Incentive Design and Differential Privacy Based Federated Learning: A Mechanism Design Perspective

SUNGWOOK KIM[ID]
Department of Computer Science, Sogang University, Seoul 04107, South Korea
e-mail: swkim01@sogang.ac.kr

ABSTRACT Due to stricter data management regulations and large size of the training data, distributed learning paradigm such as federated learning (FL) has gained attention recently. FL is capable of significantly preserving end-users' private data from being exposed to external adversaries. However, private information can still be divulged by uploading parameters from users. Therefore, a key challenge in the FL platform is how users participate to build a high-quality learning model with effectively preventing information leakage. To address the above challenge, we design a novel incentive mechanism to attract more data owners to join in the FL process with the consideration of privacy preservation. To implement our proposed scheme, we adopt the concepts of mechanism design (MD) and differential privacy (DP); MD takes an objectives-first approach to designing incentives toward desired objectives, and the DP can provide a theoretical guarantee for users' privacy in FL participations. Based on the DP based incentive mechanism, our joint approach can leverage the full synergy that gives mutual advantages for users and learning operators. Therefore, we can take various benefits in a rational way under the dynamic changing FL environments. Through simulation analysis, the numerical results validate the performance efficiency of our proposed scheme.

INDEX TERMS Federated learning, differential privacy, Internet of Things, incentive mechanism design, joint control model.

I. INTRODUCTION

With the rapid development of the Internet of Things (IoT) and social network applications, an exponential growth of data has been generated. There are currently close to 7 billion connected IoT devices and 3 billion smartphones around the world. These IoT devices are equipped with increasingly enhanced sensing and computation capabilities. Therefore, it is expected that the big data-driven IoT paradigm will soon be applied in all aspects of our daily life, including medical care, food and agriculture, intelligent transportation systems, etc. Especially, a variety of IoT applications call for data mining and learning securely and reliably in distributed systems; it represents a vision in which the Internet extends into the real world while embracing everyday objects. This new trend arises from synergically merging IoT and distributed computing [1], [2].

In recent years, machine learning is more and more popular and applied widely in both academic and industrial community. As a subset of artificial intelligence, machine learning is closely related to computational statistics, which focuses on making predictions using computers. Usually, learning mechanism builds a mathematical model based on sample data, known as 'training data', in order to make decisions. With the rapid development of machine learning technologies, there is a huge demand for collaborative model learning where many users or entities collaboratively train a common model by feeding their own local data. To analyze the collected big data and obtain useful information for detection, classification, and prediction, traditional machine learning techniques need to aggregate massive user data with personal information into a central server to perform model training.

The associate editor coordinating the review of this manuscript and approving it for publication was Juntao Fei[ID].

However, this classical centralized-learning paradigm causes excessive computation and storage cost due to the increasing data size, and the mobile devices also suffer from serious privacy leakage risk [3], [4].

To address classical machine learning problems, federated learning (FL) - also known as collaborative learning - has been introduced as an emerging distributed machine learning model to allow the IoT devices to collaboratively train a global model in a decentralized manner. Originally, it has first introduced by Google and is used to design a virtual keyboard application for smart phones named Gboard. Nowadays, the FL can be a great solution for many services. In this learning process, IoT devices only need to iteratively send local model updates trained on their local raw data to the learning operator instead of uploading the raw data outside. This approach can decouple the machine learning from acquiring, storing and training data in a central server. Therefore, the FL has demonstrated great potentials to revolutionize the distributed IoT system by i) improving the efficiency of deployment and management of IoT devices, ii) enhancing the IoT security and privacy protection, and iii) enabling various smart applications. Because of the huge market potential of distributed IoT system, the FL paradigm is a promising tool to exploit more personalized service oriented applications [4]–[6].

Despite the aforementioned great benefits, the FL is still facing critical challenges. First, traditional FL studies assume that all IoT devices contribute their resources unconditionally while not providing any incentive mechanism to motivate participation. Such an assumption may not practical in the real world due to the resource costs incurred by model training. Therefore, it is necessary to design an effective incentive mechanism for stimulating IoT devices to become available workers for federated learning tasks. Based on the reasonably evaluated contribution of each IoT device, the profit earned by the FL model can be allocated to attract more devices to join in the FL process. However, it is a complex and difficult work to design an effective incentive mechanism. Second, even though the FL enables local training without personal data exchange between the learning operator and IoT devices, private information can still be divulged to some extent by analyzing the differences of parameters trained and uploaded by the IoT device. In order to solve this issue, it is necessary to add artificial noise to preventing personal information leakage; one prominent example of which is the concept of differential privacy (DP). The major goal of DP in the FL process is to ensure that a learned model does not reveal whether a certain data point was used during training [2], [4], [7].

Usually, incentive mechanism design is a subfield in economics and game theory that takes an objective-first approach to designing economic mechanisms toward desired objectives. It is used to define a strategic situation to make a system exhibits good behaviors when independent agents pursue self-interested strategies. To develop a solution concept, incentive mechanism design considers a scenario where agents have private information and the mechanism designer desires to make a social choice depending on agents' private information. In order to elicit private information from agents, the designer uses a proper incentive mechanism. Therefore, it is concerned with the design of rules and payoff functions to implement an outcome with desirable properties when self-interested agents pursue self-interested strategies. One of the major achievements of incentive mechanism design is the Vickrey-Clarke-Groves (VCG) mechanism. It has better computational properties than the original mechanism and provides a normative guide for the outcome and payments. When applying the VCG mechanism to complex incentive mechanism problems, the optimal outcome can be obtained by the results of computationally tractable heuristic algorithms [8].

In recent years, the DP is a strong privacy concept within the research community because of the strong privacy guarantee it offers, namely that the presence or absence of any individual in a data set does not significantly influence the results of analyses on the data set. The main idea of DP is that an agent perturbs its original data by adding carefully designed random noises and then directly transmits the noisy data to a data collector. Finally, the data collector is able to compute population statistics. Originally, the concept of DP has been developed as a privacy model for the interactive setting to protect the results of queries to a database. In this setting, the DP model sits between the agent submitting queries and the data collector answering them. Compared to the traditional privacy protection model, the DP has unique advantages; it has i) a solid mathematical foundation, ii) a strict definition of privacy protection, and iii) a reliable quantitative evaluation method [9], [10].

A. MAIN CONTRIBUTIONS

Based on the concepts of VCG mechanism and DP, we develop a novel federated learning scheme for the future IoT environment. To properly induce selfish IoT devices to participate in FL work, the VCG mechanism provides a normative guide for outcomes and payments. Therefore, our proposed scheme can obtain a feasible solution from the result of a computationally tractable heuristic algorithm. For the participating device's privacy in FL services, we adopt the idea of DP, and each individual device decides its own privacy level in a distributed manner. To effectively coordinate multiple devices, the learning operator pays appropriate incentives to selfish IoT devices while ensuring individual privacy levels. By considering the heterogeneity of devices, our proposed scheme can align the goals of selfish individual devices to provide good global properties. To the best of the authors' knowledge, this is the first piece of work of its kind that provides a new FL paradigm based on DP-based VCG mechanism. The main contributions of this paper are summarized as follows:

- This study considers the incentive and privacy issues in the FL platform. During the interactive learning process, system entities are mutually dependent on each other to reach a globally desirable consensus.

- According to the VCG mechanism, the learning operator properly induces selfish IoT devices by paying appropriate incentives. It can dynamically estimate devices' contributions, and provides a normative guide for an effective outcome, which is called social optimum.

- We have adopted the idea of DP to design a new privacy-preserving FL process. This approach implies each device's whole data set, which is protected against differential attacks from others while model performance is kept high in federated learning.

- We explore the cooperative interaction of different entities and jointly design an integrated scheme to strike an appropriate performance balance among conflicting requirements. The synergy effect lies in our reciprocal combination of VCG and DP mechanisms for the FL paradigm.

- Extensive experimental comparisons show that numerical results verify the effectiveness and efficiency of our proposed approach, which outperforms the existing state-of-the art protocols in terms of device's payoff, participation ratio, and system throughput in the FL platform.

B. ORGANIZATION

The remaining parts of this paper are organized as follows. Section II reviews the related work of FL paradigm, and provides the relative advantages of other existing protocols. Section III introduces the FL system model and describes the problem formulation. And then, the basic concept and idea of VCG and DP are explained briefly to design our proposed algorithm. In addition, the main steps of the proposed scheme are delineated to increase readability. Section IV presents the simulation settings and interprets the experimental results with the numerical analysis. Finally, in Section V, we conclude the paper and discuss potential future research directions.

II. RELATED WORK

As a natural extension of distributed learning, the issues of incentive based FL paradigm have been receiving more and more attention. They address the challenges of game theory, incentive mechanism, contract theory and privacy management involving collaborations of a number of IoT devices. L. Khan *et al.* present the primary design aspects for enabling FL at network edge [17]. They model the incentive-based interaction between a global server and participating devices for the FL via a Stackelberg game to motivate the participation of the devices in the FL process. The main differences between the paper [17] and our proposed scheme is the game paradigm. The incentive model in [17] is developed based on the non-cooperative game model, and our incentive model is designed based on the VCG mechanism, which is the opposite concept of non-cooperative game approach.

In [1], the *Hierarchical Incentive Federated Learning* (*HIFL*) scheme is a new FL based privacy preserving approach to facilitate collaborative machine learning among multiple model owners in mobile crowdsensing. For workers, this scheme is an incentive design method for model owners to incentivize high quality and quantity data from different worker types in the presence of information asymmetry. The contract is also designed to maximize the model owner's payoff in the federation. For model owners, to ensure the stability of a federation through preventing free-riding attacks, the *HIFL* scheme uses the coalitional game approach that rewards model owners based on their marginal contributions. Then, it employs the merge and split algorithm to study federation formation in the system model. Finally, this study provides an analysis of the equilibrium that the system model reaches after iterations of merges and splits in the presence of multiple model owners and federations [1].

The paper in [7] proposes the *Sustainable Incentive Federated Learning* (*SIFL*) scheme, which is a dynamic payoff-sharing algorithm. It is a real-time polynomial time algorithm that can compute solutions for payoff-sharing by instalment in order to achieve fair treatment among data owners. Especially, three fairness criteria are defined; i) contribution fairness, ii) regret distribution fairness, and iii) expectation fairness. For the federation and the participating data owners, these criteria are important to the FL process. The temporary mismatch between contributions and rewards has not been accounted for by existing payoff-sharing schemes. To address this limitation, this study proposes the Federated Learning Incentivizer (FLI), which can produce near-optimal collective utility while limiting data owners' regret. Extensive experimental comparisons show that the *SIFL* scheme dynamically divides a given budget among data owners in a federation by jointly maximizing the generated collective utility while minimizing the inequality among the data owners [7].

T. Song *et al.* propose the *Federated Learning Profit Allocation (FLPA)* scheme that focuses on the scenario of horizontal enterprise FL [11]. Based on the concept of Shapley value, they define formally the Contribution Index (CI) of different data providers in a FL task, and propose two efficient methods to calculate the CIs. The first method reconstructs models by updating the initial global model in FL with the gradients in different rounds and calculates the CI by the performance of these reconstructed models. The second method calculates the CI in each round by updating the global model in the previous round with the gradients in the current round and then aggregate the CIs of multiple rounds to get the final result. The key idea of these two methods is that authors only need to records intermediate results during the training process of federated learning and use these intermediate results to calculate the CIs approximately. Finally, they conduct extensive experiments on different setting to verify the effectiveness and efficiency of the proposed methods [11].

Although some researches have exploited extensively the FL control paradigm, an efficient cooperation of privacy-sensitive IoT devices has not been fully investigated. Different from the existing *HIFL*, *SIFL* and *FLPA* protocols [1], [7], [11], our DP-preserving FL approach can make

rational decisions in a cooperative manner while effectively ensuing mutual advantages; it has more potential benefits for the distributed FL paradigm.

III. THE PROPOSED PRIVACY-PRESERVING FL ALGORITHM

In this section, a brief description of the FL infrastructure is presented with a review of the VCG and DP mechanisms. Based on the proposed joint model, we elaborate the main challenges of our privacy-preserving FL algorithm while discussing relevant control issues in IoT environments. Finally, the main step procedures of our proposed algorithm are delineated to help readers understand better.

A. IOT SYSTEM INFRASTRUCTURE FOR FEDERATED LEARNING

In this work, a distributed FL system platform in IoT environment is taken. In this structure, $\mathcal{O} = \{O_1, \ldots, O_n\}$ is the set of learning operators, and $\mathcal{D} = \{D_1, \ldots, D_m\}$ is the set of IoT devices. IoT devices are local data owners, and have the computation capability for the federated learning process. They can be assumed as FL workers, and willing to join the model training process in the machine learning paradigms. Each FL worker $D_i \in \mathcal{D}$ maintains a set of private local data χ_{D_i}. $\mathbb{S}_{O_j}$ is the set of IoT devices, which are covered by the $O_j \in \mathcal{O}$. Each O has its budget (I_O) constraint to induce local devices to participate in the FL process. In this study, the interactive situation of learning operators and IoT devices is formulated as a game ($\mathbb{G}$) in a coordination manner; $\mathbb{G}$ is operated in a slotted time structure and FL process is implemented at each time period. Formally, we define game entities, i.e., $\mathbb{G} = \{\{\mathcal{O}, \mathcal{D}\}, \{D_i \in \mathcal{D} \mid \chi_{D_i}\}, \{O_j \in \mathcal{O}, \mathbb{S}_{O_j} \subset \mathcal{D} \mid D_i \in \mathbb{S}_{O_j}\}, \{D_i \in \mathcal{D}, D_i \in \mathbb{S}_{O_j} \mid U_{D_i}^{O_j}\}, I_{O_j \in \mathcal{O}}, \psi_{D_i \in \mathcal{D}}, T\}$ of gameplay.

- $\mathcal{O}$ and $\mathcal{D}$ are game entities for the $\mathbb{G}$. They are related in a manner of mutual and reciprocal interdependency.
- $\mathbb{S}_{O_j}$ is the set of IoT devices, which are contacted to the operator O_j where $\mathcal{D} = \bigcup_{O_j \in \mathcal{O}} \mathbb{S}_{O_j}$.
- $U_{D_i}^{O_j}$ is the D_i's utility function for his FL service where $D_i \in \mathbb{S}_{O_j}$. This function maps the D_i's satisfaction to a real number, which represents the resulting outcome in the game $\mathbb{G}$.
- $I_{O_j \in \mathcal{O}}$ is the O_j's limited budget amount. It is distributed into the FL-participating devices based on the incentive mechanism.
- χ_{D_i} is the D_i's generated task, which can be assumed as a local data load for the FL process. It is generated independently in the individual D_i.
- $T = \{t_1, \ldots, t_c, t_{c+1}, \ldots\}$ denotes time, which is represented by a sequence of time steps.

B. THE BASIC CONCEPTS OF DIFFERENTIAL PRIVACY

In 2006, Cynthia Dwork first proposed a mathematically-rigorous mechanism, called DP, which formally guarantees specific levels of privacy, even from powerful adversaries with side information. DP mechanisms protect the private data by adding noise on the query answers; a common way of achieving DP is a perturbation of aggregated statistics by calibrated noise. So, regardless of the background knowledge, the attackers cannot infer any individual information even though all the information of other users is leaked and controlled. Due to its simplicity and desirable features, this model has attracted the attention of many researchers in computer science and statistics. Nowadays, DP has become a powerful tool and provides strong privacy guarantees for algorithms on aggregate databases [12], [13].

For any data sets χ_{O_i} and χ_{O_j} that differ by one record, a randomized algorithm $\mathbb{A}$ provides DP protection with $\mathcal{E}$ value ($\mathcal{E}$-DP) if and only if the following is satisfied [13], [14]:

$$Pr\left[\mathbb{A}\left(\chi_{O_i}\right) = \mathcal{S}\right] \leq \left(exp\left(\mathcal{E}\right) \times Pr\left[\mathbb{A}\left(\chi_{O_j}\right) = \mathcal{S}\right]\right)$$
$$\equiv \frac{Pr\left[\mathbb{A}\left(\chi_{O_i}\right) = \mathcal{S}\right]}{Pr\left[\mathbb{A}\left(\chi_{O_j}\right) = \mathcal{S}\right]} \leq exp\left(\mathcal{E}\right) \quad (1)$$

where $\mathcal{S}$ is the output threshold of algorithm $\mathbb{A}$, and $\mathcal{E}$ is a parameter to measure the privacy level of the algorithm. Eq.(1) indicates that by using the χ_{O_i} and χ_{O_j} as an input of the privacy protection algorithm $\mathbb{A}$. Therefore, if the attacker knows most of the records in the original data set, he still cannot accurately determine whether a record is in χ_{O_i} and χ_{O_j}. The smaller $\mathcal{E}$ value, the lower is the probability of distinguishing the two datasets and the higher the degree of privacy protection [13], [14].

For realizing the DP, Laplace mechanism is proposed to achieve DP protection of published data. For a query function $\mathcal{F}$, the DP mechanism generates the actual result $\mathcal{F}(\chi_O)$ and adds Laplacian noise to the response of the query. In order to achieve $\mathcal{E}$-DP protection, the output of $\mathbb{A}$ is defined with a continuous random variable γ [13]–[15];

$$\mathbb{A}(\chi_O) = \mathcal{F}(\chi_O) + \gamma,$$
$$\text{s.t., } P(\gamma) = \frac{1}{2 \times \psi} \times exp\left(-\frac{|\gamma|}{\psi}\right) \quad (2)$$

where ψ is a scale parameter, sometimes referred to as the diversity; the value of ψ depends on the privacy parameter $\mathcal{E}$. The random variable γ satisfies the Laplace distribution according to Eq.(2). The amount of added noise depends on the sensitivity, which is the maximum change in the query result after the removal of a record from the dataset or the addition of a record to the dataset, i.e., the added noise level is closely related to the global sensitivity. This can be defined mathematically, and is known as the sensitivity ($\Delta \mathcal{F}$) of the query function $\mathcal{F} : \chi_O \rightarrow R^d$ where R represents the mapped real space and d represents the query dimension of the function $\mathcal{F}$ [13], [14];

$$\Delta \mathcal{F} = \max_{\chi_{O_i}, \chi_{O_j}} \left\| \mathcal{F}\left(\chi_{O_i}\right) - \mathcal{F}\left(\chi_{O_j}\right) \right\| \quad (3)$$

Let noise from the Laplace distribution denote the Laplace noise, which is obtained where $\psi = \Delta \mathcal{F} / \mathcal{E}$ in the Laplace distribution. According to the new study of C. Dwork,

there is a proof that the $\mathcal{E}$-DP is guaranteed to a sensing task by adding a random Laplace noise [15].

C. THE FUNDAMENTAL IDEA OF VCG MECHANISM

Usually, mechanism design considers a scenario where agents have private information and the mechanism designer desires to make a social choice depending on agents' private information. In order to elicit private information from agents, the designer uses a proper incentive mechanism. One of the major achievements of mechanism design is the *Vickrey-Clarke-Groves* (VCG) mechanism, which has two desirable features; *direct-revelation* and *incentive-compatibility*. *Direct-revelation* means that the only actions available to agents are to make direct claims about their preferences to the mechanism. *Incentive-compatibility* captures the essence of designing a mechanism to overcome the self-interest of agents; each agent's dominant strategy is truth telling about its type. Therefore, whatever any other agent reports any type, agents can be truthful. The VCG mechanism has better computational properties than the original mechanism and can provide a normative guide for the outcome and payments [8], [16].

A mechanism $\mathcal{M}$ selects an outcome from a set of possible outcomes $\mathfrak{P}$, based on inputs from a set of agents. Each agent i has a valuation function $v_i : \mathfrak{P} \to \mathbb{R}$ where $\mathbb{R}$ is the set of nonnegative real numbers. The quantity $v_i(a)$ represents the value that the agent i assigns to outcome $a \in \mathfrak{P}$. Let $V(a)$ be the value the mechanism designer has for outcome a. We say that a mechanism $\mathcal{M}$ is truthful if it is a dominant strategy for agent i to report his valuation truthfully. For each agent i, each valuation function $v_i(\cdot)$, agent i's bid $b_i(\cdot)$ and each possible report b_{-i} of the other agents, truthful mechanism can be formally defined as follows [16];

$$u_i[v_i, b_{-i}|v_i] \geq u_i[b_i, b_{-i}|v_i]$$
$$\text{s.t.,} \begin{cases} u_i[b_i, b_{-i}|v_i] = v_i(a(b)) - p_i(b) \\ b = (b_1(\cdot), b_2(\cdot), \ldots, b_n(\cdot)) \end{cases} \tag{4}$$

where $a(b) \in \mathfrak{P}$ is the outcome selected by $\mathcal{M}$ on input b, and $p_i(b)$ is the payment of agent i. The agent i's utility function $u_i[\cdot]$ is quasi-linear; it is applicable when the value is measured in the same units as the payments. Commonly, $\left(\sum_i v_i(a) + V(a)\right)$ and $\left(\sum_i b_i(a) + V(a)\right)$ are the social surplus and reported social surplus of an outcome a, respectively. In the VCG mechanism, each individual agent is asked to report his valuation function $v_i(\cdot)$ and submits a function $b_i(\cdot)$, which may or may not equal $v_i(\cdot)$ [16]. The outcome is given by

$$a^* := a^*(b) = \arg \max_a \left(\sum_j b_j(a) + V(a) \right) \tag{5}$$

With respect to the reported bids, the agent i's payment $p_i(\mathbf{b})$ is the loss his presence causes others. It can be formally defined as follows [16];

$$p_i(\mathbf{b}) = \max_a \left(\sum_{j \neq i} b_j(a) + V(a) \right) - \left(\sum_{j \neq i} b_j(a^*) + V(a^*) \right) \tag{6}$$

In the Eq.(6), the first term is the total reported value that the other agents would obtain if the agent i was absent, and the second term is the total reported value the others obtain when the agent i is present [16]. Simply, we can assume that $V(a)$ for all outcomes a is 0 while fixing the reports $\mathbf{b}_{-i}$ of all agents except agent i. Suppose that agent i's true valuation function is $v_i(\cdot)$, but he reports $b_i(\cdot)$ instead where $v_i(\cdot) \neq b_i(\cdot)$. Then the outcome a^* and the agent i's payment are defined as follows [16];

$$a^* = \arg \max_a \sum_j b_j(a)$$
$$\text{and} \quad p_i(b) = \max_a \sum_{j \neq i} b_j(a) - \sum_{j \neq i} b_j(a^*) \tag{7}$$

Simply, we can think the term $\max_a \sum_{j \neq i} b_j(a)$ as a constant because the agent i's report has no influence on this term. Therefore, the agent i's utility is given by;

$$u_i(b \mid v_i) = (v_i(a^*) - p_i(b))$$
$$= \left(v_i(a^*) - \left(\max_a \sum_{j \neq i} b_j(a) - \sum_{j \neq i} b_j(a^*) \right) \right) \tag{8}$$

On the other hand, if the agent i were to report his true valuation function $v_i(\cdot)$, the agent i's outcome and utility are defined as follows;

$$\begin{cases} a' = \arg \max_a \left(v_i(a) + \sum_{j \neq i} b_j(a) \right) \\ u_i[(v_i, \mathbf{b}_{-i}|v_i)] \\ = v_i(a') - \left(\max_a \sum_{j \neq i} b_j(a) - \sum_{j \neq i} b_j(a') \right) \end{cases} \tag{9}$$

For every b and $v_i(\cdot)$,

$$u_i[\mathbf{b}|v_i] \leq u_i[v_i, \mathbf{b}_{-i}|v_i]$$
$$\equiv \left(v_i(a^*) - \left(\max_a \sum_{j \neq i} b_j(a) - \sum_{j \neq i} b_j(a^*) \right) \right)$$
$$\leq \left(v_i(a') - \left(\max_a \sum_{j \neq i} b_j(a) - \sum_{j \neq i} b_j(a') \right) \right) \tag{10}$$

According to Eq.(10), we can say that the VCG is a truthful mechanism while maximizing social surplus [8], [16].

D. THE PROPOSED DP-BASED VCG MECHANISM FOR FEDERATED LEARNING

In the game $\mathbb{G}$, each D's valuation function is defined considering its DP strategy. For example, each FL task is generated with its own $\mathcal{E}$ value. In the D_i, its valuation function $v_{D_i}(\cdot)$ is defined as follows;

$$v_{D_i}\left(\psi_{D_i}, \mathcal{E}_{D_i}, \mathfrak{X}_{D_i}^c\right)$$
$$= \xi \times \left(\frac{\alpha}{\beta + \exp\left(-\frac{\Omega_{D_i}}{\mathfrak{M}}\right)} - \varrho\right) - \mathcal{F}\left(\mathfrak{X}_{D_i}^c\right)$$
$$\text{s.t., } \Omega_{D_i} = \chi_{D_i} \times \left(\frac{1}{\mathcal{E}_{D_i}} + \zeta\right)$$
$$\text{and } \mathcal{F}\left(\mathfrak{X}_{D_i}^c\right) = \mu \times \log\left(\exp\left(\mathfrak{X}_{D_i}^c\right)\right) \quad (11)$$

where $\xi, \alpha, \beta, \varrho, \zeta$ and μ are coefficient parameters for the valuation function $v_{D_i}(\cdot)$, which is a function to represent the D_i's payoff with its privacy sensitivity. $\mathfrak{M}$ is the modification factor for the local data size. $\mathfrak{X}_{D_i}^c$ is the total executed FL task until the current time t_c. Based on the $v_{D_i}(\cdot)$, the D_i's utility function $U_{D_i}^{O_j}(\cdot)$ can be given by;

$$U_{D_i}^{O_j}\left(\psi_{D_i}, \mathcal{E}_{D_i}, O_j, \mathfrak{X}_{D_i}\right)$$
$$= \left(\psi_{D_i}, \mathcal{E}_{D_i}, O_j, \mathfrak{X}_{D_i} \mid D_i \in \mathbb{S}_{O_j}\right) - \mathfrak{P}_{D_i}\left(\mathbb{S}_{O_j}\right) \quad (12)$$

where $\mathcal{P}_{D_i}(\cdot)$ is the payment for the D_i; it is estimated by the O_j according to Eq.(6). In the viewpoint of O, this value should be decided to guide selfish nodes toward a socially optimal outcome. Based on the basic idea of VCG mechanism, the $\mathcal{P}_{D_i}\left(\mathbb{S}_{O_j}\right)$ is defined with the information of $\mathbb{S}_{O_j}$ and ψ_D;

$$\mathcal{P}_{D_i}\left(\mathbb{S}_{O_j}\right)$$
$$= \sum_{\substack{D_j \in \mathbb{S}_{O_j} \\ D_j \neq D_i}} F_a\left(\Omega_{D_j}\right) - \sum_{\substack{D_j \in \mathbb{S}_{O_j} \\ D_j \neq D_i}} F_b\left(\Omega_{D_j}\right)$$
$$\text{s.t., } \begin{cases} F_a\left(\Omega_{D_j}\right) = \max_{\mathbb{I}_{j}=0 \text{ or } 1}\left(\tau \times \log(\exp(\Omega_{D_j} \times I_j))\right) \\ F_b\left(\Omega_{D_j}\right) = \left(\max_{\mathbb{I}_{j}=0 \text{ or } 1} \Delta \times \log(\exp(\Omega_{D_j} \times I_j))\right) \end{cases}$$
$$(13)$$

where τ and Δ are benefit conversion factors for the $F_a(\cdot)$ and $F_b(\cdot)$, respectively. In this study, we have developed a new DP-based incentive algorithm for a FL system infrastructure. By adopting the main concepts of DP and VCG mechanisms, multiple IoT devices can get rewards fair-efficiently for their FL contributions. To design our proposed scheme, we formulate the mutual-interactive relationship of system entities as a cooperative game model. Therefore, multiple IoT devices work together through the dynamics of FL system to ensure a well-balanced system performance. By considering the individual privacy preferences, the goal of our approach is to define rules and payoff functions to reach a desired outcome, which is called social optimum. The main steps of the proposed scheme can be described as follows:

Step 1: For our simulation model, the values of system parameters and control factors can be discovered in Table 1, and the simulation scenario is given in Section IV.

TABLE 1. System parameters used in the simulation experiments.

Parameter	Value	Description
n	10	the number of operators in the FL system
m	50	the number of IoT devices in the FL system
l_o	10K	the initial energy of D
ϱ	0.5	a coefficient parameter for the $v_D(\cdot)$
α, β	1, 1	coefficient parameters for the $v_D(\cdot)$
μ	0.5	a coefficient parameter for the $v_D(\cdot)$
τ	0.5	a benefit conversion factor for the $F_a(\cdot)$
Δ	0.6	a benefit conversion factor for the $F_b(\cdot)$
ξ	10	a coefficient parameter for the $v_D(\cdot)$
ζ	1	a coefficient parameter for the $v_D(\cdot)$
$\mathfrak{M}$	10 Mb	the modification factor for the local data size
$\mathcal{E}$	$1.25 \leq \mathcal{E} \leq 2$	the range of available privacy levels for D

Task	Size of Local Data Set (χ_D)	FL Working Duration
Task I	10 Mb	180 t-unit
Task II	7.5 Mb	90 t-unit
Task III	12.5 Mb	60 t-unit
Task IV	15 Mb	120 t-unit
Task V	17.5 Mb	180 t-unit
Task VI	20 Mb	40 t-unit

Step 2: In each time step of FL process, individual IoT devices generate their learning tasks (χ) with privacy preferences. According to Eq.(1)-(3), the concept of DP is applied for each device with its privacy level ($\mathcal{E}$).

Step 3: In each device, its valuation function $v_D(\cdot)$, and utility function U_D^O are defined according to Eq.(11) and Eq.(12). These functions include the ideas of DP and VCG mechanisms.

Step 4: For each device, the $\mathcal{P}_D(\cdot)$ is calculated by the D's corresponding operator O. Individual operator $O \in \mathcal{O}$ is held responsible for its covering devices in the set $\mathbb{S}_O$ through the $\mathbb{G}$ game model.

Step 5: The $\mathcal{P}_D(\cdot)$ value is estimated based on the fundamental concept of the VCG mechanism. According to Eq.(4)-(10), the Eq.(13) is developed for the $\mathcal{P}_D(\cdot)$, and the O may pay the $\mathcal{P}_D(\cdot)$ within his permissible range I_O.

Step 6: Individual IoT devices make control decisions to get mutual advantages, and work together through the FL process while striking the appropriate system performance.

Step 7: In a coordinated manner, operators and devices are interactively dependent with each other to ensure a relevant balance between efficiency and fairness principles.

Step 8: Constantly, the game entities are self-monitoring the current FL platform situations, and proceed to Step 2 for the FL process.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of our proposed scheme and report the experimental results while comparing with other existing *HIFL*, *SIFL* and *FLPA* schemes [1], [7], [11]; these existing schemes are recently published state-of-the-art FL protocols. First, we describe the experiment settings and simulation scenario, and then present the numerical analysis to draw insights for validation. It shows how our proposed protocol works effectively. The assumptions of our simulation environments are as follows:

- The simulated FL system platform consists of 10 learning operators and 50 IoT devices where $|\mathcal{O}| = 10$ and $|\mathcal{D}| = 50$.
- Multiple IoT devices are regularly positioned. Therefore, one operator is associated with 5 devices.
- Each device generates its task (χ_D), which are six different kinds of service types based on the local data load. In each device, tasks are generated randomly.
- Each device has its budget amount (I_O) to give payments for its corresponding FL working devices.
- Each task (χ_D) gets its own privacy preference ($\mathcal{E}$) for the DP mechanism. The $\mathcal{E}$ value range is between 1.25 and 2; it is randomly decided for each individual χ_D.
- The process for task generations in individual devices is Poisson with rate λ (tasks/s), and the range of offered task load was varied from 0 to 3.0.
- System performance measures obtained on the basis of 100 simulation runs are plotted as a function of the offered task request load.
- Performance measures obtained are normalized device's payoff, FL participation ratio, and system throughput in the FL platform.
- For simplicity, we assume the absence of physical obstacles in the wireless communications between learning operators and IoT devices.

In Fig.1, we observe that the device's payoff in the FL process when the task generation rate increases. It is computed as the profit that devices can potentially derive from joining the FL model with the distributed respective. In the point view of individual IoT devices, this is the most important performance criterion. The more task generations in each device, the more profit is obtained. The simulation results reveal that our DP-based VCG mechanism can guarantee the more profit than any other protocols under light to heavy task load generations. It leads to higher device's payoff in the distributed FL system. In contrast with the *HIFL*, *SIFL* and *FLPA* schemes, we develop an effective incentive
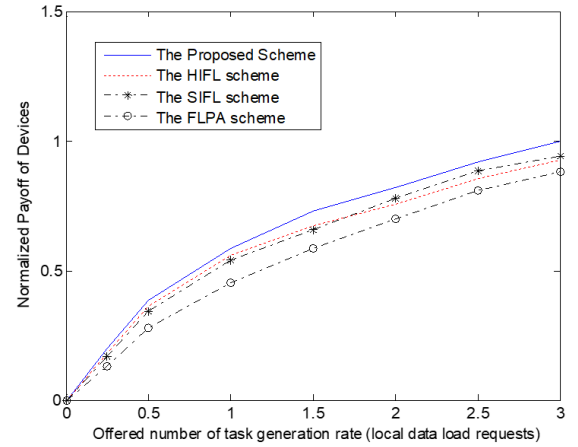

FIGURE 1. Normalized payoff of devices.

mechanism design while considering the DP idea. It is a primary advantage of our proposed method.

As illustrated in Fig.2, we can see that the FL participation ratio of devices among different protocols. Under diversified local data load changes, the device participation as a FL worker is another prominent issue in the FL operation. In this study, our main goal is to guide selfish devices toward a socially optimal outcome. Therefore, we design a socially desirable game rule, and fine tune the limited system resource to increase the rate of device participations. One of major novelty of our proposed scheme is to provide the best compromise in the presence of current system conditions until the best solution has been found during the FL process. Fig.2 confirms that we can fair-efficiently share the limited system resource to effectively facilitate individual devices while maintaining a higher device participation ratio than the existing state-of-the-art FL protocols.
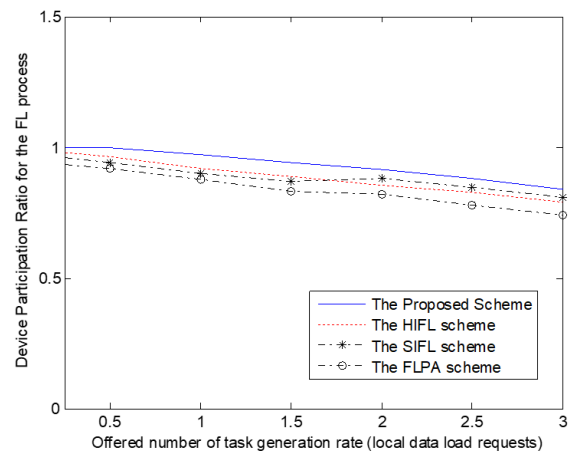

FIGURE 2. Device participation ratio for the FL process.

Fig.3 shows the comparison results about the system throughput in the FL platform. Usually, the system throughput increases in proportion to the device's payoff; it is intuitive correct. Therefore, it is strongly related to the device's payoff, and the performance trend showing
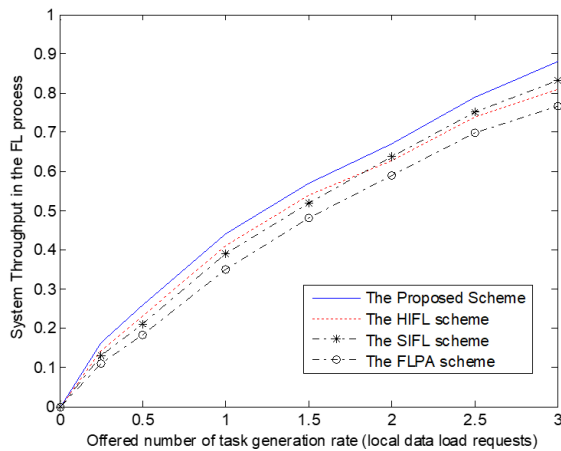
FIGURE 3. System throughput in the FL platform.

in Fig.3 is very similar to the curves in Fig.1. Thus, similar conclusions to the ones of Fig.1 are reached. Under different local data loads, our VCG-based incentive technique can align the goals of system entities with desirable characteristics. So, we can effectively make selfish IoT devices work together in an interactive manner while attempting to enhance the impact of our game paradigm. From the simulation results shown in Fig.1 to Fig.3, we can confirm that our proposed DP-based VCG mechanism can attain an appropriate performance balance in the FL system platform while outperforming the existing *HIFL*, *SIFL* and *FLPA* schemes.

V. SUMMARY AND CONCLUSION

Recently, distributed learning approaches such as FL have gained attention due to the large size of the training data. However, the system performance of FL suffers from heterogeneous participants. In this paper, we design a novel FL control scheme based on the joint model with VCG and DP mechanisms. By using the idea of VCG, the learning operator calculates each incentive as a reward for an individual IoT device; it can encourage selfish IoT devices to actively participate in the FL process. Based on the concept of DP, we can retain a provable learning performance with the consideration on preserving devices' privacy. By taking into account the current FL system condition, system entities in our scheme work together, and act cooperatively with each other toward an appropriate learning performance in a real-time online manner. Extensive experimental comparisons with three existing *HIFL*, *SIFL* and *FLPA* protocols show that our proposed approach can get the most attractive learning performance while achieving the higher device's payoff, participation ratio, and system throughput in the FL platform. The conclusion of this study gives us an insight that the joint control model of VCG and DP mechanisms can ensure a significant performance improvement in the FL paradigm.

For the future work, our current study can be extended in a number of ways. One future direction is to design a new FL framework to facilitate collaborative machine learning among multiple model owners in mobile crowdsensing. Another potential direction for the future research is to introduce a reputation concept as the metric to measure the reliability and trustworthiness of the mobile IoT devices. Therefore, we will design a novel reputation-based worker selection scheme for a reliable FL process by using a multi-weight subjective logic model. In addition, we can develop a decentralized paradigm for the big data-driven cognitive computing system by jointly using the FL paradigm and blockchain technology. Finally, we will consider the problems of adversarial classifier evasion, where the attacker changes behavior to escape being detected, and poisoning, where training data itself is corrupted.

COMPETING OF INTERESTS
The author declares that there are no competing interests regarding the publication of this paper.

AUTHOR' CONTRIBUTION
The author is a sole author of this work and ES (i.e., participated in the design of the study and performed the statistical analysis).

AVAILABILITY OF DATA AND MATERIAL
Please contact the corresponding author at swkim01@ sogang.ac.kr.

REFERENCES
[1] W. Y. B. Lim, Z. Xiong, C. Miao, D. Niyato, Q. Yang, C. Leung, and H. V. Poor, "Hierarchical incentive mechanism design for federated machine learning in mobile networks," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9575–9588, Oct. 2020.
[2] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. S. Quek, and H. V. Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454–3469, 2020.
[3] K. Toyoda and A. N. Zhang, "Mechanism design for an incentive-aware blockchain-enabled federated learning platform," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2019, pp. 395–403.
[4] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10700–10714, Dec. 2019.
[5] 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.
[6] 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.
[7] H. Yu, Z. Liu, Y. Liu, T. Chen, M. Cong, X. Weng, D. Niyato, and Q. Yang, "A sustainable incentive scheme for federated learning," *IEEE Intell. Syst.*, vol. 35, no. 4, pp. 58–69, Jul. 2020.
[8] S. Kim, *Game Theory Applications in Network Design*. Hershey, PA, USA: IGI Global, 2014.
[9] J. Soria-Comas, J. Domingo-Ferrer, D. Sánchez, and D. Megías, "Individual differential privacy: A utility-preserving formulation of differential privacy guarantees," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1418–1429, Jun. 2017.
[10] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3628–3636, Aug. 2018.
[11] T. Song, Y. Tong, and S. Wei, "Profit allocation for federated learning," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2019, pp. 2577–2586.

[12] Q. Wang, Z. Li, Q. Zou, L. Zhao, and S. Wang, "Deep domain adaptation with differential privacy," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3093–3106, 2020.

[13] G. Yang, X. Ye, X. Fang, R. Wu, and L. Wang, "Associated attribute-aware differentially private data publishing via microaggregation," *IEEE Access*, vol. 8, pp. 79158–79168, 2020.

[14] Y. Yan, X. Gao, A. Mahmood, T. Feng, and P. Xie, "Differential private spatial decomposition and location publishing based on unbalanced quadtree partition algorithm," *IEEE Access*, vol. 8, pp. 104775–104787, 2020.

[15] C. Dwork, "A firm foundation for private data analysis," *Commun. ACM*, vol. 54, no. 1, pp. 86–95, Jan. 2011.

[16] A. R. Karlin and Y. Peres, *Game Theory, Alive*. Providence, RI, USA: AMS, 2017.

[17] U. L. Khan, S. R. Pandey, H. N. Tran, W. Saad, Z. Han, N. H. M. Nguyen, and C. S. Hong, "Federated learning for edge networks: Resource optimization and incentive mechanism," 2019, *arXiv:1911.05642*. [Online]. Available: http://arxiv.org/abs/1911.05642
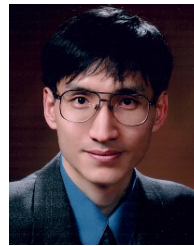
SUNGWOOK KIM received the B.S. and M.S. degrees in computer science from Sogang University, Seoul, South Korea, in 1993 and 1995, respectively, and the Ph.D. degree in computer science from Syracuse University, Syracuse, NY, USA, in 2003, supervised by Prof. Pramod K. Varshney. He has held Faculty positions with the Department of Computer Science, Choongang University, Seoul. He is currently a Professor with the Department of Computer Science and Engineering, Sogang University, where he is also a Research Director of the Network Research Laboratory. His research interests include resource management, online algorithms, adaptive quality-of-service control, and game theory for network design.

• • •