P^3: Privacy-Preserving Prediction of Real-time Energy Demands in EV Charging Networks

Beibei Li, *Member, IEEE*, Yuqing Guo, Qingyun Du, *Student Member, IEEE*, Ziqing Zhu, Xiaohui Li, *Member, IEEE*, and Rongxing Lu, *Fellow, IEEE*

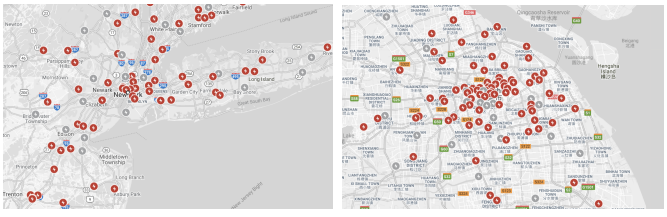
***Abstract*— Real-time and accurate prediction of charging pile energy demands in electric vehicle (EV) charging networks contributes significantly to load shedding and energy conservation. However, existing methods usually suffer from either data privacy leakage problems or heavy communication overheads. In this paper, we propose a novel blockchain-based personalized federated deep learning scheme, coined P^3, for privacy-preserving energy demands prediction in EV charging networks. Specifically, we first design an accurate deep learning-based energy demands prediction model for charging piles, by making use of the CNN, BiLSTM, and attention mechanism. Second, we develop a blockchain-based hierarchical and personalized federated learning framework with a consensus committee, allowing charging piles to collectively establish a comprehensive energy demands prediction model in a low-latency and privacy-preserving way. Last, a CKKS cryptosystem based secure communication protocol is crafted to guarantee the confidentiality of model parameters while model training. Extensive experiments on two real charging pile datasets demonstrate the superiorities of the proposed P^3 scheme in accurately predicting real-time energy demands over state-of-the-art schemes. Further, the P^3 scheme can achieve reasonably low computational costs, compared with other homomorphic-based schemes, such as Paillier and BFV.**

***Index Terms*— Electric vehicle (EV) charging networks, energy demands prediction, privacy preservation, federated learning, blockchain, CKKS homomorphic encryption.**

I. Introduction

RAPID advancements in electric vehicle (EV) technologies have facilitated the interest in establishing EV charging networks by either the governments or car manufacturers. For instance, as of November 2020, the largest fast-charging location was in California on the Tesla Supercharger network, with 56 charging stalls (see Fig. 1 for examples of Tesla EV chargers deployment in New York, USA, and Shanghai, P. R. China, respectively). EV charging networks are critical infrastructures for recharging electric vehicles. At the same time, a large number of electric vehicles themselves can also serve as mobile energy storage devices, which can be charged during the trough period of grid electricity consumption to reserve electricity and reversely transmit power to the grid during peak electricity consumption periods to achieve load shedding, thereby improving grid stability and reducing power generation costs [1]. One big challenge for EV charging networks is that during peak hours (say on weekends or public holidays), an extensive number of EVs may request for concurrent charging services, which inevitably causes energy transfer congestion problems [2]. In addition, power grids may also suffer from high disturbances if load demands change abruptly.

In this regard, a line of energy demands prediction schemes have been presented in recent years [3]–[6]. For example, in 2018, Fukushima *et al.* [3] developed a recommendation system by predicting the mileage of multiple electric vehicles on highways. In 2019, Mao *et al.* [4] proposed a model for predicting the dispatchable capacity of electric vehicles based on the parallel gradient boosting decision tree algorithm and multi-time-scale big data analysis. In 2021, Rob Shipman *et al.* [6] developed a time series prediction neural network capable of predicting the aggregated available capacity of EVs in the next 24 hours. However, since energy charging data is privacy-sensitive information, which may leak customers' traveling routes, home and office addresses, payment information, individual preferences, etc. [7], most existing energy demands prediction schemes fail to consider the privacy preservation issues. Further, many of these schemes perform energy demands prediction in a centralized way, usually leading to heavy communication and computational overheads, and delayed



(a) New York, USA (b) Shanghai, P.R. China

Fig. 1. Deployment of Tesla EV chargers in New York and Shanghai.

This work is partially supported by the National Natural Science Foundation of China under Grants No. 62002248, No. 62101368, and No. U2133208; the Sichuan Youth Science and Technology Innovation Team under Grant No. 2022JDTD0014; the Sichuan Science and Technology Program under Grant No. 2022YFG 0193; the Fundamental Research Funds for the Central Universities under Grant No. YJ201933 (*Corresponding author: Xiaohui Li*).

B. Li, Y. Guo, Q. Du, Z. Zhu, and X. Li are with the School of Cyber Science and Engineering, Sichuan University, Chengdu 610065, China (e-mail: {libeibei, lixiaohui}@scu.edu.cn; {yuqingguo, duqingyun, zhuziqing}@stu.scu.edu.cn).

R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B 5A3, Canada (e-mail: rlu1@unb.ca).

energy prediction results.

To address these problems, we are motivated to propose a privacy-preserving real-time energy demands prediction scheme, coined P^3, for EV charging networks. Specifically, we develop a blockchain-based federated learning framework, where charging piles can jointly establish an energy demands prediction scheme with no need to share their local energy consumption data. In addition, since it has been proved that model parameters or gradients may leak key information of the original data [8], we also craft a CKKS-based secure communication protocol to protect the model parameters while model training. Further, we design an accurate energy demands prediction model for energy charging piles in each cluster, by making use of convolutional neural network (CNN), bidirectional long short-term memory (BiLSTM), and the attention mechanism. The main contributions of our work are summarized as follows:

1) First, we design a deep learning based energy demands prediction model for EV charging networks, by making use of the CNN, BiLSTM, and attention mechanism, which can achieve accurate prediction of future electricity consumption at each charging pile.
2) Second, we develop a blockchain-based hierarchical and personalized federated learning framework, which allows charging piles to collectively establish a global energy demands prediction model and then create a personalized model for each cluster in a low-latency and privacy-preserving way.
3) Third, we craft a CKKS cryptosystem based secure communication protocol, which can not only guarantee the confidentiality of model parameters while model training, but also ensure the legitimate identities of charging piles in participating federated learning.

The remaining of this paper is organized as follows: Section II summarizes the related works. Section III introduces our system model and threat model. In Section IV, we elaborate on the proposed P^3 scheme. Then, in Section V, extensive experiments are conducted to evaluate the performance of our scheme. Last, we draw our conclusions in Section VI.

II. Related Work

In this section, we briefly review the state-of-the-art research works focusing on energy demands prediction, privacy preservation, and federated learning in EV-relevant systems.

A. Energy Demands Prediction

To facilitate efficient energy management and support load shedding, a growing interest in energy demands prediction in EV-relevant systems has been shown in recent years. In 2018, Fukushima *et al.* [3] developed a recommendation system based on the prediction of the mileage of multiple electric vehicles on highways, and applied the learning method based on multiple regression to improve the prediction accuracy of EVs energy consumption. In 2019, Saputra *et al.* [2] further proposed an energy demand learning method based on deep learning and federal learning to improve the accuracy of energy demand prediction and reduce the communication overhead of electric vehicle network. In 2019, Mao *et al.* [4] proposed a model for predicting the dispatchable capacity of electric vehicles based on the parallel gradient boosting decision tree algorithm and multi-time-scale big data analysis. In 2020, Yang *et al.* [5] pointed out that prediction models must take into account not only conventional behaviors but also short-term uncertainties. In 2021, Rob Shipman *et al.* [6] developed a time series prediction neural network capable of predicting the aggregate available capacity of EVs in the next 24 hours and demonstrated its enhanced predictive power on regression models trained by automatic machine learning. In the same year, Álvarez *et al.* [9] proposed a method for probabilistic load forecasting based on the adaptive online learning of hidden Markov models, which recursively updates model parameters and uses the latest parameters to obtain probabilistic forecasts.

B. Privacy Preservation

The privacy preservation issues of EV-generated data (say energy charging data, vehicle location data, etc.) have drawn extensive attention over the years. In 2016, Li *et al.* [10] proposed a privacy-preserving and fast authentication protocol, called Portunes+, for charging pads to authenticate an EV's identity. In 2018, Li *et al.* [11] proposed a new spatial decomposition algorithm by combining the random sampling algorithm with the quadtree algorithm, adding noise satisfying the differential privacy into the spatial segmentation algorithm to ensure the security of single location data. In the same year, Knirsch *et al.* [12] presented a reliable, automated, and privacy-preserving selection of charging stations based on pricing and the distance to the electric vehicle. Also in 2018, Gao *et al.* [13] proposed a blockchain-based privacy-preserving payment mechanism for vehicle-to-grid (V2G) networks, which enables data sharing while securing sensitive user information. In 2020, Feng *et al.* [14] introduced a novel framework called blockchain-assisted privacy-preserving authentication system (BPAS), which can provide authentication automatically in vehicular ad hoc networks (VANETs) and preserves vehicle privacy at the same time. In 2021, Baza *et al.* [15], leveraging blockchain technology, proposed a privacy-preserving charging-station-to-vehicle (CS2V) energy trading scheme as well as a vehicle-to-vehicle (V2V) energy trading scheme. The proposed schemes are useful in crowded cities where there is a need for charging many EVs daily.

C. Federated Learning

Federated learning has been a promising distributed learning paradigm in recent years. In 2019, Saputra *et al.* [2] proposed an energy demand learning (EDL)-based prediction solution with federated learning, in which a charging station provider gathers information from all charging stations and then performs the EDL algorithm to predict the energy demand for the considered area without revealing real datasets. In 2020, Lu *et al.* [16] proposed a federated learning based secure and intelligent mechanism and designed a two-phase mitigating scheme consisting of intelligent data transformation and collaborative data leakage detection in vehicular cyber-physical systems. In

the same year, Du *et al.* [17] conducted a brief survey of existing studies on federated learning and its use in wireless Internet of Things (IoT). Then, they discussed the significance and technical challenges of applying federated learning in vehicular IoT, and pointed out future research directions. Also in 2020, Pokhrel *et al.* [18] proposed a communication efficient and privacy-preserving federated learning framework for enhancing the performance of Internet of Vehicles (IoV). In 2021, Huang *et al.* [19] proposed FedParking, which enables parking lot operators to jointly train long-short term memory (LSTM) models for parking space estimation based on federated learning. In the same year, Chai *et al.* [20] proposed a hierarchical blockchain framework and a federated learning algorithm for knowledge sharing among smart vehicles. Chen *et al.* [21] proposed a Byzantine-fault-tolerance decentralized federated learning method for autonomous vehicles, using a publicly verifiable secret sharing scheme to protect federated learning models. Also in 2021, Kong *et al.* [22] proposed an efficient, flexible, and privacy-preserving model aggregation scheme under a federated learning-based navigation framework (named FedLoc), which achieves flexibility and robustness and supports the dynamic joining and leaving of participants.

III. System Model and Threat Model

In this section, we introduce the system model and threat model considered in this work.

A. System Model

The system model considered in this paper is shown in Fig. 2. It mainly consists of three types of entities, namely the trusted authority (TA), charging piles, and fog nodes.

1) Trusted authority: In order to realize secure communications, the trusted authority generates the public and private keys required for encryption and decryption based on the CKKS cryptosystem, and distributes them to the charging piles and fog nodes.
2) Charging pile: Each charging pile, supplying energy to electric vehicles, trains a local energy demands prediction model with its own charging records. In each round of federated learning, charing piles encrypt their local model parameters and transfer them to the corresponding fog nodes. After fog nodes update the global model, the charing piles receive the global updates and further adjust their own energy demands prediction models.
3) Fog node: As the agents of each charging pile cluster, fog nodes are responsible for aggregating the local model parameters of charging piles in their own clusters. More importantly, they also take charge of further aggregating and updating the global model parameters to the blockchain, and then distribute these parameters to charging piles.

B. Threat Model

In this work, TA is considered a fully trusted party that bootstraps the entire system and distributes the keys to all

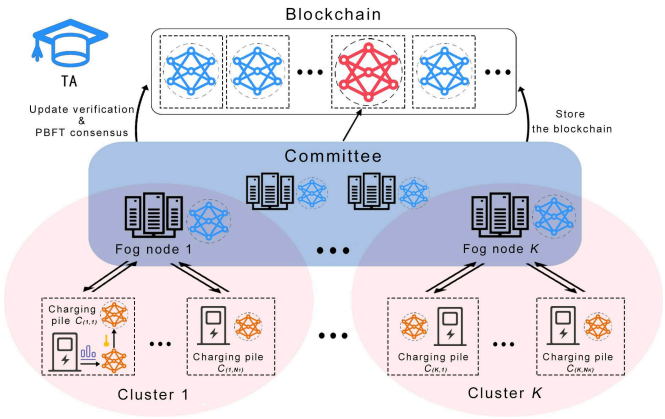


Fig. 2. The system model under consideration.

participants. Fog nodes are considered semi-trusted, which means they are honest in model training but are curious about the energy charging data as well as the model parameters at each charging pile. Charging piles are considered trusted parties that honestly collect and report energy charging data to fog nodes.

In addition, this work also considers other types of cyber threats, including malicious eavesdropping or interception over communication links for energy charging data or model parameters. Since energy charging data contains users' private information, it cannot be shared with any third party without legal authorization. Model parameters may be used to infer the partial distribution patterns of original training data, and the confidentiality of model parameters should also be guaranteed. As we see, the proposed scheme should achieve confidentiality of not only the energy charging data but also the model parameters while transmission.

IV. The Proposed P^3 Scheme

In this section, we elaborate on the proposed P^3 scheme, including the overall workflow, CNN-BiLSTM-Attention-based energy demands prediction, blockchain-based hierarchical and personalized federated learning framework, and secure communication protocol based on CKKS.

A. The Overall Workflow

The main goal of the proposed scheme is to allow multiple charging piles to jointly build an effective energy demands prediction model in a privacy-preserving way. The complete workflow can be divided into the following six phases.

1) System Initialization: The TA generates public key $pk = (b, a)$ and secret key $sk = (1, s)$ by executing $KeyGenerate()$, to establish a secure channel between charging piles. Each charging pile participating in federated learning needs to register at the TA. All N_C charging piles are divided into K clusters $\{J_1, J_2, \ldots, J_K\}$ according to their geographical locations. Thus the cluster J_k consists of charging piles $\{C_{(k,1)}, C_{(k,2)}, \ldots, C_{(k,N_k)}\}$. The fog nodes agree on the initial parameters W_0 of the energy prediction model and other relevant parameters (i.e., the learning rate η, batch size B, the

total number of communication rounds L, and the loss function F) as the common training goal of N_C charging piles, and then distribute the initial global model to each charging pile.

2) Local Model Training: The charging pile $C_{(k,i)}$ performs model training with local data $D_{(k,i)}$ to obtain local model update $W^l_{(k,i)}$ and uses $ParaEncrypt()$ to encrypt model parameters. The final generated local model update message contains the local model update ciphertext $E\left(W^l_{(k,i)}\right)$, timestamp T_s, and sample size $n_{(k,i)}$.

3) Model Parameters Aggregation: Each charging pile sends the local model update ciphertext to the corresponding fog node, and the fog node aggregates them one by one.

4) Cluster Model Uploading: Fog nodes upload the aggregated local model update ciphertexts to the blockchain, and a consensus committee is responsible for verifying the updates and executing the Practical Byzantine Fault-tolerance (PBFT) consensus algorithm [14] to generate new blocks.

5) Global Model Updating: The consensus committee performs the aggregation process to generate a new global model update block based on the verified updates in the blockchain, and distributes it back to the charging piles via the fog nodes.

6) Model Personalization: Repeat phases 2) to 5) until the global model updating converges to a steady model or meets a termination requirement. Then, the fog nodes personalize the local energy demands prediction model in their own clusters.

B. CNN-BiLSTM-Attention-Based Energy Demands Prediction Model

In this work, the CNN-BiLSTM algorithm with an attention mechanism is exploited to train the energy demands prediction model. The one-dimensional convolutional layer of CNN can extract effective features from the input data. The classical LSTM makes the weight of self-loop variable by adding the input gate, forget gate, and output gate. When the model parameters are fixed, the integral scale at different times can be dynamically changed, thus avoiding the problem of gradient disappearance or expansion. The LSTM model can be expressed as follows:

$$\begin{cases} f_t &= \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \\ i_t &= \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \\ \tilde{C}_t &= tanh(W_C \cdot [h_{t-1}, x_t] + b_C) \\ C_t &= f_t \cdot C_{t-1} + i_t \cdot \tilde{C}_t \\ o_t &= \sigma(W_o[h_{t-1}, x_t] + b_o) \\ h_t &= o_t \cdot tanh(C_t). \end{cases} \tag{1}$$

In BiLSTM, we get the hidden state $\overrightarrow{h_t}$ of the forward LSTM and the hidden state $\overleftarrow{h_t}$ of the reverse LSTM, then the hidden state of the BiLSTM at time t is given by

$$h_t = \overrightarrow{h_t} \oplus \overleftarrow{h_t}. \tag{2}$$

The attention weights and the corresponding hidden layer states are weighted and summed to obtain the final attention weights, which is given by

$$a_t = \sum_{t=1}^{m} softmax(tanh(h_t)) \cdot h_t. \tag{3}$$

Suppose that the global model needs to undergo L updates, and the local model of charging pile is iterated T times in each update. Each charging pile $C_{(k,i)}$ locally trains the proposed energy demands prediction model on their own data $D_{(k,i)}$. In the l-th round, each charging pile $C_{(k,i)}$ first uses the given updated model parameter to update its model parameter $W^l_{(k,i)}$ and retrains the model based on the Adam optimizer. v_1 and v_2 represent the exponential moving average of $W^l_{(k,i)}$ and $\left(W^l_{(k,i)}\right)^2$, respectively. ρ_1 and ρ_2 are the exponential decay rate of v_1 and v_2, which are used to control the updating speed of the model. The updating rules include:

$$\begin{cases} v_1 = \rho_1 v_1 + (1-\rho_1) W^l_{(k,i)} \\ v_2 = \rho_2 v_2 + (1-\rho_2)\left(W^l_{(k,i)}\right)^2. \end{cases} \tag{4}$$

Then, calculate the bias-corrected v_1 and v_2:

$$v_1 = \frac{v_1}{1-\rho_1^\tau}, v_2 = \frac{v_2}{1-\rho_2^\tau}, \tag{5}$$

where τ is the time step. $C_{(k,i)}$ updates the model locally by

$$W^l_{(k,i)} = W^l_{(k,i)} - \eta \frac{v_1}{\sqrt{v_2 + \theta}}, \tag{6}$$

where θ is a small constant used to stabilize the value.

C. Blockchain-Based Hierarchical and Personalized Federated Learning Framework

In this work, we design a blockchain-based hierarchical and personalized federated learning framework (see Algorithm 1), where a consensus committee is established to replace the central server in the traditional federated learning architectures to collaborate on global model update aggregation and verification. The framework can significantly enhance scalability, security, and robustness. In addition, each cluster has its own personalized model, which improves the accuracy of energy demands prediction.

Since the energy consumption data at charging piles are strongly correlated with their positions and nearby customers, the global model obtained by traditional federated learning cannot well adapt to each charging pile, leading to reduced accuracy of energy demands prediction. To solve this problem, we divide the charging piles into multiple clusters and employ both inter-cluster and inner-cluster federated learning. The inter-cluster federated learning trains a global model as the base layer, and inner-cluster federated learning trains a personalization layer for each cluster (see Fig. 3). For the charging pile clustering algorithm, we utilize the K-means algorithm, where the log data of charging piles contain their location information expressed in latitude and longitude.

In this framework, each cluster is assigned a fog node as an agent, we use the alliance chain and require only TA-certified fog nodes to join the blockchain. The consensus committee $\mathcal{F}$, composed of all fog nodes, makes use of the PBFT consensus mechanism [14]. At the beginning of federated learning, they jointly agree on the basic parameters of the initial model W_0 and the relevant parameters of the training, and then store them in block 0 of the blockchain. Later, the blockchain stores both

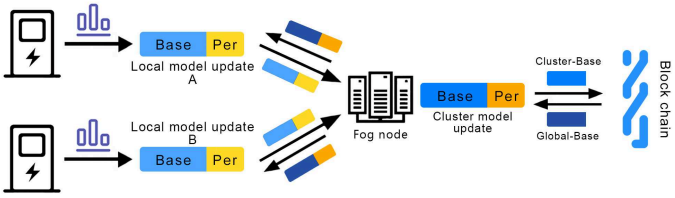


Fig. 3. The diagram of hierarchical and personalized federated learning.

cluster model update blocks and global model update blocks. The cluster model update block contains: block headers, current round number l, cluster number k, cluster model update ciphertext M_k (which is aggregated from local model update ciphertext), each sample size $\{n_{(k,1)}, n_{(k,2)}, \ldots, n_{(k,N_k)}\}$, and timestamp $\{T_{s(k,1)}, T_{s(k,2)}, \ldots, T_{s(k,N_k)}\}$. The global model update block contains: block headers, current round number l, and global model update ciphertext M. The fog nodes store the entire list of blockchains, and historical blocks in the blockchain can be used to revert to previous states in the event of an error.

Algorithm 1: Hierarchical and Personalized Federated Learning

Initialization: Initialize W_0 ;
for *round* $l = 1, 2, \ldots$ **do**
  (I). For charging piles:
  if $l > 1$ **then**
    a). Receive WG_B^{l-1} and W_{kP}^{l-1} from fog node;
    b). Set the model parameters by $W_{(k,i)}^l \leftarrow \left(WG_B^{l-1}, W_{kP}^{l-1}\right)$;
  end
  repeat local training
    for *each batch of data resource* **do**
      Compute the gradient $W_{(k,i)}^l$;
      Use Adam Optimizer to update the model parameters:$W_{(k,i)}^l \leftarrow W_{(k,i)}^l - \eta \frac{\nu_1}{\sqrt{\nu_2 + \theta}}$;
    end
  until *the loss function* f *converges*;
  Send $W_{(k,i)}^l$ to the fog node;
  (II). For fog nodes:
  a). Receive $W_{(k,i)}^l$ from each charging pile $C_{(k,i)}, i \in \{1, \ldots, N_k\}$;
  b). Aggregate $W_k^l = \left(W_{kB}^l, W_{kP}^l\right) \leftarrow \left(\sum_{i=1}^{N_k} \alpha_{(k,i)} W_{B(k,i)}^l, \sum_{i=1}^{N_k} \alpha_{(k,i)} W_{P(k,i)}^l\right)$;
  c). Upload W_{kB}^l to the blockchain;
  if *there are* K *global update blocks on the blockchain* **then**
    Aggregate $WG_B^l \leftarrow \sum_{k=1}^{K} \left(\sum_{i=1}^{N_k} \alpha_{(k,i)} W_{B(k,i)}^l\right)$;
    Send WG_B^l,W_{kP}^l to each charging pile $C_{(k,i)}$;
  end
end

In classical federated learning, the goal is to minimize the objective function:

$$F = \sum_{i=1}^{N_C} \frac{n_i}{N_s} f(WG), \tag{7}$$

where N_s is the total number of samples across all piles, f is the loss function on charging piles, and WG is global model parameters. In our proposed p^3 scheme, the goal is to minimize the objective function:

$$F = \sum_{i=1}^{N_C} \frac{n_i}{N_s} f(W_k), \tag{8}$$

where W_k is the personalization model for each cluster. Specifically, in the l-th round, each charging pile $C_{(k,i)}$ first updates its own model parameter $W_{(k,i)}^l$ according to the global base layer parameter WG_B^{l-1} and the cluster personalization layer parameter W_{kP}^{l-1} received from the fog node. It then retrains the model and sends the resulting local parameters $W_{(k,i)}^l = \left\{W_{B(k,i)}^l, W_{P(k,i)}^l\right\}$ to the fog node, where $W_{B(k,i)}^l$ is the weight of the base layer and $W_{P(k,i)}^l$ is the weight of the personalization layer. In our model, the attention layer is used as the personalization layer, and the remaining layers are used as the base layer. Charging pile $C_{(k,i)}$ only uploads the encrypted model parameter updates, while the original data is stored locally. The fog node aggregates the local model updates of each charging pile from J_k according to the following formula:

$$\begin{aligned} W_k^l &= \left\{W_{kB}^l, W_{kP}^l\right\} \\ &= \left\{\sum_{i=1}^{N_k} \alpha_{(k,i)} W_{B(k,i)}^l, \sum_{i=1}^{N_k} \alpha_{(k,i)} W_{P(k,i)}^l\right\}, \end{aligned} \tag{9}$$

where the contribution rate $\alpha_{(k,i)}$ is the proportion of training data $D_{(k,i)}$ to the total number of training samples. Then, the fog node obtains the information of N_k charging piles $\left\{W_k^l, T_{s(k,1)}, \ldots, T_{s(k,N_k)}, n_{(k,1)}, \ldots, n_{(k,N_k)}\right\}$ and upload it to the blockchain. After completing the aggregation task, fog node F_i uses this information as transaction b. It then broadcasts b and $< propose, v, u, d >$ within the committee, where v is the view number corresponding to F_i, u is the unique number of b, and d is the hash digest of b. It should be noted that for the weight part, fog nodes only upload the aggregated base layer W_{kB}^l instead of the entire weight W_k^l. Other committee members broadcast $< prepare, v, u, d, i >$ after receiving and verifying the information broadcast by other fog nodes, where i is the serial number of these members themselves. When other members receive $2f + 1$ broadcasts, they further broadcast $< commit, v, u, d, i >$ and commit b to slot. These updates that pass validation will be packaged onto the blockchain as a cluster model update block. When the number of cluster model update blocks in round l is equal to K, the committee will conduct a secondary aggregation of all cluster model updates in this round to generate a new global model update block, the principle is the same as above. Specifically, we randomly select a committee member

as the leader F_L to be responsible for secondary aggregation. When secondary aggregation is to be performed, a member F_i will start a timer $\mathcal{T}$, and if the global model update block has not been generated after the timeout, the leader is considered to be faulty and re-selected. The global model parameter $WG_B^l = \sum_{k=1}^{K}\left(\sum_{i=1}^{N_k}\alpha_{(k,i)}W_{B(k,i)}^l\right)$. Then the fog nodes distribute WG_B^l and W_{kP}^l to each charging pile, start $l+1$ round of training, and repeat the above steps. When $\left|WG_B^l - WG_B^{l-1}\right| \leq \varepsilon$, where ε is any positive number, that is to say, the global gradient converges, or when a certain number of iterations is reached, the model training stops.

The traceable, tamper-proof nature of the blockchain makes it more resistant to malicious attacks and blocks on the chain can be publicly verified thus can mitigate the impact of poison attacks. In addition, model update information is always stored in ciphertext on the chain, further ensuring that it is not exposed to unauthorized, untrusted devices.

D. CKKS-Based Secure Communication Protocol

In this part, a secure communication protocol based on CKKS is crafted to protect parameters in the federated learning process [23]. The CKKS scheme achieves homomorphic encryption on approximate numbers, which makes the scheme extremely efficient. Compared with the traditional Paillier [24] and BFV [25], CKKS has a faster operation speed, which is very beneficial for improving the training efficiency [26].

CKKS is based on hardness assumptions of Ring Learning with Errors (RLWE). Given a ring $\mathcal{R} = \mathbb{Z}[X]/\left(X^N+1\right)$ in which N is a power of two. We define $\mathcal{R}_q = \mathrm{R}/q\mathcal{R}$ for the residue ring of $\mathcal{R}$ modulo an integer q. RLWE assumption is that, given polynomials of the form $(a, b = s\cdot a + e) \in \mathcal{R}_q^2$, the term b is computationally indistinguishable from uniformly random elements of $\mathcal{R}_q$ when a is chosen uniformly at random from $\mathcal{R}_q$, s is chosen from the error distribution over $\mathcal{R}$, e is drawn from the error distribution over $\mathcal{R}$. For a real $\sigma > 0$, $\mathcal{DG}\left(\sigma^2\right)$ samples a vector in $\mathbb{Z}^N$, whose coecient are drawn independently from the discrete Gaussian distribution of variance σ^2. $\mathcal{HWT}(h)$ is the set of signed binary vectors in $\{0, \pm 1\}^N$ with Hamming weight h.

The secure communication protocol consists of the following four functions:

1) KeyGenerate()*:* Given the security parameter λ, TA first samples $s \leftarrow \mathcal{HWT}(h)$, $a \leftarrow \mathcal{R}$ and $e \leftarrow \mathcal{DG}\left(\sigma^2\right)$, and then sets the secret key as $sk \longleftarrow (1, s)$, and the corresponding public key $pk \leftarrow (b, a) \in \mathcal{R}$ where $b \leftarrow -as + e(modN)$. After that, TA distributes the key pairs to each charging pile $C_{(k,i)}$.

2) ParaEncrypt()*:* Upon sampling $v_{(k,i)} \leftarrow \mathcal{R}$ and $e_{(k,i)}^0, e_{(k,i)}^1 \leftarrow \mathcal{DG}\left(\sigma^2\right)$, the charging pile $C_{(k,i)}$ encrypts its local model parameter $W_{(k,i)}^l$ with pk as

$$\begin{aligned} E(W_{(k,i)}^l) &= v_{(k,i)}\cdot pk + \left(W_{(k,i)}^l + e_{(k,i)}^0, e_{(k,1)}^1\right) \bmod N \\ &= \left(c_{(k,i)}^0, c_{(k,i)}^1\right). \end{aligned} \tag{10}$$

3) ParaAggregate()*:* After receiving contribution ratios $\left\{\alpha_{(k,1)}, \alpha_{(k,2)}, \cdots, \alpha_{(k,N_k)}\right\}$ of all charging piles in cluster, the fog node will aggregate the ciphertext information of N_k charging piles. The ciphertext part $E(W_{(k,1)}^l), E(W_{(k,2)}^l), \cdots, E(W_{(k,N_k)}^l)$ is aggregated as follows:

$$\begin{aligned} M_k &= \sum_{i=1}^{N_k}\left(\alpha_{(k,i)}\cdot E(W_{(k,i)}^l)\right) \\ &= \left(\sum_{i=1}^{N_k}(\alpha_{(k,i)}\cdot c_{(k,i)}^0), \sum_{i=1}^{N_k}(\alpha_{(k,i)}\cdot c_{(k,i)}^1)\right) \bmod N \\ &= \left(c_k^0, c_k^1\right), \end{aligned} \tag{11}$$

where

$$\begin{aligned} c_k^0 &= \sum_{i=1}^{N_k}\left[\alpha_{(k,i)}\cdot W_{(k,i)}^l + \alpha_{(k,i)}\cdot\left(e_{(k,i)}^0 + v_{(k,i)}\cdot b\right)\right], \\ c_k^1 &= \sum_{i=1}^{N_k}\left[\alpha_{(k,i)}\cdot\left(e_{(k,i)}^1 + v_{(k,i)}\cdot a\right)\right]. \end{aligned} \tag{12}$$

Assume that the sample size of each charging pile $n = \left\{n_{(k,1)}, n_{(k,2)}..., n_{(k,N_k)}\right\}$. After the aggregation is complete, the fog node J_k sends $\{M_k, T_s', n\}$ to the blockchain. The committee verifies it and aggregates the data from each fog node for the second time in the same principle, i.e., $M = (c_0, c_1)$. Then the local model update ciphertext of all N_C charging piles is obtained and stored in the global model update block of the blockchain.

4) ParaDecrypt()*:* After downloading the global model update ciphertext M from the blockchain, each fog node distributes M to the charging pile inside the cluster. The charging pile $C_{(k,i)}$ decrypts the ciphertext using its sk:

$$\begin{aligned} D(M) &= M\cdot sk = c_0 + c_1\cdot s \bmod N \\ &= \sum_{k=1}^{K}\sum_{i=1}^{N_k}\left(\alpha_{(k,i)}\cdot W_{B(k,i)}^l\right). \end{aligned} \tag{13}$$

Thus, we obtain global parameters aggregated from N_C charging piles. Finally, according to the update, each charging pile locally calculates a new global model and start the next round of training. In the whole process, the information of parameters is transmitted in the form of ciphertext on the communication link, ensuring the attacker cannot obtain useful information when eavesdropping on the communication link.

V. Simulation and Analysis

In this section, we conduct extensive experiments to evaluate the performance of our proposed scheme. First, we give the experiment settings. Then, we compare the accuracy of the energy demands prediction model with state-of-art studies, including Saputra *et al.* [2] and Tun *et al.* [27], and compare the computational costs of the secure communication protocol with typical Paillier [24] and BFV [25] based ones.

A. Experiment Settings

The experiments are conducted on a laptop computer with an Intel Core i5-7400@3.00GHz processor and 8GB memory. The operating system is 64-bit Windows 10. The CNN-BiLSTM-Attention-based energy demands prediction model is realized by Keras[1].

The two datasets used are the real-world dataset named Electric Vehicle Charging Sessions Dundee[2] and ACN [28]. Dundee dataset includes 67,112 pieces of data from 67 charging piles in Dundee, UK from 2017 to 2018, and each consumption is recorded as one piece of data, including charging pile ID, charging pile location, charging date, charging start and end time, energy consumption, transaction ID, charging method, and other information. The first five types of data are selected as the characteristics of the model training, and the energy consumption is used as the label for training. ACN dataset includes 66,748 pieces of data from 114 charging piles in California from 2018 to 2021. The selection of characteristics is the same as in Dundee.

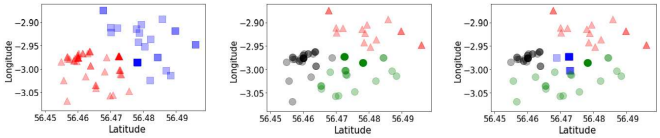
In the data preprocessing stage, we first split each charging record into its energy consumption in each hour period and delete the data whose energy field value is less than or equal to 0. Subsequently, 1% outliers were removed by DBSCAN clustering. Then we replace the original specific date and time with months $(1, 2, ..., 12)$, days $(1, 2, ..., 31)$, days of the week $(1, 2, ..., 7)$ and hours $(0, 1, ..., 23)$. The character string is encoded and all features are normalized. In the pile level prediction aspect, the output of the model is a prediction of a piece of electricity consumption data of a charging pile in the next hour. In the cluster level prediction aspect, output the total electricity consumption in the cluster in the next 24 hours.

B. Performance Comparison on Accuracy of Energy Demands Prediction Models

In this subsection, we first take the Dundee dataset as an example to show the clustering results under various K values (see Fig. 4). In the subsequent experiments, we set $K = 3$ unless otherwise specified. Then, we show the numerical results about the performance of the energy demands prediction models in two aspects, namely pile level and cluster level. Table I exhibits the energy demands prediction performance of the Dundee dataset and the ACN dataset in terms of the mean absolute error (MAE), root mean square error (RMSE), and symmetric mean absolute percentage error (SMAPE). It can be easily seen that, the proposed energy prediction model outperforms other models on most metrics at pile level, while it outperforms other models on all metrics at cluster level. On Dundee dataset, we can obtain an MAE, RMSE and SMAPE of 0.69, 1.27, and 39.95%, respectively, when aspect is pile, and 64.64, 78.36 and 16.53% when aspect is cluster. While on ACN dataset, we can obtain an MAE, RMSE and SMAPE of 0.61, 1.42 and 33.90% when aspect is pile, and 77.09, 100.81 and 44.69% when aspect is cluster.

[1]https://keras.io/

[2]https://data.dundeecity.gov.uk/dataset/ev-charging-data



(a) $K = 2$ (b) $K = 3$ (c) $K = 4$

Fig. 4. The clustering results of charging piles under various *K* values.

TABLE I
NUMERICAL RESULTS OF THE ENERGY DEMANDS PREDICTION MODEL OF DIFFERENT CLUSTERS IN TWO DATA SETS AND TWO PREDICTION ASPECTS

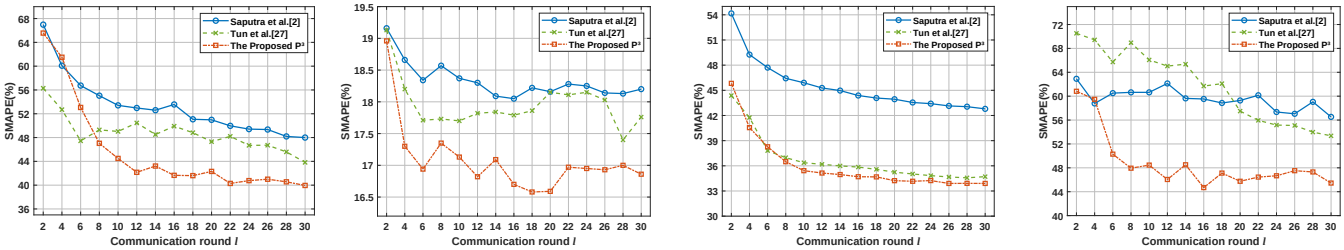
Dataset	Aspect	Cluster	Saputra *et al.* [2]			Tun *et al.* [27]			The proposed P^3		
			MAE	***RMSE***	***SMAPE***	***MAE***	***RMSE***	***SMAPE***	***MAE***	***RMSE***	***SMAPE***
Dundee	Pile level	1	**0.89**	**1.37**	42.92%	0.90	1.39	40.44%	0.90	1.38	**38.57%**
		2	0.59	**1.22**	54.37%	0.59	1.32	47.83%	**0.57**	1.27	**43.20%**
		3	0.73	1.17	38.51%	0.74	1.18	38.05%	**0.73**	**1.16**	**33.74%**
		Avg	0.70	**1.25**	48.00%	0.70	1.30	43.82%	**0.69**	1.27	**39.95%**
	Cluster level	1	63.66	75.95	17.72%	66.61	75.05	18.56%	**60.41**	**71.65**	**16.86%**
		2	67.88	84.92	19.23%	60.37	80.68	17.11%	**56.73**	**75.25**	**16.19%**
		3	81.32	95.74	17.52%	77.12	94.56	16.60%	**76.84**	**88.20**	**16.55%**
		Avg	70.94	85.53	18.16%	68.01	83.42	17.40%	**64.64**	**78.36**	**16.53%**
ACN	Pile level	1	0.72	1.33	47.01%	0.67	**1.30**	38.71%	**0.66**	1.32	**38.42%**
		2	0.79	1.60	40.16%	0.59	**1.49**	31.73%	**0.58**	1.51	**30.75%**
		3	0.58	1.07	27.99%	0.57	**1.03**	25.60%	**0.56**	1.06	**25.12%**
		Avg	0.76	1.47	42.79%	0.62	**1.40**	34.57%	**0.61**	1.42	**33.90%**
	Cluster level	1	93.98	120.56	43.19%	86.20	109.56	38.57%	**84.04**	**106.52**	**35.47%**
		2	195.63	229.96	68.68%	180.74	212.32	65.23%	**148.03**	**178.34**	**46.66%**
		3	14.05	18.67	60.51%	14.21	18.06	60.03%	**13.76**	**17.58**	**56.37%**
		Avg	109.43	133.17	56.53%	101.16	122.47	53.36%	**77.09**	**100.81**	**44.69%**

Figure 5 presents the result of SMAPE of all considered energy demands prediction models with varying communication rounds on different dataset. It is clear that as the number of communication rounds increases, the error of our model can decrease relatively quickly and the model gradually converges. In the end, it has generally the best performance over others.

In addition to the above experiments, we also carry out experiments to evaluate the performance of each locally built energy demands prediction model using limited data resources as well as the performance of the model built by traditional FedAvg. Figure 6 and Fig. 7 visually show the numerical results of all three metrics under the abovementioned local, FedAvg, and the proposed energy demands prediction models, taking the ACN dataset as an example. We can see that all local energy demands prediction models perform unsatisfactorily compared with the FedAvg model, while the performance of the models involved in P^3 is further optimized.

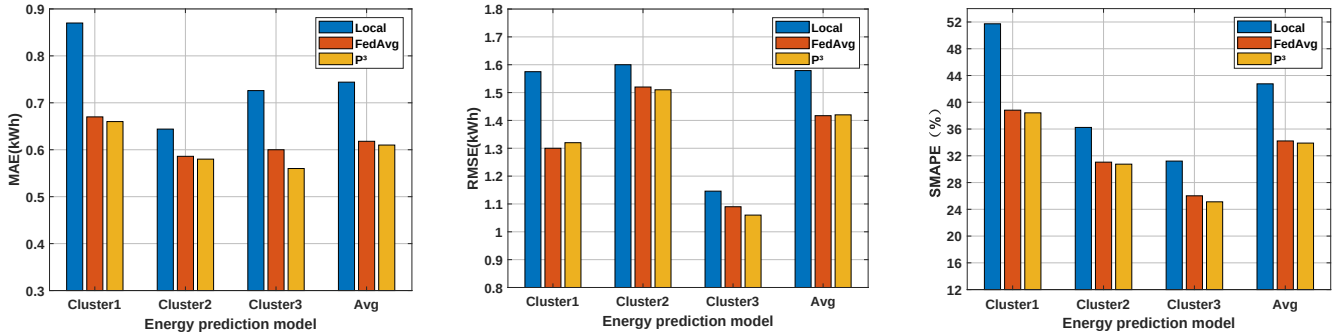
C. Performance Comparison on Communication Overheads of Federated Learning Framework

In this subsection, we compare the communication overhead between blockchain-based hierarchical personalized federated learning framework and traditional federated learning frameworks [2], [27]. Suppose a total of 114 charging piles are



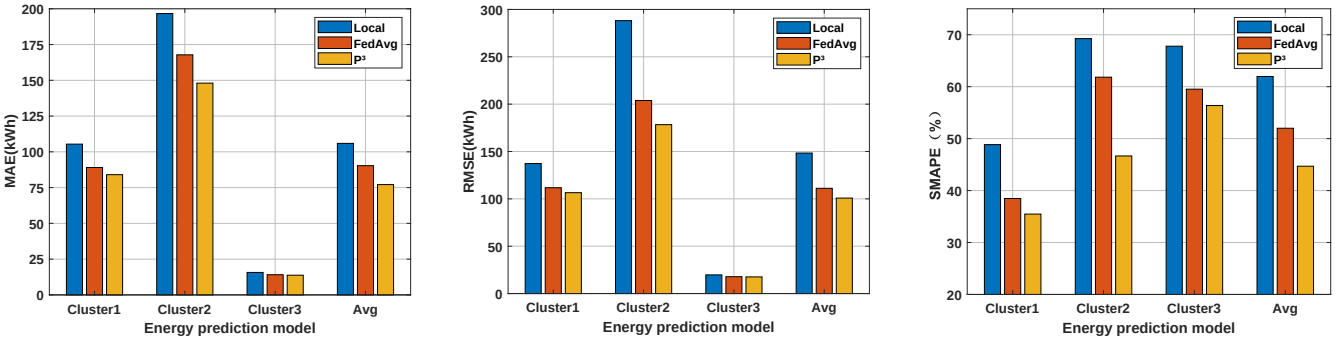
(a) Dundee-pile level (b) Dundee-cluster level (c) ACN-pile level (d) ACN-cluster level

Fig. 5. Comparison of SMAPE of different models at the cluster level in ACN and Dundee datasets.



(a) MAE (b) RMSE (c) SMAPE

Fig. 6. Performance comparison of the local, FedAvg, and the proposed energy prediction models at the pile level on ACN dataset.



(a) MAE (b) RMSE (c) SMAPE

Fig. 7. Performance comparison of the local, FedAvg, and the proposed energy prediction models at the cluster level on ACN dataset.

divided into 3 clusters. The CNN-BiLSTM-Attention model has a total of $66,627$ parameters and the precision is 32 bits, so the local update size of each charging pile is $66627 \times 32/\left(8 \times 10^6\right) \approx 0.267MB$. Figure 8 shows the comparison of the specific communication overhead per round. The blockchain-based hierarchical federated learning framework replaces the central server with fog nodes, which makes the load no longer excessively concentrated on the central server and makes the network architecture have better scalability. The communication overhead of the charging pile remains unchanged, and the fog node reduces the communication overhead by 64.1% compared with the central server.

D. Performance Comparison on Computational Costs of Secure Communication Protocols

In the proposed P^3 scheme, we use the CKKS cryptosystem to encrypt the model parameters. In this subsection, we analyze the computational costs in terms of the message encryption, decryption, and addition in P^3 scheme, compared with other homomorphic encryption based schemes, such as Paillier [24] and BFV [25]. Batch encryption is used for each homomorphic encryption scheme to optimize the computational speed in simulation experiments. The calculation cost of ciphertext operation with different size model parameters is shown in Table II. As we can see, the computation time of encryption operation increases linearly with the number of parameters of the model. For encryption and decryption operations, the computational costs of our P^3 scheme are significantly lower

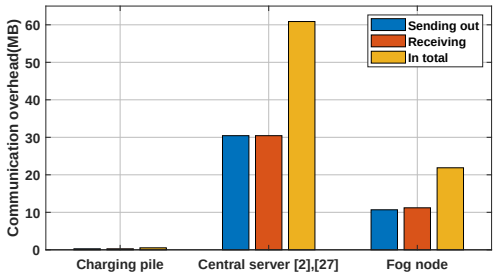


Fig. 8. Comparison of communication overheads per round.

TABLE II
COMPUTATIONAL COSTS OF PAILLIER, BFV AND CKKS

Operation	HE Method	Number of Model Parameters		
		10000	20000	40000
Encryption Time (s)	Paillier	1.21	2.32	4.53
	BFV	0.61	0.82	1.31
	CKKS	**0.02**	**0.03**	**0.07**
Decryption Time (s)	Paillier	0.72	1.32	2.53
	BFV	0.61	0.82	1.32
	CKKS	**0.01**	**0.02**	**0.04**
Addition Time (s)	Paillier	0.05	0.10	0.19
	BFV	**0.02**	**0.03**	**0.05**
	CKKS	0.04	0.08	0.13

than the other schemes. Even if the P^3 scheme is slightly slower than the BFV scheme in ciphertext addition, this deficiency is reasonably acceptable, thanks to its superior encryption and decryption speed.

VI. CONCLUSION

In this paper, we have proposed a blockchain-based federated deep learning scheme, named P^3, for privacy-preserving energy demands prediction in EV charging networks. First, we designed an energy demands prediction model based on CNN-BiLSTM-Attention, which enables charging piles to predict future electricity consumption accurately. In addition, we developed a novel blockchain-based hierarchical and personalized federated learning framework with a consensus committee to allow charging piles to collectively establish a comprehensive energy demands prediction model in a low-latency and privacy-preserving way. Further, a secure communication protocol based on the CKKS cryptosystem was crafted, which can not only ensure the confidentiality of the model parameters during model training, but also ensure that the charging pile is a legitimate participant in federated learning. Extensive experiments on two real-world EV charging datasets demonstrated the effectiveness of the proposed P^3 scheme as well as the superiorities over state-of-the-art schemes, in terms of the prediction accuracy and computational costs.

REFERENCES

[1] T. Harighi, R. Bayindir, S. Padmanaban, L. Mihet-Popa, and E. Hossain, "An overview of energy scenarios, storage systems and the infrastructure for vehicle-to-grid technology," *Energies*, vol. 11, no. 8, Aug. 2018.

[2] 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 *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Waikoloa, HI, USA, Dec. 9-13, 2019.

[3] A. Fukushima, T. Yano, S. Imahara, H. Aisu, Y. Shimokawa, and Y. Shibata, "Prediction of energy consumption for new electric vehicle models by machine learning," *IET Intelligent Transport Systems*, vol. 12, pp. 1174–1180, Aug. 2018.

[4] L. C. N. D. H. Meiqin Mao, Shengliang Zhang, "Schedulable capacity forecasting for electric vehicles based on big data analysis," *Journal of Modern Power Systems and Clean Energy*, vol. 7, pp. 1651–1662, Nov. 2019.

[5] Q. Yang, J. Li, W. Cao, S. Li, J. Lin, D. Huo, and H. He, "An improved vehicle to the grid method with battery longevity management in a microgrid application," *Energy*, vol. 198, p. 117374, May. 2020.

[6] R. Shipman, R. Roberts, J. Waldron, S. Naylor, J. Pinchin, L. Rodrigues, and M. Gillott, "We got the power: Predicting available capacity for vehicle-to-grid services using a deep recurrent neural network," *Energy*, vol. 221, p. 119813, Apr. 2021.

[7] L. F. Roman, P. R. Gondim, and J. Lloret, "Pairing-based authentication protocol for v2g networks in smart grid," *Ad Hoc Networks*, vol. 90, p. 101745, July. 2019.

[8] L. T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-preserving deep learning via additively homomorphic encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 1333–1345, May. 2018.

[9] V. Álvarez, S. Mazuelas, and J. A. Lozano, "Probabilistic load forecasting based on adaptive online learning," *IEEE Transactions on Power Systems*, vol. 36, pp. 3668–3680, July. 2021.

[10] H. Li, G. Dán, and K. Nahrstedt, "Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging," *IEEE Transactions on Smart Grid*, vol. 8, pp. 2305–2313, Sept. 2016.

[11] Y. Li, P. Zhang, and Y. Wang, "The location privacy protection of electric vehicles with differential privacy in V2G networks," *Energies*, vol. 11, pp. 1–17, Oct. 2018.

[12] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science-Research and Development*, vol. 33, pp. 71–79, Feb. 2018.

[13] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Network*, vol. 32, pp. 184–192, Nov./Dec. 2018.

[14] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Transactions on Industrial Informatics*, vol. 16, pp. 4146–4155, June. 2020.

[15] M. Baza, A. Sherif, M. M. Mahmoud, S. Bakiras, W. Alasmary, M. Abdallah, and X. Lin, "Privacy-preserving blockchain-based energy trading schemes for electric vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, pp. 9369–9384, Sept. 2021.

[16] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Federated learning for data privacy preservation in vehicular cyber-physical systems," *IEEE Network*, vol. 34, pp. 50–56, May./June. 2020.

[17] Z. Du, C. Wu, T. Yoshinaga, K.-L. A. Yau, Y. Ji, and J. Li, "Federated learning for vehicular internet of things: Recent advances and open issues," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 45–61, May. 2020.

[18] S. R. Pokhrel and J. Choi, "Improving tcp performance over wifi for internet of vehicles: A federated learning approach," *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 6798–6802, June. 2020.

[19] X. Huang, P. Li, R. Yu, Y. Wu, K. Xie, and S. Xie, "Fedparking: A federated learning based parking space estimation with parked vehicle assisted edge computing," *IEEE Transactions on Vehicular Technology*, vol. 70, pp. 9355–9368, Sept. 2021.

[20] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, pp. 3975–3986, July. 2021.

[21] J.-H. Chen, M.-R. Chen, G.-Q. Zeng, and J.-S. Weng, "BDFL: A byzantine-fault-tolerance decentralized federated learning method for autonomous vehicle," *IEEE Transactions on Vehicular Technology*, vol. 70, pp. 8639–8652, Sept. 2021.

[22] Q. Kong, F. Yin, R. Lu, B. Li, X. Wang, S. Cui, and P. Zhang, "Privacy-preserving aggregation for federated learning-based navigation in vehicular fog," *IEEE Transactions on Industrial Informatics*, vol. 17, pp. 8453–8463, Dec. 2021.

[23] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in *Advances in Cryptology ASIACRYPT 2017*, pp. 409–437, Springer, Hong Kong, China, Dec. 3-7, 2017.

[24] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology EUROCRYPT 1999*, pp. 223–238, Springer, Czech Republic, May. 26, 1999.

[25] Z. Brakerski, "Fully homomorphic encryption without modulus switching from classical gapsvp," in *Advances in Cryptology CRYPTO 2012*, pp. 868–886, Springer, Santa Barbara, CA, USA, Aug. 19-23, 2012.

[26] A. Viand, P. Jattke, and A. Hithnawi, "Sok: Fully homomorphic encryption compilers," in *2021 IEEE Symposium on Security and Privacy (SP)*, pp. 1092–1108, May. 2021.

[27] Y. L. Tun, K. Thar, C. M. Thwal, and C. S. Hong, "Federated learning based energy demand prediction with clustered aggregation," in *2021 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 164–167, Jeju Island, Korea (South), Jan. 17-20, 2021.

[28] Z. J. Lee, T. Li, and S. H. Low, "Acn-data: Analysis and applications of an open ev charging dataset," in *Proceedings of the Tenth ACM International Conference on Future Energy Systems*, e-Energy '19, (New York, NY, USA), pp. 139–149, Association for Computing Machinery, June. 2019.

Beibei Li received the B.E. degree (awarded Outstanding Graduate) in communication engineering from Beijing University of Posts and Telecommunications, P.R. China, in 2014 and the Ph.D. degree (awarded Full Research Scholarship) from the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2019.

He is currently an associate professor (doctoral advisor) with the School of Cyber Science and Engineering, Sichuan University, P.R. China. He was invited as a visiting researcher at the Faculty of Computer Science, University of New Brunswick, Canada, from March to August 2018, and also the College of Control Science and Engineering, Zhejiang University, P.R. China, from February to April 2019.

His current research interests include several areas in security and privacy issues on cyber-physical systems, with a focus on intrusion detection techniques, artificial intelligence, and applied cryptography. He has authored or co-authored works in IEEE Transactions on Information Forensics and Security, IEEE Transactions on Industrial Informatics, IEEE Transactions on Power Systems, IEEE Transactions on Neural Networks and Learning Systems, IEEE Transactions on Network and Service Management, ACM Transactions on Cyber-Physical Systems, etc. He won the Best Paper Award in IEEE ISCC 2021. Dr. Li is serving or has served as a Publicity Chair, Publication Co-Chair, Track Chair, or a TPC member for several international conferences, including The AAAI Conference on Artificial Intelligence (AAAI), IEEE International Conference on Communications (ICC), IEEE Global Communications Conference (GLOBECOM), IEEE International Conference on Computing, Networking and Communications (ICNC), and The Annual International Conference on Privacy, Security & Trust (PST).

Yuqing Guo is currently working toward the MA.Eng degree in cybersecurity with the School of Cyber Science and Engineering, Sichuan University, P.R. China. She has co-authored works in 2022 IEEE INFOCOM Workshop and 2022 Chinese Control Conference.

Her current research interests include intrusion detection, smart grids security, and artificial intelligence.

Qingyun Du is currently pursuing her master's degree in cybersecurity with the School of Cyber Science and Engineering, Sichuan University, Chengdu, P.R. China.

She has authored or coauthored works in IEEE Transactions on Industrial Informatics, 2021 International Conference on Service-Oriented Computing, and 2022 Chinese Control Conference. Her current research interests include cyberphysical system security, artificial intelligence, and applied cryptography.

Ziqing Zhu is currently working toward the MA.Eng degree in cybersecurity with the School of Cyber Science and Engineering, Sichuan University, P.R. China. She received the B.E. degree in information and computing science from Hunan University, Changsha, P.R. China.

Her current research interests include data security and privacy protection.

Xiaohui Li (Member, IEEE) received the B.S. and Ph.D. degrees in computer science from the College of Computer Science, Sichuan University, Chengdu, China, in 2012 and 2017, respectively. She is currently a teacher with the School of Cyber Science and Engineering, Sichuan University, Chengdu, China. Her research interests cover several areas in network and information security (e.g., wireless networks, satellite networks, internet of thing, cyber threat intelligence, etc.), with emphasis on design of efficient transport protocols, routing protocols, and intelligence analysis.

Rongxing Lu (Fellow, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2012. He is currently a Mastercard IoT Research Chair, a University Research Scholar, and an Associate Professor with the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Canada. Before that, he worked as an Assistant Professor at the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore, from April 2013 to August 2016. He worked as a Post-Doctoral Fellow at the University of Waterloo from May 2012 to April 2013. His research interests include applied cryptography, privacy enhancing technologies, and the IoT-big data security and privacy. He has published extensively in his areas of expertise. He was awarded the most prestigious "Governor General's Gold Medal" for his Ph.D. degree. He won the 8th IEEE Communications Society (ComSoc) AsiaPacific (AP) Outstanding Young Researcher Award in 2013. He was a recipient of nine best (student) paper awards from some reputable journals and conferences. He is the Winner of the 20162017 Excellence in Teaching Award, FCS, UNB. Currently, he serves as the Chair for IEEE Communications and Information Security Technical Committee (IEEE ComSoc CIS-TC) and the Founding Co-Chair for IEEE TEMS Blockchain and Distributed Ledgers Technologies Technical Committee (BDLT-TC).