A federated learning approach for thermal comfort management

Maysaa Khalil, Moez Esseghir, Leila Merghem-Boulahia

Version of Record: https://www.sciencedirect.com/science/article/pii/S1474034622000027
Manuscript_efab289fba9bf403bef648ff23fc6287

A Federated Learning Approach for Thermal Comfort Management

Maysaa Khalil[a,*], Moez Esseghir[a], Leila Merghem-Boulahia[a]

[a]*ERA, LIST3N, University of Technology of Troyes, 12 Rue Marie Curie, Troyes, 10000, France*

Abstract

Existing thermal comfort prediction approaches by machine learning models have been achieving great success based on large datasets in sustainable Industry 4.0 environment. However, the industrial Internet of Things (IoT) environment generates small-scale datasets where each dataset may contain lots of worker's private data. The latter is challenging the current prediction approaches as small datasets running a large number of iterations can result in overfitting. Moreover, worker's privacy has been a public concern throughout recent years. Therefore, there must be a trade-off between developing accurate thermal comfort prediction models and worker's privacy-preserving. To tackle this challenge, we present a privacy-preserving machine learning technique, federated learning (FL), where an FL-based neural network algorithm (Fed-NN) is proposed for thermal comfort prediction. Fed-NN departs from current centralized machine learning approaches where a universal learning model is updated through a secured parameter aggregation process in place of sharing raw data among different industrial IoT environments. Besides, we designed a branch selection protocol to solve the problem of communication overhead in federating learning. Experimental studies on a real dataset reveal the robustness, accuracy, and stability of our algorithm in comparison to other machine learning algorithms while taking privacy into consideration.

Keywords:
Industrial Internet of Things, Federated Learning, Neural Networks, Privacy-Preserving, Thermal Comfort Prediction.

1. Introduction

During the last decennary, the term Industry 4.0 has become a mandatory requirement for the renaissance of every industry to stay on the safe shore. The IoT, machine learning, big data, control mechanisms, management and monitoring systems, artificial intelligence, human-machine interactions, real-time data management, and automation processes all participate in the process of increasing profits while decreasing costs in the modern industry [1].

Consequently, human beings are considered key players in boosting the connectivity with the machines and for assuring the right machine operations. However, the performance of the worker is directly linked to his/her health, comfort, and well-being which are affected by the indoor environment [2]. Worker's thermal comfort is acknowledged as a core requirement in healthcare for industrial IoT environments [2]. Inadequate thermal conditions resulted by both two low or elevated temperatures, by too cool or too warm environments have significant negative impact on worker performance [3]. Studies [3] indicate that comfortable cool environment is crucial for performance at work, where avoiding elevated temperatures in summer and winter can result in measurable benefits.

Thermal comfort is defined as a condition of mind that expresses subjective satisfaction to the surrounding thermal environment [4]. A human body can be considered as a heat engine with food as an input energy. In order to allow the body to operate, the human will release excess heat to the environment. This heat transfer is proportional to the temperature difference. The body loses more heat in cold environment while it does not release enough heat in the cold environment. Both hot and cold scenarios result in discomfort. Maintaining this standard of thermal comfort for workers in buildings is one of the important goals of Heating, Ventilation, and Air Conditioning (HVAC) design engineers. It has been mentioned that thermal comfort affects the work efficiency, creativity, and happiness of an industrial worker [5]. The thermal discomfort of a worker does not only impact the productivity, performance, and engagement, but also affects the lifelong health of the worker [6]. Hence, thermal comfort prediction has been drawing attention

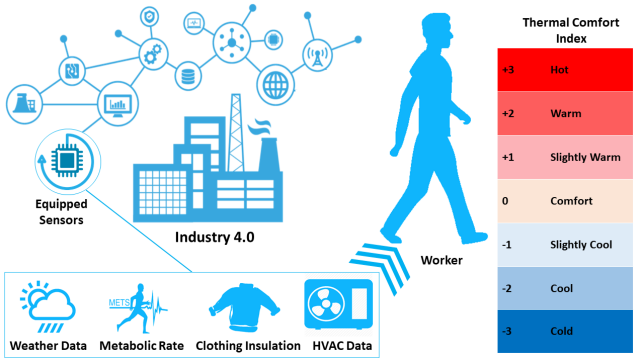

Figure 1: Collecting thermal comfort input data of a worker in an industrial environment.

*Corresponding author
Email address: maysaa.khalil@utt.fr (Maysaa Khalil)

in the industrial domain. Still, thermal comfort modeling is a demanding task considering the complexity of the worker's body and the non-linear relationship between input attributes.

In thermal comfort prediction, centralized machine learning models are commonly utilized to predict thermal comfort state [7]. Data are collected from different environmental and personal sensors equipped within the industrial IoT environment, as shown in Fig. 1. Collected data are fused to the cloud where a machine learning model is trained. In recent publications, many authors resort to applying machine learning algorithms to predict the thermal comfort of a group of workers in the same building. However, collecting a sufficient amount of data to achieve a desired training accuracy is limited. Moreover, the shared data may contain personal private information about the workers prompting privacy exposure. These information might include captured images from IoT-based camera devices, which are extremely sensitive [8]. The captured images allow us to derive the metabolic rate and clothing insulation, which are vital elements in thermal comfort index calculation [9]. To address the issue of privacy exposure and data leakage, we integrate a privacy-preserving machine learning model, federated learning (FL) [10], for thermal comfort prediction. In FL, a global shared model is trained on distributed branches locally without raw data exchange. We also propose Fed-NN, an enhanced FL algorithm with a neural network model to predict the thermal comfort state in an accurate way. The Fed-NN algorithm builds a global deep learning model after aggregating the model gradient parameters from different branches located in different geographical areas. The primary contributions of this paper are outlined as follows:

1. To the best of our knowledge, we are the first to apply federated learning approach in thermal comfort state prediction of a worker, which is a new privacy-preserving algorithm that combines the emerging FL algorithm and neural networks for thermal comfort prediction. Without data exchange, the model is trained locally providing a reliable data privacy mechanism.
2. We propose an improved version of the FedAvg algorithm by adding a branch selection protocol to avoid communication overhead which is suitable for large industrial IoT environments.
3. We conduct a variety of simulations on real data to demonstrate the accuracy of our proposal compared to other algorithms.

The rest of the paper is organized as follows. Literature about thermal comfort prediction and privacy issues in industrial IoT is presented in Section 2. The centralized and federated learning problems are defined in Section 3. The Fed-NN algorithm and the selection protocol are introduced in Section 4. Section 5 demonstrates the results of simulations. The conclusion is described in Section 6.

2. Related Work

2.1. Thermal Comfort Prediction

Thermal comfort prediction has always been a triggering issue in the IoT domain, which serves as a function of real-time thermal control. New thermal comfort state prediction techniques proposed by researchers can be divided into two types: (1) parametric models and (2) non-parametric models.

Parametric Models: Parametric models predict future data using a definite set of parameters of fixed size no matter how much the number of training examples is. Thermal comfort prediction, in most cases, implies the action of predicting the Predicted Mean Vote (PMV) index developed by Fanger but using different input parameters [7].The PMV index was developed based on principles of heat-balance equations and it was adopted by the American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) Standard 55. PMV is an index that aims to predict the mean value of votes of a group of occupants on a seven-point thermal sensation scale that ranges between (-3) for hot sensation and $(+3)$ for cold sensation. The comfort state is achieved between $-0.5, +0.5$, see Fig. 1. The thermal comfort index is scaled with six different attributes belonging to three different collections: weather data, indoor HVAC data, and personal attributes including the metabolic rate and clothing insulation. Different regressive models have been adapted to learn the PMV index including the auto-regression with exogenous variables [11], the logistic regression [12] , the locally weighted regression [13], the support vector machine [14], and the Gaussian process regression [15]. These models enhance the accuracy of thermal comfort prediction through targeting the statistical correlation between the PMV index and input parameters. They also have several advantages: high transparency and interpretation, which are trivial for a human to understand. Moreover, the computational time is totally underneath that of non-parametric models. However, these solutions are limited to simple problems and are highly constrained to a specific functional form, which may affect the training accuracy.

Non-parametric Models: Non-parametric models predict the output parameter without making strong assumptions about the form of the mapping function between input and output data. These models have acquired huge success in the thermal comfort prediction resulting from the improvement of data storage and computing. Zhang et al. [16] proposed a fine-grained deep learning neural network (DNN) approach to predict thermal comfort inside a smart building. The DNN model outperforms other machine learning models including the support vector machine and linear regression. Considering the relation between the variables, the feedforward neural network model was proposed in [17] as an explicit function of the relation between the PMV index and accessible variables.

2.2. Privacy Issues for the Industrial IoT Systems

The smart meters equipped in the Industry have unintended consequences for worker privacy. Video camera information stored serves as an information-rich side channel, exposing

worker habits and clothing style. Certain habits, such as repetitive clothing brands wear, have detectable style signatures. History has proved that if political or financial incentives coincide, data mining mechanisms will rapidly progress to suit the cravings of those who aim at exploiting that information. In industrial IoT systems, different methods and models rely on training datasets from users, occupants, workers, factories, buildings, and offices. Unfortunately, direct data exchange among different branches is prohibited by law with the increasing privacy awareness. To avoid these privacy issues, Lee et al. [18] present a WiFi-based occupancy monitoring system, which recognizes occupant's activities of daily living in a non-intrusive way by exploiting commercial off-the-shelf WiFi devices. In this approach, Channel State Information (CSI) has been extracted from several IoT devices and then transformed using the Short-Time Fourier Transform into image data. This preserves the temporal-spatial information of all the receiver data.

In [19], the authors designed a system that enables different parties to jointly learn an accurate neural network model without sharing data. That was performed through parallelizing and executing asynchronously the stochastic gradient descent (SGD) optimization problem on different training data. A feasible solution to assure that data is only accessed by authenticated parties in the industrial IoT control system is presented in [20]. A directed graph was used to present relationships between devices based on a cryptographic accumulator and an underlying standard digital signature scheme. However, these solutions have some disadvantages. First, no trade-off exists between the accuracy of the model and privacy. That is, privacy measures are considered but accuracy is not achieved. Second, these models are not capable of handling a huge amount of data in a small period of time [21]. In addition, the fact that different branches can reveal private data in the sharing process violates the legislation provided by different privacy-preserving regulations including the general data protection regulation (GDPR) issued by the EU. For example, the data transferred through the training process might include captured images of the workers. These images, as previously mentioned, help in recognizing workers metabolic rate and clothing insulation. The Art. 5 of the GDPR document presents key elements on the principles relating to processing of personal data. It is mentioned that the data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. In case of captured data leakage by a third party, the industry will be under legal accountability. Accordingly, we have to propose new methods to the growing sense of privacy in the Industry 4.0 domain.

Since the first presentation of federated learning by McMahan et al. [22] in 2017, FL models have been used to analyze private data for its privacy-preserving features. FL builds machine learning models depending on multiple datasets located across multiple devices while hindering data leakage [23]. FL was implemented for the first time to decentralized learning of mobile phone devices without taking privacy into consideration [24]. Nishio and Yonetani addressed the issue of mobile-edge computing using FL where they proposed the FedCS protocol to diminish training process time [25]. In [26], the authors proposed a federated transfer learning framework for wearable healthcare. In [27], the authors propose a federated learning framework, the federated transfer learning-enabled smart work packaging for protecting the personal image information of construction workers in occupational health and safety management.

Although researchers have developed some privacy-preserving methods in the industrial IoT systems, they do not fully preserve the workers' privacy. In this article, we propose a privacy-preserving FL method with NN for thermal comfort state prediction of workers. To the best of our knowledge, this is the only work that applies federated deep learning in the thermal comfort state prediction in the industrial domain.

3. Problem Definition

The term "branch" is used all over the article to characterize entities in the industrial IoT environment. Entities might be an office or a factory, etc. Let $\mathcal{K} = K_1, K_2, ..., K_n$ denotes the branch set. In the context of thermal comfort state prediction, we consider branches as the clients in the definition of FL. Each branch has a local database D_i. We aim at predicting whether the workers are thermally comfortable having historical sensor data information from different branches without sharing raw data and without lack of privacy. We, therefore, design a secure weight parameter aggregation mechanism as follows. The thermal comfort data collected by each branch creates a database D_i. The deep learning neural network model formulated in K_i uses local training data from D_i to adjust updated model parameters p_i. Each branch finishes the same exercise then uploads its respective p_i to the cloud, where a new global model is aggregated based on the values of p_i.

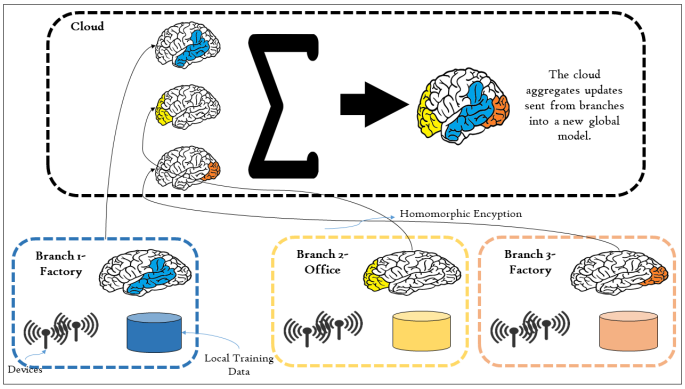

Figure 2: A secure mechanism to aggregate parameters into the cloud.

As indicated in Fig. 2, there is no data transfer among different entities due to a secure parameter aggregation mechanism. With no data exchange, the cloud creates a new global model aggregated from the multiple parameters sent by each branch.

In this paper, $f(.)$ represents the thermal comfort prediction function, t indicates the t-th timestamp in the time series, and a_t presents the state of thermal comfort at time t. A value

$a_t = 1$ *or* 0 reflects the state of being thermally comfortable or uncomfortable at time t, respectively. Three global problems are presented in the article:

1. *Information Privacy:* Information privacy attempts to employ data while conserving an individual's privacy. That is, it prevents direct access to private data including personally identifiable information. For example, information about a person's financial transactions can reveal a lot about a person's antiquity, including places he visited, whom he has met, products bought, etc., violating the information privacy definition [28]. In the following article, each branch uses local datasets to train its model locally. Then, each branch uploads the updated parameters instead of sharing data with the cloud.
2. *Centralized Thermal Comfort Prediction:* The centralized thermal comfort prediction problem is to measure $a_{t+s} = f(t+s, D)$, given a set of branches K_i, an aggregated database $D = D_1 \cup D_2 \cup ... \cup D_N$ and s is the prediction window after t.
3. *Federated Thermal Comfort Prediction:* The federated thermal comfort prediction problem is to measure $a_{t+s} = f_i(t+s, D_i)$, given a set of branches K_i, their respective databases D_i and s the prediction window after t. The function $f_i(.,.)$ is a local version of the function $f(.,.)$. Consequently, the formed results (parameters) are aggregated.

4. Methodology

In a centralized learning process, three steps are followed: data processing, data fusion, and model creation. Traditional centralized data processing techniques consist of extracting data features and labels from original data before fusing. These techniques include outliers removal, data sampling, normalization, and combinations. Through data fusion, data is shared directly by the learning model and all parties to achieve a global aggregated database for training. This approach is a subject of debate due to information privacy issues as it violates the recommendations provided by the privacy regulations including the EU GDPR. In order to address this challenge, FL is introduced. Nevertheless, most of the existing FL techniques employ simple machine learning models such as XGBoost and Decision Tree rather than neural network models[29]. These traditional models necessitate the upload of a huge number of parameters to the cloud in the federated learning process, which may cause a training failure for a local or global model due to expensive communication overhead [30] and limited network bandwidth. The communication overhead is measured by the number of bytes in each communication message sent. Accordingly, the FL framework needs to propose new aggregation mechanisms to deal with the problem of communication overhead. In this section, we propose the Fed-NN approach to predict the thermal comfort state, which is an improved version of the FedAvg algorithm as a way to reduce the communication overhead.

Algorithm 1: Federated Averaging Algorithm (FedAvg)

Input: Branches $\mathcal{K}$, s is the fraction of branches on each round, B is the local mini-batch size. η is the learning rate and E is the number of local epochs. $\mathcal{D}_k$ is the local training dataset. $\nabla\mathcal{L}(.;.)$ is the gradient optimization function and m the number of rounds.
Output: ω
Server Executes:
Initialize ω^0;
for *round* $t = 1, 2, ..., m$ **do**
  $n \leftarrow max(s \cdot \mathcal{K}, 1)$;
  $\{K_n\} \leftarrow$ random set of n branches to participate in the training;
  Send ω^0 to all branches in $\{K_n\}$;
  for *each branch* $k \in \{K_n\}$ ***in parallel*** **do**
    Initialize $\omega_t^k = \omega^0$;
    $\omega_{t+1}^k \leftarrow$ BranchUpdate(k, ω_t^k);
  end
  $\omega_{t+1} \leftarrow \frac{1}{|\{K_n\}|} \sum_{k \in K_n} \omega_{t+1}^k$;
end
Branch Executes:
BranchUpdate (k, ω):
$\mathcal{B} \leftarrow$ (split $\mathcal{D}_k$ into batches of size B);
while *local epoch i in E* **do**
  while *batch* $b \in \mathcal{B}$ **do**
    $\omega \leftarrow \omega - \eta\nabla\mathcal{L}(\omega; b)$;
  end
end
return ω to server;

4.1. Federated Learning and Deep Learning

FL is a privacy-preserving machine learning paradigm where different branches in the industrial IoT environment can contribute to the overall model training while keeping their data locally.

In particular, the FL technique requires learning both single and global prediction models from multiple databases stored locally in separate dozens or hundreds of branches [31]. In FL, a set of local datasets $\mathcal{D}_k$ of size D_k represents data from a set $\mathcal{K}$ of K set of branches. Therefore, the size of the local training datasets is $D = \sum_{k=1}^{K} D_k$. In deep learning, the typical settings are given by a set of input-output pairs $\{x_i, y_i\}_{i=1}^{D_k}$, where $x_i \in \mathbb{R}^g$ represents the input sample vector with g features and $y_i \in \{0, 1\}$ indicates the labeled output vector. Through training, we need to identify the model parameter vector (weight) $\omega \in \mathbb{R}^g$ that defines the output y_i with the loss function $f_i^{loss}(\omega)$. The goal is to learn this model locally with secure aggregation of weights among branches. The loss function on the dataset of branch k, therefore, is presented as follows:

$$J_k(\omega) := \frac{1}{D_k} \sum_{i \in D_k} f_i^{loss}(\omega) + \lambda r(\omega) \tag{1}$$

where $\omega \in \mathbb{R}^g$ is the local model weight $\forall\lambda \in [0, 1]$ and r(.) is the regularizer function, as we do not want the overall model to

be too drifted. At the cloud, the global predicted model problem is defined as:

$$\underset{\omega \in \mathbb{R}^g}{\operatorname{argmin}} J(\omega), J(\omega) = \sum_{k=1}^{K} \frac{R_k}{D} J_k(\omega) \tag{2}$$

where R_k is the regularizer for each branch. The above problem can be reformulated as follows:

$$\underset{\omega \in \mathbb{R}^g}{\operatorname{argmin}} J(\omega) := \sum_{k=1}^{K} \frac{\sum_{i \in D_k} f_i^{loss}(\omega) + \lambda r(\omega)}{D} \tag{3}$$

For the thermal comfort prediction problem, the deep neural network is used as a local model.

Algorithm 2: Federated Neural Network Algorithm (Fed-NN)

Input: $\{K_n\} \in \mathcal{K}$, l: the local mini-batch size, η: the learning rate, m the number of rounds, $\mathcal{D}_k$: the local training dataset and $\mathcal{SGD}$: the optimization function.
Output: ω
Server Executes:
Initialize ω^0;
for *round* $i = 1, 2, .., m$ **do**
  while $t_{d1} > 0$ **do**
    $\{K_n\} \leftarrow$ random set of n branches to participate in the training;
    $t_{d1} \leftarrow t_{d1} - 1$;
  end
  Send ω^0 to all branches in $\{K_n\}$;
  while $t_{d2} > 0$ **do**
    while h_ω *has not convergence* **do**
      for *each branch* $k \in \{K_n\}$ ***in parallel*** **do**
        Initialize $\omega_t^k = \omega^0$;
        Conduct a mini-batch input time step $\{X_l^i\}$;
        Conduct a mini-batch thermal comfort index series $\{Y_l^i\}$;
        $h_\omega \leftarrow \nabla_\omega \frac{1}{l} \sum_{i=1}^{l} (f_\omega(X_l^i) - Y_l^i)$;
        $\omega_{t+1}^k \leftarrow \text{BranchUpdate}(k, \omega_t^k, h_\omega)$;
      end
    end
    $t_{d2} \leftarrow t_{d2} - 1$;
  end
  $\omega_{t+1} \leftarrow \frac{1}{|\{K_n\}|} \sum_{k \in K_n} \omega_{t+1}^k$;
end
Branch Executes:
BranchUpdate (k, ω, h_ω):
$\mathcal{B} \leftarrow$ (split $\mathcal{D}_k$ into batches of size B);
while *local epoch i in l* **do**
  while *batch* $b \in \mathcal{B}$ **do**
    $\omega \leftarrow \omega - \eta(\mathcal{SGD}(\omega; b))$;
  end
end
return ω to server;

4.2. Privacy-Preserving Thermal Comfort Prediction Algorithm

Centralized learning methods merge data from different branches in the cloud. This may result in communication overhead and privacy leakage. We propose a privacy-preserving thermal comfort prediction algorithm, the Fed-NN, to address this issue. We start by introducing the FedAvg algorithm, which presents the crust of a secure gradient aggregation structure. Then, we propose an improved design of FedAvg, the Fed-NN algorithm, which is a communication-efficient scheme with a random selection of branches to address the problem of communication overhead of the FedAvg algorithm.

1. *Federated Averaging Algorithm (FedAvg):* In the following algorithm, each branch performs gradient descent optimization on the server model based on the local dataset without sending informational data to the cloud. This will hinder the problem of network bandwidth limitations in cloud aggregation. On the server, the received weights are aggregated based on the updates from all branches. Algorithm 1 shows the detailed pseudo code of the FedAvg algorithm that can be summarized in the following steps:
   - A number of branches are selected to participate in the training round for which a global model ω^0 is sent.
   - In each k selected branch, the model is trained based on local data. The ω_t^k is updated for E local epochs of SGD to obtain the next ω_{t+1}^k based on the *BranchUpdate* function.
   - Using an aggregation method ($\omega_{t+1} \leftarrow \frac{1}{|\{K_n\}|} \sum_{k \in K_n} \omega_{t+1}^k$ in Algorithm 1), the server aggregates each branch parameter ω_{t+1}^k.

   FedAvg algorithm is an iterative mechanism, it helps limit the communication overhead when transmitting parameters. At each t-th round in the training process, the model updated by each branch will be updated to the server global model.
2. *Branch Selection Protocol:* In an industrial IoT environment, the number of branches is small, including office places, factories, and other sites. In such cases, the FL problem is considered a small-scale problem. However, the number of branches might increase at any time. The increase is due to the presence of different factories all over the world. The industries wish to control the thermal comfort in all their factories. This will lead to the divergence of FedAvg algorithm due to the cost of communication overhead, and hence, decrease the accuracy of prediction in the FL framework. The communication overhead is the proportion of time the server spends communicating with the branches instead of aggregating the ML parameters. Moreover, in an FL framework, we are considering the presence of heterogeneous datasets, different computational capacities, and different channel conditions representing each branch, respectively. For instance, a branch with a large dataset compared to other branches

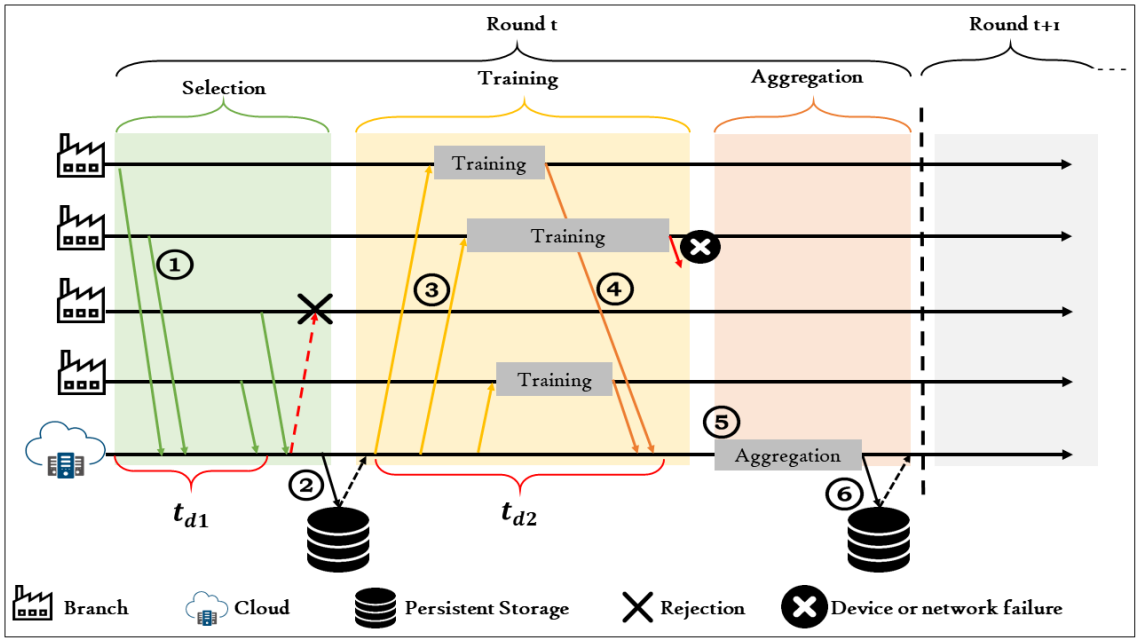

Figure 3: Branch Selection Protocol.

requires more time updating the model unless the branch possesses a better computational power. This will result in a delay of the new model update on the cloud. Furthermore, if a branch is under a poor channel condition, the upload time will become longer. The cloud can perform the *Aggregation* if and only if it receives all branches updates. Therefore, we designed a mechanism to select a set of branches that will participate in the i-th round training through a straight-forward approach. We set a deadline for random branches to accomplish the Training and Uploading steps. Submitted updates after the indicated deadlines are ignored.

The participants in the branch selection protocol are branches and the server, which is defined as a cloud-based distribution [23]. In the t-th training round, the selection protocol combines three steps: (1) selection phase, (2) training phase, and (3) aggregation phase, see Fig. 3.

- **Selection Phase:** The server selects a subset of branches to participate in the training phase depending on the eligibility of these branches, their willingness to participate, or other indicated criterion (Fig. 3-①). This periodic selection is done through a specific time t_{d1}, where each branch checks into the server by opening a bi-directional stream. If a branch opens the stream after the indicated deadline t_{d1} or if the number of selected branches in the training process has been reached, the branch will not be selected. In case a branch is not selected in the t-th round time, the server responds to the branch with instructions for an attempt in the next round time. The late response of a branch might be linked to a severely poor network channel.
- **Training Phase:** At first, the server loads the model already trained on server data (Fig. 3-②). Then, the server sends the gradient weights to the selected branches in phase 1 (Fig. 3-③). Locally, each branch will train the global model and send back the updated parameters as in Fig. 3-④. The server sets a time t_{d2} for branches to locally train their data and send the parameter updates. Some branches might fail in accomplishing training within this deadline due to large datasets. Moreover, some branches packets might be lost in the network and therefore, they will not be selected for the aggregation process.
- **Aggregation Phase:** In the cloud, the uploaded parameters are aggregated to create the new global model through a secure framework (Fig. 3-⑤). In this framework, the server implements the Fed-NN algorithm to hinder the communication costs. The global model is then updated by storing the model checkpoints (Fig. 3-⑥). Finally, we proceed to phase 1 in the $(i+1)$ round time.

3. *Federated Neural Network Algorithm (Fed-NN) with branch selection:* The Fed-NN addresses a real-time accurate prediction while maintaining privacy using FedAvg strategy, neural networks and the branch selection protocol. The pseudo-code of Fed-NN is presented in Algorithm 2 and it incorporates the following steps:
   - The server initializes the global learning model and sets a deadline t_{d1} for a limited n number of branches to open a bi-directional stream.
   - The server broadcasts the training model to the selected branches where each branch trains the neural network model based on local data and an SGD optimization problem.

- Each branch trains the model on a mini-batch input/output series to respect the given deadline.
- The loss function h_ω is then calculated in each branch until convergence is reached.
- Weights are sent to the server from each branch in t_{d2} selected deadline and the server aggregates the weights and creates a new global model.

5. Experimentation

5.1. Simulation Setup

Simulations in this section are all conducted using TensorFlow in Python 3.6. We select the first 80% of the data to train our model and 20% for testing it. Input attributes are normalized. The work is conducted on a PC running 64-bit Windows 10 ProEducation on an Intel Core i7-8700T CPU and using 16 GB of memory.

In order to precise the accuracy of our predictions, we adopt the following evaluation metrics: mean absolute error (MAE), mean squared error (MSE), accuracy, where y_i resembles the true thermal comfort state and $\hat{y}_p$ is the predicted state.

$$MAE = \frac{1}{N}\sum_{i=1}^{N}|y_i - \hat{y}_p| \tag{4}$$

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_p)^2 \tag{5}$$

$$accuracy = \frac{Number\ of\ correct\ predictions}{Total\ number\ of\ prediction\ made} \tag{6}$$

Data are collected from a one-year longitudinal case study of workers' thermal comfort in an air-conditioned office building in Center City Philadelphia, USA [32]. Thermal comfort data were collected every 15 minutes between the period of July 2012 and August 2013. There are 678 621 data samples in total related to four categories:

1. Indoor attributes include ambient temperature, relative humidity, mean radiant temperature, carbon dioxide concentration, and air velocity.
2. Outdoor attributes include ambient temperature, relative humidity, and air velocity.
3. Buildings heating and ventilation attributes include thermostat set-point and cooling set-point.
4. Worker's attributes include clothing insulation and activity level (metabolic rate).

Fig. 4 shows the variation in the value of the previously indicated input attributes. The comfort output state is divided equally between the two states. The outdoor temperature varies between −10 and 30 degrees. The outdoor humidity ranges between 20 and 100. The outdoor air velocity has values between 0 and 10. The metabolic rate has a small range related to the fact that workers in the office usually have three positions: sitting, standing, or walking. Figure 5 reveals the correlation between each attribute and the other. Our focus is concentrated on the correlation between the comfort state and any other input parameter. It can be obvious that the thermal comfort state has a high correlation with the outdoor temperature as well as the clothing insulation. Besides, the cooling set-point and the metabolic rate have a positive little correlation with the comfort state.

The mini-batch SGD is used in both the server and the branches for model optimization. Data was split equally to serve 100 branches. Throughout simulations, the local mini-batch size is $l = 100$, the learning rate $\eta = 0.002$ and $|\mathcal{K}| = 50$.

5.2. Fed-NN Model Design

In order to ensure the performance of our model, the right hyperparameters of the neural network model must be selected. These hyperparameters include the input layer size, the hidden layers number, and the hidden units in each hidden layer. From a neural network model perspective, the number of hidden layers should not be too large or too little. Therefore, we have to perform a grid search approach to figure out the best design for our Fed-NN model. So, we examined the performance of our model based on different hyperparameter selections as shown in Table 1. The MAE, MSE, and accuracy metrics are evaluated after configuring the Fed-NN model with $(1, 2, 3)$ hidden layers and $(50, 100, 200)$ hidden units. Results show that the best architecture with optimal values of hyperparameters for the Fed-NN model is two hidden layers with 50 units each.

Table 1: Architecture of Fed-NN for Thermal Comfort Prediction (HL: Hidden Layers)

HL	Hidden Units	MAE	MSE	Accuracy
1	50	0.2192	0.14012	0.6379
	100	0.2187	0.1397	0.6368
	200	0.2015	0.1408	0.7379
2	***50, 50***	***0.1164***	***0.1065***	***0.8039***
	100, 100	0.1577	0.1404	0.7321
	200, 200	0.1889	0.1399	0.7704
3	50, 50, 50	0.2183	0.1411	0.7735
	100, 100, 100	0.2197	0.1386	0.6972
	200, 200, 200	0.2138	0.1431	0.6917

5.3. Thermal Comfort Prediction Accuracy

In this section, we compare the performance of the Fed-NN algorithm with different centralized machine learning algorithms: the neural network (NN), the support vector machine (SVM), and multiple linear regression (MLR) of which are considered with good performance for prediction. The prediction evaluation metrics are presented in Table 2 where the same dataset is trained on all machine learning models. The results illustrate that the MAE of Fed-NN is higher than that of NN and lower than those of SVM and MLR. Precisely, the MAE of Fed-NN is 63.8% lower than SVM and 38.1% lower than MLR. This is because Fed-NN inherits the prediction performance of NN. That is, the crux structure of Fed-NN is NN. Hence, the

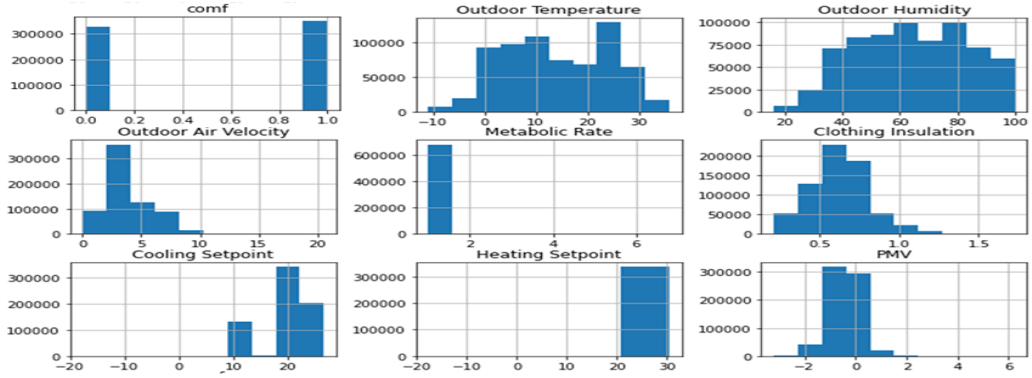

Figure 4: The count (on y-axis) of the different values of the input attributes. Note that different y-axis scales indicate the presence of outliers.

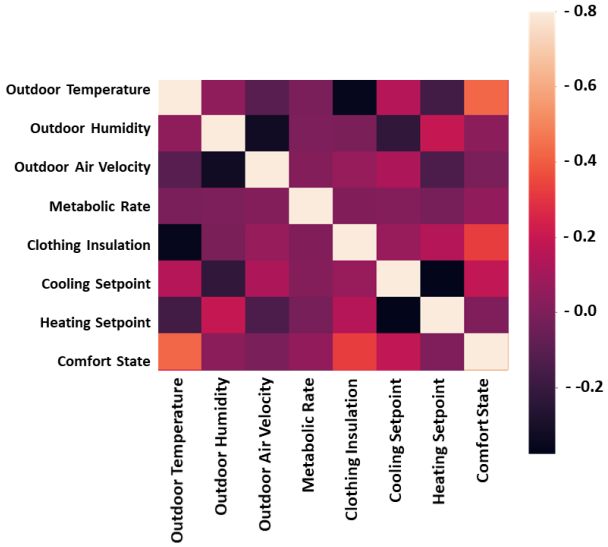

Figure 5: The correlation between the input variables and the comfort state (comf).

MAE value proves the stability of Fed-NN and the ability of Fed-NN to accurately predict thermal comfort state same as the NN model while preserving privacy.

Table 2: Performance comparison between Fed-NN and other machine learning algorithms

	MAE	MSE	Accuracy
Fed-NN (default-settings)	0.1164	0.1065	0.8039
NN	0.1032	0.1004	0.8522
SVM	0.3216	0.2145	0.6411
MLR	0.1881	0.1879	0.7954

5.4. Performance of Fed-NN depending on Branch Number

When comparing the accuracy of Fed-NN to other machine learning models, the number of branches is set to $K = 5$. Nonetheless, in a real industrial IoT environment, the number of branches increases depending on the size of the industry. In this section, we investigate the performance of the Fed-NN algorithm with branch selection protocol compared to the FedAvg algorithm.

Figure 6 shows the results of the MAE metric comparison between the FedAvg algorithm and the Fed-NN algorithm as the number of branches increase. We can notice that the number of clients affects the performance of both algorithms. This is due to the fact that more participating branches increase the communication overhead, which decrements the ability of the cloud to perform gradient aggregation.

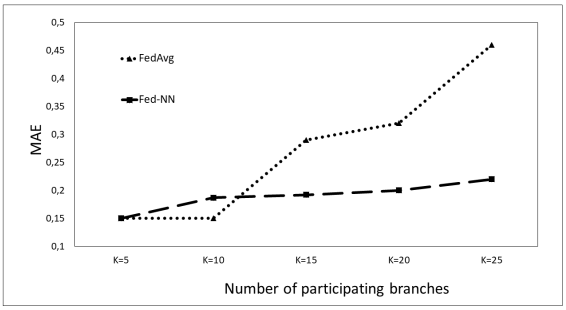

Figure 6: MAE prediction error evolution in FedAvg and Fed-NN as number of branches increases.

In this paper, we have taken advantage of the notion of FedAvg algorithm as it is able to overcome the expensive overhead communication. The FedAvg alleviates the communication overhead by measuring the gradient locally on each branch and then aggregating the gradient from all branches. However, Fig. 6 shows that FedAvg results in a good performance when the number of branches is less than $K = 10$. As the number exceeds this threshold, the performance of the FedAvg algorithm starts to deteriorate. The reason behind this decline is that when the number of branches is above $K = 10$, the probability of branch's failure increases leading to false gradient calculations, which affects the performance of the new global model [31]. Therefore, we designed the Fed-NN algorithm for large industrial IoT algorithms.

Through the branch selection protocol, we will randomly select a subset of branches to participate in the i-th round training. Therefore, in Fig. 6 and 7 the values $K = 5, 10, 15, 20, 25$

for FedAvg algorithm reflects the participation ratio $r = 10\%, 20\%, 30\%, 40\%, 50\%$ for $K = 50$ in Fed-NN algorithm. Fig. 6 shows that when $K = 25$ ($r = 50\%$) the MAE difference between Fed-Avg and Fed-NN is the highest. However, when the $K = 10$ ($r = 20\%$) the MAE of FedAvg was lower than that of Fed-NN as FedAvg results in high performance when $K \leqslant 10$. The graph shows that the performance of Fed-NN is not affected by the increase in the number of participated branches. Hence, the protocol is robust to the number of participants.

We also compare the communication overhead in both Fed-NN and FedAvg algorithms (see Fig. 7). It can be significantly demonstrated that Fed-NN with branch selection has better performance than the FedAvg algorithm. Precisely, the Fed-NN reduces the communication overhead by more than 50% when the branch number is $K = 25$ ($r = 50\%$). The figure shows that the performance of Fed-NN is not affected by the number of participated branches. This is due to the branch selection protocol that undergoes sub-sampling on the participated branches before training the model locally.

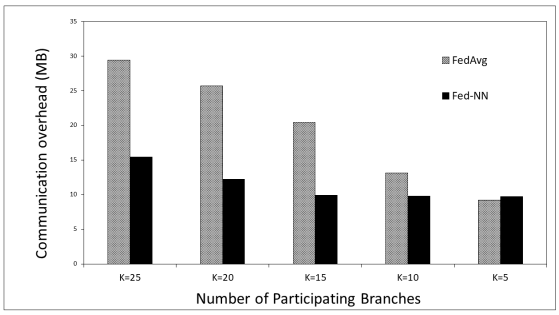

Figure 7: Communication Overhead comparison between FedAvg and Fed-NN depending on number of participating branches.

In Fig. 8, we present the loss of the Fed-NN model with different participation ratios r. It can be inferred that r has no impact on the convergence of the model. But, it has an effect on the loss of the model at the beginning of the training period (higher r results in a higher loss at the beginning). Accordingly, Fed-NN can result in an efficient, robust, and stable thermal comfort prediction model.

5.5. Discussion

In this section, we will investigate the merits of our proposal, Fed-NN algorithm, based on the above-derived results.

1. The core importance of our algorithm lies in the communication overhead reduction in large-scale industrial IoT environments where the FedAvg shows some limitations. The Fed-NN algorithm uses a branch selection protocol at each round of training, which decreases the communication overhead.
2. Some branches might fail in communicating with the server at a round time. This will result in the synchronization failure of the global model and may lead to a deviation of the local branch model from the global one affecting the next global model. To solve this problem, we randomly sub-sample the selected branches to participate in the round training that was not taken into consideration in the development of FedAvg. This will help alleviate the out-of-sync problem.

5.6. Information Privacy Interpretation

In this section, we will present the privacy-preserving concerns taken in the Fed-NN algorithm according to the analog of information privacy.

- Access to worker's data: Fed-NN is proposed based on an FL structure, which is designed as a distributed privacy-preserving platform. Precisely, the Fed-NN algorithm aggregates encrypted gradients to predict accurately worker's thermal comfort state without sharing raw data guaranteeing data protection.
- Experiments reveal the performance of the Fed-NN model when compared to other machine learning models that use a high amount of raw data to predict the thermal comfort state. Besides, the Fed-NN model derives a trade-off between privacy and accuracy, unlike all centralized machine learning models demonstrating its preeminence.

6. Conclusion

This paper proposes a Fed-NN algorithm for decentralized federated thermal comfort prediction for workers in Industry 4.0 under information privacy concerns. The algorithm trains a global thermal comfort prediction model by performing secure gradient information aggregation rather than directly accessing each branch's information data. We demonstrate the accuracy of the Fed-NN model by using real data where it was compared to other centralized machine learning models: SVM and MLR. Results show the capability of Fed-NN to predict the thermal comfort state in a private manner comparably to the centralized machine learning models used. We also testified the ability of our proposal to learn an accurate global model when the number of participating branches increases using the branch selection protocol. The communication overhead in the Fed-NN decreased by 50% when compared to the FedAvg algorithm. For future work, we are planning to apply our model to a real implemented industrial IoT environment.

CRediT authorship contribution statement

Maysaa Khalil: Conceptualization, Methodology, Software, Writing - original draft, Writing - review & editing. **Moez Esseghir:** Conceptualization, Review, Supervision. **Leila Merghem-Boulahia:** Conceptualization, Review, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

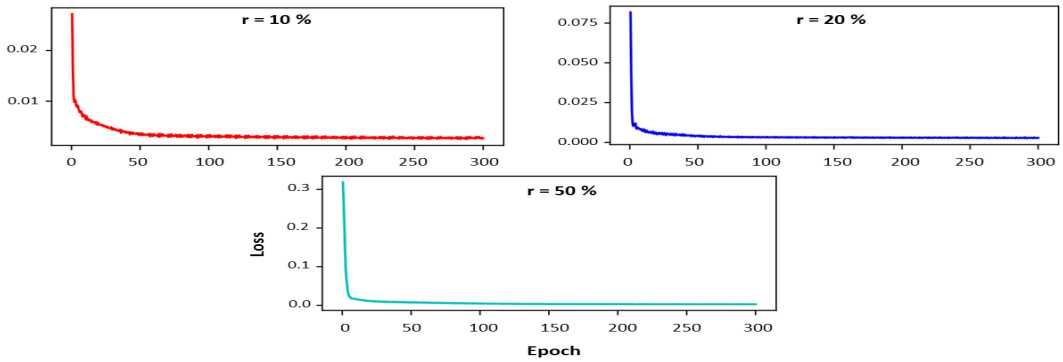

Figure 8: Loss of Fed-NN with respect to different ratio of branch participation, where the loss indicates the MAE value.

Acknowledgment

This work is partly supported by grants from Troyes Champagne métropole and the Conseil Départemental de l'Aube.

References

[1] R. Sahba, R. Radfar, A. R. Ghatari, A. P. Ebrahimi, Development of industry 4.0 predictive maintenance architecture for broadcasting chain, Advanced Engineering Informatics 49 (2021) 101324.

[2] J. Ploennigs, A. Ahmed, B. Hensel, P. Stack, K. Menzel, Virtual sensors for estimation of energy consumption and thermal comfort in buildings with underfloor heating, Advanced Engineering Informatics 25 (4) (2011) 688–698.

[3] L. Lan, P. Wargocki, Z. Lian, Optimal thermal environment improves performance of office work, Rehva Journal 49 (1) (2012) 12–17.

[4] M. Valinejadshoubi, O. Moselhi, A. Bagchi, A. Salem, Development of an iot and bim-based automated alert system for thermal comfort monitoring in buildings, Sustainable Cities and Society 66 (2021) 102602.

[5] X. Luo, L. O. Oyedele, A. O. Ajayi, C. G. Monyei, O. O. Akinade, L. A. Akanbi, Development of an iot-based big data platform for day-ahead prediction of building heating and cooling demands, Advanced Engineering Informatics 41 (2019) 100926.

[6] Z. Fang, T. Tang, Z. Zheng, X. Zhou, W. Liu, Y. Zhang, Thermal responses of workers during summer: An outdoor investigation of construction sites in south china, Sustainable Cities and Society 66 (2021) 102705.

[7] M. Khalil, M. Esseghir, L. Merghem-Boulahia, Applying iot and data analytics to thermal comfort: A review, Machine Intelligence and Data Analytics for Sustainable Future Smart Cities (2021) 171–198.

[8] F. Jazizadeh, W. Jung, Personalized thermal comfort inference using rgb video images for distributed hvac control, Applied Energy 220 (2018) 829–841.

[9] G. Ozcelik, B. Becerik-Gerber, Benchmarking thermoception in virtual environments to physical environments for understanding human-building interactions, Advanced Engineering Informatics 36 (2018) 254–263.

[10] P. K. Sharma, J. H. Park, K. Cho, Blockchain and federated learning-based distributed computing defence framework for sustainable society, Sustainable Cities and Society 59 (2020) 102220.

[11] M. Khalil, M. Esseghir, L. Merghem-Boulahia, An IoT environment for estimating occupants' thermal comfort, in: 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications, 2020, pp. 1–6.

[12] E. Laftchiev, D. Nikovski, An IoT system to estimate personal thermal comfort, in: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), IEEE, 2016, pp. 672–677.

[13] C. Manna., N. Wilson., K. N. Brown., Personalized thermal comfort forecasting for smart buildings via locally weighted regression with adaptive bandwidth, in: Proceedings of the 2nd International Conference on Smart Grids and Green IT Systems - Volume 1: SMARTGREENS,, INSTICC, SciTePress, 2013, pp. 32–40. doi:10.5220/0004375100320040.

[14] K. Liu, T. Nie, W. Liu, Y. Liu, D. Lai, A machine learning approach to predict outdoor thermal comfort using local skin temperatures, Sustainable Cities and Society 59 (2020) 102216.

[15] S. Bin, Y. Wenlai, Application of gaussian process regression to prediction of thermal comfort index, in: 2013 IEEE 11th International Conference on Electronic Measurement Instruments, Vol. 2, 2013, pp. 958–961.

[16] W. Zhang, W. Hu, Y. Wen, Thermal comfort modeling for smart buildings: A fine-grained deep learning approach, IEEE Internet of Things Journal 6 (2) (2019) 2540–2549.

[17] S. Atthajariyakul, T. Leephakpreeda, Neural computing thermal comfort index for hvac systems, Energy conversion and management 46 (15-16) (2005) 2553–2565.

[18] H. Lee, C. R. Ahn, N. Choi, Fine-grained occupant activity monitoring with wi-fi channel state information: Practical implementation of multiple receiver settings, Advanced Engineering Informatics 46 (2020) 101147.

[19] R. Shokri, V. Shmatikov, Privacy-preserving deep learning, in: Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, 2015, pp. 1310–1321.

[20] F. Zhu, W. Wu, Y. Zhang, X. Chen, Privacy-preserving authentication for general directed graphs in industrial IoT, Information Sciences 502 (2019) 218–228.

[21] Y. Jiang, Z. Luo, Z. Wang, B. Lin, Review of thermal comfort infused with the latest big data and modeling progresses in public health, Building and Environment 164 (2019) 106336.

[22] B. McMahan, E. Moore, D. Ramage, S. Hampson, B. A. y Arcas, Communication-efficient learning of deep networks from decentralized data, in: Artificial Intelligence and Statistics, PMLR, 2017, pp. 1273–1282.

[23] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečnỳ, S. Mazzocchi, H. B. McMahan, et al., Towards federated learning at scale: System design, arXiv preprint arXiv:1902.01046 (2019).

[24] K. Bonawitz, F. Salehi, J. Konečnỳ, B. McMahan, M. Gruteser, Federated learning with autotuned communication-efficient secure aggregation, in: 2019 53rd Asilomar Conference on Signals, Systems, and Computers, IEEE, 2019, pp. 1222–1226.

[25] T. Nishio, R. Yonetani, Client selection for federated learning with heterogeneous resources in mobile edge, in: ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–7.

[26] Y. Chen, X. Qin, J. Wang, C. Yu, W. Gao, Fedhealth: A federated transfer learning framework for wearable healthcare, IEEE Intelligent Systems 35 (4) (2020) 83–93.

[27] X. Li, H.-l. Chi, W. Lu, F. Xue, J. Zeng, C. Z. Li, Federated transfer learning enabled smart work packaging for preserving personal image information of construction worker, Automation in Construction 128 (2021) 103738.

[28] X. Yuan, X. Wang, C. Wang, J. Weng, K. Ren, Enabling secure and fast indexing for privacy-assured healthcare monitoring via compressive sensing, IEEE Transactions on Multimedia 18 (10) (2016) 2002–2014.

[29] T. Li, A. K. Sahu, A. Talwalkar, V. Smith, Federated learning: Challenges,

methods, and future directions, IEEE Signal Processing Magazine 37 (3) (2020) 50–60.
[30] T. Li, M. Sanjabi, A. Beirami, V. Smith, Fair resource allocation in federated learning, arXiv preprint arXiv:1905.10497 (2019).
[31] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, V. Chandra, Federated learning with non-iid data, arXiv preprint arXiv:1806.00582 (2018).
[32] J. Langevin, P. L. Gurian, J. Wen, Tracking the human-building interaction: A longitudinal field study of occupant behavior in air-conditioned offices, Journal of Environmental Psychology 42 (2015) 94–115.

Maysaa Khalil received the B.S. degree in computer science from the Lebanese University (LU), Beirut, Lebanon in 2017 and the M.S. degree in electrical engineering for smart grids and buildings from the Ecole Nationale Supérieure de l'Energie, l'Eau et l'Environnement (Grenoble INP-ENSE3), Grenoble, France in 2019. She is currently working toward the Ph.D. degree in computer science in the Environment and Autonomous Network Laboratory, University of Technology of Troyes, France. Her research interests include new privacy-preserving edge computing designs for thermal/energy management in smart buildings, the Internet of Things, and Federated Learning.

Moez Esseghir received the National Engineer Diploma degree in computer sciences from the Ecole Nationale des Sciences Informatique (ENSI), Tunis, Tunisia, in 2002, the Master of Science degree in networks from the University of Paris 6, Paris, France, in 2003, the M.S. degree in computer sciences from ENSI in 2004, and the Ph.D. degree in computer sciences from the University of Paris 6 in 2007. In 2008, he was with North Carolina State University, Raleigh, USA, as a Visiting Scholar. Since 2008, he has been an Associate Professor with the University of Technology of Troyes, France, and the Leader of ERA Research Team since 2017. He has authored or coauthored over 40 publications, including international journals and conferences. His research interests include energy management, resource allocation, and performance evaluation in different kind of networks, such as HetNets, WSN, CRN, VANET, smart grids, cloud environment, and Internet of Things. He actively participated in numerous projects and has served as a technical program committee member and a reviewer for well-known international conferences and journals. He is a member of ACM and IEEE Computer Society.

Leila Merghem-Boulahia received the engineering degree in computer science from the University of Sétif, Algeria, in 1998, the M.S. degree in artificial intelligence and the Ph.D. degree in computer science from the University of Paris 6, France, in 2000 and 2003, respectively, and the Habilitation ádiriger des recherches degree in computer science from the University of Compiégne in 2010. She is a Full Professor with the University of Technology of Troyes, France. She has authored or coauthored over 90 international journals and conference papers.Her main research topics include multi-agent systems, quality of service man-agement, autonomic networks, cognitive and sensor networks, smart grids,and Internet of Things. She was a recipient of the Best Paper Award of the IFIP WMNC2009 and GIIS2013. She also acted as a TPC Member of many conferences and workshops, such as IEEE Globecom, IEEE ICC, and IEEE WCNC. She has served as a Reviewer for internationally well-known journals,such as the IEEE COMMUNICATIONS LETTERS, *Communication Networks*, *Computer and Communications Networks*, and the *International Journal of Network Management*.