Survey of Personalization Techniques for Federated Learning

Viraj Kulkarni[1,2], **Milind Kulkarni**[1], **Aniruddha Pant**[2]
[1]Vishwakarma University
[2]DeepTek Inc

Abstract

Federated learning enables machine learning models to learn from private decentralized data without compromising privacy. The standard formulation of federated learning produces one shared model for all clients. Statistical heterogeneity due to non-IID distribution of data across devices often leads to scenarios where, for some clients, the local models trained solely on their private data perform better than the global shared model thus taking away their incentive to participate in the process. Several techniques have been proposed to personalize global models to work better for individual clients. This paper highlights the need for personalization and surveys recent research on this topic.

1 Introduction

Many datasets are inherently decentralized in nature and are distributed across multiple devices owned by different users. Traditional machine learning settings involve aggregating data samples from these users into a central repository and training a machine learning model on it. This movement of data from local devices to a central repository poses two key challenges. Firstly, it compromises the privacy and security of the data. Policies such as the General Data Protection Regulation (GDPR) [1] and Health Insurance Portability and Accountability Act (HIPAA) [2] stipulate provisions that make such movement difficult. Secondly, it imposes communication overheads which, depending on the setting, may be prohibitively expensive.

Federated learning [3] is a framework that enables multiple users known as *clients* to collaboratively train a shared global model on their collective data without moving the data from their local devices. A central server orchestrates the federated learning process which consists of multiple rounds. At the beginning of each round, the server sends the current global model to the participating clients. Each client trains the model on its local data and communicates only the model updates back to the server. The server collects these updates from all clients and makes a single update to the global model thereby concluding the round. By removing the need to aggregate all data on a single device, federated learning overcomes the privacy and communication challenges mentioned above and allows machine learning models to learn on decentralized data.

Federated learning has found numerous practical applications where data is decentralized and privacy is important. For example, it has exhibited good performance and robustness for the problem of next-word-prediction on mobile devices [4]. Bonawitz et. al. [5] propose a scalable system implementing large-scale federated learning for mobile devices. Kairouz et. al. [6] discuss broad challenges and open problems in the field.

The primary incentive for clients to participate in federated learning is obtaining better models. Clients who have insufficient private data to develop accurate local models stand to benefit the most from collaboratively learned models. However, the benefit of participating in federated learning for clients who have sufficient private data to train accurate local models is disputable. Yu et al. [7] show that, for many tasks, some participants may gain no benefit by participating since the global shared model is less accurate than the local models they can train on their own. Hanzely et al. [8] question the utility of a global model that is too far removed from the typical usage of a user. The distribution of data across clients is highly non-IID for many applications. This statistical heterogeneity makes it difficult to train a single model that will work well for all clients. The purpose of this paper is to survey recent research regarding building personalized models for clients in a federated learning setting that are expected to work better than the global shared model or the local individual models.

本文的目的是调查最近关于在联邦学习环境中为客户建立个性化模型的研究，这些模型预期比glocabl model或local model更好地工作。

2 Need for Personalization

Wu et al. [9] list three challenges faced by federated learning systems related to personalization: (1) device heterogeneity in terms of storage, computation, and communication capabilities; (2) data heterogeneity arising due to non-IID distribution of data; (3) model heterogeneity arising from situations where different clients need models specifically customized to their environment. As an example of model heterogeneity, consider the sentence: “I live in .....”. The next-word-prediction task applied on this sentence needs to predict a different answer customized for each user. If heterogeneity does not exist in the data, it may exist in the labels; different clients may assign different labels to the same data.

设备异构
数据异构
模型异构

In the original federated learning design of McMahan et al. [3], the model updates and the final model can leak participant data violating privacy [10] [11]. To preserve privacy, McMahan et al. [12] propose differential privacy techniques that limit the information the global model can reveal about individual participants. However, Yu et al. [7] argue that such privacy protection mechanisms introduce a fundamental conflict between protecting privacy and achieving higher performance for individual users. Bagdasaryan et al. [13] state that the cost of differential privacy mechanisms is the reduction in accuracy, and this cost is borne unequally by clients with the underrepresented or tail participants being affected the worst.

差分隐私保护机制可能损害模型的性能

Personalization of the global model becomes necessary to handle the challenges posed by statistical heterogeneity and non-IID distribution of data. Most techniques for personalization [14] generally involve two discrete steps. In the first step, a global model is built in a collaborative fashion. In the second step, the global model is personalized for each client using the client's private data. Jiang et al. [15] argue that optimizing solely for global accuracy yields models that are harder to personalize and propose that, in order to make federated learning personalization useful in practice, the three following objectives must all be addressed *simultaneously* and not independently: (1) developing improved personalized models that benefit a large majority of clients; (2) developing an accurate global model that benefits clients who have limited private data for personalization; (3) attaining fast model convergence in a small number of training rounds. Out of the local data samples stored with each client, it may happen that only a subset of samples are relevant for a particular task, while the irrelevant samples adversely affect the model training. Tuor et al. [16] propose a method where a relevance model built on a small benchmark set is used to separate relevant and irrelevant samples at each client, and only the relevant samples are used in the federated learning process.

为应对数据的统计异质性和非iid分布所带来的挑战，需要对全局模型进行个性化处理。

在第一步中，以协作的方式构建一个全局模型。在第二步中，使用客户机的私有数据为每个客户机定制全局模型。

(1)开发改进的个性化模型，使绝大多数客户受益;(2)开发准确的全球模型，使私人数据有限的客户受益，实现个性化;(3)在少量的训练回合中获得快速的模型收敛。

3 Techniques

This section surveys different methods for adapting global models for individual clients.

3.1 Adding User Context

Before presenting methods to personalize a global model for individual clients, we take a moment to point out that a shared global model can also generate highly personalized predictions if the client's context and personal information is suitably featurized and incorporated in the dataset. However, most public datasets do not contain contextual features, and developing techniques to effectively incorporate context remains an important open problem that has great potential to improve the utility of federated learning models [6]. It also remains to be studied if such context featurization can be performed without adversely affecting privacy. As an intermediate approach between a single global model and purely local models, Masour et al. [17] suggest *user clustering* where similar clients are grouped together and a separate model is trained for each group.

如果客户的上下文和个人信息被适当地特征化并合并到数据集中，共享的全局模型也可以生成高度个性化的预测。

建议用户聚类，将相似的客户分组在一起，并为每个组训练一个单独的模型。

3.2 Transfer Learning

Transfer learning [18] enables deep learning models to utilize the knowledge gained in solving one problem to solve another related problem. Schneider and Vlachos [19] discuss using transfer learning to achieve model personalization in non-federated settings. Transfer learning has also been used in federated settings, e.g. Wang et al. [20], where some or all parameters of a trained global model are re-learned on local data. A learning-theoretic framework with generalization guarantees is provided in [17]. By using the parameters of the trained global model to initialize training on local data, transfer learning is able to take advantage of the knowledge extracted by the global model instead of learning it from scratch. To avoid the problem of catastrophic forgetting [21] [22], care must be taken to not retrain the model for too long on local data. A variant technique freezes the base layers of the global model and retrains only the top layers on local data. Transfer learning is also known as fine-tuning, and it integrates well into the typical federated learning lifecycle.

不要对本地数据进行过长时间的训练

迁移学习也被称为微调

3.3 Multi-task Learning

In multi-task learning [23], multiple related tasks are solved simultaneously allowing the model to exploit commonalities and differences across the tasks by learning them jointly. Smith et al. [24] show that multi-task learning is a natural choice to build personalized federated models and develop the MOCHA algorithm for multi-task learning in the federated setting that tackles challenges related to communication, stragglers, and fault tolerance. One drawback of using multi-task learning in federated settings is that since it produces one model per task, it is essential that all clients participate in every round.

联邦设置中使用多任务学习的一个缺点是，因为它为每个任务生成一个模型，所以必须让所有客户机参与每一轮。

3.4 Meta-Learning

Meta-learning involves training on multiple learning tasks to generate highly-adaptable models that can further learn to solve new tasks with only a small number of training examples. Finn et al. [25] propose a model-agnostic meta-learning (MAML) algorithm that is compatible with any model that is trained using gradient descent. MAML builds an internal representation generally suitable for multiple tasks, so that fine tuning the top layers for a new task can produce good results. MAML proceeds in two connected stages: meta-training and meta-testing. Meta-training builds the global model on multiple tasks, and meta-testing adapts the global model individually for separate tasks.

元学习是对多个学习任务进行训练，生成适应性强的模型，仅通过少量的训练实例就能进一步学习解决新任务。

Jiang et al. [15] point out that if we consider the federated learning process as meta-training and the personalization process as meta-testing, then Federated Averaging [3] is very similar to Reptile [26], a popular MAML algorithm. The authors also make the observation that careful fine-tuning can produce a global model with high accuracy that can be easily personalized, but naively optimizing for global accuracy can hurt the model's ability for subsequent personalization. While other personalization approaches for federated learning treat development of the global model and its personalization as two distinct activities, Jiang et al. [15] propose a modification to the Federated Averaging algorithm that al-

lows both to be addressed simultaneously resulting in better personalized models.

A new formulation of the standard federated learning problem proposed by Fallah et al. [27] incorporates MAML and seeks to find a global model which performs well *after* each user updates it with respect to its own loss function. In addition, they propose Per-FedAvg, a personalized variant of Federated Averaging, to solve the above-mentioned formulation. Khodak et al. [28] propose ARUBA, a meta-learning algorithm inspired by online convex optimization, and demonstrate an improvement in performance by applying it to Federated Averaging. Chen et al. [29] present a federated meta-learning framework for building personalized recommendation models where both the algorithm and the model are parameterized and need to be optimized.

3.5 Knowledge Distillation

Caruana et al. [23] have demonstrated that it is possible to compress the knowledge of an ensemble of models into a single model which is easier to deploy. Knowledge distillation [30] further develops this idea and involves extracting the knowledge of a large *teacher* network into a smaller *student* network by having the student mimic the teacher. Overfitting poses a significant challenge during personalization, especially for clients whose local dataset is small. Yu et al. [7] propose that by treating the global federated model as the teacher and the personalized model as the student, the effects of overfitting during personalization can be mitigated. Li et al. [31] propose FedMD, a federated learning framework based on knowledge distillation and transfer learning that allows clients to independently design their own networks using their local private datasets and a global public dataset.

3.6 Base + Personalization Layers

In typical federated learning scenarios, data distribution varies greatly across participating devices. To temper the adverse effects of this statistical heterogeneity, Arivazhagan et al. [32] propose FedPer, a neural network architecture where the base layers are trained centrally by Federated Averaging, and the top layers (also called personalization layers) are trained locally with a variant of gradient descent. As opposed to transfer learning where all the layers are first trained on global data and then all or some layers are retrained on local data, FedPer separately trains the base layers on global data and the personalization layers on local data.

3.7 Mixture of Global and Local Models

The standard formulation of federated learning [3] is designed to find a single global model trained on private data across all clients. Hanzely et al. [8] propose a different formulation of the problem that seeks an explicit trade-off between the global model and the local models. Instead of learning a single global model, each device learns a mixture of the global model and its own local model. To solve the formulation, the authors develop a new variant of gradient descent called Loopless Local Gradient Descent (LLGD). Instead of performing full averaging, LLGD only takes steps towards averaging thus suggesting that full averaging methods such as Federated Averaging might be too aggressive.

4 Discussion

Federated learning encompasses a wide variety of settings, devices, and datasets. When local datasets are small and the data distribution is IID, global models typically outperform local models, and a majority of clients benefit from participating in the federated learning process. However, when clients have sufficiently large private datasets and the data distribution is non-IID, local models exhibit better performance than the shared global model, and clients have no incentive to participate in the federated learning process. An open theoretical question is to determine the conditions under which shared global models can perform better than individual local models.

This paper surveys personalization techniques used to adapt a global federated model to individual clients. With a few exceptions, most prior work is focussed on measuring the performance of the global model on aggregated data instead of measuring its performance as seen by individual clients. Global performance, however, has no relevance if the global model is expected to be subsequently personalized before being put to use.

Personalized models usually show better performance for individual clients than global or local models. In some cases, however, personalized models fail to reach the same performance as local models, especially when differential privacy and robust aggregation is implemented [7].

References

[1] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.

[2] G. J. Annas *et al.*, "Hipaa regulations-a new era of medical-record privacy?," *New England Journal of Medicine*, vol. 348, no. 15, pp. 1486–1490, 2003.

[3] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, *et al.*, "Communication-efficient learning of deep networks from decentralized data," *arXiv preprint arXiv:1602.05629*, 2016.

[4] A. Hard, K. Rao, R. Mathews, S. Ramaswamy, F. Beaufays, S. Augenstein, H. Eichner, C. Kiddon, and D. Ramage, "Federated learning for mobile keyboard prediction," *arXiv preprint arXiv:1811.03604*, 2018.

[5] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konecny, S. Mazzocchi, H. B. McMahan, *et al.*, "Towards federated learning at scale: System design," *arXiv preprint arXiv:1902.01046*, 2019.

[6] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings, *et al.*, "Advances and open problems in federated learning," *arXiv preprint arXiv:1912.04977*, 2019.

[7] T. Yu, E. Bagdasaryan, and V. Shmatikov, "Salvaging federated learning by local adaptation," *arXiv preprint arXiv:2002.04758*, 2020.

[8] F. Hanzely and P. Richtárik, "Federated learning of a mixture of global and local models," *arXiv preprint arXiv:2002.05516*, 2020.

[9] Q. Wu, K. He, and X. Chen, "Personalized federated learning for intelligent iot applications: A cloud-edge based framework," *arXiv preprint arXiv:2002.10671*, 2020.

[10] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 3–18, IEEE, 2017.

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

[12] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang, "Learning differentially private recurrent language models," *arXiv preprint arXiv:1710.06963*, 2017.

[13] E. Bagdasaryan, O. Poursaeed, and V. Shmatikov, "Differential privacy has disparate impact on model accuracy," in *Advances in Neural Information Processing Systems*, pp. 15453–15462, 2019.

[14] K. C. Sim, P. Zadrazil, and F. Beaufays, "An investigation into on-device personalization of end-to-end automatic speech recognition models," *arXiv preprint arXiv:1909.06678*, 2019.

[15] Y. Jiang, J. Konecny, K. Rush, and S. Kannan, "Improving federated learning personalization via model agnostic meta learning," *arXiv preprint arXiv:1909.12488*, 2019.

[16] T. Tuor, S. Wang, B. J. Ko, C. Liu, and K. K. Leung, "Data selection for federated learning with relevant and irrelevant data at clients," *arXiv preprint arXiv:2001.08300*, 2020.

[17] Y. Mansour, M. Mohri, J. Ro, and A. T. Suresh, "Three approaches for personalization with applications to federated learning," *arXiv preprint arXiv:2002.10619*, 2020.

[18] L. Y. Pratt, "Discriminability-based transfer between neural networks," in *Advances in neural information processing systems*, pp. 204–211, 1993.

[19] J. Schneider and M. Vlachos, "Mass personalization of deep learning," *arXiv preprint arXiv:1909.02803*, 2019.

[20] K. Wang, R. Mathews, C. Kiddon, H. Eichner, F. Beaufays, and D. Ramage, "Federated evaluation of on-device personalization," *arXiv preprint arXiv:1910.10252*, 2019.

[21] M. McCloskey and N. J. Cohen, "Catastrophic interference in connectionist networks: The sequential learning problem," in *Psychology of learning and motivation*, vol. 24, pp. 109–165, Elsevier, 1989.

[22] R. M. French, "Catastrophic forgetting in connectionist networks," *Trends in cognitive sciences*, vol. 3, no. 4, pp. 128–135, 1999.

[23] R. Caruana, "Multitask learning," *Machine learning*, vol. 28, no. 1, pp. 41–75, 1997.

[24] V. Smith, C.-K. Chiang, M. Sanjabi, and A. S. Talwalkar, "Federated multi-task learning," in *Advances in Neural Information Processing Systems*, pp. 4424–4434, 2017.

[25] C. Finn, P. Abbeel, and S. Levine, "Model-agnostic meta-learning for fast adaptation of deep networks," in *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pp. 1126–1135, JMLR. org, 2017.

[26] A. Nichol, J. Achiam, and J. Schulman, "On first-order meta-learning algorithms," *arXiv preprint arXiv:1803.02999*, 2018.

[27] A. Fallah, A. Mokhtari, and A. Ozdaglar, "Personalized federated learning: A meta-learning approach," *arXiv preprint arXiv:2002.07948*, 2020.

[28] M. Khodak, M.-F. F. Balcan, and A. S. Talwalkar, "Adaptive gradient-based meta-learning methods," in *Advances in Neural Information Processing Systems*, pp. 5915–5926, 2019.

[29] F. Chen, Z. Dong, Z. Li, and X. He, "Federated meta-learning for recommendation," *arXiv preprint arXiv:1802.07876*, 2018.

[30] G. Hinton, O. Vinyals, and J. Dean, "Distilling the knowledge in a neural network," *arXiv preprint arXiv:1503.02531*, 2015.

[31] D. Li and J. Wang, "Fedmd: Heterogenous federated learning via model distillation," *arXiv preprint arXiv:1910.03581*, 2019.

[32] M. G. Arivazhagan, V. Aggarwal, A. K. Singh, and S. Choudhary, "Federated learning with personalization layers," *arXiv preprint arXiv:1912.00818*, 2019.