Incentivizing Differentially Private Federated Learning: A Multidimensional Contract Approach

Maoqiang Wu, *Graduate Student Member, IEEE*, Dongdong Ye,
Jiahao Ding, *Graduate Student Member, IEEE*, Yuanxiong Guo, *Member, IEEE*,
Rong Yu, *Member, IEEE*, and Miao Pan, *Senior Member, IEEE*

***Abstract*—Federated learning is a promising tool in the Internet-of-Things (IoT) domain for training a machine learning model in a decentralized manner. Specifically, the data owners (e.g., IoT device consumers) keep their raw data and only share their local computation results to train the global model of the model owner (e.g., an IoT service provider). When executing the federated learning task, the data owners contribute their computation and communication resources. In this situation, the data owners have to face privacy issues where attackers may infer data property or recover the raw data based on the shared information. Considering these disadvantages, the data owners will be reluctant to use their data to participate in federated learning without a well-designed incentive mechanism. In this article, we deliberately design an incentive mechanism jointly considering the task expenditure and privacy issue of federated learning. Based on a differentially private federated learning (DPFL) framework that can prevent the privacy leakage of the data owners, we model the contribution as well as the computation, communication, and privacy costs of each data owner. The three types of costs are data owners' private information unknown to the model owner, which thus forms an information asymmetry. To maximize the utility of the model owner under such information asymmetry, we leverage a 3-D contract approach to design the incentive mechanism. The simulation results validate the effectiveness of the proposed incentive mechanism with the DPFL framework compared to other baseline mechanisms.**

***Index Terms*—Differential privacy, federated learning, multidimensional contract, incentive mechanism.**

I. Introduction

With the growing popularity of artificial intelligence (AI) in the Internet-of-Things (IoT) area, the AI-based IoT applications are gradually employed in all aspects of our daily life, such as transportation [1], [2]. The AI-based IoT applications generate a large amount of data that feeds into the AI system for continuous learning. Specifically, the model owner (e.g., an IoT service provider) periodically gathers the data from the mobile devices of the data owners (e.g., IoT service consumers) and trains the model over the collected data in centralized servers. However, the collected data usually contains the data owners' private information (e.g., service usage patterns) or profile information (e.g., gender and age). If the model owner is untrustworthy or the centralized servers are invaded by attackers, the data owners' data will be abused or stolen, causing the economical loss to the data owners.

To alleviate the privacy risk, federated learning is proposed as a promising distributed learning scheme. Data owners train the local models over their private data and only upload the local computation results instead of uploading their raw data to the model owner. The model owner aggregates all the local computation results to improve its global model. Under this setting, the data owners can control their raw data while the model owner can obtain a global model with good performance. Since inception by Google [3], federated learning has drawn great attention in IoT area [4]–[7].

Although in federated learning the data owners do not share their raw data, they still face the risk of privacy leakage. For example, based on the computation results from a data owner, attackers can infer whether a sample is in the data owner's data set by using membership inference attacks [8], or recover the data owner's raw data by construction attacks [9]. The attackers may be an untrustworthy model owner in the system or an eavesdropper in the communication network. There also exits the case that a malicious data owner can infer the feature distributions or data property of a specified data owner according to the global model downloaded from the model owner [10], [11]. Considering such risks, the data owners will be reluctant to participate in federated learning. The low participation rate of the data owners will lead to the poor performance of the trained global model.

Federated learning has to consider incentivizing the data owners to join the learning process. When data owners execute the federated learning tasks, their devices

Manuscript received October 13, 2020; revised November 30, 2020; accepted December 23, 2020. Date of publication January 8, 2021; date of current version June 23, 2021. The work of Maoqiang Wu, Dongdong Ye,and Rong Yu was supported in part by the National Key Research and Development Program of China under Grant 2020YFB1807802; in part by the National Natural Science Foundation of China under Grant 61971148; in part by the Guangxi Natural Science Foundation, China, under Grant 2018GXNSFDA281013; in part by the Foundation for Science and Technology Project of Guilin City under Grant 20190214-3; and in part by the Natural Science Foundation of Guangdong Province under Grant 2018A030313306. The work of Jiahao Ding and Miao Pan was supported in part by the U.S. National Science Foundation under Grant U.S. CNS-1646607, Grant CNS-1801925, and Grant CNS-2029569. The work of Yuanxiong Guo was supported in part by the National Science Foundation under Grant CNS-2029685. *(Corresponding author: Rong Yu.)*

Maoqiang Wu, Dongdong Ye, and Rong Yu are with the School of Automation, Guangdong University of Technology, Guangzhou 510006, China (e-mail: maoqiang.wu@vip.163.com; dongdongye8@163.com; yurong@ieee.org).

Jiahao Ding and Miao Pan are with the Electrical and Computer Engineering Department, University of Houston, Houston, TX 77004 USA (e-mail: jding7@uh.edu; mpan2@uh.edu).

Yuanxiong Guo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: yuanxiong.guo@utsa.edu).

Digital Object Identifier 10.1109/JIOT.2021.3050163

consistently consume computation and communication resources. Also, the data owners still worry about the data privacy issue. Without a well-designed economic incentive, the self-interested data owners are not willing to take part in federated learning. There are three main difficulties in designing a practical incentive mechanism for federated learning. First, it is hard to evaluate the contribution of data owners to the performance of the trained models. Without accurate evaluation of the contribution, the model owner cannot correctly reward the data owners, leading to financial loss or low participant rate [12]. Second, it is difficult to model the multidimensional cost of data owners. The recent incentive mechanism mainly modeled the cost of the data owners as their computation and communication expenditures but ignored their privacy risk which is also an important cost [12]–[14]. Third, there exists multidimensional information asymmetry since the self-interested data owners prefer to hide their multiple types of costs to gain more benefits. The multidimensional information asymmetry complicates the incentive design [15], [16].

In this article, we aim to eliminate the obstacles that hinder data owners from participating in federated learning, such as privacy issues and naive incentives. We first analyze a differentially private federated learning (DPFL) framework that injects artificial Gaussian noise to the local model for alleviating the privacy issue. Based on the DPFL framework, we then proposed a 3-D contract-based incentive mechanism by considering the information asymmetry and the heterogeneous types of costs. The simulation results validate the efficiency of the designed incentive mechanism with the DPFL framework compared to other incentive mechanisms. In summary, the main contributions of this article are as follows.

1) We design an incentive mechanism in a DPFL framework that is able to prevent privacy leakage in federated learning. To the best of our knowledge, we are the first to study the incentive mechanism jointly considering the task expenditure and privacy issue of federated learning.
2) By theoretical analysis and experimental evaluation of the DPFL framework, we model the data owners' contribution and heterogeneous costs consisting of computation, communication, and privacy cost. These physical models essentially support the design of the incentive mechanism.
3) Considering the information asymmetry between the model owner and the data owners, we design the incentive mechanism by using a 3-D contract, where the model owner provides the contract items specifying the training data size and offering corresponding rewards according to different cost types of data owners.

The remainder of this article is organized as follows. Section II introduces the related works of the privacy concerns and incentive mechanisms of federated learning. Section III describes the established DPFL framework and related analysis. Section IV describes the system model based on the DPFL framework. Section V provides a detailed description of multidimensional contract design problem and solution. The simulation results and performance evaluation are shown in Section VI. Finally, the conclusion remarks are made in Section VII.

II. Related Works

A. *Privacy Concerns in Federated Learning*

Despite the data owners do not share private data during the federated learning process, they still face privacy issues. The shared computation results of the data owners may be used by attackers for inferring the data owners' private information [8] or reconstruct the raw data [9]. The downloaded global model may be used by attackers for inferring the feature distribution or property of a specified data owner [10], [11].

To address the privacy issue, there emerge many studies focused on designing defense methods. Among them, homomorphic encryption and secure multiparty computation are popular methods defending against the attacks which are based on the shared local computation results [17]. But these methods are only applicable to simple tasks and cannot defend against the attacks which are based on the global model. DP provides a practical privacy analysis and is widely adopted in big data privacy-preserving systems [18]–[21] and private distributed learning systems [17], [22]–[24]. The DP-based distributed learning schemes offer a comprehensive defense against the aforementioned attacks. However, most of these studies made an optimistic assumption that the data owners voluntarily join federated learning, which is not seldom seen in practice. To incentivize the data owners to join DP-protected federated learning, we propose a contract-based incentive mechanism based on the established DPFL framework.

B. *Incentive Mechanisms for Federated Learning*

In recent years, there is an increasing number of studies focused on designing incentive mechanisms for federated learning. There are two key issues to be addressed for designing the incentive mechanism. The first is evaluating the contribution of each data owner which affects the profit of the model owner. The works in [13], [14], and [25] modeled the contribution as the completion time of learning tasks. The works in [12], [16], [26], and [27] modeled the contribution as the trained model performance depending on the training data size. The second is modeling the costs of data owners. Most of the works (in [12]–[14], [16], [25], and [27]) modeled the cost as computation and communication expenditures. Hu and Gong [28] considered the privacy issue in FL and proposed a DP budget-based incentive mechanism. However, none of them modeled the contribution and cost of the data owners and designed the incentive mechanism by jointly considering the task expenditure and privacy issue of federated learning.

We are motivated to design the incentive mechanism for federated learning jointly considering these two factors. Based on the established DPFL framework that adopts the DP for preventing privacy leakage in the federated learning process, we model the data owners' contribution by evaluating the trained model performance and model their costs by analyzing task expenditure and privacy risk. In order to deal with the information asymmetry between the model owner and the data owners, we use a multidimensional contract approach to design the incentive mechanism in the DPFL framework. Compared with the traditional single-dimensional contracts, the multidimensional contract allows the principal (the model owner) to extract more detailed private information of agents (the data owners) and thus design the more precise contracts. Lim *et al.* [16] also adopted the multidimensional contract approach to incentivize the data owners. But they focused on the UAV-based scenarios and, moreover, did not consider the privacy issue, so our models are different and our mechanisms are not comparable.

III. Differentially Private Federated Learning

In this section, we first introduce the federated learning and the threat model. Then we describe the adopted DPFL framework against the threats. The privacy analysis and convergence analysis of the DPFL framework are also given.

A. Federated Learning and Threat Model

Consider a federated learning setting that consists of a model owner and I data owners. The data owner i has a local data set $\mathcal{D}_i = \{(x_i, y_i)\}$ including sample-label pairs (x_i, y_i) from its device. For a machine learning problem, we typically take $f_i(w) = (1/D_i) \sum \ell(x_i; y_i; w)$ as the objective, where $D_i = |\mathcal{D}_i|$ denotes the size of local data set and $\ell(x_i; y_i; w)$ is the loss of the prediction on the local data set with model parameters w. The goal of the model owner is to learn a model w from the data owners while they are allowed to keep their local data sets. Therefore, each data owner trains the model on their local data sets and the model owner aggregates the model parameters from the data owners. The objective can be expressed by $f(w) = \sum_{i=1}^{I} p_i f_i(w)$, where $p_i = [D_i/(\sum_{i=1}^{I} D_i)]$ denotes the weight of the local model from the data owner i.

We consider that the adversary can be the "honest-but-curious" model owner or the malicious data owner in the system as well as the eavesdropper in the communication network. The model owner would honestly execute federated training operation, but is curious about the data owners' private information and may recover their training data from the uploaded models or gradients [9]. Meanwhile, based on the downloaded global model, some malicious data owner could adopt the auxiliary data to infer the property of a target data owner [11], or use generative adversary network (GAN) to learn its feature distribution [10]. Besides, the uploaded and downloaded message may be eavesdropped during the transmission. The eavesdropper will also infer or reconstruct the data owner's private data based on the message but will not actively inject false messages or intervene in the message transmission. We consider that the data owners will transmit the correct computed results and the data pollution attacks by the malicious data owners are not considered in this article.

B. DPFL Framework

We aim to establish a federated learning framework that enables the data owners against the above threat model without sacrificing much accuracy of the trained model. (ϵ, δ)-DP provides a standard to measure privacy risk [29], where the parameter ϵ denotes the privacy budget (detailed definition please see Appendix A). The lower ϵ, the data owners have a lower risk of privacy leakage. Inspired by works [17], [22], we set up the DPFL framework where each data owner adds artificial Gaussian noise in the local model at each iteration for guaranteeing (ϵ, δ)-DP of its local data. The overall process is summarized in Algorithm 1. Specifically, at round $0 \leq t \leq T-1$, each data owner i receives the global model w_t from the model owner and updates its local model $w_{t,0}^i = w_t$ (step 5). Each data owner splits its local data set $\mathcal{D}_i$ into batches β_i with batch size B (step 6). Thus, the expected local iteration number is $|\beta_i|E = (D_i/B)E$, where E is the local epoch number and $0 \leq s \leq |\beta_i|E$. At each local iteration, each data owner updates the local model $w_{t,s}^i$ by learning a batch of data $b_{i,s}$ (steps 9 and 10). Then the local model is added with the Gaussian noise $\mathcal{N}(0, \sigma_i^2 \mathbf{I_d})$ (steps 11 and 12), where σ_i is the Gaussian variance and d is the model dimension. At the end of each round, each data owner sends its local model to the model owner (step 15) and the model owner performs the weighted averaging to obtain new global model (steps 17 and 18).

Algorithm 1 DPFL Algorithm

```
Input: The $I$ data owners are indexd by $i$; $B$ is the local mini-batch size, $E$ is the number of local epochs; $\eta$ is the learning rate; $T$ is the communication rounds; $\sigma_i$ is the noise scale ; the local iteration is indexed by $0 \leq s \leq |\beta_i|E$
Output: Global model $w_T$
 1: initialize $w_0$
 2: for each round $t$ from 0 to $T-1$ do
 3:     The model owner sends $w_t$.
 4:     for all $I$ data owners in parallel do
 5:         Update the local parameters as $w_{t,0}^i = w_t$
 6:         $\beta_i \leftarrow$ split $\mathcal{D}_i$ into batches of size B
 7:         for each local epoch from 0 to $E-1$ do
 8:             for batch $b_i \in \beta_i$ do
 9:                 Update the local parameters as
10:                 $w_{t,s}^i \leftarrow w_{t,s-1}^i - \frac{\eta}{B} \nabla \ell(w_{t,s}^i; b_i)$
11:                 Add noise into local parameters
12:                 $w_{t,s}^i = w_{t,s}^i + \mathcal{N}(0, \sigma_i^2 \mathbf{I_d})$
13:             end for
14:         end for
15:         Send the local parameters $w_{t,|\beta_i|E}^i$ to the model owner
16:     end for
17:     The model owner aggregates the parameters
18:     $w_{t+1} \leftarrow \sum_{i=1}^{I} p_i w_{t,|\beta_i|E}^i$
19: end for
20: return $w_T$
```

C. Privacy Analysis

Now we analyze the DP guarantee of the established DPFL framework. We aim at using DP is to prevent the attackers from extracting sensitive information from the uploaded local models and the downloaded global model. The downloaded global model is the aggregation of the uploaded noisy local models at each round. Therefore, as long as the local models are differential private, the global model can also defend against privacy leakage. Instead of using DP directly, we use Renyi differential privacy (RDP) to tightly account for the privacy loss of the data owner and then convert it to a DP guarantee (detailed definition please see Appendix A). By using the RDP, we compute the overall privacy guarantee for a data owner after T rounds of training and give the (ϵ, δ)-DP guarantee in Theorem 1.

Theorem 1: For any $\delta \in (0, 1)$ and $\epsilon > 0$, Algorithm 1 satisfies (ϵ, δ)-DP when its injected Gaussian noise $\mathcal{N}(0, \sigma_i^2 \mathbf{I_d})$ is chosen to be

$$\sigma_i = \sqrt{\frac{14\alpha\eta^2 ET}{BD_i(\epsilon - \log(1/\delta)/(\alpha - 1))}} \tag{1}$$

given $\alpha - 1 \leq [(2\sigma_i^2)/3]\log([1/(\alpha\tau(1 + \delta^2))])$ with $\alpha = ([2\log(1/\delta)]/\epsilon) + 1$, and $\tau = (B/D_i)$.

Proof: See Appendix B. ■

Theorem 1 indicates that the added noise scale is inversion proportional to the local data size for guaranteeing the (ϵ, δ)-DP of local data. The reason is that the increasing data size reduces the sensitivity of the local model trained on the adjacent data sets.

D. Convergence Analysis

In this section, we analyze the convergence of the established DPFL framework under nonconvex objectives which are common in neuron networks. Similar with [17] and [30], we give the standard assumptions as follows.

Assumption 1 (Smoothness): $f_1, \ldots, f_I$ are all L-smooth: for all w and w', $f(w') \leq f(w) + (w' - w)^T \nabla f(w) + (L/2)\|w' - w\|$.

Assumption 2 (Unbiased Gradients): Let $b_{t,s}^i$ be the batch of data with batch size B sampled from $\mathcal{D}_i$ uniformly at random. The variance of stochastic gradients in each data owner is bounded: $\mathbb{E}\|\nabla f_i(w_{t,s}^i; b_{t,s}^i) - \nabla f_i(w_{t,s}^i)\| \leq (Q^2/B)$

Assumption 3 (Bounded Gradients): The expected squared norm of stochastic gradients is uniformly bounded, i.e., $\mathbb{E}\|\nabla f_i(w_{t,s}^i; b_{t,s}^i)\| \leq G^2$

For the sth local iteration at round t, we use $\overline{w}_{t,s}$ to denote an auxiliary parameter vector that follows a centralized gradient descent based on $\overline{w}_{t,s} = \sum_{i=1}^I p_i(w_{t,s}^i + n_{t,s}^i)$, which is the weighted average of local solution $w_{t,s}^i$ over all I data owners with weight $p_i = (D_i/D)$ and $n_{t,s}^i \sim \mathcal{N}(0, \sigma_i^2 \mathbf{I_d})$ is the Gaussian noise. It is immediate that

$$\begin{aligned}\overline{w}_{t,s} &= \overline{w}_{t,s-1} - \eta\sum_{i=1}^{I} p_i g_{t,s}^i + \sum_{i=1}^{I} p_i n_{t,s}^i \\ &= \overline{w}_{t,s-1} - \eta\sum_{i=1}^{I} p_i\left(g_{t,s}^i - \frac{n_{t,s}^i}{\eta}\right).\end{aligned} \tag{2}$$

Since each data owner in Algorithm 1 restarts its SGD with the same initial point $\overline{w}_t = w_t = w_t^i$ at the beginning of each round, deviation between each local solution $w_{t,s}^i$ and $\overline{w}_{t,s}$ are related to s with $1 \leq s \leq |\beta_i|E$. The following useful lemma gives the bound of the expected gap $\mathbb{E}[\|\overline{w}_{t,s} - w_{t,s}^i\|^2]$ after s local iterations at round t.

Lemma 1: For the sth iteration at round t, Algorithm 1 ensures

$$\mathbb{E}\left[\left\|\overline{w}_{t,s} - w_{t,s}^i\right\|^2\right] \leq H \tag{3}$$

where $H = s\eta^2 G^2 \sum_{i=1}^I p_i^2 + sd\sum_{i=1}^I p_i^2 \sigma_i^2 + s\eta^2 G^2 + sd\sigma_i^2$.

Proof: See Appendix C. ■

Lemma 1 indicates that the bound of the expected gap is related to the local iteration index s and the expected noise scale $d\sigma_i^2$.

Convergence Criteria: Since the objective function is nonconvex, like [17], [30], we use the expected gradient norm as an indicator of convergence. After $T - 1$ rounds and S local iterations at the Tth round, the algorithm reaches an expected suboptimal solution if

$$\frac{1}{K}\sum_{t=1}^{T-1}\sum_{s=1}^{S}\mathbb{E}\left[\left\|\nabla f\left(\overline{w}_{t,s-1}\right)\right\|^2\right] \leq \upsilon \tag{4}$$

where υ is arbitrarily small and $K = (T-1)|\beta|E+S$. This condition ensures that the algorithm can converge to a stationary point.

Theorem 2: If $0 \leq \eta \leq (1/L)$, after $T - 1$ rounds and S iterations at the Tth round, we have

$$\begin{aligned}\frac{1}{K}\sum_{t=1}^{T-1}\sum_{s=1}^{S}\mathbb{E}\left[\left\|\nabla f\left(\overline{w}_{t,s-1}\right)\right\|^2\right] &\leq \frac{2}{\eta K}\left(f\left(\overline{w}_{0,0}\right) - f^*\right) \\ &\quad + L^2\sum_{i=1}^{I} p_i^2 H + \frac{L\eta Q^2}{B}\sum_{i=1}^{I} p_i^2 \\ &\quad + L\eta d\sum_{i=1}^{I} p_i^2\sigma_i^2\end{aligned} \tag{5}$$

where f^* is the minimum value of $f(w)$ and $K = (T-1)|\beta|E + S$.

Proof: See Appendix D. ■

Theorem 2 indicates that the DPFL framework satisfies the convergence criteria and the noise magnitude will affect the convergence.

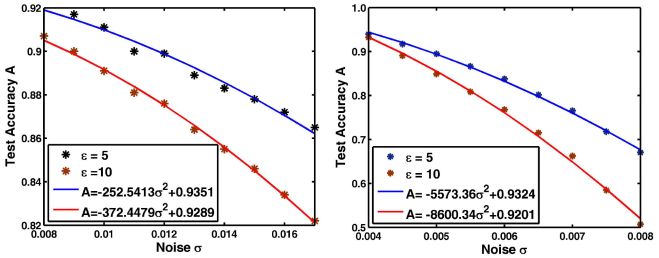
IV. Incentive Mechanism for DPFL

In this section, we consider the DPFL-incentive scenario. We give the models of the data owners' contribution and three-type costs, and provide the utility functions of the model owner and the data owners, respectively.

A. DPFL-Incentive Scenario

As aforementioned, the DPFL framework provides the privacy protection of the data owners and reaches convergence of Algorithm 1. We conduct experiments to measure the trained model performance with the DPFL framework over the MNIST data set and show the result in Fig. 1. We observe that with the same ϵ, the test accuracy of the trained model decreases with the growing noise scale under both independent and identically distributed (iid) and non-iid setting. Thus, we define a data owner's contribution as the expected trained model performance and fit the performance curve as

$$\begin{aligned}A &= -a\sigma_i^2 + b \\ &= -a\frac{14\alpha\eta^2 ET}{BD_i(\epsilon - \log(1/\delta)/(\alpha - 1))} + b\end{aligned} \tag{6}$$



(a) (b)

Fig. 1. Test accuracy with respect to noise scale under different privacy budget (under IID and non-IID setting). (a) MNIST IID. (b) MNIST NON-IID.

where a and b is system factors, and $\alpha = ([2\log(1/\delta)]/\epsilon) + 1$. Under this setting, we consider a DPFL-incentive scenario consisting of a model owner and I data owners. The model owner publishes DPFL tasks specifying the uniform privacy budget $\epsilon_{\min} \leq \epsilon \leq \epsilon_{\max}$. When $\epsilon < \epsilon_{\min}$, the added noise scale is too large so that the training cannot converge. When $\epsilon > \epsilon_{\max}$, the added noise scale is too small to perturb the model and thus cannot protect the data owner's privacy. The model owner also specifies required training data size D_i and corresponding reward R_i. Each data owner selects the data size by considering its computation cost, communication cost, and privacy cost. Then the data owners complete their tasks over private data of chosen size D_i and obtain reward R_i. In order to design the incentive mechanism matching R_i and D_i, we model the three-type costs and utilities of the model owner and data owners in next section.

B. Costs in DPFL

Privacy Cost: At each local iteration, each data owner adds Gaussian noise to perturb their local computation results, i.e., model parameters. According to (1), the noise magnitude σ_i depends on the DP budget $\epsilon \in (0, +\infty)$ which affects the level of privacy protection. With a smaller ϵ, the distribution difference of the local computation results from between the local data set D_i and adjacent data set $D_i^{'}$ becomes smaller, and the level of privacy protection is higher. In the extreme case where $\epsilon \to 0$, the attacker can not tell the difference of the computation results, and the highest privacy protection is achieved. Here, we define the privacy cost of a data owner as his economical loss from the potential privacy exposure, which is given as

$$l_i = \frac{\epsilon}{\epsilon_{\max}} v_i D_i \tag{7}$$

where v_i is the economical loss per unit data from privacy leakage and $\epsilon_{\max}$ is the constraint for the perturbation. When ϵ exceeds $\epsilon_{\max}$, the injected noise is too little to perturb the model result and is not able to protect the privacy of the data owners anymore.

Computation Cost: After downloading the initialized or aggregated global model from the model owner, each data owner carries out the local training. When the data owner i uses its local data of chosen size D_i for training, the total workload for local training is given as $W_i = N_F D_i E$, where N_F is the number of floating point operations (FLOPs) needed for processing each sample, and E is the number of local epochs set in Algorithm 1. The CPU clock frequency of device i is denoted as f_i^c, and thus the computing capability of device is $f_i = f_i^c n_i$, where n_i is the number of CPU FLOPs per cycle. The computation time of the data owner i for local training at each round is given as

$$t_i^{cp} = \frac{W_i}{f_i} = \frac{N_F E}{f_i^c n_i} D_i. \tag{8}$$

For a CMOS circuit [31], the power consumption of CPU can be given by $P_i^{cp} = \psi_i (f_i^c)^3$, where ψ_i is the coefficient [in Watt/(Cycle/s)^3] depending on the chip architecture. The computation energy consumption of the data owner i at each round can be given as

$$e_i^{cp} = P_i^{cp} t_i^{cp} = \frac{N_F E \psi_i f_i^{c2}}{n_i} D_i. \tag{9}$$

Communication Cost: At the end of each round, each data owner uploads the noisy local model to the model owner via wireless communication of frequency-division multiple access (FDMA). The bandwidth allocated for the data owner i is denoted as b_i in an arbitrary round and assumed to be fixed throughout the round. Let s be the model size (in *bit*). The communication time that the data owner i spends is $t_i^{cm} \propto (s/b_i)$ [32], [33]. Based on synchronous updates, a time constraint $T_{\max}$ of each round is set for all the data owners. Here, we assume that after computation, the data owners make full use of constraint time for transmission to save bandwidth: $t_i^{cm} = T_{\max} - t_i^{cp}$. Thus, the communication energy consumption of the data owner i at each round is

$$e_i^{cm} = P^{cm}\left(T_{\max} - t_i^{cp}\right) = P^{cm}\left(T_{\max} - \frac{N_F E}{f_i^c n_i} D_i\right) \tag{10}$$

where P^{cm} is the transmission power which is considered to be the same for all data owners [2].

C. Data Owner and Model Owner Modeling

The expected utility of data owner i is the difference between its gained rewards R_i and its total costs of completing federated learning tasks. The costs includes the privacy cost spent for economic loss caused by potential privacy leakage, and the cost spent for energy consumption of computation and communication. If the data size is D_i, the expected utility of data owner i can be expressed as

$$\begin{aligned} u_i^d(D_i, R_i) &= R_i - cT\left(e_i^{cp} + e_i^{cm}\right) - l_i \\ &= R_i - cT\frac{N_F E \psi_i f_i^{c2}}{n_i} D_i \\ &\quad - \left(cTP^{cm}T_{\max} - cT\frac{P^{cm} N_F E}{f_i^c n_i} D_i\right) - \frac{\epsilon}{\epsilon_{\max}} v_i D_i \\ &= R_i - \theta_i D_i - (\zeta - \tau_i D_i) - \rho_i D_i \end{aligned} \tag{11}$$

where c is unit cost of energy, T is number of rounds, $\theta_i = cT[(N_F E \psi_i f_i^{c2})/n_i]$, $\tau_i = cT[(P^{cm} N_F E)/(f_i^c n_i)]$, $\rho_i = (\epsilon v_i/\epsilon_{\max})$, and $\zeta = cTP^{cm}T_{\max}$. θ_i refers to the computation cost and ρ_i refers to the privacy cost. The communication cost is $\zeta - \tau_i$ and relies on τ_i since ζ is a constant. Thereby, here τ_i refers to the communication cost.

Based on (11), the data owners can be classified into different types to characterize their heterogeneity. In particular, the data owners can be categorized into a set $\Theta = \{\theta_x : 1 \leq x \leq X\}$ of X computation cost types, set $\mathcal{T} = \{\tau_y : 1 \leq y \leq Y\}$ of Y communication cost types, set $\mathcal{P} = \{\rho_z : 1 \leq z \leq Z\}$ of Z privacy cost types. Therefore, there are total XYZ types of data owners whose distribution is represented by a joint probability mass function $Q(\theta_x, \tau_y, \rho_z)$. The data owners' types are sorted in a nondecreasing orders as for each dimension: $0 < \theta_1 \leq \theta_2 \leq \cdots \leq \theta_X$, $0 < \tau_1 \leq \tau_2 \leq \cdots \leq \tau_Y$, and $0 < \rho_1 \leq \rho_2 \leq \cdots \leq \rho_Z$. The data owners are discriminated by these three cost types. For notation simplicity, we represent a data owner of computation cost type x, communication cost type y, and privacy cost type z to be that of type-(x, y, z). We then ignore the subscript i and use the combination of data size and rewards $\{D, R\}$ to write the utility of the type-(x, y, z) data owner as

$$\begin{aligned} u^d_{x,y,z}(D, R) &= R - C_{x,y,z}(D) \\ &= R - \theta_x D + \tau_y D - \rho_z D - \zeta \end{aligned} \tag{12}$$

where $C_{x,y,z}$ is the total cost of the type-(x, y, z) data owner.

As discussed in Section IV-A, the trained model performance with DPFL is a concave function with respect to the added noise scale which is converse proportional to the data size given the privacy budget. Without loss of generality, we consider the aggregate model performance to be the average contribution of all the data owners, which is expressed as

$$\begin{aligned} h(D_i) &= \frac{1}{I}\sum_{i=1}^{I}\left(-a\sigma_i^2 + b\right) \\ &= \frac{1}{I}\sum_{i=1}^{I}\left(-\frac{ak}{D_i} + b\right) \end{aligned} \tag{13}$$

where $k = ([14\alpha\eta^2 ET]/[B(\epsilon - \log(1/\delta)/(\alpha - 1))])$. Considering the contract item $\omega_{x,y,z} = \{D_{x,y,z}, R_{x,y,z}\}$ for each data owner type, the aggregate model performance can be rewritten as

$$h\left(D_{x,y,z}\right) = \sum_{x=1}^{X}\sum_{y=1}^{Y}\sum_{z=1}^{Z} Q_{x,y,z}\left(-\frac{ak}{D_{x,y,z}} + b\right) \tag{14}$$

where $Q_{x,y,z}$ is the joint probability mass function for the type of each data owner, i.e., θ_x,τ_y, and ρ_z. The expected utility of the model owner is expressed as

$$\begin{aligned} u^m &= \gamma h\left(D_{x,y,z}\right) - \sum_{x=1}^{X}\sum_{y=1}^{Y}\sum_{z=1}^{Z} IQ_{x,y,z}R_{x,y,z} \\ &= \sum_{x=1}^{X}\sum_{y=1}^{Y}\sum_{z=1}^{Z} IQ_{x,y,z}\left(\frac{\gamma}{I}\left(-\frac{ak}{D_i} + b\right) - R_{x,y,z}\right) \end{aligned} \tag{15}$$

where $\gamma > 0$ denotes the conversion parameters from model performance to profits.

V. Multidimensional Contract Design

In this section, we first formulate the problem as a 3-D contract. Then we transform the 3-D contract to the equal 1-D contract problem with constraints. Finally, we relax the constraints for contract feasibility so as to solve for the optimal contract.

A. Contract Conditions Analysis

We design a 3-D contract $\Omega(\Theta, \mathcal{T}, \mathcal{P}) = \{\omega_{x,y,z}, 1 \leq x \leq X, 1 \leq y \leq Y, 1 \leq z \leq Z\}$ for the model owner to attract the participation of data owners in DPFL under the information asymmetry condition, where the model owner doesn't know the three-type cost information of each data owner. The contract is feasible if and only if each data owner chooses the contract item corresponds to its type. This is ensured when individual rationality (IR) and incentive compatibility (IC) constraints are satisfied at the same time.

Definition 1 [Individual Rationality (IR)]: Each type-(x, y, z) data owner's utility is nonnegative when it selects the contract item $\omega_{x,y,z}$ corresponds to its type, i.e.,

$$u^d_{x,y,z}\left(\omega_{x,y,z}\right) \geq 0, \quad 1 \leq x \leq X, \quad 1 \leq y \leq Y, \quad 1 \leq x \leq Z. \tag{16}$$

Definition 2 [Incentive Compatibility (IC)]: Type-(x, y, z) data owner gets the maximum utility if it selects the contract item $\omega_{x,y,z}$ correspond to its type rather than any other contract items, i.e.,

$$\begin{aligned} u^d_{x,y,z}\left(\omega_{x,y,z}\right) \geq u^d_{x,y,z}\left(\omega_{x',y',z'}\right), \quad 1 \leq x \leq X \\ 1 \leq y \leq Y, \quad 1 \leq x \leq Z. \end{aligned} \tag{17}$$

Thus, the 3-D contract design problem is formulated as

$$\begin{aligned} &\max_{\omega} \ u^m \\ &\text{s.t. } (16), \ (17). \end{aligned} \tag{18}$$

However, the multidimensional contract design problem has XYZ IR constraints and $XYZ(XYZ - 1)$ IC constraints which are all nonconvex. It is difficult to directly handle the contract design problem with multiple nonconvex constraints. To study the contract feasibility, we first transform the multidimensional contract into a single-dimensional contract formulation. Based on (12), the total cost of a type-(x, y, z) data owner is $C_{x,y,z}(D) = \theta_x D - \tau_y D + \rho_z D + \zeta$. we derive the marginal cost α of data size for a type-(x, y, z) data owner as

$$\alpha\left(\theta_x, \tau_y, \rho_z\right) = \frac{\partial C_{x,y,z}(D)}{\partial D} = \theta_x - \tau_y + \rho_z. \tag{19}$$

Intuitively, $\alpha(\theta_x, \tau_y, \rho_z) > 0$ shows the unwillingness of the type-(x, y, z) data owner since the data owner with larger marginal cost is always more unwilling to participate in the DPFL. We sort the XYZ data owners according to their marginal cost of data size in a nondecreasing order as

$$\Phi_1(D), \Phi_2(D), \ldots, \Phi_j(D), \ldots, \Phi_{XYZ}(D) \tag{20}$$

where $\Phi_j(D)$ represent certain type-(x, y, z) as type-Φ_j data owner. Given the sorting order, the data owner types are in an ascending order according to the marginal cost of data size

$$\alpha(\Phi_1, D) \leq \ldots \alpha\left(\Phi_j, D\right) \leq \cdots \leq \alpha(\Phi_{XYZ}, D). \tag{21}$$

To ease of notation, we use type-Φ_j to represent the data owner type and denote $\omega_j = (D_j, R_j)$ as the contract item designed for type-Φ_j data owner. In addition, we use $C(\Phi_j, D_j)$ to represent the new ordering of cost subsequently. Similarly, we use $\alpha(\Phi_j, D_j)$ to represent the marginal cost of data size. We then use the data owners' marginal cost type to analyze the necessary and sufficient conditions for a feasible contract that satisfies the IR and IC conditions.

B. Feasibility of Contract

We first analyze the necessary conditions for a feasible contract.

Lemma 2: For any feasible contract $\omega(\Theta, \mathcal{T}, \mathcal{P})$, $D_j < D_{j'}$ holds if and only if $R_j < R_{j'}$.

The proof can be referred to [15]. Lemma 2 indicates that if the data owner chooses to use more data for training, the feasible contract needs a higher reward, and vise versa.

Lemma 3 (Monotonicity): For any feasible contract $\omega(\Theta, \mathcal{T}, \mathcal{P})$, if $\alpha(\Phi_j, D_j) > \alpha(\Phi_{j'}, D_j)$, it follows that $D_j \le D_{j'}$.

The proof can be referred to [15]. Lemma 3 shows that the data owner with a higher type prefers to do training with more data. According to Lemmas 1 and 2, we can achieve the necessary conditions for a feasible contract as follows.

Theorem 3 (Necessary Conditions): A feasible contract must satisfy:

$$\begin{cases} D_1 \ge D_2 \ge \cdots \ge D_j \ge \cdots \ge D_{XYZ} \\ R_1 \ge R_2 \ge \cdots \ge R_j \ge \cdots \ge R_{XYZ}. \end{cases} \tag{22}$$

We then analyze the sufficient conditions for a feasible contract. In order to achieve the solution of optimal contract by reducing the number of constraints, we relax the IR and IC constraints as follows.

According to the independence of Φ_j on the contract item $\{D, R\}$, i.e., $\Phi_j(D, R) = \Phi_j(D', R'), D \neq D', R \neq R'$, the data owner type does not change with the data size and contract rewards. In addition, based on (19), we can deduce that the data owner type with minimum marginal cost is $\omega_1 = \{\theta_1, \tau_Y, \rho_1\}$, and the data owner type with maximum marginal cost is $\omega_{XYZ} = \{\theta_X, \tau_1, \rho_Z\}$. We can derive the minimum-utility data owner type $\omega_{\max}$ as

$$\omega_{\max} = \arg\min_{\omega_j} u^d\big(D, R, \omega_j\big). \tag{23}$$

Based on (12), the utility decreases in θ_x, increase in τ_y, decreases in ρ_z. We can deduce that the minimum utility is $\{\theta_X, \tau_1, \rho_Z\}$ and $\omega_{\max} = \omega_{XYZ}$ which is the data owner type that incurs the highest marginal cost of data size.

Lemma 4 (Reduce IR Constraints): If the IR constraint of the minimum utility data owner type ω_{XYZ} is satisfied, the IR constraints of other data owner types will also satisfied.

Proof: According to the IC and IR constraints, we have

$$u_j^d \omega_j \ge u_j^d(\omega_{XYZ}) \ge u_{XYZ}^d(\omega_{XYZ}) \ge 0. \tag{24}$$

As long as the IR constraint of the type-ω_{XYZ} data owner is satisfied, the IR constraints of the other data owner type will also hold. The proof is now completed. ■

Lemma 4 enables to cut the XYZ IR constraints to only one IR constraint, i.e., $u_{XYZ}^d(\omega_{XYZ}) \ge 0$.

Definition 3 [Pairwise IC (PIC)]: If and only if

$$\begin{cases} u_j\big(\omega_j\big) \ge u_j\big(\omega_{j'}\big) \\ u_{j'}\big(\omega_{j'}\big) \ge u_{j'}\big(\omega_j\big) \end{cases} \tag{25}$$

is satisfied, the contract item ω_j and $\omega_{j'}$ are pairwise incentive compatible and denoted as $\omega_j \overset{PIC}{\Longleftrightarrow} \omega_{j'}$.

The PIC consists of all IC conditions in the two-data owner case. In other words, the $XYZ(XYZ - 1)$ IC conditions are equivalent to the $XYZ(XYZ - 1)/2$ PIC conditions for all the data owner pairs.

Lemma 5 (Reduce IC Constraints): Under the feasible contract, if $\omega_{j-1} \overset{PIC}{\Longleftrightarrow} \omega_j$ and $\omega_j \overset{PIC}{\Longleftrightarrow} \omega_{j+1}$, then $\omega_{j-1} \overset{PIC}{\Longleftrightarrow} \omega_{j+1}$.

The proof can be referred to [15]. Lemma 5 makes the contract problem more tractable. It shows that we can cut a total of $XYZ(XYZ - 1)/2$ PIC conditions to a total of $XYZ - 1$ PIC conditions for the neighbor data owner type pairs. Now, we can reduce IR and IC constraints and derive a tractable set of sufficient conditions for the feasible contract as follows.

Theorem 4 (Sufficient Conditions): A feasible contract must satisfy:

1) $R_{XYZ} - C(\Phi_{XYZ}, D_{XYZ}) \ge 0$;
2) $R_{j+1} - C(\Phi_{j+1}, D_{j+1}) + C(\Phi_{j+1}, D_j) \ge R_j \ge R_{j+1} - C(\Phi_j, D_{j+1}) + C(\Phi_j, D_j)$.

C. Optimal Contract

According to the conditions for the feasible contract, we first obtain the optimal reward given a feasible set of data size as follows.

Theorem 5 (Optimal Reward): For a feasible set of data size $\mathbf{D}$ satisfying $D_1 \ge D_2 \ge \cdots \ge D_j \ge \cdots \ge D_{XYZ}$, the optimal reward is obtained by

$$R_j^* = \begin{cases} C(\Phi_{XYZ}, D_{XYZ}), & j = XYZ \\ R_{j+1}^* - C\big(\Phi_j, D_{j+1}\big) + C\big(\Phi_j, D_j\big), & \text{otherwise.} \end{cases} \tag{26}$$

We rewrite the optimal rewards in (26) as

$$R_j^* = R_{XYZ}^* + \sum_{m=j}^{XYZ} \Delta_m \tag{27}$$

where $\Delta_{XYZ} = 0$ and $\Delta_m = C(\Phi_m, D_m) - C(\Phi_m, D_{m+1})$,$m = 1, 2, \ldots, XYZ - 1$. To analyze the optimal data size $\mathbf{D}^*$ for the data owners, we substitute the optimal rewards $\mathbf{R}^*$ into the utility function of the model owner and rewrite the optimization problem (18) as

$$\begin{aligned} \max_{\mathbf{D}} \ & \sum_{j=1}^{XYZ} G_j\big(D_j\big) \\ \text{s.t.} \ & D_1 \ge D_2 \ge \cdots \ge D_j \ge \cdots \ge D_{XYZ} \end{aligned} \tag{28}$$

where

$$\begin{aligned} G_j = I\Bigg(& Q(\Phi_j)\gamma h\big(D_j\big) + C\big(\Phi_{j-1}, D_j\big)\sum_{m=1}^{j-1} Q(\Phi_m) \\ & - C\big(\Phi_j, D_j\big)\sum_{m=1}^{j} Q(\Phi_m)\Bigg). \end{aligned} \tag{29}$$

Since the objective functions $G_j(D_j)$ and $G_i(D_i)$ are independent of each other, $i, j \in \{1, \dots, XYZ\}, i \neq j$, $G_j(D_j)$ is only related to D_j. Thus, D_j can be derived by optimizing only $G_j(D_j)$, which is given as

$$D_j^* = \arg\max_{D_j} Q(\Phi_j)\gamma h(D_j) + C(\Phi_{j-1}, D_j)\sum_{m=1}^{j-1} Q(\Phi_m) - C(\Phi_j, D_j)\sum_{m=1}^{j} Q(\Phi_m). \tag{30}$$

In addition, we observe that $G_j(D_j)$ merely consists of a concave function and a linear function such that it is a concave function. According to Fermat's Theorem [34], we can solve. $(\partial G_j/\partial D_j)|_{D_j=D_j^*} = 0$ to derive the D_i^*. If the derived solutions satisfy the monotonicity conditions, they are the optimal contract formulations. Otherwise, we use the iterative adjust algorithm [15] to obtain the solutions that satisfy the monotonicity constraint.

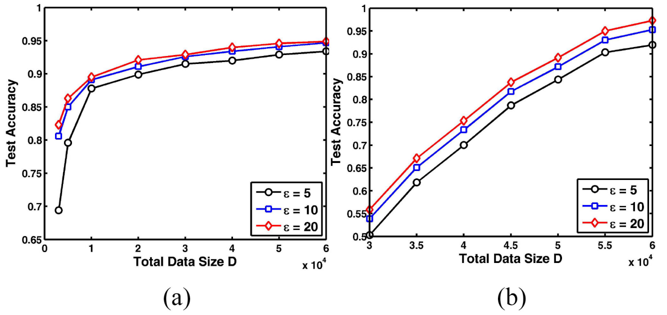
VI. Performance Evaluation

In this section, we evaluate the performance of our proposed multidimensional contract-based incentive mechanism under the DPFL framework.

A. DPFL Performance

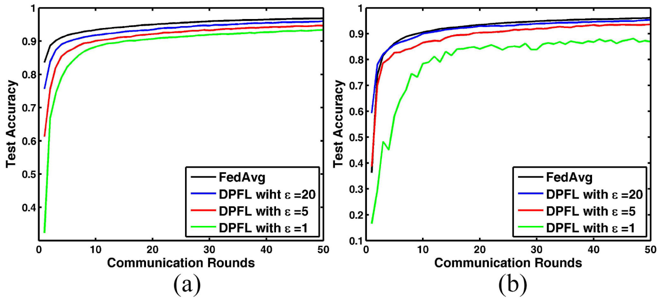
Experimental Setup: We conduct experiments on the standard MNIST data set for handwritten digit recognition including 60 000 samples for training and 10 000 samples for testing. We adopt a LeNet with two convolution layers and two fully connection layers for the multiclass classification task, namely, recognizing digit 0 to 9. Each convolution layer has 32 channels and kernel size is 3. We consider both iid and non-iid settings. For the iid setting, we uniformly split the training samples to 100 data owners. For the non-iid setting, we sort the data by digit label and distribute the data to 100 data owners by using the fashion in [3]. According to [3], we set batch size $B = 10$, number of local epochs $E = 5$, and number of communication rounds $T = 30$ for iid setting and $T = 50$ for non-iid setting. We adopt SGD for the optimizer and set the learning rate $\eta = 0.01$.

Tradeoff Between Accuracy and Privacy: Fig. 1 shows the test accuracy with respect to noise σ under different privacy budgets. When the privacy budget ϵ is fixed, the test accuracy decreases with the increasing noise σ. This is because that the model injected by larger noise has lower performance. We further fit the performance curve A related to noise scale σ and use it to model the contribution of data owners for the incentive mechanism. When the model parameters are injected by the same noise scale, the test accuracy is higher with a lower ϵ. This is because that under the same noise scale, the data owners choose a larger data size to reach a lower ϵ. With the same privacy budget, the model performance under the non-iid setting decreases more rapidly than that under the iid setting. The reason is that the non-iid data increases the difficulty of training. Fig. 2 shows the test accuracy with respect to total data size D. When ϵ is fixed, the test accuracy increases with increasing data size D. This is because that the model trained on a larger data size has better performance. When we use the same data size to train the model, the test accuracy is higher with a higher ϵ. This is because that with the same data size, the data owners choose to inject less noise to reach a higher ϵ. The test accuracy of the trained model under the iid setting outperforms that of the non-iid setting. The reason is that it is more difficult for training the model over non-iid data.



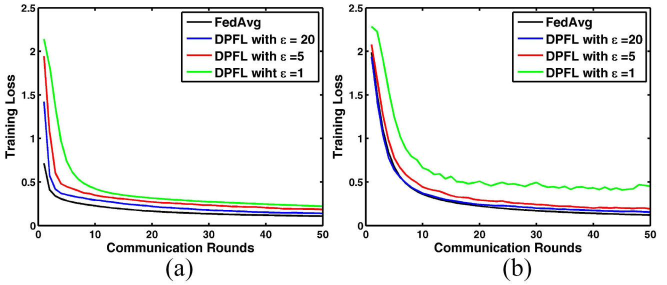
(a) (b)

Fig. 2. Test accuracy with respect to data size under different privacy budget (under IID and non-IID setting). (a) MNIST IID. (b) MNIST NON-IID.



(a) (b)

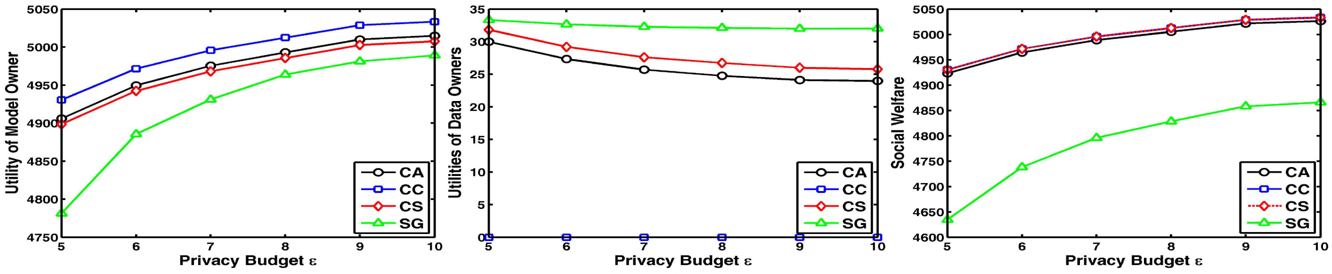
Fig. 3. Test accuracy with respect to communication rounds for the MNIST data set (under IID and non-IID setting). (a) MNIST IID. (b) MNIST NON-IID.



(a) (b)

Fig. 4. Training Loss with respect to communication rounds for the MNIST data set (under IID and non-IID setting). (a) MNIST IID. (b) MNIST NON-IID.

Convergence Properties: We set the total data size $D = 60\ 000$ and the number of communication rounds $T = 50$ to observe the algorithmic convergence properties of the DPFL framework. Fig. 3 and 4 show the test accuracy and training loss with respect to communication rounds under different privacy budget. The traditional federated



(a) (b) (c)

Fig. 5. System performance with respect to privacy budget under different incentive mechanisms. (a) Utility of model owner. (b) Total utilities of data owners. (c) Social welfare.

TABLE I
PARAMETER SETTING IN THE SIMULATION

Parameters	Setting
DPFL: B, E, T, η	10, 5, 30, 0.01
DP: δ, ϵ_{max}, a, b	10^{-5}, 50, 252.5413, 0.9351
Computation: n_i	8FLOPs/cycle
Communication: P^{cm}, T_{max}	0.2Watt, 6s

learning algorithm FedAvg [3] is considered as a baseline performance without adding noise. As the privacy budget ϵ decreases, the training loss converges to a higher bound and the test accuracy decreases. This is because that with fixed data size, a lower data budget ϵ brings to a larger noise σ which implies larger convergence error. This is consistent with the convergence analysis in Section III-D. Comparing with the training under the iid setting, the training under the non-iid setting has a higher bound of training loss and a lower test accuracy. The reason is that training over the non-iid setting brings a larger convergence error.

B. Contract Performance

Simulation Setup: We consider that 100 model owners use the LeNet on MNIST data set under iid setting and the compuation workload is $N_F = 10$MFLOPs. The CPU clock frequencies of devices f_i^c are uniformly chosen from $\{1100, 1150, 1200, 1250\}$ MHz. The Coefficient of the CMOS circuit ψ_i is uniformly chosen from $\{1, 1.5, 2, 2.5\} \times 10^{-28}$. The economical loss of unit data v_i is uniformly chosen from $\{0.01, 0.012, 0.014, 0.016\}$. The profit coefficient is $\gamma = 500$ and the unit cost of energy is $c = 0.5$. The other parameters are set based on the Table I.

Performance Comparison: We compare our proposed contract-based incentive mechanism under asymmetric information scenario (CA) with the other three incentive mechanisms: contract-based incentive mechanism under complete information scenario (CC), contract-based incentive mechanism for social maximization (CS) [15], and Stackelberg game-based incentive mechanism (SG) [35]. CC considers the scenario where the model owner knows the cost types of each data owner. CS considers the information asymmetry but the model owner aims to maximize the social welfare which is expressed as

$$u^s = u^m + \sum_{i=1}^{XYZ} u_i^d$$
$$= \sum_{i=1}^{XYZ} IQ_{x,y,z}\left(\frac{\gamma}{I}\left(-\frac{ak}{D_i}+b\right) - C_{x,y,z}\right). \qquad (31)$$

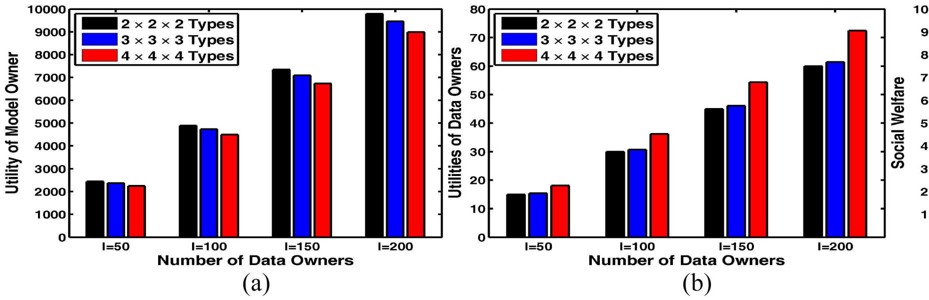
SG considers the data owners share a total reward R from the model owner based on the proportion of data size and the objective of each data owner is to maximize its own utility which is expressed as

$$u_i^d = \frac{D_i}{D}R - \theta_i D_i - (\zeta - \tau_i D_i) - \rho_i D_i. \qquad (32)$$

We consider 8 ($2 \times 2 \times 2$) data owner types. Fig. 5 shows the system performance under different incentive mechanisms. With the CC mechanism, the model owner achieves the highest utility but the utilities of data owners are zero. It is because that the model owner has full knowledge of data owners' types and thus designs the contracts for maximizing its own utility, leading minimum utilities of data owners. With the CS mechanism, the data owners achieve higher utilities while the model owners obtain lower utilities. The reason is that the CS mechanism aims at maximizing the social welfare and thus reaches the balance between the data owner side and the model owner side. We find that the CS mechanism attains the highest social welfare as well as the CC mechanism, but the CS mechanism is under information asymmetry condition. With the SG mechanism, the data owners have the highest utilities but the model owner has the lowest utility. The reason is that the objective of the data owners with SG mechanism is to maximize their own utilities and thus reduce the utility of the model owner. Compared with the three mechanisms, our proposed CA mechanism allows the model owner to obtain near-optimal utility under the information asymmetry condition.

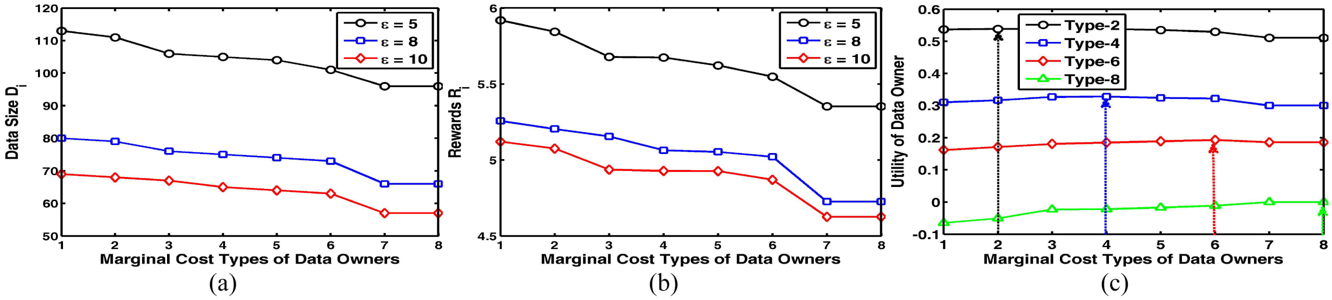
Impact of Privacy Budget ϵ: Fig. 5 shows the system performance with respect to privacy budget ϵ. With higher ϵ, the utility of model owner and the social welfare increase but the utilities of data owners decreases. It is because that setting a higher ϵ will allow the data owners to make higher contribution for the model performance and thus improve the profit of the model owner. But a higher ϵ also brings higher privacy cost to the data owners.

Impact of Multidimension Types: Fig. 6 shows the system performance with respect to number of data owners under



(a) (b) (c)

Fig. 6. System performance with respect to number of data owners under different number of data owner types. (a) Utility of model owner. (b) Total utilities of data owners. (c) Social welfare.



(a) (b) (c)

Fig. 7. Properties of contract-based incentive mechanism. (a) Data size monotonicity. (b) Reward monotonicity. (c) Utility of data owner with different contracts.

different number of data owner types. When the number of data owners increases, both the model owner and the data owners obtain higher utilities. It is because that the growing number of data owners can contribute more data for training the model and gain more rewards. Thus, the social welfare is also improved. When the number of data owner types increases, the utility of model owner decreases but the utilities of data owners increase. The reason is that when the number of data owner types increases, it becomes more difficult for the model owner to mine the information of the data owners' type and design the corresponding contract. Therefore, the data owners can extract more reward from the model owner.

Contract Properties: Fig. 7 shows the properties of the designed optimal contracts. We consider 8 (2 × 2 × 2) data owner types. Fig. 7(a) and (b) shows that both the data size and reward monotonically decrease with the increase of the marginal cost of data owners. This satisfies the feasibility of contract structure given in Theorem 3. Moreover, type-7 and type-8 have the same data size and reward. It is the result of adjusting the solutions to satisfy the monotonicity constraint. Fig. 7(c) shows the utility of different type of data owner selecting different types of designed contracts. We observe that the data owner achieves the highest utility only when it selects the contracts of its own type. This satisfies the IC constraints. When they select the contract of their own types, their utilities are nonnegative. This satisfies the IR constrains. In particular, the utility of type-8 is zero, as verified in Lemma 5.

VII. Conclusion

In this article, we proposed a practical incentive mechanism for incentivizing the data owners to join federated learning in the IoT area by jointly considering their task expenditure and privacy risk. To control the risk of privacy leakage in the federated learning process, we built up a DPFL framework and provided corresponding theoretical analysis. Under the DPFL framework, we modeled the data owners' contribution and three-type costs, which are related to local training data size and privacy budget. Based on the contribution and cost models, we designed a 3-D contract-based incentive mechanism to find the optimal reward and local training data size for different types of data owners under the information asymmetry. We also conducted simulations to validate the effectiveness of the proposed incentive mechanism.

Appendix A
Additional Notation

Definition 4 [(ϵ, δ)-DP]: A randomized machanism $f : \mathcal{X} \mapsto \mathcal{R}$ with domain $\mathcal{D}$ and range $\mathcal{R}$ offers (ϵ, δ)-differential privacy if for any two adjacent data sets $X, X' \in \mathcal{X}$ that differ in at least one sample and any outputs $S \subset \mathcal{R}$. With a bound δ, it satisfies $\Pr[f(X) \in S] \leq e^{\epsilon} \Pr[f(X') \in S] + \delta$.

Definition 5 [(α, ρ)-RDP]: A randomized mechanism $f : \mathcal{X} \mapsto \mathcal{R}$ offers (α, ρ)-Renyi different privacy, if for any adjacent $X, X' \in \mathcal{X}$ it holds $D_{\alpha}(f(X) \| f(X')) \leq \rho$.

RDP is a natural relaxation of DP that is well suited for expressing guarantees of privacy-preserving algorithms. It has the following properties [36].

Lemma 6: Gaussian mechanism $\mathcal{M} = f(D) + \mathcal{N}(0, \sigma^2 \mathbf{I_d})$ applied on a subset of samples that are drawn uniformly without replacement with probability τ satisfies $(\alpha, [(3.5\tau^2\alpha)/\sigma^2])$-RDP given $\alpha - 1 \leq [(2\sigma^2)/3] \log(1/[\alpha\tau(1 + \sigma^2)])$, where the sensitivity of f is 1.

Lemma 7: If a randomized mechanism $\mathcal{M}$ satisfies (α, ρ)-RDP, $\mathcal{M}$ satisfies $(\rho + ([\log(1/\delta)]/[\alpha - 1]), \delta)$-DP for all $\delta \in (0, 1)$.

Appendix B
Proof of Theorem 1

We use RDP to tightly account the privacy loss of the data owner and then convert it to a DP guarantee. For local iteration s of round t, the data owner i learns a batch of data with batch size B to update the local model: $w^i_{t,s} \leftarrow w^i_{t,s-1} - (\eta/B)\nabla\ell(w^i_{t,s-1}; b_{i,s})$. Given any two neighboring data sets X and X' of size B, the sensitivity of the local model at local iteration s of round t is

$$\begin{aligned}\triangle\left(w^i_{t,s}\right) &= \max_{X,X'}\|w^i_{t,s} - w^i_{t,s'}\|_2\\ &= \max_{X,X'}\frac{\eta}{B}\left\|\ell\left(w^i_{t,s-1}; X\right) - \ell\left(w^i_{t,s-1}; X'\right)\right\|_2 \le \frac{2\eta L}{B}.\end{aligned}$$

The inequality is due to the L-Lipschitz continuous of the loss function $\ell(\cdot)$. The sampling rate is $\tau = (B/D_i)$. According to Lemma 6, if we add Gaussian noise drawn from $\mathcal{N}(0, \sigma^2 I_d)$, each iteration then preserves $(\alpha, \epsilon(\alpha)')$-RDP with $\epsilon(\alpha)' = [(14\alpha\eta^2L^2)/(D_i^2\sigma_i^2)]$. After T rounds with $|\beta_i|E$ local iterations at each round, it provides $(\alpha, [(14\eta^2L^2ET\alpha)/(BD_i\sigma_i^2)])$-RDP. By Lemma 7, Algorithm 1 provides (ϵ, δ)-DP with $\epsilon = [(14\eta^2L^2ET\alpha)/(BD_i\sigma_i^2)] + ([\log(1/\delta)]/[\alpha - 1])$. We set $L = 1$ [17] and solve σ_i from ϵ and achieve (1).

Appendix C
Proof of Lemma 1

At round $t \ge 1$, each data owner calculates the update for sth iteration as $w^i_{t,s} = w_{t-1} - \eta\sum_{h=1}^{s}(g^i_{t,s} - [(n^i_{t,s})/\eta])$. By (2), we have $\overline{w}_{t,s} = w_{t-1} - \eta\sum_{h=1}^{s}\sum_{i=1}^{I}p_i(g^i_{t,s} - [n^i_{t,s}/\eta])$. Thus, we have

$$\begin{aligned}&\mathbb{E}\left[\left\|\overline{w}_{t,s} - w^i_{t,s}\right\|^2\right]\\ &= \mathbb{E}\left[\left\|\eta\sum_{h=1}^{s}\sum_{i=1}^{I}p_i\left(g^i_{t,s} - \frac{n^i_{t,s}}{\eta}\right) - \eta\sum_{h=1}^{s}\left(g^i_{t,s} - \frac{n^i_{t,s}}{\eta}\right)\right\|^2\right]\\ &= \eta^2\sum_{h=1}^{s}\sum_{i=1}^{I}p_i^2\mathbb{E}\left[\left\|g^i_{t,s}\right\|^2\right] + \sum_{h=1}^{s}\sum_{i=1}^{I}p_i^2\mathbb{E}\left[\left\|n^i_{t,s}\right\|^2\right]\\ &\quad + \eta^2\sum_{h=1}^{s}\mathbb{E}\left[\left\|g^i_{t,s}\right\|^2\right] + \sum_{h=1}^{s}\mathbb{E}\left[\left\|n_{t,s}\right\|^2\right]\\ &\overset{(a)}{\le} s\eta^2G^2\sum_{i=1}^{I}p_i^2 + sd\sum_{i=1}^{I}p_i^2\sigma_i^2 + s\eta^2G^2 + sd\sigma_i^2 \end{aligned} \tag{33}$$

where (a) follows Assumption 3 and the expected noise scale $\mathbb{E}[\|n_{t,s}\|^2] = d\sigma_i^2$ with noise dimension d.

Appendix D
Proof of Theorem 2

Based on the Assumption 1, we have

$$\begin{aligned}\mathbb{E}\left[f\left(\overline{w}_{t,s}\right)\right] &\le \mathbb{E}\left[f\left(\overline{w}_{t,s-1}\right)\right] + \frac{L}{2}\mathbb{E}\left[\left\|\overline{w}_{t,s} - \overline{w}_{t,s-1}\right\|^2\right]\\ &\quad + \mathbb{E}\left[\left\langle\nabla f\left(\overline{w}_{t,s-1}\right), \overline{w}_{t,s} - \overline{w}_{t,s-1}\right\rangle\right].\end{aligned} \tag{34}$$

Note that

$$\begin{aligned}&\mathbb{E}\left[\|\overline{w}_{t,s} - \overline{w}_{t,s-1}\|^2\right] \overset{(a)}{=} \eta^2\mathbb{E}\left[\left\|\sum_{i=1}^{I}p_i\left(g^i_{t,s} - \frac{n^i_{t,s}}{\eta}\right)\right\|^2\right]\\ &= \eta^2\mathbb{E}\left[\left\|\sum_{i=1}^{I}p_i\left(g^i_{t,s} - \frac{n^i_{t,s}}{\eta}\right) - \sum_{i=1}^{I}p_i\nabla f_i\left(w^i_{t,s-1}\right)\right\|^2\right]\\ &\quad + \eta^2\mathbb{E}\left[\left\|\sum_{i=1}^{I}p_i\nabla f_i\left(w^i_{t,s-1}\right)\right\|^2\right]\\ &= \eta^2\sum_{i=1}^{I}p_i^2\mathbb{E}\left[\left\|g^i_{t,s} - \nabla f_i\left(w^i_{t,s-1}\right)\right\|^2\right] + \sum_{i=1}^{I}p_i^2\mathbb{E}\left[\left\|n^i_{t,s}\right\|^2\right]\\ &\quad + \eta^2\sum_{i=1}^{I}p_i^2\mathbb{E}\left[\left\|\nabla f_i\left(w^i_{t,s-1}\right)\right\|^2\right]\\ &\overset{(b)}{\le} \frac{\eta^2Q^2}{B}\sum_{i=1}^{I}p_i^2 + d\sum_{i=1}^{I}p_i^2\sigma_i^2 + \eta^2\sum_{i=1}^{I}p_i^2\mathbb{E}\left[\left\|\nabla f_i\left(w^i_{t,s-1}\right)\right\|^2\right]\end{aligned} \tag{35}$$

where (a) follows from (2); (b) follows because each $g^i_{t,s} - \nabla f_i(w^i_{t,s-1})$ has 0 mean and is independent across data owners, and the expected noise scale. We further note that

$$\begin{aligned}&\mathbb{E}\left[\left\langle\nabla f\left(\overline{w}_{t,s-1}\right), \overline{w}_{t,s} - \overline{w}_{t,s-1}\right\rangle\right]\\ &\overset{(a)}{=} -\eta\mathbb{E}\left[\left\langle\nabla f\left(\overline{w}_{t,s-1}\right), \sum_{i=1}^{I}p_i\left(g^i_{t,s} - \frac{b^i_{t,s}}{\eta}\right)\right\rangle\right]\\ &\overset{(b)}{=} -\eta\mathbb{E}\left[\left\langle\nabla f\left(\overline{w}_{t,s-1}\right), \sum_{i=1}^{I}p_i\nabla f_i\left(w^i_{t,s-1}\right)\right\rangle\right]\\ &\overset{(c)}{=} -\frac{\eta}{2}\mathbb{E}\left[\left\|\nabla f\left(\overline{w}_{t,s-1}\right)\right\|^2 + \left\|\sum_{i=1}^{I}p_i\nabla f_i\left(w^i_{t,s-1}\right)\right\|^2\right.\\ &\qquad\left. - \left\|\nabla f\left(\overline{w}_{t,s-1}\right) - \sum_{i=1}^{I}p_i\nabla f_i\left(w^i_{t,s-1}\right)\right\|^2\right]\end{aligned} \tag{36}$$

where (a) follows from (2); (b) refers to [30]; (c) follows from the basic identity $\langle x, y\rangle = (1/2)(\|x\|^2 + \|y\|^2 + \|x - y\|^2)$, where x, y are any two vectors with same length. We note that

$$\begin{aligned}&\mathbb{E}\left[\left\|\nabla f\left(\overline{w}_{t,s-1}\right) - \sum_{i=1}^{I}p_i\nabla f_i\left(w^i_{t,s-1}\right)\right\|^2\right]\\ &= \mathbb{E}\left[\left\|\sum_{i=1}^{I}p_i\nabla f_i\left(\overline{w}_{t,s-1}\right) - \sum_{i=1}^{I}p_i\nabla f_i\left(w^i_{t,s-1}\right)\right\|^2\right]\\ &= \sum_{i=1}^{I}p_i^2\mathbb{E}\left[\left\|\nabla f_i\left(\overline{w}_{t,s-1}\right) - \nabla f_i\left(w^i_{t,s-1}\right)\right\|^2\right]\\ &\overset{(a)}{\le} L^2\sum_{i=1}^{I}p_i^2\mathbb{E}\left[\left\|\overline{w}_{t,s-1} - w^i_{t,s-1}\right\|^2\right] \overset{(b)}{\le} L^2\sum_{i=1}^{I}p_i^2H\end{aligned} \tag{37}$$

where (a) follows from Assumption 1; (b) follows from Lemma 1. We substitute (35) and (36) into (34) and get

$$\begin{aligned}
&\mathbb{E}\big[f\big(\overline{w}_{t,s}\big)\big] \\
&\leq \mathbb{E}\big[\overline{w}_{t,s-1}\big] - \frac{\eta - \eta^2 L}{2}\sum_{i=1}^{I} p_i \mathbb{E}\Big[\big\|\nabla f_i\big(w^i_{t,s-1}\big)\big\|^2\Big] \\
&\quad - \frac{\eta}{2}\mathbb{E}\Big[\big\|\nabla f\big(\overline{w}_{t,s-1}\big)\big\|^2\Big] + \frac{L\eta^2 Q^2}{2}\sum_{i=1}^{I} p_i^2 + \frac{L\eta^2}{2}\sum_{i=1}^{I} p_i^2 \sigma_i^2 \\
&\quad + \frac{\eta}{2}\mathbb{E}\left[\left\|\nabla f\big(\overline{w}_{t,s-1}\big) - \sum_{i=1}^{I} p_i \nabla f_i\big(w^i_{t,s-1}\big)\right\|^2\right] \\
&\leq \mathbb{E}\big[\overline{w}_{t,s-1}\big] - \frac{\eta}{2}\mathbb{E}\Big[\big\|\nabla f\big(\overline{w}_{t,s-1}\big)\big\|^2\Big] + \frac{\eta L^2}{2}\sum_{i=1}^{I} p_i^2 H \\
&\quad + \frac{L\eta^2 Q^2}{2B}\sum_{i=1}^{I} p_i^2 + \frac{dL\eta^2}{2}\sum_{i=1}^{I} p_i^2 \sigma_i^2. \qquad (38)
\end{aligned}$$

We divide both sides by $(\eta/2)$ and rearrange terms to have

$$\begin{aligned}
&\mathbb{E}\Big[\big\|\nabla f\big(\overline{w}_{t,s-1}\big)\big\|^2\Big] \\
&\quad \leq \frac{2}{\eta}\big(\mathbb{E}\big[f\big(\overline{w}_{t,s-1}\big)\big] - \mathbb{E}\big[f\big(\overline{w}_{t,s}\big)\big]\big) + L^2\sum_{i=1}^{I} p_i^2 H \\
&\qquad + \frac{L\eta Q^2}{B}\sum_{i=1}^{I} p_i^2 + L\eta d\sum_{i=1}^{I} p_i^2 \sigma_i^2. \qquad (39)
\end{aligned}$$

We set $K = (T-1)|\beta|E + S$. Sum over K local iterations and divide both side by K and achieve

$$\begin{aligned}
&\frac{1}{K}\sum_{t=1}^{T-1}\sum_{s=1}^{S}\mathbb{E}\Big[\big\|\nabla f\big(\overline{w}_{t,s-1}\big)\big\|^2\Big] \\
&\quad \leq \frac{2}{\eta K}\big(f\big(\overline{w}_{0,0}\big) - \mathbb{E}\big[f\big(\overline{w}_{t,s}\big)\big]\big) + L^2\sum_{i=1}^{I} p_i^2 H \\
&\qquad + \frac{L\eta Q^2}{B}\sum_{i=1}^{I} p_i^2 + L\eta d\sum_{i=1}^{I} p_i^2 \sigma_i^2 \\
&\quad \leq \frac{2}{\eta K}\big(f\big(\overline{w}_{0,0}\big) - f^*\big) + L^2\sum_{i=1}^{I} p_i^2 H + \frac{L\eta Q^2}{B}\sum_{i=1}^{I} p_i^2 \\
&\qquad + L\eta d\sum_{i=1}^{I} p_i^2 \sigma_i^2. \qquad (40)
\end{aligned}$$

References

[1] X. Huang, R. Yu, S. Xie, and Y. Zhang, "Task-container matching game for computation offloading in vehicular edge computing and networks," *IEEE Trans. Intell. Transp. Syst.*, early access, May 8, 2020, doi: 10.1109/TITS.2020.2990462.

[2] M. Wu, X. Huang, B. Tan, and R. Yu, "Hybrid sensor network with edge computing for AI applications of connected vehicles," *J. Internet Technol.*, vol. 21, no. 5, pp. 1503–1516, 2020.

[3] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Stat.*, 2017, pp. 1273–1282.

[4] D. Ye, R. Yu, M. Pan, and Z. Han, "Federated learning in vehicular edge computing: A selective model aggregation approach," *IEEE Access*, vol. 8, pp. 23920–23935, 2020.

[5] R. Yu and P. Li, "Toward resource-efficient federated learning in mobile edge computing," *IEEE Netw.*, vol. 35, no. 1, pp. 12–19, Jan. 2021.

[6] J. Pang, Y. Huang, Z. Xie, Q. Han, and Z. Cai, "Realizing the heterogeneity: A self-organized federated learning framework for IoT," *IEEE Internet Things J.*, early access, Jul. 7, 2020, doi: 10.1109/JIOT.2020.3007662.

[7] R. Hu, Y. Guo, H. Li, Q. Pei, and Y. Gong, "Personalized federated learning with differential privacy," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9530–9539, Oct. 2020.

[8] M. Nasr, R. Shokri, and A. Houmansadr, "Machine learning with membership privacy using adversarial regularization," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2018, pp. 634–646.

[9] L. Zhu, Z. Liu, and S. Han, "Deep leakage from gradients," in *Advances in Neural Information Processing Systems*, Red Hook, NY, USA: Curran Assoc., Inc., 2019, pp. 14774–14784.

[10] B. Hitaj, G. Ateniese, and F. Perez-Cruz, "Deep models under the GAN: Information leakage from collaborative deep learning," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2017, pp. 603–618.

[11] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," in *Proc. IEEE Symp. Security Privacy (SP)*, San Francisco, CA, USA, 2019, pp. 691–706.

[12] Y. Zhan, P. Li, Z. Qu, D. Zeng, and S. Guo, "A learning-based incentive mechanism for federated learning," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6360–6368, Jul. 2020.

[13] S. R. Pandey, N. H. Tran, M. Bennis, Y. K. Tun, A. Manzoor, and C. S. Hong, "A crowdsourcing framework for on-device federated learning," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 3241–3256, May 2020.

[14] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10700–10714, Dec. 2019.

[15] Z. Xiong, J. Kang, D. Niyato, P. Wang, H. V. Poor, and S. Xie, "A multi-dimensional contract approach for data rewarding in mobile networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 9, pp. 5779–5793, Sep. 2020.

[16] W. Y. B. Lim *et al.*, "Towards federated learning in UAV-enabled Internet of vehicles: A multi-dimensional contract-matching approach," 2020. [Online]. Available: arXiv:2004.03877.

[17] R. Hu, Y. Gong, and Y. Guo, "Concentrated differentially private and utility preserving federated learning," 2020. [Online]. Available: arXiv:2003.13761.

[18] M. Du, K. Wang, Y. Chen, X. Wang, and Y. Sun, "Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 62–67, Aug. 2018.

[19] M. Du, K. Wang, Z. Xia, and Y. Zhang, "Differential privacy preserving of training model in wireless big data with edge computing," *IEEE Trans. Big Data*, vol. 6, no. 2, pp. 283–295, Jun. 2020.

[20] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6492–6499, Dec. 2019.

[21] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 968–979, May 2020.

[22] K. Wei *et al.*, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454–3469, 2020.

[23] J. Ding, J. Wang, G. Liang, J. Bi, and M. Pan, "Towards plausible differentially private ADMM based distributed machine learning," in *Proc. 29th ACM Int. Conf. Inf. Knowl. Manag.*, Virtual Event, Ireland, Oct. 2020, pp. 285–294.

[24] J. Ding, X. Zhang, X. Li, J. Wang, R. Yu, and M. Pan, "Differentially private and fair classification via calibrated functional mechanism," in *Proc. AAAI Conf. Artif. Intell.*, New York, NY, USA, Feb. 2020, pp. 622–629.

[25] Y. Sarikaya and O. Ercetin, "Motivating workers in federated learning: A Stackelberg game perspective," *IEEE Netw. Lett.*, vol. 2, no. 1, pp. 23–27, Mar. 2020.

[26] W. Y. B. Lim *et al.*, "Hierarchical incentive mechanism design for federated machine learning in mobile networks," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9575–9588, Oct. 2020.

[27] Y. Jiao, P. Wang, D. Niyato, B. Lin, and D. I. Kim, "Toward an automated auction framework for wireless federated learning services market," *IEEE Trans. Mobile Comput.*, early access, May 14, 2020, doi: 10.1109/TMC.2020.2994639.

[28] R. Hu and Y. Gong, "Trading data for learning: Incentive mechanism for on-device federated learning," 2020. [Online]. Available: arXiv:2009.05604.

[29] M. Abadi *et al.*, "Deep learning with differential privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 308–318.

[30] H. Yu, S. Yang, and S. Zhu, "Parallel restarted SGD with faster convergence and less communication: Demystifying why model averaging works for deep learning," in *Proc. AAAI Conf. Artif. Intell.*, vol. 33, 2019, pp. 5693–5700.

[31] Q. Zeng, Y. Du, K. Huang, and K. K. Leung, "Energy-efficient resource management for federated edge learning with CPU-GPU heterogeneous computing," 2020. [Online]. Available: arXiv:2007.07122.

[32] M. Pan, C. Zhang, P. Li, and Y. Fang, "Joint routing and link scheduling for cognitive radio networks under uncertain spectrum supply," in *Proc. IEEE INFOCOM*, Shanghai, China, 2011, pp. 2237–2245.

[33] M. Pan, P. Li, Y. Song, Y. Fang, and P. Lin, "Spectrum clouds: A session based spectrum trading system for multi-hop cognitive radio networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, 2012, pp. 1557–1565.

[34] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[35] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," *IEEE/ACM Trans. Netw.*, vol. 24, no. 3, pp. 1732–1744, Jun. 2016.

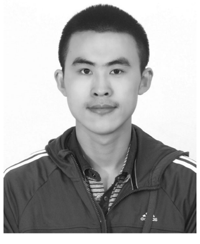
[36] I. Mironov, "Rényi differential privacy," in *Proc. IEEE 30th Comput. Security Found. Symp. (CSF)*, 2017, pp. 263–275.

Maoqiang Wu (Graduate Student Member, IEEE) received the M.S. degree in control science and engineering from the Guangdong University of Technology, Guangzhou, China, in 2017, where he is currently pursuing the Ph.D. degree.

His research interests include mobile crowdsourcing and data privacy in edge intelligence.

Dongdong Ye received the M.S. degree from the Guangdong University of Technology, Guangzhou, China, in 2018, where he is currently pursuing the Ph.D. degree.

His research interests include game theory, resource management in wireless communications and networking.



Jiahao Ding (Graduate Student Member, IEEE) received the B.S. degree in electronic information engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 2017. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX, USA.

His research interests include data analytics, privacy and fairness for machine learning and distributed algorithms.

Mr. Ding is a Student Member of AAAI.

Yuanxiong Guo (Member, IEEE) received the B.Eng. degree in electronics and information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2009, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2012 and 2014, respectively.

Since 2019, he has been an Assistant Professor with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX, USA. His current research interests include data analytics, security, and privacy with applications to Internet of Things and edge computing.

Dr. Guo is a recipient of the Best Paper Award in the IEEE Global Communications Conference in 2011. He is currently serving as an Editor for the IEEE Transactions on Vehicular Technology.

Rong Yu (Member, IEEE) received the B.S. degree in communication engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2002, and the Ph.D. degree in electronic engineering from Tsinghua University, Beijing, in 2007.

He was with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China. In 2010, he joined the School of Automation, Guangdong University of Technology, Guangzhou, where he is currently a Professor. He has authored or coauthored over 100 international journals and conference papers. He is the co-inventor of over 50 patents in China. He was a member of the Home Networking Standard Committee, China, where he led the standardization work of three standards. His research interests include wireless networking and mobile computing, such as mobile cloud, edge computing, deep learning, connected vehicles, smart grids, and the Internet of Things.

Miao Pan (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the Dalian University of Technology, Dalian, China, in 2004, the M.A.Sc. degree in electrical and computer engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2007, and the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2012.

He is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX, USA. His research interests include cybersecurity, big data privacy, deep learning privacy, cyber–physical systems, and cognitive radio networks.

Dr. Pan was a recipient of NSF CAREER Award in 2014. His work won IEEE TCGCC (Technical Committee on Green Communications and Computing) Best Conference Paper Awards in 2019, and the Best Paper Awards in ICC 2019, VTC 2018, Globecom 2017, and Globecom 2015, respectively. He is an Editor for IEEE Open Journal of Vehicular Technology and an Associate Editor for IEEE Internet of Things (IoT) Journal (Area 5: Artificial Intelligence for IoT), and used to be an Associate Editor for IEEE Internet of Things (IoT) Journal (Area 4: Services, Applications, and Other Topics for IoT) from 2015 to 2018. He has also been serving as a Technical Organizing Committee for several conferences, such as TPC Co-Chair for Mobiquitous in 2019, ACM WUWNet in 2019. He is a member of AAAI and ACM.