

Enabling Weak Client Participation via On-Device Knowledge Distillation in Heterogeneous Federated Learning

Jihyun Lim^a, Junhyuk Jo^a, Tuo Zhang^b and Sunwoo Lee^{a,*}

^aInha University, South Korea

^bUniversity of Southern California, United States

Abstract. Online Knowledge Distillation (KD) is recently highlighted to train large models in Federated Learning (FL) environments. Many existing studies adopt the logit ensemble method to perform KD on the server side. However, they often assume that unlabeled data collected at the edge is centralized on the server. Moreover, the logit ensemble method personalizes local models, which can degrade the quality of soft targets, especially when data is highly non-IID. To address these critical limitations, we propose a novel on-device KD-based heterogeneous FL method. Our approach leverages a small auxiliary model to learn from labeled local data. Subsequently, a subset of clients with strong system resources transfers knowledge to a large model through on-device KD using their unlabeled data. Our extensive experiments demonstrate that our on-device KD-based heterogeneous FL method effectively utilizes the system resources of all edge devices as well as the unlabeled data, resulting in higher accuracy compared to SOTA KD-based FL methods.

1 Introduction

Federated Learning (FL) [26] is a practical learning method to utilize the data collected on-the-fly at the edge. With recent advances in the system efficiency of edge devices, various large-scale on-device learning scenarios are being considered, such as multi-task transfer learning [6], sharpness-aware minimization [11], and even Large Language Model (LLM) fine-tuning [34]. These studies generally assume homogeneous devices, where all participants can contribute equally to model training. However, FL environments often consist of heterogeneous edge devices, such as mobile phones and IoT devices, which continuously gather new, unlabeled local data [29, 5] that could be used for training. Therefore, to exploit the ever-increasing big data collected at the edge, it is imperative to develop a new FL method that can fully utilize heterogeneous system resources.

Several recent studies tackle the system heterogeneity issue in FL by employing partial model training scheme [9, 15, 20, 19, 21, 33]. However, they enforce clients with weak resources to train only a subset of the target model’s layers or channels, significantly harming the freedom of model design. More recent works utilize Knowledge Distillation (KD) [14]. They commonly use a logit ensemble method instead of directly aggregating the local models to reduce the KD’s

communication cost in FL environments [17, 16]. In our empirical study, however, we find that the logit ensemble fails to provide sufficiently accurate soft targets when the data distribution is highly non-IID. Although a large amount of public data is available, KD with such inaccurate soft targets negatively impacts the efficiency of knowledge transfer. Some others utilize unlabeled extra data to train the target model on the server side [24, 8]. This approach assumes that unlabeled data generated on edge devices is aggregated on the server and utilized for centralized training, raising privacy concerns.

In this paper, we propose a novel heterogeneous FL method that utilizes unlabeled data at the edge to overcome the limitations of logit ensemble methods and server-side model training approaches. Specifically, we introduce a KD-based FL method that jointly utilizes additional system resources on strong devices and unlabeled local data by combining auxiliary model training and on-device KD. The core principle behind our method is that a small auxiliary model first learns global knowledge through standard model aggregation and then helps the training of the large target model by utilizing system resources and unlabeled local data on strong devices. When transferring global knowledge from the auxiliary model to the target model, only a subset of clients with sufficiently strong system resources participate in the KD process. This heterogeneous approach allows all clients to effectively join the training, exploiting their own resources and local data.

Compared to logit ensemble-based KD, our method has two strong benefits as follows. First, our approach ensures accurate soft targets for the KD process. By aggregating the small auxiliary models across clients, the local knowledge is merged into a single point, thereby significantly improving the quality of the soft targets compared to the logit ensemble. Second, our approach does not require the server to have sufficiently strong system capability nor the unlabeled data to be centralized on the server in advance. By offloading the KD workload to the strong devices, the model can learn from the local data regardless of whether it is labeled or not. Moreover, as more clients join the training, our approach allows the model to learn from more unlabeled data, likely improving the model accuracy.

We evaluate the performance of our proposed method across various machine learning benchmarks: CIFAR-10 [18], CIFAR-100 (fine-tuning), FEMNIST [3], IMDB reviews [28], and Google Speech Commands [30]. Our extensive experiments demonstrate that the proposed method outperforms SOTA KD-based FL methods under highly non-IID conditions. We also theoretically analyze the gen-

* Corresponding Author. Email: sunwool@inha.ac.kr

eralization bound for the proposed method. The contributions of our work are summarized below.

- We explain and empirically prove the fundamental limitations of the logit ensemble-based Knowledge Distillation especially when data is strongly non-IID.
- Our study demonstrates how to harmonize online Knowledge Distillation with FL to better utilize unlabeled data collected at the edge on-the-fly.
- We discuss how to exploit heterogeneous system resources in realistic FL environments via selectively offloading the distillation workload to the edge.
- Our study presents an extensive comparative analysis, demonstrating that the proposed method achieves superior soft target quality, resulting in higher accuracy.

2 Related Works

2.1 Heterogeneous Federated Learning

In realistic FL environments, some devices may not efficiently train large models or even cannot put them in their memory space. In this case, there are two options: employ a small model giving up the learning capability or keep using the large model giving up the private data owned by the weak devices. One promising solution to this system heterogeneity issue is partial model training method [9, 15, 20, 19, 21, 33, 1]. While these methods alleviate the workload for some clients, they do not consider independent model architectures across clients.

Another promising approach is heterogeneous model approximation method. Some recent works allow clients to reduce the model size according to their system capability [31, 25, 4, 27]. However, the low-rank model approximation causes a non-negligible extra computational cost. Additionally, the local models cannot be directly aggregated because each one may be approximated to a different rank.

2.2 Knowledge Distillation in Federated Learning

Table 1 summarizes the recently proposed KD-based FL methods. First, there are two homogeneous FL methods: FedAvg and MOON [23]. Neither of them considers the newly collected unlabeled data or utilizes KD.

Logit Ensemble – KD has been widely used in recent FL studies with a goal of either improving the model accuracy or training a large model. Federated KD proposed in [17] directly exchanges the soft targets across the server and the clients instead of exchanging the model parameters. DS-FL proposed in [16] exchanges only the soft targets under a strong assumption that the unlabeled data is available for all individual clients. FedMD [22] transfers knowledge by leveraging the fine-tuning mechanism. These methods commonly aggregate the local models’ output logits at the server and broadcast them to the clients. This approach significantly reduces the communication cost; however, the accuracy drop is significant.

Logit Ensemble with Server-Side Distillation – FedDF [24] trains the target model at the server-side using the logit ensemble method. This approach is under an assumption that a large amount of unlabeled data is already available at the server side. It also assumes the server has sufficient system resources to directly run KD. FedFTG [32] also uses the server-side KD together with a feature generator. This study does not consider the system heterogeneity nor the additional unlabeled data.

Logit Ensemble, Server-Side Distillation, and Heterogeneous

Method	Server Model	Exchange	Additional Data / Labeled	KD
FedAvg	=client	model	No / N/A	N/A
MOON	=client	model	No / N/A	N/A
FD	N/A	logits	No / N/A	device
DS-FL	N/A	logits	Yes / No	device
FedMD	N/A	logits	Yes / Yes	device
FedDF	=client	model	Yes / No	server
FedGEMS	> client	logits	Yes / Yes	both
FedGKT	> client	model+logits	No / N/A	both
Fed-ET	> client	model+logits	Yes / No	server
Ours	N/A	model	Yes / No	device

Table 1: The configurations of SOTA FL methods.

Models – FedGKT [12] allows the server to have its own classifier layers and train them using KD. This approach achieves promising model accuracy, however, it does not take into account locally generated unlabeled data. FedGEMS [7] also runs KD to train a large model at the server-side. Like FedMD, this method also assumes the public data to be labeled. More recently, Fed-ET [8] has been proposed, which utilizes model transfer as well as weighted ensemble at the server-side. However, this approach also performs KD on the server side, and the server-side model cannot directly learn from the clients’ private data.

3 Method

We begin with an ablation study to demonstrate how logit ensemble can harm KD performance in general FL environments. Based on this analysis, we develop our novel on-device KD-based FL method, which maximizes KD performance by fully utilizing the system resources of heterogeneous devices. Finally, we analyze the expected generalization bound for the proposed method and discuss how unlabeled local data impacts its performance.

3.1 Limitations of Logit Ensemble in Federated Learning Environments

Many existing works employ the logit ensemble method to implement communication-efficient online KD in FL environments [17, 16, 24, 8]. However, our empirical study finds that it can significantly hurt the model accuracy. Our research is strongly motivated by this ablation study result.

We compare the accuracy of logit ensemble and that of the conventional model aggregation. We use CIFAR-10 and Google Speech Command, which are computer vision and audio recognition benchmarks. First, the dataset is partitioned into two distinct subsets: one for training and the other for evaluating model accuracy. We further divide the training data into 100 small subsets using a label-based Dirichlet distribution ($\alpha = 0.1$) and assign one small subset to each client. Next, we conduct logit ensemble-based FL and model aggregation-based FL, and compare the accuracies they achieve. Note that the logit ensemble uses the full model, while the model aggregation uses a smaller model, with each layer containing 25% of the channels. This setting penalizes the model aggregation scheme in terms of the model’s learning capability, and we expect to see the adverse impact of the logit ensemble more clearly under this setting.

In Figure 1, the left bubble chart shows the class-wise data distribution per client, while the right side of the figure shows the learning curve comparisons. The bubble charts illustrate how non-IID the datasets are. Most clients have data from only a few classes, indicating highly non-IID conditions. Each learning curve chart shows the

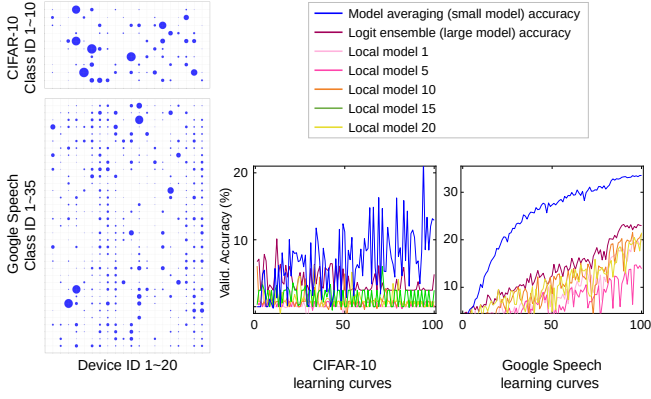


Figure 1: Non-IID distributions of CIFAR-10 (left-top) and Google Speech (left-bottom). Label-based Dirichlet distributions ($\alpha = 0.1$) are used to get 100 local distributions. Due to the limited space, we only show 20 of them. The accuracy of a small model trained via FL provides remarkably more accurate logits than the logit ensemble.

accuracies of five local models as well as the global model’s accuracy. The purple curve corresponds to the global model trained with the logit ensemble method, while the blue curve corresponds to the global model trained with conventional model aggregation. The gap between the global curve and the local curves quantifies the impact of each FL method.

When data is highly non-IID, the logit ensemble accuracy of the full model (purple curves) is considerably lower than the model aggregation accuracy of the small (25%) model (blue curves). *The logit ensemble forces all local models to be personalized without synchronizing model parameters.* Such personalized models lead to a significant degradation in the soft target quality in terms of generalization. Some previous works assume that labeled public data is available at the edge as a way to address this issue; however, having a large amount of labeled public data is unrealistic [22, 7]. In addition, new unlabeled data is most likely generated at the edge, and centralizing them to the server may pose privacy concerns. For these reasons, the logit ensemble is not an appropriate option for heterogeneous FL. Motivated by this analysis, we propose a novel on-device KD-based FL method that addresses the low-quality soft target issue.

3.2 On-Device Federated Transfer Learning

We first define two types of models: $\mathbf{w}_l$ and $\mathbf{w}_s$.

- $\mathbf{w}_l$: The large target model.
- $\mathbf{w}_s$: A smaller auxiliary model.

We also define two relative categories of clients: *strong* and *weak* clients. A client is considered *strong* if it has sufficient system resources to train the large target model $\mathbf{w}_l$. On the other hand, a client is considered *weak* if it cannot independently train the large target model $\mathbf{w}_l$. This limitation may be due to various system constraints, such as insufficient memory or too slow computational resources. We do not specify the exact reason in order to keep the definition of this type general.

Now, we focus on federated optimization, which trains the target model $\mathbf{w}_l$. Considering the natural data collection at the edge, we assume that each edge device has a certain amount of unlabeled private data. This is a valid problem formulation because it is more reasonable for new data to be generated at the edge rather than the parameter server. Our method employs KD with these unlabeled local data to improve the target model accuracy. We take advantage of

an auxiliary model $\mathbf{w}_s$, which fits within the memory capacity of all individual devices.

Given the two models, our method repeats the following two steps until a user-defined termination condition is satisfied (e.g., target accuracy or time budget). Figure 2 provides a schematic illustration of these two steps.

Step 1: Auxiliary Model Training Round – First, a random subset of clients is activated in each round. The activated devices receive $\mathbf{w}_s$ from the server and run τ local updates using their own labeled data. The resulting locally trained models, $\mathbf{w}_s^i$ for $i \in A$, are aggregated at the server using simple uniform averaging, where A is the set of active clients. This global FL round with the small auxiliary model enables the collection of local knowledge from all clients, regardless of their system capacity. The loss function in step 1 is as follows.

$$\mathcal{L}_s(\mathbf{w}_s) = \frac{1}{n} \sum_{i=1}^n \text{CE}(\mathbf{w}_s, x), \forall x \in \hat{\mathcal{D}}^i, \quad (1)$$

where $\mathbf{w}_s$ is the auxiliary model, n is the total number of clients, $\text{CE}(\cdot, \cdot)$ is the cross entropy function, and $\hat{\mathcal{D}}^i$ is the local data owned by client i .

Step 2: Target Model Training Round – Once the auxiliary models are aggregated at the server, the strong clients train the target model $\mathbf{w}_l$ using the auxiliary model. First, the strong clients receive both models, $\mathbf{w}_s$ and $\mathbf{w}_l$ from the server. Then, they locally update the target model $\mathbf{w}_l$ for τ steps using their own labeled data. After the local updates, they run additional τ local KD steps using the unlabeled private data. The auxiliary model participates in the KD process as a teacher. Finally, the local target models $\mathbf{w}_l^j, \forall j \in S$ are aggregated at the server, where S is the set of strong clients.

In step 2, all individual strong clients train the target model $\mathbf{w}_l^j$ using the following loss functions.

$$\begin{aligned} \mathcal{L}_l(\mathbf{w}_l) = & \frac{1}{s} \sum_{j=1}^s \text{CE}(\mathbf{w}_l, x), \forall x \in \hat{\mathcal{D}}^j \\ & + \frac{1}{s} \sum_{j=1}^s \lambda \cdot \text{KL}(\mathbf{w}_s, \mathbf{w}_l, x'), \forall x' \in \mathcal{D}^j, \end{aligned} \quad (2)$$

where $\mathbf{w}_l$ is the target model, s is the number of strong clients, $\text{KL}(\cdot, \cdot, \cdot)$ is the Kullback–Leibler divergence function, and the λ is a hyper-parameter that determines how strongly the $\text{KL}(\cdot, \cdot, \cdot)$ affects the total loss. Note that the first term on the right-hand side uses the local labeled data $x \in \hat{\mathcal{D}}^j$ while the second term uses the local unlabeled data $x' \in \mathcal{D}^j$.

3.3 Discussion on Design Choices of On-Device Knowledge Distillation

The Role of Auxiliary Model – The core principle of our heterogeneous FL method is to use a small auxiliary model trained with a conventional model aggregation scheme. This design choice ensures local data privacy, as the auxiliary model is trained locally, and only its parameters are aggregated. In contrast, logit ensemble assumes that clients can access the same unlabeled data (also known as public data), enabling logits from different local models to be computed using the same input data. Our method does not depend on this strong assumption and allows each client to fully utilize their local data, whether labeled or unlabeled.

In addition, the logit ensemble allows local models to remain personalized, as model parameters are not directly averaged across clients. If data is highly non-IID – for example, if each client has

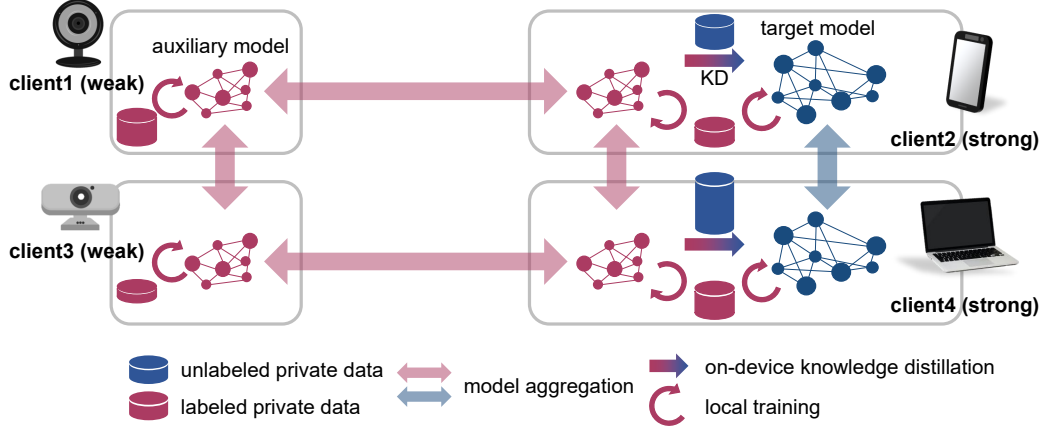


Figure 2: The schematic illustration of the proposed heterogeneous FL method. For simplicity, the server is omitted in this schematic. An auxiliary (small) model is trained by all the devices using their private data. Then, the global knowledge is transferred to the target (large) model through on-device KD. This distributed knowledge transfer approach enables to not only fully utilize heterogeneous edge devices’ system resources but also effectively use the unlabeled private data for training.

local data limited to one or two classes – these personalized models are likely to suffer from poor generalization performance. Our ablation study results are shown in Figure 1. Thus, we can conclude that aggregating local logits alone is insufficient to provide accurate soft targets for KD.

Comparison to Server-side Knowledge Distillation – Our on-device KD method has three advantages over conventional server-side distillation. First, it enables the target model to utilize both labeled and unlabeled data on the clients. This is a critical benefit in terms of scalability, as the target model can learn from more unlabeled data as the number of strong clients grows. In other words, our method is better suited for on-device learning, where new data is continuously generated at the edge. Second, our method takes advantage of system heterogeneity, allowing clients with stronger system resources to run more training and distillation steps than others. This approach naturally maximizes system utilization at the edge. Finally, our method enables each client to locally utilize new data collected at runtime without sharing it with others. Some logit ensemble-based KD methods [24, 8, 7] assume that ‘public data’ are accessible at both clients and server. Such an assumption is overly strong and unrealistic, as it may pose privacy issues.

Communication Cost Analysis – We compare the communication cost of our method with that of representative logit ensemble-based KD methods. Table 2 presents the results of the comparative study conducted on CIFAR-10 (ResNet20). FedDF employs server-side KD, whereas DS-FL adopts client-side KD. To ensure a fair comparison, we align the total number of rounds, regardless of whether they involve training or KD.

For the homogeneous FL methods (FedAvg and FedDF), we consider two cases: one case involves training the small model w_s (with 25% of the channels at every layer) on all clients, while the other case trains the large model w_l only on a subset of clients with sufficiently strong system resources. First, FedAvg (small) has a lower communication cost than FedAvg (large), but suffers from significantly lower accuracy. Interestingly, the accuracy of FedDF is lower than that of FedAvg, regardless of the model size. This result indicates that the soft targets generated by the logit ensemble are of insufficient quality to make meaningful progress in KD. FedDF can leverage KD without incurring extra communication cost. However, it runs KD on the server-side with inaccurate soft targets, which could ultimately harm model accuracy. DS-FL, the client-side KD-based FL method,

Method	Comm. Cost	Message Size	Acc (%)
FedAvg(small)	$ w_s $	19K	$57.47 \pm 0.8\%$
FedAvg(large)	$ w_l $	274K	$59.21 \pm 1.5\%$
FedDF(small)	$ w_s $	19K	$41.62 \pm 0.1\%$
FedDF(large)	$ w_l $	274K	$58.94 \pm 0.1\%$
DS-FL	C	10	$25.95 \pm 0.1\%$
On-Device KD	$ w_s + w_l $	19K + 274K	$62.43 \pm 0.1\%$

Table 2: The communication cost comparison across different FL methods. C is the number of classes. w_l is ResNet20 while w_s is a modified one which has only 25% channels at every layer.

adopts the logit ensemble and entirely avoids the model aggregation cost. Thus, the communication cost is only the number of classes C , but the model accuracy is significantly reduced.

The communication cost of our method is slightly higher than that of FedAvg(large) due to the extra communication for the auxiliary model training. However, the accuracy improves remarkably, even surpassing that of FedAvg (large). This analysis demonstrates that our method strikes a practical trade-off between communication cost and model accuracy.

Computational Cost Analysis – We also compare the computational cost of our method to that of the same logit ensemble-based KD methods discussed in Table 2. Since FedDF and FedAvg are homogeneous FL methods that consider only a single type of model, a fair comparison of their computational costs with that of our method is not possible. Therefore, we focus on the training cost of w_l only. Our method has the same computational cost as FedAvg (large) and FedDF (large), while achieving significantly higher accuracy. DS-FL is a heterogeneous FL method and its computational cost is directly comparable to our method. However, its accuracy is significantly lower than all the other methods due to the ineffective knowledge transfer through logit ensemble. This computational cost comparison suggests that our auxiliary model improves the target model’s accuracy without significantly increasing the total computational cost.

3.4 Discussion on Impact of On-Device Knowledge Distillation on Generalization Performance

Here, we theoretically analyze the benefit of our design choices in terms of the target model’s generalization bound. Our analysis builds upon that of [8], extending it to account for the combination of labeled and unlabeled local data.

Problem Definition – We first define hypothesis $h : \mathcal{X} \rightarrow \mathcal{Y}$, with input space $\mathbf{x} \in \mathcal{X}$ and label space $y \in \mathcal{Y}$, and the hypothesis space $h \in \mathcal{H}$. The general loss function $l(h(\mathbf{x}), y)$ quantifies the classification error of the given hypothesis. The true global data distribution is defined as $\mathcal{D}$. Then, the true local data distribution from each client’s perspective is defined as $\mathcal{D}_i, i \in [n]$. The data distribution of the limited number of local observations is defined as $\hat{\mathcal{D}}_i$. We also define the expected loss over an arbitrary data distribution $\mathcal{D}'$ as $\mathcal{L}_{\mathcal{D}'}(h) = \mathbb{E}_{\mathbf{x}, y \sim \mathcal{D}'} [l(h(\mathbf{x}), y)], \forall h \in \mathcal{H}$. Finally, we assume that $\mathcal{L}(h)$ is convex. In these settings, the generalization bound of the target model trained by our proposed method satisfies the following condition.

Now, to make our analysis self-contained, we state the two lemmas proposed in the previous work, which will be used to analyze the generalization of our proposed method.

Lemma 1 (Domain Adaptation [2]) *With two true distributions $\mathcal{D}_1$ and $\mathcal{D}_2, \forall p \in (0, 1)$ and hypothesis $\forall h \in \mathcal{H}$, with probability at least $1 - p$ over the choice of samples, it satisfies*

$$\mathcal{L}_{\mathcal{D}_1}(h) \leq \mathcal{L}_{\mathcal{D}_2}(h) + \frac{1}{2}d(\mathcal{D}_1, \mathcal{D}_2) + v_1, \quad (3)$$

where $d(\mathcal{D}_1, \mathcal{D}_2)$ quantifies the distribution discrepancy between the two data distributions, $\mathcal{D}_1$ and $\mathcal{D}_2$, v_1 is the minimal loss such that $v_1 = \inf_h \mathcal{L}_{\mathcal{D}_1}(h) + \mathcal{L}_{\mathcal{D}_2}(h)$.

Lemma 2 (Generalization with limited training samples) [8]. *For all individual client i , with probability at least $1 - p$ over the choice of samples, there exists:*

$$\mathcal{L}_{\mathcal{D}_i}(h_{\hat{\mathcal{D}}_i}) \leq \mathcal{L}_{\hat{\mathcal{D}}_i}(h_{\hat{\mathcal{D}}_i}) + \sqrt{\frac{\log 2/p}{2|\hat{\mathcal{D}}_i|}}, \quad (4)$$

where $|\hat{\mathcal{D}}_i|$ is the size of client i ’s local dataset.

The first lemma measures the generalization bound for one data distribution based on the maximum discrepancy between the given two distributions. The second lemma elaborates the bound taking the limited training samples into account based on Hoeffding’s inequality. Our proposed method trains the target model $\mathbf{x}_l$ using $s < n$ strong clients only. Thus, we will analyze the generalization bound with respect only to the strong clients’ labeled data using the above two lemmas. Then, we will revise this bound concerning the on-device knowledge distillation with unlabeled local data.

Proposition 1 *Consider n clients in total and s of them are strong clients. Each client has its own data distribution $\mathcal{D}_i, \forall i \in [n]$. We define a combination of the labeled local data and the unlabeled local data as $\tilde{\mathcal{D}}_i$. For an arbitrary data distribution $\mathcal{D}'$, $h_{\mathcal{D}'}$ is the model best-trained on $\mathcal{D}'$. Then, with probability of $1 - p$, our proposed on-device knowledge distillation-based FL guarantees the following generalization bound for the target model.*

$$\begin{aligned} \mathcal{L}_{\mathcal{D}} \left(\frac{1}{s} \sum_{i=1}^s h_{\hat{\mathcal{D}}_i} \right) &\leq \frac{1}{s} \sum_{i=1}^s \left(\mathcal{L}_{\tilde{\mathcal{D}}_i}(h_{\tilde{\mathcal{D}}_i}) + \sqrt{\frac{\log 2/p}{2|\tilde{\mathcal{D}}_i|}} \right) \\ &\quad + \frac{1}{2s} \sum_{i=1}^s d(\mathcal{D}_i, \mathcal{D}) + \frac{1}{s} \sum_{i=1}^s v_i. \end{aligned}$$

Proof. First, let us bound the loss over the true global data distribution $\mathcal{L}_{\mathcal{D}}(\frac{1}{s} \sum_{i=1}^s h_{\hat{\mathcal{D}}_i})$ based on lemma 1. Note that the hypothesis

Dataset	Auxiliary Model (<i>weak</i>) (relative model size)	Target Model (<i>strong</i>)
CIFAR-10	ResNet20 {25%, 50%, 75%}	ResNet20 100%
FEMNIST	CNN {25%, 50%, 75%}	CNN 100%
CIFAR-100 (Fine-tuning)	ResNet50 ~ 29%	ViT-b16 100%
IMDB	Bi-LSTM 25%	Bi-LSTM 100%
Google Speech	CNN {25%, 50%, 75%}	CNN 100%

Table 3: The model configurations for all five benchmarks. i is the model averaged only across s strong clients.

$$\begin{aligned} \mathcal{L}_{\mathcal{D}} \left(\frac{1}{s} \sum_{i=1}^s h_{\hat{\mathcal{D}}_i} \right) &\leq \frac{1}{s} \sum_{i=1}^s \mathcal{L}_{\mathcal{D}}(h_{\hat{\mathcal{D}}_i}) \\ &\leq \frac{1}{s} \sum_{i=1}^s \left(\mathcal{L}_{\mathcal{D}_i}(h_{\hat{\mathcal{D}}_i}) + \frac{1}{2}d(\mathcal{D}_i, \mathcal{D}) + v_i \right). \end{aligned} \quad (5)$$

Then, (5) can be further bounded using lemma 2 as follows.

$$\begin{aligned} \mathcal{L}_{\mathcal{D}} \left(\frac{1}{s} \sum_{i=1}^s h_{\hat{\mathcal{D}}_i} \right) &\leq \frac{1}{s} \sum_{i=1}^s \left(\mathcal{L}_{\hat{\mathcal{D}}_i}(h_{\hat{\mathcal{D}}_i}) + \sqrt{\frac{\log 2/p}{2|\hat{\mathcal{D}}_i|}} \right) \\ &\quad + \frac{1}{2s} \sum_{i=1}^s d(\mathcal{D}_i, \mathcal{D}) + \frac{1}{s} \sum_{i=1}^s v_i. \end{aligned}$$

Finally, the on-device knowledge distillation utilizes not only the strong clients’ labeled data but also the unlabeled data. Thus, we can simply replace the local dataset $\hat{\mathcal{D}}_i$ with the combination of the labeled and unlabeled data $\tilde{\mathcal{D}}_i$.

$$\begin{aligned} \mathcal{L}_{\mathcal{D}} \left(\frac{1}{s} \sum_{i=1}^s h_{\hat{\mathcal{D}}_i} \right) &\leq \frac{1}{s} \sum_{i=1}^s \left(\mathcal{L}_{\tilde{\mathcal{D}}_i}(h_{\tilde{\mathcal{D}}_i}) + \sqrt{\frac{\log 2/p}{2|\tilde{\mathcal{D}}_i|}} \right) \\ &\quad + \frac{1}{2s} \sum_{i=1}^s d(\mathcal{D}_i, \mathcal{D}) + \frac{1}{s} \sum_{i=1}^s v_i. \end{aligned} \quad (6)$$

□

Remark 1. *This result highlights the key advantage of our method: on-device KD reduces the second term on the right-hand side of (6), leading to better generalization. Note that $|\hat{\mathcal{D}}_i| \leq |\tilde{\mathcal{D}}_i|$, where $\hat{\mathcal{D}}_i$ denotes the labeled data and $\tilde{\mathcal{D}}_i$ denotes the union of labeled and unlabeled data. Therefore, by expanding the data distribution, the proposed method can achieve a lower empirical loss.*

Remark 2. *As each client collects more unlabeled data, the size of $\tilde{\mathcal{D}}_i$ may increase and the bound decreases even further. This is a critical benefit in realistic FL environments because the new unlabeled data is most likely collected at the edge rather than the server. Thus, our method can be considered as a more scalable FL method especially when the strong clients can collect data on-the-fly. Note that in the server-side KD, the $\tilde{\mathcal{D}}_i$ can only be the unlabeled data which is still smaller than $\hat{\mathcal{D}}_i$.*

4 Experiments

We conduct performance evaluations in computer vision: CIFAR-10 (ResNet20 [13]), CIFAR-100 (ViT [10]), FEMNIST (CNN), natural language processing: IMDB (Bidirectional LSTM), and audio

Dataset	Batch (LR)	Local Steps	Epochs	# of clients	Weak-only	Strong-only	Proposed
CIFAR-10	32 (0.2)	30	400	100	$57.47 \pm 0.8\%$	$59.21 \pm 1.5\%$	$62.43 \pm 0.1\%$
FEMNIST	20 (0.02)	30	200	100	$64.27 \pm 0.1\%$	$53.75 \pm 0.6\%$	$67.44 \pm 0.1\%$
CIFAR-100 (Fine-tuning)	32 (0.04)	60	40	100	$40.56 \pm 0.1\%$	$52.17 \pm 0.1\%$	$59.73 \pm 0.1\%$
IMDB review	10 (0.4)	20	90	50	$81.46 \pm 0.1\%$	$59.63 \pm 0.1\%$	$82.50 \pm 0.1\%$
Google Speech	32 (0.02)	40	100	100	$66.83 \pm 0.3\%$	$68.83 \pm 0.1\%$	$71.95 \pm 0.5\%$

Table 4: The FL performance comparison: weak model-only, strong model-only and the proposed method.

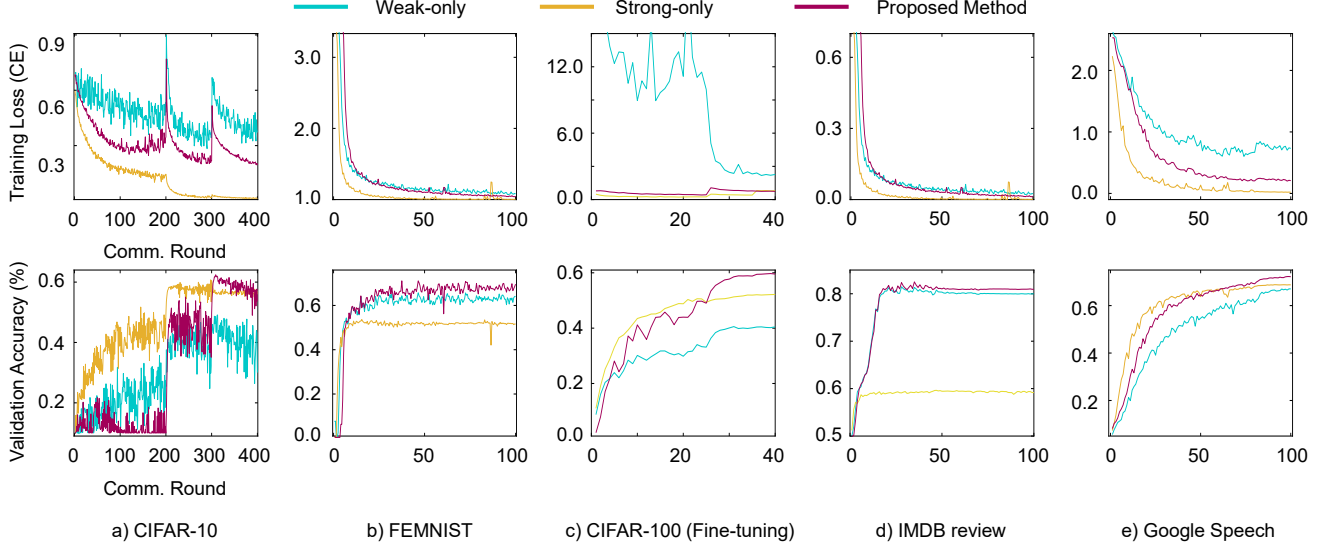


Figure 3: The training loss (top) and validation accuracy (bottom) curves corresponding to Table 4.

recognition: Google Speech Command (CNN) benchmarks. We report accuracy averaged across at least 3 independent runs. For all the methods in our comparative study, the algorithm-specific hyper-parameters were highly tuned using appropriate grid searches. See Appendix for the hyper-parameter settings in detail ¹.

Non-IID Dataset Settings – We use label-based Dirichlet distributions ($\alpha = 0.1$ which represents highly non-IID FL environments). FEMNIST is naturally non-IID, and we use 100 clients’ data as unlabeled local data. Google Speech is also naturally non-IID, but each local dataset is quite large. So, we use an artificial distribution to make it more strongly non-IID. We activate random 20% of the total clients at every round. In all our experiments, half of the dataset is distributed to all clients as unlabeled local data.

4.1 Performance Evaluation

In all our experiments, we follow the definitions of *strong* and *weak* clients as discussed in Section 3.2. As shown in Table 3, we explore a variety of auxiliary model sizes for a comprehensive empirical study.

Table 4 shows the performance comparison between two baselines and the proposed method, and Figure 3 shows the corresponding training loss and validation accuracy curves, respectively. We consider two baselines: *weak-only*, where the model size is reduced to fit within all clients’ memory space and *strong-only*, where the *weak* clients are excluded and only the *strong* clients participate in the large model training. These two baselines are the most straightforward options for standard FL. By comparing our method to these two baselines, we can evaluate how well the proposed on-device KD utilizes the *weak* clients’ local data to strengthen the large target model. To ensure a fair comparison in terms of computational

cost, the *weak-only* and *strong-only* methods perform 2τ local steps, while our method runs τ local SGD steps and τ KD steps.

Table 4 shows that the proposed method remarkably improves the target model accuracy. The performance gap mainly comes from the knowledge transferred from the auxiliary model which learns from all clients’ local data. The same result can be observed across different applications, computer vision benchmarks and audio command detection benchmark. It also works well with the transformer-based fine-tuning task. Therefore, we can conclude that the proposed method effectively improves the large model’s performance by utilizing many *weak* clients’ local data.

4.2 Comparative Study

We compare our method to three homogeneous FL methods: FedAvg, MOON, and FedDF, and heterogeneous FL methods: DS-FL, FedMD, and FedGEM [7], as shown in Table 5. The homogeneous FL methods use a small model that has 25% of channels at each layer. The heterogeneous FL methods use the full model at 20% of the clients and the small model at the rest of the clients. These settings well represent the realistic FL environments consisting of edge devices with heterogeneous system resources.

We do not compare our method to FedGKT [12] and Fed-ET [8] since they are composed of several features independent of KD. E.g., their representation transfer can be applied to our method without any conflicts. We also do not present time vs. accuracy results because all the methods have a different computation to communication ratio per round. Our study instead focuses on the achievable accuracy within a sufficiently large epoch budget.

Comparison to Homogeneous FL Methods – MOON achieves higher accuracy than FedAvg, demonstrating a practical use-case of contrastive loss. FedDF achieves even higher accuracy than MOON

¹ Appendix is available at <https://www.arxiv.org/abs/2503.11151>

Dataset	FedAvg (homo)	MOON (homo)	FedDF (homo)	DS-FL (hetero)	FedMD (hetero)	FedGEM (hetero)	Proposed (hetero)
Public Data	N/A	N/A	Unlabeled	Unlabeled	Labeled	Labeled	Unlabeled
CIFAR-10	57.47 $\pm$ 0.8%	58.38 $\pm$ 0.1%	41.62 $\pm$ 0.1%	25.95 $\pm$ 0.1%	61.13 $\pm$ 0.1%	34.27 $\pm$ 0.1%	62.43 $\pm$ 0.1%
FEMNIST	64.27 $\pm$ 0.1%	64.80 $\pm$ 0.1%	66.90 $\pm$ 0.2%	56.71 $\pm$ 0.5%	65.23 $\pm$ 0.1%	65.06 $\pm$ 0.1%	67.44 $\pm$ 0.1%
Google Speech	66.05 $\pm$ 0.7%	N/A	59.58 $\pm$ 0.2%	19.14 $\pm$ 0.1%	65.90 $\pm$ 0.1%	25.20 $\pm$ 0.2%	71.95 $\pm$ 0.5%

Table 5: The FL performance comparison across SOTA KD-based FL methods. 20% of the total clients are *strong* clients and the auxiliary model size is 25% of the target model. Our method achieves the best accuracy without extra labeled data (public data). MOON is designed only for image data, and thus we do not apply it to Google Speech, the audio benchmark.

thanks to its server-side KD with public data. However, because these methods do not consider the system heterogeneity, they cannot train large models that do not fit into weak clients’ memory space. In contrast, our method can train large target models, achieving superior performance by exploiting the strong clients’ system resources.

Comparison to Heterogeneous FL Methods – DS-FL shows much lower accuracy than others due to the personalized local models. This result is well aligned with our ablation study shown in Figure 1, indicating that the logit ensemble dramatically harms the soft target quality, leading to a loss in accuracy. FedMD achieves much higher accuracy than DS-FL. However, the performance gain mainly comes from the labeled public data shared across all the clients. In addition, FedMD is not applicable to environments where unlabeled data is distributed to the edge since the global logit should be calculated from the local logits obtained from the same data across all the clients. FedGEM achieves inconsistent performance across benchmarks. Due to the poor soft target quality caused by the logit ensemble, it severely loses the accuracy. FedGEM also assumes the labeled public data like FedMD, which is not realistic. Based on this comparative study, we can conclude that our method utilizes the unlabeled data more effectively than other methods.

4.3 Ablation Study

Auxiliary Model Size – To analyze the impact of the auxiliary model size on the target model’s performance, we conduct an ablation study as shown in Table 6. First, we set the number of strong clients to 20% of the total clients. Then, we measure the accuracy of the auxiliary and target models using different auxiliary model sizes. One clear trend observed across all settings is that the target model accuracy improves as the auxiliary model size increases. This trend demonstrates that *the auxiliary model more effectively transfers the global knowledge to the target model as its size grows*.

One intriguing observation is that, for CIFAR-10 and Google Speech, the auxiliary model achieves even higher accuracy than the target model when its size is 75%. This is the case where the amount of data plays a more important role in achieving good accuracy than the model size difference. That is, the increased learning capability from a larger target model does not significantly improve performance, as the sufficiently strong auxiliary model can already learn global knowledge effectively. This result shows that the proposed method becomes more practical as the system becomes strongly heterogeneous.

Strong Client Ratio – We conduct another ablation study to analyze the impact of strong client ratio on FL performance. Table 7 shows the target model’s accuracy with a varying number of strong clients. The auxiliary model size is 25% of the target model. The unlabeled data size is fixed regardless of the number of strong clients. In all the benchmarks, the target model performance is improved as the ratio of the strong clients increases. This result demonstrates the benefit

Dataset	Ratio	Auxiliary Acc.	Target Model Acc.
CIFAR-10 ResNet20	25%	49.11 $\pm$ 0.1%	62.43 $\pm$ 0.1%
	50%	60.86 $\pm$ 1.5%	64.62 $\pm$ 0.5%
	75%	66.65 $\pm$ 0.6%	66.39 $\pm$ 0.8%
FEMNIST CNN	25%	64.19 $\pm$ 0.1%	67.44 $\pm$ 0.1%
	50%	65.89 $\pm$ 0.4%	67.73 $\pm$ 0.2%
	75%	66.67 $\pm$ 0.3%	68.63 $\pm$ 0.3%
Google Speech CNN	25%	66.83 $\pm$ 0.3%	71.95 $\pm$ 0.5%
	50%	74.54 $\pm$ 0.1%	75.25 $\pm$ 0.1%
	75%	76.77 $\pm$ 0.1%	75.94 $\pm$ 0.2%

Table 6: The accuracy comparison across varying auxiliary model sizes. 20% of the total clients are strong.

Dataset	Strong / Total Clients	Target Model Acc.
CIFAR-10 ResNet20	10 / 100	64.37 $\pm$ 0.1%
	20 / 100	68.29 $\pm$ 0.7%
	40 / 100	70.20 $\pm$ 0.8%
FEMNIST CNN	10 / 100	66.36 $\pm$ 0.1%
	20 / 100	67.44 $\pm$ 0.1%
	40 / 100	67.78 $\pm$ 0.1%
Google Speech CNN	10 / 100	67.91 $\pm$ 0.1%
	20 / 100	71.95 $\pm$ 0.5%
	40 / 100	74.72 $\pm$ 0.4%

Table 7: The accuracy comparison across varying strong client ratios. The auxiliary model size is 25%.

of having an auxiliary model: *As the ratio of the strong clients increases, the target model can learn from more unlabeled data, which results in improving its validation accuracy*. Therefore, our method can be considered as a promising heterogeneous FL method which scales up more effectively.

5 Conclusion

We proposed a novel on-device KD-based heterogeneous FL method. Our method exploits the heterogeneous system resources at the edge via local KD with periodic model aggregations. This approach enables the target model to learn from the local data regardless of whether they are labeled or not. This is the key advantage as it will allow FL applications to leverage the continuously generated local data at the edge without needing to share it across clients. Our study demonstrates that the proposed on-device KD method also effectively improves the knowledge transfer efficiency even under extremely non-IID environments. More importantly, our study empirically proves that the large model can be well trained on the distributed non-IID data without relying on the server-side resources or the centralized public data. We believe that harmonizing our method and the communication-efficient model aggregation methods is critical future work.

Acknowledgments

This work was supported by INHA UNIVERSITY Research Grant.

References

- [1] S. Alam, L. Liu, M. Yan, and M. Zhang. Fedrolex: Model-heterogeneous federated learning with rolling sub-model extraction. *Advances in neural information processing systems*, 35:29677–29690, 2022.
- [2] S. Ben-David, J. Blitzer, K. Crammer, A. Kulesza, F. Pereira, and J. W. Vaughan. A theory of learning from different domains. *Machine learning*, 79:151–175, 2010.
- [3] S. Caldas, P. Wu, T. Li, J. Konečný, H. B. McMahan, V. Smith, and A. Talwalkar. Leaf: A benchmark for federated settings. *arXiv preprint arXiv:1812.01097*, 2018. URL <https://arxiv.org/abs/1812.01097>.
- [4] Y. H. Chan and E. C. Ngai. Fedhe: Heterogeneous models and communication-efficient federated learning. In *2021 17th International Conference on Mobility, Sensing and Networking (MSN)*, pages 207–214. IEEE, 2021.
- [5] H.-R. Chen, L. Yang, X. Zhang, J. Shen, and J. Cao. Distributed semi-supervised learning with consensus consistency on edge devices. *IEEE Transactions on Parallel and Distributed Systems*, 35(2):310–323, 2023.
- [6] Q. Chen, Z. Zheng, C. Hu, D. Wang, and F. Liu. On-edge multi-task transfer learning: Model and practice with data-driven task allocation. *IEEE Transactions on Parallel and Distributed Systems*, 31(6):1357–1371, 2019.
- [7] S. Cheng, J. Wu, Y. Xiao, and Y. Liu. Fedgems: Federated learning of larger server models via selective knowledge fusion. *arXiv preprint arXiv:2110.11027*, 2021.
- [8] Y. J. Cho, A. Manoel, G. Joshi, R. Sim, and D. Dimitriadis. Heterogeneous ensemble knowledge transfer for training large models in federated learning. In *Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence (IJCAI) Main Track*, pages 2881–2887, 2022.
- [9] E. Diao, J. Ding, and V. Tarokh. Heterofl: Computation and communication efficient federated learning for heterogeneous clients. In *Proceedings of International Conference on Learning Representations (ICLR)*, pages 1–24, 2021.
- [10] A. Dosovitskiy, L. Beyer, A. Kolesnikov, D. Weissenborn, X. Zhai, T. Unterthiner, M. Dehghani, M. Minderer, G. Heigold, S. Gelly, et al. An image is worth 16x16 words: Transformers for image recognition at scale. In *Proceedings of the International Conference on Learning Representations (ICLR)*, pages 1–21, 2021.
- [11] Z. Fan, S. Hu, J. Yao, G. Niu, Y. Zhang, M. Sugiyama, and Y. Wang. Locally estimated global perturbations are better than local perturbations for federated sharpness-aware minimization. In *International Conference on Machine Learning*, volume 235, pages 12858–12881, 2024.
- [12] C. He, M. Annamaram, and S. Avestimehr. Group knowledge transfer: Federated learning of large cnns at the edge. *Advances in Neural Information Processing Systems*, 33:14068–14080, 2020.
- [13] K. He, X. Zhang, S. Ren, and J. Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778, 2016.
- [14] G. Hinton, O. Vinyals, and J. Dean. Distilling the knowledge in a neural network. In *Deep Learning and Representation Learning Workshop in conjunction with NIPS*, 2014.
- [15] S. Horvath, S. Laskaridis, M. Almeida, I. Leontiadis, S. Venieris, and N. Lane. Fjord: Fair and accurate federated learning under heterogeneous targets with ordered dropout. *Advances in Neural Information Processing Systems*, 34:12876–12889, 2021.
- [16] S. Itahara, T. Nishio, Y. Koda, M. Morikura, and K. Yamamoto. Distillation-based semi-supervised federated learning for communication-efficient collaborative training with non-iid private data. *IEEE Transactions on Mobile Computing*, 22(1):191–205, 2021.
- [17] E. Jeong, S. Oh, H. Kim, J. Park, M. Bennis, and S.-L. Kim. Communication-efficient on-device machine learning: Federated distillation and augmentation under non-iid private data. In *2nd Workshop on Machine Learning on the Phone and Other Consumer Devices (MLPCD 2) in conjunction with the 32nd Conference on Neural Information Processing Systems (NeurIPS)*, 2018.
- [18] A. Krizhevsky, G. Hinton, et al. Learning multiple layers of features from tiny images. 2009.
- [19] S. Lee, A. K. Sahu, C. He, and S. Avestimehr. Partial model averaging in federated learning: Performance guarantees and benefits. *Neurocomputing*, 556:126647, 2023.
- [20] S. Lee, T. Zhang, and A. S. Avestimehr. Layer-wise adaptive model aggregation for scalable federated learning. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 37, pages 8491–8499, 2023.
- [21] S. Lee, T. Zhang, S. Prakash, Y. Niu, and S. Avestimehr. Embracing federated learning: Enabling weak client participation via partial model training. *IEEE Transactions on Mobile Computing*, 2024.
- [22] D. Li and J. Wang. Fedmd: Heterogeneous federated learning via model distillation. In *Federated Learning for Data Privacy and Confidentiality Workshop in conjunction with the 33rd Conference on Neural Information Processing Systems (NeurIPS)*, 2019.
- [23] Q. Li, B. He, and D. Song. Model-contrastive federated learning. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 10713–10722, 2021.
- [24] T. Lin, L. Kong, S. U. Stich, and M. Jaggi. Ensemble distillation for robust model fusion in federated learning. *Advances in neural information processing systems*, 33:2351–2363, 2020.
- [25] J. Liu, K. Huang, and L. Xie. Hetefed: Heterogeneous federated learning with privacy-preserving binary low-rank matrix decomposition method. In *2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pages 1238–1244. IEEE, 2023.
- [26] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics*, pages 1273–1282. PMLR, 2017.
- [27] Y. Niu, S. Prakash, S. Kundu, S. Lee, and S. Avestimehr. Federated learning of large models at the edge via principal sub-model training. In *Workshop on Federated Learning: Recent Advances and New Challenges in Conjunction with NeurIPS*, 2022.
- [28] A. Pal, A. Barigad, and A. Mustafi. Imdb movie reviews dataset, 2020. URL <https://dx.doi.org/10.21227/zm1y-b270>.
- [29] A. Tashakori, W. Zhang, Z. J. Wang, and P. Servati. Semipfl: Personalized semi-supervised federated learning framework for edge intelligence. *IEEE Internet of Things Journal*, 10(10):9161–9176, 2023.
- [30] P. Warden. Speech commands: A dataset for limited-vocabulary speech recognition. *arXiv preprint arXiv:1804.03209*, 2018.
- [31] D. Yao, W. Pan, Y. Shi, M. J. O’Neill, Y. Dai, Y. Wan, P. Zhao, H. Jin, and L. Sun. Fedhm: Efficient federated learning for heterogeneous models via low-rank factorization. *Artificial Intelligence*, 344:104333, 2025.
- [32] L. Zhang, L. Shen, L. Ding, D. Tao, and L.-Y. Duan. Fine-tuning global model via data-free knowledge distillation for non-iid federated learning. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 10174–10183, 2022.
- [33] T. Zhang, L. Gao, S. Lee, M. Zhang, and S. Avestimehr. Timelyfl: Heterogeneity-aware asynchronous federated learning with adaptive partial training. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 5064–5073, 2023.
- [34] L. Zhu, L. Hu, J. Lin, W.-M. Chen, W.-C. Wang, C. Gan, and S. Han. Pockengine: Sparse and efficient fine-tuning in a pocket. In *Proceedings of the 56th Annual IEEE/ACM International Symposium on Microarchitecture*, pages 1381–1394, 2023.