frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 17 March 2023
DOI 10.3389/fenrg.2023.1061779

OPEN ACCESS

EDITED BY
Xin Ning,
Institute of Semiconductors (CAS), China

REVIEWED BY
Zhekang Dong,
Hangzhou Dianzi University, China
Ghulam Hafeez,
University of Engineering and Technology, Mardan, Pakistan
Zhibin Zou,
University at Albany, United States
Hongwu Peng,
University of Connecticut, United States

*CORRESPONDENCE
Nan Zhang,
znan0602@163.com

SPECIALTY SECTION
This article was submitted to Smart Grids, a section of the journal Frontiers in Energy Research

RECEIVED 05 October 2022
ACCEPTED 07 March 2023
PUBLISHED 17 March 2023

CITATION
Li W, Zhang N, Liu Z, Ma S, Ke H, Wang J and Chen T (2023), A trusted decision fusion approach for the power internet of things with federated learning. *Front. Energy Res.* 11:1061779. doi: 10.3389/fenrg.2023.1061779

A trusted decision fusion approach for the power internet of things with federated learning

Wenjing Li[1], Nan Zhang[1]*, Zhu Liu[1], Shiqian Ma[2], Huaqiang Ke[1], Jinfa Wang[1] and Ting Chen[1]

[1]State Grid Information & Telecommunication Group Co., Ltd., Beijing, China, [2]State Grid Tianjin Electric Power Company, Tianjin, China

The power Internet of Things generates a large amount of data at any time, which can be transformed into precise decisions with the help of artificial intelligence approaches. However, the owners of electricity data with boundaries are often concerned with data leakage. Therefore, when building models that feed big data into deep learning artificial intelligence approaches for precise decision-making within the power Internet of Things, it is essential to ensure the data's security. This paper proposes a framework for model training and decision making system applied to the field of power IoT, which consists of two parts: data security sharing and hierarchical decision making. The proposed framework utilizes a homomorphic encryption-based federated learning approach to protect private data from leakage. In addition, data augmentation and transfer learning are used to address the issue of insufficient local training data. Moreover, the framework attempts to incorporate the specialized nature of traditional manual decision-making in the power field by fusing expert and model values after stratifying the requirements. Experiments are conducted to simulate the decision requirements in the field of power Internet of Things (e.g., electrical material identification), using image recognition as an example. The experimental results show that the proposed models can achieve high accuracy rates and the fusion approach is feasible.

KEYWORDS

smart grid, power internet of things, data security sharing, federated learning, deep learning

Introduction

In recent years, the rapid development of science and technology has facilitated the gradual integration of Internet of Things (IoT) technology into various aspects of people's daily lives, making it an integral and closely connected part of modern life. IoT technology has an important role in public services (Wu and Xiao, 2022), smart homes (Choi et al., 2021), medical security (Wu et al., 2020), labour free farms (Ratnaparkhi et al., 2020) and smart grids (Alhariry et al., 2021), which brings a lot of convenience to people's lives. Power IoT constitutes a crucial component of IoT development, which can provide important support for the intelligence, digitalization and transparency of the electricity grid through the collection and transmission of electricity grid data to cloud platform for processing and analysis (Zhang et al., 2022a).

Modern society is highly dependent on electric energy, which is related to the people's lives and the stability of the country, and is a strategic energy source for the country (Li et al.,

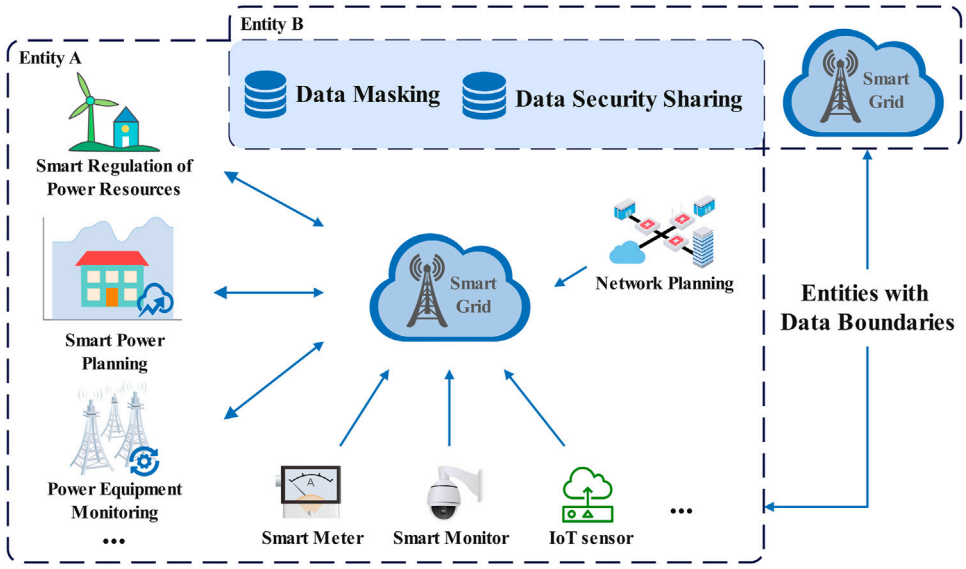

FIGURE 1
Entities with data boundaries.

2020). A smart grid is the integration of a traditional power grid with a communication system and network (Mashal, 2022), which is also one of the most important applications of IoT (Gunduz and Das, 2020). The application of IoT in the smart grid is called power IoT. Power IoT generates a large amount of data under the edge cloud architecture, and the way these data are processed is very critical (Jiang et al., 2020). Effectively utilizing such data through advanced methods like machine learning can help power companies make accurate and informed decisions, leading to a significant improvement in economic efficiency (Gilanifar et al., 2020).

However, the current power IoT still in need of effective solutions for data security sharing and decision-making. The direct collection of electricity consumption data from customers for efficient energy management is insecure from an information point of view (Wang et al., 2021). For example, users regularly report electricity consumption data to the power company through smart meters, thereby rendering their privacy exceedingly vulnerable (Xia et al., 2022). Consequently, the privacy, security and trustworthiness of data remain unconsidered in the current power IoT. The research of user information security for power data has become a hot research topic (Yan et al., 2020).

With the continued promotion of information technology in today's society, data has become increasingly valuable to humans (Corallo et al., 2022) and fine-grained security management in the IoT requires effective access control (Pal et al, 2022). However, the data collected in power IoT is often diverse and data-intensive. A large scale of data makes old supporting parsing systems and decision-making systems seem overwhelming in their presence, leading to a situation where it is challenging to tap into the total value of more data in the field.

Figure 1 shows a simple schematic of smart grids in the area of the Internet of Things for electricity. A smart grid with a well-arranged IoT path can be used to rationalize the deployment of power resources or to efficiently identify the level of wear and tear of power equipment by obtaining data from smart city devices (e.g., smart meters, smart monitors and high-performance IoT sensors). It is worth noting that most electricity data is private data, and for entities with boundaries, a secure way of sharing data is required, e.g., data masking and federated learning. However, potential security threats, such as reconstruction attacks, membership inference and model inversion, may arise in this scenario.

With the *introduction* of emerging concepts such as Industry 4.0 (Hong et al., 2021; Priya et al., 2021), the industrial and power IoT sector has put forward new requirements for mining and utilizing various electricity data. The industry is eager to obtain sufficient data from smart meters (Ahammed and Khan, 2022) or other intelligent power devices for decision-making purposes, such as using power consumption data for rational allocation of power resources, using power equipment implementation images for equipment wear and tear identification and early warning, using images data to ensure physical security of IoT devices (Yang et al., 2022) and using cross-regional electricity data to develop top-level strategies with solid generalization.

Data such as customer usage information, regional distribution lines, and internal electricity equipment is often identified as private data that needs protection. However, there exists a scarcity of credible data that can be controlled by the decision-making entities themselves on a national or even global basis. Such entities may include many electricity companies, regions, or even countries with boundaries. The difficulty in aggregating data across regions to derive practical benefits while ensuring data privacy protection poses significant challenges for these decision-making entities. Furthermore, existing machine learning methods that rely on data suffer from issues related to accuracy and reliability. With the development of the smart grid, the safety of electric power materials has attracted widespread attention, and the safety of electric power equipment is a key part of it. Since power equipment may cause some safety accidents due to overheating,

effective identification and temperature detection of power equipment is extremely important, which can guarantee the safety of the energy supply (Ni, 2020).

Traditional power IoT business decision-making relies on experts' professional experience and knowledge, with layers of feedback and modifications before making decisions. This approach relies heavily on expert authoritative knowledge, and requires reconstructing the expert knowledge base if the structure of the power IoT changes. At the same time, the accuracy of the decisions made using this approach gradually decrease over time due to the accumulation of obsolete knowledge. Spending a lot of cost to update the knowledge base is often not a good choice. To address these challenges, more and more companies are building their automated decision-making solutions, hoping to fully exploit the value of power IoT data with the assistance of computers. However, these decision-making systems are typically based on traditional data analysis methods, and many aspects require manual intervention, which is time-consuming and low resource utilization. Traditional decision-making systems for the power IoT are often based on a small data level of model training, which may have problems with effectiveness and generalization. It is worth noting that traditional electricity decision-making systems have difficulty ensuring the secure sharing of data across regions. Private data cannot be secured, significantly impacting the power IoT if the data is compromised. Fortunately, research for artificial intelligence decision-making systems has also been in order at recent stages (Kaur et al., 2022). Many teams are studying the decision task of introducing artificial intelligence methods into the field of power Internet of Things, which is also the place to explore in this field. It is still a challenge to transfer the task from the traditional decision-making method to the application of artificial intelligence. For the traditional machine learning method, a large number of available features are required, while for the deep learning method, a large number of standard available data sets are required.

To address the limitations of the existing decision-making system in the field of power Internet of Things, and maximize the adaptation of new industrial equipment such as smart grid in popularity, the work of this paper integrates traditional expert decision-making and in-depth learning methods. Furthermore, in order to reduce the risk of privacy data leakage, which accounts for a large proportion of data in the field of power Internet of Things, this work also focuses on integrating a new data security sharing method. The proposed data security sharing and decision-making approach for the power IoT consist of two main parts: data security sharing and the decision-making approach. The data security sharing scheme for the power IoT is based on federated learning and homomorphic encryption, which integrates data within each region after determining the boundaries of a specific scenario. The model's performance at small data levels is further improved by using data augmentation and transfer learning. The proposed decision-making approach is a hierarchical model that integrates an expert knowledge base and machine learning (ML) decision-making. The scenario-specific requirements are hierarchically fed into the decision-making system. The machine learning model generates plausible values with expert knowledge base values to produce a decision score. The weighted fusion of models and decisions can reduce the possible effects caused by federated learning features, such as intermediate data being recovered by attackers and leading to leakage (Zhang et al., 2022b).

In summary, the main contributions of this paper are as follows.

- A security-driven decision model is proposed for the power IoT that enables deep learning-based big data analysis and decision-making for the power IoT under high security. Machine learning tools and expert knowledge bases are also integrated into the decision-making process to produce a comprehensive decision result.
- Federated learning is used to ensure the secure sharing of power IoT data by unifying different entities for collaborative training and unified management by a trusted third party without revealing sensitive data. This approach enables reasonable exploitation of data value while ensuring data security.
- Homomorphic encryption is used to prevent malicious activities, such as inference attacks, that may occur in federation learning. Homomorphic encryption processes the data without decryption, thus securing the intermediate data in the power IoT.

The remainder of this paper is organized as follows.

Section 2 provides an overview of the related work. Section 3 focuses on design details and a description of the methods for the power IoT. Section 4 shows the experimental data and analysis of an example scenario, along with a discussion of the results. Section 5 makes a summary of the paper and future perspective.

Related work

In this section, some work similar to the topic of this paper will be presented, mainly covering decision systems and privacy protection elements.

Decision-making methods

Most decision-making methods in the field of power IoT are based on traditional manual analysis or single-user machine learning. Al Metrik and Musleh (2022) proposed a medium-term prediction model that can predict electricity consumption for a given location. Predicting energy use ensures the stability of the power supply. Wang et al. (2022) have constructed a structured LSTM based on a prediction-guided autoencoder. A single model enables the accurate prediction of short-term loans for all types of users. Guang et al. (2021) proposed a decision-making approach. Power communication resource data features are analyzed and combined with data mining algorithms to design and propose intelligent application scenarios geared towards grid and communication network collaboration and assisted decision-making. Tian and Dong (2021) proposed a long-term investment decision model for transmission grid frames containing flexible transmission devices. Due to the nature of the power IoT domain, specific tasks are targeted.

Most decision-making approaches in the power IoT field are based on a single independent machine learning model or other

methods. These methods may work well for specific tasks but are not highly generalizable and will be challenging to extend to other tasks. There is also a risk of privacy breaches in handling sensitive data, which is often not shared securely with the power data.

Data security sharing

Friha et al. (2022) proposed a federated learning-based intrusion detection system. They used federated learning for a specific task (i.e., intrusion detection) to protect the infrastructure of the Internet of agriculture. Their experiments demonstrate the excellence of federated learning in the Internet of agriculture. Image recognition is the main task theme in the IoT for electricity, for example, identifying wear and tear on electrical equipment. Tanwar et al. (2021) proposed a privacy-preserving image recognition model for encrypted data over the cloud. Their proposed block-based image encryption scheme can be effective in securing private images. Bhansali et al. (2022) presented a system with secure data collection and transmission for IoMT architecture integrated with federated learning and illustrated the value of this system in the medical field. The same type of federated learning is used in the medical field, Xu et al. (2021) proposed a general multi-view federated learning approach using multisource data, and it can extend the traditional machine learning model to support federated learning across different institutions or parties. To address the issue of user privacy protection in federated learning, Mugunthan et al. (2020) proposed PrivacyFL, a scalable, easily configurable and extensible simulator for federated learning environments. Miao et al. (2021) proposed a federated learning-based secure data sharing mechanism for IoT called FL2S, which improves data security and data quality. Li et al. (2021) proposed a novel privacy-preserving FL framework based on an innovative chained secure multi-party computing technology called chain-PPFL to address the leakage of participants' sensitive information due to exchanging model data in federated learning.

It is worth noting that the amount of data available for each local user may be very small after applying federal learning, resulting in a certain degree of overfitting and poor accuracy. Therefore, this paper uses federated learning, transfer learning, data augmentation methods, and model weighting fusion methods to improve the model's accuracy.

Materials and methods

In this section, the data security sharing and decision-making approach for the power IoT is introduced.

Problem formulation

This part focuses on abstract modeling of data security sharing and decision-making within the field of power IoT and illustrates the main processes and specific details of the approach proposed in this paper.

Problem description

Consider the set $ENV = \{env_1, env_2, \cdots, env_n\}$ of requirements that may need to be decided within the power IoT, and for each $env \in ENV$, determine the region boundary $LOC = \{loc_1, loc_2, \cdots, loc_m\}$ for collaborative training while dividing the env hierarchically into sub-requirements e_{ij}, where n and m are the total number of requirements and the total number of region boundaries, respectively. i and j are the j^{th} division of the i^{th} layer, respectively.

For the decision approach, the hierarchical output of the plausible decision values Sug_i of the expert knowledge base, combined with the possible values $mValue$ given by the collaboratively trained completed machine learning model $Model$, and results in the corresponding solution set $Solution = \{sol_1, sol_2, \cdots, sol_v\}$, where i is the division of the hierarchy and v is the number of solutions.

For the model to be run so that it can be trained efficiently and give credible decision recommendations, a complete description of the scenario is as follows:

- ***Input:*** i) The basic set of requirements $ENV = \{env_1, env_2, \cdots, env_n\}$ for which decision information may need to be obtained and the region boundaries $LOC = \{loc_1, loc_2, \cdots, loc_m\}$ for collaborative training. ii) A trusted central server $CServer$ for federated learning and a hierarchical algorithm for partitioning requirements. iii) Homomorphic encryption algorithms, models for migration learning, and an expert knowledge base.
- ***Output:*** A set of solutions $Solution = \{sol_1, sol_2, \cdots, sol_v\}$ corresponding to each actual requirement.
- ***Objective:*** Maximize machine learning model accuracy ACC' and complete data security sharing and decision making.

The overall flow of the proposed approach

This paper proposes a data security sharing and decision-making model to solve the problem described in the above scenario. The overall process is shown in Figure 2. The model is divided into three parts: data preparation, regional collaborative training, and output of decision making. Data preparation is mainly responsible for collecting, cleaning, and data augmentation. According to the overall training standard, these parts are mainly carried out in the local area.

The regional collaborative training component is responsible for securely sharing power IoT data. The use of federated learning and homomorphic encryption ensures private data security. The use of migration learning reduces costs and improves training effectiveness on small volumes of data. All methods are carried out under the integration of a trusted central server. The decision output part is mainly responsible for outputting credible decision values given by the decision hierarchy algorithm to give plausible suggested values by the expert knowledge base. The plausible suggested values are weighted and combined with the reasonable discounts offered by the model in the previous session to provide reference values that can be used for decision-making. The first and second of these parts are described in the following sub-section. The detailed step-by-step description is shown below:

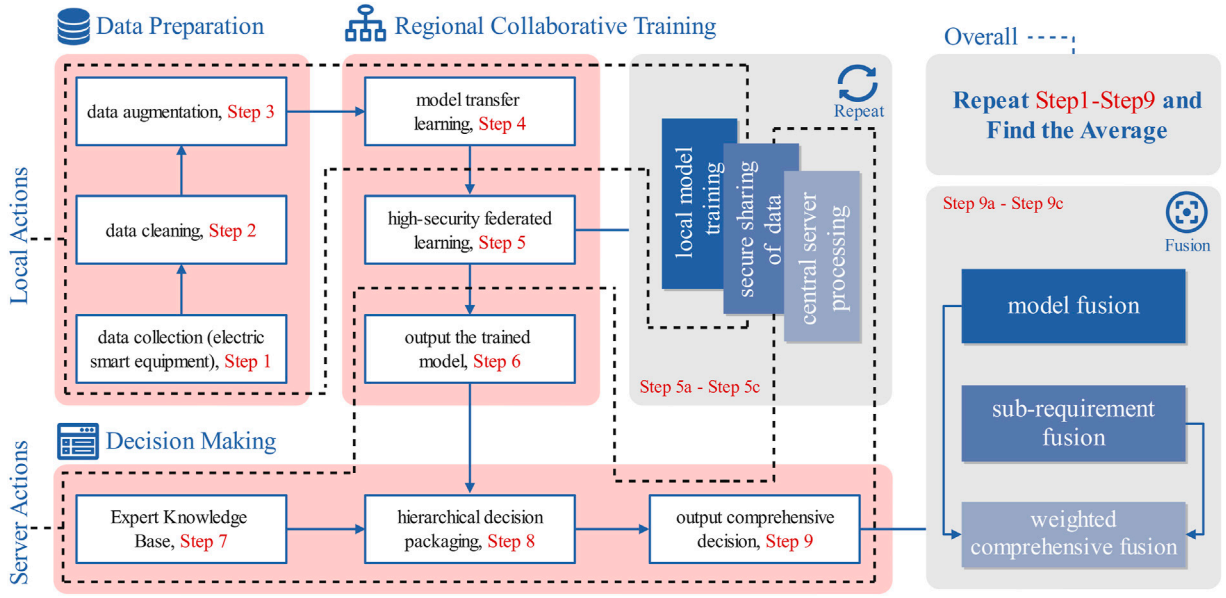

FIGURE 2
Overall flow of model.

- STAGE I: Data preparation

Step 1. Using smart electricity devices, such as smart meters, collect local data. Data collection, in this case, is a locally trusted operation;

Step 2. The regions pre-process private data. The primary check is for data consistency, followed by processing invalid and missing values;

Step 3. Due to the specific features of some of the data in the power IoT, local areas with boundaries often do not share private data with others. The methods of data augmentation vary for different tasks, e.g., for the task of identifying and warning about the wear and tear of power equipment, the main focus is on enhancing the picture data of power equipment;

- STAGE II: Collaborative training

Step 4. The model proposed in this paper evaluates the possibility of applying migration learning in actual experiments for different power IoT decision tasks;

Step 5a. Local model training. Each local model training is done by trusted operations and data;

Step 5b. Use homomorphic encryption to ensure secure sharing of data. Here the intermediate data of the local model training process is encrypted and transmitted to the central server;

Step 5c. The central server averages the local intermediate data and then distributes it to all local models;

Step 6. Output information about the completed training model. There is not necessarily only one model used for transfer in a decision process, and therefore not necessarily only one model information is output;

- STAGE III: Decision making

Step 7. The expert knowledge base is used to support the decision from the other side and is set to 0 if no matching decision information is found.

Step 8. The expert experience is packaged according to a hierarchical approach to electricity demand, all of which is provided to the subsequent decision model;

Step 9a. If multiple models are used in the co-training section, then all models are weighted and fused here;

Step 9b. If multiple sub-requirements are used in the co-training section, then all sub-requirements are weighted and fused here;

Step 9c. Weighted fusion of data from Step 9a and Step 9b.

The data security sharing approach

This part focuses on the first part of the model proposed in this paper, i.e., the data security sharing approach for the power IoT, mainly consisting of data preparation and collaborative training.

Data collection and cleaning

Data is collected by uniform standards for all smart power devices in areas with boundaries. For example, for electricity consumption data, from a uniformly deployed smart meter platform, the data is collected and stored by category number,

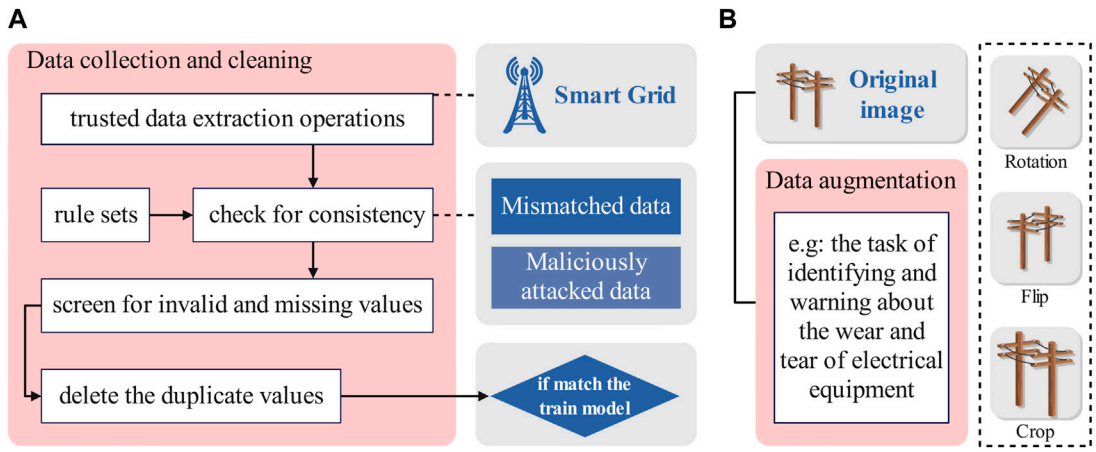

FIGURE 3
Pre-processing stage. **(A)** Data collection and data cleaning **(B)** Data augmentation.

with different regions lending themselves to a uniform standard for implementation between them.

As described in Figure 3A, the regions pre-process the privacy data. The data is first checked for consistency, starting from a prepared rule set and screens for data that does not match the characteristics of the power IoT. For example, the existing electricity theft may influence the data from smart meters (Xia et al., 2021). Then the processing of invalid and missing values is carried out, and the method used in this paper is to use sample means instead of invalid and missing values.

The third step carries out the processing of duplicate values, and the same data are deleted to reduce the model training cost.

Due to the small amount of data in this region, there may be cases where the amount of data is below the standard training threshold set after cleaning. Suppose the training requirements are still not met after data augmentation. In that case, the model proposed in this paper uniformly flags all data in this region with boundaries, and some parameters will be modified in the subsequent training process to reduce overfitting.

Local training data augmentation

Due to the unique data features in the power IoT, local areas with boundaries tend not to share private data with other regions. A possible direct result is that the dataset for local training is extremely limited, and for many machine learning models, the quality of the trained model is largely influenced by the amount of data. This paper uses data augmentation to expand the datasets in the local areas.

As described in Figure 3B, the data augmentation methods vary for different tasks. For example, for the task of identifying and warning about the wear and tear of electrical equipment, the main focus is on augmenting the picture data of electrical equipment. In this paper, the data augmentation methods for tasks involving image recognition include random cropping, image rotation, and flipping.

For random cropping, use the transformation as shown in Formula 1.

$$(l_i, w_i) \leftarrow (\alpha l_i, \beta w_i) \tag{1}$$

where l_i is the length of the i^{th} image, w_i is the width of the i^{th} image, α and β are the parameters in the transformation. Here a tuple is used to store its length and width attributes. Adjust the image to a uniform aspect ratio after cropping:

$$image_i^{'} = resize\left(image_i\right) \tag{2}$$

Where $image_i$ and $image_i^{'}$ are the i^{th} image before and after the random crop is completed, respectively, and $resize(\cdot)$ is a conversion function to maintain the aspect ratio.

For image rotation and flipping, use the transformations shown in Formulas 3, 4:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \tag{3}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} -1 & 0 & w \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \tag{4}$$

where, y and x', y' are the position of pixel points in length and width before and after rotation and flip, respectively. θ is the rotation angle and w is the width of the image.

For other tasks within the power IoT, such as text processing, this paper uses random removal and disruption methods commonly used in the field for text data augmentation.

Transfer learning based on practical assessment

Considering a power IoT decision-making task where a local area with boundaries has only a small amount of controllable data, this paper incorporates the transfer learning method in the proposed model.

Transfer learning transposes a well-established model trained on the source domain with a large amount of data to the target domain with a small amount of local data so that the target model can also achieve excellent results. The model proposed in this paper evaluates the possibility of applying transfer learning in practical experiments for different power IoT decision-making tasks. For example, in the task of identifying and warning about the wear and tear of power equipment, this paper uses a model-based transfer learning algorithm. At the model level, the source and target domains can

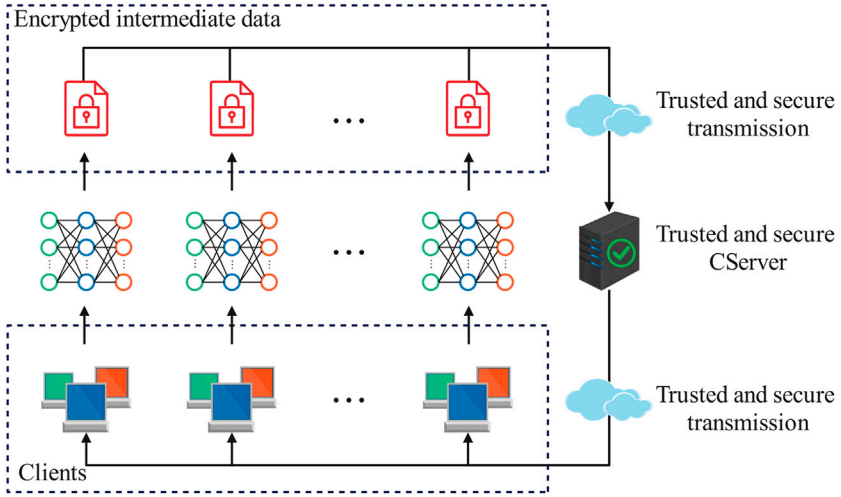

FIGURE 4
Federated learning based on homomorphic encryption.

share some of the parameters and then be trained with fine-tuning in the local domain to obtain a usable target model with stronger generalization performance.

Iterate through local area information to generate LOC;
for rd in range (Round) **do**
for loc_i in LOC **do**
if loc_i meet the requirement **then**
$V_c^i = doEnc(C_i, PK)$
end if
end for
$V_c \leftarrow$ Transmits intermediate data and integrated into the central server
$V_p = UD(V_p^{'}, V_c)$
$V = doDec(V_p, SK)$
for loc_i in LOC **do**
$C_i^{'} = UDLoc(V, C_i)$
end for
end for
return $model$

Algorithm 1. The model with federated learning.

The details of the experiments on the image task are described in the next section.

Federated learning based on homomorphic encryption

Federated learning is a typical example of a small data scale model training approach, where distributed learning can effectively break down the problems caused by "data silos." At the same time, much of the private data that is not expected to be shared can be securely trained in a local bounded area, which is greatly protected by the inclusion of homomorphic encryption.

Simple homomorphic encryption-based federated learning can be easily described. As in Figure 4, suppose there are n local-area data holders $L = \{l_1, l_2, \cdots, l_n\}$, each of whom has private data $D_i\,(i \in [1, n])$ that is not shared. A trusted central server *CServer* is set up, and multiple local-area clients are coordinated by it for collaborative training.

It is further described that each local client freezes the parameters of the first k layers and initializes the remaining layers randomly after determining the original model. The local area client performs a training round and encrypts the intermediate data upon completion:

$$V_c^i = doEnc(C_i, PK) \tag{5}$$

where $doEnc(\cdot)$ is the encryption function, V_c^i is the information of the i^{th} local area client after encrypting the intermediate data, PK is the public key of the encryption process, and C_i is the actual intermediate data of the i^{th} local area client.

The trusted central server receives the encrypted intermediate data from the local area client and performs the parameter update:

$$V_p = UD\left(V_p^{'}, V_c\right) \tag{6}$$

where $V_p^{'}$ is the encrypted intermediate data received by the central server from local clients in the previous round, V_c is the total set of intermediate data received from all local geographical clients ($V_c = \{V_c^1, V_c^2, \cdots, V_c^3\}$), $UD(\cdot)$ is the data processing function of the central server, and in this paper, the averaging method is used, which means that the average of each intermediate data is taken, and after the calculation is completed the central server issues a new round of parameters V_p.

Each local client obtains the latest parameters from the central server, decrypts them with the private key, and receives the actual data in plaintext:

$$V = doDec\left(V_p, SK\right) \tag{7}$$

where V is the latest round's parameters from the central server after decryption, $doDec(\cdot)$ is the decryption function and SK is the private key. The local area client performs the update of the

parameters in the local model based on the data obtained in this round:

$$C_i^{'} = UDLoc(V, C_i) \tag{8}$$

where $C_i^{'}$ is the actual update of the parameters of the model for the i^{th} local area client for this round, $UDLoc(\cdot)$ is the parameter update function for this local area client, V is the decrypted parameters from the central server for the latest round, and C_i is the intermediate data for the i^{th} local area client. The update here generally replaces the parameters with the new decrypted parameters, or a weighted average method can be used. For a more precise description of the algorithm, see Algorithm 1. It has a time complexity of $O(rd{\times}n)$.

The above homomorphic encryption-based federated learning approach for the power IoT also requires a comparison with traditional training methods, assuming that the model's accuracy obtained from the above process is ACC and considering traditional training:

$$Model = Train\left(\bigcup_{i=1}^{n} D_i\right) \tag{9}$$

where $Model$ is the trained model, $Train(\cdot)$ is the abstract process representation of the training process, and the accuracy obtained from $Model$ is represented as ACC'. The following comparisons are generally considered:

$$\Delta A = \left|ACC' - ACC\right| < \delta \tag{10}$$

where δ is a very small non-negative actual number, which has also become one of the criteria for measuring federated learning.

The hierarchical fusion decision model

This sub-section focuses on the second part of the model proposed in this paper, a hierarchical fusion decision model for the power IoT, consisting of two main parts, demand hierarchy, and decision credible value fusion.

Hierarchical power IoT demand

The delineation model is central to this subsection, considering that the actual requirements of the power IoT are often complex and diverse and usually consist of multiple sub-requirements, where individual sub-requirements can clearly unambiguously express the decisional boundaries.

Due to the complex features of the power IoT, existing segmentation methods may not reach the goal. A better solution is to cross natural language processing domain knowledge for automatic delineation or to be supported by an expert knowledge base for delineation. The hierarchical model proposed in this paper focuses on using expert knowledge base support for the delineation. The model subscribes to a single requirement (vectorized when necessary) and retrieves the expert knowledge base to delineate several linked sub-requirements. It is worth mentioning that the hierarchical results are not always optimal.

Decision credible value fusion

This paper introduces a weighted fusion strategy at the decision level, referring to various existing model fusion strategies. It can be shown in Figure 5. The weighted fusion strategy can reduce the impact of errors from the model. Considering the sources of plausible decision values: the data obtained after the completion of federated learning of multiple models and the data provided by the expert knowledge base, the weights of each fusion term should be given after lightweight testing or dynamically adjusted during the iterative training process, and the weighted fusion is given by Formula (11):

$$V = \frac{1}{2m}\sum_{j=1}^{m}\left(\frac{Z_{ML}^{j}}{n}\sum_{i=1}^{n} w_i^j \cdot v_i^j + \frac{Z_{KL}^{j}}{k}\sum_{k=1}^{p} c_k^j \cdot x_k^j\right) \tag{11}$$

Where m, n, and p are the number of decisions, the number of fused models in federated learning, and the number of sub-requirements divided by the expert knowledge base, respectively. Z_{ML}^{j} is the weight on the model side at the j^{th} decision round, and Z_{KL}^{j} is the weight on the model knowledge base side at the j^{th} training round. w_i^j is the weight of the i^{th} model fused in federated learning at the j^{th} decision round, and v_i^j is the result of the i^{th} model fused in federated learning at the j^{th} decision round vector. c_k^j is the weight of the k^{th} sub-requirement divided at the expert knowledge base level at the j^{th} decision round, and x_k^j is the result vector of the k^{th} sub-requirement divided at the expert knowledge base level at the j^{th} decision round. It has a time complexity of $O(m{\times}\max\{n,p\})$.

Results and discussion

In this section, several experiments are conducted to evaluate the model proposed in this paper. In this paper, the proposed model is implemented by PyTorch code framework in Python language and tested on personal computers (PCs) such as i5-7300HQ CPU, GTX1050Ti graphics card and 8 GB RAM. There are many decision-making tasks in the field of power IoT that are worth exploring (e.g., electrical material identification). To better represent the fusion and decision-making approach proposed in this paper, the experimental part will use the power equipment wear and tear assessment task as the primary requirement. Due to the high privacy of power data, the team could not obtain sufficient data, so the experiments mainly used Caltech-256 dataset as an example and attached the data collected by our team. The approach proposed in this paper is fully extensible to specific tasks in the power domain.

Model transfer learning with (Non-) Federated learning

For the image task, this paper uses the VGG-19 and ResNet-50 models for federated learning. Using the transfer learning training dataset, the parameters used in transfer learning are shown in Table 1. For the training process, the transformation formula for the learning rate is shown in Formula (12):

$$\theta_e = \theta_{\min} + \frac{1}{2}(\theta_{\text{init}} - \theta_{\min})\left(1 + \cos\left(\frac{E_{\text{cur}}}{E_{\text{init}}}\right)\right) \tag{12}$$

where θ_{init} is the initial learning rate, θ_{min} is the minimum value of learning rate and is set as 0 in this paper, E_{cur} is the current train epoch.

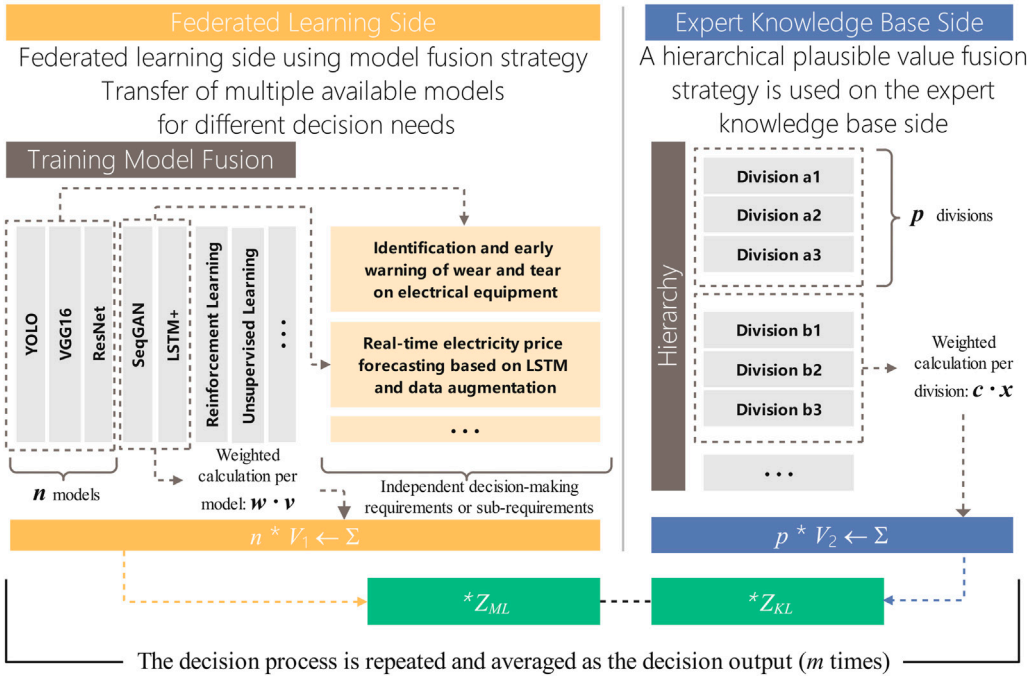

FIGURE 5
Decision confidence value fusion process.

TABLE 1 The parameters used in transfer learning.

Parameters	Value
Batch size	32
Initial learning rate	0.001
Optimizer	SGD
Loss function	Cross entropy

TABLE 2 The parameters used in federated and transfer learning.

Parameters	Value
Batch size	32
Initial learning rate	0.001
Optimizer	SGD
Loss function	Cross entropy
Number of global iterations	30
Local training rounds	2
Regularization parameter	0.5

The models after adding federated learning were evaluated on the server-side for model performance after the intermediate data had gone through FedAvg. It is worth noting that the models used in the experiments in this paper were pre-trained on ImageNet and then downloaded during the first round of training. The experiments used two clients to simulate.

The federated learning scenario, and the transfer learning used the same two models mentioned above, with some specific parameter settings in Table 2.

The effective range of the simulated federation learning used for the experiments in this paper is within a local area network, using homomorphic encryption to ensure secure data transmission. For the security of cross-domain information transmission, it is not considered in this paper for the time being. Also, due to transfer learning, most neural network layers do not need to be updated with parameters, dramatically reducing network communication's burden.

The model training results for the four combinations are shown in Table 3. Excellent accuracy can be achieved for all the mature models selected for training under transfer learning. The two models using federal learning were generally better in terms of accuracy, with the time spent on a single training session varying between models due to the fact that the VGG-19 model used had far more parameters than ResNet-50.

Model fusion

The image task selected as an example in the experiments in this paper is a simple stand-alone task, so fusing sub-requirements will not be considered for use. This part focuses on model fusion. Model fusion allows for better generalization performance of the completed training model and can compensate for possible accuracy problems associated with federated learning. This paper used the model-weighted fusion, which reduces the impact on the overall model due to errors in one

TABLE 3 Transfer learning effects of the two models with (non-)federated learning.

Model	Epoch	Training time (%)	ACC-OPT (%)	ΔA	Security strategy
non-federated transfer learning & VGG-19	30	100	93.6	0.6%	False
non-federated transfer learning & ResNet-50	30	275.07	94.4	≈0%	False
federated transfer learning & VGG-19	60	414.33	94.2	0.6%	True
federated transfer learning & ReNet-50	60	334.96	94.4	≈0%	True
Average		**281.09**	**94.15**	**0.3%**	

Bold values are highlighted for the average of the data in this column.

TABLE 4 Experimental results of model-weighted fusion.

ResNet-50: VGG-19	ACC-OPT (%)	ΔA (VGG-19) (%)	ΔA (ResNet-50) (%)	Security strategy
1.5	94.3	0.7	0.1	True
2.33	95.2	1.6	0.8	True
4	93.1	0.5	1.3	True
9	94.2	0.6	0.2	True
Average	**94.2**	**0.85**	**0.6**	

Bold values are highlighted for the average of the data in this column.

model. When there is a significant difference in structure and performance between the models to be fused, the better performing models are given more substantial weight, and the average performing models are given a lower weight, as shown in Formula (11).

As seen from the experimental results, ResNet-50 outperformed the VGG-19 model in front of the multi-classification task in both experiments with and without federated learning. Therefore, in the model-weighted fusion experiments in this subsection, greater weight was given to ResNet-50. A comparison of the experimental results is shown in Table 4. It can be seen that the best results for model fusion are obtained when the ratio is 2.33, with an optimal accuracy of 95.2%. However, it is worth noting that better than VGG-19 converges faster, and the convergence speed of the fusion model is also affected in the case of its low weights.

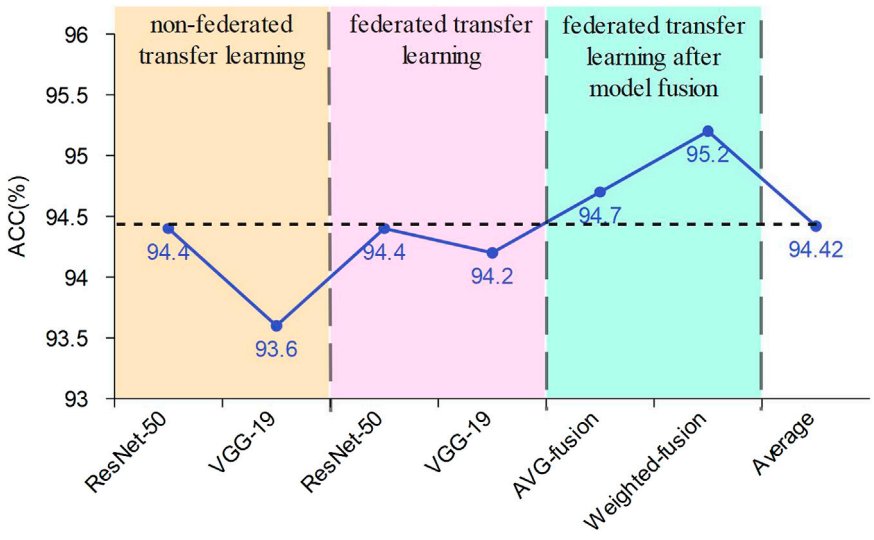

FIGURE 6
The specific experimental comparison data.

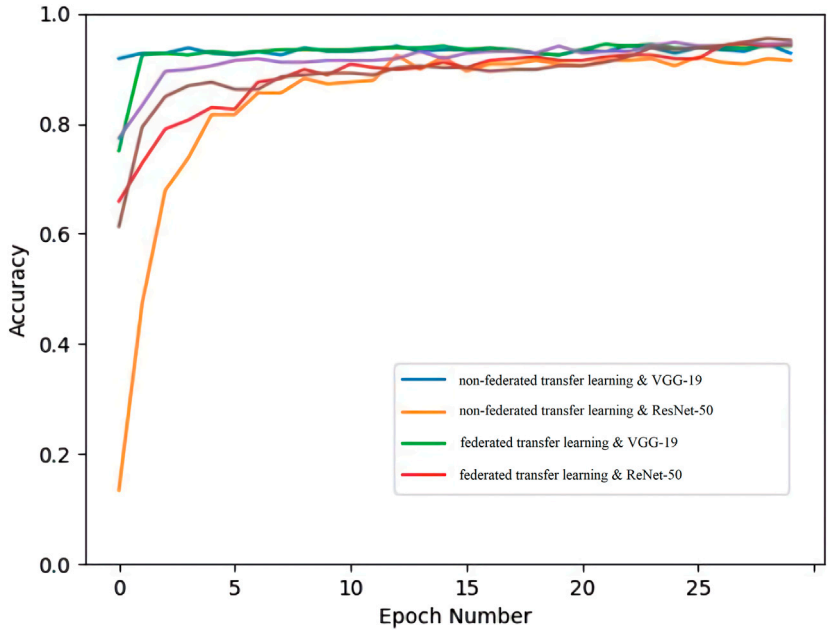

FIGURE 7
Comparison of convergence speed between different combinations.

Overall analysis

The experimental results for the two parts of the model are obtained in the first and second part. At the same time, the corresponding data are also available for the other model fusion method, as shown in Figure 6 for the specific experimental comparison data.

In comparing the best results for this task, model fusion can be optimal, with the weighted fusion method obtaining the first place at 95.2%. However, its convergence is slower in the actual training process. The fusion model is more generalizable than a single model and gives better results.

The weighted calculated result vectors are not listed in the experiments tables, as all experimental results are already expressed in accuracy. As the expert knowledge base requires a certain base reserve, the weight of this part is set to 0 in many tasks of the experiments in this paper, but this is still very scalable for tasks in the field of power IoT. In addition, the experiments in this paper focus on the security protection of electricity data, and the model is more interested in applying a secure method of secure data sharing in the power IoT domain than accuracy. From the data in Tables 3, 4, it can be seen that the experimental group considering the security strategy and the experimental group without incorporating federated learning have less than 1.7% bias in the experimental effect. The decision framework proposed in the text for federated security policies for power IoT can protect independent private data while ensuring accuracy. It improves the confidence level of decision making compared to traditional manual decision making, and it effectively and securely partitions the training data for secure sharing for privacy protection compared to the overall trained model. In addition, the use of models as well as decision-level fusion can be extended to a wide range of power decision tasks in the context of smart grid. It is worth noting that although the proposed approach in this paper is effective in the power IoT domain to ensure that the privacy data used in power tasks are shared securely, its convergence speed is slower than traditional training methods (Figure 7) and requires additional communication time. To test the extensibility of the framework in this paper, we also tested the electricity price forecasting task under smart grid, and the results were similar to this set of experiments, and the secure sharing of private data was ensured from various aspects.

Conclusion and future work

To address the complexity of traditional decision-making methods in the field of power IoT and the privacy protection of power data, this paper introduces homomorphic cryptography-based federated learning to the task of power IoT. Also, transfer learning and model fusion are used to improve the performance of the overall model. This paper also proposes a hierarchical decision model that integrates traditional expert decision making in the power IoT domain and deep learning decision making under new industrial devices, combining machine learning models and plausible values from expert knowledge bases to obtain integrated decisions with excellent results.

Future research will focus on designing new machine learning models for the data characteristics of the power IoT in order to reduce the reliance on transfer models. In addition, we hope to conduct targeted research on data types in the power IoT space to incorporate more advanced security strategies and further adapt to emerging industrial devices such as smart grids.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding authors.

Author contributions

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

Funding

This work is funded by the National Key R&D Program of China (2020YFB0905900); The work is funded by the Science and technology project of SGCC(State Grid Corporation of China): SGTJDK00DWJS2100223.

Conflict of interest

WL, NZ, ZL, HK, JW, and TC were employed by State Grid Information & Telecommunication Group Co., Ltd. SM is employed by State Grid Tianjin Electric Power Company.

The authors declare that this study received funding from State Grid Corporation of China. The funder had the following involvement in the study: A trusted decision fusion approach for the power internet of things with federated learning.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Ahammed, M. T., and Khan, I. (2022). Ensuring power quality and demand-side management through iot-based smart meters in a developing country. *Energy* 250, 123747. doi:10.1016/j.energy.2022.123747

Al Metrik, M. A., and Musleh, D. A. (2022). Machine learning empowered electricity consumption prediction. *CMC-COMPUTERS Mater. CONTINUA* 72 (1), 1427–1444. doi:10.32604/cmc.2022.025722

Alhariry, A., Brown, S., Eshenbaugh, D., Whitt, N., and Browne, A. F. (2021). A survey of sensing methodologies in smart grids. *SoutheastCon* 2021, 9401840. doi:10.1109/SoutheastCon45413.2021.9401840

Bhansali, P. K., Hiran, D., and Gulati, K. (2022). Secure data collection and transmission for iomt architecture integrated with federated learning. *Int. J. Pervasive Comput. Commun.* 2022. (ahead-of-print). doi:10.1108/ijpcc-02-2022-0042

Choi, W., Kim, J., Lee, S., and Park, E. (2021). Smart home and internet of things: A bibliometric study. *J. Clean. Prod.* 301, 126908. doi:10.1016/j.jclepro.2021.126908

Corallo, A., Crespino, A. M., Lazoi, M., and Lezzi, M. (2022). Model-based big data analytics-as-a-service framework in smart manufacturing: A case study. *Robotics Computer-Integrated Manuf.* 76, 102331. doi:10.1016/j.rcim.2022.102331

Friha, O., Ferrag, M. A., Lei, S., Maglaras, L., Choo, K., and Nafaa, M. (2022). Felids: Federated learning-based intrusion detection system for agricultural internet of things. *J. Parallel Distributed Comput.* 165, 17–31. doi:10.1016/j.jpdc.2022.03.003

Gilanifar, M., Wang, H., Ozguven, E. E., Zhou, Y., and Arghandeh, R. (2020). Bayesian spatiotemporal Gaussian process for short-term load forecasting using combined transportation and electricity data. *ACM Trans. CYBER-PHYSICAL Syst.* 4 (1), 1–25. doi:10.1145/3300185

Guang, Z., Tang, J., Li, Y., Fan, X., Song, G., Zhang, N., et al. (2021). Data value mining and auxiliary decision making of power communication service. *Electr. POWER ICT* 19 (10), 5. doi:10.1109/IMCEC51613.2021.9482236

Gunduz, M. Z., and Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* 169, 107094. doi:10.1016/j.comnet.2019.107094

Hong, Q., Chen, Z., Dong, C., and Xiong, Q.: A dynamic demand-driven smart manufacturing for mass individualization production. In: Proceedings of the 2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 3297–3302. (2021). January 2021, Melbourne, Australia, doi:10.1109/SMC52423.2021.9659114

Jiang, G., Su, L., Liu, H., Cao, Y., Sun, R., and Diao, F. (2020). "Constructing the power knowledge graph by multi-source electricity data," in PROCEEDINGS OF THE 2020 INTERNATIONAL CONFERENCE ON COMPUTER, INFORMATION AND TELECOMMUNICATION SYSTEMS (CITS). International Conference on Computer Information and Telecommunication Systems, Hangzhou, China, October 2020. Editors M. Obaidat, K. Hsiao, P. Nicopolitidis, and D. CascadoCaballero, 111–115.

Kaur, D., Uslu, S., Rittichier, K. J., and Durresi, A. (2022). Trustworthy artificial intelligence: A review. *ACM Comput. Surv. (CSUR)* 55 (2), 1–38. doi:10.1145/3491209

Li, Y., Zhou, Y., Jolfaei, A., Yu, D., Xu, G., and Zheng, X. (2021). Privacy-preserving federated learning framework based on chained secure multiparty computing. *IEEE INTERNET THINGS J.* 8 (8), 6178–6186. doi:10.1109/JIOT.2020.3022911

Li, Z., Liu, J., and Jin, Y. (2020). Analysis of load characteristics changes in the case of large-scale electric energy substitution load connected-in. *IOP Conf. Ser. Earth Environ. Sci.* 446 (4), 042085. doi:10.1088/1755-1315/446/4/042085

Parimala, M., Priya, R. M. S., Pham, Q., Dev, K., Maddikunta, P. K. R., Gadekallu, T. R., et al. (2021). Fusion of federated learning and industrial internet of things: A survey. https://arxiv.org/abs/2101.00798.doi:10.48550/arXiv.2101.00798

Mashal, I. (2022). Smart grid reliability evaluation and assessment. *KYBERNETES*. doi:10.1108/K-12-2020-0910

Miao, Q., Lin, H., Wang, X., and Hassan, M. M. (2021). Federated deep reinforcement learning based secure data sharing for internet of things. *Comput. Netw.* 197, 108327. doi:10.1016/j.comnet.2021.108327

Mugunthan, V., Peraire-Bueno, A., and Kagal, L. (2020). "Privacyfl: A simulator for privacy-preserving and secure federated learning," in Proceeding of the CIKM '20: PROCEEDINGS OF THE 29TH ACM INTERNATIONAL CONFERENCE ON INFORMATION and KNOWLEDGE MANAGEMENT, October, 2020 (Ireland: Assoc Comp Machinery), 3085–3092. doi:10.1145/3340531.3412771

Ni, M. (2020). "Study of a quality monitoring system of electric power using internet of things technology," in Proceedings of the IOP Conference Series-Earth and Environmental Science, Bristol, UK, December, 2019. doi:10.1088/1755-1315/440/3/032005440

Pal, S., Dorri, A., and Jurdak, R. (2022). Blockchain for iot access control: Recent trends and future research directions. *J. Netw. Comput. Appl.* 203, 103371. doi:10.1016/j.jnca.2022.103371

Ratnaparkhi, S., Khan, S., Arya, C., Khapre, S., Singh, P., Diwakar, M., et al. (2020). Withdrawn: Smart agriculture sensors in iot: A review. *Mater. Today Proc.* 0. doi:10.1016/j.matpr.2020.11.138

Tanwar, V. K., Raman, B., Rajput, A. S., and Bhargava, R. (2021). SecureDL: A privacy preserving deep learning model for image recognition over cloud. *J. Vis. Commun. Image Represent.* 86, 103503. doi:10.1016/j.jvcir.2022.103503

Tian, K., and Dong, W. (2021). Investment decision-making model of transmission grids under new style power system. *Smart Power* 15, 1112. doi:10.3390/en15031112

Wang, G., Xia, X., Ji, S., and Lai, C.-F. (2021). A privacy-preserving multi-dimensional data aggregation scheme with forward security in smart grid. *J. INTERNET Technol.* 22 (1), 91–99. doi:10.3966/160792642021012201009

Wang, Z., Li, T., Wang, B., Zhang, B., and Zhao, W. (2022). Global short-term load forecasting for multi decision making units in the new power system. *China J. Econ.* 2 (1), 20. doi:10.12012/CJoE2021-0082

Wu, J., and Xiao, J. (2022). Development path based on the equalization of public services under the management mode of the internet of things. *Socio-Economic Plan. Sci.* 80, 101027. doi:10.1016/j.seps.2021.101027

Wu, X., Zhang, Y., Wang, A., Shi, M., and Liu, L. (2020). Mnssp3: Medical big data privacy protection platform based on internet of things. *Neural Comput. Appl.* 34 (4), 11491–11505. doi:10.1007/s00521-020-04873-z

Xia, X., Lin, J., Xiao, Y., Cui, J., Peng, Y., and Ma, Y. (2021). A control-chart-based detector for small-amount electricity theft (set) attack in smart grids. *IEEE Internet Things J.* 9 (9), 6745–6762. doi:10.1109/jiot.2021.3113348

Xia, Z., Zhang, Y., Gu, K., Li, X., and Jia, W. (2022). Secure multi-dimensional and multi-angle electricity data aggregation scheme for fog computing-based smart metering system. *IEEE Trans. GREEN Commun. Netw.* 6 (1), 313–328. doi:10.1109/TGCN.2021.3122793

Xu, X., Peng, H., Bhuiyan, M. Z. A., Hao, Z., Liu, L., Sun, L., et al. (2021). Privacy-preserving federated depressiondetection from multisource mobile health data. *IEEE Trans. Industrial Inf.* 18 (7), 4788–4797. doi:10.1109/tii.2021.3113708

Yan, R., Lin, C., Zhang, W.-f., Chen, L.-w., and Peng, K.-n. (2020). Research on information security of users' electricity data including electric vehicle based on elliptic curve encryption. *Int. J. DISTRIBUTED Sens. Netw.* 16 (11), 155014772096845. doi:10.1177/1550147720968458

Yang, X., Shu, L., Liu, Y., Hancke, G. P., Ferrag, M. A., and Huang, K. (2022). Physical security and safety of iot equipment: A survey of recent advances and opportunities. *IEEE Trans. Industrial Inf.* 18 (7), 4319–4330. doi:10.1109/tii.2022.3141408

Zhang, H., Zhang, H., Wang, Z., Zhou, Z., Wang, Q., Xu, G., et al. (2022). Delay-reliability-aware protocol adaption and quality of service guarantee for message queuing telemetry transport-empowered electric internet of things. *Int. J. Distributed Sens. Netw.* 18 (5), 155013292210978. doi:10.1177/15501329221097815

Zhang, K., Song, X., Zhang, C., and Yu, S. (2022). Challenges and future directions of secure federated learning: A survey. *Front. Comput. Sci.* 16 (5), 165817–165818. doi:10.1007/s11704-021-0598-z