Management Science

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Understanding Partnership Formation and Repeated Contributions in Federated Learning: An Analytical Investigation

Xuan Bi, Alok Gupta, Mochen Yang

To cite this article:
Xuan Bi, Alok Gupta, Mochen Yang (2024) Understanding Partnership Formation and Repeated Contributions in Federated Learning: An Analytical Investigation. Management Science 70(8):4974-4994. https://doi.org/10.1287/mnsc.2023.00611

https://pubsonline.informs.org/journal/mnsc

MANAGEMENT SCIENCE
Vol. 70, No. 8, August 2024, pp. 4974–4994
ISSN 0025-1909 (print), ISSN 1526-5501 (online)

Understanding Partnership Formation and Repeated Contributions in Federated Learning: An Analytical Investigation

Xuan Bi,[a] Alok Gupta,[a] Mochen Yang[a,*]

[a] Carlson School of Management, University of Minnesota, Minneapolis, Minnesota 55455
*Corresponding author
Contact: xbi@umn.edu, https://orcid.org/0000-0002-4683-1411 (XB); gupta037@umn.edu, alok@umn.edu, https://orcid.org/0000-0002-2097-1643 (AG); yang3653@umn.edu, https://orcid.org/0000-0001-5101-9041 (MY)

Received: February 24, 2023
Revised: June 27, 2023
Accepted: July 13, 2023
Published Online in Articles in Advance: October 17, 2023

https://doi.org/10.1287/mnsc.2023.00611

Abstract. Limited access to large-scale data is a key obstacle to building machine learning (ML) applications in practice, partly due to a reluctance of information exchange among data owners out of privacy and data security concerns. To address this "information silo" problem, federated learning (FL) techniques have been proposed to enable decentralized model training via an orchestrating central server and have received increasing attention in several industries (including healthcare and finance). Despite its superior privacy protection property, adoption of FL is limited by a lack of systematic understanding of its underlying economics. In this paper, we take an analytical approach to answer two questions: (1) when do data owners prefer to form a FL partnership over building ML models by themselves and (2) how can different contractual mechanisms be used to promote repeated contributions to FL (the cooperative outcome that benefits all participants). We formulate an iterated prisoner's dilemma (IPD) model that accounts for unique FL characteristics, including the specification of the payoff matrix and the involvement of a central server to sanction noncooperation. We find that partnership formation requires participants to be not too forward-looking in temporal preferences, which is contrary to the conventional wisdom in IPD. Furthermore, to promote repeated contributions, it is insufficient to only rely on penalties imposed by the central server or by participants for noncooperation, but a combination of both is enough. Our work advances theoretical understanding of the economics of FL and provides prescriptive insights that can inform FL participant selection and contract design.

History: Accepted by D. J. Wu, information systems.

Funding: This work was partially supported by Cisco Research.
Supplemental Material: The online appendices are available at https://doi.org/10.1287/mnsc.2023.00611.

Keywords: federated learning • information silo • analytical modeling • iterated prisoner's dilemma • data privacy

1. Introduction

The lack of access to large-scale and high-quality data are one of the critical barriers to building practical machine learning (ML) applications. In many domains, the advantage of data abundance is offset by the challenge that data are scattered and fragmented—often owned by separated individuals or organizations in disconnected "information silos." For example, data on patients and diseases are typically collected and held by individual healthcare providers (e.g., individual hospitals or hospital systems) with limited information exchange (Miller and Tucker 2014). Similarly, consumer data, such as financial information, shopping history, online journeys, transaction records, or demographics, are often scattered across different financial institutions, retailers, insurance companies, or data brokers (Kairouz et al. 2019). This "information silo" problem greatly limits the applicability and quality of ML applications in practice (Miller and Tucker 2014, Yang et al. 2019).

Privacy and data security concerns are among the key reasons of data owners' reluctance to share information with each other. Taking the healthcare industry as an example, data breaches are extremely costly to providers (Bai et al. 2017, McCoy and Perlis 2018), and privacy protection regulations have been shown to inhibit the adoption of enterprise electronic health record technology that enables information exchange (Miller and Tucker 2009).

To address this information silo problem while also safeguarding data privacy and security, *federated learning* (FL) stands out as a novel computational approach that enables decentralized training of ML models.

Originally developed by Google,[1] FL allows multiple parties to collectively train a ML model without the need to share the raw data with each other. Specifically, each party privately uses its own data to train and update a *local model* and then shares the local model (but *not* the raw data used during training) with a central server. The server then aggregates the local models (via certain FL algorithm, such as Federated Averaging (FedAvg); McMahan et al. 2017) to effectively construct a *global model*. Models trained via FL have been shown to achieve very similar levels of performance as if the actual data were pooled together (Sheller et al. 2020).

Despite growing research interests in FL (Kairouz et al. 2019), deploying FL in the real world still faces considerable challenges. Through open-ended interviews of several FL researchers and practitioners (see Online Appendix A for more details), we identified notable challenges regarding *partnership formation* and *long-term contribution*. The healthcare industry again offers a case in point. Currently, FL among healthcare institutions is typically one-shot partnerships formed in ad hoc manners (Sheller et al. 2020, Dayan et al. 2021). In particular, partnership formation usually relies on preexisting relationships (e.g., personal relationships among scientists of different institutions who are interested in leading FL efforts), and the partnership dissolves after a global model is trained, without updating that model in the long term as new data becomes available. For institutions that do not necessarily have established relationships, forming an FL partnership usually takes substantial effort. Even after a partnership is formed, it can be vulnerable to strategic behaviors of certain participants who reduce contribution efforts, stop contributing, or engage in adversarial activities (Zhang et al. 2022). Lack of long-term engagement may also limit the quality of FL models, especially because the performance of a model can deteriorate over time due to changes in data (e.g., distributional shifts) and external environments.

At the root of these challenges lies the lack of systematic understanding of the economic incentives and tradeoffs involved in FL. Therefore, in this paper, we seek to advance the theoretical knowledge of factors that may contribute to or hinder the success of FL by asking the following two fundamental research questions:

1. **RQ1 (Partnership Formation):** Under what conditions would data owners prefer to participate in FL (rather than building ML models by themselves)?
2. **RQ2 (Long-Term Contribution):** How to promote repeated contributions among participants in the long term?

These two research questions are closely connected. RQ1 seeks to understand when it is more advantageous for data owners to form a FL partnership over building ML models with their own private data. Conditional on partnership formation, RQ2 then seeks to examine several contractual mechanisms and analyze their effectiveness in promoting repeated contributions. To answer these questions, we leverage a game theoretical model known as the *iterated prisoner's dilemma* (IPD). In a basic model, we consider an IPD with two identical players (i.e., two data owners), each deciding whether to form a FL partnership and, if so, whether to cooperate (i.e., contribute its local model with the central server) or to defect (i.e., do not contribute) in every round of the game. For RQ1, we solve the game to derive boundary conditions for partnership formation. For RQ2, we consider several contractual mechanisms and analyze their effectiveness in preventing defection and promoting repeated cooperation.[2] Beyond the basic model, we further examine (1) two alternative ways in which players may defect (making partial contribution or adversarial contribution, Section 4.4) and (2) the case of two heterogeneous players that differ in several important characteristics as well as the case of multiple players with more than one defector (Section 5). These analyses generate nuanced and practically relevant insights about cooperation dynamics in FL.

Importantly, our model is informed by a few unique features of FL. First, besides the decision to cooperate versus to defect, each player also has an outside option of simply not participating in the FL and instead building the ML model by itself. We therefore need to solve for the partnership formation conditions and the repeated contribution conditions separately. Second, the specifications of utility and cost associated with players' decisions, as well as the design of the payoff matrix, all reflect characteristics of data-driven ML tasks. For example, the utility gain from FL saturates as the amount of data increases, following the observation that ML models' performance improvement typically slow down with more data. The payoff matrix specification leads to findings that are different from those in a standard IPD model. Third, the existence of a central server in a FL partnership gives rise to a novel contractual mechanism, which we refer to as *sanction* (i.e., temporarily denying a defector's access to the global model). This sanction mechanism is different from other contractual mechanisms commonly studied in an IPD setting, for example, the trigger strategies such as grim trigger or tit-for-tat. These unique features of FL motivate the formulation of our model and capture the key tensions of a FL partnership.

Our analyses show that long-term FL partnership formation requires players to have low-cost sensitivity, have access to a small amount of new information per round, and are not too forward-looking in temporal preferences. The finding on temporal preference stands in contrast to the conventional wisdom of IPD models, where the cooperative outcome typically requires participants to be not too myopic. Furthermore, players who are "on board" with FL may nevertheless choose to defect during the FL process, unless the proper contractual mechanism is adopted. We find that neither a server-imposed sanction nor a player-initiated trigger

strategy alone can fully prevent defection, but a combination of the two would be sufficient. These results generally remain robust when defection takes the form of partial or adversarial contributions (with a few nuances to be discussed later).

Our work makes both theoretical and prescriptive contributions. FL is an emerging technology that has already started to impact healthcare, finance, and other industries, and we are among the first to formulate and analyze the incentives and strategic tradeoffs associated with FL. Taking an analytical approach, we advance the understanding of economic decisions faced by participants in long-term FL and derive the boundary conditions under which participants would be willing to form an FL partnership and engage in repeated contributions to build a ML model. These theoretical insights also have significant practical value. For instance, our results on the effectiveness of several contractual mechanisms in preventing defection can serve as the basis for contract design in FL. In the case of heterogeneous participants, our analyses can identify the "bottleneck" player that determines the success of a FL partnership, thereby informing FL client selection (an important yet underexplored problem in FL; Donahue and Kleinberg 2021b). Finally, our model and the findings are broadly relevant for different contexts where FL may be applied (e.g., healthcare providers, finance and insurance institutions, pharmaceutical companies, smart manufacturers, and geo-distributed data centers).

2. Related Literature

In this section, we briefly review relevant literature on FL and iterated prisoner's dilemma, which inform our theoretical model.

2.1. Federated Learning

In general, FL is defined as a machine learning paradigm where multiple clients cooperate to solve one (or more) learning problem under central orchestration (Kairouz et al. 2019, Li et al. 2020). While keeping the raw data sets local and private, participating clients share intermediate statistics (such as gradients) of their local models with a central server, which aggregates the information to construct a global model and share it with all the clients. With advancements in complementary technologies such as 5G networks and Internet-of-Things (IOT) applications, FL represents a technology innovation that can create substantial values.

There are several types of FL settings. First, depending on the size and type of clients, FL can be categorized as either cross-device or cross-silo. The term "federated learning" was originally coined under the cross-device setting, where a large number (e.g., millions or billions) of mobile or IOT devices are connected under the coordination of a central service provider. Google's mobile keyboard prediction model (Hard et al. 2018) and Apple's private federated learning in iOS 13 (Bhowmick et al. 2018) are some representative examples. Although the total number of potential clients is very large in a cross-device setting, at any time there are usually only a small fraction of clients available for information exchange, and most clients may only engage in one round of federated computations, due to limitations in connectivity, hardware, and other issues. In contrast, cross-silo FL refers to the setting that involves a relatively small number of reliable participants, such as financial organizations (Webank 2019), healthcare institutions (Kaissis et al. 2020), pharmaceutical companies (Melloddy 2019), or industrial manufacturers (Musketeer 2019). These clients usually have more sophisticated technical capabilities (e.g., stable servers and computational hardware) and are willing to engage in multiple rounds of FL (Kairouz et al. 2019). Second, it is also useful to differentiate horizontal versus vertical FL. In horizontal FL, each client holds different data samples with the same set of features. In vertical FL, clients hold the same set of data samples but nonoverlapping features. In this paper, we focus on the *cross-silo horizontal* setting.

Healthcare represents a fertile ground and burgeoning field for cross-silo FL due to the industry's high demand for data privacy/security and abundant opportunities for ML applications (Aledhari et al. 2020, Kaissis et al. 2020, Rieke et al. 2020, Xu et al. 2020, Yang et al. 2021). FL has been applied in a number of medical research areas, such as brain tumor (Li et al. 2019, Sheller et al. 2020), kidney diseases (Wu et al. 2019), breast cancer (Roth et al. 2020), pancreatic cancer (Wang et al. 2020b), prostate cancer (Sarma et al. 2021), and lung diseases (Han et al. 2020, Kaissis et al. 2021). Beyond medical research, FL is also starting to be deployed in practice. For example, Massachusetts General Hospital, Harvard Medical School, and NVIDIA orchestrated a partnership among 20 institutes across eight countries and used FL to build a model that predicts the future oxygen requirements of COVID-19 patients. The federated model achieves 16% improvement in predictive performance over the local models of participating sites while preserving data privacy, demonstrating the great potential of FL for broader applications in healthcare (Dayan et al. 2021).

The majority of FL literature focuses on designing FL algorithms to deal with different ML tasks, data characteristics, or computational constraints (Kairouz et al. 2019). Take the FedAvg algorithm (McMahan et al. 2017), one of the most popular FL algorithms that is applicable to various other ML tasks, as an example. Each client uses its private data to compute the gradients associated with a local ML model. The central server then aggregates the gradients of local models via weighted averaging (weights determined by the relative size of each client's data) and use the federated

gradients to update the global model. An illustration of this process is included in Online Appendix B. In practice, to make sure that it is actually meaningful to aggregate the gradients of local models (e.g., via weighted averaging), all clients typically reach an agreement in terms of the type of the ML model (e.g., a convolutional neural network) and hyperparameters (e.g., batch size and learning rate) to se, before the FL process begins. They often also share nonprivate and aggregate information about their data (such as data size and types of features) with each other. This is necessary for participants to gauge the benefits to participate before getting on board.

Beyond the computational/algorithmic research of FL, an emerging set of research has begun to study the economics of FL by proposing incentive mechanisms that can achieve different objectives, such as fair division of rewards (Yu et al. 2020), maximization of social welfare (Tang and Wong 2021), envy-freeness in information exchange (Blum et al. 2021), or minimization of free-riders who do not engage in training local models (Zhang et al. 2022). Our work builds on this stream of incentive-aware FL literature by studying the conditions for partnership formation and repeated contributions in long-term FL.

Our work is motivated by both the gaps in FL research literature and the practical difficulties to orchestrate long-term FL. In particular, most of the existing literature *assumes* successful FL (i.e., that the FL partnership has already formed, and all participants have contributed their data to the central server), then focus on analyzing certain FL outcome of interest, such as fair division of rewards (Yu et al. 2020) or maximization of social welfare (Tang and Wong 2021). In contrast, our work seeks to understand what affects partnership formation and repeated contributions in the first place. Additionally, some studies (Blum et al. 2021; Donahue and Kleinberg 2021a, b) examine the incentive problem in participants' contribution decisions, but they do so under the one-round FL setting, where data contributions and model training last only for a single round. The one-round FL setting may have limited practical relevance in the domains that we consider (such as healthcare and finance) with frequent arrival of new information and opportunities to continuously improve the FL model over multiple rounds of training. Notably, Zhang et al. (2022) study the contribution condition under a long-term FL setting. Compared with Zhang et al. (2022), our work offers a more comprehensive analysis of long-term FL by (i) accounting for both the utility and cost of participation and (ii) considering a richer set of contractual mechanisms to deter defection. Finally, based on our interviews with several FL researchers and practitioners in the field (Online Appendix A), recruiting participants to form the FL partnership and enforcing repeated contributions over time are two of the most frequently mentioned obstacles to successful long-term FL.

2.2. Iterated Prisoner's Dilemma

Our analyses rely on the prisoner's dilemma framework, which is one of the classic game theory tools that seeks to model cooperative behaviors (and lack thereof) among rational agents (Axelrod and Hamilton 1981). In a standard one-shot prisoner's dilemma of two identical players, defection (i.e., noncooperation) turns out to be the dominant strategy for both players. As a result, both players defect in the equilibrium, even though cooperation would be beneficial to them overall.

IPD extends the one-shot prisoner's dilemma model to a repeated setting, where players engage in multiple rounds of decisions. If the total number of rounds is finite and known to all players a priori, then a straightforward backward induction would indicate that defection is still the dominant strategy (i.e., each round is essentially a separate prisoner's dilemma). However, if the total number of rounds is infinite or unknown to players, then cooperative equilibrium may arise when players adopt certain trigger strategy, such as grim trigger or tit-for-tat (Axelrod and Hamilton 1981, Aumann 2006). Next, we lay out some basic results in a canonical IPD game, which serve as the foundation for our solutions discussed later.

As a standard setup, consider an IPD with two identical players, A and B, with the payoff matrix specified in Table 1 at each round of the game. Consider a nonstochastic game with complete information (i.e., the payoff matrix at each round is fixed and known to both players), the different payoff elements satisfy $T > R > P > S$; that is, defection while the other player cooperates gives the highest payoff, followed by the payoff of mutual cooperation, mutual defection, and being defected. The literature on IPD often also assumes $2R > T + S$, such that mutual cooperation generates a higher payoff than alternating between cooperation and defection (Akin 2016). Finally, a player's preference between short-term rewards and long-term rewards is characterized by a discount rate $\gamma \in (0, 1)$—A smaller (larger) discount rate indicates a more myopic (forward-looking) player.

The consequence of defection in an IPD depends on the choice of trigger strategy, that is, a strategy that determines what a player would do if the other party defects. Players in a FL partnership can pick a mutually agreed trigger strategy at the beginning of the FL process to deter potential defection. Here, we consider two

Table 1. Payoff Matrix in Each Round

A/B	Cooperate (C)	Defect (D)
Cooperate (C)	(R, R)	(S, T)
Defect (D)	(T, S)	(P, P)

commonly studied trigger strategies, namely the "grim trigger" and "tit-for-tat." Under the grim trigger strategy, each player would cooperate unless the other player defects, in which case the focal player will retaliate by defecting for the rest of the game (Axelrod and Hamilton 1981). Under the tit-for-tat strategy, a player would cooperate at first and then copy what the other player does in the preceding round (e.g., if the other player defects at round t, the focal player will retaliate and defects at round $t + 1$). Under both trigger strategies, one can show that mutual cooperation requires that both players are not too myopic (see Online Appendix C for details).

Beyond the previous canonical examples, a large body of research has been developed that extends IPD to account for other factors (Kendall et al. 2007, Jurišić et al. 2012, Akin 2016). For example, Tomochi and Kono (2002) examined an IPD game (in a spatial setting) where the payoff matrix dynamically evolved based on the proportion of defectors in the previous round. Rezaei and Kirley (2009) studied the effects of having time-varying payoffs on the equilibrium cooperation level of a population with many individuals. Chong and Yao (2006) endogenized the dynamic payoff matrices as part of the design of IPD rules and investigated the corresponding strategic behaviors and utility outcomes of players. Our work builds on this line of research and integrates insights from federated machine learning into the configuration of dynamic payoff matrices (e.g., how the benefits and costs of FL change with respect to the amount of information shared). Furthermore, Arend and Seale (2005) studies alliance formation in an IPD framework with an "exit option," where each participant can choose to drop out at any time during the alliance. Compared with Arend and Seale (2005), our work focuses more on deriving how partnership formation depends on the characteristics of participants (such as their temporal preferences), and we consider a richer set of noncooperative behaviors and possible contractual mechanisms.

3. Basic Model Setup

In this section, we introduce the notations and set up the basic game theoretic model to characterize a long-term FL process. In the basic model, we consider two identical players (e.g., two data owners): A and B. The cases of nonidentical players and multiple players are considered in Section 5. In a long-term FL partnership, the FL process lasts for multiple *rounds*, and each round represents a time period (e.g., a month or a quarter, agreed upon by both players) during which new information would arrive for players to train and update the FL model (Zhang et al. 2022).[3] Both players decide whether to contribute during each round, and we model their decisions as an IPD game. The FL process is orchestrated by a central server. Importantly, the central server is *not* a strategic actor: It is typically an algorithmic system operating independently of the two (strategic) players to perform FL-related computations and exchange model-specific information with the players.[4] As such, any mechanisms to promote contribution and deter defection can be hard-coded into the central server and enforced automatically.

3.1. Dynamics in One Round of FL

In each round of the FL process, both players collect an x amount of new information (e.g., new data gathered during the current time period), and we assume that $x > 0$ to rule out the edge case where a lack of contribution is due to having no new information to contribute. Note that x should be conceptualized as a measure of information, which can be proportional to the size of new data (e.g., number of data instances).[5]

Meanwhile, each player makes an independent choice between two decisions: (1) to *cooperate* or (2) to *defect*. Specifically, cooperation means that the focal player will share the new information with the FL central server. Under the FL regime, cooperating players do not share the actual raw data they have collected but rather certain forms of model-specific information computed using the raw data, such as gradients, parameters, or intermediate results. Nonetheless, FL algorithms can leverage such information to effectively improve ML models, *as if* the raw data has been directly shared (Sheller et al. 2020). Because of this unique property of FL, we operationalize the amount of information that is shared to also be x, that is, the same as the amount of information privately collected by a player. Meanwhile, in this basic model, defection means that the focal player holds on to the new information and does not share it with the central server (similar to what has been considered in Zhang et al. 2022). Beyond this stylized defection setting, we also study two other types of defection (i.e., contributing partial information or adversarial information) in Section 4.4.

To understand the consequence of cooperation vs. defection for a player, it is important to differentiate the *global* model from the *local* models in FL. In a typical FL partnership, the central server maintains a global model by aggregating the information shared by cooperative players, and updates that model over time (when new information is shared). In the meantime, each player, regardless of its contribution decision, also maintains a local model trained using the information it self-collects and receives from the server. Under mutual cooperation, the global model is identical to the local models. For instance, if both players choose to share x information with the server, then their respective local models as well as the global model can all benefit from a total of $2x$ information. However, if one player chooses to defect while the other cooperates, then the global model and the cooperator's local model will only have access to x information

(shared by the cooperator), whereas the defector's local model will have access to $2x$ information (x self-collected and x received from the central server). In other words, the defector can "free-ride" the cooperator by tapping into the information shared via the global model.[6] Finally, if both players defect in a round, then their respective local models can only benefit from self-collected x information, whereas the global model will not be updated.

3.2. Utility and Cost of Contribution

To quantify how information benefits a player p, we define the utility function $U(X_t^p)$ to represent the utility of a player who possess X_t^p amount of information up to round t, including the information collected by the player itself as well as the information shared by the other player (received via central server). We set $X_0^p = 0$ for completeness. This utility is associated with the performance of player p's *local model* that has been trained on X_t^p amount of information. Importantly, we assume that $U(.)$ is a *strictly increasing and concave* function, that is, $U'(.) > 0$ and $U''(.) < 0$. This is a realistic assumption, because (1) ML models usually achieve better predictive performance with more training data, but (2) the performance improvement typically slows down or saturates as more data becomes available. For technical convenience, we also assume that $U''(.)$ is continuous, that is, the utility gain is "smooth" with respect to information acquisition, and that $U(0) = 0$ to represent zero utility with no information. In later sections, we consider several different functional forms of $U(.)$ as part of numerical analyses, such as an exponential form $U(X_t^p) = 1 - e^{-X_t^p}$.

At the same time, there are costs associated with contributing one's information, such as operational overhead to transmit information to the central server and the potential risks of data leakage.[7] Although the sensitive raw data are not directly shared under FL, they are still not perfectly secure. For example, research has shown that even a small amount of model-specific information publicly shared in FL, such as gradients, can breach private information about a participant's local data (Geiping et al. 2020, Zhu and Han 2020). We model the cost associated with contributing x information as a linear function $C(x) = \alpha x$, where $\alpha > 0$ is a weight parameter that reflects the "sensitivity" of a player to the cost of contribution. Unlike the concave utility function, we model cost as a linear function of x because the privacy risk grows proportionally with respect to the amount of information shared.[8]

In Table 2, we can now write down the payoff matrix of the two players, $\{A, B\}$, in round t.

Table 2. Payoff Matrix in Round t

A/B	Cooperate (C)	Defect (D)
Cooperate (C)	$R(x \mid X_{t-1}^A), R(x \mid X_{t-1}^B)$	$S(x \mid X_{t-1}^A), T(x \mid X_{t-1}^B)$
Defect (D)	$T(x \mid X_{t-1}^A), S(x \mid X_{t-1}^B)$	$P(x \mid X_{t-1}^A), P(x \mid X_{t-1}^B)$

Each element in the payoff matrix is defined as

$$R(x \mid X_{t-1}^p) = U(X_{t-1}^p + 2x) - U(X_{t-1}^p) - C(x),$$
$$T(x \mid X_{t-1}^p) = U(X_{t-1}^p + 2x) - U(X_{t-1}^p),$$
$$S(x \mid X_{t-1}^p) = U(X_{t-1}^p + x) - U(X_{t-1}^p) - C(x),$$
$$P(x \mid X_{t-1}^p) = U(X_{t-1}^p + x) - U(X_{t-1}^p).$$

Take $R(x \mid X_{t-1}^p)$ as an example. It corresponds to the payoff for player p in round t if both players decide to cooperate and, as a result, each player would end up getting $2x$ information on top of its information stock, X_{t-1}^p, accumulated over previous rounds. Therefore, the player's payoff in round t is calculated as the marginal utility gain, $U(X_{t-1}^p + 2x) - U(X_{t-1}^p)$, less the cost of contributing x amount of information. The other three elements can be understood analogously. At first sight, the payoff matrix resembles that in a special case of IPD known as the "donation game" (Hilbe et al. 2013).[9] However, it is important to keep in mind that the payoff matrix in our model is time-varying and strategy dependent—The values of its elements change over time and depend on players' decisions over previous rounds.

Finally, we denote a discount rate as $\gamma \in (0, 1)$. A player's payoff obtained in round t is discounted by γ^{t-1} to the beginning of the game (i.e., $t = 1$). The magnitude of the discount rate reflects the importance of future payoffs. For example, a small γ implies that future payoffs are less important compared with present payoffs. The discount rate characterizes how forward-looking (versus myopic) a player behaves, with larger/smaller γ indicating more forward-looking/myopic preference.

3.3. Trigger Strategies and Central Server Sanction

From a design perspective, several potential mechanisms may be used (e.g., as part of a contractual agreement) to encourage mutual cooperation in FL. For instance, as demonstrated in Section 2.2, players can implement trigger strategies, such as the grim trigger or tit-for-tat.[10]

However, deploying trigger strategies is not the only way to induce cooperation in FL. Unlike the standard IPD setting, a unique characteristic of FL is the presence of the independent (and nonstrategic) central server that maintains the global model. Recall that the major incentive for a player to defect is to obtain the other player's information "for free" *via the global model*. Therefore, after detecting the defection behavior (e.g., fail to receive the updated gradients from the defector), the central server can sanction the defector by temporarily removing its access to the global model. The defector may regain access to the global model when it starts to cooperate at a later round. This sanctioning mechanism is intuitive and appealing, as it directly cuts off the benefits of defection until the defector starts to cooperate and, unlike trigger

strategies, does not require any extra effort from the players to impose. In other words, it can be adopted and hard-coded into the central server algorithm as a rule, for example, IF defection detected on round t, THEN server withholds global model to defecting party on round t. Finally, the server-imposed sanction may be used in conjunction with trigger strategies. The relative efficacy of different mechanisms (specifically trigger strategy, sanction, and trigger strategy + sanction) in deterring defection remains unclear a priori and is one of the focuses of our theoretical analyses.

4. Theoretical Results

In this section, we solve the IPD model to answer two research questions of interest. First, we identify conditions under which players would prefer to form a long-term FL partnership rather than building ML models by themselves. Second, suppose players prefer long-term FL over building models themselves, we seek to evaluate the effectiveness of different contractual mechanisms in deterring defection and encouraging repeated cooperation in the FL partnership. We adopt the standard Nash equilibrium concept and specifically look for cooperative equilibria (i.e., successful partnership formation and repeated contributions). We start by reporting the results of the basic model, where defection represents a lack of contribution (Sections 4.1 and 4.2). We then discuss the results when defection takes other forms, namely contributing partial information or adversarial contribution (Section 4.4).

4.1. Conditions for Long-Term FL Partnership Formation

As mentioned before, a unique characteristic of FL partnership is that players have the "outside option" of not participating at all. For players to form a long-term FL partnership rather than building ML models by themselves, the payoff of the former has to outweigh that of the latter, creating a net benefit for players. This ensures that FL participation satisfies individual rationality (IR). The promise of a long-term FL partnership is that players can benefit from each other's private information and jointly build a better (global) ML model through repeated contributions, although each player bears the cost of contribution.[11] Formally, player $p \in \{A, B\}$ would have access to information $X_t^p = 2tx$ by the end of round t, and the discounted total payoff is

$$\begin{aligned}\pi^C(p) &= \sum_{t=1}^{+\infty} \gamma^{t-1} R(x \mid X_{t-1}^p) \\ &= \sum_{t=1}^{+\infty} \gamma^{t-1} (U(2tx) - U(2tx - 2x) - C(x)) \\ &= -\frac{C(x)}{1-\gamma} + (1-\gamma) \sum_{t=1}^{+\infty} \gamma^{t-1} U(2tx). \end{aligned} \tag{1}$$

Meanwhile, not participating in FL avoids the cost of contribution completely but also means that a player can only leverage their own data to build the (local) ML model, which may limit its performance. Therefore, player $p \in \{A, B\}$ has access to information $X_t^p = tx$ by the end of round t, and the discounted total payoff is

$$\begin{aligned}\pi^{NP}(p) &= \sum_{t=1}^{+\infty} \gamma^{t-1} P(x \mid X_{t-1}^p) \\ &= \sum_{t=1}^{+\infty} \gamma^{t-1} (U(tx) - U(tx - x)) \\ &= (1-\gamma) \sum_{t=1}^{+\infty} \gamma^{t-1} U(tx). \end{aligned} \tag{2}$$

The condition for long-term FL partnership formation is then given by requiring $\pi^C(p) > \pi^{NP}(p)$. We summarize the result in the following Theorem 1.

Theorem 1. *Two players prefer to form a long-term FL partnership rather than building ML models by themselves if and only if*

$$C(x) < (1-\gamma)^2 \sum_{t=1}^{+\infty} \gamma^{t-1} \{U(2tx) - U(tx)\}. \tag{3}$$

The proofs of all theoretical results are included in Online Appendix D. Although closed-form solutions for the values of γ that lead to FL partnership formation cannot be obtained (due to the infinite sum that cannot be simplified), we derive the following corollaries to make sense of this result.

Corollary 1. *Let* $\alpha^+ = \sup_{x>0} \frac{U(2x)-U(x)}{x}$. *The following statements are true*:

(i) *If* $\alpha \geq \alpha^+$, *then players would not form a long-term FL partnership.*

(ii) *If* $0 < \alpha < \alpha^+$, *then there exists a finite* $x^+ > 0$, *such that when* $x \geq x^+$, *players would not form a long-term FL partnership.*

Intuitively, this corollary shows that players have no incentive to participate in FL if (1) they are too cost sensitive, or (2) the amount of information they can gather within each round by themselves is sufficiently large, to the point where the marginal payoff gain of being a part of the FL is smaller than the cost associated with contribution. In other words, FL partnerships are more likely to form in domains where the cost of contribution is not prohibitive, and each player has limited information acquisition capability to achieve satisfactory model performance by itself. These results align well with our observation that most healthcare FL initiatives are currently in the medical imaging domain (as discussed in Section 2.1), where the cost of contribution can be managed by privatization techniques (e.g., differentially

private FL; Geyer et al. 2017) and each participant only possesses a relatively small number of images.

The $\alpha \geq \alpha^+$ condition in part (i) of Corollary 1 can also be expressed as $\forall x, C(x) \geq U(2x) - U(x)$. This equivalent expression provides an alternative interpretation of the result; that is, players would not form a long-term FL partnership if the marginal benefit of doing so (over building models by themselves) does not even overcome the contribution cost *in the first round*. Because of the concave nature of $U(.)$, the contribution cost would overwhelm the benefit from FL to a greater degree in subsequent rounds.

Next, we show that when cost sensitivity and information acquisition are not large enough to prohibit partnership formation (i.e., when $0 < \alpha < \alpha^+$ and $0 < x < x^+$), there turns out to be an *upper bound* on the values of γ that can lead to FL partnership formation.

To show the existence of an upper bound, we approximate the infinite sums in Theorem 1 by a (large) finite number of terms until the marginal increase in the summation falls below a fixed threshold (i.e., a chosen precision level). Such an approximation is warranted in practice. Although long-term FL can last for an infinite number of rounds in theory, it has to end at some point in reality, for example, when the marginal utility for additional rounds becomes ignorable. In addition, computational precision for numerical calculations are usually finite, and it is common to drop the tail terms in an (convergent) infinite series. Formally, we can see from the proof of Corollary 1 part (i) that the infinite sum in the right-hand side of Inequality (3) is convergent and upper bounded by $U(2x) - U(x)$ for any given $\gamma \in (0,1)$ and finite x, which implies diminishing tail terms. Therefore, it is reasonable to approximate this infinite sum of discounted payoff with a finite number of terms $g(T) = (1-\gamma)^2 \sum_{t=1}^{T} \gamma^{t-1}\{U(2tx) - U(tx)\}$. Specifically, suppose $\varepsilon > 0$ is a desirable precision level, we can select T as the smallest integer such that for any $t > T$, we have $g(t) - g(T) < \varepsilon$.[12]

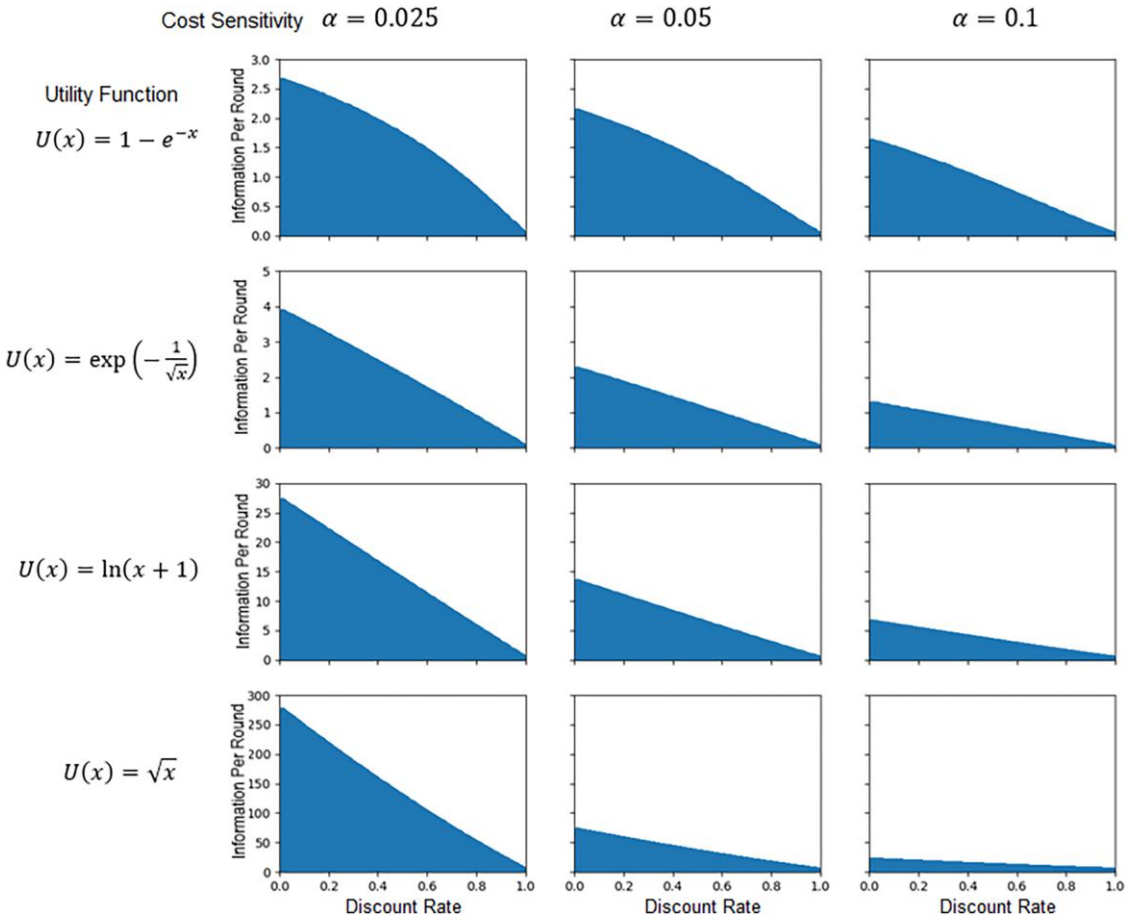
Corollary 2. *Given a precision level $\varepsilon > 0$, there exists $\gamma_u < 1$ such that players would not participate in long-term FL when $\gamma \geq \gamma_u$.*

Although this corollary shows the existence of an upper bound, a closed-form expression for the upper bound is generally unavailable. In Online Appendix E, we provide some examples of how specific upper bounds may be obtained if one is willing to make additional assumptions. We further note that, supposing $\gamma < \gamma_u$, there generally is *not* a lower bound on γ. To see this, consider the extreme case of $\gamma = 0$, which reduces Inequality (3) to $C(x) < U(2x) - U(x)$. As we discussed before, this condition is equivalent to $\alpha \in (0, \alpha^+)$. In other words, having highly myopic players do not necessarily prohibit FL partnership formation, as long as the immediate benefit (i.e., $U(2x) - U(x)$) is sufficiently attractive.[13]

The existence of a meaningful upper bound (i.e., an upper bound less than one) on the values of γ that lead to partnership formation in long-term FL may appear counter-intuitive at first, because higher γ indicates more forward-looking players who, presumably, should value the additional payoffs having access to more information in the FL. An intuitive explanation of this finding is that, if players are highly forward-looking, they can also become more "self-reliant." The extra benefits of engaging in FL over building ML models by themselves (i.e., the additional marginal utility of getting $2x$ information over getting x information per round) shrinks over time due to the concave nature of the utility function. However, the cost of contributing to the FL stays the same each round due to its linear form. Taken together, as the discount rate increases, the outside option of building ML models by themselves becomes more attractive. This finding stands in contrast to conventional wisdom in IPD where the cooperative outcome typically requires players to be not too myopic and represents a unique dynamic of FL partnership formation.

Because the partnership formation condition does not have a closed-form solution, we take a numerical approach to obtain approximate solutions under several specifications of $U(x)$ and values of α. Specifically, we consider four functional forms of $U(x)$: (1) exponential $U(x) = 1 - e^{-x}$; (2) exponential square root $U(x) = e^{-\frac{1}{\sqrt{x}}}$; (3) logarithm $U(x) = \ln(x+1)$; and (4) square root $U(x) = \sqrt{x}$. They are chosen to cover different kinds of concave functions that characterize the value generation processes of ML applications. While all four functions are strictly concave, the first two are bounded and the last two are unbounded. A bounded utility function is appropriate in ML applications that generate a fixed value beyond certain performance level, whereas an unbounded utility function may be used to model ML applications that keep generating new values with additional data.[14] Within both the bounded and unbounded categories, we consider two utility functions that grow at different speeds ($1 - e^{-x}$ grows faster than $e^{-\frac{1}{\sqrt{x}}}$ and $\sqrt{x}$ grows faster than $\ln(x+1)$) to capture different rates of value creation. Furthermore, the exponential and logarithm forms are, respectively, constant absolute risk aversion (CARA) and hyperbolic absolute risk aversion (HARA), which are commonly used to model risk aversion. In terms of the cost function, we consider three different values for the cost sensitivity: $\alpha \in \{0.025, 0.05, 0.1\}$, to represent increasing sensitivity to contribution. Finally, to numerically approximate each infinite sum in the theoretical results, we pick a precision level $\varepsilon = 0.001$ and compute a finite number of terms until the marginal increase in the summation falls below this level. Using smaller ε values increases computation time but does not qualitatively change our findings. The following Figure 1 visualizes

Figure 1. (Color online) Region of Partnership Formation in Long-Term FL



the region of γ that leads to long-term FL partnership formation under different values of x.

We make several observations based on the numerical results. First, across all functional forms of $U(.)$ and values of α, the values of γ that lead to partnership formation have an upper bound for a given x that is not too large. When x grows beyond a certain point, there is no feasible γ for partnership formation. Expectedly, the region of partnership formation (i.e., the shaded area) shrinks as α increases, as both players become more sensitive to the cost of contributions. These patterns confirm our theoretical results.

Second, the upper bound on γ decreases as x becomes larger. Since the closed-form expression of the upper bound is unavailable, this empirical observation adds to our understanding of the boundary conditions for partnership formation. As players gather more information per round, their incentives to participate in long-term FL decline accordingly.

Third, the region of partnership formation varies in *size* for different forms of $U(.)$. For a fixed level of α, the region is largest under the square root specification, followed by logarithm, exponential, and exponential square root. In other words, the region of partnership formation tends to be larger if the underlying utility function *saturates slower* with a unit increase in x. Conceptually, the utility gain from a unit increase of information measures how much ML model performance improvement can be expected if more information is available. It is analogous to the concept of a "learning curve" and can be a property of the underlying ML task. Compared with a relatively easier task, the performance of a more challenging task typically saturates much slower with the increase in data size. Therefore, this result suggests that FL partnership formation is more likely when the underlying ML task is more challenging, such that players benefit more from having access to additional information via the FL partnership. This is also consistent with the observations that FL has mostly been applied in challenging predictive tasks, such as brain tumor and cancer detection (Roth et al. 2020, Sheller et al. 2020, Wang et al. 2020b, Sarma et al. 2021).

In summary, long-term FL partnership formation depends on the interplay among (1) players' cost sensitivity, (2) the amount of information they gather in each round, and (3) their discount rates. Partnerships are

harder to form when players are too cost sensitive or gather too much information by themselves. Furthermore, the overall size of the partnership formation region appears to be associated with the characteristics of the underlying ML tasks—The region tends to be larger for more "data hungry" tasks, where the utility saturates slower with additional information.

4.2. Roles of Contractual Mechanisms

Suppose the two players prefer to participate in long-term FL over building ML models by themselves (i.e., Inequality (3) in Theorem 1 holds), we next evaluate the effectiveness of different contractual mechanisms, including trigger strategies, central server sanction, and the combination of the two, to mitigate defection and promote repeated contributions throughout the FL. Specifically, we derive conditions under which a player's utility of defection is dominated by the utility of repeated contributions (thereby ensuring that repeated contribution is regret-free).

4.2.1. Trigger Strategy Only. When players adopt a trigger strategy, defection behavior of one player will receive retaliation from the other player. Depending on the specific trigger strategy used, retaliation also takes different forms. In Table 3, we first present how grim trigger and tit-for-tat strategies affect the information that the defector can access (which subsequently determines the utility associated with defection). Without loss of generality, we assume player B is the initial defector.

We then derive the boundary conditions for repeated cooperation when players only rely on trigger strategy under the grim trigger and the tit-for-tat strategy, which are presented in Theorem 2.

Theorem 2. *Under grim trigger strategy, two players will cooperate repeatedly if and only if*

$$C(x) < (1-\gamma)^2 \sum_{t=2}^{+\infty} \gamma^{t-1}\{U(2tx) - U((t+1)x)\}. \tag{4}$$

Under tit-for-tat strategy, two players will cooperate repeatedly if and only if

$$C(x) < (1-\gamma) \sum_{t=2}^{+\infty} \gamma^{t-1}\{U(2tx) - U((2t-1)x)\}. \tag{5}$$

Following similar theoretical arguments in our proof of Corollary 2, we can show that the cooperation-inducing values of γ under both trigger strategies have an upper bound. However, we also find a lower bound on γ, below which players will have incentive to defect.

Corollary 3. *Under both trigger strategies, there exists* $\gamma_l = \frac{C(x)}{U(4x)-U(3x)}$ *such that two players will not cooperate repeatedly in long-term FL when* $\gamma \le \gamma_l$.

Corollary 3 suggests that when the payoff discounts too fast, the discounted sum of future payoff from repeated cooperation is not large enough to cover the cost of contribution, making repeated cooperation unattractive relative to defection despite the trigger strategies. The existence of both a lower bound and an upper bound implies that, under both trigger strategies, repeated cooperation in FL requires that the players' temporal preferences fall into a "Goldilocks zone"—being either too myopic or too forward-looking can lead to defection.

Moreover, let $(\gamma_l^{(GT)}, \gamma_u^{(GT)})$ and $(\gamma_l^{(TfT)}, \gamma_u^{(TfT)})$ denote the cooperation-induced ranges of γ under the two trigger strategies, respectively, then one can readily derive the conditions under which players are on board with FL and would refrain from defection. As an example, $\gamma \in (0, \gamma_u) \cap (\gamma_l^{(GT)}, \gamma_u^{(GT)})$ is a necessary condition for players to form a long-term FL partnership and engage in repeated contributions under the grim trigger strategy. We can further show that $(\gamma_l^{(GT)}, \gamma_u^{(GT)}) \subset (0, \gamma_u)$ by observing that any γ that satisfies Inequality (4) would also satisfy Inequality (3) in Theorem 1 (but not vice versa). It implies that simply implementing a grim trigger strategy *cannot* fully prevent defection. For instance, highly myopic players (e.g., those with $\gamma \in (0, \gamma_l^{(GT)})$) would be motivated to defect despite the grim trigger. This theoretical result is not available under the tit-for-tat strategy, although our numerical analyses later (Section 4.2.4) show that there exists $\gamma \in (0, \gamma_u)$ but $\gamma \notin (\gamma_l^{(TfT)}, \gamma_u^{(TfT)})$, indicating that tit-for-tat strategy alone cannot fully prevent defection either.

4.2.2. Sanction Only. Instead of trigger strategies, now suppose the central server imposes a sanction on the defecting player by removing access to the global model until the defector starts to cooperate. To derive the cooperation conditions under this sanction mechanism, we first summarize the information accessible to the defector across all rounds in Table 4. For player B, defecting on the first round means that it cannot access the global

Table 3. Information Accessible to Defector Under Trigger Strategy

	Grim trigger						Tit-for-tat					
A	C	D	D	…	D	…	A	C	D	C	…	C	…
B	D	D	D	…	D	…	B	D	C	C	…	C	…
X_t^B	$2x$	$3x$	$4x$	…	$(t+1)x$	…	X_t^B	$2x$	$3x$	$5x$	…	$(2t-1)x$	…

Note. C, cooperation; D, defection.

Table 4. Information Accessible to Defector Under Sanction

	Sanction Only:					
A	C	C	C	…	C	…
B	D	C	C	…	C	…
X_t^B	x	$4x$	$6x$	…	$2tx$	…

Note. C, cooperation; D, defection.

model (which contains information contributed by player A) and can only rely on the x information collected by itself. However, as player B starts to cooperate in round 2, the sanction will be lifted and the player will have access to the global model that contains $3x$ information (specifically, $2x$ contributed by player A in the first 2 rounds and x contributed by B in round 2). This adds up to $4x$ information in total. Accordingly, the boundary condition for repeated cooperation under sanction is presented in Theorem 3.

Theorem 3. *Under central server sanction, two players will cooperate repeatedly if and only if*

$$\gamma < 1 - \frac{C(x)}{U(2x) - U(x)}. \tag{6}$$

Denote $\gamma_u^{(S)} = 1 - \frac{C(x)}{U(2x)-U(x)}$, the cooperation-inducing range of γ can be represented as $(0, \gamma_u^{(S)})$. It follows that under the sanction mechanism, players will form a long-term FL partnership and engage in repeated contributions if $\gamma \in (0, \gamma_u) \cap (0, \gamma_u^{(S)}) = (0, \min\{\gamma_u, \gamma_u^{(S)}\})$. The sanction mechanism is not guaranteed to fully prevent defection, despite its intuitive appeal to cut off access to the global model during the defecting round. This is because, as can be seen in Table 4, the defector will be able to receive the global model (and all the cumulative information it contains) as soon as it starts cooperating. In other words, the sanction can only *delay* the benefits of defection but not entirely erase it.[15] Numerical analyses later (Section 4.2.4) confirm this claim and identify the specific cases where a sanction-only strategy falls short.

4.2.3. Sanction and Trigger Strategy. Finally, we consider the combination of sanction imposed by the central server and the trigger strategies adopted by players. Again, we summarize the information accessible to the defector across all rounds in Table 5.

The information accessible to the defecting player under both sanction and grim trigger is *identical* to the case when the player chooses not to participate in the FL at all. With the sanction cutting off the benefit of defection in round 1, and grim trigger effectively terminating cooperation for all other rounds, it is as if the player never participated in the FL. As a result, the condition for cooperation under both sanction and grim trigger is the same as that shown in Theorem 1, that is, $(\gamma_l^{(S+GT)}, \gamma_u^{(S+GT)}) \equiv (0, \gamma_u)$. Put differently, in an FL partnership with both sanction and grim trigger implemented, players have no incentive to defect as long as they prefer to form an FL partnership over building models by themselves.

Although the combination of sanction and grim trigger fully prevents defection in FL, it is important to keep in mind that grim trigger is an extremely unforgiving strategy—The FL partnership essentially dissolves after even one defection. As such, it may not always be feasible or desirable in practice. Therefore, we also derive the cooperation condition under sanction and tit-for-tat, as presented in Theorem 4.

Theorem 4. *Under both central server sanction and the tit-for-tat strategy, two players will cooperate repeatedly if and only if*

$$C(x) < (1-\gamma)\sum_{t=1}^{+\infty} \gamma^{t-1}\{U(2tx) - U((2t-1)x)\}. \tag{7}$$

.Denoting the cooperation-inducing range of γ under sanction and tit-for-tat as $(\gamma_l^{(S+TfT)}, \gamma_u^{(S+TfT)})$, it is not immediately clear how this cooperation range compares to $(0, \gamma_u)$, and we rely on numerical analysis in Section 4.2.4 to understand their relationship. However, we can derive the following corollary that compares the effectiveness of trigger strategy with and without being combined with sanction in mitigating defection.

Corollary 4. *The following statements are true:* $(\gamma_l^{(GT)}, \gamma_u^{(GT)}) \subset (\gamma_l^{(S+GT)}, \gamma_u^{(S+GT)})$ *and* $(\gamma_l^{(TfT)}, \gamma_u^{(TfT)}) \subset (\gamma_l^{(S+TfT)}, \gamma_u^{(S+TfT)})$.

That is to say, a combination of sanction and trigger strategy is strictly more effective at deterring defection in FL than only using the trigger strategy. This finding demonstrates that central server sanction, as a contractual mechanism unique in the context of FL, represents

Table 5. Information Accessible to Defector Under Sanction and Trigger Strategy

	Grim trigger + sanction							Tit-for-tat + sanction					
A	C	D	D	…	D	…	A	C	D	C	…	C	…
B	D	D	D	…	D	…	B	D	C	C	…	C	…
X_t^B	x	$2x$	$3x$	…	tx	…	X_t^B	x	$3x$	$5x$	…	$(2t-1)x$	…

Note. C, cooperation; D, defection.

an advantageous tool to promote repeated cooperation when used together with trigger strategies.

4.2.4. Numerical Results. We again rely on a numerical approach to compare the relative effectiveness of different contractual mechanisms in promoting repeated cooperation. We focus on two forms of $U(.)$, namely the (bounded) exponential function and the (unbounded) logarithm function, and fix the value of α to be 0.05. In Figure 2, we plot the cooperation-inducing values of γ against the values of x, when different contractual mechanisms are applied. We also include a "participation boundary" in each plot, which marks the upper bound of γ (i.e., γ_u) for each value of x that still leads to FL partnership formation.[16]

Two findings are worth noting. First, under a sanction-only mechanism (i.e., the first plot in each row), we can see that the interior of the participation boundary is largely covered by the cooperation region, except in the bottom-right corner. This implies (1) that a sanction-only mechanism is quite effective—for most combinations of x and γ, players who are willing to participate in FL would also engage in repeated cooperation, but (2) it is unable to prevent defection when x is small and γ is large (i.e., when a player collects a small amount of information per round and is highly forward-looking). Second, adding sanction on top of trigger strategies significantly enlarges the cooperation region, confirming our theoretical result in Corollary 4. Moreover, for both grim trigger and tit-for-tat strategy, combining with sanction *fully* covers the interior of the participation boundary. This observation is particularly important for understanding the effectiveness of the tit-for-tat + sanction strategy in preventing defection because the theoretical result is unavailable.

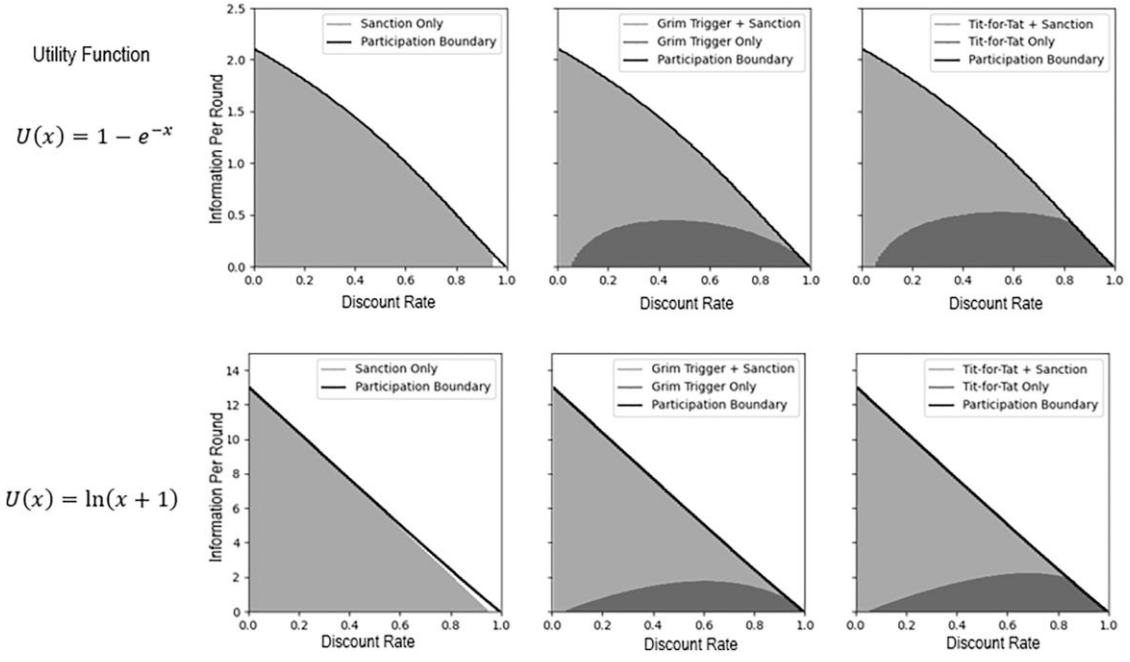
To summarize, our theoretical and numerical analyses have offered three key takeaways regarding the effectiveness of different contractual mechanisms: (1) a server-imposed sanction can prevent defection in most cases, except when information acquisition is small and players are highly forward-looking; (2) player-initiated trigger strategies alone are unable to fully prevent defection; and (3) implementing trigger strategy together with sanction can fully prevent defection. Taken together, a combination of tit-for-tat and server sanction emerges as an advantageous mechanism, as it is both more *effective* (than tit-for-tat or sanction alone) and more *forgiving* (than grim trigger).

4.3. Other Forms of Cost Functions

In practice, the costs of participation and contribution in long-term FL may take more complex forms than the linear form we have considered in the basic model. In this section, we examine two variations of the cost function to understand the robustness of our findings.

4.3.1. One-Time Fixed Cost of Partnership Formation. First, suppose a one-time fixed cost $c_0 \geq 0$ is incurred to form any FL partnership. Such a fixed cost may stem from computational hardware/software purchases and setup and initial communications among interested participants (e.g., to reach an agreement on the FL model specification and cooperation mechanisms). Because the

Figure 2. Region of Cooperation Under Different Contractual Mechanisms



incorporation of this fixed cost affects participants' decision to form an FL partnership, we revisit the partnership formation condition (i.e., Theorem 1) and derive the following results.

Theorem 5. *In the presence of a one-time fixed cost $c_0 \geq 0$, two players prefer to form a long-term FL partnership rather than building ML models by themselves if and only if*

$$(1-\gamma)c_0 + C(x) < (1-\gamma)^2 \sum_{t=1}^{+\infty} \gamma^{t-1}\{U(2tx) - U(tx)\}. \quad (8)$$

Intuitively, compared with the result in Theorem 1, we can see that the partnership formation region will shrink in the presence of the fixed cost, since the cost to overcome (i.e., left-hand side of the inequality) has increased. Moreover, the fixed cost has a greater impact on the partnership formation region for myopic players (smaller γ) than for forward-looking players (larger γ). Results in Corollaries 1 and 2 would still hold, namely the existence of upper bounds on cost sensitivity, information acquisition, and discount rate beyond which FL partnership formation would not take place. Their mathematical proofs are included in Online Appendix D. Furthermore, suppose the above partnership formation condition is satisfied, then all results in Section 4.2 would remain unchanged because the fixed cost is incurred as long as participants form an FL partnership, regardless of their subsequent contribution decisions.

Furthermore, this fixed cost also allows us to intuitively model how players' prior reputations may affect FL partnership formation. For two participants with positive cooperative reputations, the fixed cost will likely be smaller than for participants with no prior knowledge of each other or even with negative reputations. Based on Theorem 5, having a smaller fixed cost c_0 also implies a larger partnership formation region (i.e., it becomes easier to form a FL partnership).

4.3.2. General Cost Functions. Next, suppose we have a general cost function $C(x) > 0$ that is not necessarily a linear function of x. Most results in Sections 4.1 and 4.2 (namely Theorems 1–4 and Corollaries 2–4) still hold because they do not require an explicit form of $C(x)$.[17] Meanwhile, the results in Corollary 1 can be generalized. The cost sensitivity parameter, α, is no longer meaningful when $C(x)$ is nonlinear. Instead, we consider its first-order derivative $C'(x)$ to derive Corollary 5.

Corollary 5. *Suppose $C(x)$ satisfies three conditions:* (i) *it has first-order derivative $C'(x)$,* (ii) *there exists $x^+ > 0$, such that $C(x^+) \geq U(2x^+) - U(x^+)$, and* (iii) *$C'(x) \geq U'(x)$ for any $x \geq x^+$. Then for any $x \geq x^+$, players would not form a long-term FL partnership.*

This corollary provides a broader scope for our previous finding that players who collect a large amount of information per round by themselves have no incentive to form an FL partnership. The same finding is true even under nonlinear cost functions, as long as (1) there exists a critical threshold of information quantity where even the (undiscounted) first-round participation benefit cannot cover the associated cost, and (2) the cost of information exchange grows at least as fast as the corresponding benefit beyond that threshold.

4.4. Partial Contribution or Adversarial Contribution

In our basic model setup, we assume that a defecting player contributes no information to the central server in the defecting round. Although this aligns with the prior literature (Zhang et al. 2022) and the formulation facilitates model tractability, it does not fully capture how defection may take place. In practice, players may defect in less "conspicuous" ways. For instance, instead of contributing no information at all, a player may reduce its cooperation effort and contribute only a part of the new information gathered in a round (e.g., the defecting player can choose to upload its local gradients computed on part of its new data), or it may send poisoned information to the central server in disguise of useful information to mislead the federated model for adversarial purposes (Guerraoui et al. 2018, Bagdasaryan et al. 2020, Wang et al. 2020a).

From a game-theoretic perspective, if nonconspicuous defections can go undetected (and therefore unpunished), then we can expect mutual defection to become the stable outcome, as defection is the dominant strategy regardless of what the other player chooses to do. Fortunately, researchers have developed several techniques to detect and address abnormalities in information exchange (which may result from partial contributions) and malicious attacks, thereby improving the resilience of FL (Blanchard et al. 2017, Liu et al. 2017, Damaskinos et al. 2018, Tran et al. 2018, Xie et al. 2018, Yin et al. 2018, Lecuyer et al. 2019). Although these techniques are far from perfect (because defection mechanisms also continue to evolve), they are shown to have desirable theoretical and computational properties, making them good candidates to be applied in FL practices. We therefore assume that nonconspicuous defections can still be detected.

4.4.1. Defection by Contributing Partial Information. We first consider defection by contributing partial information. In a given round, although each player still collects x amount of information that can be shared, a defecting player only shares x' amount of information ($0 < x' < x$). We repeat the analyses and derive the following results.

Theorem 6. *When players defect by contributing partial information x' $(0 < x' < x)$, two players will cooperate*

repeatedly if and only if

$$C(x)-(1-\gamma)C(x')<(1-\gamma)^2\sum_{t=1}^{+\infty}\gamma^{t-1}\{U(2tx)-U((t+1)x)\}$$
(under grim trigger only),

$$C(x)-C(x')<(1-\gamma)\sum_{t=2}^{+\infty}\gamma^{t-1}\{U(2tx)-U(2tx-x+x')\}$$
(under tit-for-tat only),

$$\gamma<1-\frac{C(x)-C(x')}{U(2x)-U(x)}$$
(under sanction only),

$$C(x)-(1-\gamma)C(x')<(1-\gamma)^2\sum_{t=1}^{+\infty}\gamma^{t-1}\{U(2tx)-U(tx)\}$$
(under sanction and grim trigger),

$$C(x)-C(x')<(1-\gamma)(U(2x)-U(x))+(1-\gamma)\sum_{t=2}^{+\infty}\gamma^{t-1}\{U(2tx)-U(2tx-x+x')\}$$
(under sanction and tit-for-tat).

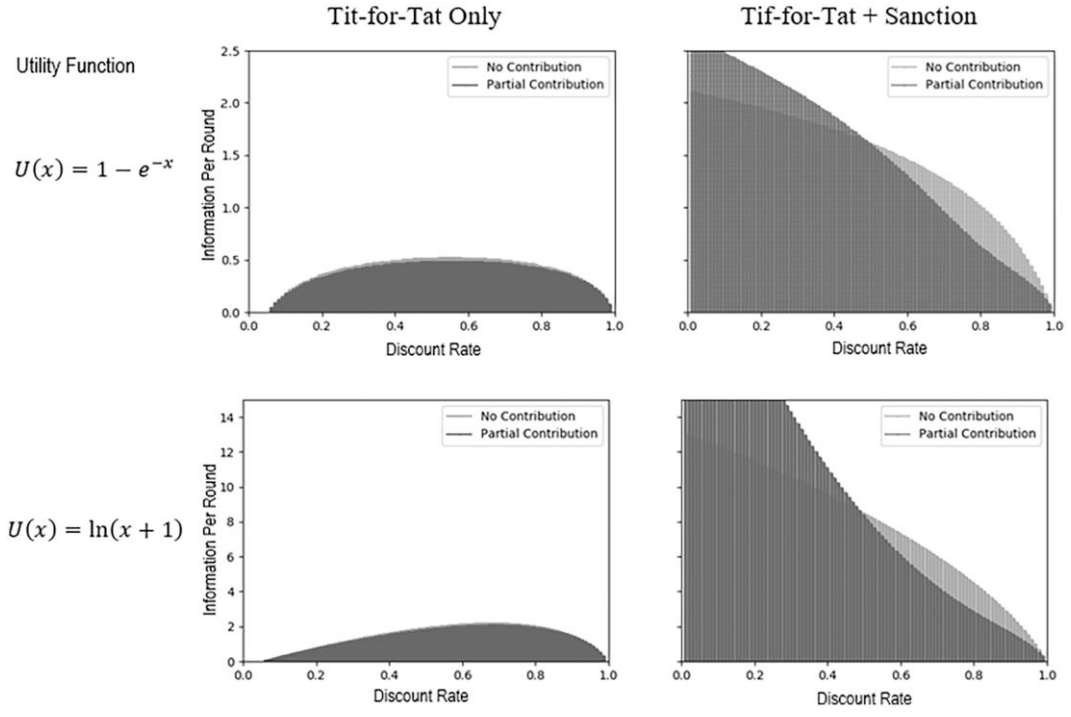
We compare the conditions for repeated cooperation with those obtained in the basic model and make several observations. First, under the grim trigger strategy (both with and without sanction), the left-hand-side term that involves cost of contribution decreases from $C(x)$ to $C(x)-(1-\gamma)C(x')$, which would lead to a wider range for cooperation-inducing γ for a given value of x. This is also true under sanction alone, as the upper bound on γ increases. Intuitively, unlike defection by contributing no information, contributing partial information is not cost-free to a player, which makes cooperation comparatively more attractive.

However, the same cannot be said under the tit-for-tat strategy (both with and without sanction). Although the cost-related term decreases from $C(x)$ to $C(x)-C(x')$, the term associated with marginal utility also decreases from $U(2tx)-U(2tx-x)$ to $U(2tx)-U(2tx-x+x')$. Numerically, we compare the cooperation region in the basic model (where defection means no contribution) with that under partial contribution (setting $x'=0.5x$). Same as before, we focus on exponential and logarithm utility functions and fix $\alpha=0.05$, and plot the results in Figure 3. We observe that the two forms of defection lead to almost identical cooperation regions under the tit-for-tat strategy alone. However, when sanction is added, partial contribution leads to narrower/wider cooperation range for smaller/larger x. In other words, how the cooperation region would change depends jointly on the contractual mechanism (i.e., whether sanction is imposed) as well as the value of x.

4.4.2. Defection by Sending Adversarial Information.

As another defection mechanism, players may also be malicious and send noisy or poisoned information in disguise of useful information to mislead the federated model. This can be achieved in multiple ways. For example, a player may send a vector of randomly

Figure 3. Region of Cooperation Under Two Forms of Defection



generated values to represent the actual gradients or engage in adversarial attacks where the player strategically introduces errors into the data (e.g., "backdoor attacks," which misclassifies certain carefully selected instances; Chen et al. 2017, Bagdasaryan et al. 2020, Wang et al. 2020a). Sending adversarial information poses almost no privacy risks to the defecting player, because the information being shared does not truthfully represent the actual data that the player owns. However, receiving poisoned information can actually *hurt* the other player, because it pollutes the global model. As an example, under the FedAvg algorithm, injecting random noises would reduce the quality of the federated gradients. In other words, defection by sending adversarial information imposes negative externality on the victim at almost no cost to the defector.

To model such dynamics, we set the amount of "adversarial information" being sent by a defecting player as $-\xi < 0$ and assume that $C(-\xi) = 0$. Suppose the other player cooperates and contributes x information, the net information available to update the global model would become $x - \xi$. We again repeat the analyses and derive the following conditions of repeated cooperation.

Theorem 7. *When players defect by sending adversarial information $-\xi < 0$, two players will cooperate repeatedly if and only if*

$$C(x) < (1-\gamma)^2 \sum_{t=1}^{+\infty} \gamma^{t-1}\{U(2tx) - U((t+1)x)\} \quad \text{(under grim trigger only)},$$

$$C(x) < (1-\gamma) \sum_{t=2}^{+\infty} \gamma^{t-1}\{U(2tx) - U(2tx - x - \xi)\} \quad \text{(under tit-for-tat only)},$$

$$\gamma < 1 - \frac{C(x)}{U(2x) - U(x)} \quad \text{(under sanction only)},$$

$$C(x) < (1-\gamma)^2 \sum_{t=1}^{+\infty} \gamma^{t-1}\{U(2tx) - U(tx)\} \quad \text{(under sanction and grim trigger)},$$

$$C(x) < (1-\gamma)(U(2x) - U(x)) + (1-\gamma) \sum_{t=2}^{+\infty} \gamma^{t-1}\{U(2tx) - U(2tx - x - \xi)\} \quad \text{(under sanction and tit-for-tat)}.$$

We find that, under grim trigger, sanction, and the combination of the two, the conditions for repeated cooperation are exactly the same as in the basic model. This is because defection by sending adversarial information affects only the recipient player on the defecting round but does not create any cost for the defecting player. Under the tit-for-tat strategy, interestingly, sending adversarial information in fact *increases* the marginal utility term on the right-hand-side from $U(2tx) - U(2tx - x)$ to $U(2tx) - U(2tx - x - \xi)$. As a result, the range of cooperation-inducing γ would become *wider*. This is because, immediately after the defection round, the defector would get tit-for-tat retaliation from the other player and receive adversarial information (via access to the global model). The negative impact of adversarial information on the defector's utility would make mutual cooperation a comparatively more attractive option. Put differently, from a game-theoretic perspective, defection by sending adversarial information under the tit-for-tat strategy actually deters defection to some extent.

This result also has implications for how players should deal with malicious defection. Technically speaking, after detecting a malicious attack, the victim player can always discard the federated gradients and instead rely on its own information for model training in the defection round. Doing so at least protects the victim player from being hurt by the adversarial information. This is equivalent to setting $\xi = 0$, which reverts the result back to that in the basic model. However, it turns out that tit-for-tat retaliation by sending adversarial information in the next round can be more effective in *deterring* defection from happening in the first place. Therefore, from a contract design perspective, implementing a tit-for-tat trigger strategy and requiring players to accept the global model (even with adversarial information) can in fact encourage repeated cooperation.

5. Extension to Nonidentical Players and Multiple Players

In this section, we extend our analyses to examine the cases of nonidentical players and multiple players. Although the theoretical analyses of these two cases involve more technicalities, the main findings about players' incentive to form long-term FL partnership and the effectiveness of different contractual mechanisms remain largely consistent with the case of two identical players. Therefore, we include the technical details in Online Appendix F, while focusing on the additional insights revealed by the analyses in this section. Specifically, in the case of nonidentical players, we discuss which of the two players is the "bottleneck" that determines repeated cooperation; in the case of multiple players, we discuss how the cooperation dynamics are affected by the percentage of defectors.

5.1. Case of Two Nonidentical Players

We start by considering two players with different degrees of sensitivity or vulnerability toward the cost of contribution. For example, players that have adopted rigorous privacy and data security measures and protocols may be less vulnerable to information exchange in a FL partnership than less well-prepared ones. To operationalize it, we assign different unit costs for the two

players, such that $C_A(x) = \alpha_A x$ and $C_B(x) = \alpha_B x$. We find that cooperation is determined by the player who is more sensitive/vulnerable to the risk of contribution. In other words, if the more cost sensitive player is willing to engage in repeated cooperation, then the less cost sensitive player is also willing to do so.

The two players may also have different capabilities to extract value from a federated ML model, depending on their operational abilities to use the model for effective decision making. In the specific context of healthcare, the value of a ML model can be affected by whether a healthcare institution can successfully integrate/implement the model into its operations to deliver better healthcare services. There are potentially multiple ways to characterize the differential value extraction capabilities. Here, we assign different weights to the utility functions of different players; specifically, $U_A(x) = \beta_A U(x)$ and $U_B(x) = \beta_B U(x)$, where the weights $\{\beta_A, \beta_B\}$ essentially describe the "efficiency" of value extraction. The two players still share the same (unweighted) utility function $U(.)$, which is determined by the performance of the global FL model, but they differ in how much utility they can realize based on the shared global model. We find that cooperation is determined by the player that is less efficient in extracting value from the global FL model.

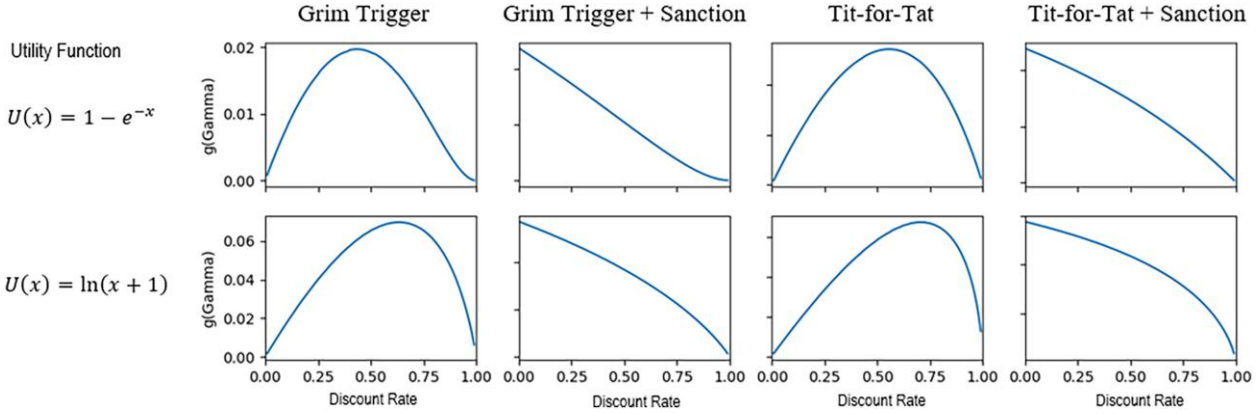
The third scenario we consider is when the two players differ in the amount of information they collect (and decide whether to contribute) in each round. In particular, suppose the amount of information gathered by players A and B is x_A and x_B, respectively. Regardless of the contractual mechanism, the defection payoff is always higher for the player with larger information acquisition capacity. Let $\pi^D(.)$ be the discounted total payoff of defection. Then $x_A < x_B \Rightarrow \pi^D(A) < \pi^D(B)$. As a result, cooperation will be determined by the player who collects a larger amount of information per round. An intuitive explanation of this pattern is that the player with larger information acquisition capacity is more "self-sufficient" and is therefore less threatened by the lack of cooperation. This finding remains unchanged even when the amount of information varies across different rounds.

Overall, these three scenarios suggest a consistent pattern. In FL with nonidentical players, repeated cooperation is determined by the player who bears more cost or extracts less benefit from contributing to the FL. Finally, we consider the scenario where the two players have different discount rates. This particular scenario is singled out because deriving theoretical results turns out to require stronger assumptions on the functional form of $U(.)$ (such as conditions on its derivatives), and we therefore rely on numerical analyses to understand how differential discount rates of the two players determine cooperation outcomes with specific forms of $U(.)$.

Suppose the two players have discount rates γ_A and γ_B and assume that $\gamma_A < \gamma_B$. Although the discount rate does not affect how much payoff a player receives within a given round, it will affect how future payoffs discounts to the present and thereby determine the total payoff for the player. Taking the grim trigger strategy as an example, let $g_T(\gamma) = (1-\gamma)^2 \sum_{t=2}^{T} \gamma^{t-1}\{U(2tx) - U((t+1)x)\}$ denote the approximation of the corresponding infinite sum up to a given precision level ε. The cooperation condition is then given by $C(x) < \min\{g_T(\gamma_A), g_T(\gamma_B)\}$. Taking a numerical approach, we plot the images of $g_T(\gamma)$ for both exponential and logarithm utility functions under different contractual mechanisms in Figure 4 (keeping $x = 0.5$ and precision level $\varepsilon = 0.001$, although changing these parameters do not change the overall shapes of the $g_T(\gamma)$ functions).

As we can see, under trigger strategy alone, the image of $g_T(\gamma)$ has an inverted-U shape. Therefore, the relative size of $g_T(\gamma_A)$ and $g_T(\gamma_B)$ depends on where γ_A and γ_B are located with respect to the γ value that maximizes $g_T(\gamma)$. More specifically, let $\gamma^* = \arg\max g_T(\gamma)$. If $\gamma_A < \gamma_B \le \gamma^*$, then two players will cooperate if and only if $C(x) < g(\gamma_A)$. Conversely, if $\gamma^* \le \gamma_A < \gamma_B$, then two players will cooperate if and only if $C(x) < g(\gamma_B)$. If

Figure 4. (Color online) Images of $g_T(\gamma)$ Under Different Contractual Mechanisms



$\gamma_A < \gamma^* \leq \gamma_B$, then we cannot say which player will drive the cooperation outcome a priori—It would depend on the symmetry and shape of the $g_T(\gamma)$ function. In contrast, under the combination of trigger strategy and sanction, $g_T(\gamma)$ is monotonically decreasing, which implies that two players will cooperate if and only if $C(x) < g(\gamma_B)$.

Beyond the aforementioned results, our framework also allows for the analyses of scenarios where players simultaneously differ on multiple dimensions. As one illustrative example, if player B is more sensitive to the cost of contribution (i.e., $\alpha_A < \alpha_B$), whereas player A has a lower value extraction capability (i.e., $\beta_A < \beta_B$), then the cooperation outcome will be determined jointly by player B's contribution cost $C_B(x)$ and player A's value extraction capability coefficient β_A (see Online Appendix F for results). These results offer actionable insights to promote cooperation in long-term FL. For example, recent FL literature has examined the use of monetary transfer among FL participants as a way to incentivize contribution (Tang and Wong 2021, Tu et al. 2022), and our insights here can inform the selection of the least motivated participant to receive monetary transfer from other (more motivated) participants, thereby encouraging repeated contribution over time.

5.2. Case of Multiple Players

We now discuss the case where multiple players participate in an FL partnership. For expositional simplicity, we assume the players are identical and defection takes the form of contributing no information. Formally, suppose there are K identical players in total, denoted as $\{P_1, \ldots, P_K\}$, each gathering x amount of information that can potentially be contributed during one round of the FL process. Further suppose there can be s defectors ($s < K$) who contribute no information with any of the other players during defection rounds. For each defector, comparing the utility associated with defection (under different contractual mechanisms) with the utility associated with cooperation would produce the boundary conditions for repeated cooperation, which we summarize in Online Appendix F.

We find that, given a fixed K (i.e., total number of players), having a larger s (i.e., more defectors) in fact *widens* the range of cooperation-inducing γ. This is because having a larger percentage of defectors dilutes the benefit of defection, that is, the total information shared by cooperators becomes smaller, which naturally makes defection a less attractive action for the players. Put differently, although being the only defector is certainly advantageous during the defection round, being one of many defectors is less so. From a practical perspective, such a "crowding-out" effect may act as a natural barrier against defection in a multiplayer FL setting.

6. Discussion

Practical applications of machine learning is often hindered by the "information silo" problem, where the data necessary to build the ML models are scattered across many individuals or organizations, who are reluctant to share their data with each other due to privacy and security concerns. Although federated learning represents a promising technical solution to address this problem, we are yet to witness its wide deployment in practice. The understanding of some fundamental questions around FL partnership formation and repeated contribution in the long term is lacking. In this paper, we take an analytical approach to provide a formal analysis of the incentives and tradeoffs involved in a long-term FL partnership.

6.1. Key Findings and Implications

Using an iterated prisoner's dilemma framework, our analyses provide several key insights regarding (1) the boundary conditions for players to form a long-term FL partnership rather than building ML models by themselves and (2) the effectiveness of different contractual mechanisms in promoting repeated cooperation throughout the FL process.

First, we find that player with higher cost sensitivity or larger information acquisition capability generally has lower incentive to participate in long-term FL, because the total cost of contributions overwhelms the benefits. These findings contribute to our understanding of FL partnership formation. Taking healthcare FL as an example, the implication of these findings is that FL partnership may be harder to form among large institutions with heavy patient traffics (which generate large amounts of patient information) or for very prevalent diseases such as the common cold (for which each institution naturally has a lot of data). Meanwhile, from a prescriptive perspective, innovations in privacy protection techniques (e.g., differential privacy and homomorphic encryption for data protection, and the blockchain technology for secure information transmission) that reduce the cost of contribution can facilitate FL partnership formation.

Second, players' temporal preferences, which determines how myopic versus forward-looking they behave, also determine their willingness to participate in long-term FL. Contrary to the conventional wisdom in IPD, we find an *upper* bound on the discount rate, indicating that highly forward-looking players are unwilling to form long-term FL partnerships as they tend to rely on the accumulation of their own data to avoid the cost of contributions. Meanwhile, our numerical analyses also provide empirical evidence that FL partnership is more likely to form if the underlying ML problem benefits more from a unit increase in information. Keeping in mind that a player's temporal preference is also affected

by properties of the ML problem (e.g., how the value of a ML model changes over time), these two findings collectively implies that FL is more attractive for ML tasks that are more time sensitive and data hungry. For example, infectious disease (e.g., COVID-19) control or rare disease diagnoses, which are challenging tasks with pressing clinical importance, may be more suitable to be tackled by FL (Rieke et al. 2020, Dayan et al. 2021).

Third, players who are "on board" with FL may nevertheless choose to defect during the FL process, and proper contractual mechanisms need to be put in place to promote repeated cooperation. A unique characteristic of FL is that such mechanisms can be imposed by the central server (i.e., sanction) or by players themselves (i.e., trigger strategies such as grim trigger or tit-for-tat). Our theoretical and numerical analyses demonstrate that, by itself, a server-imposed sanction or a player-initiated trigger strategy is not sufficient to fully prevent defection. Under sanction, defection can take place for forward-looking players who gather a small amount of information per round. Under grim trigger or tit-for-tat strategies, both myopic or forward-looking players have incentive to defect. Fortunately, we find that implementing sanction and a trigger strategy jointly is able to fully prevent defection. Considering that grim trigger is highly unforgiving, the combination of sanction and the tit-for-tat strategy represents an effective and practical contractual mechanism to promote repeated cooperation in long-term FL.

Taken together, our findings offer concrete and actionable managerial insights. As an illustration, suppose a policy maker seeks to facilitate a FL partnership to contain an infectious disease. On one hand, the time-sensitive nature of the task is appropriate for FL; On the other hand, different healthcare institutions likely differ in their sizes, which affects how much data they collect by themselves. Our findings suggest that the policy maker should focus on selecting relatively small institutions to form the FL. Moreover, institutions with challenging financial situations (hence higher cost sensitivities) may be hesitant to participate despite their willingness. To get them on board, the policy maker can consider providing a subsidy or establishing a "reward transfer" scheme that allows participants with low cost sensitivities to compensate them (see Tang and Wong (2021) for an example). In this case, our work informs the identification of *who* should receive reward transfer, and other research such as Tang and Wong (2021) can inform how to carry out reward transfer (e.g., *how much* and *when* to transfer). These mechanisms satisfy the individual rationality (IR) condition, because a successful FL can create a larger net benefit for all participants than what they would have obtained without the FL. Our findings also inform contract design. The effectiveness of central server sanction (in addition to trigger strategy) in promoting repeated contributions strongly supports the adoption of an algorithmic FL platform (such as FedML, Flame, and FedScale) that not only orchestrates the exchange of model information but can also automate central server sanctions when needed. Our analyses in Section 4.2.3 have shown that such a mechanism is regret-free for participants since repeated contributions yield higher utilities than defection.

We further analyze the cooperation dynamics under (1) two alternative types of defection; (2) heterogeneous players; and (3) multiple players. These analyses generated additional findings with practically relevant implications, some of which we highlight here. Defection by sharing adversarial information poses a nontrivial challenge to FL, as one player's "contribution" can actually hurt others. However, we find that adversarial defection can be effectively deterred under the tit-for-tat strategy. In the case of heterogeneous players, we identify that repeated cooperation is determined by the player with higher cost sensitivity, lower value extraction capability, larger information acquisition capacity, or more extreme temporal preference. These findings can help FL practitioners to identify the "bottleneck" in a partnership and inform partner selection decisions. Finally, in a FL partnership with multiple players, being a defector becomes economically less beneficial as more players defect. Such a "crowding-out" effect can serve as a natural barrier against defection in a multiplayer FL partnership.

Although we have used healthcare as an example application domain throughout the paper, our results are highly relevant for a number of other prominent domains. For example, finance and insurance institutions possess rich demographic and financial information of different individuals and can engage in FL to jointly build machine learning models that predict credit scores or loan defaults (Yu et al. 2020). Pharmaceutical companies (such as Novartis and Merck) can pool their medical research data via FL to accelerate drug discovery.[18] Furthermore, smart manufacturers can use FL to aggregate their sensor data to build models that facilitate product defect detection and production process optimization (Hegiste et al. 2022). More generally, because our model considers *cross-silo horizontal* FL (as discussed in Section 2.1), it is broadly relevant to domains where a relatively small number of large entities (e.g., a handful of companies or institutions, as opposed to millions of individuals) each possessing different data samples that share the same set of features (rather than a same data sample with nonoverlapping features).

6.2. Future Research Directions

Our work opens up a number of important directions for future research. First, there are several ways to extend our model to incorporate more realistic considerations in FL. As we have shown, the cost of contribution is a key

determinant of cooperation outcome. If players could strategically decide the amount of information they share during each round, then one needs to go beyond a binary choice between cooperate (share all information) and defect (share no information or a fixed amount of information) and instead consider a continuous and potentially time-varying strategy space and solve for mixed strategy equilibria. In addition, we have focused on two canonical trigger strategies that represent two "extremes": the grim trigger as an extremely unforgiving strategy and the tit-for-tat a highly forgiving one. Future work may examine a wide variety of other strategies, such as win-stay lose-switch (Pavlov; Wedekind and Milinski 1996), and zero-determinant (Press and Dyson 2012) strategies. Second, understanding the economics of FL in other settings that our model does not consider also represents promising future research directions. For example, our current model mainly focuses on the quantities of data rather than the variety of data from different FL participants, partly because combining local models that are trained on data from different probability distributions (e.g., from very different patient populations) or data with different feature sets (i.e., vertical FL) to form a global model remains a key challenge in FL algorithm design (Kairouz et al. 2019, Li et al. 2020). Studying these settings may require characterizing the values of different types of data to different participants. Moreover, cross-device FL is also an important setting, where millions of individuals (or devices) are potential participants. How to select the most productive participants and incentivize their contributions in a cross-device FL are interesting research questions. Finally, successful deployment of FL in practice would likely require more than the cooperation among partners but also the active involvement of many other stakeholders. For example, FL deployment in healthcare would rely on collaborations across technology providers, insurance companies, policy makers, and regulatory bodies (e.g., the US Food and Drug Administration). Similarly, successful FL applications in finance need joint efforts from financial institutions and multiple policy agencies (e.g., Federal Deposit Insurance Corporation and U.S. Securities and Exchange Commission). We therefore advocate for future work that offers a comprehensive investigation of other relevant stakeholders and their roles in FL.

Endnotes

[1] See https://ai.googleblog.com/2017/04/federated-learning-collaborative.html.

[2] We use "repeated cooperation" and "repeated contributions" interchangeably in the paper—Both terms refer to a player's decision to repeatedly share its local model with the server as a form of cooperative behavior.

[3] One "round" in the FL process is different from one "iteration" in the FL algorithm. In each round, most FL algorithms (e.g., FedAvg) need to run for multiple iterations before convergence. We follow the FL literature to assume that, within each round, the learning algorithm runs till it fully converges.

[4] Example algorithmic systems that act as the central server in FL: NVIDIA Clara (https://developer.nvidia.com/blog/federated-learning-clara/), FedML (https://fedml.ai/), Flame (https://github.com/cisco-open/flame), and FedScale (https://github.com/SymbioticLab/FedScale).

[5] For example, given a sample of size n, one may model the amount of information x (e.g., embedded in model gradients) to be proportional to the sample size, e.g., $x = \delta n$, as gradients aggregate the information across n data points. Because the scaling parameter δ remains a constant, we do not carry it in the model.

[6] Technically, to achieve this free-riding, the defector can first update its local model using the gradients of the global model (which incorporate the data from the other player), then further update the local model with its own private data.

[7] Some recurring costs associated with data storage, processing, and computations are not included here, because they would be incurred every round even if a player defects (i.e., the player would still store the new information and use it for local model training).

[8] For instance, if the player were to compensate the victims of a data breach, the total compensation would be a linear function of the number of victims, as was the case in Target's 2013 credit card data breach settlement and an ongoing class-action lawsuit against Google's Chrome browser privacy violation (McCoy 2017, Winder 2020).

[9] Specifically, fixing t and X^p_{t-1} and subtracting $U(X^p_{t-1} + x) - U(X^p_{t-1})$ from every element would transform the payoff matrix to be that in a donation game.

[10] We focus on grim trigger and tit-for-tat as two canonical examples of trigger strategies. They are chosen to represent a highly unforgiving strategy and a highly forgiving one.

[11] Of course, players may choose to participate in long-term FL but strategically defect instead of engaging in repeated contributions later. Contractual mechanisms need to be put in place to deter defection and promote cooperation, which we consider in Section 4.2.

[12] This is guaranteed by the Cauchy's convergence criterion.

[13] In fact, the case of $\gamma = 0$ essentially corresponds to a one-round FL setting, where players only care about the cost and benefit in the first round of FL.

[14] As an example of bounded utility, an ML model for medical diagnosis, after reaching a required level of predictive performance, can apply for FDA approval to be integrated as part of a medical device. Although the model's predictive performance (and value) can further improve with more data, it is ultimately bounded by a fixed level (e.g., the utility at 100% predictive accuracy). In contrast, generative AI likely falls into the unbounded category. As more data (e.g., textual content in EHRs or doctors' notes) become available, generative AI can potentially develop new/emerging capabilities that create additional values.

[15] Following the same logic, we can further show that a harsher sanction, where the central server withholds the global model until a defector cooperates for multiple consecutive rounds, results in a wider cooperation-inducing range of γ.

[16] We plot the cooperation region in the interior of the boundary, because willingness to form a FL partnership is a prerequisite for repeated cooperation.

[17] The specific numerical values of partnership formation and repeated contribution boundaries would be different under different cost functions.

[18] See, for example, the MELLODDY project joined by 10 major pharmaceutical companies: https://venturebeat.com/ai/major-pharma-companies-including-novartis-and-merck-build-federated-learning-platform-for-drug-discovery/.

References

Akin E (2016) The iterated prisoner's dilemma: Good strategies and their dynamics. Assani I, ed. *Ergodic Theory, Advances in Dynamical Systems* (De Gruyter, Berlin), 77–107.

Aledhari M, Razzak R, Parizi RM, Saeed F (2020) Federated learning: A survey on enabling technologies, protocols, and applications. *IEEE Access* 8:140699–140725.

Arend RJ, Seale DA (2005) Modeling alliance activity: An iterated prisoners' dilemma with exit option. *Strategic Management J.* 26(11):1057–1074.

Aumann RJ (2006) War and peace. *Proc. National Acad. Sci. USA* 103(46):17075–17078.

Axelrod R, Hamilton WD (1981) The evolution of cooperation. *Science* 211(4489):1390–1396.

Bagdasaryan E, Veit A, Hua Y, Estrin D, Shmatikov V (2020) How to backdoor federated learning. Chiappa S, Calandra R, eds. *Proc. Internat. Conf. on Artificial Intelligence and Statist.*, 2938–2948. https://aistats.org/aistats2020/.

Bai G, Jiang JX, Flasher R (2017) Hospital risk of data breaches. *JAMA Internal Medicine* 177(6):878–880.

Bhowmick A, Duchi J, Freudiger J, Kapoor G, Rogers R (2018) Protection against reconstruction and its applications in private federated learning. Preprint, submitted December 3, https://arxiv.org/abs/1812.00984.

Blanchard P, El Mhamdi EM, Guerraoui R, Stainer J (2017) Machine learning with adversaries: Byzantine tolerant gradient descent. von Luxburg U, Guyon I, Bengio S, Wallach H, Fergus R, eds. *Proc. 31st Internat. Conf. on Neural Inform. Processing Systems* (Curran Associates Inc., Red Hook, NY), 118–128.

Blum A, Haghtalab N, Phillips RL, Shao H (2021) One for one, or all for all: Equilibria and optimality of collaboration in federated learning. Meila M, Zhang T, eds. *Proc. 38th Internat. Conf. Machine Learn. (ICML)*, vol. 139 (PMLR, New York), 1005–1014.

Chen X, Liu C, Li B, Lu K, Song D (2017) Targeted backdoor attacks on deep learning systems using data poisoning. Preprint, submitted December 15, https://arxiv.org/abs/1712.05526.

Chong SY, Yao X (2006) Self-adapting payoff matrices in repeated interactions. Louis SJ, Kendall G, eds. *Proc. IEEE Sympos. on Comput. Intelligence and Games* (IEEE, Piscataway, NJ), 103–110.

Damaskinos G, Guerraoui R, Patra R, Taziki M, et al. (2018) Asynchronous byzantine machine learning (the case of SGD). Dy JG, Krause A, eds. *Proc. 35th Internat. Conf. Machine Learn. (ICML)*, vol. 80 (PMLR, New York), 1145–1154.

Dayan I, Roth HR, Zhong A, Harouni A, Gentili A, Abidin AZ, Liu A, et al. (2021) Federated learning for predicting clinical outcomes in patients with covid-19. *Nature Medicine* 27(10):1735–1743.

Donahue K, Kleinberg J (2021a) Model-sharing games: Analyzing federated learning under voluntary participation. *35th AAAI Conf. Artificial Intelligence, 33rd Conf. Innovative Appl. Artificial Intelligence (IAAI), 11th Sympos. Ed. Adv. Artificial Intelligence (EAAI)*, vol. 35 (AAAI Press, Washington, DC), 5303–5311.

Donahue K, Kleinberg J (2021b) Optimality and stability in federated learning: A game-theoretic approach. Ranzato M, Beygelzimer A, Dauphin Y, Liang PS, Wortman Vaughan J, eds. *Adv. Neural Inform. Processing Systems*, vol. 34 (Curran Associates, Inc., Red Hook, New York), 1287–1298.

Geiping J, Bauermeister H, Dröge H, Moeller M (2020) Inverting gradients: How easy is it to break privacy in federated learning? Larochelle H, Ranzato M, Hadsell R, Balcan MF, Lin H, eds. *Adv. Neural Inform. Processing Systems*, vol. 33 (Curran Associates Inc., Red Hook, NY), 16937–16947.

Geyer RC, Klein T, Nabi M (2017) Differentially private federated learning: A client level perspective. Preprint, submitted December 20, https://arxiv.org/abs/1712.07557.

Guerraoui R, Mhamdi EME, Guerraoui R, Rouault S (2018) The hidden vulnerability of distributed learning in byzantium. Dy JG, Krause A, eds. *Proc. 35th Internat. Conf. on Machine Learn.* (PMLR, New York), 3521–3530.

Han T, Nebelung S, Haarburger C, Horst N, Reinartz S, Merhof D, Kiessling F, et al. (2020) Breaking medical data sharing boundaries by using synthesized radiographs. *Sci. Adv.* 6(49):eabb7973.

Hard A, Rao K, Mathews R, Ramaswamy S, Beaufays F, Augenstein S, Eichner H, et al. (2018) Federated learning for mobile keyboard prediction. Preprint, submitted November 8, https://arxiv.org/abs/1811.03604.

Hegiste V, Legler T, Ruskowski M (2022) Application of federated machine learning in manufacturing. *Proc. Internat. Conf. on Industry 4.0 Tech* (IEEE, Piscataway, NJ), 1–8.

Hilbe C, Nowak MA, Sigmund K (2013) Evolution of extortion in iterated prisoner's dilemma games. *Proc. National Acad. Sci. USA* 110(17):6913–6918.

Jurišić M, Kermek D, Konecki M (2012) A review of iterated prisoner's dilemma strategies. *Proc. 35th Internat. Convention MIPRO* (IEEE, Piscataway, NJ), 1093–1097.

Kairouz P, McMahan HB, Avent B, Bellet A, Bennis M, Bhagoji AN, Bonawitz K, et al. (2019) Advances and open problems in federated learning. Preprint, submitted December 10, https://arxiv.org/abs/1912.04977.

Kaissis G, Ziller A, Passerat-Palmbach J, Ryffel T, Usynin D, Trask A, Lima I, et al. (2021) End-to-end privacy preserving deep learning on multi-institutional medical imaging. *Nature Machine Intelligence* 3(6):473–484.

Kaissis GA, Makowski MR, Rückert D, Braren RF (2020) Secure, privacy-preserving and federated machine learning in medical imaging. *Nature Machine Intelligence* 2(6):305–311.

Kendall G, Yao X, Chong SY (2007) *The Iterated Prisoners' Dilemma: 20 Years on*, vol. 4 (World Scientific, Singapore).

Lecuyer M, Atlidakis V, Geambasu R, Hsu D, Jana S (2019) Certified robustness to adversarial examples with differential privacy. *Proc. IEEE Sympos. on Security and Privacy* (IEEE, Piscataway, NJ), 656–672.

Li T, Sahu AK, Talwalkar A, Smith V (2020) Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine* 37(3):50–60.

Li W, Milletarì F, Xu D, Rieke N, Hancox J, Zhu W, Baust M, et al. (2019) Privacy-preserving federated brain tumour segmentation. *Proc. Internat. Workshop on Machine Learn. in Medical Imaging* (Springer, Berlin), 133–141.

Liu Y, Xie Y, Srivastava A (2017) Neural trojans. *Proc. IEEE Internat. Conf. on Computer Design* (IEEE, Piscataway, NJ), 45–48.

McCoy K (2017) Target to pay $18.5m for 2013 data breach that affected 41 million consumers. Accessed July 27, 2023, https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932.

McCoy TH, Perlis RH (2018) Temporal trends and characteristics of reportable health data breaches, 2010–2017. *JAMA* 320(12):1282–1284.

McMahan B, Moore E, Ramage D, Hampson S, Arcas BA (2017) Communication-efficient learning of deep networks from decentralized data. Singh A, Zhu J, eds. *Artificial Intelligence and Statistics* (PMLR, New York), 1273–1282.

Melloddy (2019) Machine learning ledger orchestration for drug discovery. Accessed July 27, 2023, https://www.melloddy.eu/.

Miller AR, Tucker C (2009) Privacy protection and technology diffusion: The case of electronic medical records. *Management Sci.* 55(7):1077–1093.

Miller AR, Tucker C (2014) Health information exchange, system size and information silos. *J. Health Econom.* 33:28–42.

Musketeer (2019) Machine learning to augment shared knowledge in federated privacy-preserving scenarios. Accessed July 27, 2023, https://musketeer.eu/.

Press WH, Dyson FJ (2012) Iterated prisoner's dilemma contains strategies that dominate any evolutionary opponent. *Proc. National Acad. Sci. USA* 109(26):10409–10413.

Rezaei G, Kirley M (2009) The effects of time-varying rewards on the evolution of cooperation. *Evolution Intelligence* 2(4):207–218.

Rieke N, Hancox J, Li W, Milletari F, Roth HR, Albarqouni S, Bakas S, et al. (2020) The future of digital health with federated learning. *NPJ Digital Medicine* 3(1):1–7.

Roth HR, Chang K, Singh P, Neumark N, Li W, Gupta V, Gupta S, et al. (2020) Federated learning for breast density classification: A real-world implementation. *Domain Adaptation and Representation Transfer, and Distributed and Collaborative Learning* (Springer, Berlin), 181–191.

Sarma KV, Harmon S, Sanford T, Roth HR, Xu Z, Tetreault J, Xu D, et al. (2021) Federated learning improves site performance in multicenter deep learning without data sharing. *J. Amer. Medical Inform. Assoc.* 28(6):1259–1264.

Sheller MJ, Edwards B, Reina GA, Martin J, Pati S, Kotrotsou A, Milchenko M, et al. (2020) Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data. *Sci. Rep.* 10(1):1–12.

Tang M, Wong VW (2021) An incentive mechanism for cross-silo federated learning: A public goods perspective. *Proc. IEEE INFOCOM Confe. on Computer Comm.* (IEEE, Piscataway, NJ), 1–10.

Tomochi M, Kono M (2002) Spatial prisoner's dilemma games with dynamic payoff matrices. *Phys. Rev. E* 65(2):026112.

Tran B, Li J, Madry A (2018) Spectral signatures in backdoor attacks. Preprint, submitted November 1, https://arxiv.org/abs/1811.00636.

Tu X, Zhu K, Luong NC, Niyato D, Zhang Y, Li J (2022) Incentive mechanisms for federated learning: From economic and game theoretic perspective. *IEEE Trans. Cognitive Comm. Networks* 8(3):1566–1593.

Wang H, Sreenivasan K, Rajput S, Vishwakarma H, Agarwal S, Sohn J, Lee K, et al. (2020a) Attack of the tails: Yes, you really can backdoor federated learning. Preprint, submitted July 9, https://arxiv.org/abs/2007.05084.

Wang P, Shen C, Roth HR, Yang D, Xu D, Oda M, Misawa K, et al. (2020b) Automated pancreas segmentation using multi-institutional collaborative deep learning. *Domain Adaptation and Representation Transfer, and Distributed and Collaborative Learning* (Springer, Berlin), 192–200.

Webank (2019) WeBank and Swiss resigned cooperation MOU. Accessed July 27, 2023, https://markets.businessinsider.com/news/stocks/webank-and-swiss-re-signed-cooperation-mou-1028228738.

Wedekind C, Milinski M (1996) Human cooperation in the simultaneous and the alternating prisoner's dilemma: Pavlov vs. generous tit-for-tat. *Proc. National Acad. Sci. USA* 93(7):2686–2689.

Winder D (2020) Google chrome privacy lawsuit: Could you get a $5,000 payout? Accessed July 27, 2023, https://www.forbes.com/sites/daveywinder/2020/06/03/google-chrome-privacy-lawsuit-could-you-get-a-5000-payout-incognito-mode-class-action/?sh=596e26d51485.

Wu B, Zhao S, Sun G, Zhang X, Su Z, Zeng C, Liu Z (2019) P3SGD: Patient privacy preserving SGD for regularizing deep CNNs in pathological image classification. *Proc. IEEE/CVF Conf. on Computer Vision and Pattern Recognition* (IEEE, Piscataway, NJ), 2099–2108.

Xie C, Koyejo O, Gupta I (2018) Generalized Byzantine-tolerant SGD. Preprint, submitted March 23, https://arxiv.org/abs/1802.10116.

Xu J, Glicksberg BS, Su C, Walker P, Bian J, Wang F (2020) Federated learning for healthcare informatics. *J. Healthcare Inform. Res.* 5:1–19. https://doi.org/10.1007/s41666-020-00082-4.

Yang Q, Fan L, Tong R, Lv A (2021) IEEE federated machine learning. *IEEE Federated Machine Learning - White Paper*, 1–18.

Yang Q, Liu Y, Cheng Y, Kang Y, Chen T, Yu H (2019) Federated learning. *Synthetic Lectures Artificial Intelligence Machine Learn.* 13(3):1–207.

Yin D, Chen Y, Kannan R, Bartlett P (2018) Byzantine-robust distributed learning: Toward optimal statistical rates. Dy JG, Krause A, eds. *Proc. 35th Internat. Conf. Machine Learn. (ICML)*, vol. 80 (PMLR, New York), 5650–5659.

Yu H, Liu Z, Liu Y, Chen T, Cong M, Weng X, Niyato D, et al. (2020) A sustainable incentive scheme for federated learning. *IEEE Intelligent Systems* 35(4):58–69.

Zhang N, Ma Q, Chen X (2022) Enabling long-term cooperation in cross-silo federated learning: A repeated game perspective. *IEEE Trans. Mobile Comput.* 22(7):3910–3924.

Zhu L, Han S (2020) Deep leakage from gradients. *Federated Learning* (Springer, Berlin), 17–31.