Pain-FL: Personalized Privacy-Preserving Incentive for Federated Learning

Peng Sun, Haoxuan Che, Zhibo Wang, *Senior Member, IEEE*, Yuwei Wang, Tao Wang, Liantao Wu, and Huajie Shao

***Abstract*— Federated learning (FL) is a privacy-preserving distributed machine learning framework, which involves training statistical models over a number of mobile users (i.e., workers) while keeping data localized. However, recent works have demonstrated that workers engaged in FL are still susceptible to advanced inference attacks when sharing model updates or gradients, which would discourage them from participating. Most of the existing incentive mechanisms for FL mainly account for workers' resource cost, while the cost incurred by potential privacy leakage resulting from inference attacks has rarely been incorporated. To address these issues, in this paper, we propose a contract-based personalized privacy-preserving incentive for FL, named Pain-FL, to provide customized payments for workers with different privacy preferences as compensation for privacy leakage cost while ensuring satisfactory convergence performance of FL models. The core idea of Pain-FL is that each worker agrees on a customized contract, which specifies a kind of privacy-preserving level (PPL) and the corresponding payment, with the server in each round of FL. Then, the worker perturbs her calculated stochastic gradients to be uploaded with that PPL in exchange for that payment. In particular, we respectively derive a set of optimal contracts analytically under both complete and incomplete information models, which could optimize the convergence performance of the finally learned global model, while bearing some desired economic properties, i.e., budget feasibility, individual rationality, and incentive compatibility. An exhaustive experimental evaluation of Pain-FL is conducted, and the results corroborate its practicability and effectiveness.**

***Index Terms*— Federated learning, differential privacy, incentive mechanism, contracts.**

I. Introduction

With the proliferation of sensor-rich mobile devices (e.g., smartphones), Internet of Things (IoT) end nodes (e.g., RFID tags), and the ubiquitous deployment of wireless communication infrastructures, an unprecedented amount of data has been generated at the network edge [1]–[3]. Collecting and mining this massive data could help build various machine learning models that can empower a wide range of intelligent applications, such as smart cities and homes [4]. The conventional machine learning paradigm requires centralizing data from data owners (e.g., mobile users), which raises serious privacy concerns [5].

To alleviate privacy risks, federated learning (FL) [5]–[8] has recently been proposed as a promising distributed machine learning methodology. A typical FL system (e.g., Gboard [9] developed by Google) consists of two parties: a crowd of workers carrying mobile devices and a central server. The involved workers collaboratively learn a machine learning model under the orchestration of the server while keeping data localized. Specifically, each worker computes the updates of the current global model based on her local data and uploads the model updates (or intermediate gradients) to the server. The server aggregates the information from the participating workers and updates the global model. Then, the server feeds the updated global model back to the workers for the next-round distributed on-device training. The interactions between workers and the server are repeated until a desired accuracy level of the global model is achieved. In this setup, many system privacy risks resulting from traditional centralized machine learning can be significantly mitigated.

However, recent works have demonstrated that FL is vulnerable to inference attacks launched by malicious workers or an honest but curious server. These inference attacks include reconstruction attacks [10]–[12] that recover workers' private training data (e.g., private images), and membership inference attacks [13], [14] that infer whether or not a particular data sample (e.g., a specific patient profile) belongs to the private training dataset of a worker. To safeguard

Manuscript received March 1, 2021; revised July 25, 2021; accepted August 27, 2021. Date of publication October 8, 2021; date of current version November 22, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 62102337, Grant 62122066, Grant U20A20182, and Grant 61872274; and in part by the National Key Research and Development Program of China under Grant 2020AAA0107705. *(Corresponding author: Zhibo Wang.)*

Peng Sun is with the State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China, and also with the School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen, Shenzhen 518172, China (e-mail: sunpeng@cuhk.edu.cn).

Haoxuan Che is with the School of Software, Northwestern Polytechnical University, Xi'an 710129, China (e-mail: chehx.cs@gmail.com).

Zhibo Wang is with the School of Cyber Science and Technology and the Key Laboratory of Blockchain and Cyberspace Governance of Zhejiang Province, Zhejiang University, Hangzhou 310027, China (e-mail: zhibowang@zju.edu.cn).

Yuwei Wang is with the State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China (e-mail: 3150103680@zju.edu.cn).

Tao Wang is with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China (e-mail: taowangnuaa@163.com).

Liantao Wu is with Shanghai Institute of Fog Computing Technology (SHIFT), ShanghaiTech University, Shanghai 201210, China (e-mail: wult@shanghaitech.edu.cn).

Huajie Shao is with the Department of Computer Science, College of William and Mary, Williamsburg, VA 23185 USA (e-mail: hshao@wm.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JSAC.2021.3118354.

Digital Object Identifier 10.1109/JSAC.2021.3118354

workers against these advanced privacy attacks, researchers have employed several privacy preservation mechanisms in FL, including homomorphic encryption (HE) [15], secure multi-party computation (MPC) [16], and differential privacy (DP) [17]. Note that DP-based techniques, where workers obfuscate local computation results by injecting random noises before sharing, are usually more favorable than HE and MPC schemes due to their rigorous privacy guarantee and easy implementation. Nevertheless, under DP with a normal privacy budget and query sensitivity, workers still sustain a certain degree of potential privacy disclosure, leading to privacy cost. The generated privacy cost would discourage self-interested workers from participating, which necessitates an efficient incentive mechanism.

Researchers have already developed several incentive mechanisms for FL thus far, using game theory (e.g., [18]–[20]), contract theory (e.g., [21]–[24]), and auction theory (e.g., [25], [26]). However, most of them mainly account for workers' resource cost (i.e., computational cost when computing model updates and communication cost when uploading updated model parameters or calculated gradients). Still, they largely neglect the cost induced by potential privacy leakage resulting from advanced inference attacks. Moreover, different workers generally demonstrate heterogeneous sensitivity levels towards the same degree of potential privacy leakage. That is, they deliver different privacy preferences [27]. More precisely, workers with higher privacy preferences would desire larger economic compensation than those with lower privacy preferences even when they are guarded with an identical privacy-preserving level (PPL).

To address these issues, this paper presents Pain-FL, a contract-based Personalized privacy-preserving incentive for Federated Learning. Pain-FL could provide personalized payments for workers with different privacy preferences as compensation for privacy cost while achieving desired convergence performance of model learning. Specifically, in each round of Pain-FL, a set of personalized contracts are first designed at the server under a given budget for workers with different privacy preferences. Each contract specifies a PPL and the corresponding payment that a worker will receive if he or she adopts that PPL for local perturbation. Each worker makes her independent decision to sign a customized contract with the server. Then, he or she computes stochastic gradients of the current global model downloaded from the server using a mini-batch randomly sampled from her local training data and then obfuscates the calculated gradients in accordance with the PPL specified in the signed contract. The server updates the global model following a gradient descent step by aggregating the perturbed stochastic gradients from all participating workers and redeems the corresponding payments to workers. The next round begins thereafter.

The design goal of Pain-FL is to derive a set of optimal contracts, which could optimize the convergence performance of both convex and non-convex FL models, under both complete information model, where the server knows each worker's particular privacy preference beforehand, and incomplete information model, where the server only knows the distribution of workers' privacy preferences. Meanwhile, the set of designed contracts could satisfy several desired economic properties, including the budget feasibility (BF) property ensuring that the total payments of the server do not exceed the system budget available, the individual rationality (IR) property ensuring that each worker's privacy cost is accordingly compensated, and the incentive compatibility (IC) property ensuring that workers would truthfully unveil their privacy preferences.

To summarize, this paper makes the following contributions:

- *Personalized Privacy-Preserving Incentive Mechanism Design:* To the best of our knowledge, this is one of the first analytical studies on personalized privacy-preserving incentive mechanism design for federated learning that customizes personalized privacy-preserving levels for workers, and explicitly measures and appropriately compensates workers' heterogeneous privacy costs.
- *Theoretical Analysis:* We quantitatively analyze each participating worker's PPL and privacy cost based on the variance of the injected Gaussian noise for gradient perturbation and her personalized privacy preference, by employing the notion of ρ-zero-concentrated differential privacy. We conduct rigorous convergence analysis of both strongly convex and non-convex loss functions, in the case where the global model is updated by aggregating heterogeneously perturbed stochastic gradients from participating workers.
- *Optimal Contract Design:* We formulate the optimal contract design problems under complete/incomplete information models. The problems are intractable to solve directly due to a significant number of constraints. We identify several inherent properties of them, which are used to simplify the problems. We analytically derive a set of optimal contracts which could maximize the global model accuracy while guaranteeing several desired economic properties (e.g., budget feasibility, individual rationality, and incentive compatibility).
- *Performance Evaluation:* We conduct an exhaustive experimental evaluation of Pain-FL on various models (convex and non-convex) and learning configurations (independent and identically distributed (IID) and Non-IID data partitions). The results corroborate its practicability and effectiveness.

The remainder of this paper is organized as follows: We summarize related works in Section II. Then, we provide preliminaries regarding federated learning and differential privacy in Section III. Section IV presents the framework and workflow of Pain-FL. Subsequently, in Section V, we quantitatively measure workers' PPL and privacy cost and conduct theoretical convergence analyses of Pain-FL to define the system design objective formally. Section VI elaborates on the design details of Pain-FL. Afterward, we conduct an exhaustive performance evaluation of Pain-FL in Section VII. Finally, Section VIII concludes the paper.

II. Related Work

FL [1], [7], [8] is becoming an increasingly popular distributed machine learning paradigm due to its promising performance in mitigating user privacy concerns. Nevertheless, recent works [10]–[14], [28] have demonstrated that FL is still susceptible to advanced inference attacks (e.g., reconstruction

attacks and membership inference attacks) launched by malicious (or honest but curious) servers/clients by exploiting the shared model updates. To thwart these privacy attacks, techniques including homomorphic encryption (HE) [15], secure multi-party computation (MPC) [16], and differential privacy (DP) [17] have been employed. These works put emphasis on the privacy preservation mechanism itself, while the privacy cost of workers participating in an FL task is not explicitly measured and compensated.

Another line of previous work, which is highly related to this paper, is a series of incentive mechanisms developed for FL, using game theory (e.g., [18]–[20]), contract theory (e.g., [21]–[24]), and auction theory (e.g., [25], [26]). Specifically, researchers in [25] developed an auction based incentive mechanism for FL in cellular wireless networks, where the interaction between the base station (i.e., buyer) and mobile users (i.e., sellers) was modeled as an auction game. To construct a high-quality statistical model through FL, authors in [18] formulated the cooperation between the parameter server and the participating clients as a two-stage stackelberg game, where each side maximizes its own utility. Similarly, a stackelberg game model was adopted in [19] to incentivize participation for FL in IoT applications. This designed incentive mechanism jointly studied the payoff maximization problem of the parameter server and a number of edge computing nodes in charge of several IoT devices. The authors derived the Nash equilibrium given the full knowledge of workers' contributions. In [23], researchers designed a contract-theoretic incentive mechanism, which integrated a reputation based worker selection scheme, in order to motivate high-reputation workers with high-quality data to participate in FL tasks. The work in [22] presented a contract-theoretic incentive mechanism for FL given workers with multi-dimensional private information including training cost and communication delay. The authors summarized workers' multi-dimensional private information with a single dimension metric and then analytically solved the server's optimal contract design problem.

Nonetheless, most of the existing incentive mechanisms for FL merely take workers' resource cost (i.e., computational cost and communication cost) into consideration, while the cost induced by potential privacy leakage resulting from advanced inference attacks has been largely neglected. In this work, instead, we quantitatively measure and compensate for workers' personalized privacy cost in undertaking FL tasks. Although the work in [29] started to account for workers' cost of privacy leakage, they employed a game-theoretic framework, where workers decide on the privacy budget by themselves. In contrast, in this work, we open a new avenue to capitalize on contract theory to design a personalized privacy-preserving incentive mechanism for FL. In our proposed framework, the server acts as the monopolist operator, as it directly determines the PPL and payment for each participating worker by customizing a contract for her.

III. Preliminaries

In this section, we introduce preliminaries and relevant background knowledge about FL and DP.

A. Federated Learning Basics

With the increasingly stringent privacy protection legislation and growing user privacy concerns, FL has gained considerable popularity. FL enables a number of clients (i.e., workers) to collaboratively train a shared machine learning model under the coordination of a central server without revealing their raw training data. Assume that there is a set $\mathcal{M}$ of M (i.e., $|\mathcal{M}| = M$) workers in total registered in the FL system. Each worker $m \in \mathcal{M}$ owns a private training dataset $\mathcal{D}_m = \left\{\left(\mathbf{x}_1^m, y_1^m\right), \ldots, \left(\mathbf{x}_{N_m}^m, y_{N_m}^m\right)\right\}$ including N_m data samples (i.e., $|\mathcal{D}_m| = N_m$), with $\mathbf{x}_n^m$ and y_n^m respectively denoting the feature vector and the corresponding label of the n-th training sample at worker m (without loss of generality, we assume that each data sample resides in a unit ball, which can be enforced through normalization). The goal of FL is to learn a globally shared machine learning model with parameter vector $\boldsymbol{\theta} \in \mathbb{R}^d$ by solving the following empirical risk minimization (ERM) problem

$$\min_{\boldsymbol{\theta}\in\mathbb{R}^d} \frac{1}{M} \sum_{m\in\mathcal{M}} f_m(\boldsymbol{\theta}) \text{ with } f_m(\boldsymbol{\theta}) := \frac{1}{N_m} \sum_{n=1}^{N_m} \ell\left(\mathbf{x}_n^m, y_n^m; \boldsymbol{\theta}\right), \tag{1}$$

where $\ell(\mathbf{x}, y; \boldsymbol{\theta}) : \Theta \rightarrow \mathbb{R}$ represents the loss function associated with the data sample $(\mathbf{x}, y)$ and the parameter vector $\boldsymbol{\theta}$, which is assumed to be continuously differentiable; $f_m(\boldsymbol{\theta})$ stands for the local loss function corresponding to $\boldsymbol{\theta}$ and all training data at worker m. For ease of exposition, we use the shorthand notation $f(\boldsymbol{\theta}) := \frac{1}{M}\sum_{m\in\mathcal{M}} f_m(\boldsymbol{\theta})$ to denote the global loss function.

Throughout this paper, we employ the classic and widely-adopted distributed stochastic gradient descent to solve the above ERM problem in Eq. (1). Generally, it requires a number of global iterations (i.e., communication rounds) between workers and the server to achieve a desired accuracy level of the learned global model $\boldsymbol{\theta}$. Specifically, in each communication round $t \in \{1, 2, \ldots, T\}$, the server distributes the latest global model (a random initialization of $\boldsymbol{\theta}_0$ at the very beginning) to all workers via broadcasting. Then, each worker calculates the stochastic gradient of the global model using a mini-batch $\mathcal{X}_m \subseteq \mathcal{D}_m$ of size X_m randomly sampled from her training dataset, and hereupon transmits the local computation result to the server. Upon receiving stochastic gradients from all participating workers, the server updates the global model following a gradient descent step as

$$\boldsymbol{\theta}^t = \boldsymbol{\theta}^{t-1} - \eta \sum_{m\in\mathcal{M}} g\left(\mathcal{X}_m; \boldsymbol{\theta}^{t-1}\right), \tag{2}$$

where the superscript t indexes the communication round, η is the learning rate. $g(\mathcal{X}_m; \boldsymbol{\theta}) = 1/X_m \sum_{(\mathbf{x}_n^m, y_n^m)\in\mathcal{X}_m} \nabla\ell\left(\mathbf{x}_n^m, y_n^m; \boldsymbol{\theta}\right)$ is the stochastic gradient computed based on a randomly sampled mini-batch $\mathcal{X}_m$ at worker m.

The interactions between workers and the server are repeated either for a pre-determined number of communication rounds T or until the global model converges.

B. Differential Privacy

While it allows private training data to remain local for each worker, FL does disclose sensitive information via shared model updates or gradients that are based on the training data. In FL systems, malicious workers or an honest but curious server may launch inference attacks to infer other parties' private information. For example, researchers in [11] demonstrated that the adversary could steal a worker's private images from shared gradients in just a few iterations via an optimization process. To safeguard workers against these privacy attacks, differential privacy (DP) techniques have been widely adopted [17]. DP is a rigorous mathematical framework wherein a randomized mechanism $\mathcal{A}$ is considered as differentially private if and only if the inclusion of a single instance in the training dataset causes statistically indistinguishable changes to the output of $\mathcal{A}$. Formally, DP is defined as follows:

Definition 1 ((ϵ, δ)-DP [30]): A randomized mechanism $\mathcal{A}: \mathcal{D} \to \mathcal{R}$ with domain $\mathcal{D}$ and range $\mathcal{R}$ is considered to satisfy (ϵ, δ)-DP if for any two adjacent datasets $D, D' \in \mathcal{D}$ that differ on at most one data sample and any subsets $\mathcal{S} \subseteq \mathcal{R}$, it satisfies that

$$\Pr[\mathcal{A}(D) \in \mathcal{S}] \leq e^{\epsilon} \Pr\left[\mathcal{A}\left(D'\right) \in \mathcal{S}\right] + \delta. \tag{3}$$

where ϵ is the privacy budget, and δ accounts for the probability that plain ϵ-DP is broken.

A popular mechanism to achieve (ϵ, δ)-DP is the Gaussian mechanism (denoted by $\mathcal{A}$). Specifically, given any function f that maps a dataset $D \in \mathcal{D}$ to a vector $\mathbf{o} \in \mathbb{R}^d$, we can achieve (ϵ, δ)-DP through adding Gaussian noises to each of the d coordinates of the output vector $\mathbf{o}$, i.e.,

$$\mathcal{A}(D) = f(D) + \mathcal{N}(0, \sigma^2 \mathbf{I}_d), \tag{4}$$

where $\mathcal{N}$ indicates the Gaussian distribution, $\mathbf{I}_d$ denotes the d-dimensional identity matrix, and the noise magnitude σ is proportional to the sensitivity of f, which is defined as $\Delta_f = \max_{D,D'} \|f\left(D\right) - f\left(D'\right)\|_2$.

Apart from (ϵ, δ)-DP, a number of alternative privacy notions have been proposed over the past years, one of which is ρ-zero-concentrated differential privacy (henceforth ρ-zCDP). The formal definition of ρ-zCDP is presented as below.

Definition 2 (ρ-zCDP [31]): A randomized mechanism $\mathcal{A}: \mathcal{D} \to \mathcal{R}$ with domain $\mathcal{D}$ and range $\mathcal{R}$ is considered to satisfy ρ-zCDP if for any two adjacent datasets $D, D' \in \mathcal{D}$ that differ on at most one data sample and all $\alpha \in (1, \infty)$, we have

$$\mathbb{E}\left[e^{(\alpha-1)Z}\right] \leq e^{(\alpha-1)(\rho\alpha)} \tag{5}$$

where $\mathbb{E}$ denotes the expectation operator, $Z = \text{PrivLoss}\left(\mathcal{A}(D) \| \mathcal{A}\left(D'\right)\right)$ is the privacy loss random variable defined below.

Definition 3 (Privacy Loss Random Variable): Let Y and Y' be random variables on $\mathcal{D}$, we define the privacy loss random variable between Y and Y', denoted by $Z = \text{PrivLoss}\left(Y \| Y'\right)$ as follows. Define a function $h: \mathcal{D} \to \mathcal{R}$ by $h(y) = \log(\Pr[Y = y] / \Pr[Y' = y])$. Then, Z is a random variable distributed according to $h(y)$.

Thus, the value of the privacy loss $Z = \text{PrivLoss}\left(\mathcal{A}(D) \| \mathcal{A}\left(D'\right)\right)$ represents how well we can distinguish D from D' given only the output $\mathcal{A}(D)$ or $\mathcal{A}(D')$. A larger value of Z means more significant differences between $\mathcal{A}(D)$ and $\mathcal{A}(D')$, which helps better distinguish D from D', i.e., less privacy protection.

Following the same analysis method in [31], [32], based on the definition of privacy loss random variable Z, a randomized mechanism $\mathcal{A}$ satisfying (ϵ, δ)-DP is equivalent, up to a small loss in parameters, to the requirement that $\Pr[Z > \epsilon] \leq \delta$.

As shown in Definition 2, ρ-zCDP entails a bound on the moment generating function of the privacy loss Z (i.e., $\mathbb{E}\left[e^{(\alpha-1)Z}\right]$). The bound (5) implies that Z is a *subgaussian* random variable with small mean, which intuitively resembles a Gaussian distribution with mean ρ and variance 2ρ. Thus, the parameter ρ can be employed to indicate the privacy-preserving level (PPL). Clearly, a smaller value of ρ implies a higher PPL. In particular, according to the definition and properties of *subgaussian* random variables [33], from the bound (5) we have $\Pr[Z > \lambda + \rho] \leq e^{-\lambda^2/4\rho}$ for all $\lambda > 0$.

Consider the case where $\rho = \epsilon$ and $\lambda = \sqrt{\epsilon}$, we have $\Pr[Z > \sqrt{\epsilon} + \epsilon] \leq e^{-1/4}$. Therefore, ρ-zCDP is clearly weaker than (ϵ, δ)-DP because the probability of privacy loss exceeding $\sqrt{\epsilon} + \epsilon$ can be constant in the former but the probability of privacy loss exceeding ϵ is only δ, which is tiny, in the latter. Thus, we would say that ρ-zCDP is a relaxed version of (ϵ, δ)-DP. This relaxed version has a tight composition bound and is more suitable to track and analyze the overall privacy loss of iterative algorithms. We introduce the following property of ρ-zCDP [31], which will be utilized in our subsequent privacy analysis in Section V.

Lemma 1 (Gaussian Mechanism): The Gaussian mechanism (i.e., Eq. (4)) satisfies $\Delta_f^2/2\sigma^2$-zCDP (i.e., $\rho = \Delta_f^2/2\sigma^2$), where σ^2 is the noise variance and Δ_f is the query sensitivity.

IV. System Framework

The FL system considered in this paper consists of a honest but curious central server, which may infer workers' private information, and a set $\mathcal{M}$ of M (i.e., $|\mathcal{M}| = M$) workers. Assume that each worker $m \in \mathcal{M}$ owns a private training dataset $\mathcal{D}_m$ including N_m data samples (i.e., $|\mathcal{D}_m| = N_m$), and each data sample contains the feature vector and its corresponding label. The goal of the server is to recruit a sufficient number of workers to collaboratively train a high-quality machine learning model without requesting their raw training data. The framework of Pain-FL is depicted in Fig. 1, and the workflow in each communication round is described as follows. (The following steps are repeated until the pre-determined number of communication rounds is reached or the global model converges to a desired accuracy level.)

1) The server designs a set of personalized contracts (each contract is a PPL-payment bundle) under a given budget for the current communication round, which could optimize learning performance, while guaranteeing IR and IC properties (step ①).

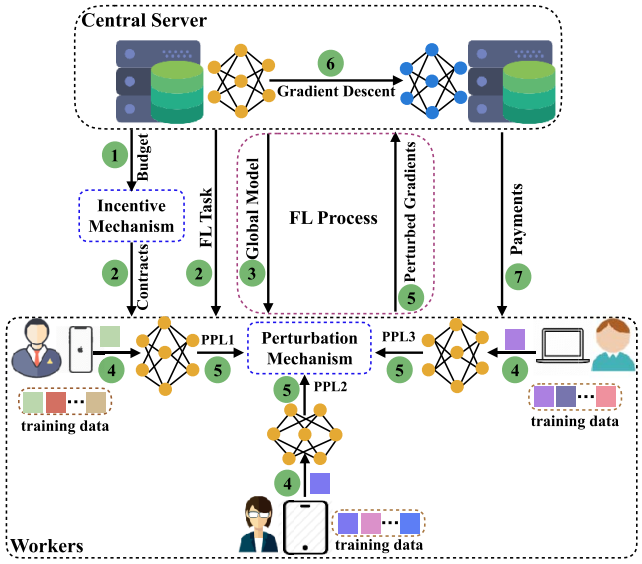

Fig. 1. Framework of Pain-FL (where circled numbers represent the sequence of the events in each communication round).

2) The server publicizes the set of designed contracts along with the FL task to workers registered in the system (i.e., $\mathcal{M}$). Each worker $m \in \mathcal{M}$ makes her own decision to sign one specific contract with the server to maximize her utility, which will be defined in Section V (step ②).
3) Each participating worker $m \in \mathcal{M}$ downloads the latest global model from the server (step ③).
4) Each worker $m \in \mathcal{M}$ computes the stochastic gradient of the current global model using a mini-batch $\mathcal{X}_m \subseteq \mathcal{D}_m$ of size X_m from her training dataset (step ④).
5) Then, each worker $m \in \mathcal{M}$ perturbs her calculated stochastic gradient using the Gaussian mechanism, where the noise level is determined by the PPL specified in the signed contract, and subsequently uploads the perturbed stochastic gradient to the server. (step ⑤).
6) The server updates the global model following a gradient descent procedure by aggregating (i.e., averaging) the heterogeneously perturbed stochastic gradients from all the participating workers (step ⑥).
7) Upon accomplishing the global model update, the server redeems the payment for each worker according to the valuation specified in the signed contract (step ⑦).

There are two critical concerns in Pain-FL. On one hand, each participating worker's personalized privacy cost should be appropriately compensated for. On the other hand, under a given budget, the finally learned global model should achieve a desired accuracy level. Hence, in the next section, we respectively conduct theoretical analyses from the perspectives of worker privacy and model convergence performance.

V. Theoretical Analysis: Privacy Versus Convergence Performance

In this section, we first quantitatively analyze workers' PPL and privacy cost, and then conduct rigorous convergence analyses of Pain-FL for both convex and non-convex machine learning models.

A. Privacy Analysis

In this part, we leverage the notion of ρ-zCDP to quantify each worker's PPL, with which we explicitly measure her privacy cost by incorporating her personalized privacy preference.

To thwart privacy attacks via shared gradients, each participating worker adopts the Gaussian mechanism to obfuscate the calculated stochastic gradient before transmission. Formally,

$$\tilde{g}\left(\mathcal{X}_m;\boldsymbol{\theta}\right) = g\left(\mathcal{X}_m;\boldsymbol{\theta}\right) + \mathbf{b}_m, \tag{6}$$

where $\boldsymbol{\theta} \in \mathbb{R}^d$ is the current global model, $\mathcal{X}_m$ is a mini-batch of size X_m from the local training data of worker m, $g\left(\mathcal{X}_m;\boldsymbol{\theta}\right)$ (or g for short) is the calculated stochastic gradient, $\mathbf{b}_m \sim \mathcal{N}\left(0, \sigma_m^2 \mathbf{I}_d\right)$ is the injected Gaussian noise. After local gradient perturbation, the update of the global model $\boldsymbol{\theta}$ is implemented as

$$\begin{aligned}\boldsymbol{\theta}^t &= \boldsymbol{\theta}^{t-1} - \eta \sum_{m\in\mathcal{M}} \tilde{g}\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right) \\ &= \boldsymbol{\theta}^{t-1} - \eta \sum_{m\in\mathcal{M}} \left(g\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right) + \mathbf{b}_m\right).\end{aligned} \tag{7}$$

Note that in this paper we assume that the injected noise into each coordinate of the gradient is sampled from the same Gaussian distribution (i.e., the same noise level for all coordinates), and leave the study of the scenario where different noise levels are used for different coordinates in our future work. Finally, $\tilde{g}\left(\mathcal{X}_m;\boldsymbol{\theta}\right)$ (or $\tilde{g}$ for short) is the perturbed stochastic gradient. Intuitively, worker m's acquired PPL is related to the injected noise. In particular, when the variance σ_m^2 of the Gaussian noise adopted by worker m is larger, there is a higher probability for the magnitude of $\mathbf{b}_m$ to be large, and thus a higher PPL is expected.

We link the noise variance σ_m^2 to the obtained PPL ρ_m with regard to worker m in the theorem below.

Theorem 1: In each round of FL, using the Gaussian mechanism (i.e., Eq. (6)) for gradient perturbation, worker m achieves ρ_m-zCDP, and the explicit relationship between ρ_m and the adopted noise variance σ_m^2 is represented as $\rho_m = \frac{2L^2}{X_m^2\sigma_m^2}$.

Proof: Suppose $\mathcal{X}_m$ and $\mathcal{X}'_m$ are two neighboring mini-batches of worker m, which are of the same size X_m and differ only on the j-th data sample. Then, the sensitivity of the stochastic gradient function taking as input $\mathcal{X}_m$ and $\mathcal{X}'_m$ is computed as

$$\begin{aligned}\Delta_g &= \max_{\mathcal{X}_m,\mathcal{X}'_m} \left\|g\left(\mathcal{X}_m;\boldsymbol{\theta}\right) - g\left(\mathcal{X}'_m;\boldsymbol{\theta}\right)\right\|_2 \\ &= \max_{\mathcal{X}_m,\mathcal{X}'_m} \frac{1}{X_m} \left\| \sum_{\mathbf{x}\in\mathcal{X}_\mathbf{m}} \nabla\ell(\mathbf{x};\boldsymbol{\theta}) - \sum_{\mathbf{x}\in\mathcal{X}'_\mathbf{m}} \nabla\ell(\mathbf{x};\boldsymbol{\theta}) \right\|_2 \\ &= \max_{\mathcal{X}_m,\mathcal{X}'_m} \frac{1}{X_m} \left\|\nabla\ell\left(\mathbf{x_j};\boldsymbol{\theta}\right) - \nabla\ell\left(\mathbf{x'_j};\boldsymbol{\theta}\right)\right\|_2.\end{aligned} \tag{8}$$

Assume the stochastic gradient function $\nabla\ell(\cdot)$ is L-Lipschitz continuous (we will present the formal definition

of Lipschitz continuity in the next subsection), we have

$$\left\|\nabla \ell\left(\mathbf{x_j};\boldsymbol{\theta}\right)-\nabla \ell\left(\mathbf{x_j'};\boldsymbol{\theta}\right)\right\|_2 \leq L\left\|\mathbf{x_j}-\mathbf{x_j'}\right\|_2. \tag{9}$$

Without loss of generality, the training data of worker m can be normalized into a unit ball, then the sensitivity of the stochastic gradient at worker m is $\Delta_g = \frac{2L}{X_m}$. According to Lemma 1, when worker m adopts a Gaussian noise with variance σ_m^2 for gradient perturbation, the obtained PPL ρ_m in each communication round is computed as $\frac{2L^2}{X_m^2\sigma_m^2}$. ■

As stated in Theorem 1, in a specific communication round, when worker m decides to sign a contract specifying a PPL ρ_m with the server, she would adopt the Gaussian noise with the variance of $\sigma_m^2 = \frac{2L^2}{\rho_m X_m^2}$ accordingly for gradient perturbation in this round. Specifically, if worker m signs a contract specifying a higher PPL (i.e., a smaller ρ_m), she will perturb her local stochastic gradient using a Gaussian noise with a larger variance. Throughout the FL process, to ensure that each worker chooses the noise variance in strict accordance with the PPL specified in the signed contract, a trusted specialized app could be installed on workers' smart mobile devices [34]. In this case, once a contract is signed between a worker and the server, the noise variance adopted by the worker could be controlled by the installed app. Thus, the actual PPL of each worker could be monitored by the server. Note that Theorem 1 applies to each worker $m \in \mathcal{M}$ as they all adopt the same Gaussian mechanism in Eq. (6).

After quantifying workers' PPL in each communication round, we can derive their privacy cost. Evidently, a worker's privacy cost is related to her obtained PPL, and a lower PPL (i.e., a higher degree of privacy leakage) leads to higher privacy cost. In other words, the privacy cost of worker m, denoted by $C_m(\rho_m)$, is positively correlated with the privacy parameter ρ_m. Moreover, $C_m(\rho_m)$ is also dependent on her privacy preference, which indicates how sensitive about privacy leakage she is. Without loss of generality, in this paper, we adopt the linear privacy cost function [35], i.e., $C_m(\rho_m) = c_m\rho_m$, where c_m indicates the cost of unit privacy leakage for worker m, which is referred to as her personalized privacy preference. Based on the above analysis, a worker's utility in each communication round can be defined as follows.

Definition 4 (Worker Utility): In a specific communication round of the launched FL task, if worker m chooses to sign the contract, which specifies the payment r_m to her if she uploads perturbed stochastic gradient with the PPL ρ_m, with the server, then the utility of worker m (denoted by u_m) for participating in this round of model training, is calculated as

$$u_m = r_m - c_m\rho_m. \tag{10}$$

It is worth noting that although we only consider privacy cost when defining worker utility in Eq. (10), the results reported in this paper can be easily adapted to the case where workers' resource cost is incorporated. Specifically, if we denote the resource cost of worker m for participating in one round of FL model training by q_m, her obtained utility in this round is calculated as $u_m = r_m - q_m - c_m\rho_m$, which can then be reformulated as $u_m = r_m{}' - c_m\rho_m$ if we define $r_m{}' = r_m - q_m$, and this is equivalent to Eq. (10).

B. Convergence Analysis

In this part, we conduct rigorous convergence analyses of Pain-FL for both convex and non-convex machine learning models, in order to link the performance of the finally learned global model to workers' PPLs.

Our subsequent convergence analyses of Pain-FL rely on several assumptions on the global loss function $f(\cdot)$. With the assumptions that the sample-wise loss function $\ell(\cdot)$ is continuously differentiable and that the stochastic gradient $\nabla\ell(\cdot)$ is G-Lipschitz continuous, it is reasonable for us to make the following Assumptions 1 and 2 given the ERM problem formulation in Eq. (1).

Assumption 1 (Lipschitz-Continuity): The overall loss function $f(\boldsymbol{\theta}) : \mathbb{R}^d \to \mathbb{R}$ is continuously differentiable and its corresponding gradient function $\nabla f(\boldsymbol{\theta})$ is Lipschitz continuous with Lipschitz constant $L > 0$, i.e.,

$$\|\nabla f(\boldsymbol{\theta}_1) - \nabla f(\boldsymbol{\theta}_2)\|_2 \leq L\|\boldsymbol{\theta}_1 - \boldsymbol{\theta}_2\|_2 \ \forall \boldsymbol{\theta}_1, \boldsymbol{\theta}_2 \in \mathbb{R}^d. \tag{11}$$

Moreover, for all $\boldsymbol{\theta}_1, \boldsymbol{\theta}_2 \in \mathbb{R}^d$, we also have [36]

$$f(\boldsymbol{\theta}_1) \leq f(\boldsymbol{\theta}_2) + \nabla f(\boldsymbol{\theta}_2)^T(\boldsymbol{\theta}_1 - \boldsymbol{\theta}_2) + \frac{1}{2}L\|\boldsymbol{\theta}_1 - \boldsymbol{\theta}_2\|_2^2. \tag{12}$$

Assumption 2 (First and Second Moment Limits): The overall loss function $f(\boldsymbol{\theta})$ ($f(\cdot)$ for short) and the stochastic gradients satisfy the following:

a) The sequence of iterates $\{\boldsymbol{\theta}^t\}$ is contained in an open set over which $f(\cdot)$ is bound below by a scalar f_{inf}.

b) There exist scalars $\mu_G \geq \mu > 0$ such that, for all $t \in \mathbb{N}$ and each worker $m \in \mathcal{M}$,

$$\nabla f(\boldsymbol{\theta}^t)^T\mathbb{E}[g(\mathcal{X}_m;\boldsymbol{\theta}^t)] \geq \mu\|\nabla f(\boldsymbol{\theta}^t)\|_2^2 \quad and \tag{13}$$

$$\|\mathbb{E}[g(\mathcal{X}_m;\boldsymbol{\theta}^t)]\|_2 \ \leq \mu_G\|\nabla f(\boldsymbol{\theta}^t)\|_2. \tag{14}$$

c) There exist scalars $M_\mu \geq 0$ and $M_V \geq 0$ such that, for all $t \in \mathbb{N}$ and each worker $m \in \mathcal{M}$, the variance of $g(\mathcal{X}_m;\boldsymbol{\theta}^t)$, i.e., $\mathbb{V}[g(\mathcal{X}_m;\boldsymbol{\theta}^t)] = \mathbb{E}[\|g(\mathcal{X}_m;\boldsymbol{\theta}^t)\|_2^2] - \|\mathbb{E}[g(\mathcal{X}_m;\boldsymbol{\theta}^t)]\|_2^2$

$$\mathbb{V}[g(\mathcal{X}_m;\boldsymbol{\theta}^t)] \leq M_\mu + M_V\|\nabla f(\boldsymbol{\theta}^t)\|_2^2. \tag{15}$$

1) Convex Setting: We first consider the most benign setting, where the loss function $f(\cdot)$ is assumed to be strongly convex. We formalize a strong convexity assumption as below.

Assumption 3 (Strong Convexity): The overall loss function $f : \mathbb{R}^d \to \mathbb{R}$ is strongly convex in that there exists a constant $c > 0$ such that for all $\boldsymbol{\theta}_1, \boldsymbol{\theta}_2 \in \mathbb{R}^d$, we have

$$f(\boldsymbol{\theta}_2) \geq f(\boldsymbol{\theta}_1) + \nabla f(\boldsymbol{\theta}_1)^T(\boldsymbol{\theta}_2 - \boldsymbol{\theta}_1) + \frac{1}{2}c\|\boldsymbol{\theta}_2 - \boldsymbol{\theta}_1\|_2^2. \tag{16}$$

Hence, f has a unique minimizer, denoted as $\boldsymbol{\theta}^* \in \mathbb{R}^d$ with $f^* := f(\boldsymbol{\theta}^*)$.

Under Assumption 3, we could derive a useful result that the optimality gap at a given iterate $\boldsymbol{\theta}$ is upper bounded in terms of the squared ℓ_2-norm of the gradient of the loss function at that iterate [36], i.e.,

$$2c(f(\boldsymbol{\theta}) - f^*) \leq \|\nabla f(\boldsymbol{\theta})\|_2^2 \ \ \forall \boldsymbol{\theta} \in \mathbb{R}^d. \tag{17}$$

Before presenting the convergence result of strongly convex statistical models, we introduce the following lemma.

Lemma 2: The expectation of the squared ℓ_2-norm of the summation of the stochastic gradients computed by all workers $m \in \mathcal{M}$ satisfies that

$$\mathbb{E}[\| \sum_{m\in\mathcal{M}} g\left(\mathcal{X}_m;\boldsymbol{\theta}^t\right)\|_2^2] \le M^2(M_\mu + M_G\|\nabla f(\boldsymbol{\theta}^t)\|_2^2). \quad (18)$$

where $t \in \mathbb{N}$, M is the number of participating workers, and

$$M_G := \mu_G^2 + M_V. \quad (19)$$

where μ_G, M_μ, M_V are constants defined in Assumption 2.

Proof: Based on fundamental inequalities, we have

$$\begin{aligned}&\mathbb{E}[\|\frac{1}{M}\sum_{m\in\mathcal{M}} g\left(\mathcal{X}_m;\boldsymbol{\theta}^t\right)\|_2^2]\\ &= \frac{1}{M^2}\mathbb{E}[\|\sum_{m\in\mathcal{M}} g\left(\mathcal{X}_m;\boldsymbol{\theta}^t\right)\|_2^2]\\ &\le \frac{1}{M}\mathbb{E}[\sum_{m\in\mathcal{M}}\left\|g\left(\mathcal{X}_m;\boldsymbol{\theta}^t\right)\right\|_2^2] = \frac{1}{M}\sum_{m\in\mathcal{M}}\mathbb{E}[\left\|g\left(\mathcal{X}_m;\boldsymbol{\theta}^t\right)\right\|_2^2].\end{aligned} \quad (20)$$

Then, according to the definition of $\mathbb{V}[g(\mathcal{X}_m;\boldsymbol{\theta}^t)]$ in Assumption 2(c), we have

$$\begin{aligned}&\frac{1}{M}\sum_{m\in\mathcal{M}}\mathbb{E}[\left\|g\left(\mathcal{X}_m;\boldsymbol{\theta}^t\right)\right\|_2^2]\\ &\quad= \frac{1}{M}\sum_{m\in\mathcal{M}}\left(\|\mathbb{E}[g(\mathcal{X}_m;\boldsymbol{\theta}^t)]\|_2^2 + \mathbb{V}_{\mathcal{X}_m}[g(\mathcal{X}_m;\boldsymbol{\theta}^t)]\right).\end{aligned} \quad (21)$$

Finally, from Assumption 2(b)(c) we obtain

$$\begin{aligned}&\mathbb{E}[\|\frac{1}{M}\sum_{m\in\mathcal{M}} g\left(\mathcal{X}_m;\boldsymbol{\theta}^t\right)\|_2^2]\\ &\quad\le \frac{1}{M}\sum_{m\in\mathcal{M}}\left(M_\mu + (\mu_G^2 + M_V)\|\nabla f(\boldsymbol{\theta}^t)\|_2^2\right)\\ &\quad= M_\mu + M_G\|\nabla f(\boldsymbol{\theta}^t)\|_2^2,\end{aligned} \quad (22)$$

which is equivalent to Eq. (18). ∎

We now state the convergence theorem of Pain-FL, describing its behavior when minimizing a strongly convex objective function with a fixed learning rate.

Theorem 2: Under Assumptions 1, 2, 3 (with $f_{inf} = f^*$), suppose the global model $\boldsymbol{\theta}$ is updated according to Eq. (7) with a fixed learning rate η satisfying that

$$0 < \eta \le \frac{\mu}{LM_G}. \quad (23)$$

Then, the expected optimality gap satisfies the following inequality for a pre-determined number of communication rounds T

$$\mathbb{E}[f(\boldsymbol{\theta}^T)] - f^* \le (1-(1-\eta\mu c)^T)\Phi + (1-\eta\mu c)^T\left(f(\boldsymbol{\theta}^0) - f^*\right), \quad (24)$$

where $(1-(1-\eta\mu c)^T) \in (0,1]$ and

$$\Phi := \frac{L\eta(M^2M_\mu + d\sum_{m\in\mathcal{M}}\sigma_m^2)}{2\mu M^2 c}. \quad (25)$$

Moreover, when T is sufficiently large, we have

$$\mathbb{E}[f(\boldsymbol{\theta}^T)] - f^* \le \Phi. \quad (26)$$

Proof: Under Assumption 1 (in particular Eq. (12)), the iterates generated based on the update rule in Eq. (7) satisfy the following inequalities for all $t \in \{1, 2, \ldots, T\}$

$$\begin{aligned}f(\boldsymbol{\theta}^t) - f(\boldsymbol{\theta}^{t-1}) \le \nabla f(\boldsymbol{\theta}^{t-1})^T\left(-\frac{\eta}{M}\sum_{m\in\mathcal{M}}\tilde{g}\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right)\right)\\ +\frac{1}{2}L\|-\frac{\eta}{M}\sum_{m\in\mathcal{M}}\tilde{g}\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right)\|_2^2.\end{aligned} \quad (27)$$

Since the injected Gaussian noises $\mathbf{b}_m \sim \mathcal{N}\left(0, \sigma_m^2\mathbf{I}_d\right)$ at each worker $m \in \mathcal{M}$ are independent, and $\mathbf{b}_m$ is independent of $\sum_{m\in\mathcal{M}} g\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right)$, we have

$$\mathbb{E}[\mathbf{b}_m] = \mathbf{0}, \quad (28)$$

$$\mathbb{E}[\|\sum_{m\in\mathcal{M}}\mathbf{b}_m\|_2^2] = \sum_{m\in\mathcal{M}}\mathbb{E}[\|\mathbf{b}_m\|_2^2] = d\sum_{m\in\mathcal{M}}\sigma_m^2, \quad (29)$$

$$\mathbb{E}[\mathbf{b}_m^T\sum_{m\in\mathcal{M}} g\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right)] = \mathbb{E}[\mathbf{b}_m]^T\mathbb{E}[\sum_{m\in\mathcal{M}} g\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right)] = 0. \quad (30)$$

Taking expectations in Eq. (27) with respect to the distribution of $\mathcal{X}_m$, we obtain

$$\begin{aligned}&\mathbb{E}[f(\boldsymbol{\theta}^t)] - f(\boldsymbol{\theta}^{t-1})\\ &\le -\frac{\eta}{M}\nabla f(\boldsymbol{\theta}^{t-1})^T\left(\sum_{m\in\mathcal{M}}\mathbb{E}[g\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right)] + \sum_{m\in\mathcal{M}}\mathbb{E}[\mathbf{b}_m]\right)\\ &\quad+\frac{L\eta^2}{2M^2}\left(\mathbb{E}[\|\sum_{m\in\mathcal{M}} g\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right)\|_2^2] + \mathbb{E}[\|\sum_{m\in\mathcal{M}}\mathbf{b}_m\|_2^2]\right)\\ &\quad+\frac{L\eta^2}{M^2}\mathbb{E}[\sum_{m\in\mathcal{M}}\mathbf{b}_m^T\sum_{m\in\mathcal{M}} g\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right)].\end{aligned} \quad (31)$$

Then, based on Eq. (28), Eq. (29), and Eq. (30), we have

$$\begin{aligned}&\mathbb{E}[f(\boldsymbol{\theta}^t)] - f(\boldsymbol{\theta}^{t-1})\\ &\le -\frac{\eta}{M}\nabla f(\boldsymbol{\theta}^{t-1})^T\left(\sum_{m\in\mathcal{M}}\mathbb{E}[g\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right)]\right)\\ &\quad+\frac{L\eta^2}{2M^2}\left(\mathbb{E}[\|\sum_{m\in\mathcal{M}} g\left(\mathcal{X}_m;\boldsymbol{\theta}^{t-1}\right)\|_2^2] + d\sum_{m\in\mathcal{M}}\sigma_m^2\right).\end{aligned} \quad (32)$$

It follows from Assumption 2, Eq. (17), and Lemma 2 that

$$\begin{aligned}&\mathbb{E}[f(\boldsymbol{\theta}^t)] - f(\boldsymbol{\theta}^{t-1})\\ &\le \frac{L\eta^2}{2M^2}(M^2M_\mu + d\sum_{m\in\mathcal{M}}\sigma_m^2)\\ &\quad-(\eta\mu - \frac{L\eta^2\ M_G}{2})\|\nabla f(\boldsymbol{\theta}^{t-1})\|_2^2\\ &\le -\frac{1}{2}\eta\mu\|\nabla f(\boldsymbol{\theta}^{t-1})\|_2^2 + \frac{L\eta^2}{2M^2}(M^2M_\mu + d\sum_{m\in\mathcal{M}}\sigma_m^2)\\ &\le -\eta\mu c\left(f(\boldsymbol{\theta}^{t-1}) - f^*\right) + \frac{L\eta^2}{2M^2}(M^2M_\mu + d\sum_{m\in\mathcal{M}}\sigma_m^2).\end{aligned} \quad (33)$$

Defining Φ as in Eq. (25), subtracting $(f^* + \Phi)$ from both sides of Eq. (33), taking expectations, and rearranging, yields

$$\mathbb{E}[f(\boldsymbol{\theta}^t) - f^*] - \Phi \leq (1 - \eta\mu c)\left(\mathbb{E}[f(\boldsymbol{\theta}^{t-1}) - f^*] - \Phi\right). \tag{34}$$

Applying Eq. (34) repeatedly through iterations $t \in \{1, 2, \ldots, T\}$ (i.e., $\boldsymbol{\theta}^0$ to $\boldsymbol{\theta}^T$), and rearranging, we obtain

$$\mathbb{E}[f(\boldsymbol{\theta}^T)] - f^* \leq (1 - (1 - \eta\mu c)^T)\Phi + (1 - \eta\mu c)^T\left(f(\boldsymbol{\theta}^0) - f^*\right). \tag{35}$$

Since we have $\mu_G \geq \mu > 0$ in Assumption 2(b), then

$$M_G = \mu_G^2 + M_V \geq \mu^2. \tag{36}$$

Moreover, since the inequality (16) should not be conflicting with the inequality (12), we have $c \leq L$. Then, according to Eq. (23) and Eq. (36), it is obvious that

$$0 < \eta\mu c \leq \frac{\mu^2 c}{M_G L} \leq \frac{\mu^2 c}{\mu^2 L} = \frac{c}{L} \leq 1. \tag{37}$$

Therefore, we have $0 < (1 - (1 - \eta\mu c)^T) \leq 1$. ■

2) Non-Convex Setting: Considering that many useful machine learning models (e.g., deep neural networks) lead to non-convex objective functions, we thus investigate the convergence property of Pain-FL in non-convex setting in this subsection. Different from the convex case where the expected optimality gap is employed to measure the convergence rate, we leverage the expected average-squared ℓ_2-norm of gradients of f after T communication rounds (i.e., $\mathbb{E}[\frac{1}{T}\sum_{t=1}^{T}\|\nabla f(\boldsymbol{\theta}^t)\|_2^2]$) as an indicator of convergence performance in the non-convex setting. With the same assumptions on stochastic gradients $g\left(\mathcal{X}_m; \boldsymbol{\theta}^t\right)$ except that on strong convexity of $f(\cdot)$, we have the following result.

Theorem 3: Under Assumptions 1, 2 (with $f_{inf} = f^*$), suppose that the global model $\boldsymbol{\theta}$ is updated according to Eq. (7) with a fixed learning rate η satisfying that

$$0 < \eta \leq \frac{\mu}{LM_G}. \tag{38}$$

Then, the expected average-squared ℓ_2-norm of gradients of f satisfies the following inequality for a pre-determined number of communication rounds T

$$\mathbb{E}[\frac{1}{T}\sum_{t=0}^{T-1}\|\nabla f(\boldsymbol{\theta}^t)\|_2^2] \leq \frac{2(f(\boldsymbol{\theta}^0) - f^*)}{T\eta\mu} + \Psi, \tag{39}$$

where

$$\Psi := \frac{L\eta(M^2\ M_\mu + d\sum_{m\in\mathcal{M}}\sigma_m^2)}{\mu M^2}. \tag{40}$$

Proof: Under the same requirement on the learning rate η, we know from the proof of Theorem 2 that

$$\mathbb{E}[f(\boldsymbol{\theta}^t)] - \mathbb{E}[f(\boldsymbol{\theta}^{t-1})] \leq -\frac{1}{2}\eta\mu\mathbb{E}[\|\nabla f(\boldsymbol{\theta}^{t-1})\|_2^2] + \frac{L\eta^2}{2M^2}(M^2 M_\mu + d\sum_{m\in\mathcal{M}}\sigma_m^2). \tag{41}$$

Summing both sides of the above inequality for $t \in \{1, 2, \ldots, T\}$ and recalling Assumption 2(a) gives

$$\begin{aligned} f^* - f(\boldsymbol{\theta}^0) &\leq \mathbb{E}[f(\boldsymbol{\theta}^T)] - f(\boldsymbol{\theta}^0) \\ &\leq -\frac{1}{2}\eta\mu\mathbb{E}[\sum_{t=1}^{T}\|\nabla f(\boldsymbol{\theta}^{t-1})\|_2^2] \\ &\quad + \frac{TL\eta^2}{2M^2}(M^2 M_\mu + d\sum_{m\in\mathcal{M}}\sigma_m^2). \end{aligned} \tag{42}$$

Rearranging yields

$$\mathbb{E}[\frac{1}{T}\sum_{t=0}^{T-1}\|\nabla f(\boldsymbol{\theta}^t)\|_2^2] \leq \frac{2(f(\boldsymbol{\theta}^0) - f^*)}{T\eta\mu} + \frac{L\eta(M^2\ M_\mu + d\sum_{m\in\mathcal{M}}\sigma_m^2)}{\mu M^2}, \tag{43}$$

which is equivalent to (39) given (40). ■

As shown in Theorem 2 and Theorem 3, for both convex and non-convex models, the convergence performance of the finally learned global model is related to $\sum_{m\in\mathcal{M}}\sigma_m^2$, where σ_m^2 is the variance of the injected Gaussian noise at worker m for gradient perturbation. Therefore, we have two conflicting objectives. On one hand, we aim to minimize $\sum_{m\in\mathcal{M}}\sigma_m^2$ to achieve satisfactory model performance. On the other hand, workers tend to inject Gaussian noises with larger variances to pursue higher PPLs. In the next section, we present our contract-based incentive mechanism to reconcile this conflict.

VI. Design Details of Pain-FL

In this section, we elaborate on the design details of Pain-FL. Specifically, we first formally define the design objective of Pain-FL, and then we respectively derive a set of optimal contracts analytically under two information models, i.e., complete information model and incomplete information model.

A. Design Objective

Without loss of generality, it is assumed in this paper that all workers can be classified into K privacy groups according to their privacy preferences, and that the number of workers in the k-th privacy group is m_k (i.e., $\sum_{k=1}^{K} m_k = M$). We denote the privacy preference of workers in the k-th ($1 \leq k \leq K$) privacy group by c_k, and the privacy preferences of workers in the K different privacy groups can be sorted in ascending order, i.e.,

$$c_1 < c_2 < \cdots < c_K. \tag{44}$$

In a nutshell, the design objective of Pain-FL is to derive a set of optimal contracts $\{(\rho_1^*, r_1^*), (\rho_2^*, r_2^*), \ldots, (\rho_K^*, r_K^*)\}$ for workers in all K privacy groups, which could maximize the accuracy of the finally learned global model $\boldsymbol{\theta}$. In order to maximize the global model accuracy, we resort to minimizing the upper bounds derived in Theorem 2 and Theorem 3 for convex and non-convex models, respectively. In particular, for a pre-determined number of communication rounds T, a given

number of participating workers M, a fixed learning rate η, a given model size d (the number of model parameters), along with all the constants including μ, c, $f(\boldsymbol{\theta}^0)$, f^*, L, M_μ, we could turn to minimizing the noise term in Φ and Ψ, i.e., $\sum_{m\in\mathcal{M}}\sigma_m^2$ for an optimized model performance regardless of the convexity of the loss function f. This is equivalent to minimizing $\sum_{m\in\mathcal{M}}\frac{2L^2}{\rho_m X_m^2}$ recalling Theorem 1. Without loss of generality, we assume that the mini-batches used by each worker $m\in\mathcal{M}$ for computing stochastic gradients are of the same fixed size (i.e., X_m is a constant across workers and iterations). Thus, finally, we are aimed at minimizing $\sum_{m\in\mathcal{M}}\frac{1}{\rho_m}$. Besides, the set of designed contracts need to satisfy the following three economic properties.

Firstly, the server could only afford a given system budget in each communication round. Thus, the first property that needs to be guaranteed is the budget feasibility defined in Definition 5.

Definition 5 (Budget Feasibility (BF)): A set of contracts is budget feasible, if and only if the total payment for all participating workers does not exceed the budget B, i.e.,

$$\sum\nolimits_{m\in\mathcal{M}} r_m \le B. \tag{45}$$

Secondly, in order not to discourage workers from participating, it is necessary for the set of contracts to satisfy the individual rationality, defined in Definition 6.

Definition 6 (Individual Rationality (IR)): A set of contracts is considered to satisfy IR if they provide workers in any privacy groups with non-negative utility, i.e.,

$$r_k - c_k\rho_k \ge 0,\ (1\le k\le K)\,. \tag{46}$$

Lastly, the set of contracts should satisfy the incentive compatibility, defined in Definition 7, which ensures that selfish and strategic workers cannot gain more utility by falsifying their privacy groups (i.e., privacy preferences).

Definition 7 (Incentive Compatibility (IC)): A set of contracts is considered to satisfy IC if they ensure that workers in the k-th privacy group achieve larger utility when they sign the contract (ρ_k, r_k) customized for the privacy group they belong to than signing contracts $(\rho_{k'}, r_{k'})$ $(k'\neq k)$ designed for other privacy groups, i.e.,

$$r_k - c_k\rho_k \ge r_{k'} - c_k\rho_{k'},\ (1\le k\,,k'\le K, k\neq k')\,. \tag{47}$$

With the IC property, each worker achieves the maximum utility only when he or she signs the contract customized for his or her actual privacy group, which ensures that workers would truthfully report their privacy groups (i.e., privacy preferences) to the server.

In the subsequent two subsections, we formulate the problems mathematically, conduct theoretical analyses, and derive optimal contracts under two different information models given as below.

1) **Complete Information Model**: Under this model, the server has the knowledge of each worker's precise privacy group (i.e., privacy preference) beforehand. In other words, there exists no information asymmetry between workers and the server. Note that this is an ideal case which may not hold in reality, and we introduce it as a benchmark.
2) **Incomplete Information Model**. Under this model, rather than each worker's precise privacy group, the server only knows the distribution of workers in different privacy groups, say the number of workers in each privacy group. In this case, there exists information asymmetry between workers and the server, which is a more realistic and complicated scenario.

B. Optimal Contract Design Under Complete Information

This section investigates the optimal contract design under complete information. We first mathematically formulate the problem, and then simplify it to derive the analytical solution.

Knowing each worker's precise privacy group in advance, the server could specializedly design and offer only one contract for each worker corresponding to her privacy group. That is, the workers in the k-th privacy group could only receive the contract (ρ_k, r_k) from the server. Therefore, the IC property is satisfied spontaneously, and the server only needs to account for the BF and IR properties. (Note that we assume the server maintains a fixed budget in each communication round, and the set of workers $\mathcal{M}$ remains unchanged throughout the learning process, and thus we would experience an identical optimal contract design problem across different rounds. Therefore, in the analyses hereafter, we focus on the optimal contract design in a specific communication round.)

With the above analysis, the optimal contract design under complete information model can be formulated as

$$\min\ \sum\nolimits_{k=1}^{K}\frac{m_k}{\rho_k} \tag{48a}$$

$$\text{s.t. } \sum\nolimits_{k=1}^{K} m_k r_k \le B, \tag{48b}$$

$$r_k - c_k\rho_k \ge 0,\ \text{for } 1\le k\le K, \tag{48c}$$

where B is the system budget that the server could afford for this round.

Instead of directly solving the optimization problem (48), we first try to simplify it as detailed in Lemma 3.

Lemma 3: The inequality constraints Eq. (48b) and (48c) can be simplified to equality constraints simultaneously, i.e., $\sum_{k=1}^{K} m_k r_k = B$ and $r_k - c_k\rho_k = 0\,,\ 1\le k\le K$.

Proof: Suppose there exists an optimal contract that provides workers in the k-th privacy group with utility $u_k = r_k - c_k\rho_k > 0$. However, the server could always choose a larger ρ_k to improve the convergence performance of the model as long as the IR constraint is not violated until $u_k = r_k - c_k\rho_k = 0$. Similarly, if the set of contracts satisfy $\sum_{k=1}^{K} m_k r_k < B$, the server could always choose a larger r_k, which allows for a larger ρ_k, to enhance the model performance until $\sum_{k=1}^{K} m_k r_k = B$. The proof is thus complete. ∎

Lemma 3 demonstrates that the server could design a set of contracts that are able to offer each worker zero utility to optimize the FL model performance by exhausting the available budget. Consequently, the optimization problem (48)

could be equivalently transformed into

$$\min \sum_{k=1}^{K} \frac{m_k}{\rho_k} \tag{49a}$$

$$\text{s.t. } \sum_{k=1}^{K} m_k r_k = B, \tag{49b}$$

$$r_k - c_k \rho_k = 0, \text{ for } 1 \le k \le K, \tag{49c}$$

Compared to the original one, the simplified optimization problem (49) can be easily solved by Lagrange analysis with KKT conditions. The corresponding Lagrangian of the optimization problem is

$$L(\rho_k, \gamma) = \sum_{k=1}^{K} \left(\frac{m_k}{\rho_k} + \gamma m_k c_k \rho_k \right) - \gamma B, \tag{50}$$

where γ is the Lagrange multiplier.

By enforcing the first-order derivative of the Lagrangian with regard to ρ_k to be zero, and conducting some simple derivations, we obtain the following set of optimal contracts. We would like to stress that the derived set of contracts are the global optima due to the convexity of problem (49).

$$\rho_k^* = \frac{B}{\sum_{k=1}^{K} m_k c_k^{\frac{1}{2}}} c_k^{-\frac{1}{2}}, \; r_k^* = \frac{B}{\sum_{k=1}^{K} m_k c_k^{\frac{1}{2}}} c_k^{\frac{1}{2}}. \tag{51}$$

C. Optimal Contract Design Under Incomplete Information

A more pragmatic and complicated scenario is the incomplete information model, where the server only knows the distribution of workers in different privacy groups, i.e., the number of workers m_k in the k-th privacy group (for $1 \le k \le K$). Note that this can be achieved in various ways, such as making a survey questionnaire [37].

Due to the existence of information asymmetry, the server needs to release all the designed contracts to each worker. In this case, selfish and strategic workers have the tendency to fabricate their privacy groups to sign contracts designed for other privacy groups to earn more utility. Thus, apart from the BF and IR properties, it is essential for the set of designed contracts to satisfy the IC property. This leads to the following problem formulation for the optimal contract design under incomplete information model.

$$\min \sum_{k=1}^{K} \frac{m_k}{\rho_k} \tag{52a}$$

$$\text{s.t. } \sum_{k=1}^{K} m_k r_k \le B, \tag{52b}$$

$$r_k - c_k \rho_k \ge 0, \text{ for } 1 \le k \le K, \tag{52c}$$

$$r_k - c_k \rho_k \ge r_{k'} - c_k \rho_{k'}, \text{ for } 1 \le k, \; k' \le K, \; k \ne k'. \tag{52d}$$

As we can observe from the optimization problem (52), there are K IR constraints and $K \times (K-1)$ IC constraints in total, making it intractable to solve directly. According to [38], we can equivalently reduce these K^2 constraints to K constraints, and the simplification procedures are elaborated in the following lemmas.

First, we facilitate the IR constraints as in Lemma 4.

Lemma 4: The IR constraints Eq. (52c) can be equivalently reduced to

$$r_K - c_K \rho_K \ge 0. \tag{53}$$

Proof: Recall that $c_1 < c_2 < \cdots < c_K$ and based on the IC property, for $\forall k < K$, we have

$$r_k - c_k \rho_k \ge r_K - c_k \rho_K > r_K - c_K \rho_K. \tag{54}$$

As described in Eq. (54), workers in the highest privacy group (i.e., with the largest privacy preference) achieve the lowest utility. Hence, if the set of designed contracts could ensure these workers to obtain non-negative utility, the IR property is guaranteed for all kinds of workers. Then, it is sufficient to ensure that $r_K - c_K \rho_K \ge 0$. ■

Moreover, the BF constraint Eq. (52b) and the IR constraints Eq. (52c) (degenerated into Eq. (53)) can be jointly predigested as in Lemma 5.

Lemma 5: The BF constraint Eq. (52b) and IR constraints Eq. (52c) (degenerated into Eq. (53)) can be jointly simplified to $\sum_{k=1}^{K} m_k r_k = B$ and $r_K - c_K \rho_K = 0$.

Proof: We omit the proof here since it is similar to that of Lemma 3. ■

Before simplifying the IC constraints Eq. (52d), we first present Lemma 6.

Lemma 6 (PPL Monotonicity): The set of designed contracts for K privacy groups would provide workers in higher privacy groups (i.e., with larger privacy preferences) with higher PPLs. Specifically, for any two feasible contracts (ρ_k, r_k) and $(\rho_{k'}, r_{k'})$, $\rho_{k'} \le \rho_k$ if $c_k \le c_{k'}$.

Proof: To guarantee the IC property, for $k \ne k'$, we have

$$r_k - c_k \rho_k \ge r_{k'} - c_k \rho_{k'} \tag{55}$$

and

$$r_{k'} - c_{k'} \rho_{k'} \ge r_k - c_{k'} \rho_k. \tag{56}$$

Adding the above two inequalities leads to

$$(\rho_{k'} - \rho_k)(c_k - c_{k'}) \ge 0, \tag{57}$$

which implies $\rho_{k'} \le \rho_k$ if $c_k \le c_{k'}$. ■

Based on the property of PPL monotonicity, we next try to simplify the IC constraints Eq. (52d). First, we introduce the following two properties: Local Downward Incentive Compatibility (LDIC) (i.e., Eq. (58)) and Local Upward Incentive Compatibility (LUIC) (i.e., Eq. (59)).

$$r_k - c_k \rho_k \ge r_{k-1} - c_k \rho_{k-1}. \tag{58}$$

$$r_k - c_k \rho_k \ge r_{k+1} - c_k \rho_{k+1}. \tag{59}$$

With the above LDIC and LUIC properties, the simplification of the IC constraints can be implemented in three steps, which are respectively presented in Lemma 7, Lemma 8, and Lemma 9.

Lemma 7: If the LUIC constraints are satisfied, the global upward incentive compatibility (GUIC) constraints are satisfied naturally, i.e., $r_k - c_k \rho_k \ge r_{k+1} - c_k \rho_{k+1} \ge \cdots \ge r_K - c_k \rho_K$. Also, if the LDIC constraints are satisfied, the global downward incentive compatibility (GDIC) constraints are satisfied, i.e., $r_k - c_k \rho_k \ge r_{k-1} - c_k \rho_{k-1} \ge \cdots \ge r_1 - c_k \rho_1$.

Proof: Without loss of generality, we assume $c_k \le c_{k+1} \le c_{k+2}$. Then, based on Lemma 6 and the LUIC constraints,

we have

$$\begin{aligned} & r_{k+1} - c_{k+1}\rho_{k+1} \geq r_{k+2} - c_{k+1}\rho_{k+2} \\ & \Rightarrow r_{k+1} - r_{k+2} \geq c_{k+1}\left(\rho_{k+1} - \rho_{k+2}\right) \\ & \Rightarrow r_{k+1} - r_{k+2} \geq c_{k}\left(\rho_{k+1} - \rho_{k+2}\right) \\ & \Rightarrow r_{k+1} - c_k\rho_{k+1} \geq r_{k+2} - c_k\rho_{k+2}. \end{aligned} \tag{60}$$

We also have

$$r_k - c_k\rho_k \geq r_{k+1} - c_k\rho_{k+1}. \tag{61}$$

Then, from Eq. (60) and Eq. (61), we obtain $r_k - c_k\rho_k \geq r_{k+1} - c_k\rho_{k+1} \geq \cdots \geq r_K - c_k\rho_K$, demonstrating that the GUIC constraints hold.

In a similar manner, we could also prove that the GDIC constraints are satisfied if LDIC holds. We omit the proof of this case for brevity. ∎

Obviously, with Lemma 7, we only need to guarantee the LUIC and LDIC properties in order to satisfy the IC constraints Eq. (52d).

Lemma 8: If (ρ_k^*, r_k^*) $(1 \leq k \leq K)$ are the set of optimal contracts, then the LUIC constraint (Eq. (59)) is active in such contract design, that is, $r_k^* - c_k\rho_k^* = r_{k+1}^* - c_k\rho_{k+1}^*$.

Proof: We prove Lemma 8 by contradiction. Suppose that the LUIC constraint is inactive in the current contract design, i.e., $r_k^* - c_k\rho_k^* > r_{k+1}^* - c_k\rho_{k+1}^*$, then based on Lemma 7 and Lemma 6, we have $r_k^* - c_k\rho_k^* > r_K^* - c_k\rho_K^* > r_K^* - c_K\rho_K^* = 0$. Without disobeying any constraints, the server could expect better model performance by increasing the privacy parameter ρ_k^* until the LUIC inequality becomes active. ∎

Thus, the LUIC constraint Eq. (59) can be degenerated into

$$r_k - c_k\rho_k = r_{k+1} - c_k\rho_{k+1}. \tag{62}$$

Lemma 9: If the LUIC constraint is active, the LDIC constraint is satisfied spontaneously.

Proof: According to Lemma 6 and the active LUIC constraint Eq. (62), we have

$$\begin{aligned} r_k - c_k\rho_k \; &= \; r_{k+1} - c_k\rho_{k+1} \\ & \Rightarrow r_k - r_{k+1} = c_k\left(\rho_k - \rho_{k+1}\right) \\ & \Rightarrow r_k - r_{k+1} \leq c_{k+1}\left(\rho_k - \rho_{k+1}\right) \\ & \Rightarrow r_{k+1} - c_{k+1}\rho_{k+1} \geq r_k - c_{k+1}\rho_k. \end{aligned} \tag{63}$$

∎

Therefore, with Lemma 5, Lemma 7, Lemma 8, and Lemma 9, the original optimization problem (52) for optimal contract design under incomplete information model can be transformed into

$$\min \; \sum\nolimits_{k=1}^{K} \frac{m_k}{\rho_k} \tag{64a}$$

$$\text{s.t.} \; \sum\nolimits_{k=1}^{K} m_k r_k = B, \tag{64b}$$

$$r_K - c_K\rho_K = 0, \tag{64c}$$

$$r_k - c_k\rho_k = r_{k+1} - c_k\rho_{k+1}, \; 1 \leq k \leq K-1. \tag{64d}$$

The closed-form solution to the optimization problem (64) is presented in the theorem below.

Theorem 4: Under incomplete information model, the set of optimal contracts are given as

$$\rho_k^* = WQ_k^{-\frac{1}{2}} m_k^{\frac{1}{2}}, \tag{65}$$

$$r_k^* = \begin{cases} W\left(c_k Q_k^{-\frac{1}{2}} m_k^{\frac{1}{2}} + \sum_{j=k+1}^{K} \Delta c_j Q_j^{-\frac{1}{2}} m_j^{\frac{1}{2}}\right), \\ \qquad\qquad k \leq K-1 \\ c_K W Q_K^{-\frac{1}{2}} m_K^{\frac{1}{2}}, \quad k = K, \end{cases} \tag{66}$$

where

$$\Delta c_k = c_k - c_{k-1} \tag{67}$$

$$Q_k = \begin{cases} m_1 c_1, & k = 1 \\ m_k c_k + \Delta c_k \sum_{j=1}^{k-1} m_j, & 2 \leq k \leq K \end{cases} \tag{68}$$

$$W = \frac{B}{\sum_{k=1}^{K} Q_k^{\frac{1}{2}} m_k^{\frac{1}{2}}} \tag{69}$$

Proof: According to Eq. (64d), we have

$$r_{K-1} - c_{K-1}\rho_{K-1} = r_K - c_{K-1}\rho_K \tag{70}$$

Substituting $r_K = c_K\rho_K$ (i.e., Eq. (64c)) into it, we have

$$\begin{aligned} r_{K-1} &= c_{K-1}\rho_{K-1} + \left(c_K - c_{K-1}\right)\rho_K \\ &= c_{K-1}\rho_{K-1} + \Delta c_K \rho_K, \end{aligned} \tag{71}$$

where $\Delta c_K = c_K - c_{K-1}$.

Following the same methodology, we can represent r_k $(1 \leq k \leq K)$ as follows

$$r_k = \begin{cases} c_k\rho_k + \sum_{j=k+1}^{K} \Delta c_j \rho_j, k \leq K-1 \\ c_K\rho_K, k = K \end{cases} \tag{72}$$

Substituting r_k into Eq. (64b), we have

$$\begin{aligned} \sum\nolimits_{k=1}^{K} m_k r_k = \sum\nolimits_{k=1}^{K-1} \left(m_k c_k \rho_k + m_k \sum\nolimits_{j=k+1}^{K} \Delta c_j \rho_j\right) \\ + m_K c_K \rho_K = B, \end{aligned} \tag{73}$$

which can be summarized as

$$\sum\nolimits_{k=1}^{K} m_k r_k = \sum\nolimits_{k=1}^{K} Q_k \rho_k = B, \tag{74}$$

where Q_k is defined in Eq. (68).

Thus, the corresponding Lagrangian of the optimization problem (64) is formulated as

$$L\left(\rho_k, \gamma\right) = \sum\nolimits_{k=1}^{K} \left(\frac{m_k}{\rho_k} + \gamma Q_k \rho_k\right) - \gamma B, \tag{75}$$

where γ is the Lagrange multiplier.

Based on KKT conditions, we set the first-order derivatives of the Lagrangian with respect to ρ_k and γ equal to zero, and after some derivations, we obtain the privacy parameters in the optimal contracts as

$$\rho_k^* = WQ_k^{-\frac{1}{2}} m_k^{\frac{1}{2}}, \quad k = 1, 2, \ldots, K, \tag{76}$$

where Q_k and W are defined in Eq. (68) and Eq. (69), respectively. Obviously, the optimal payment for workers in the K-th privacy group is given by

$$r_K^* = c_K\rho_K^* = c_K W Q_K^{-\frac{1}{2}} m_K^{\frac{1}{2}}, \tag{77}$$

while the optimal payments for workers in other privacy groups can be calculated according to Eq. (72). ∎

VII. Performance Evaluation

In this section, we conduct an experimental evaluation of Pain-FL on various models (convex and non-convex) and learning configurations (IID and Non-IID data partitions) and make comparisons with three baselines.

A. Experimental Settings

Our experiments consider an FL system that consists of a central server and $M = 100$ workers. We assume that $M = 100$ workers are uniformly at random distributed in $K = 10$ privacy groups. The privacy preferences of workers in each group are sampled from a uniform distribution of $\mathbb{U}(20, 100)$, and we sort them in ascending order. In each communication round of the launched FL task, we assume that the server has a fixed budget of B to incentivize workers to perform local model updates. We configure two options for the budget B, i.e., $B = 10,000$ and $B = 20,000$ (by default).

For the learning configurations, unless otherwise specified, we adopt the synchronous federated learning scheme. Each worker only conducts one step of local model update in each communication round with a mini-batch of 64 data samples, generating a stochastic gradient. Due to privacy concerns, each worker would perturb the calculated stochastic gradient following Eq. (6), where the noise variance σ_m^2 is determined by the PPL ρ_k specified in the signed contract. We employ SGD as the optimizer and set the learning rate $\eta = 0.01$. In each round of global model update, we randomly select 50% of the incentivized workers for gradient aggregation to simulate the unpredictable drop-out of workers and alleviate the straggler's effect. Next, we introduce the dataset and models used in the experiments and the baselines for performance comparison.

1) Dataset: Like most existing FL studies, we conduct experiments on the standard MNIST dataset for handwritten digit recognition, which consists of $60,000$ training samples and $10,000$ testing samples. As in [5], we consider two different ways of partitioning the MNIST data over the $M = 100$ workers, i.e., IID and Non-IID. Specifically, for the IID case, the data is first shuffled and then partitioned into 100 workers, each receiving 600 examples; for the Non-IID case, we first sort the data by digit label, and then divide them into 100 shards of size 600, each of 100 workers receiving only 1 shard (also 600 examples per worker). Note that this is a pathological non-IID partition of the data, as most of the workers will only have examples of one class (i.e., digit). Obviously, either of the two data partitions is balanced among the workers.

2) Models:

- **LR Classifier.** For the convex model, we employ a multi-nomial logistic regression classifier, and use the softmax cross-entropy as the loss function.
- **CNN.** For the non-convex model, we employ a CNN, which consists of two 5×5 convolution layers (the first with 10 channels, the second with 20 channels, each followed with 2×2 max pooling), a Drop-out layer (0.5), a fully connected layer with 120 units and ReLu activation, a Drop-out layer (0.5), a fully connected layer with 84 units and ReLu activation, a fully connected layer with 10 units and ReLu activation, and a final softmax output layer.

3) Baselines: As described above, in each communication round of Pain-FL, we customize contracts for workers with different privacy preferences to provide personalized PPLs and payments. However, none of the existing work has considered the same scenario as this work, and thus they are not comparable with Pain-FL. Instead, we employ a simple single-contract strategy as the baseline. The server designs and offers the same contract to all the participating workers regardless of their different privacy preferences. In particular, we consider the following three policies in the single-contract design.

- **Single Contract with Full Individual Rationality (SC-FIR)**: This single contract offers all workers the same payment, which exactly provides workers in the highest privacy group with zero utility. In this case, workers in all privacy groups would accept the contract since they could all earn non-negative utility by signing the contract. In SC-FIR, all workers will participate in this round of FL with a gradient perturbation level (noise variance) corresponding to the highest privacy group.
- **Single Contract with Half Individual Rationality (SC-HIR)**: This single contract offers all workers the same payment, which exactly provides workers in the median privacy group with zero utility. In this case, only workers in lower privacy groups (with lower privacy preferences) than the median would accept the contract since they could earn non-negative utility by signing the contract. In SC-HIR, workers in lower privacy groups than the median will participate in this round of FL with a gradient perturbation level (noise variance) corresponding to the median privacy group.
- **Single Contract with Random Individual Rationality (SC-RIR)**: This single contract offers all workers the same payment, which exactly provides workers in a randomly selected privacy group with zero utility. In this case, only workers in lower privacy groups (with lower privacy preferences) than the selected one would accept the contract since they could earn non-negative utility by signing the contract. In SC-RIR, workers in lower privacy groups than the selected one will participate in this round of FL with a gradient perturbation level (noise variance) corresponding to the selected privacy group.

B. Practicability

In this subsection, we examine the practicability of the contracts designed in Pain-FL.

1) PPL Monotonicity: We first present the PPL ρ_k in the set of contracts designed for workers in different privacy groups under both complete and incomplete information models. As shown in Fig. 2, for both information models, ρ_k decreases as the index of privacy groups rises. This shows that workers with higher privacy preferences pursue a higher PPL (i.e., a smaller ρ_k), which is consistent with our theoretical analysis (i.e., Lemma 6) in Section VI. Additionally, workers in the same privacy group achieve a higher PPL under incomplete information model than complete one. This is because there exists information asymmetry between workers and the server under incomplete information model. Thus, the server has to

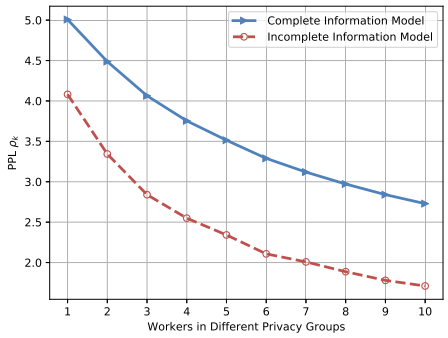

Fig. 2. PPL ρ_k in the set of contracts designed for different privacy groups.

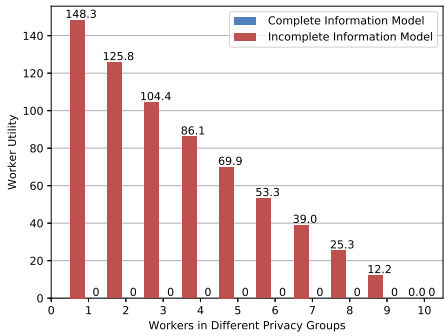

Fig. 3. The utility of workers in different privacy groups.

provide workers in lower privacy groups with positive utility to incentivize them to truthfully reveal their privacy groups. In this case, given a fixed budget of B, only a smaller ρ_k can be designed, offering higher PPLs for workers.

2) IR Property: We present the utility of workers in different privacy groups in Fig. 3, from which we have the following observations. Apparently, under both complete and incomplete information models, workers in arbitrary privacy groups could achieve non-negative utility, which validates the IR property. In particular, workers in each of K privacy groups achieve zero utility under complete information model, as in this case the server has the knowledge of each worker's precise privacy group and thus could customize a zero-utility contract for each worker. Under incomplete information model, however, only workers in the highest privacy group achieve zero utility, while workers in other privacy groups achieve positive utility. The reason behind that lies also in the information asymmetry existing between workers and the server.

3) IC Property: Under incomplete information model, we present the utility of workers in the 3-rd, 5-th, 7-th privacy group when they sign contracts designed for different privacy groups in Fig. 4. As indicated by the arrows in the figure, workers achieve the maximum utility when they sign the contract customized for the privacy group which they belong to. Besides, we could observe that when workers in different privacy groups sign the same contract, workers in the lower privacy groups achieve higher utility. This results from the fact that the privacy preference of workers in lower privacy groups is smaller. Specifically, in accordance with the definition on worker utility in Eq. (10), a smaller privacy preference c_k yields larger utility when signing the same contract (ρ_k, r_k).

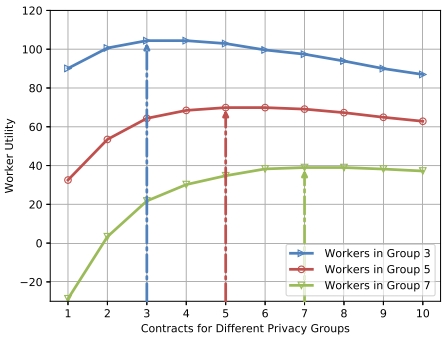

Fig. 4. The utility of workers when signing different contracts.

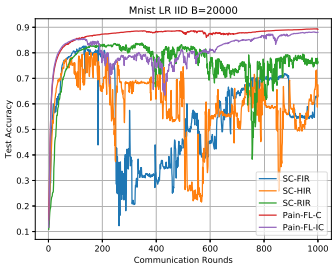

Fig. 5. Comparison of test accuracy of LR with IID MNIST dataset and a budget of $20,000$ among the five schemes.

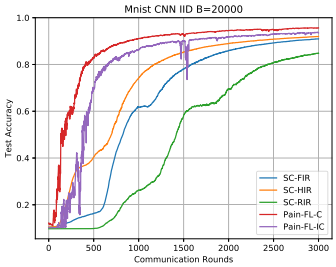

Fig. 6. Comparison of test accuracy of CNN with IID MNIST dataset and a budget of $20,000$ among the five schemes.

C. Model Convergence Performance

In this subsection, we evaluate the performance of the proposed Pain-FL in terms of model test accuracy by comparing with the above-mentioned three single contract baselines. Besides, we investigate the impact of some system settings and parameters on Pain-FL's performance.

1) IID Case: We first show the convergence performance in terms of test accuracy for both LR and CNN models for the proposed Pain-FL (under complete/incomplete information) and the three single contract baselines under IID data partition. We consider two different budget settings (i.e., $B = 10,000$ and $B = 20,000$). Note that hereafter we represent Pain-FL under complete and incomplete information by Pain-FL-C and Pain-FL-IC, respectively.

a) Performance comparison with baselines: As shown in Fig. 5 and Fig. 6, when $B = 20000$, the Pain-FL-C achieves the highest test accuracy, as the server knows each worker's precise privacy group. The server could make the utmost of the budget to design and offer an optimal contract with exactly zero utility for all kinds of workers and incentivize them to adopt a relatively weak perturbation level on the gradient, contributing to high model accuracy. However, when there exists information asymmetry, the server needs to sacrifice

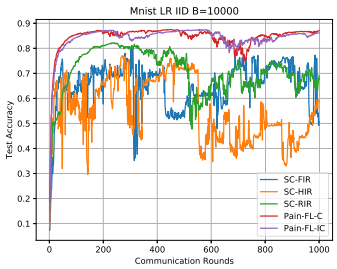

Fig. 7. Comparison of test accuracy of LR with IID MNIST dataset and a budget of $10,000$ among the five schemes.

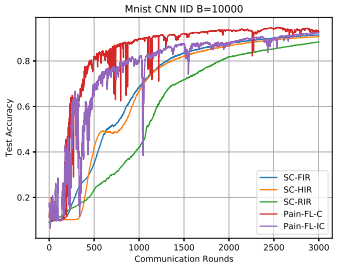

Fig. 8. Comparison of test accuracy of CNN with IID MNIST dataset and a budget of $10,000$ among the five schemes.

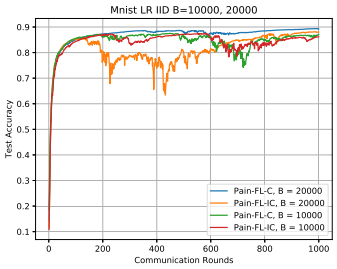

Fig. 9. Comparison of test accuracy of LR with IID MNIST dataset and different budget and information models for the proposed Pain-FL.

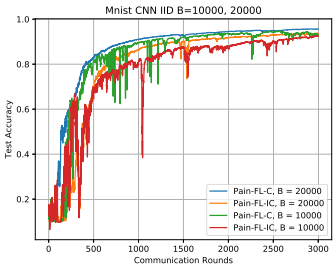

Fig. 10. Comparison of test accuracy of CNN with IID MNIST dataset and different budget and information models for the proposed Pain-FL.

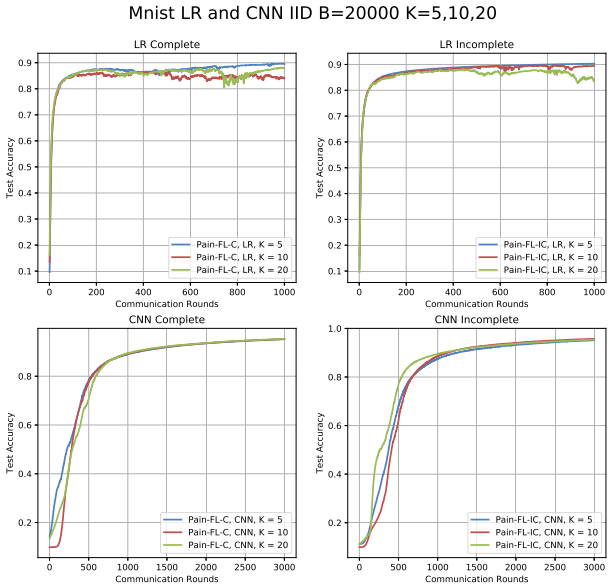

Fig. 11. Comparison of test accuracy of LR and CNN with IID MNIST dataset among different number of divided privacy groups K.

some budget for workers truthfully reporting their privacy preferences, inducing higher PPLs for workers (smaller ρ_k as shown in Fig. 2), thus slightly deteriorating model accuracy. Moreover, we would like to highlight that our proposed Pain-FL (C or IC) scheme significantly outperforms the two single-contract baselines. We inspect a different budget setting (i.e., $B = 10,000$) in Fig. 7 and Fig. 8 for the two models, from which we could observe consistent results as Fig. 5 and Fig. 6.

b) Impact of budget B: To investigate the impact of the system budget B on the proposed Pain-FL scheme, we present the test accuracy comparison between Pain-FL-C and Pain-FL-IC with $B = 10,000$ and $B = 20,000$ in Fig. 9 and Fig. 10 using LR and CNN, respectively. We know from the two figures that Pain-FL achieves higher test accuracy as B rises regardless of other settings. This result is self-explanatory. When the server maintains more budget, it could provide larger payments to incentivize workers to choose lower PPLs, which is favorable for model training.

c) Impact of group number K: We study the impact of the number of divided privacy groups K among workers on the model performance. The results are in Fig. 11, from which we can see that the test accuracy of both LR and CNN models remains relatively stable under varying K ($K = 5, 10, 20$), given IID training data and under both complete and incomplete information models. This is because given a fixed total number of workers $M = \sum_{k=1}^{K} m_k$ with their uniform distribution among K privacy groups, along with a fixed range (i.e., $\mathbb{U}(20, 100)$) of all workers' privacy preferences, the average privacy-preserving level ρ among workers suffers negligible changes with the variation of K.

2) Non-IID Case: In this subsection, we divert our attention from IID case to Non-IID case and conduct the same series of experiments with a budget of $B = 20,000$.

a) Performance comparison with baselines: As shown in Fig. 12 and Fig. 13, although the data is now Non-IID among workers, the comparison results in terms of test accuracy for both LR and CNN models remain consistent as the IID case. Specifically, the proposed Pain-FL (C and IC) with personalized contract design outperforms the single contract baseline methods; Pain-FL-C under complete information achieves higher test accuracy than Pain-FL-IC under incomplete information.

b) Non-IID vs. IID: Finally, we compare the test accuracy achieved by Pain-FL between IID and Non-IID data partitions among workers. The results are respectively depicted in Fig. 14 and Fig. 15 for LR and CNN models. As expected, for both models and under both information models (complete/incomplete), lower test accuracy is achieved in the Non-IID case.

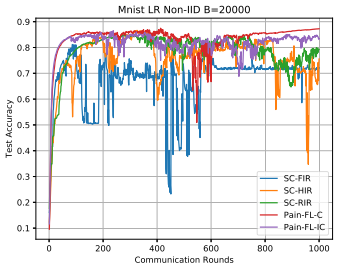

Fig. 12. Comparison of test accuracy of LR with Non-IID MNIST dataset and a budget of 20, 000 among the five schemes.

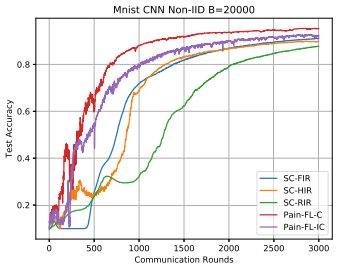

Fig. 13. Comparison of test accuracy of CNN with Non-IID MNIST dataset and a budget of 20, 000 among the five schemes.

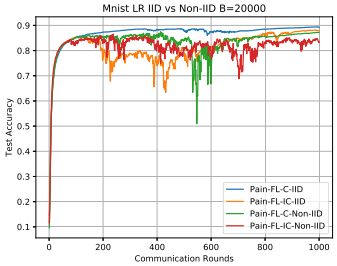

Fig. 14. Comparison of test accuracy of LR with a budget of 20, 000 and different data partitions (IID and Non-IID) and information models for the proposed Pain-FL.

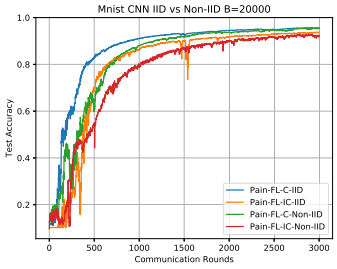

Fig. 15. Comparison of test accuracy of CNN with a budget of 20, 000 and different data partitions (IID and Non-IID) and information models for the proposed Pain-FL.

VIII. Conclusion

This paper presented Pain-FL, a contract-theoretic personalized privacy-preserving incentive mechanism for federated learning systems. Pain-FL aims to customize the payment for each participating worker as compensation for privacy cost with her personalized privacy preference taken into consideration while achieving satisfactory model accuracy of the finally learned global models. To this end, we first leverage the notion of ρ-zCDP to explicitly quantify workers' privacy-preserving levels (PPLs) and the resulting privacy cost. Then, we conduct rigorous convergence analyses of Pain-FL for convex and non-convex models and capitalize on the derived convergence error bounds to link the performance of the learned model to workers' PPLs. Eventually, we derive a set of optimal contracts analytically under both complete and incomplete information models, which could optimize the convergence performance of the FL models while bearing desired economic properties, including budget feasibility, individual rationality, and incentive compatibility. Extensive experimental results on different models and learning configurations validate the practicability and effectiveness of the proposed Pain-FL. One potential direction for our future work is to incorporate defenses against free-rider attacks in FL, where workers dissimulate participation to steal the final aggregated model without actually contributing with any data, into our personalized privacy-preserving incentive.

References

[1] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge intelligence: Paving the last mile of artificial intelligence with edge computing," *Proc. IEEE*, vol. 107, no. 8, pp. 1738–1762, Aug. 2019.

[2] H. Li, K. Ota, and M. Dong, "Learning IoT in edge: Deep learning for the Internet of Things with edge computing," *IEEE Netw.*, vol. 32, no. 1, pp. 96–101, Jan./Feb. 2018.

[3] G. Zhu, D. Liu, Y. Du, C. You, J. Zhang, and K. Huang, "Toward an intelligent edge: Wireless communication meets machine learning," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 19–25, Jan. 2020.

[4] S. Pouyanfar *et al.*, "A survey on deep learning: Algorithms, techniques, and applications," *ACM Comput. Surv.*, vol. 51, no. 5, pp. 1–36, Sep. 2018.

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

[6] W. Y. B. Lim *et al.*, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2031–2063, 3rd Quart., 2020.

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

[8] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol. (TIST)*, vol. 10, no. 2, pp. 1–19, 2019.

[9] A. Hard *et al.*, "Federated learning for mobile keyboard prediction," 2018, *arXiv:1811.03604*. [Online]. Available: http://arxiv.org/abs/1811.03604

[10] M. Song *et al.*, "Analyzing user-level privacy attack against federated learning," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 10, pp. 2430–2444, 2020.

[11] L. Zhu, Z. Liu, and S. Han, "Deep leakage from gradients," in *Proc. Adv. Neural Inf. Process. Syst.*, 2019, pp. 14774–14784.

[12] Z. Wang, M. Song, Z. Zhang, Y. Song, Q. Wang, and H. Qi, "Beyond inferring class representatives: User-level privacy leakage from federated learning," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2019, pp. 2512–2520.

[13] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 3–18.

[14] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 691–706.

[15] L. T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-preserving deep learning via additively homomorphic encryption," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1333–1345, May 2018.

[16] Y. Li, Y. Zhou, A. Jolfaei, D. Yu, G. Xu, and X. Zheng, "Privacy-preserving federated learning framework based on chained secure multi-party computing," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6178–6186, Apr. 2021.

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

[18] 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.

[19] 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.
[20] 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.
[21] N. Ding, Z. Fang, and J. Huang, "Incentive mechanism design for federated learning with multi-dimensional private information," in *Proc. 18th Int. Symp. Modeling Optim. Mobile, Ad Hoc, Wireless Netw. (WiOPT)*, 2020, pp. 1–8.
[22] N. Ding, Z. Fang, and J. Huang, "Optimal contract design for efficient federated learning with multi-dimensional private information," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 1, pp. 186–200, Jan. 2021.
[23] 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, Sep. 2019.
[24] W. Y. B. Lim *et al.*, "Dynamic contract design for federated learning in smart healthcare applications," *IEEE Internet Things J.*, early access, Oct. 27, 2020, doi: 10.1109/JIOT.2020.3033806.
[25] T. H. T. Le, N. H. Tran, Y. K. Tun, Z. Han, and C. S. Hong, "Auction based incentive design for efficient federated learning in cellular wireless networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, May 2020, pp. 1–6.
[26] 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.*, vol. 20, no. 10, pp. 3034–3048, Oct. 2021.
[27] Y. Wang, G. Norice, and L. F. Cranor, "Who is concerned about what? A study of American, Chinese and Indian users' privacy concerns on social network sites," in *Proc. Int. Conf. Trust Trustworthy Comput.* Berlin, Germany: Springer, 2011, pp. 146–153.
[28] 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. Secur.*, Oct. 2017, pp. 603–618.
[29] R. Hu and Y. Gong, "Trading data for learning: Incentive mechanism for on-device federated learning," 2020, *arXiv:2009.05604*. [Online]. Available: http://arxiv.org/abs/2009.05604
[30] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.
[31] M. Bun and T. Steinke, "Concentrated differential privacy: Simplifications, extensions, and lower bounds," in *Proc. Theory Cryptography Conf.* Berlin, Germany: Springer, 2016, pp. 635–658.
[32] C. Dwork and G. N. Rothblum, "Concentrated differential privacy," 2016, *arXiv:1603.01887*. [Online]. Available: http://arxiv.org/abs/1603.01887
[33] O. Rivasplata. (2012). *Subgaussian Random Variables: An Expository Note*. [Online]. Available: http://www.stat.cmu.edu/~arinaldo/36788/subgaussians.pdf
[34] Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 9, pp. 1432–1437, Sep. 2011.
[35] A. Ghosh and A. Roth, "Selling privacy at auction," *Games Econ. Behav.*, vol. 91, pp. 334–346, May 2015.
[36] L. Bottou, F. E. Curtis, and J. Nocedal, "Optimization methods for large-scale machine learning," *SIAM Rev.*, vol. 60, no. 2, pp. 223–311, 2018.
[37] L. Tian, J. Li, W. Li, B. Ramesh, and Z. Cai, "Optimal contract-based mechanisms for online data trading markets," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7800–7810, Oct. 2019.
[38] P. Bolton *et al.*, *Contract Theory*. Cambridge, MA, USA: MIT Press, 2005.

Peng Sun received the B.E. degree in automation from Tianjin University, China, in 2015, and the Ph.D. degree in control science and engineering from Zhejiang University, China, in 2020. He is currently a Research Assistant with the State Key Laboratory of Industrial Control Technology, Zhejiang University, China, and a Post-Doctoral Researcher with the School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen, China. From November 2018 to November 2019, he was a Visiting Ph.D. Student with the Department of Electrical Engineering and Computer Science, The University of Tennessee, Knoxville, TN, USA. His research interests include the Internet of Things, mobile crowdsensing/crowdsourcing systems, and federated learning.

Haoxuan Che received the B.E. degree in software engineering from Northwestern Polytechnical University, Xi'an, China, in 2019. He is currently a Research Assistant with the School of Software, Northwestern Polytechnical University. His main research interests include reinforcement learning and federated learning.

Zhibo Wang (Senior Member, IEEE) received the B.E. degree in automation from Zhejiang University, Hangzhou, China, in 2007, and the Ph.D. degree in electrical engineering and computer science from The University of Tennessee, Knoxville, TN, USA, in 2014. He is currently a Professor with the School of Cyber Science and Technology, Zhejiang University. His current research interests include mobile crowdsensing systems, AI security, and data security and privacy protection. He is a member of ACM.

Yuwei Wang received the B.S. degree in statistics from Zhejiang University, Hangzhou, China, in 2019. He is currently pursuing the Ph.D. degree with the State Key Laboratory of Industrial Control Technology, Zhejiang University, China. His research interests include indoor localization and federated learning.

Tao Wang received the B.E. degree in network engineering from Anhui University, Hefei, China, in 2020. He is currently pursuing the master's degree with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics. His research interests focus on security and privacy issues in federated learning.

Liantao Wu received the B.E. degree in automation from Shandong University, China, in 2012, and the Ph.D. degree in control science and engineering from Zhejiang University, China, in 2017. From 2017 to 2020, he was with Shanghai Huawei Technologies Company Ltd. He is currently a Research Assistant Professor with Shanghai Institute of Fog Computing Technology (SHIFT), ShanghaiTech University. His research interests include the IoT, wireless communications, and compressive sensing.

Huajie Shao received the M.E. degree in control engineering from Zhejiang University, China, in 2014, and the Ph.D. degree in computer science from the University of Illinois at Urbana-Champaign (UIUC), USA, in 2021. He is currently an Assistant Professor with the Department of Computer Science, College of William and Mary, USA. He has published more than 20 papers in international journals and conferences, such as WWW, ICML, INFOCOM, Ubicomp, VLDB, Sensys, TOC, TSP, and TPDS. His research interests mainly focus on data mining, deep learning-based recommender systems, and social sensing. He received the ICCPS'17 Best Paper Award and FUSION'19 Best Student Paper Award.