IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 May 2024, accepted 24 May 2024, date of publication 30 May 2024, date of current version 6 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3407121

TOPICAL REVIEW

Advancing Power System Services With Privacy-Preserving Federated Learning Techniques: A Review

RAN ZHENG, ANDREAS SUMPER, (Senior Member, IEEE), MONICA ARAGÜÉS-PEÑALBA, (Member, IEEE), AND SAMUEL GALCERAN-ARELLANO, (Member, IEEE)

Departament d'Enginyeria Elèctrica, Centre d'Innovació Tecnològica en Convertidors Estàtics i Accionaments (CITCEA-UPC), Universitat Politècnica de Catalunya, 08028 Barcelona, Spain

Corresponding author: Ran Zheng (ran.zheng@upc.edu)

This publication is part of the I+D+i project ATLAS (Digitalization using novel data analytic methods and toolboxes for secure, renewable, and flexible grids) with reference PID2021-128101OB-I00 funded by MCIN/AEI/10.1 3039/501100011033 and by ERDF A way of making Europe. The work of Ran Zheng was supported by the Department de Recerca i Universitats de la Generalitat de Catalunya under FI_SDUR Pre-doctoral grants and scholarships (FI_SDUR 2022). The work of Andreas Sumper was supported by the Catalan Institution for Research and Advanced Studies (ICREA) Academia Program.

ABSTRACT Digitalization has enabled the potential for artificial intelligence techniques to lead the power system to a sustainable transition by extracting the data generated by widely deployed edge devices, including advanced sensing and metering. Due to the increasing concerns about data privacy, federated learning has attracted much attention and is emerging as an innovative application for machine learning solutions in the power and energy sector. This paper presents a holistic analysis of federated learning applications in the energy sector, ranging from applications in generation, microgrids, and distribution systems to the energy market and cyber security. The following federated learning-based services for energy sectors are analyzed: non-intrusive load monitoring, fault detection, energy theft detection, demand forecasting, generation forecasting, energy management systems, voltage control, anomaly detection, and energy trading. The identification and classification of the data-driven methods are conducted in collaboration with federated learning implemented in these services. Furthermore, the interrelation is mapped between the categories of machine learning, data-driven techniques, the application domain, and application services. Finally, the future opportunities and challenges of applying federated learning in the energy sector will be discussed.

INDEX TERMS Data-driven techniques, energy service, federated learning, smart grid.

I. INTRODUCTION

The energy sector is currently experiencing a rapid digital transformation characterized by a significant increase in data availability. The dramatic increase in data is largely generated by the adoption of Intelligent edge devices, such as advanced metering infrastructure [1], [2], which have paved the way for the digitalization of energy systems, fundamentally reshaping the way we approach energy management. The vast amount of data, including operational and non-operational data collected by these intelligent systems, opens doors to a multitude of potentials to power a wide array of service applications to optimize and enhance the efficiency of energy systems [3]. To harness this potential and make better-informed decisions regarding grid services [4], data-driven techniques are imperative. Nevertheless, raw data from the power system need to be preprocessed before developing data-driven algorithms for energy services [5].

While data-driven techniques bring considerable benefits, they simultaneously introduce significant challenges,

The associate editor coordinating the review of this manuscript and approving it for publication was Hamdi Abdi.

particularly in data privacy and security. The extensive data centralization required for model training will compromise end-user privacy, as some sensitive information could be disclosed. Users may be unwilling to share the data with others, considering business competition and technical problems. Additionally, regulations on data privacy, such as the General Data Protection Regulation (GDPR), which was applied in the EU in 2018, enhance data privacy when data is shared between different parties [6].

Besides, traditional data-driven algorithms will also have technical issues, especially communication overhead problems, due to the frequent data exchange with central servers [7]. Data insufficiency is another critical problem since centralized models typically need massive datasets to avoid overfitting. However, customers are usually either unable or reluctant to provide sufficient data for accurate model training, such as limited available data from individual customers or new buildings [8], [9].

To address the referred concerns, federated learning (FL) has attracted much attention due to its unique training methodology and features. Federated learning is a distributed learning paradigm that allows training the local in each agent without collecting all data from other agents to the central server, which will result in heavy network traffic. Moreover, privacy concerns will also be alleviated since only the updated parameters are transferred in the model training process. Regarding data insufficiency, transfer federated learning can help set up the model by applying datasets from similar customers without leaking their privacy [9].

Several recently published papers review the state-of-the-art of FL in various fields [6], [10], [11], [12], [13], [14], [15], [16], offering insight into the definition, categories, challenges, opportunities, and general applications. In [6], promising applications related to service recommendations and edge computing integrating mobile edge devices and FL are introduced. The work in [11] summarized the characteristics of FL and addressed the optimization algorithms to tackle the challenges in communication efficiency and data privacy and security, classifying the real-world applications in various domains, including mobile devices (smartphone keyboards and motion sensors), industrial engineering (environment protection, image detection, and representation), and healthcare (MRI). Furthermore, [12] presents how FL works in some critical areas such as finance, transportation, and natural language processing (NLP), while [13] identifies the current main applications of FL and the future use directions, classifying them into applications to technologies including AI, NLP, blockchain, the Internet of Things (IoT), autonomous vehicles as well as resource allocation. Additionally, [13] discusses application to market use cases in healthcare, data science, education, and industry are presented. Future use cases such as IoT, battery management, autonomous vehicles, and recommendation engines are also discussed.

Some review papers delve into FL applications within specialized domains. The authors of [14] concentrate on FL applications in IoT networks, encompassing Industry 4.0, smart city and home, metaverse and virtual reality, healthcare, and autonomous driving. Reference [15] highlights FL applications in wireless communications covering the spectrum of management, edge computing, caching, and 5G networks. Besides, [16] provides a detailed context of FL applications in the Internet of underwater things, spanning environmental monitoring, navigation and localization, and underwater exploration.

However, little attention has been paid to the applications of FL in power and energy systems. In [10], some FL use cases for energy systems are presented after describing the data aggregation algorithms and how the updates from each local model of the local client are aggregated into the central server. These cases refer to some FL applications. Nevertheless, the whole range of possible applications is not classified. Furthermore, data-driven techniques that collaborated with FL to fulfill each energy service have not been analyzed in depth. Apart from this, the interrelationship between data-driven techniques, machine learning categories, potential energy services, and application domains has not yet been addressed.

To the best of the authors' knowledge, there is no systematic assessment paper that holistically analyses and evaluates machine learning techniques collaboratively employed with federated learning, specifically within energy applications. Motivated by the increasing growth of research and promising application in power systems, this study is to conduct a comprehensive assessment within the domain of power systems. In particular, the federated learning potential for ensuring data privacy in energy services that enhances the operation of electrical power systems is analyzed. These services are based on operational and non-operational data that would play critical roles in fulfilling energy services, including weather data, socioeconomic data, and energy market data. The objective is to provide valuable insights that can serve as a foundation for future applications and implementations in this field. This study summarizes the characteristics of FL and analyzes the challenges of various applications where data-driven models have been integrated with FL. In addition to this, the interrelation between the data-driven techniques, the application domains, and energy services will be mapped.

The main contributions of this study are listed as follows:

- This study provides a comprehensive review and analysis of FL-based applications in the energy sector. It contains a detailed examination of FL techniques integrated with energy services, like non-intrusive load monitoring, fault detection, energy theft detection, demand forecasting, generation forecasting, energy management systems, voltage control, anomaly detection, and energy trading.
- The data-driven techniques that collaborate with federated learning to enable energy services are identified in this paper. The interrelationships between models and the grid services are mapped, identifying the different machine-learning techniques integrated with FL that can facilitate the respective grid services.

- Besides, this paper identifies future opportunities and challenges for FL applications in power systems. It analyzes the FL-based applications where FL could significantly influence the advancement of intelligent power systems, such as data privacy and security, communication cost reduction, and data availability. At the same time, challenges, including aggregation algorithm selection and collaborated machine learning model selection, are also highlighted.

This paper is structured as follows. The overview of federated learning is presented in Section II, where the definition, the driving forces to apply FL in power systems, and the machine learning techniques integrated with FL are detailed. The categories of FL based on data partition and network structure are presented in Section III. In Section IV, federated aggregation algorithms are introduced. Data-driven services based on the application of FL in power systems are analyzed in Section V. Discussions on the interrelationship between the four dimensions, including the machine learning categories, the data-driven techniques, the application domains and services, and the opportunities and challenges for the energy sector, are presented in Section VI. In Section VII, some conclusions are drawn.

II. FL CONCEPT, OPPORTUNITIES, AND COLLOBORATED MACHINE LEARNING TECHNIQUES FOR POWER SYSTEMS

The goal of this section is to present the FL definition and conception (Subsection A), to identify current opportunities for the applications of FL in power systems (Subsection B), and to analyze the machine learning techniques that can be collaborated with FL (Subsection C). Federated Learning is a decentralized learning technology that can be used to alleviate challenges such as data privacy protection, data transmission overhead, and data insufficiency [7], [8], [17], [18], [19], [20]. This potential opens up opportunities for its application to the energy sector.

A. DEFINITION AND CONCEPTUAL EXPLANATION OF FEDERATED LEARNING

Federated learning, as a decentralized paradigm learning, was first introduced by Google in 2016 [11], [21], which has changed the way collaborative model training is formulated across distributed datasets located in edge devices while enabling privacy preservation and security. The fundamental difference between FL and traditional centralized learning methods lies in the ability to train a model without necessitating the centralized collection of raw data from local clients to a central server.

In comparison with federated learning, distributed learning approaches show different characteristics in their objectives and training methodologies, though both learning approaches enable collaborative learning across multiple agents. As described in [22] and [23], distributed learning involves agents working collaboratively to solve a common problem or achieve a shared objective, with agents sharing information with each other and learning from their individual knowledge or data. Meanwhile, federated learning focuses on training a global model through machine learning models across edge agents without exchanging raw data. This distinction reveals why FL outperforms distributed learning approaches in terms of data privacy preservation and communication overhead reduction. In relation to privacy protection issues, [24] highlights the utilization of the Pailier cryptosystem encryption approach between the communication, while federated learning can inherently preserve data privacy by transmitting only model updates in the training system. Moreover, federated learning can incorporate encryption approaches such as differential privacy encryption mechanisms, which can also be adopted into federated learning to further enhance sensitive information in the training process.

Based on the operational framework of FL, it can be described as a multi-stage process that is structured into six steps: initialization, local training, model update, model aggregation, iterative process, and global model update [25], [26]. These six stages together constitute the process of federated learning, enabling collaborative model training across decentralized data sources while safeguarding data privacy. This approach has found applications in diverse domains, including engineering, healthcare, finance, and IoT. This article will give a conceptual explanation of how FL works as follows:

1. Initialization: the FL process will commence since the central server initializes a global model, and this global model typically serves as a preliminary model.
2. Local training: In this phase, the global model is distributed to the edge clients, and local training will be demonstrated using their own local datasets. Besides, the individual characteristics will be adapted to the global model.
3. Model update: after the local training process, the edge clients will generate the model updates, which will be sent to the central server. The model updates differ across clients due to the diversity in local training with different local datasets.
4. Model aggregation: in this stage, model updates will be sent to the central server, where the updates are aggregated using federated aggregation algorithms such as FedAvg and FedSGD, as further elucidated in Section IV.
5. Iterative process: This process will repeat from stage 2 to stage 4 until convergence is achieved.
6. Global model update: In the final stage, after achieving convergence, the updated global model will be sent back to the participating edge clients.

B. THE CHALLENGES TO BE ADDRESSED APPLYING FL IN THE POWER SYSTEM

Federated learning has been adopted in various domains, such as healthcare, transportation, finance, and natural language processing, benefiting from its capabilities to enhance data privacy, reduce communication overhead, and distribute

computational complexity. Notably, in the context of the energy sector, the scientific community is increasingly exploring the adoption of federated learning to address some challenges resulting from data-driven approaches in the energy sector. This section outlines the primary motivations for integrating FL in power systems, with each point offering an opportunity to contribute to energy systems improvement.

To attain a comprehensive understanding of motivating factors, their definitions and a brief explication will be given as follows:

- Data privacy and security: this refers to the protection of sensitive information from unauthorized access and breaches. In the power system, where data often contain confidential consumer information, FL can preserve data privacy by allowing model training locally on local device clients without sharing raw data. Techniques like federated averaging and differential privacy ensure that only model updates without the sensitive information being transferred for global model training [25].
- Communication overhead or cost: it indicates the cost and overhead during data transmissions across the communication networks. FL can reduce communication overhead by minimizing the need to transmit large volumes of raw data to a central server. Instead, only model updates are shared between central servers and clients, significantly reducing communication costs, which can be particularly advantageous in power systems with remote or distributed data sources [27].
- Computational complexity: this involves the power and time required to process the data. FL distributes the computational load across local devices or clients, which can enhance computational efficiency. This is particularly beneficial when dealing with complex system models and large datasets [28].
- Scalability: scalability is the capability of a system to handle an increase in workload without performance degradation. FL is inherently scalable as it can handle an increasing number of devices or clients participating in the model learning process [29].
- Data insufficiency: data insufficiency occurs when the available data is too limited to build accurate models. FL can be employed in scenarios with insufficient data by leveraging information from multiple sources without sharing raw data. This is valuable in power systems, especially for some newly equipped components in the power system, which may have limited data availability [7].
- Model generalization ability: model generalization ability refers to the ability of a machine learning model to deal with unfamiliar datasets. FL can improve model generalization by training on diverse and distributed datasets [30].
- Data heterogeneity: data heterogeneity refers to the data with diverse or varied formats, contents, or characteristics within one dataset or multiple datasets. FL is well-suited for dealing with heterogeneity, as it can train models on data with varying characteristics and distributions across different locations or entities within the power system [20].

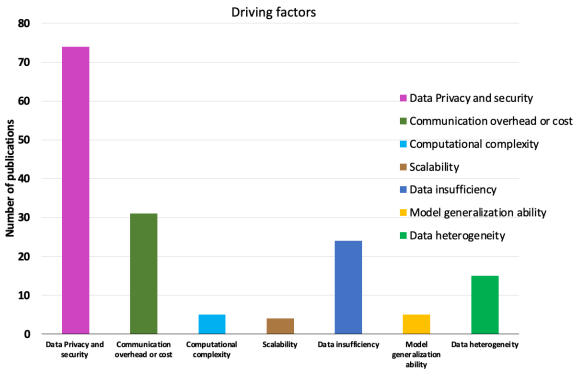

FIGURE 1. Motivating factors for applying FL in publications from 2019 until 2023.

Table 1 outlines the driving forces to apply FL within energy services, providing a brief introduction to the specific challenges FL is proposed to overcome in energy sectors. Fig. 1 portrays a bar graph encapsulating the predominant driving forces to integrate federated learning within the energy sector in recent literature. As indicated from the illustration, preeminent concerns are centered around data privacy and security, followed by communication overhead or cost, data insufficiency, and data heterogeneity. Scalability and model generalization ability have remained less emphasized areas of research within this domain.

C. OVERVIEW OF MACHINE LEARNING TECHNIQUES COLLABORATING WITH FEDERATED LEARNING

The substantial amount of data generated in the power system has provided the potential for innovative energy services through the application of machine learning (ML) algorithms. When compared to traditional centralized machine learning approaches, machine learning techniques trained in a federated manner can fulfill energy services while addressing challenges such as data privacy and data silos.

Federated Learning serves as a collaborative approach during the model training process, where the initial data-driven model is distributed to clients for local training. Therefore, a variety of ML techniques that can be integrated with federated learning will drive innovation in the power and energy sectors. Fig. 2 provides a depiction of the ML techniques mentioned in the reviewed literature with respect to their classifications.

As outlined in the study [93], machine learning approaches are typically divided into three categories: supervised learning, unsupervised learning, and reinforcement learning. Supervised learning is a type of machine learning algorithm that is trained on a labeled dataset, where the training data is paired with an output label. This process is used in classification tasks where the labeled dataset represents categories and regression tasks, where the labeled dataset indicates the data to be forecasted. Within the energy context, regression

TABLE 1. The driving factors for applying FL in the power and energy systems.

Ref.	Data privacy and security	Communication overhead or cost	Computational complexity	Scalability	Data insufficiency	Model generalization ability	Data heterogeneity
[4], [17], [18], [25], [27], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44]	x	x					
[45]					x	x	
[46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60]	x						
[61]	x				x		x
[28], [62], [63]	x		x				
[64]	x					x	
[7], [20]	x	x			x		x
[8], [9], [19], [65], [66], [67], [68], [69], [70], [71], [72], [73]	x				x		
[74]	x			x			
[26]	x		x		x		
[75]	x	x			x		
[29]	x	x		x			
[76]	x	x		x	x		x
[77]	x				x		
[78]	x	x	x				
[79]					x		
[80], [81], [82], [83], [84], [85]	x	x					x
[30], [86], [87]	x				x	x	
[88], [89], [90], [91]	x						x
[92]	x			x			x

methods are primarily applied to prediction tasks such as demand forecasting [70], [77], generation forecasting [38], and voltage forecasting [61]. Classification methods are typically employed in scenarios where the objective is to identify specific cases based on historical data. The general applications mainly involve energy theft detection [83] and anomaly detection [87].

In comparison to supervised learning, unsupervised learning aims to learn patterns from unlabeled data [94]. For instance, clustering techniques such as K-means are used to group data points based on similarity without prior labels. In the energy sector, clustering can be used in load profile clustering.

Reinforcement learning (RL) is a type of machine learning where agents learn to make decisions by interacting with an environment to maximize the cumulative rewards [95]. This computational and model-free approach is applicable for control, operation and management. Hence, it can be implemented in energy management systems [28], [89] and voltage control issues [29] for optimal control.

Additionally, deep learning (DL) algorithms are also employed to implement various tasks across all categories of machine learning in power systems. DL is a special artificial neural network, which is a sophisticated approach to function approximation. It utilizes multi-layered neural networks to model complex relationships in data and can be used in generation forecasting [53], [88], energy management systems [41], [58], and fault detection [42] for power devices.

III. FEDERATED LEARNING CATEGORIES

Federated learning is typically classified into two groups, one based on data partitioning and the other based on network topology. In federated learning, data partitioning refers to how the data is divided among various devices or nodes that participate in the learning process, including horizontal (or sample-based) partitioning and vertical (or feature-based) partitioning. In this context, features are the distinct attributes or properties of the dataset that are used for analysis in machine learning. Network topology refers to the structure of how nodes (devices or servers) are

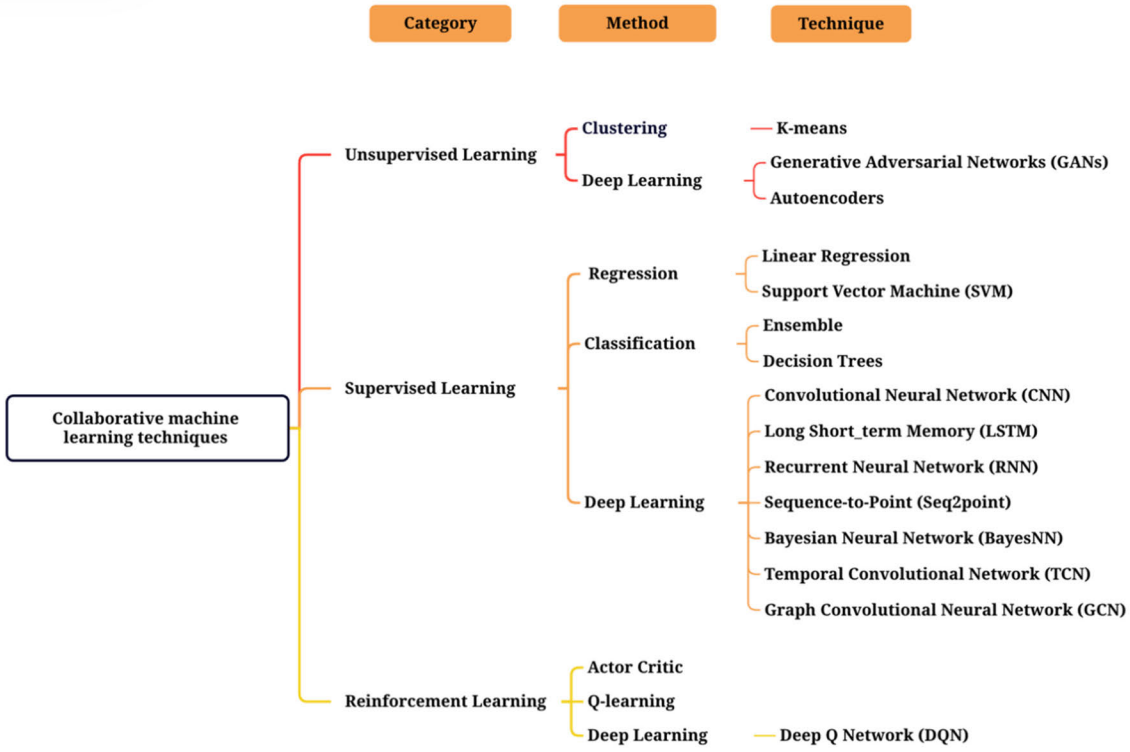

FIGURE 2. Machine learning techniques integrated with FL in power systems.

connected and communicate with each other in the federated learning system, which will significantly affect the learning process and includes centralized topology and decentralized topology.

A. FEDERATED LEARNING BASED ON DATA PARTITION

Based on the data partition of how the features and the samples are distributed, federated learning can be categorized into three dimensions: horizontal federated learning, vertical federated learning, and federated transfer learning [21].

1) HORIZONTAL FEDERATED LEARNING

Horizontal federated learning, also referred to as samples-oriented federated learning, is typically employed in scenarios where datasets exhibit similar features but contain rare identical samples. As shown in Fig. 3, these datasets exhibit significant overlapping in features with little overlapping in the samples. This approach leverages the same set of features across different samples, effectively increasing the sample size. For example, there are two datasets from two different distribution grid operators located in different districts. Despite differences in their customer bases, these datasets share identical business-related features.

Hence, the characteristics of horizontal federated learning can be concluded to be similar features and different samples. In [92], a privacy-preserving approach is developed to forecast energy demand for retail energy providers using a horizontal federated learning framework to handle

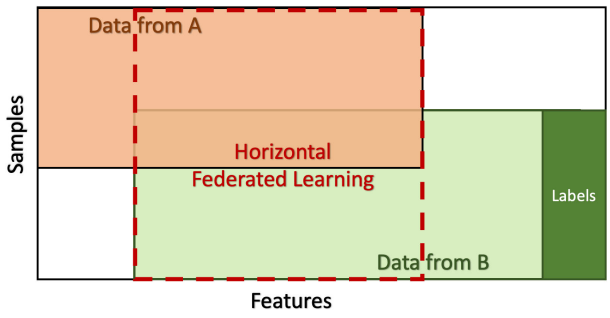

FIGURE 3. Horizontal federated learning [21].

the residential household energy data collected from the smart meters. Reference [47] provides a horizontal federated learning approach for household load identification. Besides this application, horizontal federated learning schemes are also used for load forecasting [25], [27], residential load profile identification [18], energy management [49], generation forecasting [35], and energy forecasting for EV networks [31].

2) VERTICAL FEDERATED LEARNING

When compared to horizontal federated learning, vertical federated learning finds applications in scenarios where datasets share similar samples but exhibit distinct rare features (e.g., data, time, temperature, electricity usage., etc.). It is also referred to as features-oriented federated learning. As illustrated in Fig. 4, these datasets display significant overlapping in samples but limited overlapping in the features. In vertical federated learning, datasets are partitioned vertically based

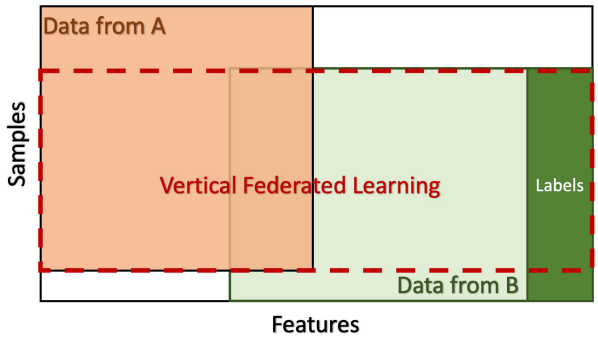

FIGURE 4. Vertical federated learning [21].

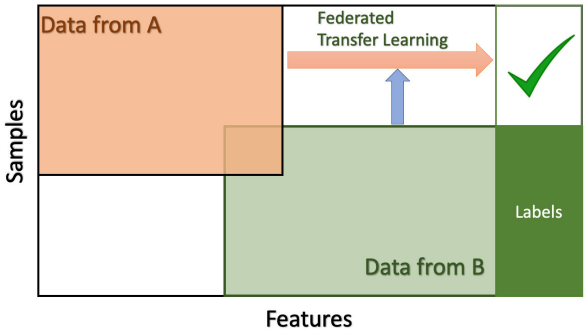

FIGURE 5. Federated transfer learning [21].

on their feature perspectives, extracting columns of data with identical samples but differing features for subsequent training [21].

For example, consider two different organizations located in the same geographic region, such as distributed energy retailers and regional banks. Hence, they may have the majority of customers, representing significant overlapping in samples. However, the retailer has energy usage data, while the bank possesses financial transaction records, which can have different features. Vertical federated learning enables these organizations to collaboratively train models that can fully utilize customer data without sharing sensitive information directly.

Vertical FL is particularly valuable in environments where the parties hold the same samples but with scattered features. For example, vertical FL is employed in scenarios for accurate load forecasting using different features located in different data partitions for model training [96]. For example, in [38], an innovative learning framework integrating vertical federated learning and horizontal learning with an XGBoost-based learning framework is proposed to address the distributed features of datasets for utility power prediction in China.

3) FEDERATED TRANSFER LEARNING

Federated transfer learning is applied in scenarios where two datasets share few common features and few overlapping samples, as depicted in Fig. 5. For instance, two organizations located in different districts are considered, such as one supermarket located in Spain and one regional bank in France. Due to their different locations, there is little overlapping in their consumer groups. Moreover, they share very few similar features owing to their distinct businesses.

Federated transfer learning holds significant potential despite the difference in data across different domains. By definition, transfer learning leverages the knowledge gained from one domain and applies it to another. It is particularly effective when there are underlying similarities or commonalities between domains. However, even in a federated setting where samples and features differ significantly, transfer learning can still be facilitated by identifying abstract patterns or representations that can be common across domains.

In federated transfer learning, different parties collaborate to improve a global model without sharing their data directly, benefiting from the federated architecture to gain a broader insight into varied data. This is characterized by having different features and samples. In [17], transfer learning is used to test the proposed NILM approach in different datasets to verify the transferability. Reference [9] proposed a novel approach based on transfer learning for building energy demand forecasting, addressing the data insufficiency problem by utilizing the buildings with sufficient operational information without privacy leakage. Similarly, an approach based on federated transfer learning is proposed to predict the load consumption of a novel power system, where federated learning is used to transfer the parameter features from non-mask load to local data [97].

While the direct application of models from one domain to another with no commonality is challenging, federated transfer learning can exploit even a few similarities. It may use some strategies, including instance transfer, parameter transfer, feature-representation transfer, or relational knowledge, to identify and leverage between source and target domains [98]. These approaches allow the model to abstract knowledge that can be generalized across different domains, which is particularly useful when dealing with different datasets in federated learning environments.

Fig. 5 illustrates the concept of federated transfer learning [21], where, despite the inherent differences in datasets, collaborative and strategic model training can generate a model that is robust and applicable across various domains.

B. FEDERATED LEARNING BASED ON NETWORK TOPOLOGY

Based on the network layout, federated learning consists of two categories: centralized and decentralized FL, respectively. Actually, both kinds of FL function the same, whereas the main difference between the centralized and decentralized FL is the central server or global model, where all updated parameters will be collected. In terms of the decentralized FL, there is no central server, and any client can perform as the central server randomly to update the global model.

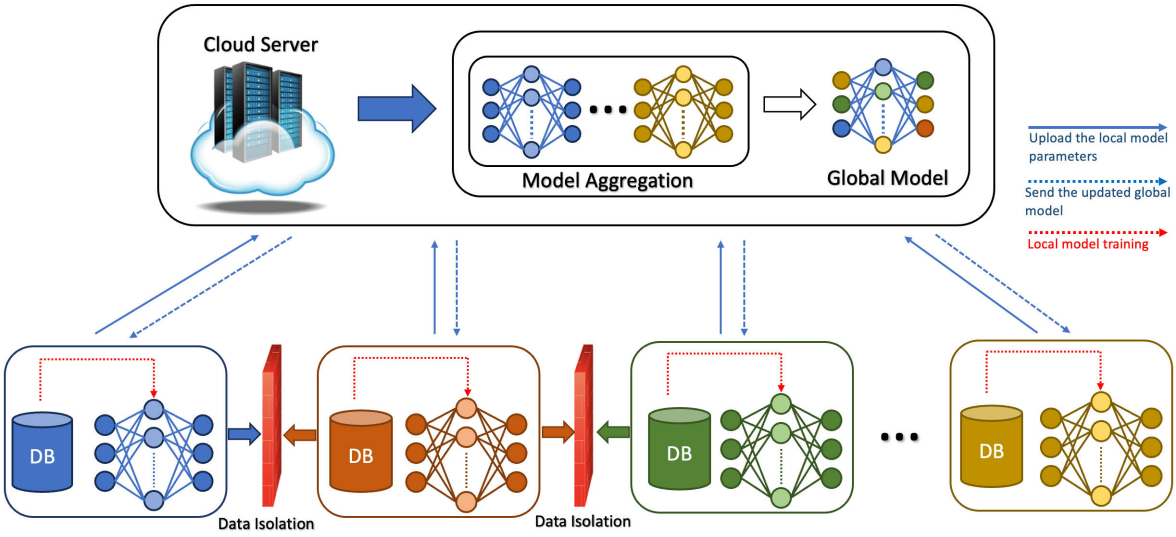

FIGURE 6. Centralized federated learning.

1) CENTRALIZED FL

Centralized FL, also referred to as central server-based FL, represents the prevailing network topology for federated learning. Fig. 6 provides an illustration of the typical network architecture of centralized FL. This structure encompasses a central server and multiple edge devices serving as clients that could be capable of storing the datasets and implementing local model training. For each training round, the process can be separated into several stages. Initially, local models are trained and set up in the clients locally. Subsequently, in the second stage, the encrypted parameters of these local models will be sent to the central server. The central server aggregates the encrypted parameters using federated aggregation algorithms, such as FedAvg and FedMa (detailed in Section IV). Consequently, the global model is updated. At the next stage, the updated global model will be transmitted back to the edge clients. Finally, at the last stage, each client will update the local model based on the received global model and await the commencement of another training iteration. Throughout the training process, the parameters from the local model remain securely isolated from the other clients, thereby ensuring the preservation of the privacy of end-users.

2) DECENTRALIZED FL

Decentralized FL, also referred to as distributed FL, distinguishes itself from centralized FL by its absence of a central server within the framework. The typical network structure of decentralized FL is depicted in Fig. 7. During the training process, each client independently refines its local model using its own datasets. Subsequently, the client shares its model parameters with the neighboring clients under peer-to-peer (P2P) communication agreements who are also engaged in the training process. In parallel, the client receives the updated models from other participants, resulting in model aggregation and distribution. The aggregated model is then compared with the local model of the clients, with the superior one retained as the new local model for the subsequent iterations until convergence. Importantly, each client also acts as a server for other participants. Due to the sparse communication topology, decentralized FL demonstrates enhanced robustness against potential cyber-attacks, thereby mitigating vulnerabilities that a centralized approach may encounter when targeted by malicious actors.

To alleviate the problem caused by malicious attacks on the central server, a possible solution based on a fully decentralized federated learning approach has been applied to a non-intrusive load monitoring topic [44], with the performance and applicability are also validated. Ref. [20] introduces a collaborative fault detection algorithm with serverless federated learning topology, which can effectively improve the model generalization, as well as address challenges such as data islands, training time, and communication overhead and efficiency.

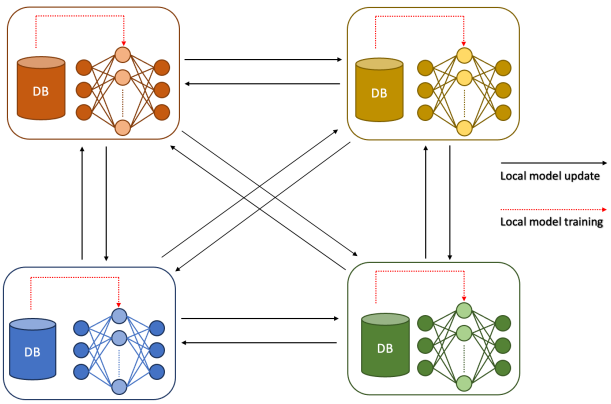

FIGURE 7. Decentralized federated learning.

IV. FEDERATED AGGREGATION ALGORITHMS

Federated aggregation algorithms play a critical role in governing the operation of federated learning, particularly in the aggregation of updated local models. Currently, several

algorithms have been adopted, such as FedAvg, FedSRC, FedSGD, FedMa, FedPer [58], and FedGMA. This section will introduce selected algorithms that are used in the energy sector.

- FedSGD (Federated Stochastic Gradient Descent): this algorithm employs a straightforward approach by executing a single gradient update on selected devices during each training round. It randomly selects a subset of edge devices, transmitting the updated model parameters (weights) to the central server. This central server then aggregates these parameters from locally trained models and update the global model. The averaging of weights is proportional to the volume of locally trained samples, essentially representing one gradient descent step [74]. The approach of performing a single SGD per iteration necessitates multiple iterations for the global model to converge.
- FedAvg (Federated Averaging): FedAvg, a commonly used strategy in centralized federated learning, operates similarly to FedSGD with a key distinction. FedAvg allows devices to perform multiple training steps locally before sending their updates. This means each device works on improving its local model for a while, thereby decreasing the communication frequency with the server [25]. This method has been shown to enhance accuracy and efficiency, particularly in applications such as residential load prediction.
- FedGMA (Federated Gradient Masked Averaging): to address the issue of outliers in model updates, which may arise with FedAvg, FedGMA uses a geometric mean for aggregation. This can provide a more robust global model update, particularly when there's significant variance among the local updates [39].
- FedProx (Federated Proximal Algorithm): an enhancement of FedAvg, FedProx introduces a proximal term that helps handle data heterogeneity. This term helps to stabilize the learning process and makes the model updates more consistent, even when the data is quite diverse. Evaluation in [85] indicates that FedProx outperforms FedAvg, particularly in handling heterogeneous settings for NILM, more effectively than FedAvg.

In addition to these federated aggregation algorithms mentioned above, various open federated platforms have been developed by organizations, including TensorFlow Federated, PySyft, Fed-BioMed, Flower, IBM FL, FATE, FedAI, FedML, and Paddle FL. These platforms offer potential solutions for applications in the energy sector, with examples like the use of the FATE-based federated platform for enterprise energy consumption prediction to secure the data privacy of power enterprises [77].

V. APPLICATIONS OF FL IN POWER AND ENERGY SYSTEMS

In this section, an exhaustive review of recent literature on innovative applications utilizing federated learning within the power and energy domains is undertaken. Following Kitchenham's approach, the literature review was systematically organized and implemented [99]. The literature was searched in academic databases, including IEEE Xplore, Scopus, and Web of Science, to gather peer-reviewed research articles published between 2019 and 2023. Papers were selected based on their relevance to the application of FL in energy systems, mainly focusing on non-intrusive load monitoring, fault detection, energy theft detection, demand forecasting, generation forecasting, energy management systems, voltage control, and anomaly detection. Only relevant papers in terms of scope, relevance, and quality have been taken into account for this study. Titles and abstracts were first checked for relevance, followed by a full-text review to ensure that the studies met the inclusion criteria. In total, 76 papers related to federated learning applications within power systems were selected for review and analysis, which provided a clear methodology and quantitative results on the use of FL.

For each selected paper, relevant information was extracted and systematically organized into tables based on the defined energy services. The tables highlight the data-driven techniques, federated learning algorithms, aggregation algorithms employed, application scenarios, and contributions of each study. Additionally, applications that utilize decentralized, federated learning are denoted with an asterisk (*), whereas those based on centralized learning-based applications are not marked. Applications with horizontal, vertical, and transfer learning will be marked with numbers (^{1}, ^{2}, and ^{3}) respectively.

To offer a clear comprehension of the scope and focus of FL applications in the energy sector, a bar graph (Fig. 8) was constructed. This graph illustrates the prevalence of FL techniques applied to different energy services, based on the number of publications in each category within the specified timeframe. Moreover, to enhance the understanding of the driving forces presented in Section II-B, Table 2 is established to clarify the relationship between the identified FL applications and the driving forces outlined in Section II-B, providing a cohesive narrative that maps the advantages of FL to practical implementations in the energy sector.

A. NON-INTRUSIVE LOAD MONITORING

Non-intrusive load monitoring, also known as energy disaggregation, was initially proposed by George in 1991 [100]. It typically applies data-driven techniques to disaggregate the total energy consumption readings from smart meters at the residential or microgrid levels into appliance level. Energy consumption characteristics with respect to the specific devices can help the power company to analyze the consumption behavior of the customers and enable diversified grid applications such as demand response and energy management. However, most advanced metering infrastructure systems only collect the overall consumption data of the subsystem at the electrical entry. Hence, NILM would be more economical than installing AMI at the appliance level.

TABLE 2. The benefits, challenges, and approaches of FL within varied energy services.

Energy Services		Ref.	Benefits	Challenges	Key parameters	Approaches
Non-intrusive load monitoring		[4], [17], [18], [36], [44], [47], [52], [56], [75], [76], [82], [84], [85], [86]	Preserving data privacy, reducing communication overhead and computation cost, and good scalability.	Risk for criminals to attack this transmitted information; trade-off between communication cost and network load; trade-off among privacy protection, model performance, and effectiveness; limited geospatial data; optimal frequency of federated aggregation; communication latency; not perform well in decomposing the signals of appliances with small amplitudes.	Historical consumption patterns, consumer characteristics to be identified, calendar information	The privacy-preserving federated frameworks are developed for NILM that integrates federated learning with a machine learning architecture to conduct NILM to disaggregate smart meter data form household level to the appliance level.
Fault detection for the power devices		[20], [42], [57]	Improving model generalization; reducing the communication overhead and training time; enabling the identity of more fault types; high robustness against the communication noises; preserving data privacy; high computational efficiency; addressing data insufficiency problems.	Model efficiency and model generalization; data leakage during data aggregation; processing the nonideal data.	The I-V characteristic curves of the normal and different fault states under different circumstances, system log records the system behaviors and operations when the system failure occurs	Federated learning is utilized to combine with machine learning techniques, especially CNN to train a collaborative model for fault detection, which can improve the accuracy while addressing the data insufficiency, communication efficiency and preserving data privacy.
Energy theft detection		[50], [83]	Preserving data privacy; high detection accuracy; and reducing communication overhead.	New data security schemes for data aggregation.	Energy consumption data, energy theft behavior	The privacy-preserving energy theft detection framework is established, including a central server, several detection stations, and consumer devices. The local model is trained in detection stations, and the shared parameters will be sent to a central server for global model training.
Forecasting	Demand forecasting	[8], [9], [19], [25], [26], [27], [30], [31], [32], [33], [34], [40], [51], [55], [63], [65], [66], [67], [69], [70], [73], [74], [77], [79], [81], [90], [91], [92]	Achieving competitive accuracy while preserving data privacy; reducing communication overhead reduction; speeding up the convergence, improving computational efficiency; addressing data island problems, improving the generalization ability, handling data heterogeneity, and good scalability.	Data leakage when transferring model weights; trade-off between forecasting performance, training time and communication overhead; potential model inversion attack; optimizing the model parameters for better model performance.	Historical consumption patterns, weather data, and calendar information	The distributed algorithm for demand forecasting based on federated learning is proposed to mitigate the data privacy and reduce the communication overhead. Besides, before training process, the dataset can be grouped by the similarities to improve the performance.
	Generation forecasting	[7], [35], [38], [46], [55], [68], [71], [72], [88]	Preserving data privacy, communication overhead reduction; addressing data insufficiency.	The non-independently and identically distribution (IID) data problem; limited communication bandwidth; communication latency and overload;	Historical generated electricity patterns, weather	A hybrid generation forecasting model integrated is proposed based on federated learning and deep learning, which can achieve high forecasting performance while preserving data privacy.
	Voltage forecasting	[61]	Preserving data privacy; mitigating data heterogeneity and data scarcity.	Potential model inversion attack	Historical local load, renewables generation, calendar information, node location	A federated model with differential privacy is used to keep the data privacy and the trade-off can be made between model performance improvement and data privacy by tunning the parameters of models.

TABLE 2. *(Continued.)* **The benefits, challenges, and approaches of FL within varied energy services.**

Energy management systems	[28], [37], [41], [46], [49], [58], [62], [78], [89]	Preserving data privacy, reducing computational complexity and communication overhead; addressing data heterogeneity; fast convergence.	Additional dataset for more practical model training; the impact of data tampering and false information.	Electricity pricing, charging/discharging energy of energy storage, states of the flexible loads (like washing machine), fixed load demand, the renewables energy production	Distributed energy management system model consists of local energy management systems and a global server. Local energy management systems are trained by using the energy consumption data, and then transfers the updates to global servers. The iteration ends when the global model convergence.
Voltage control	[29], [54]	Enhancing scalability, privacy and communication efficiency remarkably.	Impact of communication links and further reducing the communication burden.	active / reactive power injection of continuous regulation devices at the node，upper/lower limit of desired voltage range	A cloud-edge coordination strategy based on federated learning can be used to implement decentralized voltage control in distribution networks. Most computation of training process is conducted in local agents while some coordination information exchanges between central server and local agents.
Anomaly detection	[39], [43], [80], [87]	High detection accuracy; improve the privacy; high communication efficiency; good scalability.	The reliability and security; optimizing retraining mechanism for real intrusion data.	Records of normal, disturbance, control, and cyberattack	The proposed model integrates machine learning techniques and federated learning for anomaly detection while maintaining data privacy.
Energy trading	[59], [60], [64]	Preserving data privacy and improving model generalization ability.	Robustness against failures; effectiveness improvement; privacy problems.	Trading price, the amount of energy requested/provided, participant capabilities, successful energy resource provided by the device at time t	Federated learning usually adopts blockchain in energy markets for security and privacy concerns, and enables for end-to-end service as well as energy prediction over smart contracts.

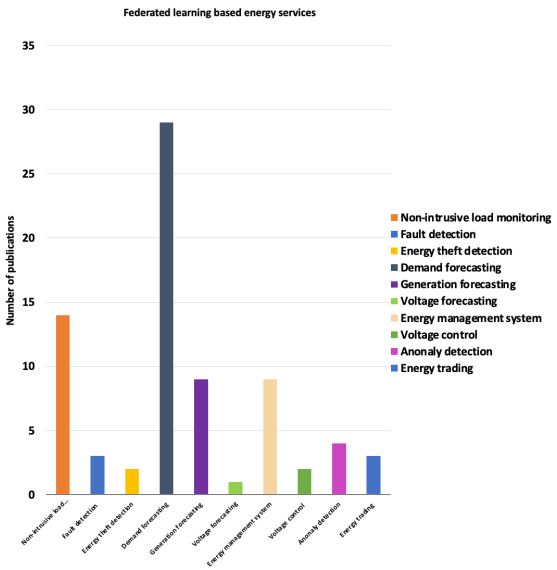

FIGURE 8. **Applications of FL in the energy sector in recent literature from 2019 until 2023.**

The demand for electricity consumption pattern extraction provides the main driving force for further development.

The research on this topic has gained more and more attention in recent years. Typically, this work for NILM will be conducted in a centralized manner, assuming that the data recorded by smart meters are fully accessible. However, this will rise privacy concerns as the data is owned by various power companies or retailers. Consequently, decentralized algorithms become essential for NILM. Data privacy is the primary concern in the energy disaggregation applications, as highlighted in [4], [17], [18], [36], [47], [52], and [82], and communication overhead problems and communication efficiency are significant factors to apply FL to address in [4], [18], [36], [44], [76], [82], and [84]. Furthermore, some researchers also aim to improve the scalability and model generalization ability [86], and address data insufficiency [76], and tackle data heterogeneity problems [76], [82], [84], [85] in NILM.

Various data-driven techniques incorporated with FL have been applied to extract important value and hidden characteristic pattern. In [17], the author compares the performance with different learning models, including sequence-to-point (Seq2Point), long short-term memory (LSTM), and convolutional neural networks (CNN). It was found that Seq2Point demonstrated superior performance. Furthermore, different deep neural network (DNN) structures based on seq2point employing CNNs are proposed in [44], [56], [76], and [82], while artificial neural network (ANN) is applied for model training with principal component analysis (PCA) for feature extraction from smart meter data. A gated recurrent unit (GRU) model is selected in [4] due to the comparable performance in complexity reduction; meanwhile, it is applied to help solve the vanishing gradient problem. According to [36], a clustering algorithm based on K-means is trained in two strategies, including gradient-sharing and model-averaging,

TABLE 3. Data-driven techniques collaborated with FL for NILM.

Ref.	Year	Data-driven technique	Data aggregation algorithm	Application domain	Dataset source	Evaluation metrics	Contributions
[4][1]	2021	GRU (RNN)	FedAvg	Residential	The Pecan Street dataport	Not mentioned	Reducing communication cost while data privacy preserving
[17][3]	2021	Seq2point	FedAvg	Residential	UK-DALE, REFIT, and REDD	MAE	Achieving comparable performance with privacy protection
[18][1]	2021	ANN	Adam	Residential	Irish CER dataset	MCC	Achieving comparable performance with privacy protection
[36][1]	2022	K-means	Model averaging-based and gradient sharing-based methods	Residential	Irish CER Dataset and Low-Carbon London Dataset	Avg-I, DBI, WCBCR, SMI, CHI	Achieving comparable performance with privacy protection
[44][*1]	2022	See2point	DeFedAvg	Residential	REFIT dataset	MAE	Achieving comparable performance
[47][1]	2021	CNN-LSTM	Asynchronous stochastic gradient descent with delay compensation (ASGDDC)	Residential	Irish CER dataset	ACC, MCC	Achieving comparable performance with privacy protection
[52][1]	2021	BNN	Layerwise parameters aggregation	Residential	Ausgrid Solar Home Electricity (ASHE) dataset	RMSE, NRMSE, MQS	Achieving comparable performance with privacy protection, enough robustness with some non-serious communication failures and noises
[56][1]	2021	Seq2point	FedAvg	Residential	REFIT dataset	F1-score	Achieving comparable performance with privacy protection
[75][1]	2022	Decision Trees	Global voting	Residential	UK-DALE, REDD, and REFIT	MAE, SAE, NDE, scoring metric	Achieving comparable performance in convergence, accuracy, communication efficiency
[76][1]	2021	Seq2point	FedAvg	Residential and industrial	REFIT and IMDELD	F1-score	Achieving comparable performance with privacy protection, good scalability
[82][1]	2022	Seq2point	Not-mentioned	Residential	REFIT, UKDALE and REDD	MAE, SAE, F1-score	Achieving accurate energy disaggregation without scarifying data privacy
[84][1]	2022	GRU	FedMeta	Residential	Pecan Street dataset	MAE, SAE, F1-score, accuracy	Achieving comparable performance, reducing the communication and computation cost
[85][1]	2022	DNN	FedAvg, FedProx	Residential	UKDALE, REDD and REFIT	Accuracy, recall, precision, F1-score	Achieving acceptable performance while preserving privacy, good scalability
[86][1]	2021	DNN	FedAvg	Residential	UK-DALE dataset	Accuracy, recall, precision, F1-score.	Achieving comparable performance with privacy protection

and then verified in two real-world datasets. The gradient boosting machine-based NILM algorithm achieves a competitive accuracy compared with the centralized learning algorithm [75].

In addition to identifying residential consumption characteristics, NILM can also be used to determine the solar generation behind the meter at the community level [52]. This approach leverages a Bayesian neural network (BNN) method to overcome uncertainties, thereby enhancing the decision-making progress.

Table 3 presents the machine learning algorithms used for NILM in the literature reviewed, along with the corresponding evaluation metrics and datasets employed in the evaluation for various algorithms. Evaluation metrics are employed as a measure of the efficacy and performance of the proposed federated learning models. Data-driven models are integrated with federated learning, a distributed paradigm that collaborates with data-driven models to deliver exceptional performance, particularly in data privacy preservation. This collaborative relationship is explored in Subsection III-B, which describes the mechanics of federated learning. Here, various data-driven techniques or models, such as ANN or DNN, are used for local training and model aggregation. In contrast with data-driven techniques, data aggregation algorithms delineate the process of how to aggregate the model updates from local models for global model aggregation, exemplified by techniques such as FedAvg or FedSGD.

B. PREDICTIVE MAINTENANCE AND FAULT DETECTION FOR POWER DEVICES

Predictive maintenance and fault detection are crucial for power systems, ensuring power systems operate reliably

TABLE 4. Data-driven techniques collaborated with FL for fault detection in power systems.

Ref.	Year	Data -driven technique	Data aggregation algorithm	Application domain	Dataset source	Evaluation metrics	Contributions
[20]*[1]	2022	CNN	Decentralized model	PV stations	Records of the I-V characteristic curves and environmental information as the dataset	Accuracy of local model without ADFL, accuracy of the global model with ADFL, communication and Training Efficiency	Improve model generalization; reduce the communication overhead and training time; enable to identity more fault types
[42][1]	2022	LSTM	Periodic Update (PUpdate), Incremental Update (AUpdate), Triggered Update (TUpdate)	Power terminals	Historical system logs records from the manufacturers and managers	The time of model updating, the amount of data transmission of each terminal, and detection accuracy	Reduce data transmission; protect the privacy; improve the accuracy of detection
[57][1]	2022	CNN	Hierarchical parameters aggregation strategy	Power transformer	DGA dataset	Accuracy, F1-score.	Improve the accuracy, high computational efficiency, high robustness and privacy

and continuously. Predictive maintenance is a maintenance strategy that can predict potential equipment failures using data from various sensors [101]. For instance, the authors in [102] utilized a hybrid approach that combines a fuzzy logic controller with fuzzing clustering means to diagnose and prognose incipient faults and assess the insulation status of power transformers, enhancing the accuracy and reliability over previous experimental and data analysis methodologies. However, traditional machine leaning-based predictive maintenance approaches confront challenges such as data communication overhead and data security issues, which federated learning can be potentially applied to address [103].

Fault detection in power systems is becoming increasingly critical with large installations of distributed generation and new devices in the power networks. The reliability of these complex systems is crucial; hence, the deployment of fault detection services is indispensable. Existing fault detection methods can be generally categorized into two approaches. The first is the model-based approach that utilizes sensor data and model results to detect anomalies [5]. The second approach employs machine learning techniques to predict and identify faults, representing a significant advancement over traditional methods.

Applying federated learning to fault detection can address several challenges in power systems. This includes overcoming the fragmented nature of data across different installations, referred to as data islands, while also respecting data privacy requirements [20], [42], [57]. Additionally, FL is beneficial in reducing communication overhead to improve communication efficiency, which is crucial given the vast amounts of data generated by sensors across the grid [42].

For instance, in photovoltaic (PV) stations, fault detection focuses on identifying key issues such as short-circuit faults, degradation faults, and partial shading faults [20]. A novel algorithm combining serverless FL with CNN is proposed to enhance the detection and diagnosis of such faults. In [42], a decentralized fault detection method is introduced for power terminals, which are essential devices in smart grids responsible for measuring, monitoring, controlling, and performing other functions. This method adopts a three-tier structure (terminal-edge-server) model and employs long short-term memory (LSTM) to enhance detection accuracy. In another case, hierarchical federated learning is applied for transformer fault diagnosis, with CNN used to identify fault types [57].

Table 4 offers a summary of data-driven techniques employing FL for fault diagnosis across different devices, including PV stations, power terminals, and power transformers. The table outlines dataset sources, contributions, and evaluation metrics for these techniques, providing a clear overview of the state-of-the-art in this critical field.

C. ENERGY THEFT DETECTION

In the power system, energy losses are typically categorized into two main types: technical losses and non-technical losses. Technical losses primarily encompass electrical resistance losses within the conductors, whereas non-technical losses, also referred as to financial losses, relate to billed electricity without payment and non-billed electricity [104]. The latter often arises from consumers taking electricity illegally, also called energy theft or energy fraud. Energy theft poses a significant economic loss for power companies and necessitates the development of effective detection methods. Such incidents of energy fraud cases are reported in many countries, with instances like electricity theft leading to substantial financial losses of 6 billion US dollars in the USA [105]. In Spain, the utility company Endesa reported the recovered electricity from 1,636 fraud cases, amounting to 159 million kWh, equivalent to the annual consumption of 45,000 households [106].

Recognizing the importance and urgency of addressing this issue, numerous researchers have focused on energy theft detection. A systematic review in [105] explores the various types of energy theft and energy theft detection techniques, analyzing their limitations, strengths, challenges, and future prospects. This review categorizes the detection techniques into three types: data mining techniques, state and

TABLE 5. Data-driven techniques collaborated with FL for energy theft detection.

Ref.	year	Data-Driven technique	Data aggregation algorithm	Application domain	Datasets source	Models for comparison	Evaluation metrics	Contributions
[50][1]	2022	TCN	Averaging	Distribution grid	SGCC	FedMLP. FedCNN, FedRNN, FedLSTM	Accuracy	Data privacy; high detection accuracy; and computation overhead reduction
[83][1]	2022	Ensemble (RF, KNN, BG)	Averaging	Distribution grid	SGCC	FedTCN, FedCNN, FedMLP, FedRNN, FedLSTM, FedGRU	Accuracy, precision, F-measure, recall, log loss, RMSE	High accuracy, low computation overhead

network-based techniques, and game theoretic techniques, with the latter rarely being used. Another comprehensive review [107] covering more than 100 selected studies found that non-hardware-based solutions have gained significant attention [104].

Federated learning is applied to address data privacy preservation [50], [83], and to manage data heterogeneity [83] in energy theft detection. For instance, in [83], a federated deep neural network framework based on temporal convolutional networks (TCN) is introduced. This innovative approach achieves competitive detection accuracy compared to other federated methods (federated multi-layer perceptron (FedMLP), FedCNN, federated recurrent neural network (FedRNN)and FedLSTM), as well as centralized models (CNN and TCN). Furthermore, the research in [83] introduces the FVC model, a voting-based classifier that combines KNN, RF, and BG to create an optimal prediction model. This prediction model outperforms other federated models, including FedTCN [50].

Table 5 provides an overview of data-driven models integrated with FL for energy theft detection. It details the evaluation metrics, contributions, and models used for comparison.

D. FORECASTING

The increasing integration of intermittent and distributed renewable energy systems (RESs) into the current power grids makes a significant transition into an active, bidirectional, and smart grid. The transition also introduces new challenges for grid operation and planning due to the inherent intermittency of RESs. Consequently, accurate forecasting has become crucial by utilizing historical data to predict trends for generation, demand, flexibility provision, and energy price, which provides valuable information for grid management and the electricity market. This section will discuss the recent improvements in demand and generation forecasting, as well as voltage forecasting, applying machine learning techniques combined with FL.

The research on forecasting can be classified generally into three categories based on the forecasting time horizon, including short-term, medium-term, and long-term [108], [109], [110]. In some instances, very short-term forecasting is added to the classification [111], [112], [113]. These forecasting horizons are defined as follows:

- Very short-term forecasting refers to prediction time from seconds to one hour;
- Short-term forecasting refers to prediction time from one hour to one week;
- Medium-term forecasting refers to one week to a few months;
- Long-term forecasting refers to a few months upward;

As illustrated in [110], most studies concentrate on short-term forecasting tasks commonly employed in the optimal operation of energy and power systems [5]. Very short-term forecasting is frequently applied in tasks to maintain the balance of the power system, while medium-term forecasting plays a crucial role in operation and planning [11], [114]. For long-term forecasting, it is typically used for grid expansion [108].

1) DEMAND FORECASTING

Demand forecasting plays a pivotal role in balancing generation and demand. However, besides the uncertainty from historical records and weather conditions, the flexible loads and prosumers who can consume and produce energy have increased the uncertainty and complexity of the task, especially for residential end-users [115]. The study [116] highlights that AI-based techniques perform well across all forecasting horizons and application domains, whereas conventional techniques are better suitable for long-term prediction at the utility level. In [114], different machine learning algorithms for building load prediction are analyzed. However, these centralized machine techniques cannot overcome challenges such as data privacy and security [19], [31], [32], [51], [74], communication overhead [25], [31], [32], [34], computational ability [63], data insufficiency [66], [77]; hence, the federated learning based model has been introduced, which can also be used to improve the model's scalability [74], [92] and the model generation ability [30], and to mitigate the problems of data heterogeneity [81], [92].

Most studies of FL applications for demand forecasting focus on short-term forecasting, but only a few studies on very short-term and long-term forecasting because AI-based algorithms can provide highly accurate short-term demand

forecasting at the regional level compared with traditional models [116]. Typically, the historical load dataset, along with some relevant information such as temperature and housing attributes, serves as the primary input data for short-term forecasting [32], [33]. For long-term forecasting at the regional level, more influential factors need to be considered, such as urbanization rate, resident population, carbon emission, load profile, and weather conditions [30]. These additional considerations significantly increase the complexity of long-term predictions compared to short-term predictions at the individual level.

As presented before, the literature indicates that load forecasting services are implemented at individual and aggregated levels. At the individual level, demand forecasting usually applies within a house or building, either residential, commercial, or campus building. The authors implement the LSTM model integrated with FL to predict the residential load with a one-hour horizon, considering the stochastic characteristic of the load [19]. The study [9] integrates an ANN with FL to forecast the short-term demand for a building to solve the data insufficiency problems. At the aggregated level, forecasting services can be applied to scenarios such as communities, EV networks, and virtual plants. Ref. [81] approaches a novel multi-center model-based FL with LSTM for load prediction of virtual power plants to improve the prediction accuracy. In this research, the virtual plant is considered an aggregator of electric vehicles, energy storage, flexible loads, and distributed generations. In [31] and [79], the authors apply LSTM for energy prediction in the EV charging station network.

Table 6 presents the data-driven model cooperated with FL utilized for demand forecasting based on various application domains and forecasting time intervals. Besides, it describes the evaluation metrics used for the data-driven models.

2) GENERATION FORECASTING

With the increasing integration of renewable energy resources, accurate generation prediction is essential to manage uncertainty. Initially, approaches mainly relied on physical models, which encountered challenging issues, including prior assumptions, complicated modeling processes, and unsatisfied forecasting results [35], [88], paving the way for data-driven approaches. However, these methods will suffer from issues including data privacy, heavy communication overheads, and data islands. Consequently, federated learning-based models have been proposed to alleviate these concerns [7], [35], [48], [53], [68], [88].

Several machine learning algorithms have been integrated with FL for renewable generation prediction. A federated framework utilizing the least square generative adversarial network (LSGAN) has been proposed for this purpose and the robustness of this method has been verified [35]. The research in [88] introduces an approach for PV power forecasting based on the CNN-LSTM model. This algorithm is also proposed for net-energy forecasting, analyzing the renewable generation profile and power consumption data [53]. The authors in [48] present an approach integrated with federated learning and Bayesian LSTM neural network (BayesLSTM-NN) to forecast solar irradiation and identify that the proposed approach can provide competitive performance compared with centralized BayesLSTM-NN and other state-of-the-art approaches. Additionally, fuzzy clustering is another possible solution for solar power forecasting [7].

Table 7 displays the data-driven approaches integrated with Fl for generation forecasting, including the datasets and metrics for evaluation.

3) VOLTAGE FORECASTING

Voltage forecasting is critical for distribution system operators (DSOs) to ensure the efficient, stable, and reliable operation of the distribution network. This becomes particularly important with the increasing integration of DERs including electric vehicles, distributed generation, and flexible loads, which contribute to voltage variations. While traditional voltage prediction methods have relied on network models and centralized data [118], [119], data-driven approaches, such as deep learning methods [120] and ensemble machine learning techniques [121], offer high accuracy but typically require extensive data collection.

Federated learning, introduced in [61], aims to mitigate these privacy issues while also data heterogeneity and data scarcity problems. This study proposes a privacy-preserving model that combine LSTM with federated learning for probabilistic nodal voltage prediction in local energy communities. It verifies that the performance outcomes of locally trained models and the trade-off between model performance and privacy can be optimized according to the privacy preference of the energy communities.

E. CONTROLS IN POWER SYSTEMS

Energy systems are transitioning from traditional to smarter, more efficient operations, necessitating more effective control approaches to manage the complex grids. Conventional control approaches typically focus on maintaining the system in a stable, reliable, and efficient way by adjusting the parameter settings, while these approaches are limited by the challenges of centralization of the real-time data. In contrast, smart energy systems require adaptive and data-driven control methods that can respond to fluctuations of energy resources and demand. Machine leaning-based control strategies, such as reinforcement learning (RL) and model predictive control, offer promising solutions. RL-based approaches, particularly those enhanced by deep learning, can provide optimal control strategies without the need for a predefined model. Meanwhile, MPC can optimize control strategies over a forecasting horizon for real-time energy management.

Integrating federated learning with these control approaches can mitigate the challenges of data privacy and security without centralization of data for model training. Such control approaches for energy systems can leverage the localized data, enhancing data privacy and security. Based

TABLE 6. Data-driven techniques collaborated with demand forecasting.

Ref.	Year	Data-driven technique	Data aggregation algorithm	Dataset source	Scenarios	Prediction horizon	Evaluation metrics	Contributions
[8][1]	2022	ANN	The optimizer Adam	The Irish CER dataset	Residential demand forecasting	Very short-term	MAE, RMSE	Achieving competitive performance
[9][3]	2021	ANN	The secure aggregation algorithm	The Building Data Genome Project (Miller and Meggers 2017)	Building energy demand forecasting	Short-term	MAE, MAPE, RMSE	Reducing the training time and addressing the data availability while reserving privacy
[19][1]	2020	LSTM	FedAvg	The Pecan Street Dataport	Residential demand forecasting	Short-term	MAPE, RMSE	Achieving high prediction accuracy with data preserving, reducing communication network load significantly
[25][1]	2022	LSTM	FedAvg, FedSGD	Green Button Connect My Data (CDM)	Residential demand forecasting	Short-term	MAPE, RMSE	Achieving higher accuracy while retaining data privacy
[26][1]	2022	CNN-LSTM	FedAvg	UK Power Networks led Low Carbon London project	Residential demand forecasting	Very short-term	MAE, MAPE	Reducing the computation time and communication overhead
[27]*[1]	2021	LSTM	FedAvg	The Pecan Street dataset	Residential building demand forecasting	Short-term	Hyperparameters selection, Prediction accuracy, communication efficiency	Achieving high prediction accuracy while data privacy preservation
[30][1]	2022	LSTM	Not mentioned	China Electricity Council, China Statistical Yearbook and China Energy Statistical Yearbook	Utility demand forecasting	Long-term	Not mentioned	Solving the problem of insufficient data, improving the model generalization ability
[31][1]	2019	DNN	Adam optimizer	The real data from charging stations in Dundee, UK between 2017 and 2018	Energy demand prediction for EV networks	Very short-term	RMSE	Achieving the accuracy and communication overhead reduction significantly
[32][1]	2021	RNN	FedAvg	HUE: The Hourly Usage of Energy Dataset for Buildings in British Columbia dataset	Residential demand forecasting	Short-term	Not-mentioned	Reducing the communication cost, speeding up the convergence
[33][1]	2020	LSTM	Average algorithm	Global Energy Forecasting Competition 2012 (CEFCom2012) and 2018 real load data of a State Grid provincial company	Regional load forecasting	Short-term	MAPE	Achieving accurate forecasting while retaining data privacy
[34][1]	2022	LSTM	FedAvg	The data was provided by EPCOR distribution company, Edmonton (not public)	Residential demand forecasting	Short-term	RMSE	Reducing the convergence time
[40][1]	2021	LSTM	FedAvg	CER in Ireland	Residential demand forecasting	Very short-term	MAE, NRMSE	Improving prediction accuracy while preserving data privacy
[51][1]	2021	LSTM	FedAvg	The Low Carbon London project delivered by UK power networks	Residential demand forecasting	Short-term	RMSE	Improving model performance and computational efficiency while maintaining the privacy
[55][1]	2022	LSTM-SAC	FedAvg	Nuuka open API from Helsinki	Utility demand forecasting	Short-term	MAPE, RMSE	Achieving competitive prediction accuracy while data privacy preservation, fast training time
[63][1]	2021	CNN	FedAvg	Dataset on daily basis collected from a building in Tomsk, Russia	Building heating load prediction	Short-term	MAE, MAPE, RMSE, R^2	Producing acceptable accuracy while preserving data privacy

TABLE 6. *(Continued.)* **Data-driven techniques collaborated with demand forecasting.**

[65][1]	2021	LSTM	FedAvg	Pecan Street Dataport	Residential demand prediction	Short-term	MAPE, RMSE	Achieving the model accuracy while retaining the privacy
[66][1]	2021	DNN	FedAvg	The ASHRAE dataset	Energy forecasting for smart building	Short-term	RMSLE	Reducing the training time, achieving enhancement of data privacy
[67][1]	2021	LSTM	FedAvg	Australian "Smart Grid, Smart City" customer trial dataset	Residential demand forecasting	Short-term	MAE, MAPE, RMSE	Improving prediction accuracy significantly without revealing the data
[69][1]	2021	LSTM	FedAvg	The Pecan Street dataset	Residential demand forecasting	Short-term	MAPE, RMSE	Achieving high prediction accuracy while data privacy preservation, decreasing communication overhead
[70][1]	2021	Regression	FedAvg	Smart meter data from campus	Campus building demand forecasting	Short-term	MAPE	Achieving high prediction accuracy while data privacy preservation
[73] [1]	2022	LSTM	FedAvg	Low Carbon London dataset	Residential load forecasting	Short-term	MSE, MAE, MAPE, RMSE	To gain accurate residential load without share the historical data
[74][1]	2021	LSTM	FedAvg	Dataset collected and published by the energy company UK power networks	Residential demand forecasting	Short-term	RMSE	Competitive forecasting performance while preserving data privacy, less training time, communication overhead reduction
[77][1]	2021	Decision Trees	Vertical SecureBoost	From the quarterly power consumption information of 1000 enterprises in a certain area of Jiangsu Province	Enterprise energy demand prediction	Long-term	MAE, MAPE, RMSE, R^2	Improving model accuracy
[79][1]	2021	LSTM	FedAvg	Dataset from the city of Dundee, UK	Energy demand forecasting for EV charging station network	Short-term	RMSE	Improving prediction accuracy significantly
[81][1]	2021	LSTM	Stochastic Gradient Descent (SGD)	The Irish Energy Regulatory Commission (CER)	Load prediction for virtual power plant	Short-term	MAPE, RMSE	Improving the accuracy and training efficiency while protecting privacy
[90][1]	2023	LSTM	Gradient descent method	Open dataset BDG2 (collecting energy consumption data from 1636 buildings across North America and Europe)	Building load prediction	Short-term	MAE, RMSE, MAPE, adjusted p-norm error	Achieving accuracy improvement greatly, addressing load volatility and data heterogeneity successfully
[91][1]	2023	LSTM	ECDH agreement, pair-wise masking	Building dataset BDGP2	Building load prediction	Short-term	CV, MAE, MAPE, RMSE	Achieving good performance while preserving data privacy, addressing data insufficiency, good scalability
[92][1]	2022	LSTM	FedAvg	Solar Home Electricity Data from Ausgrid	Residential demand forecasting for retail energy providers	Very short-term	MSE	Achieving competitive prediction accuracy while data privacy preservation

on the control domains, controls in energy systems can be classified into three types: energy management systems, voltage control, and energy trading, which are crucial for maintaining the grid system in a stable and reliable operation.

TABLE 7. Data-driven techniques collaborated with FL for generation forecasting.

Ref.	Year	Data-driven technique	Data aggregation algorithm	Dataset source	Scenarios	Prediction horizon	Evaluation metrics	Contributions
[7][1]	2022	Clustering	Stochastic gradient descent (SGD),	AMS 2013-2014 solar energy prediction contest	Solar power generation	Very short-term	The average accuracy	Prediction accuracy improvement, and the communication overhead reduction
[35][1]	2021	LSGANs	FedAvg	National Renewable Energy Laboratory (NREL)	Wind and solar power generation forecasting	Very short-term	MAE, RMSE, FID, NMD, 1-NN, ES	Competitive performance without scarifying the data privacy; communication overhead reduction; reducing the vulnerability for data leakage and cyber attacks
[38][1,2]	2022	Decision tree	FederBoost with SecureBoost	Smart City project in China	Distributed power forecasting	Very short-time	MSE	Improving communication delay, addressing data heterogeneity
[48][1]	2020	BeyesLSTM -NN	FL With Differential Privacy	Datasets collected in Ningxia, China; Kansas, the United States; benchmark dataset of Folsom, the United States	Solar power generation forecasting	Short-term	MAE, NRMSE, continuous rank probability score (CRPS), the CRPS skill score (CRPSS)	Achieve good performance with data privacy preservation
[53][1]	2022	CNN-LSTM	Baby-step giant-step algorithm	Real power consumption and generation readings released by Ausgrid	Net-energy forecasting	Very short-term	MAE, MAPE, RMSE	Lowering the computation overhead, achieving the competitive accuracy while preserving data privacy
[68][1]	2021	DNN	FeSGD	The Pecan Street dataset	DER prediction	Very short-term	RMSE	Accurate prediction while data privacy preservation
[71][1]	2022	CNN	Not-mentioned	Dataset from Iran	Wind power forecasting	Short-term	RMSE, MAE, MAPE	Preserving data privacy and security. accurate performance
[72][1]	2023	Actor-critic	FedAvg	Wind farm in Washington state, USA	Wind power Forecasting	Very short-term	NMAE, NRMSE	Achieving more accurate prediction with privacy preservation; reducing the network load
[88][1]	2022	CNN-LSTM	Semi-asynchronous aggregation	German Solar Farm dataset with 21 PV facilities	PV forecasting	Short-term	RMSE	Achieving better forecasting performance with data privacy preservation

1) ENERGY MANAGEMENT SYSTEMS

Energy management systems are typically used to improve energy efficiency by optimizing the schedule of power devices adopted in the power system through demand response programs, including flexible loads, energy storage systems, electric vehicles, and renewable generation sources. This section will address energy management systems (EMS) in the distribution grid and microgrid levels, covering applications in residential homes, multiple homes, EV charging stations, and shared energy storage, utilizing machine learning techniques collaborated with FL-based methods. As presented in [107], AI-based approaches are promising tools to address the challenges of EMS in the digital era, aiding in decision-making and scheduling the devices when considering the preferences of the end-users. These studies on this topic have witnessed a sharp increase in recent years.

Centralized energy management systems aggregate the load demand information of the end-users, potentially violating data privacy. Federated learning has been applied in [28], [41], [49], [62], [78], and [89] to address privacy concerns. Meanwhile, the authors in [28], [62], and [78] aim to achieve computational complexity and communication overhead reduction, respectively.

A systematic review [122] of reinforcement learning approaches to the control of power and energy illustrates why reinforcement learning (RL) can provide optimal solutions related to optimization and control issues. RL is capable of deriving optimal operation data from historical information through continuous interaction with the environment, without relying on the physical models. Its scalable learning strategy makes it well-suited for online decision-making and can be widely applied in demand-side management. In [78], a Q-learning-based RL framework is proposed to optimize the energy demand of vehicle-to-grid (V2G) networks.

In addition, deep reinforcement learning (DRL)-based EMS has been applied in studies [28], [41], [49], [62], [89], with actor-critic algorithms utilized in [28], [49], [62],

TABLE 8. Data-driven techniques collaborated with FL for energy management systems.

Ref.	Year	Data-driven techniques	Data aggregation algorithm	Application domain	The data-driven model as comparison	Contributions
[28][3]	2021	SAC	FedSGD	Distribution Grid EV charging stations	Soft actor–critic	Fast convergence, better performance
[37][1]	2020	ANN	Not-mentioned	Virtual power plant	Conventional model, individual learning model	Speeding up convergence, improving data privacy and security
[41][1]	2022	DRL	Not mentioned	Residential	(1) Local based load forecasting + local based EMS, (2) Cloud based load forecasting + local based EMS; (3) Federated learning-based load forecasting + local based EMS (4) Federated learning-based load forecasting + federated learning -based EMS	Increase system speed to better performance
[46][1]	2021	Not-mentioned	Federated cluster average algorithm (FedClusAvg).	Distribution grid	FedAvg	Reducing the communication rounds
[49][1]	2021	Actor-critic	FedAvg	Distribution Grid	Centralized actor-critic method, Q-learning, and double Q-learning	Fast Convergence and Communication rounds reduction
[58][1]	2022	LSTM	FedAvg	Office building	Central, CNN, ResNet, DenseNet	Decreasing training time and network load
[62][1]	2022	A2C	Federated stochastic gradient descent (FedSGD)	Microgrid, Multiple homes	DRL without FL	Communication overhead reduction and data privacy preservation
[78][1]	2022	Q-learning	FedAvg	Distribution Grid EV integration network	The baseline centralized methods	80% Communication overhead reduction, computation time reduction by 15 times
[89][1]	2021	Actor-critic	FedSGD	Microgrid Shared energy storage	Distributed multi-agent model without FRL, Mixed-integer linear programming optimization	Fast convergence, more economical energy consumption scheduling

and [89]. The following research studies related to demand response (DR) programs apply DRL techniques. A DRL framework based on A2C has been proposed in [62] to optimally schedule the consumption of devices, including air conditioners (ACs), energy storage systems (ESSs), and washing machines (WMs), across multiple homes considering the comfort of residential users. A federated DRL with an actor-critic method is designed for HEMS with respect to real-time pricing [49]. Reference [28] creates an EMS integration with model-free based DRL with the SAC method to maximize the revenues of multiple electric vehicle stations. A DRL model with an actor-critic method is used to optimize the scheduling of a shared ESS for three smart buildings [89]. In [41], The author proposes a new approach based on DRL to reduce the standby energy in residential buildings.

Besides RL-based control models, model predictive control (MPC) offers another strategy for data-driven energy management. MPC employs a mathematical model to forecast future behavior and optimizes control inputs to minimize a defined cost function. This predictive capability proves particularly effective in real-time energy management, as illustrated by the stochastic MPC approach implemented in [123]. Additionally, [124] developed a model predictive approach for cost optimization by optimizing the electrical assets in real-time energy markets.

While research on combining MPC with federated learning is still emerging, [125] implemented a decentralized model of predictive control and federated learning. This innovative approach aims to achieve an effective and efficient solution for energy management, providing optimal performance in precision, convergence speed, and scalability.

Table 8 illustrates the data-driven techniques used in collaboration with FL for energy management systems. It also details the application domain, the model used for comparison, and contributions.

2) VOLTAGE CONTROL

Renewable energy resources have been increasingly integrated into the distribution grid, leading to significant challenges concerning grid voltage, such as voltage rise and voltage fluctuation, which require advanced operation and control strategies [126]. The traditional regulation strategy is applied by regulating the on-load tap changers of transformers and shunt capacitor banks, but this approach rarely used in practice since system-level regulation fails provide accurate and on-time services based on historical data [54], [126]. As discussed in the review literature [127], various control approaches, including centralized, decentralized, and decentralized coordinated control methods, have been employed to enhance voltage regulation performance. With the digitalization of the distribution grid, data-driven methods, which are used to optimize the operation of the grid based on historical data or the data collected from AMI, have drawn more attention.

TABLE 9. Data-driven techniques collaborated with FL for voltage control.

Ref.	Year	Data-Driven Technique	Data aggregation algorithm	Application Domain	Contributions
[29][1]	2022	SAC	Stochastic gradient descent (SGD)	Decentralized Voltage Control in Distribution Networks	Enhancing scalability, privacy and communication efficiency remarkably
[54][1]	2022	GCN	Weighted averaging	Local Voltage Control for DGs	Effectively enhancing the adaptability to fast DG fluctuations and privacy preserving

TABLE 10. Data-driven techniques collaborated with FL for energy trading.

Ref.	Year	Data-driven Technique	Data-driven aggregation algorithm	Application domain	Contributions
[59][1]	2021	Game theory	Weighted average based on homomorphic encryption	Wholesale market	Enable energy trading transparent, and data privacy protection
[60][1]	2022	CNN	FedAvg	Microgrid	To develop the P2P trading platform and increase the efficiency
[64][1]	2022	Clustering	FeSGD	Microgrid	To introduce a Secure and safe trading platform

Table 9 outlines the data-driven techniques incorporated with FL for voltage control in distribution grids. As illustrated in [128], DRL is an effective approach for voltage control due to its feedback-based nature. A federated multi-agent-based DRL framework with a soft actor-critic algorithm is developed in [29] for voltage regulation in distribution networks. Federated learning is used for its ability to address significant challenges, such as heavy communication overhead and data privacy concerns, which are often encountered by centralized learning systems. Compared to centralized approaches, scalability, and privacy have been improved by the decentralized model while similar convergence is maintained. In [54], a local voltage regulation method based on cloud-edge collaboration is introduced for a distributed network with distributed generators (DGs) integration. A graph convolutional neural network (GCN) serves as a surrogate model at the cloud level to estimate the voltage, and federated learning is used in the inter-area coordination to update the parameters of the control curves for DGs, thereby preserving the data privacy related to DG behaviors.

3) ENERGY TRADING

To facilitate the current energy system's transition towards sustainability, energy trading services are essential in adapting to the new energy infrastructure. Recently, data-driven approaches have been applied in the electricity market, including both the wholesale and distributed local energy markets, to optimize the activities of participants like energy communities, prosumers, and operators.

The deployment of blockchain technology, a decentralized ledger system, enables energy trading or sharing within a P2P market, allowing participants to directly exchange energy using smart contracts [60], [64]. In [59], a bidding application combining blockchain and federated learning is proposed for power plants in the wholesale electricity market, where federated learning is used for cost data aggregation while maintaining privacy and security. The researchers in [64] develop a decentralized trading platform for prosumers, optimizing the energy resource request based on profit maximization with the aid of federated learning. Similarly, a Peer-to-peer (P2P) energy trading framework assisted by blockchain and FL is formulated in [60], enabling autonomous transactions between active participants in microgrids. Besides, CNN integrated with FL is used for demand prediction for the smart contract.

Table 10 displays federated learning applications for energy trading in the energy system, identifying the application level and contributions.

F. ANOMALY DETECTION

The rapid integration of Internet of Things (IoT) technologies is transforming the power grid to an advanced cyber-physical system in monitoring, communication, control, as well as other services. While this transition improves reliability and energy efficiency, it also increases the vulnerability to anomaly threats such as cyber-attacks [39], [108]. Currently, anomaly detection approaches are used to distinguish or identify unusual data from the distribution of normal datasets. According to [129], many detection methods including statistical, classical analysis, and machine learning-based approaches) are applied to detect an anomaly. This subsection will focus on the machine learning techniques combined with FL to address communication efficiency issues and privacy concerns [39], [43], [80], [87]. Additionally, FL is employed to address the issues of data heterogeneity, which is challenging for an accurate model generation [80].

TABLE 11. Data-driven techniques collaborated with FL for anomaly detection.

Ref.	Year	Data-driven technique	Data aggregation algorithm	Application domain	Dataset sources	Evaluation metrics	Contributions
[39][1]	2022	GAN	FedGMA	Transmission system	Three open-source power datasets, comprising records of normal, disturbance, control, and cyberattack traffic belonging to the electric transmission systems	Accuracy, F1-score	High detection accuracy; robust detection performance; improve the communication efficiency
[43][1]	2022	DNN	FedAvg	AMI	NSL-KDD dataset	Accuracy, recall, precision F1-score, computational cost	Maintain the privacy; better performance for detection
[80][1]	2021	LSTM	Weighted averaging	PV systems	Using the hardware OPAL-RT simulator that can provide real-time simulation for cyber security by recreating cyberattacks	Convergence, communication overhead, local computation cost	High detection accuracy; improve the privacy; high communication efficiency
[87][1]	2022	Autoencoders	Weighted aggregation	Energy storage deployment	The local measurement dataset	Precision, recall	Privacy protection, effective detection of anomalous batteries

Table 11 lists recent academic studies on data-driven techniques with FL for anomaly detection in smart grids. Besides, it specifies the application domain and evaluation metrics. In the context of power electronics, the author proposed an FL-based frame with an LSTM model for false data injection detection in PV systems, verifying that this approach achieves competitive accuracy compared to the centralized approach [80]. A promising solution based on semi-supervised generative adversarial networks (GANs) is presented to deal with the small scale of labeled data and class-imbalanced data in the smart grid [39]. The artificial metering infrastructure (AMI) system, crucial for information exchange between the power system devices, including energy management systems, DGs, and energy storage systems, is vulnerable to security threats. In [43], a federated method utilizing a deep neural network (DNN) model is developed for intrusion detection, and this method is implemented in the NSL-KDD dataset. This method outperforms centralized models in detection rate for R2L attacks and detection accuracy for U2R attacks, approximately 7% and 60% −70%, respectively. Furthermore, [43] offers a solution for anomaly detection based on an autoencoder implemented in a distributed manner, suitable for early deployment stage in energy storage systems without relying on the previous dataset.

VI. DISCUSSION

A. FL-BASED APPLICATIONS IN THE POWER AND ENERGY SECTOR

This study has conducted a comprehensive technical assessment of federated learning applications in the power and energy sector, focusing on the data-driven techniques combined with FL for advancing energy services. Federated learning is typically employed in collaboration with other machine learning techniques to implement services that address issues such as data privacy protection, data insufficiency, data silos, data heterogeneity, communication overhead reduction, computational complexity reduction, and scalability improvement. More importantly, FL-based applications in the energy sector have been identified, specifically in the areas such as NILM, forecasting services, energy management systems, fault detection, energy theft detection, voltage control, anomaly detection, and energy trading.

Furthermore, the previous section presented an analysis of how machine learning techniques collaborated with FL to improve the model performance for each identified application in the energy sector, highlighting the core point of this study. Fig. 9 maps the recent literature on the collaborated data-driven techniques and energy services and outlines the interrelationships among the most-applied techniques, categories of machine learning, corresponding application services, and application domains.

This graph analyses the interrelationships among the four previously mentioned dimensions. As presented, it reveals that currently, the application of federated learning in small customers (mainly in residential domains), microgrid, and distribution grids domains, is attracting more focus from researchers than other domains. In addition, most of the literature on FL applications in the energy sector concentrates on solving NILM and forecasting problems, while fewer studies are focused on fault detection, energy theft detection, voltage control, and energy trading problems. Notably, among forecasting services, demand forecasting emerges as one of the most addressed topics in microgrid and distribution domains.

The collaboration of data-driven techniques has been analyzed for applications in the energy sector. Generally, machine learning algorithms, ranging from unsupervised machine learning to deep learning, have been prominent in recent related publications. Deep learning is the most-applied machine learning algorithm to integrate with FL to implement

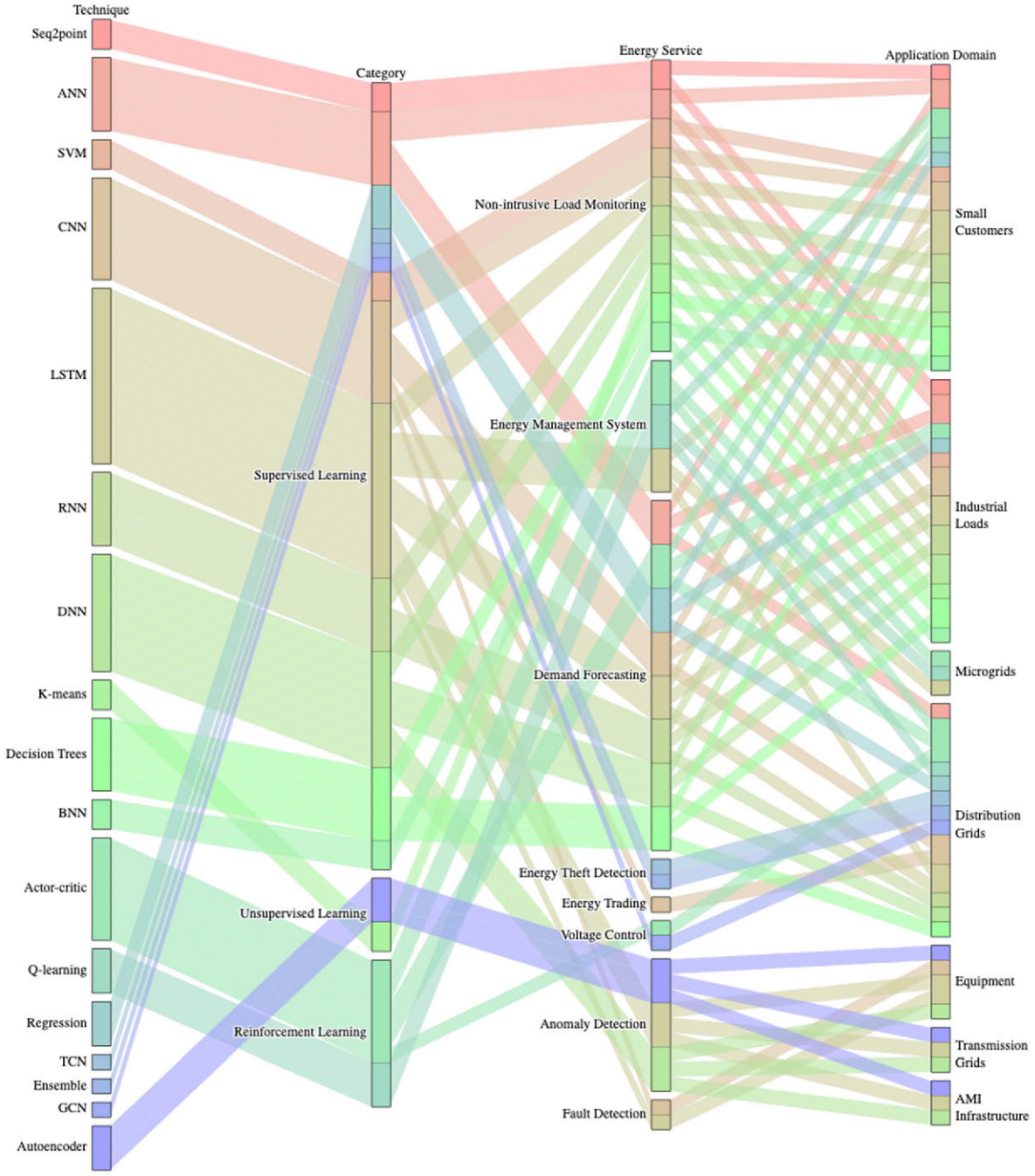

FIGURE 9. The interrelation between energy services and the most-used machine learning techniques integrated with FL in literature from 2019 until 2023.

energy services, especially in non-intrusive load monitoring, demand forecasting, and generation forecasting services. As to energy management systems and voltage control, reinforcement learning is widely applied due to its suitability for addressing power system control and operation problems in power systems. Among the data-driven techniques employed for fault detection, only deep learning models are used. Seq2point is the most used deep learning model for NILM service. For forecasting applications, LSTM and CNN are usually used to collaborate with FL. Actor-critic and Q-learning are the most used reinforcement learning algorithms for energy management systems and voltage control.

B. OPPORTUNITIES AND CHALLENGES

Federated learning has recently attracted more attention from researchers for its applications in power systems, aiming to provide innovative energy services to address the challenges due to energy digitalization. However, this kind

of federated learning integrated application is still in the research phase, with the validation stage yet to be fully developed. This brings new challenges resulting from the features of distributed algorithms. This section will discuss the opportunities and challenges of applying FL to power systems. The opportunities are outlined below:

- Data privacy and security: the decentralized nature of FL has been effectively used in scenarios involving sensitive user data. FL is a distributed learning algorithm that does not need to transfer the data from the edge devices to the central device for model training as that centralized learning algorithm acts. For instance, the study [25] introduced the federated learning process of how sensitive data like the consumption habits of customers will be protected. FL just transmits the parameter updates needed for the global model. This effectively avoids data leakage and protects data privacy and security. It is noteworthy that although centralized FL can be employed to address concerns about privacy and security, it still encompasses centralization of the data and model updates in the training process, which may not align with the application that needs to fulfill stringent privacy requirements. In [44], decentralized FL provides inherent advantages for data privacy and security since model training and aggregation are distributed across clients without centralization of model updates.
- Communication overhead reduction and scalability: traditional centralized methods need intensive computation for model training, and this will have negative implications on communication efficiency and scalability when aggregating data from numerous edge devices. In contrast, FL algorithms enable the intelligent edge devices to implement most of the computation that normally happens at the central cloud, transferring the central computing to edge computing [29] and [74]. This shift reduces the communication overhead of the network and improves scalability remarkably.
- Data availability: typically, machine learning methods require massive datasets for training to avoid overfitting, but data sharing between owners can impose the threat of data leakage. The research in [19] illustrates how federated learning can be employed for collaborative model training across different houses, allowing the model training without sacrificing customers' privacy.

The challenges are listed as follows:

- Communication efficiency enhancement: as presented in [130], FL is more time-consuming for the training process and has higher computational costs than traditional ML algorithms. Most recent work focuses on communication size reduction to reduce the training time in each iteration of the FL training process [6]. While computation ability can be enhanced through the adoption of advanced infrastructures and techniques for higher computing performance, there is still a notable gap in research on how to optimize the balance of communication and computation effort in such applications.
- Improvement of ICT infrastructures: besides the communication size reduction, enhancing ICT infrastructure can also improve training efficiency. However, improving ICT infrastructure, including communication networks, intelligent devices and central devices, involve significant investments. Hence, further research is needed to identify the optimal tradeoff between investment and the enhancement of the ICT infrastructure.
- Better data aggregation algorithms: federated aggregation algorithm is used to work on data aggregation in a central server and the agent updates [65]. For a specific scenario, a suitable aggregation algorithm needs to be selected. For example, FedProx and FedAvg have good performance when dealing with non-IID (non-identically and independently distributed) datasets, such as the AMI metering data from different residential buildings [4]. FedGMA has fast convergence abilities compared to other aggregation algorithms such as FedAvg, FedProx, and FedSRC [39]. Additionally, FedAvg can achieve faster convergence and lower communication costs due to fewer training iterations than typical algorithms [4]. Therefore, customizing a suitable aggregation algorithm is demanding.
- Robustness to cyber-attacks: machine learning techniques are known to be vulnerable to certain typical attacks, such as malicious attacks. However, federated learning is even more sensitive to security issues due to its inherent distribution natures, especially for centralized federated learning. It will be difficult to determine the fault detection approach for attack identification that can provide satisfactory security for federated learning applications.
- Collaborative ML techniques in FL framework: FL operates as a collaborative machine learning algorithm, allowing integration with various machine learning techniques to provide good performance in energy services. Hence, the selection of suitable collaborative learning techniques is a challenge. For example, reinforcement learning is typically used for power system control and operation, and then reinforcement learning integrated FL is validated to perform well in energy management systems and voltage control [28], [29], [89].

Moreover, the deployment of federated learning in power systems faces unique challenges due to the distinctive attributes of power system infrastructure. These challenges are further compounded by the stringent requirements for reliability and security inherent to this critical domain.

- Data privacy and regulation: data extracted from power systems, including power measurements, grid operation data, and smart metering measurements for the end-user, is highly sensitive. It is essential to follow the regulations and laws to preserve data privacy such as the General Data Protection Regulation (GDPR) and the European Program for Critical Infrastructure Protection (EPCIP). FL inherently offers a structure that promotes

data privacy since it is training models locally. However, there is still unintended data leakage by analyzing the gradients during the training process [131]. Therefore, the actual effectiveness of federated learning in offering real privacy protection remains a question and requires assessment and verification. Additionally, techniques like differential privacy are adopted within power systems when processing sensitive data or undisclosed data (e.g., user data, operational data, smart meter data), as they provide a quantifiable privacy guarantee by introducing some noises to the model updates. The extent and manner of applying differential privacy depend on the desired balance between privacy and model utility.

- Model evaluation: evaluating models in decentralized FL setups is particularly challenging. With each node holding limited data, these non-IID data, which may have distinct characteristics and distributions, will result in difficulty in achieving convergence, which is a key factor for model evaluation. Another challenge is the limited generalization potential of FL in low data availability settings. With limited data, it is rather difficult to train a model that can generalize effectively on unknown data. This may lead to poor performance of the global model. Additionally, there is a lack of access to the data on each node during evaluation, which will make it challenging to evaluate the performance of the global model on each node [131], [132].
- Initial model origin: in federated learning, a significant concern regarding the origin of the initial model is its potential to compromise data privacy. Generally, the central server distributes an initial model to the clients for training. This initial model is typically trained on a large dataset that may contain sensitive information. If this initial model is shared with the clients, it can potentially leak information about the training data and compromise privacy. Besides, transferring the model updates between the central server and clients will also encounter data privacy issues because some private information can be revealed from the model updates [131], [132].
- Success or failure of FL performance: the effectiveness of FL, particularly with non-IID data, can be influenced by several factors [132]:
  - Data availability: data availability plays a crucial role in federated learning; limited data availability can lead to poor performance and convergence issues.
  - Data heterogeneity: non-IID data, which exhibits significant variations across different agents, affects model generalization ability and convergence effectively.
  - Convergence: federated learning relies on the assumption that each agent generates non-IID data. If the assumption is violated, such as concept drift or non-IID, it can lead to convergence issues.
  - Causal relationships: FL struggles to learn correct causal relationships, particularly with non-IID data. This will limit the ability of the model to make precise forecasting, which will impact the downstream optimization tasks.
  - Domain augmentation: domain-informed data augmentation would determine the success of FL with non-IID data. By incorporating the data with domain features, the model will perform better in convergence and generalization.

These challenges highlight the complexity of applying federated learning within energy services. It indicates that issues related to privacy, evaluation, and robustness need to be addressed, considering energy infrastructure, where the requirements for reliability and security is high and strict. Hence, not only the technical challenges need to be fulfilled but also regulatory ones, ensuring that FL can provide the services needed while following the rules of the power system operations.

VII. CONCLUSION

Driven by the widespread deployment of intelligent devices across the grid, the current energy sector is undergoing rapid digitalization, handling an extremely large amount of data. However, the data-driven techniques essential for enhancing the efficiency of power systems are experiencing communication overhead issues and also present challenges in data privacy. This paper presents a comprehensive analysis of the integration of federated learning with machine learning techniques within the power sector, showcasing its potential to tackle challenging issues such as data privacy and security, heavy communication overhead, and data insufficiency problems. By utilizing data from intelligent devices like smart meters and sensors, these FL-based solutions provide important contributions to the efficiency and security operation of distribution grids.

Besides, how to detect errors or anomalies needs to be illustrated when applying federated learning algorithms. Generally, machine learning algorithms can effectively identify obvious errors in data by performing basic validation checks, such as verifying ranges, formats, and consistency. Additionally, these models are trained to recognize patterns indicating errors or inaccuracies by comparing observed data with expected outcomes. For the federated learning algorithm, the averaging algorithm can help mitigate inaccuracies by averaging model updates from various clients, thus enhancing the model's accuracy and robustness. However, the fact that federated learning strategies cannot have access to the entire dataset, limits the direct examination of data for error or anomaly detection, requiring the algorithms for local data examination.

Specifically, this research makes several significant contributions to the potential use of research in federated learning applications in the field of power systems. Firstly, it provides a clear identification and classification of energy services within power systems that can benefit from FL,

including NILM, energy forecasting, fault detection, energy theft detection, energy management systems, voltage control, and energy trading. This categorization establishes a foundational framework for integrating FL to enhance grid operations and services.

Secondly, this study conducts a holistic review and critical analysis of machine learning techniques enabling FL-based energy services. It maps the benefits, challenges, and innovative approaches of FL to the corresponding energy services. Importantly, this paper highlights the data-driven techniques, federated learning algorithms, and aggregation algorithms employed, as well as the application scenarios and contributions of each reviewed study, thereby providing a comprehensive resource for future research in this area.

Thirdly, this paper delves into the interrelationships between machine learning techniques and grid services, highlighting a significant increase in federated learning applications for NILM and forecasting services (including demand and generation forecasting). Notably, deep learning is used as the primary learning algorithm combined with federated learning for these services, while reinforcement learning stands out in energy management systems and voltage control applications. This mapping illustrates the effectiveness of FL in addressing a wide range of energy service needs.

Finally, this paper also outlines future opportunities and challenges regarding FL applications in power systems. FL-based solutions for energy applications can outperform traditional centralized learning methods by addressing data privacy, data security, and data islands issues. However, there are also some challenges to overcome, especially in communication capacity enhancement, optimal data aggregation algorithm selection, ensuring robustness against cyber-attacks, and choosing effective collaborative machine learning algorithms.

ACKNOWLEDGMENT

The authors thank Prof. Marta Aguilar from UPC for proofreading the article.

REFERENCES

[1] N. Good, K. A. Ellis, and P. Mancarella, "Review and classification of barriers and enablers of demand response in the smart grid," *Renew. Sustain. Energy Rev.*, vol. 72, pp. 57–72, May 2017.

[2] M. H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci, and M. Radenkovic, "Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 2814–2825, Jul. 2018.

[3] K. Zhou, C. Fu, and S. Yang, "Big data driven smart energy management: From big data to big insights," *Renew. Sustain. Energy Rev.*, vol. 56, pp. 215–225, Apr. 2016.

[4] N. Hudson, M. J. Hossain, M. Hosseinzadeh, H. Khamfroush, M. Rahnamay-Naeini, and N. Ghani, "A framework for edge intelligent smart distribution grids via federated learning," in *Proc. Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2021, pp. 1–9.

[5] S. Barja-Martinez, M. Aragués-Peñalba, Ì. Munné-Collado, P. Lloret-Gallego, E. Bullich-Massagué, and R. Villafafila-Robles, "Artificial intelligence techniques for enabling big data services in distribution networks: A review," *Renew. Sustain. Energy Rev.*, vol. 150, Oct. 2021, Art. no. 111459.

[6] Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, Y. Li, X. Liu, and B. He, "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 4, pp. 3347–3366, Apr. 2023.

[7] E. Yoo, H. Ko, and S. Pack, "Fuzzy clustered federated learning algorithm for solar power generation forecasting," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 4, pp. 2092–2098, Oct. 2022.

[8] Y. Wang, N. Gao, and G. Hug, "Personalized federated learning for individual consumer load forecasting," *CSEE J. Power Energy Syst.*, vol. 9, no. 1, pp. 326–330, Jan. 2023.

[9] J. Li, C. Zhang, Y. Zhao, W. Qiu, Q. Chen, and X. Zhang, "Federated learning-based short-term building energy consumption prediction method for solving the data silos problem," *Building Simul.*, vol. 15, no. 6, pp. 1145–1159, Jun. 2022.

[10] X. Cheng, C. Li, and X. Liu, "A review of federated learning in energy systems," in *Proc. IEEE/IAS Ind. Commercial Power Syst. Asia*, Jul. 2022, pp. 2089–2095.

[11] L. Li, Y. Fan, M. Tse, and K. Y. Lin, "A review of applications in federated learning," *Comput. Ind. Eng.*, vol. 149, Nov. 2020, Art. no. 106854.

[12] P. M. Mammen, "Federated learning: Opportunities and challenges," 2021, *arXiv:2101.05428*.

[13] S. Banabilah, M. Aloqaily, E. Alsayed, N. Malik, and Y. Jararweh, "Federated learning review: Fundamentals, enabling technologies, and future applications," *Inf. Process. Manag.*, vol. 59, no. 6, Nov. 2022, Art. no. 103061.

[14] T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, and A. S. Avestimehr, "Federated learning for the Internet of Things: Applications, challenges, and opportunities," *IEEE Internet Things Mag.*, vol. 5, no. 1, pp. 24–29, Mar. 2022.

[15] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 46–51, Jun. 2020.

[16] N. Victor, M. Alazab, S. Bhattacharya, S. Magnusson, P. K. R. Maddikunta, K. Ramana, and T. R. Gadekallu, "Federated learning for IoUT: Concepts, applications, challenges and opportunities," 2022, *arXiv:2207.13976*.

[17] Q. Li, J. Ye, W. Song, and Z. Tse, "Energy disaggregation with federated and transfer learning," in *Proc. IEEE 7th World Forum Internet Things (WF-IoT)*, Jun. 2021, pp. 698–703.

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

[19] A. Taïk and S. Cherkaoui, "Electrical load forecasting using edge computing and federated learning," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[20] Q. Liu, B. Yang, Z. Wang, D. Zhu, X. Wang, K. Ma, and X. Guan, "Asynchronous decentralized federated learning for collaborative fault diagnosis of PV stations," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1680–1696, May 2022.

[21] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowl.-Based Syst.*, vol. 216, 2021, Art. no. 106775.

[22] F. Li, J. Qin, and W. X. Zheng, "Distributed Q-learning-based online optimization algorithm for unit commitment and dispatch in smart grid," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 4146–4156, Sep. 2020.

[23] A. Azari and C. Cavdar, "Self-organized low-power IoT networks: A distributed learning approach," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–7.

[24] X. Cui, Z. Liang, Y. Chai, W. Chen, R. Yu, and G. Ruan, "Privacy-preserving operation of interconnected distribution networks with soft open points," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2023, pp. 1–5.

[25] M. N. Fekri, K. Grolinger, and S. Mir, "Distributed load forecasting using smart meter data: Federated learning with recurrent neural networks," *Int. J. Electr. Power Energy Syst.*, vol. 137, May 2022, Art. no. 107669.

[26] Y. Shi and X. Xu, "Deep federated adaptation: An adaptative residential load forecasting approach with federated learning," *Sensors*, vol. 22, no. 9, p. 3264, Apr. 2022.

[27] J. Gao, W. Wang, Z. Liu, M. F. R. M. Billah, and B. Campbell, "Decentralized federated learning framework for the neighborhood: A case study on residential building load forecasting," in *Proc. 19th ACM Conf. Embedded Networked Sensor Syst.*, Nov. 2021, pp. 453–459.

[28] S. Lee and D.-H. Choi, "Dynamic pricing and energy management for profit maximization in multiple smart electric vehicle charging stations: A privacy-preserving deep reinforcement learning approach," *Appl. Energy*, vol. 304, Dec. 2021, Art. no. 117754.

[29] H. Liu and W. Wu, "Federated reinforcement learning for decentralized voltage control in distribution networks," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3840–3843, Sep. 2022.

[30] Z. Shen, Q. Wu, J. Qian, C. Gu, F. Sun, and J. Tan, "Federated learning for long-term forecasting of electricity consumption towards a carbon-neutral future," in *Proc. 7th Int. Conf. Intell. Comput. Signal Process. (ICSP)*, Apr. 2022, pp. 789–793.

[31] Y. M. Saputra, D. T. Hoang, D. N. Nguyen, E. Dutkiewicz, M. D. Mueck, and S. Srikanteswara, "Energy demand prediction with federated learning for electric vehicle networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[32] Y. L. Tun, K. Thar, C. M. Thwal, and C. S. Hong, "Federated learning based energy demand prediction with clustered aggregation," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Jan. 2021, pp. 164–167.

[33] J. Li, Y. Ren, S. Fang, K. Li, and M. Sun, "Federated learning-based ultra-short term load forecasting in power Internet of Things," in *Proc. IEEE Int. Conf. Energy Internet (ICEI)*, Aug. 2020, pp. 63–68.

[34] N. Gholizadeh and P. Musilek, "Federated learning with hyperparameter-based clustering for electrical load forecasting," *Internet Things*, vol. 17, Mar. 2022, Art. no. 100470.

[35] Y. Li, J. Li, and Y. Wang, "Privacy-preserving spatiotemporal scenario generation of renewable energies: A federated deep generative learning approach," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2310–2320, Apr. 2022.

[36] Y. Wang, M. Jia, N. Gao, L. Von Krannichfeldt, M. Sun, and G. Hug, "Federated clustering for electricity consumption pattern extraction," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2425–2439, May 2022.

[37] Z. Wang, M. Ogbodo, H. Huang, C. Qiu, M. Hisada, and A. B. Abdallah, "AEBIS: AI-enabled blockchain-based electric vehicle integration system for power management in smart grid platform," *IEEE Access*, vol. 8, pp. 226409–226421, 2020.

[38] H. Liu, X. Zhang, X. Shen, and H. Sun, "A fair and efficient hybrid federated learning framework based on XGBoost for distributed power prediction," 2022, *arXiv:2201.02783*.

[39] M. Abdel-Basset, N. Moustafa, and H. Hawash, "Privacy-preserved generative network for trustworthy anomaly detection in smart grids: A federated semisupervised approach," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 995–1005, Jan. 2023.

[40] M. Biswal, A. S. M. Tayeen, and S. Misra, "AMI-FML: A privacy-preserving federated machine learning framework for AMI," 2021, *arXiv:2109.05666*.

[41] J. Gao, W. Wang, and B. Campbell, "Poster abstract: Residential energy management system using personalized federated deep reinforcement learning," in *Proc. 21st ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, May 2022, pp. 541–542.

[42] S. Hou, J. Lu, E. Zhu, H. Zhang, and A. Ye, "A federated learning-based fault detection algorithm for power terminals," *Math. Problems Eng.*, vol. 2022, pp. 1–10, Jul. 2022.

[43] H. Liang, D. Liu, X. Zeng, and C. Ye, "An intrusion detection method for advanced metering infrastructure system based on federated learning," *J. Mod. Power Syst. Clean Energy*, vol. 11, no. 3, pp. 927–937, May 2023.

[44] A. Giuseppi, S. Manfredi, D. Menegatti, A. Pietrabissa, and C. Poli, "Decentralized federated learning for nonintrusive load monitoring in smart energy communities," in *Proc. 30th Medit. Conf. Control Autom. (MED)*, Jun. 2022, pp. 312–317.

[45] J. Zhang, Y. Wang, K. Zhu, Y. Zhang, and Y. Li, "Diagnosis of interturn short-circuit faults in permanent magnet synchronous motors based on few-shot learning under a federated learning framework," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8495–8504, Dec. 2021.

[46] Y. Li, X. Li, G. Li, and Z. Li, "Privacy protection in prosumer energy management based on federated learning," *IEEE Access*, vol. 9, pp. 16707–16715, 2021.

[47] J. Lin, J. Ma, and J. Zhu, "Privacy-preserving household characteristic identification with federated learning method," *IEEE Trans. Smart Grid*, vol. 13, no. 2, pp. 1088–1099, Mar. 2022.

[48] X. Zhang, F. Fang, and J. Wang, "Probabilistic solar irradiation forecasting based on variational Bayesian inference with secure federated learning," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7849–7859, Nov. 2021.

[49] S. Bahrami, Y. C. Chen, and V. W. S. Wong, "Deep reinforcement learning for demand response in distribution networks," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1496–1506, Mar. 2021.

[50] M. Wen, R. Xie, K. Lu, L. Wang, and K. Zhang, "FedDetect: A novel privacy-preserving federated learning framework for energy theft detection in smart grid," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6069–6080, Apr. 2022.

[51] C. Briggs, Z. Fan, and P. Andras, "Federated learning for short-term residential load forecasting," 2021, *arXiv:2105.13325*.

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

[53] M. M. Badr, M. I. Ibrahem, M. Mahmoud, W. Alasmary, M. M. Fouda, K. H. Almotairi, and Z. M. Fadlullah, "Privacy-preserving federated-learning-based net-energy forecasting," in *Proc. SoutheastCon*, Mar. 2022, pp. 133–139.

[54] J. Zhao, Z. Zhang, H. Yu, H. Ji, P. Li, W. Xi, J. Yan, and C. Wang, "Cloud-edge collaboration-based local voltage control for DGs with privacy preservation," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 98–108, Jan. 2023.

[55] C. Huang, W. Chen, S. Bu, and Y. Zhang, "Deep reinforcement learning-assisted federated learning for robust short-term utility demand forecasting in electricity wholesale markets," 2022, *arXiv:2206.11715*.

[56] H. Wang, C. Si, and J. Zhao, "A federated learning framework for non-intrusive load monitoring," 2021, *arXiv:2104.01618*.

[57] J. Lin, J. Ma, and J. Zhu, "Hierarchical federated learning for power transformer fault diagnosis," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–11, 2022.

[58] R. Schwermer, J. Buchberger, R. Mayer, and H.-A. Jacobsen, "Federated office plug-load identification for building management systems," in *Proc. 13th ACM Int. Conf. Future Energy Syst.*, Jun. 2022, pp. 114–126.

[59] B. Xiao, Q. Xu, C. He, and J. Lin, "Blockchain and federated learning based bidding applications in power markets," *Proc. Comput. Sci.*, vol. 202, pp. 21–26, Jan. 2022.

[60] O. Bouachir, M. Aloqaily, Ö. Özkasap, and F. Ali, "FederatedGrids: Federated learning and blockchain-assisted P2P energy sharing," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 424–436, Mar. 2022.

[61] J.-F. Toubeau, F. Teng, T. Morstyn, L. V. Krannichfeldt, and Y. Wang, "Privacy-preserving probabilistic voltage forecasting in local energy communities," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 798–809, Jan. 2023.

[62] S. Lee and D.-H. Choi, "Federated reinforcement learning for energy management of multiple smart homes with distributed energy resources," *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 488–497, Jan. 2022.

[63] A. Moradzadeh, H. Moayyed, B. Mohammadi-Ivatloo, A. P. Aguiar, and A. Anvari-Moghaddam, "A secure federated deep learning-based approach for heating load demand forecasting in building environment," *IEEE Access*, vol. 10, pp. 5037–5050, 2022.

[64] S. Otoum, I. A. Ridhawi, and H. Mouftah, "A federated learning and blockchain-enabled sustainable energy trade at the edge: A framework for Industry 4.0," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3018–3026, Feb. 2023.

[65] Y. Zhao, W. Xiao, L. Shuai, J. Luo, S. Yao, and M. Zhang, "A differential privacy-enhanced federated learning method for short-term household load forecasting in smart grid," in *Proc. 7th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2021, pp. 1399–1404.

[66] S. V. Dasari, K. Mittal, S. G. V. K. Sasirekha, J. Bapat, and D. Das, "Privacy enhanced energy prediction in smart building using federated learning," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Apr. 2021, pp. 1–6.

[67] Y. He, F. Luo, G. Ranzi, and W. Kong, "Short-term residential load forecasting based on federated learning and load clustering," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2021, pp. 77–82.

[68] V. Venkataramanan, S. Kaza, and A. M. Annaswamy, "DER forecast using privacy-preserving federated learning," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2046–2055, Feb. 2023.

[69] Y. Xu, C. Jiang, Z. Zheng, B. Yang, and N. Zhu, "LSTM short-term residential load forecasting based on federated learning," in *Proc. Int. Conf. Mech., Aerosp. Automot. Eng.*, Dec. 2021, pp. 217–221.

[70] S. Zhang, Z. Xu, J. Wang, J. Chen, and Y. Xia, "Improving the accuracy of load forecasting for campus buildings based on federated learning," in *Proc. IEEE Int. Conf. Netw., Sens. Control (ICNSC)*, vol. 1, Dec. 2021, pp. 1–5.

[71] H. Moayyed, A. Moradzadeh, B. Mohammadi-Ivatloo, A. P. Aguiar, and R. Ghorbani, "A cyber-secure generalized supermodel for wind power forecasting based on deep federated learning and image processing," *Energy Convers. Manag.*, vol. 267, Sep. 2022, Art. no. 115852.

[72] Y. Li, R. Wang, Y. Li, M. Zhang, and C. Long, "Wind power forecasting considering data privacy protection: A federated deep reinforcement learning approach," *Appl. Energy*, vol. 329, Jan. 2023, Art. no. 120291.

[73] J. D. Fernández, S. P. Menci, C. M. Lee, A. Rieger, and G. Fridgen, "Privacy-preserving federated learning for residential short-term load forecasting," *Appl. Energy*, vol. 326, Nov. 2022, Art. no. 119915.

[74] M. Savi and F. Olivadese, "Short-term energy consumption forecasting at the edge: A federated learning approach," *IEEE Access*, vol. 9, pp. 95949–95969, 2021.

[75] X. Chang, W. Li, and A. Y. Zomaya, "Fed-GBM: A cost-effective federated gradient boosting tree for non-intrusive load monitoring," in *Proc. 13th ACM Int. Conf. Future Energy Syst.*, 2022, pp. 63–75.

[76] H. Wang, C. Si, G. Liu, J. Zhao, F. Wen, and Y. Xue, "Fed-NILM: A federated learning-based non-intrusive load monitoring method for privacy-protection," *Energy Convers. Econ.*, vol. 3, no. 2, pp. 51–60, 2022.

[77] Q. Zhai, X. Zhang, and J. Cheng, "Enterprise electricity consumption forecasting method based on federated learning," in *Proc. Int. Conf. Artif. Intell. Secur.* Cham, Switzerland: Springer, 2021, pp. 554–567.

[78] S. R. Pokhrel and M. B. Hossain, "Data privacy of wireless charging vehicle to grid (V2G) networks with federated learning," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 9032–9037, Aug. 2022.

[79] D. Perry, N. Wang, and S.-S. Ho, "Energy demand prediction with optimized clustering-based federated learning," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.

[80] L. Zhao, J. Li, Q. Li, and F. Li, "A federated learning framework for detecting false data injection attacks in solar farms," *IEEE Trans. Power Electron.*, vol. 37, no. 3, pp. 2496–2501, Mar. 2022.

[81] M. Yan, L. Wang, X. Wang, L. Li, L. Xu, and A. Fei, "Matching theory aided federated learning method for load forecasting of virtual power plant," in *Proc. 17th Int. Conf. Mobility, Sens. Netw. (MSN)*, Dec. 2021, pp. 327–333.

[82] Y. Zhang et al., "FedNILM: Applying federated learning to NILM applications at the edge," *IEEE Trans. Green Commun. Netw.*, vol. 7, no. 2, pp. 857–868, Jun. 2023.

[83] M. M. Ashraf, M. Waqas, G. Abbas, T. Baker, Z. H. Abbas, and H. Alasmary, "FedDP: A privacy-protecting theft detection scheme in smart grids using federated learning," *Energies*, vol. 15, no. 17, p. 6241, 2022.

[84] R. Liu and Y. Chen, "Learning task-aware energy disaggregation: A federated approach," 2022, *arXiv:2204.06767*.

[85] S. Dai, F. Meng, Q. Wang, and X. Chen, "DP^2-NILM: A distributed and privacy-preserving framework for non-intrusive load monitoring," 2022, *arXiv:2207.00041*.

[86] S. Dai, F. Meng, Q. Wang, and X. Chen, "FederatedNILM: A distributed and privacy-preserving framework for non-intrusive load monitoring based on federated deep learning," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jun. 2023, pp. 1–8.

[87] X. Wang, Y. Chen, and O. A. Dobre, "Federated learning for anomaly detection: A case of real-world energy storage deployment," in *Proc. IEEE Int. Conf. Commun.*, May 2022, pp. 4312–4317.

[88] W. Zhang, X. Chen, K. He, L. Chen, L. Xu, X. Wang, and S. Yang, "Semi-asynchronous personalized federated learning for short-term photovoltaic power forecasting," *Digit. Commun. Netw.*, vol. 9, no. 5, pp. 1221–1229, Oct. 2023.

[89] S. Lee, L. Xie, and D.-H. Choi, "Privacy-preserving energy management of a shared energy storage system for smart buildings: A federated deep reinforcement learning approach," *Sensors*, vol. 21, no. 14, p. 4898, Jul. 2021.

[90] D. Qin, C. Wang, Q. Wen, W. Chen, L. Sun, and Y. Wang, "Personalized federated DARTS for electricity load forecasting of individual buildings," *IEEE Trans. Smart Grid*, vol. 14, no. 6, pp. 4888–4901, Nov. 2023.

[91] L. Tang, H. Xie, X. Wang, and Z. Bie, "Privacy-preserving knowledge sharing for few-shot building energy prediction: A federated learning approach," *Appl. Energy*, vol. 337, May 2023, Art. no. 120860.

[92] M. A. Husnoo, A. Anwar, N. Hosseinzadeh, S. N. Islam, A. N. Mahmood, and R. Doss, "FedREP: Towards horizontal federated load forecasting for retail energy providers," 2022, *arXiv:2203.00219*.

[93] C. Bishop, *Pattern Recognition and Machine Learning*, vol. 2. Berlin, Germany: Springer, 2006, pp. 35–42.

[94] T. Hastie, R. Tibshirani, J. H. Friedman, and J. H. Friedman, *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*, vol. 2. New York, NY, USA: Springer, 2009, pp. 1–758.

[95] E. F. Morales and J. H. Zaragoza, "An introduction to reinforcement learning," in *Decision Theory Models for Applications in Artificial Intelligence: Concepts and Solutions*. Hershey, PA, USA: IGI Global, 2012, pp. 63–80.

[96] Z. Mao, H. Li, Z. Huang, Y. Tian, P. Zhao, and Y. Li, "Full data-processing power load forecasting based on vertical federated learning," *J. Electr. Comput. Eng.*, vol. 2023, pp. 1–9, Jan. 2023.

[97] J. Wang, B. Wei, J. Zeng, and F. Deng, "Research on load forecasting of novel power system based on efficient federated transfer learning," *Energies*, vol. 16, no. 16, p. 6070, Aug. 2023.

[98] S. Saha and T. Ahmad, "Federated transfer learning: Concept and applications," *Intelligenza Artificiale*, vol. 15, no. 1, pp. 35–44, Jul. 2021.

[99] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele Univ.*, vol. 33, pp. 1–26, Jul. 2004.

[100] G. W. Hart, "Nonintrusive appliance load monitoring," *Proc. IEEE*, vol. 80, no. 12, pp. 1870–1891, Jun. 1992.

[101] M. Y. Arafat, M. J. Hossain, and M. M. Alam, "Machine learning scopes on microgrid predictive maintenance: Potential frameworks, challenges, and prospects," *Renew. Sustain. Energy Rev.*, vol. 190, Feb. 2024, Art. no. 114088.

[102] R. Soni and B. Mehta, "Diagnosis and prognosis of incipient faults and insulation status for asset management of power transformer using fuzzy logic controller & fuzzy clustering means," *Electric Power Syst. Res.*, vol. 220, Jul. 2023, Art. no. 109256.

[103] J. Ahn, Y. Lee, N. Kim, C. Park, and J. Jeong, "Federated learning for predictive maintenance and anomaly detection using time series data distribution shifts in manufacturing processes," *Sensors*, vol. 23, no. 17, p. 7331, 2023.

[104] J. L. Viegas, P. R. Esteves, R. Melício, V. M. F. Mendes, and S. M. Vieira, "Solutions for detection of non-technical losses in the electricity grid: A review," *Renew. Sustain. Energy Rev.*, vol. 80, pp. 1256–1268, Dec. 2017.

[105] M. Ahmed, A. Khan, M. Ahmed, M. Tahir, G. Jeon, G. Fortino, and F. Piccialli, "Energy theft detection in smart grids: Taxonomy, comparative analysis, challenges, and future research directions," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 4, pp. 578–600, Apr. 2022.

[106] (Jul. 2022). *Endesa—Electricity Theft From Cannabis Growing Increases in Spain, Smart Energy International*. [Online]. Available: https://www.smart-energy.com/industry-sectors/energy-grid-management/endesa-electricity-theft-from-cannabis-growing-increases-in-spain/

[107] I. Antonopoulos, V. Robu, B. Couraud, D. Kirli, S. Norbu, A. Kiprakis, D. Flynn, S. Elizondo-Gonzalez, and S. Wattam, "Artificial intelligence and machine learning approaches to energy demand-side response: A systematic review," *Renew. Sustain. Energy Rev.*, vol. 130, Sep. 2020, Art. no. 109899.

[108] L. Wen, K. Zhou, and S. Yang, "Load demand forecasting of residential buildings using a deep learning model," *Electric Power Syst. Res.*, vol. 179, Feb. 2020, Art. no. 106073.

[109] N. Son, S. Yang, and J. Na, "Deep neural network and long short-term memory for electric power load forecasting," *Appl. Sci.*, vol. 10, no. 18, p. 6489, 2020.

[110] S. Bouktif, A. Fiaz, A. Ouni, and M. Serhani, "Optimal deep learning LSTM model for electric load forecasting using feature selection and genetic algorithm: Comparison with machine learning approaches," *Energies*, vol. 11, no. 7, p. 1636, Jun. 2018.

[111] S. Aslam, H. Herodotou, S. M. Mohsin, N. Javaid, N. Ashraf, and S. Aslam, "A survey on deep learning methods for power load and renewable energy forecasting in smart microgrids," *Renew. Sustain. Energy Rev.*, vol. 144, Jul. 2021, Art. no. 110992.

[112] H. Dagdougui, F. Bagheri, H. Le, and L. Dessaint, "Neural network model for short-term and very-short-term load forecasting in district buildings," *Energy Buildings*, vol. 203, Nov. 2019, Art. no. 109408.

[113] P.-H. Kuo and C.-J. Huang, "A high precision artificial neural networks model for short-term energy load forecasting," *Energies*, vol. 11, no. 1, p. 213, Jan. 2018.

[114] K. G. Boroojeni, M. H. Amini, S. Bahrami, S. S. Iyengar, A. I. Sarwat, and O. Karabasoglu, "A novel multi-time-scale modeling for electric power demand forecasting: From short-term to medium-term horizon," *Electric Power Syst. Res.*, vol. 142, pp. 58–73, Jan. 2017.

[115] D. Wu, B. Wang, D. Precup, and B. Boulet, "Multiple kernel learning-based transfer regression for electric load forecasting," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1183–1192, Mar. 2020.

[116] N. Wei, C. Li, X. Peng, F. Zeng, and X. Lu, "Conventional models and artificial intelligence-based models for energy consumption forecasting: A review," *J. Petroleum Sci. Eng.*, vol. 181, Oct. 2019, Art. no. 106187.

[117] L. Zhang, J. Wen, Y. Li, J. Chen, Y. Ye, Y. Fu, and W. Livingood, "A review of machine learning in building load prediction," *Appl. Energy*, vol. 285, Mar. 2021, Art. no. 116452.

[118] A. Bracale, P. Caramia, G. Carpinelli, A. R. Di Fazio, and P. Varilone, "A Bayesian-based approach for a short-term steady-state forecast of a smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 1760–1771, Dec. 2013.

[119] B. P. Hayes and M. Prodanovic, "State forecasting and operational planning for distribution network energy management systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 1002–1011, Mar. 2016.

[120] M. Mokhtar, V. Robu, D. Flynn, C. Higgins, J. Whyte, C. Loughran, and F. Fulton, "Predicting the voltage distribution for low voltage networks using deep learning," in *Proc. IEEE PES Innov. Smart Grid Technol. Eur. (ISGT-Europe)*, Sep. 2019, pp. 1–5.

[121] A. F. Bastos, S. Santoso, V. Krishnan, and Y. Zhang, "Machine learning-based prediction of distribution network voltage and sensor allocation," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2020, pp. 1–5.

[122] D. Cao, W. Hu, J. Zhao, G. Zhang, B. Zhang, Z. Liu, Z. Chen, and F. Blaabjerg, "Reinforcement learning and its applications in modern power and energy systems: A review," *J. Modern Power Syst. Clean Energy*, vol. 8, no. 6, pp. 1029–1042, Nov. 2020.

[123] M. Yousefi, A. Hajizadeh, M. N. Soltani, and B. Hredzak, "Predictive home energy management system with photovoltaic array, heat pump, and plug-in electric vehicle," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 430–440, Jan. 2021.

[124] J. R. Nelson and N. G. Johnson, "Model predictive control of microgrids for real-time ancillary service market participation," *Appl. Energy*, vol. 269, Jul. 2020, Art. no. 114963.

[125] A. Khalatbarisoltani, L. Boulon, and X. Hu, "Integrating model predictive control with federated reinforcement learning for decentralized energy management of fuel cell vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 13639–13653, Dec. 2023.

[126] P. Vongvilasack, S. Premrudeepreechacharn, and K. Ngamsanroaj, "The application of machine learning for the voltage and reactive power control in power distribution network," in *Proc. 19th Int. Conf. Electr. Eng./Electron., Comput., Telecommun. Inf. Technol. (ECTI-CON)*, May 2022, pp. 1–6.

[127] N. Mahmud and A. Zahedi, "Review of control strategies for voltage regulation of the smart distribution network with high penetration of renewable distributed generation," *Renew. Sustain. Energy Rev.*, vol. 64, pp. 582–595, Oct. 2016.

[128] M. Khodayar, G. Liu, J. Wang, and M. E. Khodayar, "Deep learning in power systems research: A review," *CSEE J. Power Energy Syst.*, vol. 7, no. 2, pp. 209–220, Mar. 2021.

[129] M. Braei and S. Wagner, "Anomaly detection in univariate time-series: A survey on the state-of-the-art," 2020, *arXiv:2004.00433*.

[130] M. Alazab, R. M. S. Priya, M. Parimala, P. K. R. Maddikunta, T. R. Gadekallu, and Q.-V. Pham, "Federated learning for cybersecurity: Concepts, challenges, and future directions," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3501–3509, May 2022.

[131] D. Jang, L. Spangher, T. Srivastava, L. Yan, and C. Spanos, "Personalized federated hypernetworks for multi-task reinforcement learning in microgrid energy demand response," in *Proc. 10th ACM Int. Conf. Syst. Energy-Efficient Buildings, Cities, Transp.*, Nov. 2023, pp. 79–88.

[132] A. Balint, H. Raja, J. Driesen, and H. Kazmi, "Using domain-augmented federated learning to model thermostatically controlled loads," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 4116–4124, Sep. 2023.

RAN ZHENG received the M.Sc. degree in electrical engineering from Tampere University, Tampere, Finland, in 2019. He is currently pursuing the Ph.D. degree in electrical engineering with the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain.

From 2020 to 2021, he was a Project Researcher with the University of Vaasa, Vaasa, Finland. He is also with the CITCEA-UPC Research Group. His research interests include AI applications in power systems, active distribution grids, and energy management systems.

ANDREAS SUMPER (Senior Member, IEEE) was born in Villach, Austria. He received the Dipl.-Ing. degree in electrical engineering from Graz University of Technology, Austria, in 2000, and the Ph.D. degree from the Universitat Politècnica de Catalunya, Barcelona, Spain, in 2008.

In 2002, he joined the Center for Technological Innovation in Static Converters and Drives (CITCEA), Universitat Politècnica de Catalunya. Since 2006, he has been teaching with the Department of Electrical Engineering. He is currently a Full Professor with the Escola Superior d'Ingenieria Industrial de Barcelona (ESTEIB), Universitat Politècnica de Catalunya. His research interests include renewable energy, digitalization of the power grids, micro- and smart grids, power system studies, and energy management.

MONICA ARAGÜÉS-PEÑALBA (Member, IEEE) received the M.Sc. degree in industrial engineering and the Ph.D. degree in electrical engineering from the School of Industrial Engineering of Barcelona (ETSEIB), Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 2011 and 2016, respectively.

She is currently an Associate Professor with the Electrical Engineering Department, UPC (a Serra Hunter Fellow). Since 2010, she has been with CITCEA-UPC. Her main research interests include data science applications to power systems, HVDC and HVAC transmission, active distribution grids, microgrids, renewable power generation, and its grid integration.

SAMUEL GALCERAN-ARELLANO (Member, IEEE) was born in Lleida, Spain, in 1971. He received the M.Sc. degree in electrical engineering and the Ph.D. degree from the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 1997 and 2002, respectively.

In 1997, he joined the Department of Electrical Engineering, UPC, as an Assistant Professor. He developed several projects for industry. In 2001, he joined the Center of Technological Innovation in Static Converters and Drives (CITCEA-UPC), UPC, where he belongs to the CITCEA-UPC Directorate Staff. His primary research interests include motor control and converters for power supplies and drives.