Privacy-Preserving Federated Learning for Value-Added Service Model in Advanced Metering Infrastructure

Xiao-Yu Zhang, *Member, IEEE,* José-Rodrigo Córdoba-Pachón, Peiqian Guo, *Member, IEEE,* Chris Watkins, and Stefanie Kuenzel, *Senior Member, IEEE*

***Abstract*—Advanced metering infrastructure (AMI) is the backbone of the next generation smart city and smart grid, it not only provides near real-time two-way communication between the consumers and the energy systems but also enables third parties to provide relevant value-added services to the consumers to improve user satisfaction. However, the existing services are implemented in a centralised manner which has potential and associated security and privacy risks also increased with Internet-of-things (IoT) devices. To better balance the quality of the services and ensure users' privacy, a third-party AMI service model based on differentially private federated learning is proposed in this paper. Instead of sending the private energy data to the cloud server, the proposed service model trains the neural network models locally, and only model parameters are shared with the central server. Moreover, the identity of individuals is eliminated by adding random Gaussian noise during the secure aggregation. Furthermore, an attention-based bidirectional long short-term memory neural network model is adopted to solve the long-range dependency problem of conventional neural networks. In the case study, a residential short-term load forecasting task is implemented to evaluate the performance of the proposed model. Compared with other state-of-the-art energy service models, the proposed one can achieve similar accuracy as the typical centralized model and balances the trade-off between privacy loss and prediction accuracy flexibly.**

***Index Terms*—Advanced metering infrastructure, federated service, energy cyber physical social system, differential privacy, attention-based deep learning.**

Manuscript received 8 April 2022; revised 19 Jul 2022 and 30 July 2022; accepted 30 August 2022. The authors would like to acknowledge the funding by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1.For the purpose of open access, the author(s) has applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising. (*Xiao-Yu Zhang and José-Rodrigo Córdoba-Pachón contributed equally to this work.*) (*Corresponding author: Stefanie Kuenzel and Peiqian Guo*).

The data that support the findings of this study are available from the corresponding authors upon reasonable request.

X. Y. Zhang is with School of Artificial Intelligence, Anhui University, Hefei 230601, Anhui, China (e-mail: zhangxiaoyu@ahu.edu.cn).

J. R. Cordoba-Pachon is with the School of Business and Management, Royal Holloway, University of London, TW20 0EX, U.K. (e-mail: J.R.Cordoba-Pachon@rhul.ac.uk).

P. Q. Guo is with the State Key Laboratory of Power System and Generation Equipment and with the Department of Electrical Engineering, Tsinghua University, Beijing 100083, China (e-mail: guopeiqian@tsinghua.edu.cn).

C. Watkins is with the Department of Computer Science, Royal Holloway, University of London, TW20 0EX, U.K. (C.J.Watkins@rhul.ac.uk).

S. Kuenzel is with the Department of Electronic Engineering, Royal Holloway, University of London, TW20 0EX, U.K. (e-mail: stefanie.kuenzel@rhul.ac.uk).

I. Introduction

With new models to help transition from Cyber-Physical Systems (CPS) to Cyber-Physical-Social Systems (CPSSs), there are challenges related to the active participation of systems users (the social system). In areas like energy, the Advanced Metering Infrastructure (AMI) construction enables the energy consumers to get involved in the demand response programme [1]. As the backbone of the smart grid, AMI is an integrated system which consists of the smart meter and smart sensors (physical), data management system and communication network (cyber). AMI enable two-way communication between the energy consumers and energy control centres to transmit data from smart meters reading electrical consumption and the Time-of-Use (ToU) prices at a high frequency [2]. At the same time, new value-added services introduce new market opportunities and engage the innovation of the electricity market [3], and smart meter crates opportunities to innovate in Business to Consumer (B2C) and Government to Consumer (G2C) projects [4]. Various value-added services are available to consumers, including demand response, Nonintrusive Load Monitoring (NILM), energy awareness and load forecasting. The software companies may also try to link their smart speakers (Echo [5], Google Home [6]) to the consumer's smart meter to help the consumers improve their energy awareness [4]. These value-added services are operated by Third Parties (TPs) representing non-license companies.

Furthermore, advanced data analytics and data mining techniques help the TPs provide consumers with much more innovative or revolutionary services and platforms than originally intended. Such energy services require frequent interaction between end users and the TPs, increasing the risk of security and privacy. Sufficiently robust privacy and data security strategy are required to protect sensitive consumer data. Privacy and security problems related to AMI and value-added services have been overlooked for a long time. This is the case despite proposals for a Consumer-Centred Energy System (CCES) which could help securely connect consumers' social worlds with physical power grids and the cyberworld (computing and communications) [7] and which could be implemented with the help of software

algorithms and schemes like federated learning to protect user's relevant information (i.e., location) and other attributes via differential privacy.

Traditional value-added services are based on a centralised model, subject to severe concerns. Firstly, most value-added services require consumers to send detailed Consumer Energy Usage Data (CEUD) of their house or specific appliances with timestamps. Attacks such as NILM attacks [8], [9] can extract detailed behaviour patterns of consumers by disaggregating power consumption into detailed appliance usages. Secondly, there could be trade-offs to be achieved by allowing more services to be implemented versus protecting the data from these services from unauthorised use. Thirdly, energy harvesting needs not to take up much equipment space whilst allowing for adequate utilisation of renewable energy, enabling other performance indicators and their evaluation to be considered [10].

In this context, users' privacy and security become key issues to address. Energy consumers worry about their electricity data and how it could be inferred by CPSS attackers when they share their smart metre data with energy utility companies. The European Commission's General Data Protection Regulation (GDPR) [11] states that data collected by household smart metres belongs to personal data, and the collection or storage of such information is strictly limited by the data minimization principle and the consent principle [12]. Moreover, the European Commission also suggested that value-added services should have separate communication channels where the type of data to be collected and stored should be specified [13]. However, the conflict between the GDPR and the CEUD required by the service cannot be a trade-off in the existing AMI. In [14], M. Asghar et al. provided several suggestions and outlooks for future privacy-preserving value-added services; these suggestions can be concluded as follows: (1) implement value-added services on customers' private computing platforms (such as mobile phones and personal computers). (2) Develop new privacy-preserving distributed machine learning algorithms to provide better privacy guarantees to consumers.

Therefore, the following knowledge gaps in the existing literature on CPSS need to be addressed: (1) It is expected smart grid network will be "100 or 1,000 times larger than the Internet" [15], and traditional centralized energy services are under great pressure of the communication and computation overhead. (2) The flexibility and scalability of value-added services should be considered for developing the next generation AMI as CPSSs. (3) A dearth of research looks at trade-offs between energy CPSS functionalities and social systems users' privacy. (4) There is a need to develop and evaluate differential privacy deep learning algorithms to process time-series data efficiently and securely in AMI. (5) The existing smart metering system can only share 15-minute interval meter data with TP due to Department for Business, Energy & Industrial Strategy (BEIS), U.K. specifications [16], and only half-hourly data is stored. However, value-added services may require multi-resolution data, which needs data with intervals higher than 15 and 30 minutes. (6) Many value-added energy services need make comparison of the data among different consumers, which is unavailable with the existing localized service model.

To address these gaps discussed above and follow the guideline in [14], this paper develops and evaluates a privacy-preserving AMI value-added service model based on Differential Private Federated Learning (DPFL) model. The model can provide multiple services to consumers without sharing their data (e.g., load demand data) to cloud servers and other parties. The specific contributions are summarized as follows:

1) A decentralized energy value-added service model. In contrast to the traditional centralized cloud-based service model which requires all consumers to upload their personal CEUD, the proposed decentralized topological structure of the proposed method enables edge computing, which reduces the computation and communication capacity of the cloud server.
2) A hybrid DPFL operation scheme with an attention mechanism. The decentralized service model employs a federated learning framework to enable the communication between the smart meters and the central cloud server, the private CEUD is sent to the local model only without sharing with the central cloud server, which reduces the risk of personal information being eavesdropped by the external attackers. Moreover, random Gaussian noise is added during the secure aggregation process to resist the honest-but-curious TP utilizes inference and membership attacks on the shared model parameters.
3) A malicious client detection algorithm to resist low-quality local model update attack. This paper utilizes a K-means clustering detection algorithm to detect malicious clients before the training round start, which protect the global model from collapse.
4) A case study of Short-Term Load Forecasting (STLF) is implemented to assess the model performance. The performance of the proposed model is fully evaluated by comparing the proposed model with centralized/localized service models, whilst the influence of the client number and privacy parameter on the model performance is also investigated.

The remainder of this article is structured as follows. The related work is introduced in Section II, and the preliminaries are covered in Section III. Section IV introduces the proposed decentralized energy value-added service model. The implementation and experiment set-up details are presented in V. The simulation methodology and experiment results analysis are presented in Section Section VI. Finally, Section VII gives the conclusion and shows the limitations of the proposed method.

II. Related Work

A. Energy CPSSs: Privacy-Preserving AMI and Value-added Service

Internet-of-Energy (IoE) combines the concepts of smart grid and Internet-of-Things (IoT), which utilises the flexible and integrated IoT structure to manage physical elements of CPSS such as the smart grid, the smart sensors and meters. The functionality of the electricity network can go beyond providing energy to the consumers and include cyber and social systems elements. The consumers also get involved into the energy system actively by efficiently using their home appliances and IoT devices like smart meters. The assembly of physical, cyber (computing and algorithms) and social elements, connected via IoT networks and devices, can be considered a form of CPSS [1]. This configuration is called the smart metering system or AMI in the energy field.

In this context of AMI, the concept of social energy was first proposed by F.-Y. Wang et al. in 2017 [17], [18], the authors developed social energy as a complex socio-technical system which has intensive interactions between energy components and the social system of users and their IoT devices. Authors in [19] regard energy as one key area for improving CPSS visions. IoT networks can be viewed as an effective medium to complete the interconnection of multiply distributed CPSS. More CPSS cases and evaluations are needed.

To date, however, implementation of existing energy services via AMI follows a top-down hierarchy with centralised authority and decision-making [20], [21], which requires energy consumers to upload their smart meter data to central servers for analysis. Centralized cloud-based value-added service platform is introduced in [20], [22], [23]. M. Tao et al. [20] develop a multi-layer cloud architectural model which enables interaction between service providers and household appliances; the cloud-enabled platform solves the heterogeneity issues by employing the ontology method. Lloret et al. [22] propose an integrated IoT AMI that can be deployed in smart cities. The centralized architecture relies on a cloud server which utilizes big data/machine learning technologies. The developed platform enables multiple Value-added services, including consumption prediction, incident detection, and customer characterization. In [23], A. Meloni and L. Atzori introduce a virtualization middleware to improve the capabilities and opportunities of the cloud-based value-added service platform. However, for a city with a large number of smart meters, the platform would have a high demand for communication bandwidth and cause serve latency which cannot be acceptable for real-time services. Moreover, recent research has indicated that the attackers can reveal personal information by eavesdropping on the communication between the energy consumers and the central server [24].

The localized value-added service model downloads the model to the personal private devices (such as smartphones and personal computers) from the cloud server, and the consumer can send the inquiry to the offline local model. X. Zhang et al. [25] designed a localized demand-side management framework. The consumers will upload their private electricity data to the cloud server while a random Gaussian noise is added to protect the dataset, and then the model trained by the server is sent to IoT devices where the consumers can send a query and obtain feedback. The limitation of the localized service is most value-added services require to compare data from different customers, hence distributed privacy preserving service model would be essential for implementing value-added services.

B. Federated Energy Service

Due to the serious isolated data island problem and the information leakage issue, the traditional centralized cloud server cannot guarantee consumers' privacy. The federate service framework was first introduced by [26] in 2021, aiming to guarantee the consumers' privacy and security while making intelligent management decisions. This framework utilizes federated learning, blockchain, and Distributed Artificial Intelligence (DAI) techniques to enable distributed and edge computing. Federated learning is a decentralized machine learning algorithm that shifts the learning process from the centralized cloud server to decentralized clients [27]. Moreover, federated learning has been employed in various applications such as anomaly detection [28], [29] and social media networks [30]. A FL-based samples exchange mechanism is introduced in [31] to solve the data-hungry issue. More specifically, in the power system and energy area, FL has been applied in power system fields such as solar irradiation forecasting [32], electricity consumer characteristic identification [33], and energy management [34]. However, these applications are limited to the interactions between retailers/Photovoltaic (PV) stations and the server; little work emphasizes customer-level applications. Although a federated learning-based decentralized system provides a privacy guarantee, there are still security issues when the edge devices share the model parameters with the cloud server. Techniques such as differential privacy [30], multi-party protocol [35] are introduced to better defend the personal data from the cyber attackers.

III. The Preliminaries

In this section, preliminaries of the proposed value-added service platform are introduced, which include attention-based bidirectional long short-term memory recurrent neural network, differential privacy, and federated learning.

A. Differential Privacy

Differential privacy is a technology proposed by C. Dwork in 2006 to protect an individual's identification information by adding random noise over the original aggregated data, so that every individual has little effect on the result [36], [37], [38]. In this case, the adversary cannot distinguish the change of the aggregated data with/without one individual

data point. There are several noise addition mechanisms available in the literature [38], including the Laplace, exponential, and Gaussian mechanisms. The privacy level, ε, is guaranteed via the above noise addition mechanism, and the lower ε is, the higher the privacy level that can be achieved.

Definition 1. *$\mathfrak{R}$ is a random function that transforms input β to a random output $\mathfrak{R}(\beta)$.*

Definition 2. *$d(\beta, \hat{\beta}')$ which is the distance between two neighbouring datasets, represents the minimum number of individual samples required to shift dataset β to $\hat{\beta}'$.*

Definition 3 (Global Sensitivity)**.** *For a random function f, the global sensitivity, S_f, is the maximum difference between the outputs of two neighbouring datasets β and $\hat{\beta}'$.S_f also determines the overall noise to be added into the DP mechanism.*

$$\Delta f = \max_{d(\beta,\beta')=1} \|f(\beta) - f(\beta')\| \tag{1}$$

Definition 4. *The Gaussian privacy mechanism denoted $\mathfrak{R}$ is defined as f plus the noise term N.*

$$\mathfrak{R}(\beta) \triangleq f(\beta) + N(0, \Delta f^2 \sigma^2) \tag{2}$$

where N is the Gaussian distribution with mean 0 and standard deviation $\Delta f^2 \sigma^2$. The scale σ is computed as

$$\sigma = \sqrt{2ln((1.25/\delta)}\Delta_2/\varepsilon \tag{3}$$

Definition 5. *A randomized function $\mathfrak{R}$ satisfies (ε, δ) privacy $\mathbb{P}_\mathbb{R}$ for any two neighbouring datasets β and $\hat{\beta}'$:*

$$\mathbb{P}_\mathbb{R}[\mathfrak{R}(\beta) \in \varepsilon] \leq e^{\varepsilon} \mathbb{P}_\mathbb{R}[\mathfrak{R}(\beta') \in \varepsilon] + \delta \tag{4}$$

where ε denotes all possible outcomes in range $\mathfrak{R}$, and δ is the possibility that the differential privacy is broken. In this paper, we select 10^{-5} as δ. The overall privacy cost throughout the learning process is computed by the following composition theorem:

Theorem 1 (Composition Theorem)**.** *If f is $(\varepsilon_1, \delta_1)$-differential privacy and g is $(\varepsilon_2, \delta_2)$-differential privacy, then*

$$f(D), g(D) is (\varepsilon_1 + \varepsilon_2, \delta_1 + \delta_2) - DifferentialPrivacy \tag{5}$$

B. Federated Learning

Federated learning is a decentralized machine learning algorithm that shifts the learning process from the centralized cloud server to decentralized clients [12]. An FL model contains $K \in N^*$ clients indexed by k and one cloud server denoted as S. The target of the FL algorithm is to minimize a local objective function that can be expressed as:

$$\min_{w \in \mathbb{R}^d} \frac{1}{m} \sum_{i=1}^{m} f_i(w) \tag{6}$$

For client $k \in K$, a local model will be trained with their private data on an edge device (such as smartphone or laptop):

$$\forall k, w_{t+1}^k \leftarrow w_t - \eta \nabla \mathcal{L}(w_t) \tag{7}$$

The parameters of the local model w_{t+1}^k for a client are then sent to S, the parameters of all local models are aggregated, and a data-weighted average over all parameters is performed to update the global model w_{t+1}:

$$w_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k \tag{8}$$

where n_k is the number of samples of client k, and n is the number of samples of all clients. Then, the new global model is broadcast to clients, and clients will retrain the local model with their data. The above steps will be repeated until convergence.

C. Attention-Based Bidirectional Long Short-Term Memory Recurrent Neural Network

Attention-Bidirectional Long Short-Term Memory (ATT-BLSTM) architecture improves the traditional LSTM model's accuracy by assigning the probability weights to each previous hidden state to find the most informative for the output at the current time step [39] (Fig. 1). Hence, the utilization of the attention mechanism can improve the output of the BLSTM and better solve the long-term memory problem [39]. ATT-BLSTM model consists of two parts: the conventional BLSTM and an attention layer, see Fig. 1. In a BLSTM structure, given a minibatch input $\boldsymbol{X}_t$, the forward hidden state $\overrightarrow{\boldsymbol{h}_t}$ and backward hidden state $\overleftarrow{\boldsymbol{h}_t}$ at time step t can be expressed as Eqns. (9-10):

$$\vec{h}_t - \phi\left(\boldsymbol{W}_{2h}^f \boldsymbol{X}_t + \boldsymbol{W}_{hht}^f \overrightarrow{\boldsymbol{h}}_{t-1} + b_h^f\right) \tag{9}$$

$$\overleftarrow{h}_t = \phi\left(\boldsymbol{W}_{2h}^b \boldsymbol{X}_t + \boldsymbol{W}_{hht}^b \overleftarrow{h}_{t-1} + b_h^b\right) \tag{10}$$

where $\boldsymbol{W}_{xh}^f, \boldsymbol{W}_{hh}^f, \boldsymbol{W}_{xh}^b, \boldsymbol{W}_{hh}^b$ represent the weights of the model, and $\boldsymbol{b}_h^f, \boldsymbol{b}_h^b$ are the biases of the model. Then, by integrating the forward and backward hidden states, the hidden state is obtained as $\boldsymbol{h}_t$. Finally, $\boldsymbol{h}_t$ is fed to the output layer to compute the output $\boldsymbol{o}_t$:

$$\boldsymbol{h}_\mathrm{t} = \left[\overrightarrow{\boldsymbol{h}_t}^T; \overleftarrow{\boldsymbol{h}_t}^T\right]^T \tag{11}$$

$$\boldsymbol{o}_\mathrm{t} = \boldsymbol{h}_t \boldsymbol{W}_{hq} + \boldsymbol{b}_q \tag{12}$$

where $\boldsymbol{W}_{hq}$ is the weight and $\boldsymbol{b}_q$ is the bias of the output layer. As for the attention layer, denoting the current hidden state as h_t and the previous hidden state as $\boldsymbol{h}_i (1 \leq i < t)$. Referring to the definition in [40], a context vector $\boldsymbol{c_t}$ is computed, which is the weighted sum of all hidden states:

$$\boldsymbol{c_t} = \sum_{i=1}^{t-1} \alpha_{t,i} \boldsymbol{h}_i \tag{13}$$

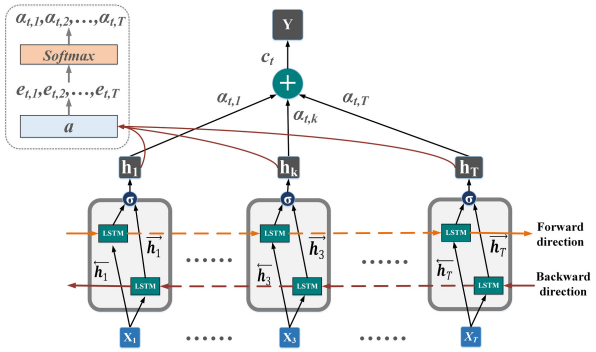

Fig. 1. Structure of attention based bidirectional LSTM.

where $\alpha_{t,i}$ is the weight for the hidden state $\boldsymbol{h}_i$ at timestep t. An attention matrix $\alpha_{t,i}$ is obtained by adopting the softmax function, as shown in Eqns. (14) and (15):

$$\boldsymbol{\alpha}_{\mathrm{t}} = [\alpha_{t,1}, \alpha_{t,2}, ..., \alpha_{t,t-1}] \tag{14}$$

$$\alpha_{t,i} = \frac{\exp\left(e_{t,i}\right)}{\sum_{k=1}^{T} \exp\left(e_{t,k}\right)} \tag{15}$$

In the above equations, $e_{t,i}$ represents the score (or energy) of a feed-forward neural network (denoted as function a), and the purpose of $e_{t,i}$ is to capture the influence of the previous hidden state $\boldsymbol{h}_i$ on the current hidden state $\boldsymbol{h}_t$. Three a functions are introduced in [41]: location-based attention function (location), general attention function (general), and concatenation-based attention function (concat) [40]. Detailed functions are illustrated below:

$$e_{t,i} = a\left(e_{t,k}\right) = \begin{cases} \boldsymbol{W}_e^{\top} \boldsymbol{h}_i + b_e & \text{Location} \\ \boldsymbol{h}_t^{\top} \boldsymbol{W}_e \boldsymbol{h}_i & \text{General} \\ \boldsymbol{v}_e^{\top} \tanh\left(\boldsymbol{W}_e\left[\boldsymbol{h}_t; \boldsymbol{h}_i\right]\right) & \text{Concat} \end{cases} \tag{16}$$

where $\boldsymbol{v}_e$ is the parameter to be learned by the neural network. Referring to the experiment implemented by [42], attention-based BLSTM achieves excellent performance in processing power consumption data as its characteristic in allocating the importance to the overall power consumption data points that correspond to the state changes of appliances. As a result, the model can better extract relevant features from the collected data.

IV. Proposed Value-Added Service Model

In this section, the proposed AMI value-added service model is introduced. Detailed services and functionalities, the adversary model, service model components, and the service process are covered in this section.

A. Enabled Service and Functionality

Comparing to the basic functionalities such as billing and grid operations, privacy-preserving value-added services have received much less attention at current stage. The value-added services enabled by the proposed service model are data analytic and management services based on CEUD measured by the smart meter. These services include STLF, renewable energy forecasting (REF), NILM, energy management, etc. An introduction of the representative services is shown below.

1) STLF: STLF service aims to predict future household power consumption from a few minutes to 24 hours [43]. STLF is a vital service for consumer to improve their energy awareness and help them better manage their electricity usage. Moreover, an accurate STLF result also provides preknowledge to implement various demand response plans.

2) REF: In many countries, especially Europe countries such as the U.K., many houses install rooftop solar panels and energy storage systems. Such grid-connect generation will not only supply the energy to the consumer's house, but the consumer will also sell the extra energy to the energy market [44]. However, renewable energy generation is heavily influenced by weather factors, and the high penetration of such renewable energy introduces problems such as voltage fluctuation, frequency deviation, etc. Hence, a precise REF helps the consumer better schedule and manage the energy.

3) NILM: NILM service improves the consumer's energy awareness by extracting the power consumption of single appliances out of aggregated power data. Especially, precise estimation of the composition of Thermostatically Controlled Loads (TCLs), including Heating, Ventilation and Air Conditioning (HVAC), Air Conditioner (AC), heat pumps, and furnaces, can optimize capacity bids into ancillary services markets [45].

4) Energy Management: In a smart home, the smart meter plays the role of an energy hub and connects with smart appliances such as AC, washing machine, and refrigerator. With such a large volume of CEUD generated, the smart meter needs to optimize the energy consumption in collaboration with other smart homes.

B. Adversary Model

Privacy and security are the emerging issues of the AMI, especially the value-added services. In this paper, both the internal and external adversaries are considered, as shown in Fig. 2. Internal adversaries indicate the threat/adversary inside AMI. Whilst Third Parties (TPs), which reparents non-licence third-party service providers/commercial companies, are considered the Honest-but-Curious (HBC) adversaries, which are widely used in smart grid/ smart meter privacy problems in the literature [46]. The definition of honest-but-curious/semi-honest adversary is shown below:

Theorem 2 (Honest-But-Curious Adversary)**.** *The honest-but-curious adversary represents a legitimate member of a protocol who will not deviate from the defined protocol but will attempt to study as much information as possible from received messages.*

The honest-but-curious TPs will follow the communication protocol honestly without malicious actions, and they cannot obtain more information than they receive (honest),

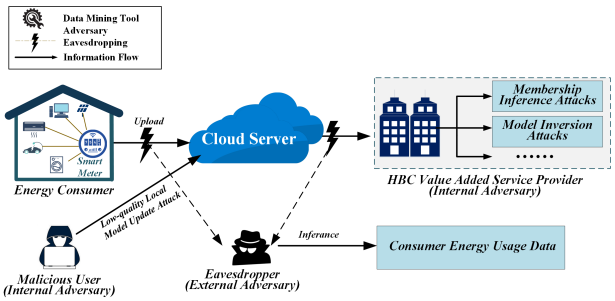

Fig. 2. Adversary model in AMI value added service channel.

but they would keep all information received from other parties and try to infer individual measurements (curious). In other words, all parties work properly to maintain the system's operation while they try to maximize the chance of acquiring individual' privacy. TPs can use membership inference attacks [47] and model inversion attacks [48] to infer private data from the system . Another internal adversary is the malicious client. The malicious client may send bad and low-quality updated parameters to the global model (Low-quality local model update attack [49]). As a result, the global model's accuracy is influenced, and even worse, the overall system may collapse. In the proposed system, the system should defend against attacks from malicious servers and clients.

AMI highly rely on the wireless communication network, while the wireless communication channel is vulnerable to cyber-attacks from the external adversary as the channel is naturally a broadcast transmission medium [50]. The external adversary in this paper is the eavesdropper who can eavesdrop on the communication between the cloud server and the consumer/TPs. The purpose of the external adversary is to obtain the personal smart meter data from the communication channel.

C. Model Components

As shown in Fig.3, the proposed service model contains components: smart meters, the cloud server, an aggregator, and the TP service provider.

1) Smart Meter: the smart meter is the fundamental sensor/device in AMI which generates the CEUD of the house. The smart meter in this paper also works as an edge device and the gateway of the smart home [51]. The smart meter can either communicate with the cloud server bidirectionally via the Wide Area Network (WAN) or communicate with the smart appliances and renewable generation (such as PV panels, and and household energy storage systems) via Home Area Network (HAN). The smart meter enables data analytics, prediction, and energy management locally with a computation and storage capacity. Denote the smart meters set under the cloud server as $\mathcal{H} = \{1, \ldots, k, \ldots, K\}$. For each smart meter $k \in K$, it collects and owns a private electricity consumption dataset $\mathbb{R}_k$, which is employed to train the local model.

2) Aggregator: aggregator, which locates in the cloud server, is employed to receive the updated model parameters and aggregate those parameters by implementing a weighted averaging algorithm such as Federated Averaging (FedAvg). Then the aggregated model parameters are sent from the aggregator to the centralized server to update the global model.

3) Cloud Server: cloud server is the central server which is responsible for training the global model G. Compared with the smart meter, the cloud server has much more powerful computation and storage capacity.

4) TP Service Provider: TP service provider is a non-licensed company, responsible for providing the energy service of K energy consumers. TP service provider sends the service tasks to the cloud server and receives the trained global model provided by the cloud server.

D. Overview of the Service Model

The overall system is demonstrated in the block-diagram shown in Fig. 3. The clients in this framework are the consumers who install smart meters at home; they use IoT devices such as smartphones and personal computers to train local models and communicate with the cloud server. The proposed framework contains six procedures that can be concluded as follows:

- ***Procedure 1.*** Service Task Assignment. In the beginning, the TP will determine the specific value-added service and assign the task to the cloud server.
- ***Procedure 2***. Global model initialization. Initially, the global model at the TP cloud server is initialized by allocating random values to its parameters. Then, the model parameters are downloaded by clients and broadcast to local models.
- ***Procedure 3.*** Local model training. After receiving the parameters from the cloud server, the local model is updated in the IoT device; then, the IoT device will train the new model with private data locally.
- ***Procedure 4.*** Local model parameters upload. After the training process, the parameters of all local models are uploaded to the cloud server.
- ***Procedure 5.*** Secure aggregation with differential privacy. An aggregator is responsible for secure aggregation once it receives a response from the required number of clients. It aggregates the data with a random mechanism to maintain client-level differential privacy. After the aggregation of each round, the collected local model parameters are discarded.
- ***Procedure 6.*** Global model update. The global model is updated with the output of the aggregator.
- ***Procedure 7.*** Model broadcast. Parameters of the new global model are broadcast to all local models that run on IoT devices.
- ***Procedure 8.*** Report to TP. After the global model is trained well and capable of making a precise prediction, the global model is sent back to TP.

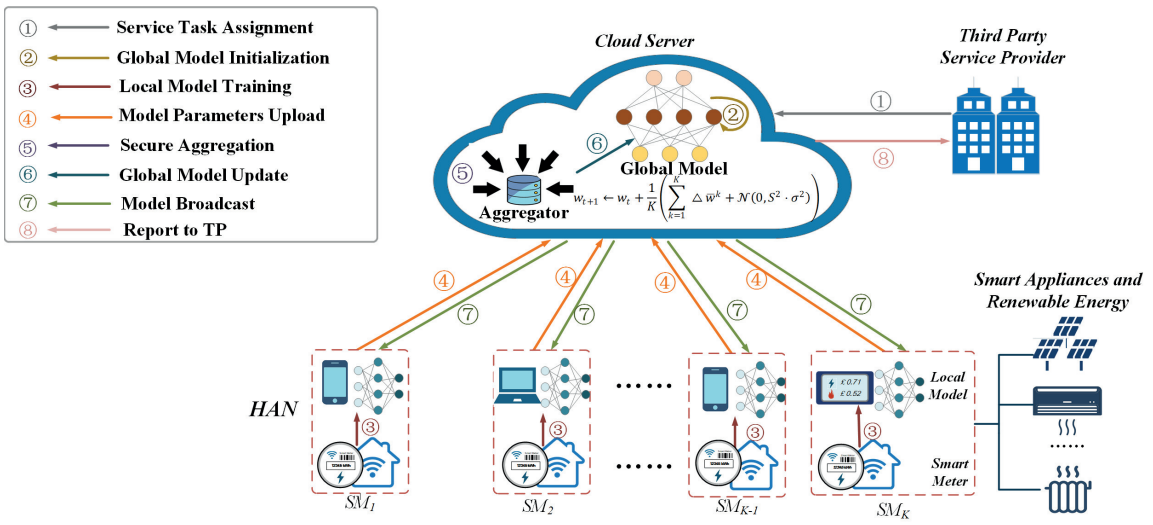

Fig. 3. Overall differential private federated third-party service model.

E. Local Deep Neural Network Model

The local and global models employ the deep neural network model, and the models have the same architecture. As shown in Fig. 4, the structure of the local neural network consists of seven layers:

- The input layer: The power consumption data collected by the smart meter are fed into the model.
- Two BLSTM layers: BLSTM is adopted to extract high-level representation from the input data. Although more BLSTM layers enable the model to better extract nonlinear features from the input sequences, too many BLSTM layers will cause overfitting problems, and the training time is also highly extended. Considering the above issues, two BLSTM layers are easier to implement with high efficiency.
- An attention layer: As introduced in Section III, the attention layer utilizes the attention mechanism to rank the importance of the previous hidden states and selects the most informative hidden state to predict the output values.
- A concatenated layer: As the optional layer, the function of the concatenated layer is to load data from external databases that are related to the evaluation of the desired value-added service. External databases include meteorological, calendar, and electricity market databases.
- A fully connected layer: The fully connected layer links the recurrent layers with the output layer. The purpose of the layer is to fully extract the nonlinear correlation between all input variables and outputs.
- The output layer: For classification tasks, the probability of each category is generated as the output; for regression tasks (such as load forecasting or NILM), the prediction value at the current timestep is generated by the output layer.

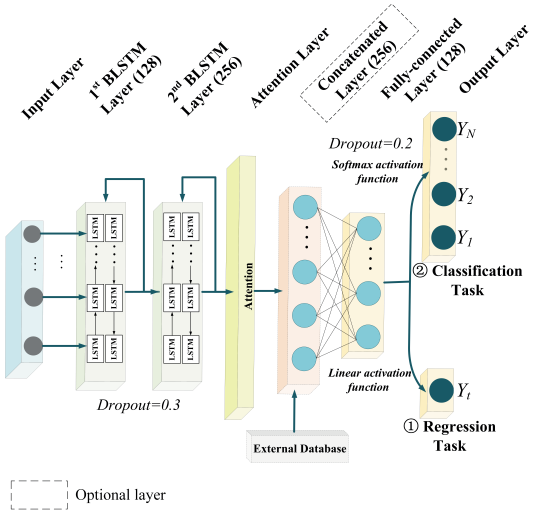

Fig. 4. Structure of local neural network model.

F. Cloud Server

The central cloud server is responsible for secure aggregation, and global model update. Although federated learning models avoid sharing private data with a cloud server or third parties, privacy is still a significant concern. By continuously sharing the parameters of local models, the adversary can still infer some sensitive information from the parameters [52]. DPFL provides a strong privacy guarantee and simultaneously reduces communication costs [53]. Hence, a DPFL algorithm is adopted in this work to provide a stronger privacy guarantee to the system. The DPFL adopted in this paper is based on the randomized Gaussian mechanism introduced in [54], detailed processes are shown in Algorithm 1. Denoting the global model at timestep t as w_t; the model is optimized by the local model of client k, and we denote the optimized model as w^k. The

mismatch between w_t and w^k is client k's update and can be expressed as:

$$\Delta w^k = w^k - w_t \tag{17}$$

To reduce the sensitivity of Δw^k with a considerable value, a scaling function is applied to Δw^k to ensure that the second norm $\left\|\Delta w^k\right\|_2$ is limited by sensitivity $\mathcal{S}$. Hence, the scaled version of the updates is obtained as:

$$\Delta \bar{w}^k = \Delta w^k / max(1, \frac{\zeta^k}{\mathcal{S}}) \tag{18}$$

where $\zeta^k = \left\|\Delta w^k\right\|_2$ and $\mathcal{S}$ is the median of norms of clients' update and can be expressed as:

$$\mathcal{S} = median(\zeta^k) \tag{19}$$

By adding random Gaussian noise scaled to $\mathcal{S}$, $N(0, S^2 \cdot \sigma^2)$ into the sum of all scaled updates from K clients $\sum_{k=1}^{K} \Delta \bar{w}^k$, the Gaussian mechanism approximating the sum of updates is obtained. The new global model w_{t+1} is computed by adding the original global model with averaged approximation:

$$w_{t+1} \leftarrow w_t + \frac{1}{K}\left(\sum_{k=1}^{K} \Delta \bar{w}^k + \mathcal{N}\left(0, S^2 \cdot \sigma^2\right)\right) \tag{20}$$

V. Implementation

This section presents the implementation details, including data preparation, simulation setup, evaluation metrics, and benchmark models.

A. Data Description

This paper used a real-world dataset from Pecan Street Dataport (Dataport) [55] to evaluate the forecasting performance. Dataport is a commercial electricity dataset, while a part of the data is free to access for academic research. The dataset contained over 1200 houses and was collected in Austin, Texas, the United States (N 30° 15', W 97° 43') between January 1st and December 31st, 2018. Both household and appliance power consumption in each house was recorded with sampling frequencies of 1 min and 15 min, respectively.

Moreover, the corresponding weather and temporal information at the same location are obtained from the National Solar Radiation Database (NSRDB) [56]. Weather parameters include Dew point (°C), Temperature (°C), Pressure (Pa), and Relative Humidity (%RH). As for temporal information, four variables are introduced which are: Holiday (1 for holiday days and 0 for non-holiday days), Hour of the Day (HOD) (index range from 0 to 23), Day of the Week (DOW) (index range from 0 to 6), and Month of the Year (MOY) (index ranges from 1 to 12). As categorical variables, DOY, HOD, DOW, and MOY should be pre-processed by one-hot encoding.

Algorithm 1: Differential Private Federated Learning-based Third-Party Service.

Input: Clients number $\tilde{K}$ indexed by k; communication round t; the maximum communication round T; the maximum pre-train communication round T_p; B is the mini-batch size; q is the fraction of clients; ε is the target differential privacy; σ is the Gaussian Mechanism parameter; δ represents the probability that $\varepsilon - DP$ is broken, and Q is the threshold for δ.
Output: Local model paramters w

Function `Pretraining(`$\tilde{K}, w_t$`)`**:**
  if $k \leq \tilde{K}$ **then**
    $w^k \leftarrow Local(k)$ `// Pretraining the local models to obtain the weights`
  $C \leftarrow K - MeansClustering(2, \Delta w)$ `// Cluster clients into normal/abnormal clusters.`
  return $C_1, C_2, K, \hat{K}$ `// return the normal clients cluster and client number` C_1 `and` K`, and abnormal clients cluster and client number` C_2 `and` $\hat{K}$`.`

Function `DPFL(`K, w_t`)`**:**
  initialize the global model w_0
  initialize Accountant (ε, K)
  while $r < R$ **do**
    $\delta \leftarrow Accountant(\varepsilon, q)$ `// accumulate the privacy loss.`
    if $\delta > Q$ **then**
      return w_t `// return the model when the privacy threshold reached.`
    for *client* k *in* qK **do**
      $\Delta w_{t+1}^k, \zeta^k \leftarrow ClientUpdate(k, w_t)$ `// the client k's update and norm update on local model.`
    $S = median\zeta^k$ `// compute the median of norms of clients' update as sensitivity.`
    $w_{t+1} \leftarrow w_t + \frac{1}{K}\left(\sum_{k=1}^{K} \Delta \bar{w}^k + \mathcal{N}\left(0, S^2 \cdot \sigma^2\right)\right)$ `// update the global model by adding averaged approximation.`
  return w_{t+1}

Function `ClientUpdate(`k, w_t`)`**:**
  $w \leftarrow w_t$
  while $r < r_{max}$ **do**
    for $b \in B$ **do**
      $w \leftarrow w - \eta \nabla \mathcal{L}(w_t)$ `// mini-batch gradient descent.`
    $\Delta w_{t+1} = w^k - w_t$ `// client k's local model update.`
    $\zeta^k = \|\Delta w_{t+1}\|_2$ `// second norm update.`
  return $\Delta w_{t+1}, \zeta^k$

Function `Clustering(`X, Δw`)`**:**
  random place centroids C_1, C_2 across Δw
  repeat
    for $i \in K$ **do**
      $\gamma_{ij} = \begin{cases} 1 \text{ if } j = \text{argmin}_j \|\Delta w_i - C_j\|^2 \\ 0 \text{ otherwise} \end{cases}$ `// find the nearest cluster` j `for model` i`.`
    for $j \in 2$ **do**
      $n_j = \sum_{i=1}^{K} \gamma_{i,j}$ `// assign the data points to clusters.`
      $C_j = \frac{1}{n_j} \sum_{i=1}^{K} \gamma_{i,j} \Delta w_i$
  until *Convergence* `// assign the average of points to cluster` j`.`
  return C_1, C_2 `// assign the regular clients to` C_1 `and the malicious clients to` C_2`.`

B. Simulation Environment

In this paper, the case study is implemented in a virtual environment. A workstation with a Core i7-7700HQ CPU, NVIDIA GTX 1060 GPU (8 cores), and 8 GB RAM is utilized for the simulation. The DPFL ATT-BLSTM is operated on Python 3.6 with PyTorch [57], and the privacy loss is computed via the TensorFlow-Privacy library [58].

To simulate the proposed DPFL service model, a subset of K houses from the Dataport dataset is selected as the data for simulation. Moreover, all houses are the same type (single-family homes) and located in the same location (Austin, Texas, U.S.). For each smart meter $k \in K$, a household dataset from the subset is assigned. The data is pre-processed (data cleaning, encoding, and feature scaling) before feeding into the local model. Then the household training data were split into 36-week data, and one-week data (672 samples) were adopted for each communication round. When the communication round reaches 36, it will start dragging data from the first week again at the next communication round until it reaches the threshold of δ.

C. Evaluation Metrics

The performance of the scheme is evaluated with the normalized mean absolute error (nMAE), mean absolute percentage error (MAPE), and root mean square error (RMSE). The smaller the values of MAE, MAPE and RMSE are, the better the model's performance.

$$nMAE = \frac{\sum_{i=1}^{N} |y_i - \hat{y}_i|}{NP_{max}} \tag{21}$$

$$MAPE = \frac{\sum_{i=1}^{N} |(y_i - \hat{y}_i)/y_i}{N} \times 100\% \tag{22}$$

$$nRMSE = \sqrt{\frac{\sum_{i=1}^{N} |y_i - \hat{y}_i|^2}{N}} \tag{23}$$

D. Benchmark model

Several benchmark models are designed better to demonstrate the accuracy and robustness of the proposed method. First, the proposed model is compared with three different service frameworks, such as the centralized framework, localized framework, and FL framework, without adding noise during the aggregation process:

1) Conventional centralized ATT-BLSTM model (denoted as a centralized model): Centralised service model is developed in [20]. As the basic and conventional method, this method is especially suitable when the smart meters and private devices have limited computation capacity and cannot operate the local model alone. In this model, the cloud server collects information from all smart meters, and then the collected data is used to train and update a global model to make the prediction, and then the results are sent back to the consumers.

2) Localized ATT-BLSTM model (denoted as Localized model). A localized model is proposed in [25]. Rather than sending personal data to the cloud server, the personal energy data will be sent to the local model to make the prediction. Firstly, the training data is loaded from the public electricity database. Then the global model is trained with the training data and broadcasted the trained model parameters to the smart meters via Wide Area Network (WAN). The consumer can send a query, and once the smart meter receives the query, it will evaluate the local model with private electricity data to compute the outputs of the query. Then a detailed report is sent to the consumer via In-Home Display (IHD). To simulate the Localized model in the virtual environment, K smart meters are developed in Python, and all personal datasets remain confidential and cannot be seen by other smart meters and the cloud server under this model and the training process of each smart meter is independent. Hence, this model results in personalized deep learning models tailored to each consumer. However, the local model cannot learn the knowledge from other local models.

3) FL ATT-BLSTM model without DP (denote as FL model). Similar to the proposed DPFL service model introduced above, the FL service model is based on a federated structure, and the FL service model's hyperparameters are exactly the same as the DPFL model. The only difference between these two models is that no noise is added during the data aggregation process.

Then, three benchmark models under the DPFL framework utilizing different DNN algorithms (MLP, LSTM, BLSTM) are selected. By comparing the proposed model with the models listed below, the efficiency of ATT-BLSTM can be validated.

4) The DPFL model utilizes LSTM as a training algorithm (denoted as the DPFL-LSTM model). The DPFL-LSTM model contains four hidden layers (two LSTM layers with 128 and 256 cells and two fully connected layers with 1024 cells).

5) The DPFL model utilizes BLSTM as a training algorithm (denoted as the DPFL-BLSTM model). The DPFL-BLSTM model contains four hidden layers (two LSTM layers with 128 and 256 cells and two fully connected layers with 1024 cells).

6) The DPFL model utilizes MLP as a training algorithm (denoted as the DPFL-MLP model). The DPFL-MLP model contains four layers (two LSTM layers with 128 and 256 cells and two fully connected layers with 1024 cells).

E. Hyperparameters Configuration

The hyperparameters of the pretraining model and the proposed DPFL ATT-BLSTM value-added service platform are summarized in Table I. The pretraining model is a shallow MLP with only one dense layer. The number of layers contains 16 cells, and the activation function of the dense layer is the Rectified Linear Unit (ReLU), which enables the model to learn nonlinear correlations better. The optimizer is SGD with the learning rate 1×10^{-3}.

As shown in Fig. 4 and Table I, the ATT-BLSTM network contains two BLSTM layers, with 128 and 256 cells, respectively. This was followed by an attention layer with size 28

and one dense layer with 128 cells. The activation function of hidden layers is ReLU, and the optimizer is Adam with the learning rate 1×10^{-4}. As the STLF task is a regression task, the size of the output layer is one. Moreover, dropout and L2 regularization are used to avoid overfitting problems. 0.3 and 0.2 are selected as the dropout rates of the BLSTM layer and the dense layer, respectively. In addition, 1×10^{-3} is selected as the weight decay value.

F. Computation Cost

Computation complexity is evaluated in terms of the overall runtime of the service. To quantify the computation complexity, we define the following variables:

Phase I: Pre-train the model with a traditional DPFL learning method.

Phase II: Cluster clients into several groups and implement the proposed clustered DPFL model.

Phase III: Respond to the clients' query with the updated local model.

T_{pre} : Time for pre-training the clients to filter out malicious clients.

$T_{local}(t)$: Time for clients to train local model at communication round t.

$T_{agg}(t)$: Time for the central server to aggregate the local model parameters with differential privacy at communication round t.

$T_{upload}(t)$: Time for the clients to upload the local models to the cloud server at communication round t.

$T_{broadcast}(t)$: Time for the central server to broadcast the global model to the clients at communication round t.

$T_{global}(t)$: Time for the central server to update the global model at communication round t.

T_{qurey}: Time for the local server responses to the consumer's query.

In Phase II, also known as clustered federated learning period, we assume all cluster servers operate in parallel, so the runtime of the proposed model with client k in a communication round t can be estimated by the following equation:

$$\begin{aligned} T_{\text{phaseII}}(t) =& T_{\text{local}}(t) + T_{\text{upload}}(t) + T_{\text{aag}}(t) + \\ & T_{\text{broadcast}}(t) + T_{\text{alobal}}(t) \end{aligned} \tag{24}$$

Then the total time cost during Phase II is calculated as:

$$T_{\text{phaseII , total}} = \sum_{t=1}^{T} T_{\text{phaseII}}(t) \tag{25}$$

Finally, the overall computation complexity of the proposed model is evaluated by

$$\begin{aligned} T_{\text{total}} &= T_{\text{phaseI, ,total}} + T_{\text{phaseII , total}} + T_{\text{phaseIII , total}} \\ &= T_{\text{pre}} + \sum_{t=1}^{T} T_{\text{phaseII}}(t) + T_{\text{qurey}} \end{aligned} \tag{26}$$

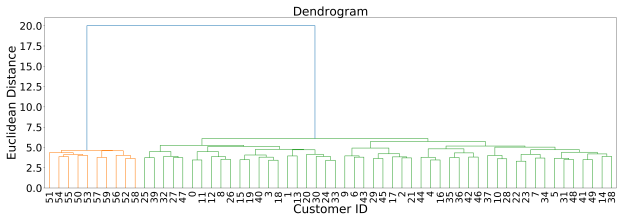

Fig. 5. Clustering results with K-means clustering algorithm.

VI. Case Study

In this section, the accuracy and efficiency of the proposed DPFL attention-BLSTM value-added service framework are validated using the scheme for a typical value-added service residential STLF task. Both the proposed scheme and traditional centralized framework are tested with real-world datasets. Moreover, the impacts of exogenous meteorological and calendar features are also investigated. Finally, the privacy performance, as well as the communication cost, is studied.

A. Malicious Clients Detection

Malicious clients present the internal attackers who would utilize low-quality local model update attack that the cloud failed the FL model, and the distributions of the parameters from these malicious models were distinctive from the data of regular clients. The cloud server should detect these malicious clients efficiently to prevent the system from collapsing. The clustering mechanism outputs two clusters: the normal and the malicious client groups. A K-means clustering malicious clients detection algorithm is proposed to filter out the malicious clients based on the similarity of the weights. This case study includes 50 regular consumers (ID number between 0 and 49) and 10 abnormal consumers (ID number from 50 to 59). The malicious clients will upload fake weights to the central server; the generated fake weights follow the Gaussian Distribution.

As shown in Fig. 5, the central server applies the K-means clustering algorithm to the collected weights, and the algorithm detects all the malicious clients and classifies these models into the same group (the clients labelled with light orange). Meanwhile, the rest of the clients are clustered into another group (the clients labelled with light green). The Euclidean Distance of the regular consumers is below seven, which is considerably small compared to the distance between malicious clients and normal clients.

B. Comparison of the Proposed Model with Centralized and Localized Models

In this case study, to evaluate the accuracy and effectiveness of the proposed DPFL service model, benchmark models including centralized , localized and naive FL service models are employed to compare with the proposed model. All models utilize ATT-BLSTM as the algorithm of the local/global models. The forecasting results are presented in

TABLE I
HYPERPARAMETER CONFIGURATION OF DIFFERENTIALLY PRIVATE FEDERATED LEARNING MODEL

Hyperparameter	Value/range
Lookback	4
Optimizer	Adam
Loss	MSE
Activation function	ReLU
Layers	2 BLSTM layers with 128 and 256 cells, respectively; 2 fully connected layers with 1024 cells.
Epochs for each client in every communication round	5
Privacy budget	1, 2, 4, 6, 8, 10, 12 1e-1, 1e-2, 1e-3, 1e-4, 1e-5, 1e-6, 1e-7, 1e-8
The GM parameter σ	1.12
Number of batches per client B	128
Dropout rate	0.5
Weight decay	1e-3
Attention size	28
Learning rate	1e-4
Total clients	5-100
Percentage of clients selected each round	30%

Table II. In Fig. 6, the prediction results in three houses of the proposed service model as well as the benchmark models are plotted. From this figure, solid blue line indicates the ground truth load curve, and the red solid curve represents DPFL model.

The conventional centralized model can access all individuals' CEUD without any constraint and limitation, and the model can better learn the characteristics of the loads among all houses. Hence, in Fig. 6, the centralized model achieves the highest prediction accuracy among all models.

The localized model can only train the local model with an individual household dataset without the ability to obtain knowledge from other household datasets and local models. With such limited samples to train the service model, the localized model has the worst prediction performances among all models. Although the localized model has the strongest privacy guarantee and does not need to communicate with other sectors, this model cannot provide a high quality service to the consumers.

There are few limitations for the naive FL model: 1) the cloud server cannot access the individual's CEUD directly. 2) the global model can only be trained with the updated local model parameters. With such strict constraints, the naive FL model still achieves an nRMSE of 6.67% when $K = 50$, which is very close to the performance of the centralized model. Based on this result, it is concluded that the proposed decentralized service model achieves a trade-off between functionality (prediction accuracy) and privacy (prevent personal CEUD from being eavesdropped.

In the turn of the DPFL service model, the prediction accuracy is limitted by the privacy constraints set by DP. The privacy level of the DPFL model can be adjusted flexibly by setting the two DP parameters, the privacy budget ε and the probability of information being leaked δ. Typically, a smaller ε means a smaller distance between the two neighbouring databases when sending a query. Hence, the adversary has difficulty distinguishing these two databases by observing the query output. Hence, a smaller ε provides better privacy but less accuracy. From the results shown in

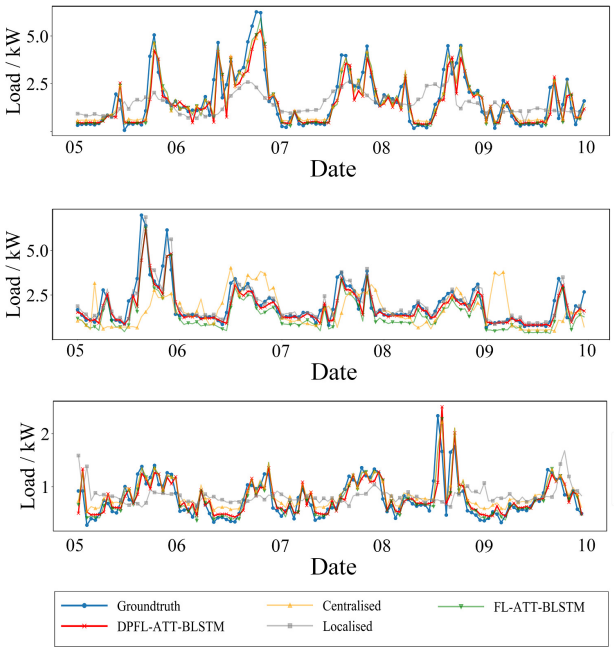

Fig. 6. Short-term load forecasting results of three houses predicted by the proposed differential private federated learning scheme and three conventional schemes ($\varepsilon = 8, \delta = 10^{-5}$).

Table II, when $\varepsilon = 8$ and $\delta = 10^{-5}$, the DPFL scheme's performance is 3.75% and 12.31% worse than that of the FL scheme from the perspective of nRMSE and MAPE. Although the accuracy of the DPFL scheme stays below non-differentially private schemes, it is significantly better than the Localized model, which only trains the model with its data.

C. Comparison of the Proposed Model with Other Algorithms

In the first case study, the proposed DPFL ATT-BLSTM model is compared with DPFL models that utilize different DNN algorithms (benchmark Models (4)-(5)). The forecasting results of all models are shown in Table II. nMAE,

nRMSE and MAPE were used to measure the accuracy of the prediction results, and the communication and computational costs were recorded. The privacy budget ε ranged from 1 to 8, and the client number K ranged from 5 to 50. To visualize the performance of the proposed scheme and benchmark models, 30-minute forecasting results of three random houses are presented in Fig. 7 (under the condition $\varepsilon = 8$ and $\delta = 10^{-5}$). In each communication round, only 30% of clients (e.g., 15 clients when $K = 50$) were selected to participate in the training process. Unlike feeder-level load forecasting, which has a regular peak load every day, household-level load forecasting is more challenging, as the load profile on different days varies greatly. As shown in Fig. 7, the proposed DPFL-ATT-BLSTM model (solid red curve) predicts with the highest accuracy among all four algorithms. Moreover, the DPFL-ATT-BLSTM model tracks the ground truth load curve (solid blue curve) almost all the time: For both peak load period (between 7 am – 13 pm, and 19 pm – 23 pm) when the load fluctuates significantly and off-peak load (between 23 pm – 7 am) when load curve is flat, the proposed model can track the ground truth load curve precisely. The average nRMSE during the peak load period is 8.37% and the average nRMSE during the off-peak load period is 4.21%. Considering the evaluation metrics, the proposed model had the lowest MAPE, nRMSE, and nMAE values in the same comparison group. Referring to the results shown in Table II, when $\varepsilon = 8$ and $\delta = 10^{-5}$, the nRMSE and nMAE values of the proposed model were reduced by 31.95% and 11.22%, respectively, compared to DPFL-BLSTM.

DPFL-MLP (light green solid curve) had the worst performance in most cases. It had very limited predictability in forecasting time-series data without the memory cell. From Fig. 6, DPFL-MLP tracked neither the peak nor off-peak loads. However, this method also has an advantage: the computational cost was the lowest among all algorithms. In the situation when the computation ability of the edge devices is limited, this method could be the priority choice. The DPFL-LSTM (solid orange curve) and DPFL-BLSTM (solid pink curve) models had similar prediction performances, while the DPFL-BLSTM model was slightly better. When $\varepsilon = 8$ and $\delta = 10^{-5}$, the nRMSE values of DPFL-LSTM and DPFL-BLSTM were 9.94% and 10.17%, respectively.

These results demonstrate that ATT-BLSTM is more efficient in processing time-series data, especially when the data are nonstationary and nonlinear. The ATT-BLSTM's superior prediction performance can be summarized as follows: (1) The bidirectional structure enables the model to extract features from both forward and backward directions; (2) The attention mechanism helps the model find the essential hidden state of the current output.

D. Influence of Client Number

Another vital parameter that influences the performance of the proposed DPFL scheme is the client number K. Referring to [59], the choice of DP parameter δ is influenced by K and

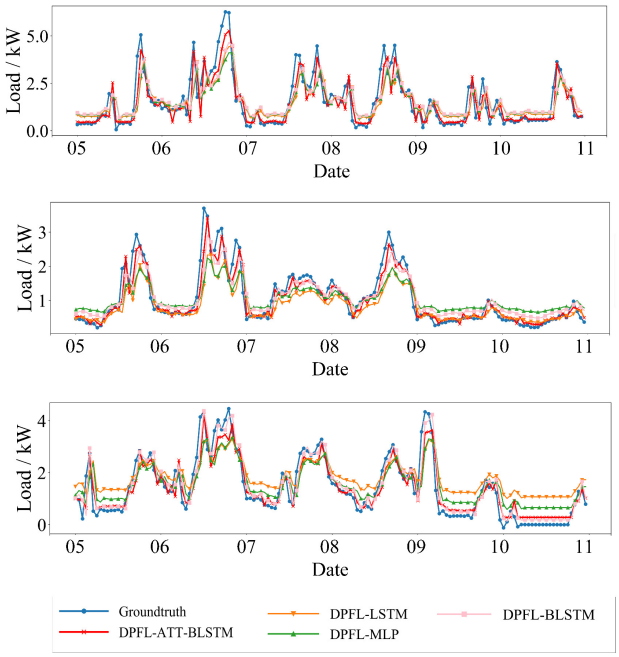

Fig. 7. Short-term load forecasting results of three houses predicted by four differential private federated learning algorithms ($\varepsilon = 8$, $\delta = 10^{-5}$).

should obey the following constraint:

$$\delta \ll \frac{1}{K} \tag{27}$$

This condition is to avoid protecting the majority of consumers' privacy by revealing a few consumers' [59]. According to this requirement, we set the threshold of δ, Q as 1×10^{-5}. In this experiment, the value of K ranges from 5 to 100, and the corresponding model performance and computation cost are shown in Figs. 8 and 9, respectively. From Fig. 8, when $K = 5$, the prediction error was considerably high, and it is observed that the model performance increases significantly from $K = 5$ to $K = 10$, and then the prediction accuracy increases steadily when K is between 10 and 50. When K is larger than 50,it is find that the performance improvement is not significant, and the accuracy of the model almost reached the same accuracy as non-DP schemes.

However, the computation cost raises dramatically when the value of K keeps increasing (see Fig. 9), which results in the extra investment in the cloud server which has higher computation and storage capacity. Based on the above simulation results, the conclusion was made that under the same privacy budget, more clients can efficiently reduce the accuracy cost, this is because during the secure aggregation process, more clients will reduce the standard deviation of the additive noise.

E. Influence of Privacy Parameter

In the DPFL scheme, the most important parameters to make the trade-off between privacy and accuracy are the two DP parameters ε and δ. Recall Algorithm 1: During the

TABLE II
PERFORMANCES OF THE PROPOSED MODELS AND BENCHMARK SERVICE MODELS

Model	ε	K	Round	MAPE (%)	nMAE (%)	nRMSE (%)
DPFL-MLP	1	5	1	221.4	32.99	35.25
		10	1	99.6	26.52	28.97
		50	1	76.51	16.51	20.38
	4	5	6	78.67	25.16	26.16
		10	3	70.82	9.06	11.59
		50	3	70.41	7.68	10.99
	8	5	36	162.87	20.32	21.64
		10	15	69.58	8.08	10.85
		50	18	63.68	8.32	10.5
DPFL-LSTM	1	5	1	257.2	29.51	31.87
		10	1	146.04	15.08	19.39
		50	1	75.12	10.63	13.06
	4	5	6	94.83	14.14	17.41
		10	3	71.55	7.4	10.65
		50	3	71.43	11.61	13.3
	8	5	36	73.88	15.65	21.91
		10	15	68.31	7.57	10.97
		50	18	62.43	7.24	9.94
DPFL-BLSTM	1	5	1	176.51	21.41	24.6
		10	1	152.1	12.13	17.11
		50	1	102.31	11.54	16.72
	4	5	6	79.17	15.46	16.49
		10	3	72.92	14.64	15.67
		50	3	70.98	9.72	12.13
	8	5	36	69.67	17.21	18.73
		10	15	65.95	10.01	11.68
		50	18	61.37	6.16	9.3
DPFL ATT-BLSTM	1	5	1	323.89	16.27	20.44
		10	1	400.23	19.89	23.09
		50	1	376.45	29.65	41.2
	4	5	7	51.21	20.73	21.44
		10	3	40.38	7.13	10.53
		50	3	36.35	5.68	8.07
	8	5	36	29.06	4.49	12.03
		10	15	24.67	4.36	7.52
		50	18	14.44	4.32	6.92
FL ATT-BLSTM	-	5	50	19.62	4.19	7.45
		10	50	17.2	3.76	6.7
		50	50	12.59	3.7	6.67
Centralised ATT-BLSTM	-	-	-	10.34	2.87	4.34
Localised ATT-BLSTM	-	-	-	68.73	10.01	10.69

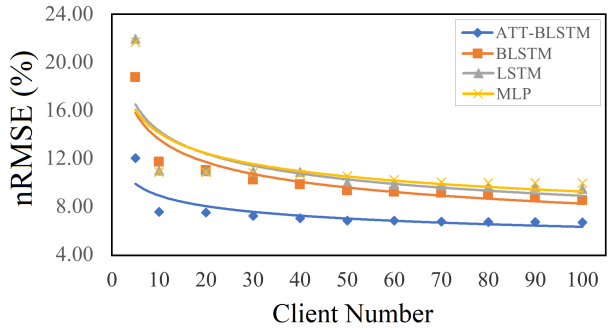

Fig. 8. (Comparison of total computation cost of proposed DPFL and benchmark service models.

secure aggregation process in each communication round, given ε and GM parameter σ; the central server accountant evaluates δ [54]. The central server will continue the communication rounds until δ reaches the threshold Q, then the whole training process will be stopped, and the server sends the well-trained model to all clients. As defined in

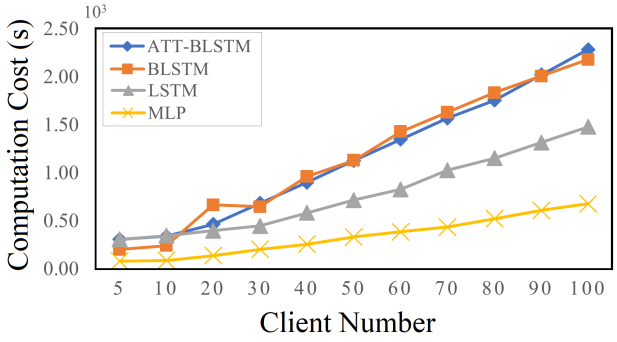

Fig. 9. (Computation costs of the proposed DPFL and benchmark service models.

Section V, Q is selected as 1×10^{-5}. In this case study, the influence of different values of ε (7 values chosen ranging from 1 to 12) on the model performance was investigated. From Fig. 7 (b), the DPFL-ATT-BLSTM scheme with small ε (1, 2, 4) reached the threshold Q quickly within just a few communication rounds. However, the model accuracy is undesirable, as the nRMSE maintains a high level, even higher than the localized scheme, the benchmark model with the worst performance. At this privacy level, although the privacy of consumers is protected perfectly, functionality is ultimately sacrificed. In contrast, when ε is large enough (such as 10 or 12 in our case), it takes more communication rounds until δ reaches the threshold. More communication rounds allow the central model to be fully trained with frequent updates of its model parameters. Consequently, the model accuracy increases as ε increases (as shown in Fig. 7 (a)). However, a large ε allows less similarity of the outputs from different clients, the adversary can distinguish different clients more effortlessly, and the model consequently provides less privacy. Hence, when ε is between 6 and 8, the proposed scheme can enable accurate load forecasting and provide a good level of privacy protection at the same time. In summary:

1) When $\varepsilon < 4$, the model provides strong privacy guarantee but low prediction accuracy.
2) When $4 < \varepsilon < 8$, the model reaches a balance between privacy and accuracy.
3) When $\varepsilon > 8$, the model reaches a higher accuracy but sacrifices privacy.

F. Privacy and Security Assessment

The privacy performance of the proposed scheme is discussed in the following aspects:

1) The proposed model resists inference and membership attacks from HBC TP. As stated in adversary model, the TPs are HBC adversary who would employ inference and membership attacks to infer whether a client participated during decentralized training. The proposed service model utilizes a secure aggregation mechanism during the data aggregation process and adds the Gaussian noise during the

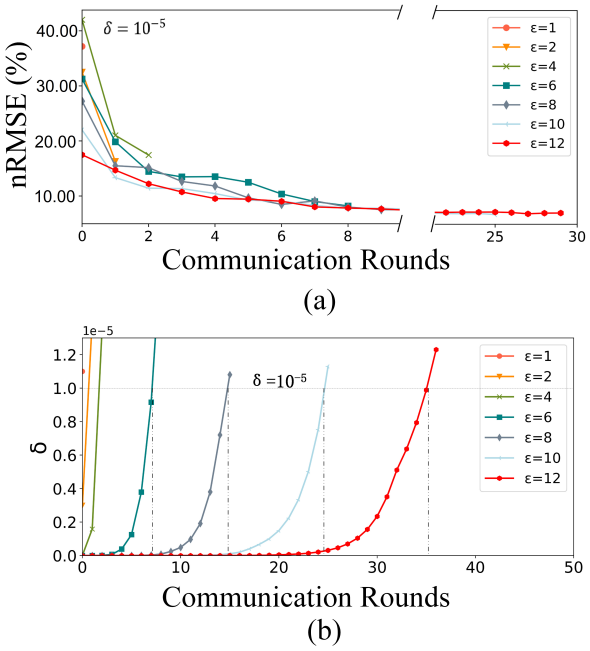

Fig. 10. (a) model performance of the differential private federated learning scheme with different levels of privacy budget; (b) accumulation of total δ with increasing communication rounds under different privacy budgets.

aggregation. As a result, individual participant's contribution during the training process is obscured. Hence, the proposed service model can resist inference and membership attacks from HBC TPs.

2) The proposed model resists low-quality local model update attack from the malicious clients. While the malicious clients may employ low-quality model attack to send low quality model parameters to the cloud server, the proposed service model utilizes K-means clustering algorithm to identify the malicious clients before the training round start. Hence, the proposed service model can resist low-quality model attack.

3) The proposed method resists eavesdropping attacks from the external adversary. The proposed model is constructed based on the FL framework, CEUD which contains sensitive information that never leaves the consumer's house. The external attacker cannot eavesdrop individual's CEUD from the communication channel.

VII. Conclusion

In this paper, we have proposed and validated a novel decentralized privacy-preserving value-added service model by considering both privacy and functionality requirements. The platform is constructed based on the DPFL framework and utilizes state-of-the-art ATT-BLSTM algorithm to train the local models. In the case study of household-level STLF, we evaluate the proposed scheme with six benchmark models. After simulation, it is validated that the proposed system achieves prediction accuracy with low computation cost, and the privacy loss can be controlled flexibility by adjusting privacy budget. Furthermore, the security of the proposed system is evaluated as well, the case study shows that the proposed DPFL based service model can resist attacks from: 1) the malicious clients who can employ low-quality local model update attack; 2) the HBC TPs who can utilize inference and membership attacks on the shared model parameters; and 3) the external attackers who want to eavesdrop the communication channel between the smart meter and the cloud server.

The limitation of this paper is this work is based on the virtual environment, and the proposed service model is not validated in the real world. For future work, a hardware-based service platform is expected to be built, the platform can better evaluate the proposed model especially when transient faults happen (such as a large of smart meters are offline due to a blackout). Moreover, we will investigate other kinds of energy services such as demand response, and renewable energy management. Furthermore, other privacy-preserving techniques such as block-chain and multi-party computation are expected to provide a better privacy guarantee to the energy consumer.

References

[1] Y. Xue and X. Yu, "Beyond smart grid—cyber–physical–social system in energy future [point of view]," *Proceedings of the IEEE*, vol. 105, no. 12, pp. 2290–2292, 2017.

[2] I. Kaur, "Chapter 29 - metering architecture of smart grid," in *Design, Analysis, and Applications of Renewable Energy Systems*, ser. Advances in Nonlinear Dynamics and Chaos (ANDC), A. T. Azar and N. A. Kamal, Eds. Academic Press, 2021, pp. 687–704. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128245552000307

[3] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Pérez-González, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 75–86, 2013.

[4] V. T. Hayashi, R. Arakaki, T. Y. Fujii, K. A. Khalil, and F. H. Hayashi, "B2b b2c architecture for smart meters using iot and machine learning: A brazilian case study," in *2020 International Conference on Smart Grids and Energy Systems (SGES)*. IEEE, 2020, pp. 826–831.

[5] Y. Gao, Z. Pan, H. Wang, and G. Chen, "Alexa, my love: analyzing reviews of amazon echo," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. IEEE, 2018, pp. 372–380.

[6] K. Noda, "Google home: smart speaker as environmental control unit," *Disability and rehabilitation: assistive technology*, vol. 13, no. 7, pp. 674–675, 2018.

[7] Y. Zhou, F. R. Yu, J. Chen, and Y. Kuo, "Cyber-physical-social systems: A state-of-the-art survey, challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 389–425, 2019.

[8] X.-Y. Zhang, C. Watkins, C. C. Took, and S. Kuenzel, "Privacy boundary determination of smart meter data using an artificial intelligence adversary," *International Transactions on Electrical Energy Systems*, vol. 31, no. 9, pp. 1–1, 2021.

[9] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "Real-time privacy-preserving data release for smart meters," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5174–5183, 2020.

[10] X. Cheng, R. Zhang, and L. Yang, "Consumer-centered energy system for electric vehicles and the smart grid," *IEEE intelligent systems*, vol. 31, no. 3, pp. 97–101, 2016.

[11] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, no. 3152676, pp. 10–5555, 2017.

[12] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.

[13] R. to the European Commission *et al.*, "Essential regulatory requirements and recommendations for data handling, data safety, and consumer protection," Technical Report version 1.0, 2011. https://ec. europa. eu/energy/sites/ener . . . , Tech. Rep.

[14] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys and Tutorials*, vol. PP, no. 4, pp. 1–1, 2017.

[15] M. LaMonica, "Cisco: Smart grid will eclipse size of internet," *Interview, May*, 2009.

[16] Z. Zhongming, L. Linong, Y. Xiaona, Z. Wangqiang, L. Wei, *et al.*, "Smart metering implementation programme: review of the data access and privacy framework," 2018.

[17] F.-Y. Wang, J. J. Zhang, R. Qin, and Y. Yuan, "Social energy: Emerging token economy for energy production and consumption," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 3, pp. 388–393, 2019.

[18] J. J. Zhang, D. W. Gao, Y. Zhang, X. Wang, X. Zhao, D. Duan, X. Dai, J. Hao, and F.-Y. Wang, "Social energy: mining energy from the society," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 3, pp. 466–482, 2017.

[19] J. J. Zhang, F.-Y. Wang, X. Wang, G. Xiong, F. Zhu, Y. Lv, J. Hou, S. Han, Y. Yuan, Q. Lu, *et al.*, "Cyber-physical-social systems: The state of the art and perspectives," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 829–840, 2018.

[20] T. Ming, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for iot-based smart homes," *Future Generation Computer Systems*, vol. 78, no. PT.3, pp. 1040–1051, 2016.

[21] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, and F.-Y. Wang, "Decentralized autonomous organizations: Concept, model, and applications."

[22] Jaime, Lloret, Jesus, Tomas, Alejandro, Canovas, Lorena, and Parra, "An integrated iot architecture for smart metering," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 50–57, 2016.

[23] M. Alessio and L. Atzori, "A cloud-based and restful internet of things platform to foster smart grid technologies integration and re-usability," in *2016 ICC - 2016 IEEE International Conference on Communications Workshops (ICC)*, 2016.

[24] X.-Y. Zhang, S. Kuenzel, J.-R. Córdoba-Pachón, and C. Watkins, "Privacy-functionality trade-off: A privacy-preserving multi-channel smart metering system," *Energies*, vol. 13, no. 12, p. 3221, 2020.

[25] X.-Y. Zhang and S. Kuenzel, "Differential privacy for deep learning-based online energy disaggregation system," in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*. IEEE, 2020, pp. 904–908.

[26] F.-Y. Wang, R. Qin, J. Li, X. Wang, H. Qi, X. Jia, and B. Hu, "Federated management: Toward federated services and federated security in federated ecology," *IEEE Transactions on Computational Social Systems*, vol. 8, no. 6, pp. 1283–1290, 2021.

[27] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.

[28] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for iot security attacks," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 2545–2554, 2022.

[29] H. Liang, D. Liu, X. Zeng, and C. Ye, "An intrusion detection method for advanced metering infrastructure based on federated learning," *Journal of Modern Power Systems and Clean Energy*, 2022.

[30] S. Salim, B. Turnbull, and N. Moustafa, "A blockchain-enabled explainable federated learning for securing internet-of-things-based social media 3.0 networks," *IEEE Transactions on Computational Social Systems*, pp. 1–17, 2021.

[31] D. Połap, G. Srivastava, J. C.-W. Lin, and M. Woźniak, "Federated learning model with augmentation and samples exchange mechanism," in *Artificial Intelligence and Soft Computing*, L. Rutkowski, R. Scherer, M. Korytkowski, W. Pedrycz, R. Tadeusiewicz, and J. M. Zurada, Eds. Cham: Springer International Publishing, 2021, pp. 214–223.

[32] X. Zhang, F. Fang, and J. Wang, "Probabilistic solar irradiation forecasting based on variational bayesian inference with secure federated learning," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7849–7859, 2021.

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

[34] S. Lee and D.-H. Choi, "Federated reinforcement learning for energy management of multiple smart homes with distributed energy resources," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 488–497, 2022.

[35] A. K. Roy, K. Nath, G. Srivastava, T. R. Gadekallu, and J. C.-W. Lin, "Privacy preserving multi-party key exchange protocol for wireless mesh networks," *Sensors*, vol. 22, no. 4, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/5/1958

[36] C. Dwork, "Differential privacy: A survey of results," in *International Conference on Theory and Applications of Models of Computation*, 2008.

[37] T. Ha, T. K. Dang, T. T. Dang, T. A. Truong, and M. T. Nguyen, "Differential privacy in deep learning: An overview," in *2019 International Conference on Advanced Computing and Applications (ACOMP)*, 2019.

[38] Muneeb, Ul, Hassan, Mubashir, Husain, Rehmani, Jinjun, and Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 746–789, 2019.

[39] M. Yang, W. Tu, J. Wang, F. Xu, and X. Chen, "Attention based lstm for target dependent sentiment classification," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 31, no. 1, 2017.

[40] D. Bahdanau, K. H. Cho, and Y. Bengio, "Neural machine translation by jointly learning to align and translate," in *3rd International Conference on Learning Representations, ICLR 2015*, 2015.

[41] F. Ma, R. Chitta, J. Zhou, Q. You, T. Sun, and J. Gao, "Dipole: Diagnosis prediction in healthcare via attention-based bidirectional recurrent neural networks," in *ACM*, 2017.

[42] V. Piccialli and A. M. Sudoso, "Improving non-intrusive load disaggregation through an attention-based deep neural network," *Energies*, vol. 14, 2021.

[43] X. Zhang, S. Kuenzel, N. Colombo, and C. Watkins, "Hybrid short-term load forecasting method based on empirical wavelet transform and bidirectional long short-term memory neural networks," *Journal of Modern Power Systems and Clean Energy*, Jan. 2022.

[44] X. Zhang, S. Kuenzel, and C. Watkins, "A hybrid data-driven online solar energy disaggregation system from the grid supply point," *Complex & Intelligent Systems*, July 2022.

[45] X. Zhang, C. Watkins, and S. Kuenzel, "Multi-quantile recurrent neural network for feeder-level probabilistic energy disaggregation considering roof-top solar energy," *Engineering Applications of Artificial Intelligence*, Apr. 2022.

[46] A. Moradi, N. K. Venkategowda, S. P. Talebi, and S. Werner, "Distributed kalman filtering with privacy against honest-but-curious adversaries," in *2021 55th Asilomar Conference on Signals, Systems, and Computers*. IEEE, 2021, pp. 790–794.

[47] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *2017 IEEE symposium on security and privacy (SP)*. IEEE, 2017, pp. 3–18.

[48] M. Fredrikson, S. Jha, and T. Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures," in *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, 2015, pp. 1322–1333.

[49] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342–1363, 2015.

[50] L. Zhu, M. Li, Z. Zhang, X. Du, and M. Guizani, "Big data mining of users' energy consumption patterns in the wireless smart grid," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 84–89, 2018.

[51] S. Zhang, J. Rong, and B. Wang, "A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain," *International Journal of Electrical Power & Energy Systems*, vol. 121, p. 106140, 2020.

[52] N. Carlini, C. Liu, U. Erlingsson, J. Kos, and D. Song, "The secret sharer: Evaluating and testing unintended memorization in neural networks," in *Proceedings of the 28th USENIX Conference on Security Symposium*, ser. SEC'19. USA: USENIX Association, 2019, p. 267–284.

[53] N. Agarwal, A. T. Suresh, F. X. X. Yu, S. Kumar, and B. McMahan, "cpsgd: Communication-efficient and differentially-private distributed sgd," *Advances in Neural Information Processing Systems*, vol. 31, 2018.
[54] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Differentially private asynchronous federated learning for mobile edge computing in urban informatics," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2134–2143, 2019.
[55] O. Parson, G. Fisher, A. Hersey, N. Batra, J. Kelly, A. Singh, W. Knottenbelt, and A. Rogers, "Dataport and nilmtk: A building data set designed for non-intrusive load monitoring," in *2015 ieee global conference on signal and information processing (globalsip)*. IEEE, 2015, pp. 210–214.
[56] N. Oceanic and A. A. (NOAA), "National centers for environmental information (ncei)." *Historical Palmer Drought Indices.*, 2016.
[57] A. Paszke, S. Gross, F. Massa, A. Lerer, J. Bradbury, G. Chanan, T. Killeen, Z. Lin, N. Gimelshein, L. Antiga, *et al.*, "Pytorch: An imperative style, high-performance deep learning library," *Advances in neural information processing systems*, vol. 32, 2019.
[58] C. Radebaugh and U. Erlingsson, "Introducing tensorflow privacy: learning with differential privacy for training data," *Medium. com (accessed 2022-01-27). https://medium. com/tensorflow/introducing-tensorflowprivacy-learning-with-differential-privacy-for-trainingdata-b143c5e801b6*, 2019.
[59] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, ser. Proceedings of Machine Learning Research, A. Singh and J. Zhu, Eds., vol. 54. PMLR, 20–22 Apr 2017, pp. 1273–1282. [Online]. Available: https://proceedings.mlr.press/v54/mcmahan17a.html

Xiao-Yu Zhang received the B. Eng. degree from the North China Electric Power University, Beijing, China in 2016. The M.S.degree with distinction in electrical power system from University of Birmingham, Birmingham, U.K., in 2017, and the Ph.D. degree in electrical engineering from the Royal Holloway, University of London, London, U.K., in 2022. He is currently a lecturer in School of Artificial Intelligence, Anhui University, Hefei, China. His research interests include deep learning technology & data analytics in smart grids, smart grid privacy and security, and, demand-side management.

José-Rodrigo Córdoba-Pachón obtained a computer science and systems engineering degree at Universidad de los Andes in Bogota, Colombia. The MA (Master of Arts) degree with distinction in Management Systems at the University of Hull, Hull, U.K.. And was offered a fully funded PhD scholarship to research on critical systems thinking and information systems at Hull's centre for systems studies. José-Rodrigo is currently a senior lecturer in information and technology management at the School of Business and Management of Royal Holloway, University of London, London, U.K.. José-Rodrigo's research interests lie at the intersection between technological, ethical and social systems. He currently serves as application area editor (social responsibility) of the journal Systems Research and Behavioural Science. and as international researcher at the Social and Business Research Lab (SBRLab) of Universitat Rovira i Virgili in Tarragona, Catalonia, Spain.

Peiqian Guo received the B.S. and the M.Sc. degrees in Electrical and Electronic Engineering from the University of Birmingham, Birmingham, U.K. in 2015 and 2017. He is currently an Assistant Researcher (medium level) with the Department of Electrical Engineering, Tsinghua University, where he has been since 2018. His research interests include power system operation and control, renewable integration, voltage sourced converter-based direct current transmission and distribution systems, power quality research, energy storage system, and FACTS.

Chris Watkins received the Ph.D. degree from University of Cambridge, U.K.. He is a world-class authority on reinforcement learning & evolutionary theory and professor of Artificial Intelligence at Royal Holloway, University of London, U.K.. He coined the Q-Table algorithm approach that spurred the resurgence in reinforcement learning (this approach was at the heart of Google's recent successful AI projects). Prior to returning to academia, Chris was employed as a quant at a hedge fund firm in London for several years. Chris is presently working on how to make generally intelligent machines, along with abstract models of evolution, and statistical visualization.

Stefanie Kuenzel (S'11-M'14-SM'19) received the M.Eng.and Ph.D. degrees from Imperial College London, London,U.K., in 2010 and 2014, respectively. She is currently the Head of the Power Systems Group and a Senior Lecturer with the Department of Electronic Engineering, Royal Holloway, University of London, London, U.K.. Her current research interests include renewable generation and transmission, including HVDC as well as Smart Meters. Dr Kuenzel also functions as editor for IEEE Transactions on Sustainable Energy, IEEE Power Engineering Letters.