inadequate model generalization, allowing the model to be applied to other buildings.
3) A novel protocol is created for the above two algorithms to protect the privacy of building data and model parameters during the training processes. It also contains a secure transmission scheme that can guarantee communication security and provide identity authentication. Further, each building processes data locally, which effectively preserves the privacy of the building's data.

The rest of this paper is organized as follows. In Section II, the problem background, threat model, and design goals in this work are introduced. The proposed method and technical details are elaborated on in Section IV. In Section V, the effectiveness of the proposed method is validated by numerical experiments. Finally, Section VI concludes this paper.

II. Problem Statement

In this section, we introduce the problem of regulation capacity evaluation, the security and privacy threat model, and the design goals in this paper.

A. Regulation Capacity Evaluation

We consider an aggregator coordinating a group of heterogeneous buildings in this paper. Each building evaluates its regulation capacity in advance, and then the aggregator aggregates these regulation capacities and represents buildings when bidding in the regulation market. We assume that buildings have some historical data on power load profiles and regulation capacities. Suppose that the regulation capacity at time t is y_t, and because the bid needs to be made in advance, we denote the feature vector used to evaluate y_t as $\boldsymbol{x}_{t-n}$ (we set $n = 1$ in this paper for the 1-hour-ahead evaluation). Therefore, we utilize a data-driven model to evaluate the regulation capacity of HVAC systems in buildings via regression:

$$y_t = f(\boldsymbol{x}_{t-n}; \theta), \tag{1}$$

where $f(\cdot; \theta)$ is the evaluation model with parameters θ.

However, accurately evaluating buildings' regulation capacities ahead of time is challenging. On the one hand, some buildings may not have sufficient historical data owing to the low quality of data collection, and the data requirements of the model also increase as the problem becomes more complex and difficult. Therefore, it is difficult to accurately evaluate the regulation capacity through an individual building's data, according to Eq. (1). This insufficient data problem may be tackled by collecting multiple buildings' data for joint model training. However, on the other hand, different buildings belong to different entities, so they may be unwilling to share their data with the aggregator or each other because it may lead to the disclosure of their privacy.

B. Threat Model

The security and privacy threats considered in this paper may come from both the internal system and the external world, primarily against building data and model parameters.

1) Threats From the Internal System: Within the system, we assume that the cloud server (i.e., the aggregator in this paper) is a semi-honest party that performs the given tasks honestly but is curious about building data and model parameters. In addition, it is assumed that all buildings are also honest but curious; that is, they complete their work as specified but also attempt to access data from other buildings. This may be because most buildings do not have sufficient data to train a high-performance model of their own.

2) Threats From the External World: For threats from outside, we take malicious eavesdroppers into consideration as the primary attackers, who may intercept the communication channels to access the model parameters or even make reverse inference about the building data.

C. Design Goals

Based on the aforementioned background and threat model, the proposed framework should have the following objectives.

1) Accuracy: The devised framework should be able to build a data-driven model that can accurately evaluate the capacities of the HVAC systems in heterogeneous buildings. The framework also needs to overcome the limited data of buildings, which leads to low model accuracy.

2) Generalization: Considering that heterogeneous buildings are involved in training processes, the model needs to have adequate generalization. This means that the model can accurately evaluate regulation capacity for all buildings involved in its training processes and even new ones (whose data are not available). However, the excessive pursuit of generalization may lead to a decrease in model accuracy. The proposed framework should properly balance model accuracy and generalization.

3) Privacy: The proposed framework needs to meet privacy requirements, which means that its data cannot be compromised and model parameters cannot be accessed without permission. If privacy issues are not safeguarded, buildings may be reluctant to participate in the collaborative training processes, and the capacity evaluation model may not be built correctly.

III. Preliminaries

In this section, we briefly introduce some preliminaries about the federated learning and transfer learning algorithm.

A. Federated Learning

The federated learning algorithm aims to build a machine learning model, which collaboratively trains the model by different participants. Each participant utilize some data to train a local model, and the data are stored and processed locally during the training process. The collaborative training exchanges model-related information (parameters or gradients of the local model) rather than raw data, so the data privacy is protected. The goal of the federated learning algorithm can typically be expressed as minimizing the following objective function [18].

$$\min_{\omega} F(\omega), \text{ where } F(\omega) \coloneqq \sum_{k=1}^{K} p_k \cdot F_k(\omega), \tag{2}$$

where K is the total number of participants; p_k is the weight of the k-th participant, $p_k \geq 0$ and $\sum_k p_k = 1$; F_k is the local objective function of the k-th participant.

In addition, to ensure that model-related information is not compromised through Eq. (2), the information is encrypted by the encryption algorithm, and then transmitted and exchanged between participants. The model built by the federated learning algorithm should be able to closely approximate the performance of the ideal model, which is a machine learning model directly trained by gathering all data.

B. Transfer Learning

Transfer learning can take advantage of the similarity between data, tasks, or models to improve the model performance in a new domain (termed the target domain) based on the knowledge learned from an old domain (termed the source domain). Specifically, the model learned in the source domain is transplanted to the target domain to help accomplish the corresponding task [28]. Before giving the formal definition of transfer learning, we define the domain and the task. A domain $\mathcal{D}$ consists of two parts: a feature space $\mathcal{X}$

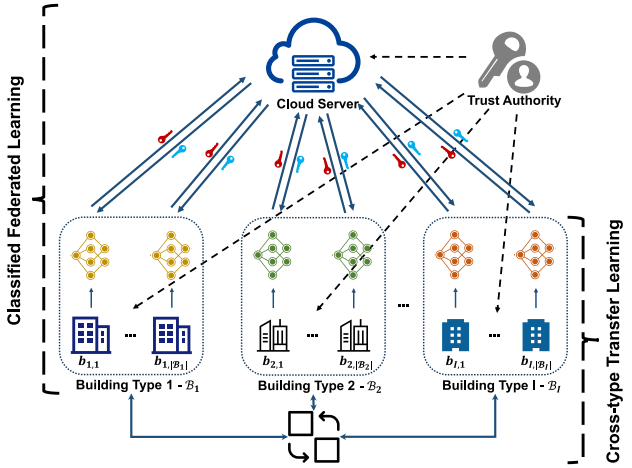


Fig. 2. The privacy-preserving framework with federated learning and transfer learning.

and a marginal distribution $P(X)$ of a possible feature vector X; thus, $\mathcal{D} = \{\mathcal{X}, P(X)\}$. The symbol $\mathcal{X}$ is the space of all feature vectors, and the symbol X denotes an instance set of feature space, where $X = \{\boldsymbol{x}|\boldsymbol{x}_i \in \mathcal{X}, i = 1, \ldots, n\}$. For a given domain $\mathcal{D}$, a task $\mathcal{T}$ is defined by two parts: a label space $\mathcal{Y}$ and a decision function f (i.e., $y = f(x)$); thus, $\mathcal{T} = \{\mathcal{Y}, f\}$. The symbol $\mathcal{Y}$ is the set of all labels, and the symbol f is learned from the feature vector and label pairs $\{(\boldsymbol{x}_i, y_i)|\boldsymbol{x}_i \in \mathcal{X}, y_i \in \mathcal{Y}, i = 1, \ldots, n\}$.

Given a source domain $\mathcal{D}_s$ with a corresponding source task $\mathcal{T}_s$ and a target domain $\mathcal{D}_t$ with a corresponding target task $\mathcal{T}_t$, the transfer learning algorithm utilizes the knowledge from $\mathcal{D}_s$ and $\mathcal{T}_s$ to improve the performance of the target decision function f_t, where $\mathcal{D}_s \neq \mathcal{D}_t$ or $\mathcal{T}_s \neq \mathcal{T}_t$. As such, the transfer learning algorithm learns f_t using the source domain data, so the decision loss of f_t in the target domain is the smallest, as follows:

$$f_t^* = \arg\min_{f_t} \mathbb{E}_{\boldsymbol{x}\in\mathcal{X}_s, y\in\mathcal{Y}_s} \mathcal{L}(f_t(\boldsymbol{x}), y), \tag{3}$$

where f_t^* is the optimal target decision function, and $\mathcal{L}$ is the loss function, which measures the decision discrepancy.

IV. Proposed Methodology

In this section, we expound on our proposed framework that combines federated learning and transfer learning. In the following sections, $\mathcal{B} = \{\mathcal{B}_i|i \in \mathcal{I} = \{1, 2, \ldots, I\}\}$ denotes the set of buildings, where $\mathcal{B}_i$ is the set of building of type i. Symbol $b_{i,j} \in \mathcal{B}$ denotes an arbitrary building, where i indicates its building type, and $j \in \mathcal{J}_i = \{1, 2, \ldots, |\mathcal{B}_i|\}$ is the index of this building in its type. Symbol $\mathcal{K}_i \subseteq \mathcal{J}_i$ denotes the set of buildings that participate in collaboration.

A. Framework Overview

The framework in this paper roughly consists of one classified federated learning algorithm and one cross-type transfer learning algorithm, and it can preserve privacy and security, as shown in Fig. 2. When the data of a certain building are insufficient or missing, the evaluation model can be trained using data information from other buildings of the same type via the classified federated learning algorithm. Moreover, if there are no similar buildings of the same type or all buildings in a type do not have sufficient data, the cross-type transfer learning improves the performance of the model, by leveraging models of other types of buildings whose data are sufficient. In this paper, a model is considered as a high-performance one if: 1) it has high accuracy that not only the discrepancy between the evaluated value and the real value is small, but also all the evaluated values are relatively stable; that is, all of them are close to the corresponding real values; and 2) it has high generalization, which means it can make an accurate evaluation for unknown samples that are not involved in training or even from new buildings.

There are mainly three types of entities in the framework: the trust authority, the cloud server, and the buildings.

1) Cloud Server: The cloud server undertakes the initialization, aggregation, and distribution of model parameters. By aggregating the local model parameters from each building, the cloud server eventually obtains a comprehensive model, which is then sent back to the buildings. Note that the cloud server does not have data to train the model.

2) Buildings: Each building has an HVAC system and may have some historical data to exploit. Thus, the building is in charge of training a local regulation capacity evaluation model through its data and updating parameters of the local model by interacting with the cloud server. Furthermore, with the coordination of the cloud server, the models of the same type of buildings are identical after aggregation.

3) Trust Authority: The trust authority is responsible for the initialization of the secure privacy-preserving protocol, which generates the public key and private key for the Paillier cryptosystem and establishes secure communication channels between each building and the cloud server. In addition, it also distributes the tag, which is used to identify the building type, to others. Furthermore, the trust authority is assumed to be a fully trusted third party, which does not pose any threat to the framework.

B. Classified Federated Learning Algorithm

The classified federated learning algorithm connects multiple buildings to collaboratively train high-performance regulation capacity evaluation models. Unlike traditional federated learning, the proposed algorithm train a personalized model for each building type. We classify buildings according to their usage types, such as office, hotel, and other commercial buildings. HVAC systems in different types of buildings usually have different regulation characteristics considering that they have different building structures, daily social activities, and load patterns. The whole process of the algorithm has five stages (see Algorithm 1).

1) System Initialization: In the first stage, the trust authority establishes secure communication channels between each building and server and produces the public key $\mathcal{PK}$ and private key $\mathcal{SK}$ for privacy-preserving federated learning according to the Paillier cryptosystem (see details in Section IV-D1). Then, the cloud server initializes regulation capacity model

Algorithm 1: Classified Federated Learning With Privacy-Preserving

Input : Participating building index set $\{\mathcal{K}_i | i \in \mathcal{I}\}$, data resources for all participating buildings $\{D_{i,j} | j \in \mathcal{K}_i\}$.
Output : The capacity evaluation model.
Initialization:
Generate the key pair $\{\mathcal{PK}, \mathcal{SK}\} = KeyGenerate()$; Initialize the model parameters $\omega^{(0)}$ and other parameters $LB, LE, \mathcal{L}, \eta, \Psi$; Determine the communication round R^c; Report the data size $|D_{i,j}|$ to the cloud server; Calculate contribution weight $\alpha_{i,j}$ for each building, where $\alpha_{i,j} = |D_{i,j}| / \sum_{j \in \mathcal{K}_i} |D_{i,j}|$.
Procedure:
for $i \in \mathcal{I}, j \in \mathcal{K}_i$ **do**
  Set $\omega_{i,j}^{(0)} = \omega^{(0)}$ and other parameters with $LB, LE, \mathcal{L}, \eta, \Psi$;
end
Set $r = 0$;
while $r < R^c$ **do**
  For Buildings:
  for $i \in \mathcal{I}, j \in \mathcal{K}_i$ **do**
    Perform local training with local data $D_{i,j}$ as per Algorithm 2 and obtain updated parameters $(\omega_{i,j}^{(r)})'$;
    Encrypt $(\omega_{i,j}^{(r)})'$ and get encrypted parameters $c_{i,j}$ by Eq. (10), where $c_{i,j} = FedEncrypt((\omega_{i,j}^{(r)})')$;
    Upload $c_{i,j}$ to the cloud server;
  end
  For Cloud Server:
  Aggregate ciphertexts by type and obtain aggregated encryptred parameters $c_i = FedAggregate(c_{i,j})$, according to Eq. (11);
  Send c_i back to $b_{i,j}$;
  For Buildings:
  for $i \in \mathcal{I}, j \in \mathcal{K}_i$ **do**
    Decrypt c_i and get the aggregated model parameters $\omega_{i,j}^{(r+1)} = FedDecrypt(c_i)$, according to Eq. (12);
    Update the local model parameters by $\omega_{i,j}^{(r+1)}$;
  end
  $r \leftarrow r + 1$;
end

parameters $\omega^{(0)}$ and determines some other parameters related to model training, such as the local batch size LB, local training epoch LE, loss function $\mathcal{L}$, learning rate η, and optimizer Ψ. The above parameters are assigned to each building so that the local training settings are identical for each building and $\omega_{i,j}^{(0)} = \omega^{(0)}$. In addition, the communication round R^c is defined by the cloud server as the total number of interactions between buildings and the cloud server. Finally, the cloud server calculates the corresponding contribution weights $\alpha_{i,j}$ for each building based on the local training dataset $D_{i,j}$, where $\alpha_{i,j} = |D_{i,j}| / \sum_{j \in \mathcal{K}_i} |D_{i,j}|$.

2) Local Model Training: After receiving the initial model parameters $\omega^{(0)}$ and other parameters LB, LE, $\mathcal{L}$, η, Ψ from the cloud server, the building begins to train the regulation capacity evaluation model using its own data. For the r-th round, the building $b_{i,j}$ calculates the model gradient and updates its parameters $\omega_{i,j}^{(r)}$. After this round of local training, the model parameters are updated to $(\omega_{i,j}^{(r)})'$. The details of the local training are summarized in Algorithm 2.

Algorithm 2: Local Model Training

Input : Local model parameters $\omega_{i,j}^{(r)}$, local data $D_{i,j}$, local batch size LB, local epoch LE, optimizer Ψ.
Output : Local updated model parameter $(\omega_{i,j}^{(r)})'$.
Initialization:
Divide $D_{i,j}$ into batches by LB; Set $epoch = 1$;
Procedure:
while $epoch <= LE$ **do**
  for *each batch of data* **do**
    Compute loss $\mathcal{L}$ and gradient $\nabla_{\omega_{i,j}^{(r)}} \mathcal{L}$;
    Update the parameters using the Adam algorithm, according to Eqs. (4)–(8): $\omega_{i,j}^{(r)} \leftarrow \omega_{i,j}^{(r)} - \eta \Psi(\nabla_{\omega_{i,j}^{(r)}})$;
  end
  $epoch \leftarrow epoch + 1$;
end
$(\omega_{i,j}^{(r)})' \leftarrow \omega_{i,j}^{(r)}$;

We select the quadratic loss function to quantify the discrepancy between the real regulation capacity and the evaluated regulation capacity. Furthermore, we choose the Adam algorithm for model optimization [29], which uses momentum as the direction of the parameter update and also adaptively adjusts the learning rate, as follows:

$$u_t = \gamma_1 \cdot u_{t-1} + (1 - \gamma_1) \cdot \nabla_t, \tag{4}$$

$$v_t = \gamma_2 \cdot v_{t-1} + (1 - \gamma_2) \cdot \nabla_t \odot \nabla_t, \tag{5}$$

$$\hat{u}_t = \frac{u_t}{1 - \gamma_1^t}, \tag{6}$$

$$\hat{v}_t = \frac{v_t}{1 - \gamma_2^t}, \tag{7}$$

$$\omega_t = \omega_{t-1} - \frac{\eta}{\sqrt{\hat{v}_t} + \epsilon} \cdot \hat{u}_t, \tag{8}$$

where ∇_t denotes the gradient at iteration t; u_t and v_t are the first and second moment estimates of the gradient, respectively; γ_1 and γ_2 denote two exponential decay rates; $\odot$ is the element-wise multiplication; ω_t is the model parameters at iteration t; η denotes the learning rate; and ϵ is a small constant to maintain numerical stability.

3) Encryption and Transmission: After the local training and model parameters update, the building $b_{i,j}$ encrypts its model parameters $(\omega_{i,j}^{(r)})'$ based on the *FedEncrypt* function to generate the ciphertext $c_{i,j}$ (i.e., the encrypted model parameters). Then, $c_{i,j}$ is uploaded to the cloud server.

4) Classified Aggregation: The cloud server aggregates the received ciphertexts $c_{i,j}$ for each building type i based on the buildings' contribution weights $\alpha_{i,j}$ using the *FedAggregate* function. Then, the aggregated ciphertext c_i is delivered back to the corresponding buildings of type i.

5) Decryption and Update: The *FedDecrypt* function is applied to decrypt the aggregated ciphertext c_i to obtain the aggregated parameter $\omega_{i,j}^{(r+1)}$, which is equal for the same i. Then, building $b_{i,j}$ updates its local model parameters from $(\omega_{i,j}^{(r)})'$ to $\omega_{i,j}^{(r+1)}$, which also represents the completion of a round of communication.

The last four stages described above are repeated until all communication rounds have been completed. Eventually,

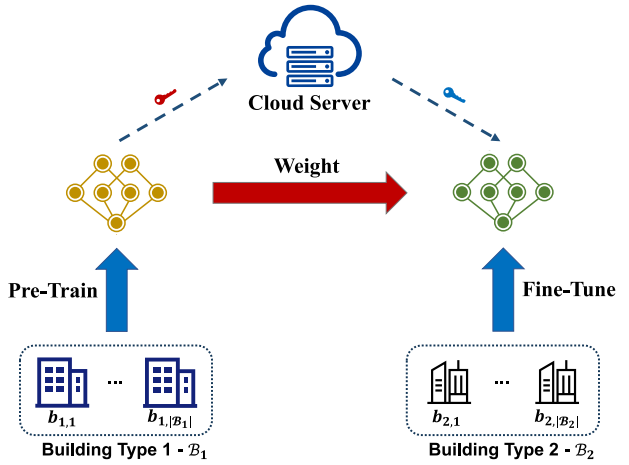


Fig. 3. Illustration of cross-type transfer learning algorithm.

buildings of the same type collaboratively train an identical model for regulation capacity evaluation. Although the buildings do not share data directly and sacrifice privacy, they can significantly enhance their model performance through this collaboration. Furthermore, as long as there are sufficient data in the same type of buildings, even a building with limited or no data can obtain a comparatively accurate evaluation model.

C. Cross-Type Transfer Learning Algorithm

When the overall data from the same type of buildings are not sufficient, the proposed federated learning model may still not achieve high performance. Thus, we propose the cross-type transfer learning algorithm. Unlike the classified federated learning algorithm that targets cooperation between buildings of the same type, this algorithm synergizes models between different building types. Specifically, according to Eq. (3), it utilizes models from building types with better performance to help relatively poor ones with insufficient data.

There are three main categories of transfer learning: the instance-weighting method, feature transformation method, and model pre-training method [28], [30], [31]. In our problem, each building only has its own data and no access to other buildings' data owing to security and privacy issues. The first two transfer learning approaches cannot be used because they need to acquire others' data. However, different types of buildings have the same data format and model target, and their only differences are building types and data scales. Hence, we employ the model pre-training method to transplant knowledge from one type to the other, which does not need to directly access any data from other buildings.

There are three entities involved in the algorithm: the source building (the building with a high-performance model), the target building (the building with a low-performance model), and the cloud server, which is shown in Fig. 3. The general process of the algorithm has five steps. First, the target building initiates a request for assistance from other types of buildings. Second, the source building encrypts and uploads its model parameters using the Paillier cryptosystem to the cloud server. After receiving the encrypted model parameters from the cloud server, the target building decrypts them and replaces them as local model parameters. Last, the target building fine-tunes the model parameters with its own data. Fine-tuning is done to adjust the model parameters of the source building and make them more suitable for the target building's task based on a small dataset of the target building. In order to make better use of the source building model and avoid overfitting, the optimal fine-tuned model parameters are:

$$\omega^* = \arg\min_{\omega} \frac{1}{|D^{\mathrm{T}}|} \sum_{t=1}^{|D^{\mathrm{T}}|} \mathcal{L}\Big(f\Big(x_t; \omega^{\mathrm{S}}\Big), y_t\Big) + \beta \frac{d}{\sqrt{|D^{\mathrm{T}}|}} ||\omega - \omega^{\mathrm{S}}||^2, \tag{9}$$

where D^{T} is the dataset of the target building; symbol ω^{S} denotes the model parameters of the source building; symbol $\mathcal{L}$ is the loss function of the model; symbol $f(x_t; \omega^{\mathrm{S}})$ and y_t are the evaluated and true value of the t-th training data of the target building, respectively; symbol β is a regularization factor to be tuned; and symbol $d = ||\overline{D^{\mathrm{T}}} - \overline{D^{\mathrm{S}}}||^2$ is the discrepancy measured by the Euclidean distance between the average data of the source building and the target building.

The fine-tuned model using Eq. (9) allows the target building to make a more accurate evaluation, which further improves the model performance. Further, the source building also enhances its model generalization by applying its model to other data through transfer learning.

D. Secure Privacy-Preserving Protocol

In this part, we design a secure privacy-preserving protocol for the proposed framework to guarantee the privacy of data and the security of the communication processes. The Paillier cryptosystem [32] is utilized in our protocol to ensure privacy-preserving of the classified federated learning algorithm in Section IV-B and the cross-type transfer learning algorithm in Section IV-C. To effectively mitigate the malicious eavesdroppers or other attackers, we exploit the advanced encryption standard (AES) algorithm [33] to establish secure communication channels between each building and the cloud server. Moreover, the MD5 message-digest algorithm [34] is used to implement authentication and tamper resistance when transmitting messages through secure communication channels. In addition, tags indicating building types not only play a key role in the classified federated learning algorithm but also assist in identity authentication. The protocol consists of four functions and one scheme, introduced as follows.

1) KeyGenerate(): The trust authority generates the public key $\mathcal{PK} = (n, g)$ and private key $\mathcal{SK} = (\lambda, \mu)$ according to the standard Paillier cryptosystem. Then, the public key $\mathcal{PK}$ is made public, as is the private key $\mathcal{SK}$ distributed to all buildings. The key generation process is divided into the following three steps. First, select two random large prime numbers p and q that satisfy $gcd(pq, (p-1)(q-1)) = 1$, where gcd is the greatest common divisor. Second, calculate $n = pq$ and $\lambda = lcm(p-1, q-1)$, where lcm is the least common multiple. Then, select a random base number $g \in \mathcal{Z}^*_{n^2}$ as the generator, and let $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$. The g can be found

efficiently by checking whether $gcd((L(g^{\lambda} \bmod n^2)), n) = 1$, where $L(x) = \frac{x-1}{n}$.

2) FedEncrypt(): Given a message $m_{i,j}$, which represents the model parameters of $b_{i,j}$, that is, $\omega_{i,j}^{(r)}$ in the corresponding round r, select a random number $z \in \mathcal{Z}_n^*$, $0 < z < n$. Then, encrypt the model parameters using the public key $\mathcal{PK}$ and obtain the corresponding ciphertext $c_{i,j}$ by

$$c_{i,j} = g^{m_{i,j}} \cdot z^n \bmod n^2. \tag{10}$$

3) FedAggregate(): With the uploaded ciphertexts $\{c_{i,j} \mid j \in \mathcal{K}_i\}$, the cloud server aggregates them according to the corresponding contribution weights $\{\alpha_{i,j}\}$. Then, the cloud server calculates the aggregated encrypted model parameters c_i by

$$\begin{aligned} c_i &= \prod_{j \in \mathcal{K}_i} \left(c_{i,j}\right)^{\alpha_{i,j}} \\ &= \prod_{j \in \mathcal{K}_i} \left(g^{\alpha_{i,j} m_{i,j}} \cdot z^{\alpha_{i,j} n}\right) \bmod n^2 \\ &= g^{\sum_{j \in \mathcal{K}_i} \alpha_{i,j} m_{i,j}} \cdot \prod_{j \in \mathcal{K}_i} z^{\alpha_i n} \bmod n^2. \end{aligned} \tag{11}$$

4) FedDecrypt(): After receiving the aggregated ciphertext c_i back from the cloud server, building $b_{i,j}$ decrypts it with the private key $\mathcal{SK}$ and obtains the aggregated parameters m_i through the following equation:

$$\begin{aligned} m_i &= L\left(c_i^{\lambda} \bmod n^2\right) \cdot \mu \bmod n \\ &= \frac{L\left(g^{\lambda \sum_{j \in \mathcal{K}_i} \alpha_{i,j} m_{i,j}} \cdot \prod_{j \in \mathcal{K}_i} z^{\lambda \alpha_i n} \bmod n^2\right)}{L\left(g^{\lambda} \bmod n^2\right)} \bmod n \\ &= \frac{L\left(g^{\lambda \sum_{j \in \mathcal{K}_i} \alpha_{i,j} m_{i,j}} \bmod n^2\right)}{L\left(g^{\lambda} \bmod n^2\right)} \bmod n \\ &= \frac{\lambda \cdot \sum_{j \in \mathcal{K}_i} \alpha_{i,j} \cdot m_{i,j}}{\lambda} \bmod n \\ &= \sum_{j \in \mathcal{K}_i} \alpha_{i,j} \cdot m_{i,j} \bmod n. \end{aligned} \tag{12}$$

5) Secure Transmission Scheme: The trust authority sets up secure communication channels between each building and the cloud server, and assigns the symmetric key $s_{i,j}$ to both sides of the channel. Thus, each building only has a key for its own channel, while the cloud server has keys for all channels. Further, the trust authority also distributes a tag to each building, which indicates its building type. In other words, buildings of the same type have identical tags. Note that the cloud server also receives tags for all buildings, but they have been processed into hash values by the MD5 algorithm. Thus, although the cloud server does not know the exact value of the tag, it can still use the hash value to determine the sender of the message and whether the message has been tampered with. The details of the protocol are shown below, and also illustrated in Fig. 4:

(i) The building calculates the hash of its tag and splices it in front of the ciphertext to form the valid information.
(ii) The building exploits the MD5 algorithm to generate a digital fingerprint corresponding to its valid information and splices it before the valid information to form the complete information.
(iii) The building encrypts the complete information using its symmetric key based on the AES algorithm, and then uploads it to the cloud server through its communication channel.
(iv) The cloud server decrypts the received content with the symmetric key that is selected according to the channel.
(v) The cloud server generates a new digital fingerprint of the received valid information and compares it with the received digital fingerprint. If the two fingerprints are the same, it justifies the valid information has not been tampered with.
(vi) The cloud server verifies the received tag; afterward, the comparison of the digital fingerprint is passed. If the tag verification succeeds, it means that the ciphertext is sent from the building corresponding to the channel. Conversely, the ciphertext is from another building or malicious attackers.

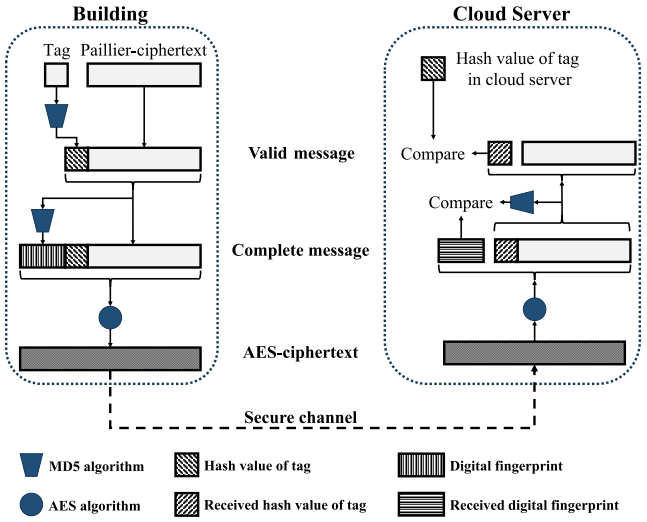


Fig. 4. Illustration of secure transmission scheme.

The Paillier cryptosystem is used to protect the privacy of the proposed framework, enabling the server to aggregate the building's encrypted information without decryption. As the Paillier cryptosystem is based on the decisional composite residuosity assumption and cannot be cracked by the server [32], the data privacy is protected (see the proof in Appendix A). Moreover, the security of the proposed framework is guaranteed by the AES. Because AES cannot be cracked within a limited time [35], the training-related information cannot be obtained by third parties other than buildings and the server (see the proof in Appendix B).

V. Case Studies

A. Experiment Settings

1) Dataset Description: The numerical experiments are conducted on a dataset of HVAC systems in heterogeneous buildings. Owing to the lack of historical regulation capacity data, we adopt a reinforcement-learning-based simulation method to collect and form a dataset [36], which is public on

Github.[1] The simulation is based on real HVAC systems and buildings in Zhuhai, Guangdong, China (including commercial buildings, office buildings, and hotels), and the weather data are from the Meteorological Bureau of Zhuhai (see simulation details in Appendix B). Each piece of data consists of 12 input features (including physical attributes, operational status, and environmental information) and one output (i.e., regulation capacity), with 1-hour granularity. Because the construction time and data collection time of buildings may be not identical, the range of data varies from building to building, where the longest span is 3 years, from November 2018 to October 2021.

In this paper, data insufficiency is caused by an inadequate data range (e.g., some historical data are not collected), especially under extreme weather conditions, when accurate regulation capacity evaluation is more challenging. Thus, we define a building with sufficient data, in that its data cover the majority of historical extreme weather, while a building with insufficient data has only historical data under a few or even no extreme weather events.

2) Performance Metrics: The following metrics are selected to measure the performance of the proposed model:

- Mean Absolute Error (MAE), $MAE = \frac{1}{T}\sum_{t=1}^{T}|y_t - \hat{y}_t|$, where y_t is the prediction, $\hat{y}_t$ is the true value, and T is the total number of test data.
- Root Mean Square Error (RMSE), $RMSE = \sqrt{\frac{1}{T}\sum_{t=1}^{T}(y_t - \hat{y}_t)^2}$.
- Median Absolute Error (MedAE), $MedAE = median(|\boldsymbol{Y} - \hat{\boldsymbol{Y}}|)$, where $\boldsymbol{Y} = (y_1, \ldots, y_T)$, $\hat{\boldsymbol{Y}} = (\hat{y}_1, \ldots, \hat{y}_T)$, and function $median(\boldsymbol{X})$ takes the median of all values in $\boldsymbol{X}$.
- Coefficient of Determination (R^2), $R^2 = 1 - \frac{\sum_{t=1}^{T}(y_t - \hat{y}_t)^2}{\sum_{t=1}^{T}(y_t - \frac{1}{T}\sum_{t=1}^{T} y_i)^2}$.

The former three metrics describe the gaps between the predicted and true values in $[0, +\infty)$. The last one indicates how well the predictions approximate the real data in $[0, 1]$. If the predictions perfectly fit the data, $R^2 = 1$.

3) Scenarios and Benchmarks: To demonstrate the effectiveness of the proposed method, we consider three different scenarios.

- Scenario I: There is a building with insufficient data, while some other buildings of the same type have sufficient data.
- Scenario II: There is a new building with no historical data, while some buildings of the same type with or without sufficient data are similar to this new building.
- Scenario III: There is a building type of which all buildings have insufficient data, while some buildings in other types have sufficient data.

Because the problem of insufficient data is mainly manifested as little or no building data, we believe that these three typical scenarios can represent most occurrences of data insufficiency. Scenarios I and II verify the classified federated learning algorithm, while Scenario III demonstrates the effectiveness of the cross-type transfer learning algorithm.

[1] https://github.com/KunWang-22/regulation-capacity-data

TABLE I
IMPLEMENTATION DETAILS OF CASE STUDIES

Parameter	Definition	Value
layer 1	the first layer of model	12 - 64[1]
layer 2	the second layer of model	64 - 128
layer 3	the third layer of model	128 - 64
layer 4	the fourth layer of model	64 - 16
layer 5	the fifth layer of model	16 - 1
E	the number of epochs	100
B	the batch size	32
$\mathcal{L}$	the loss function	MSE
optimizer	the optimization algorithm	Adam
η	the learning rate of optimizer	0.001
(γ_1, γ_2)	the exponential decay rate pair	(0.9, 0.999)

[1] **Each entry of layer refers "input size - output size".**

4) Environmental Setup: The proposed framework is implemented by an open-source machine learning framework PyTorch [37], and the communication processes are simulated using flask.[2] The details of model structures and training parameters are summarized in Table I. All of the experiments are conducted on a desktop with Intel Core i7-9700 CPU and NVIDIA GeForce RTX 2080TI GPU (64GB RAM) on a Windows 10 Enterprise platform.

B. Performance of Capacity Evaluation Model

In this part, we validate the performance of our proposed framework in the aforementioned three scenarios. For the comprehensive validation, in every scenario, we construct 50 cases of insufficient data for each type of building (i.e., commercial building, office building, and hotel), where each type of case involves different buildings and different days. The following five benchmarks are selected for comparison with our proposed method, all of which use MLPs as the evaluation model, as in the proposed method.

- Benchmark A: The model for the objective building in Scenario I is trained based on its own insufficient data.
- Benchmark B: The model for the objective building in Scenario II is trained by a similar building with insufficient data.
- Benchmark C: The model for the objective building in Scenario II is trained by a similar building with sufficient data.
- Benchmark D: The model for the objective building in Scenario III is trained by the federated learning algorithm using all the data from all of the buildings of the same type.
- Benchmark E: The model for the objective building in Scenario III is trained by the federated learning algorithm using all the data from all of the buildings of the same type and other types with sufficient data.

We compare the evaluation performance of the proposed method on 450 problem instances in each scenario with benchmarks, and the statistical results are summarized in Table II. It can be seen that the proposed method outperforms the corresponding benchmarks on all of the evaluation metrics

[2] Flask:Web development framework (https://flask.palletsprojects.com).

TABLE II
PERFORMANCE OF OVERALL SITUATION

Scenario	Method	MAE (kW)	RMSE (kW)	MedAE (kW)	R^2
Scenario I	Benchmark A	483.519 (45.157)	583.648 (35.254)	420.682 (33.823)	0.0011 (0.0003)
	Proposed	**135.865 (9.518)**	**178.065 (10.228)**	**93.448 (7.904)**	**0.725 (0.022)**
Scenario II	Benchmark B	306.119 (13.312)	427.211 (22.139)	173.740 (16.622)	0.0012 (0.0003)
	Benchmark C	158.806 (9.566)	208.656 (11.365)	153.563 (9.209)	0.796 (0.056)
	Proposed	**81.184 (7.568)**	**95.068 (6.625)**	**77.872 (4.835)**	**0.958 (0.013)**
Scenario III	Benchmark D	264.111 (17.606)	357.828 (15.942)	177.295 (17.705)	0.739 (0.048)
	Benchmark E	255.101 (17.508)	350.520 (15.021)	172.244 (13.529)	0.741 (0.049)
	Proposed	**103.094 (5.417)**	**155.03 (9.651)**	**61.333 (3.876)**	**0.941 (0.016)**

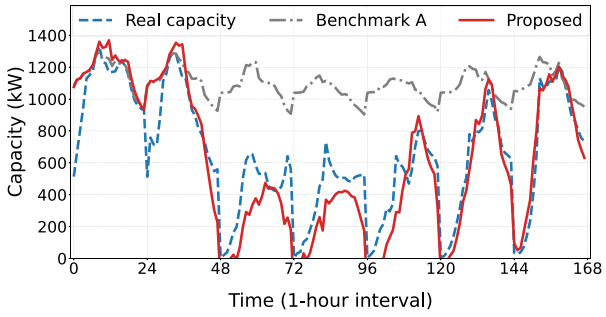
***Each entry gives a pair of AVG. (STD.).**

regardless of the scenario. From the perspective of evaluation error, the average MAE, RMSE, and MedAE of the proposed method are at least roughly halved compared to the benchmarks, with a maximum reduction of more than 400 kW. Moreover, the standard deviations of error metrics in the proposed method are mostly controlled within 10, while those in the benchmarks are distributed between 10 and 450. Therefore, the proposed method not only has accurate evaluation results, but also the evaluation performance is stable, which indicates that it can effectively solve the problem of insufficient data. As for the R^2 value, the standard deviation of the proposed method is also lower than that of the benchmarks, except for benchmarks A and B, because their R^2 values are small and close to zero. In scenarios B and C, the average R^2 values of the proposed method also exceed 0.9, which indicates that the proposed method can effectively fit the regulation capacity of HVAC systems in buildings and make an accurate evaluation.

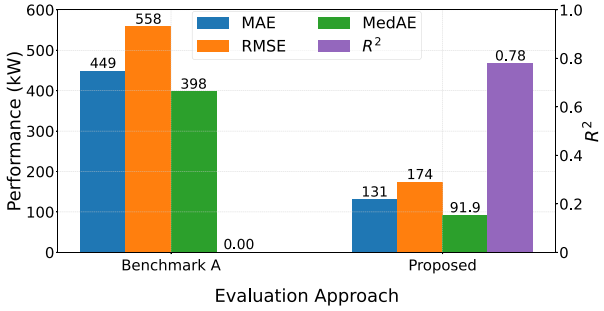
To demonstrate the evaluation details, we randomly select one instance from each scenario for a more intuitive and clear comparison, as follows.

1) Scenario I - Insufficient Data for One Building: In this scenario, we validate the performance of the proposed model when a building has insufficient data. Fig. 5 shows the evaluation results and performance of 1 week in scenario I utilizing benchmark A and the proposed model, respectively.

It is clear that benchmark A has poor evaluation accuracy, with a maximum error up to 1000 kW (see Fig. 5(a)). This is because this building does not have sufficient data to confront the sudden drop in regulation capacity under extreme weather conditions, and its data does not cover the majority of historical extreme weather, while that of other buildings do. In contrast, our proposed method can identify extreme weather conditions and significantly improve the evaluation performance. This results in a reduction of the maximum error rate by nearly 60%. The problem of insufficient data is addressed by data from other buildings of the same type. In Fig. 5(b), for the model developed by our proposed method, the MAE, RMSE, and MedAE metrics decrease from 472.37, 577.44, and 423.58 to 103.04, 141.33, and 77.82, respectively, which indicates a distinct improvement in model performance. In addition, the value of R^2 increases from 0.01 to 0.85, implying a boost in evaluation performance due to the classified federated learning algorithm.



(a)



(b)

Fig. 5. Evaluation result and performance metric of capacity evaluation models under scenario I.

2) Scenario II - No Data for One Building: In this scenario, we target the building without any data, which cannot train the model at all. Likewise, the proposed method tackles this kind of data deficiency using data from other same-type buildings. The evaluation results and the performance metrics of benchmark B, Benchmark C, and the proposed method in scenario II are shown in Fig. 6.

Although benchmark B trains the target model based on the data of a similar building, it still has large regulation capacity evaluation errors; for example, benchmark B's RMSE reaches up to 438.12. This is because the data of the similar building it used are insufficient. In comparison, benchmark C trains the target model based on a similar building with sufficient data. Its evaluation accuracy is significantly enhanced; for example, its RMSE is reduced to 212.48. This performance difference is more notable under extreme weather conditions that are learned by benchmark C but not benchmark B. However, because benchmark C only utilizes one building's data, its model still has significant errors. In contrast, the proposed

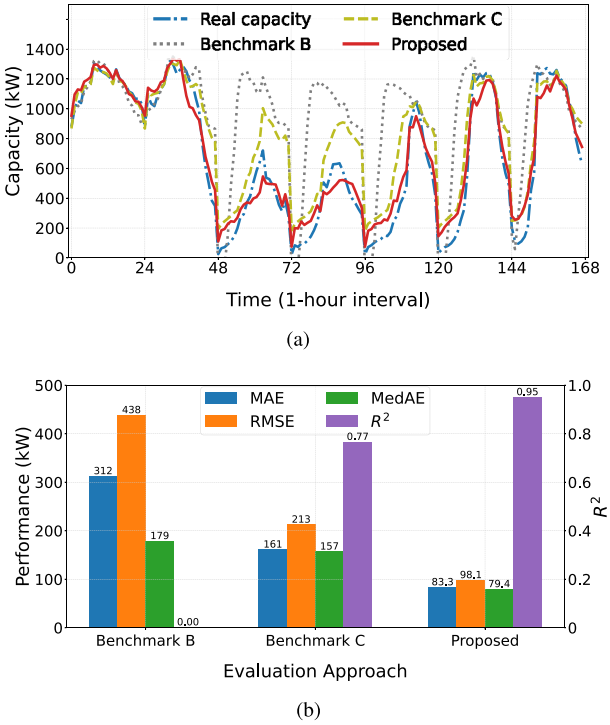


Fig. 6. Evaluation result and performance metric of capacity evaluation models under scenario II.

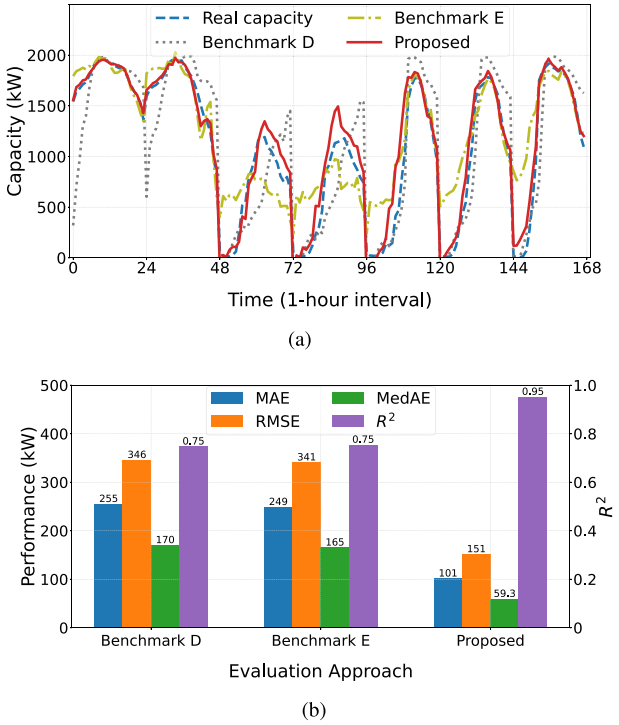


Fig. 7. Evaluation result and performance metric of capacity evaluation models under scenario III.

method exploits a large amount of data from buildings of the same type so that it can accurately evaluate the regulation capacity in the new building. The three error metrics of the proposed model are all reduced to within 100, which is significantly lower than those of the other two benchmarks. Meanwhile, the R^2 of the above three models is 0.01, 0.77, and 0.95, respectively, indicating that the model has been remarkably enhanced through our proposed method.

3) Scenario III - Insufficient Data for All Buildings in One Type: In this scenario, even all of the data from one type of buildings are not enough to train a high-performance model. Unlike the previous two scenarios, we tackle this form of data insufficiency with the help of data from other types of buildings. The evaluation results and the performance metrics of benchmark D, benchmark E, and the proposed method in scenario III are shown in Fig. 7.

Benchmark D can identify extreme weather owing to similar weather conditions in some data from other same-type buildings. However, there is a drift in the evaluation; that is, the estimated maximum capacity appears several hours later than the corresponding real value, resulting in its MAE of 255.05. Although benchmark E has utilized a massive amount of data from buildings of other types, its performance is only marginally enhanced compared with benchmark D. The two benchmarks' MAE, RMSE, MedAE metrics, and R^2 value are all close. In contrast, the model of the proposed method, which has been pre-trained by the source buildings and fine-tuned by the target building, outperforms the two benchmarks D and E significantly, with distinct progress in each metric. Additionally, its R^2 value reaches 0.95, indicating that the evaluations fit the real capacities well. This proves that our proposed method can address the data deficiency problem by utilizing data from different types of buildings with the help of the cross-type transfer learning algorithm.

C. Performance Comparison With Existing Methods

In this subsection, we further verify the performance of our proposed framework by comparing it with existing state-of-the-art methods. Because there are few data-driven models for regulation capacity evaluation in existing studies and the regulation capacity evaluation can also be treated as a regression problem, we select some regression models in the load forecasting field as benchmarks, as follows.

- Benchmark F1: an unshared convolutional neural network (CNN) proposed by Li et al. [38] for both deterministic and interval load forecasting.
- Benchmark F2: a grey wolf optimizer-based CNN proposed by Jalali et al. [39] for electricity load forecasting.
- Benchmark F3: a stacked long-short term memory (LSTM) network proposed by Li et al. [40] to predict the HVAC consumption in buildings.
- Benchmark F4: a hybrid forecasting model based on the temporal convolution network (TCN) and light gradient boosting machine (LightGBM) proposed by Wang et al. [41] for industrial load forecasting.

We compare the proposed method with the above four benchmarks in three scenarios, and the results are shown in Table III. It can be observed that the model performance of the four benchmarks is enhanced to some extent compared to MLPs because the benchmarks are all improved for regression tasks, e.g., unshared CNN, grey wolf optimizer, and TCN.

TABLE III
PERFORMANCE COMPARISON WITH EXISTING METHODS

Scenario	Metric	Benchmark F1	Benchmark F2	Benchmark F3	Benchmark F4	Proposed
Scenario I	MAE	338.731 (28.076)	305.299 (23.862)	269.954 (20.421)	225.304 (17.719)	**130.901 (9.209)**
	RMSE	370.933 (25.057)	346.879 (23.272)	290.869 (16.902)	280.470 (15.426)	**174.023 (9.839)**
	MedAE	306.491 (23.189)	260.025 (19.338)	203.411 (15.095)	183.534 (13.387)	**91.885 (7.129)**
	R^2	0.127 (0.043)	0.242 (0.040)	0.336 (0.038)	0.414 (0.036)	**0.779 (0.029)**
Scenario II	MAE	221.035 (11.250)	215.623 (10.599)	209.247 (10.105)	202.132 (9.901)	**83.568 (7.558)**
	RMSE	285.327 (12.592)	264.185 (11.371)	220.259 (10.983)	193.753 (10.326)	**97.910 (6.018)**
	MedAE	143.064 (8.514)	122.414 (8.212)	115.075 (7.775)	103.949 (7.322)	**79.431 (4.512)**
	R^2	0.479 (0.026)	0.523 (0.027)	0.652 (0.028)	0.724 (0.022)	**0.950 (0.013)**
Scenario III	MAE	284.392 (17.381)	256.010 (16.202)	222.082 (12.763)	196.641 (9.957)	**101.389 (5.145)**
	RMSE	305.447 (13.920)	273.469 (12.865)	240.933 (12.421)	218.845 (11.621)	**151.463 (9.237)**
	MedAE	240.820 (20.248)	201.015 (18.454)	168.479 (14.080)	116.079 (11.486)	**59.307 (3.249)**
	R^2	0.411 (0.028)	0.503 (0.027)	0.549 (0.025)	0.696 (0.023)	**0.951 (0.018)**

***MAE, RMSE and MedAE are all in kilowatts(kW), and each entry gives a pair of AVG. (STD.).**

However, because of the insufficient data problem, the evaluation results in the three scenarios are still not good enough; where the maximum error is close to 400 kW, and the minimum error is still over 100 kW. In contrast, although the proposed method only uses the multi-layer perceptron as the evaluation model, its evaluation performance far outperforms all the benchmarks in each scenario because it addresses the data deficiency via the classified federated learning algorithm and the cross-type transfer learning algorithm. For example, the evaluation error of the proposed method in Scenario I is reduced by at least 90 kW compared to the benchmarks, nearly 40%. In Scenario II, the R^2 value of our method is more than 30% higher than the best benchmark, and the three error metrics are also decreased by about 30 kW on average. Similarly, in Scenario III, the R^2 value is also increased by 0.255 (over 35%), and the MAE, RMSE, and MedAE are all been reduced by almost half. These experiments prove the superiority of the proposed method compared with other the state-of-the-art methods.

The average training and inference time of the proposed method are also compared with the four benchmarks. Table IV shows that the training time of the proposed method is significantly longer than the other four benchmarks. This is because the encryption and decryption operations are involved in our proposed method. However, the data-driven model is usually trained offline and is not be deployed until the training has been completed. After training, it can be used for a period of time. Therefore, even if the training time of our method is long, the speed of evaluation is not reduced and the timeliness in the actual application is not affected. This can be seen in the inference time, which is around 1 millisecond for both our method and the four benchmarks. Considering that we mainly focus on 1-hour-ahead regulation capacity evaluation, the inference time is almost negligible, which verifies that our method is timely and does not affect efficiency in application.

TABLE IV
THE TIMELINESS OF THE PROPOSED METHOD

Method	Training time (sec)	Inference time (sec)
Benchmark F1	1465.39	0.001005
Benchmark F2	1383.91	0.001013
Benchmark F3	1774.28	0.000969
Benchmark F4	1146.56	0.000997
Proposed	2298.54	0.000958

TABLE V
NUMERICAL RESULTS OF THE LOCAL MODEL, THE IDEAL MODEL, AND THE PROPOSED METHOD

		Local model	Proposed	Ideal model
Scenario I	**MAE**	449.162	135.865	**133.853**
	RMSE	558.463	178.065	**175.991**
	MedAE	397.837	93.448	**91.889**
	$\boldsymbol{R^2}$	0.001	0.725	**0.727**
Scenario II	**MAE**	236.697	81.184	**79.845**
	RMSE	325.299	95.068	**94.582**
	MedAE	167.739	77.872	**76.058**
	$\boldsymbol{R^2}$	0.383	0.958	**0.959**
Scenario III	**MAE**	375.923	**103.094**	103.535
	RMSE	423.171	**155.032**	156.387
	MedAE	309.414	**61.333**	63.138
	$\boldsymbol{R^2}$	0.295	**0.941**	0.940

***MAE, RMSE and MedAE are all in kilowatts(kW)**

D. Performance Comparison With Local and Ideal Models

In this part, we compare the performances of the proposed method with local models and ideal models. The local models are trained by individual buildings using their own data, while the ideal models are trained via the traditional centralized way, which gathers all of the data in a central server and trains a model using all of the data. Note that the ideal model is still a data-driven model rather than an actual load model so it still inevitably has evaluation errors. As our proposed method is based on the federated learning, its performance should be close to the corresponding ideal model [18].

Table V summarizes the performance of the three types of models in terms of MAE, RMSE, MedAE, and R^2 under the three scenarios I, II, and III. It is clear that the proposed method outperforms the local models in all aspects and scenarios. The three error metrics are reduced by 62% on average and the average R^2 is raised from 0.226 to 0.893. The performance of our proposed method is also close to that of the ideal models, as the metric differences between these two models are negligible. In Scenario III, the performance of our method even exceeds that of the ideal model. Because the ideal model is still a data-driven model, and the performance of the proposed

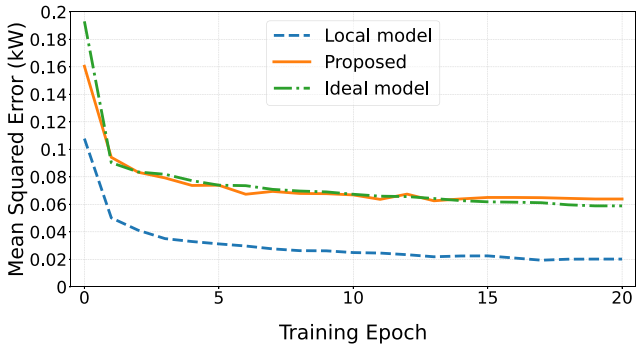


Fig. 8. Training loss of the three models.

method is close to the ideal model, it is reasonable that the proposed method outperforms the ideal model in some cases, especially when the test data significantly differ from the training data. Therefore, our model satisfies the losslessness within the acceptable range.

Fig. 8 shows the average training loss of the aforementioned three types of models in the three scenarios. It can be seen that the convergence of our proposed method and the ideal model is approximately identical, which further proves the losslessness of the proposed method. Although our proposed method adopts the classified federated learning algorithm to preserve the privacy of data, it still has a high performance close to that of the ideal model. As for the local model, although the training loss is the lowest, its numerical results are inferior to the other two models. This may be because of insufficient training data, resulting in the overfitting of the model.

VI. Conclusion

In this paper, we studied the regulation capacity evaluation problem of HVAC systems in heterogeneous buildings, which is hard to solve through physical-based and traditional centralized data-driven methods. We proposed a deep learning framework that consisted of classified federated learning, cross-type transfer learning, and the secure privacy-preserving protocol. This framework can perform accurate regulation capacity evaluation by addressing data insufficiency through the collaboration of buildings without compromising privacy. Case studies under three scenarios demonstrate that our proposed framework has high regulation capacity evaluation accuracy and generalization, even when building data are not sufficient or unavailable. The average estimation error of the proposed framework is decreased by 77%, 49% and 64% in three scenarios. Through a comparison with existing state-of-the-art methods, the R^2 value of the proposed framework increases by at least 50% on average, where the effectiveness and superiority have been further validated. In addition, the results indicate that the performance and efficiency of our method are close to the centralized method. The differences between the two methods in estimation error and training loss are within only 2kW and 0.0024kW, respectively. Although the secure privacy-preserving protocol has no impact on the accuracy of the proposed framework because it only protects data privacy and security, it is necessary because it avoids data leakage and makes collaborative training possible.

In this paper, we used the Paillier cryptosystem to encrypt sensitive data, and completed the information exchange by communicating with the server. Although data privacy was protected, the designed protocol also increased the computational burden and time consumption. In future work, we intend to reduce the computational cost of the cryptosystem, and improve the interaction processes of the transmission scheme, which makes the proposed method more secure and efficient in practical applications. Moreover, we focused on the regulation capacity evaluation in this paper, and the use of evaluation values during real-time operations was usually regarded as the market bidding or operation issue. Because different electricity markets had different policies on the regulation reward and punishment mechanism, it was necessary for the aggregator to bid or operate strategically, which is an important research topic and will also be our future work.

Appendix A

A. Security and Privacy Proof

1) Privacy: The Paillier algorithm is used to ensure user privacy, and the objective is that the adversary cannot drive the corresponding plaintext even if they obtain the ciphertext [32]. This is also an asymmetric encryption algorithm in which the user utilizes the public key for encryption and the private key for decryption. Because the adversary can obtain the public key that is open to anyone, the attack model is the chosen-plaintext attack, which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts using the public key [42]. The adversary hopes to use these ciphertexts to crack the user's ciphertext and obtain the user's plaintext; thus, the user's privacy is compromised.

In this paper, the parameters of the user local model were encrypted using the Paillier algorithm, and the calculation process is as follows:

$$c = g^m \cdot r^n \bmod n^2,$$

where m and c are the plaintext and the ciphertext, respectively; g and n form the public key (n, g); and $n = p \cdot q$, where p and q are large primes.

Therefore, the chosen-plaintext attack process for this algorithm was that the adversary constructed a set of plaintext ciphertext pairs $\{(m_i, c_i)\}$, intended to match the user's plaintext ciphertext pairs (m, c), and thus infered the plaintext of the user. We could reduce this attack to a mathematical problem. Given a composite n and an integer z, we can decides whether z is an n-th residue modulo n^2, that is, whether there exists a y such that:

$$z = y^n \bmod n^2.$$

This problem is also regraded as the problem of deciding the n-th residuosity, which distinguishes the n-th residues from the non n-th residues. Similar to the problem of deciding quadratic or higher-degree residuosity [43], the problem of deciding the n-th residuosity is a random-self-reducible problem whereby all of its instances are polynomially equivalent, so this problem

TABLE VI
CHARACTERISTICS OF BUILDING TYPES

		Commercial building	Office building	Hotel
Building structure	**floor area (m^2)**	$10000 \sim 30000$	$2500 \sim 8000$	$1000 \sim 5000$
	floor height (m)	6	4	3
	number of floors	$4 \sim 10$	$20 \sim 60$	$10 \sim 30$
Social activity	**opening time (hour)**	13 (9 a.m. $\sim$ 10 p.m.)	10 (8 a.m. $\sim$ 6 p.m.)	24
	foot traffic (person/day)	$5000 \sim 20000$	$2500 \sim 5000$	$500 \sim 2000$
	cooling temperature ($^\circ C$)	≈ 20	$20 \sim 24$	≥ 24
Load pattern	**load range (MW)**	$5 \sim 7$	$6 \sim 8$	$3 \sim 5$
	peak number	1	1	2
	load periodicity	weekend/holiday ascend	weekend/holiday descend	weekend/holiday ascend

is either uniformly intractable or uniformly polynomial [44]. In addition, the problem of deciding the n-th residuosity is computationally hard for prime residuosity [45]. Because we choose a square number n^2 as modulus and $n = p \cdot q$, there exists no polynomial time distinguisher for the n-th residues modulo n^2; that is, the above mathematical problem is intractable [46]. Therefore, the Paillier algorithm achieves indistinguishability under the chosen-plaintext attack, in that the ciphertext does not leak any information in the plaintext, also known as semantic security [47].

2) Security: The AES algorithm is used to protect communication security, and the objective is to prevent the adversary from deriving plaintext from ciphertext [33]. The difference is that the AES algorithm is a symmetric encryption algorithm where the user exploits the same key for encryption and decryption, and the key is a top secret. The AES algorithm involves four kinds of operations: byte substitution, row shift, column mixture, and round-key addition. The sequence of all processes in encryption and decryption are exactly the opposite, which ensures that the decryption operation can restore the plaintext from ciphertext completely and correctly.

In this paper, because the adversary cannot obtain the key, the brute force method is usually adopted, which calculates each possible combination of the password and tests whether it is the correct password. However, the time complexity of this approach exponentially increases with the key length, that is, the bits of the key [48]. Take the AES-128 (i.e., the key length is 128 bits) algorithm as an example; 2^{127} attempts are required on average. Even using the computing resources of the Bitcoin network (around $3 * 10^{19}$ operations per second), it would approximately take a staggering 200 billion years to crack, yet the Big Bang only occurred an estimated 13.8 billion years ago. Moreover,it would cost over 10^7 trillion dollars to crack AES-128, while the global GDP is less than 100 trillion dollars a year. Thus, in terms of time complexity and economic cost, it is almost impossible to crack the AES algorithm [49].

APPENDIX B

A. Building Characteristics and HVAC System Simulation

In this paper, we defined building types according to the way buildings were used, including office buildings, commercial buildings, and hotels. We separated commercial buildings from hotels because of their different building structures and uses, resulting in significant differences in load patterns and regulation capacities. The characteristics of the different building types are summarized in Table VI.

Because we focused on evaluating the regulation capacity of HVAC systems in buildings, we simulated the operation of HVAC systems and record the corresponding data for training and testing. The HVAC system converted energy between water and wind, thereby controlling the indoor temperature through cold wind. The details of thermal dynamic processes are described below [50], [51].

The power consumption of HVAC systems can be calculated based on the energy and mass balance, as follows:

$$P_t^{\text{hvac}} = Q_t^{\text{hvac}} / COP,$$

where P_t^{hvac} and Q_t^{hvac} are the electrical power and cooling power of the HVAC system at time t, respectively, both in kW; COP denotes the HVAC system's coefficient of performance.

The Q_t^{hvac} is determined by the HVAC system's return water temperature, as follows:

$$Q_t^{\text{hvac}} = c^{\text{water}} \cdot m_t^{\text{water}} \cdot \left(T_t^{\text{water},r} - T_t^{\text{water},s}\right),$$

where c^{water} is the specific heat capacity of water, in kJ/(kg $\cdot^\circ C$); m_t^{water} is the instantaneous mass flow rate of water at time t, in kg/s; $T_t^{\text{water},r}$ and $T_t^{\text{water},s}$ denote the return water temperature and supply water temperature of the HVAC system at time t, respectively.

The HVAC system adjusts the indoor temperature by providing cooling wind, and the return wind temperature can be calculated by

$$T_t^{\text{wind},r} = (1-\alpha) \cdot T_t^{\text{in}} + \alpha \cdot T_t^{\text{out}},$$

where $T_t^{\text{wind},r}$ is the return wind temperature at time t; T_t^{in} and T_t^{out} denote the indoor temperature and outdoor temperature of the building at time t, respectively; and α is the ventilation coefficient, which is 0 when there is no air exchange.

The cooling power of the supply wind comes from the cooling power of the HVAC system, and there are some losses during energy transfer. The supply wind temperature can be calculated from the energy of the cold air and the return air temperature, expressed as

$$Q_t^{\text{wind}} = \eta_1 \cdot Q_t^{\text{hvac}},$$
$$Q_t^{\text{wind}} = c^{\text{air}} \cdot m_t^{\text{wind}} \cdot \left(T_t^{\text{wind},r} - T_t^{\text{wind},s}\right),$$

where Q_t^{wind} is the cooling power of the supply wind at time t; η_1 is the transfer efficiency coefficient of an HVAC system to the air-handling unit; c^{air} is the specific heat capacity of air; m_t^{wind} is the instantaneous mass flow rate of wind at time t; $T_t^{\text{wind},r}$ and $T_t^{\text{wind},s}$ denote the return wind temperature and supply wind temperature of the HVAC system at time t, respectively.

Then, the indoor thermal dynamic is described as

$$c^{\text{air}} \cdot \rho \cdot V \cdot \frac{\mathrm{d}T^{\text{in}}}{\mathrm{d}t} = U \cdot A \cdot \left(T_t^{\text{in}} - T_t^{\text{out}}\right) - \eta_2 \cdot Q^{\text{wind}} + \xi \cdot \left(T_t^{\text{in}} - T_t^{\text{out}}\right),$$

where ρ is the density of the air, in kg/m^3; V and A denote the volume and surface area of the building in m^3 and m^2, respectively; U is the heat transfer coefficient of the building, in $kW/(m^2 \cdot^\circ C)$; η_2 is the transfer efficiency coefficient of air handling unit to indoor air; and ξ denotes the heat loss coefficient.

According to the change of indoor temperature, the PID controller adjusts the mass flow rate of wind at the next time and controls the subsequent temperature variation, which can be expressed as

$$m_{t+1}^{\text{wind}} = PID\left(T_t^{\text{in}} - T^{\text{set}}\right),$$

where m_{t+1}^{wind} is the instantaneous mass flow rate of wind at time $t+1$; $PID(\cdot)$ is the PID controller; and T^{set} denotes the setting temperature of the HVAC system.

REFERENCES

[1] B. Mohandes, M. S. El Moursi, N. Hatziargyriou, and S. El Khatib, "A review of power system flexibility with high penetration of renewables," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3140–3155, Jul. 2019.

[2] A. Nikoobakht, J. Aghaei, M. Shafie-Khah, and J. P. Catalao, "Assessing increased flexibility of energy storage and demand response to accommodate a high penetration of renewable energy sources," *IEEE Trans. Sustain. Energy*, vol. 10, no. 2, pp. 659–669, Apr. 2019.

[3] N. G. Paterakis, O. Erdinç, and J. P. Catalão, "An overview of demand response: Key-elements and international experience," *Renew. Sustain. Energy Rev.*, vol. 69, pp. 871–891, Mar. 2017.

[4] M. Song, W. Sun, Y. Wang, M. Shahidehpour, Z. Li, and C. Gao, "Hierarchical scheduling of aggregated TCL flexibility for transactive energy in power systems," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2452–2463, May 2020.

[5] C. Vivekananthan and Y. Mishra, "Stochastic ranking method for thermostatically controllable appliances to provide regulation services," *IEEE Trans. Power Syst.*, vol. 30, no. 4, pp. 1987–1996, Jul. 2015.

[6] Q. Zhou, Z. Li, Q. Wu, and M. Shahidehpour, "Two-stage load shedding for secondary control in hierarchical operation of islanded microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3103–3111, May 2019.

[7] R. Ghorani, M. Fotuhi-Firuzabad, and M. Moeini-Aghtaie, "Main challenges of implementing penalty mechanisms in transactive electricity markets," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 3954–3956, Sep. 2019.

[8] L. Fabietti, T. T. Gorecki, F. A. Qureshi, A. Bitlislioğlu, I. Lymperopoulos, and C. N. Jones, "Experimental implementation of frequency regulation services using commercial buildings," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1657–1666, May 2016.

[9] G. S. Pavlak, G. P. Henze, and V. J. Cushing, "Optimizing commercial building participation in energy and ancillary service markets," *Energy Build.*, vol. 81, pp. 115–126, Oct. 2014.

[10] M. Ali, A. Safdarian, and M. Lehtonen, "Demand response potential of residential HVAC loads considering users preferences," in *Proc. IEEE PES Innov. Smart Grid Technol. Europe*, 2014, pp. 1–6.

[11] N. Lu, "An evaluation of the HVAC load potential for providing load balancing service," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1263–1270, Sep. 2012.

[12] G. Goddard, J. Klose, and S. Backhaus, "Model development and identification for fast demand response in commercial HVAC systems," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 2084–2092, Jul. 2014.

[13] A. Javed, H. Larijani, A. Ahmadinia, R. Emmanuel, M. Mannion, and D. Gibson, "Design and implementation of a cloud enabled random neural network-based decentralized smart controller with intelligent sensor nodes for HVAC," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 393–403, Apr. 2017.

[14] Y.-J. Kim, "A supervised-learning-based strategy for optimal demand response of an HVAC system in a multi-zone office building," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4212–4226, Sep. 2020.

[15] L. Yu et al., "Deep reinforcement learning for smart home energy management," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2751–2762, Apr. 2020.

[16] H. Li, Z. Wan, and H. He, "Real-time residential demand response," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4144–4154, Sep. 2020.

[17] L. Yu et al., "Multi-agent deep reinforcement learning for HVAC control in commercial buildings," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 407–419, Jan. 2021.

[18] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019.

[19] Y. Wang, I. L. Bennani, X. Liu, M. Sun, and Y. Zhou, "Electricity consumer characteristics identification: A federated learning approach," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3637–3647, Jul. 2021.

[20] J. Lin, J. Ma, and J. Zhu, "A privacy-preserving federated learning method for probabilistic community-level behind-the-meter solar generation disaggregation," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 268–279, Jan. 2022.

[21] V. Venkataramanan, S. Kaza, and A. M. Annaswamy, "DER forecast using privacy preserving federated learning," *IEEE Internet Things J.*, early access, Mar. 8, 2022, doi: 10.1109/JIOT.2022.3157299.

[22] S. J. Pan and Q. Yang, "A survey on transfer learning," *IEEE Trans. Knowl. Data. Eng.*, vol. 22, no. 10, pp. 1345–1359, Oct. 2010.

[23] Y. Liu, X. Wang, and W. You, "Non-intrusive load monitoring by voltage–current trajectory enabled transfer learning," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5609–5619, Sep. 2019.

[24] H. Yin, Z. Ou, J. Fu, Y. Cai, S. Chen, and A. Meng, "A novel transfer learning approach for wind power prediction based on a serio-parallel deep learning architecture," *Energy*, vol. 234, Nov. 2021, Art. no.121271.

[25] Y. Zhang, X. Wang, X. Jiang, and Y. Zhou, "Marginalized graph self-representation for unsupervised hyperspectral band selection," *IEEE Trans. Geosci. Remote Sens.*, vol. 60, pp. 1–12, 2022.

[26] C. Ren and Y. Xu, "Transfer learning-based power system online dynamic security assessment: Using one model to assess many unlearned faults," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 821–824, Jan. 2020.

[27] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. AISTATS*, 2017, pp. 1273–1282.

[28] F. Zhuang et al., "A comprehensive survey on transfer learning," *Proc. IEEE*, vol. 109, no. 1, pp. 43–76, Jan. 2021.

[29] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2014, *arXiv:1412.6980*.

[30] Y. Zhang, Y. Wang, X. Chen, X. Jiang, and Y. Zhou, "Spectral–spatial feature extraction with dual graph autoencoder for hyperspectral image clustering," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 12, pp. 8500–8511, Dec. 2022.

[31] J. Yosinski, J. Clune, Y. Bengio, and H. Lipson, "How transferable are features in deep neural networks?" in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 27, 2014, pp. 3320–3328.

[32] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 1999, pp. 223–238.

[33] M.-L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2001, pp. 309–318.

[34] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Hoboken, NJ, USA: CRC Press, 2018.

[35] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, p. 1301, 2009.

[36] P. Yu, H. Zhang, Y. Song, H. Hui, and C. Huang, "Frequency regulation capacity offering of district cooling system: An intrinsic-motivated reinforcement learning method," *IEEE Trans. Smart Grid*, early access, Nov. 9, 2022, doi: 10.1109/TSG.2022.3220732.
[37] A. Paszke et al., "Pytorch: An imperative style, high-performance deep learning library," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 32, 2019, pp. 8024–8035.
[38] Z. Li, Y. Li, Y. Liu, P. Wang, R. Lu, and H. B. Gooi, "Deep learning based densely connected network for load forecasting," *IEEE Trans. Power Syst.*, vol. 36, no. 4, pp. 2829–2840, Jul. 2021.
[39] S. M. J. Jalali, S. Ahmadian, A. Khosravi, M. Shafie-khah, S. Nahavandi, and J. P. Catalão, "A novel evolutionary-based deep convolutional neural network model for intelligent load forecasting," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8243–8253, Dec. 2021.
[40] L. Li, C. J. Meinrenken, V. Modi, and P. J. Culligan, "Short-term apartment-level load forecasting using a modified neural network with selected auto-regressive features," *Appl. Energy*, vol. 287, Apr. 2021, Art. no. 116509.
[41] Y. Wang et al., "Short-term load forecasting for industrial customers based on TCN-LightGBM," *IEEE Trans. Power Syst.*, vol. 36, no. 3, pp. 1984–1997, May 2021.
[42] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the fresnel domain," *Opt. Lett.*, vol. 31, no. 22, pp. 3261–3263, 2006.
[43] D. Hofheinz and E. Kiltz, "The group of signed quadratic residues and applications," in *Proc. Annu. Int. Cryptol. Conf.*, 2009, pp. 637–653.
[44] K. S. Booth, "Isomorphism testing for graphs, semigroups, and finite automata are polynomially equivalent problems," *SIAM J. Comput.*, vol. 7, no. 3, pp. 273–279, 1978.
[45] D. Naccache and J. Stern, "A new public key cryptosystem based on higher residues," in *Proc. 5th ACM Conf. Comput. Commun. Security*, 1998, pp. 59–66.
[46] C. Peikert, V. Vaikuntanathan, and B. Waters, "A framework for efficient and composable oblivious transfer," in *Proc. Annu. Int. Cryptol. Conf.*, 2008, pp. 554–571.
[47] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Proc. Annu. Cryptol. Conf.*, 2012, pp. 294–311.
[48] P. Mahajan and A. Sachdeva, "A study of encryption algorithms AES, DES and RSA for security," *Glob. J. Comput. Sci. Technol.*, vol. 13, no. 15, p. 18, 2013.
[49] A. Al Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," in *Proc. IEEE 3rd Int. Conf. Converg. Hybrid Inf. Technol.*, vol. 2, 2008, pp. 505–510.
[50] W. W. Che et al., "Energy consumption, indoor thermal comfort and air quality in a commercial office with retrofitted heat, ventilation and air conditioning (HVAC) system," *Build. Environ.*, vol. 201, pp. 202–215, Oct. 2019.
[51] Y. Yu, S. You, H. Zhang, T. Ye, Y. Wang, and S. Wei, "A review on available energy saving strategies for heating, ventilation and air conditioning in underground metro stations," *Renew. Sustain. Energy Rev.*, vol. 141, May 2021, Art. no. 110788.

Zhenyi Wang (Graduate Student Member, IEEE) received the B.E. degree in cybersecurity from Sichuan University, Chengdu, China, in 2021. He is currently pursuing the Ph.D. degree in electrical and computer engineering with the University of Macau, Macau, China.

His research interests include data analytics in demand response, anomaly detection in power systems, and trustworthy artificial intelligence.

Peipei Yu (Graduate Student Member, IEEE) received the B.S. and M.S. degrees in mathematics from Zhejiang University, Hangzhou, China, in 2016 and 2019, respectively. She is currently pursuing the Ph.D. degree with University of Macau, Macau, China.

Her research interests include Internet of Things for smart energy, demand response, and reinforcement learning control.

Hongcai Zhang (Member, IEEE) received the B.S. and Ph.D. degrees in electrical engineering from Tsinghua University, Beijing, China, in 2013 and 2018, respectively.

He is currently an Assistant Professor with the State Key Laboratory of Internet of Things for Smart City and Department of Electrical and Computer Engineering, University of Macau, Macau, China. From 2018 to 2019, he was a Postdoctoral Scholar with the Energy, Controls, and Applications Laboratory, University of California at Berkeley, Berkeley, where he also worked as a Visiting student Researcher in 2016. His current research interests include Internet of Things for smart energy, optimal operation and optimization of power and transportation systems, and grid integration of distributed energy resources.