Towards Unbiased Training in Federated Open-world Semi-supervised Learning

Jie Zhang[1], Xiaosong Ma[1], Song Guo[1], and Wenchao Xu[1]

[1]Department of Computing, The Hong Kong Polytechnic University (PolyU)

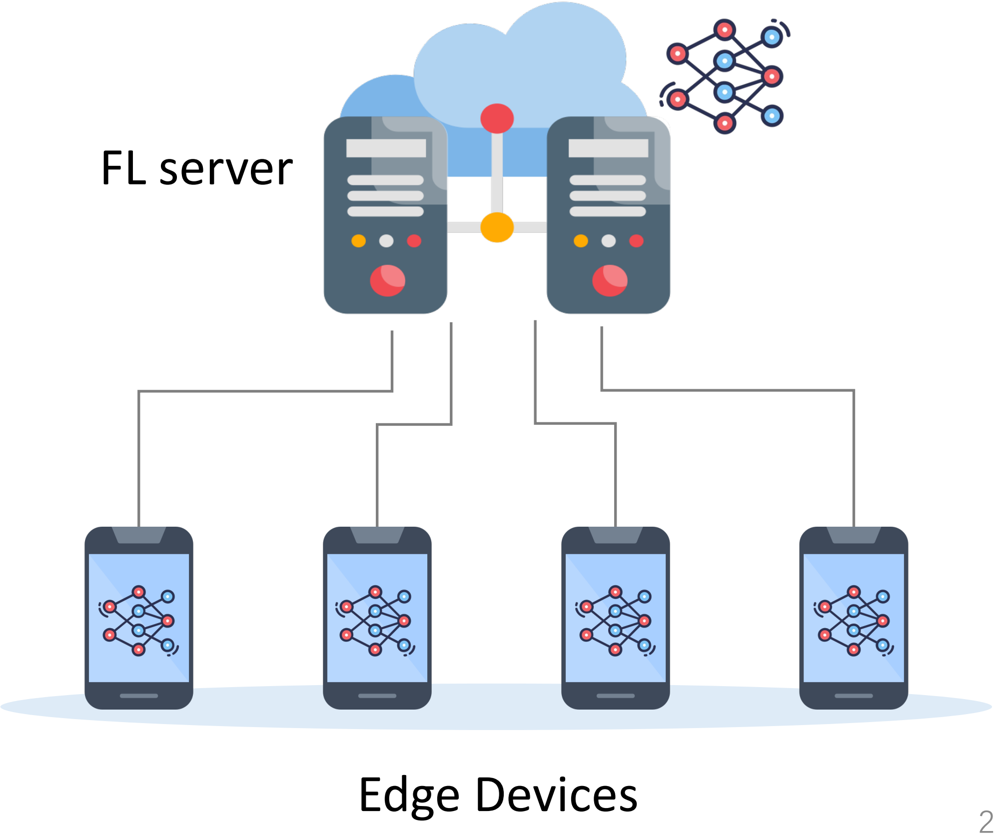
THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

ICML
International Conference On Machine Learning

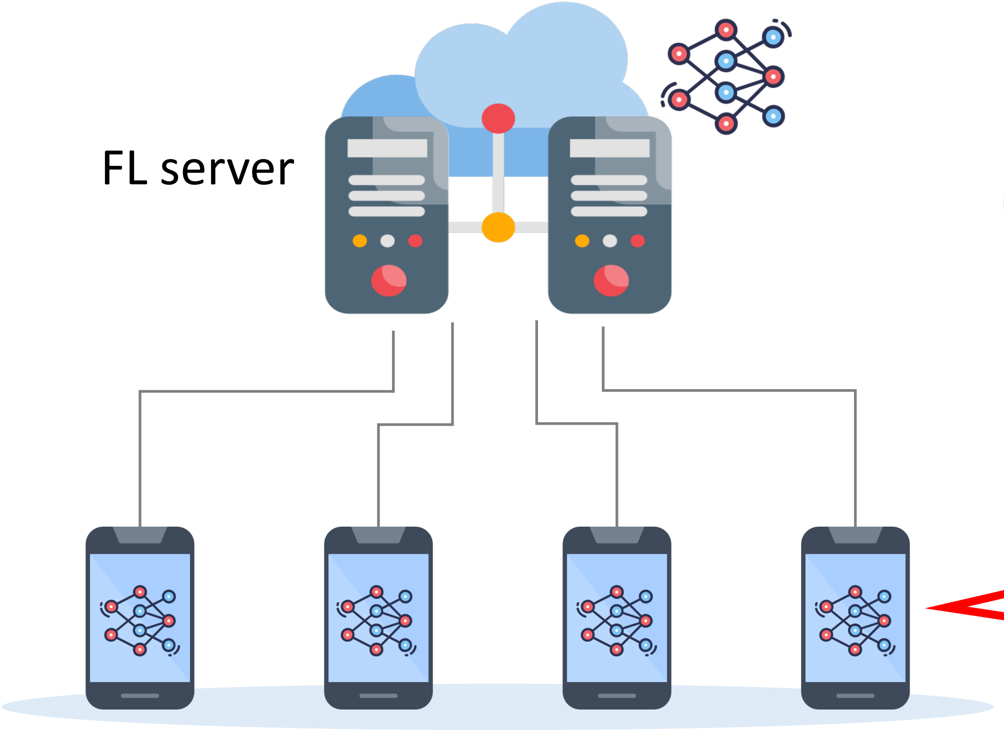
Federated Learning (FL)

- Increasing strict laws on data protection
  e.g., GDPR of EU, 2018; CCPA of USA, 2018; Cyber Security Law of China, 2017
- Federated Learning (FL) aims to collaboratively train a ML model while keeping the data decentralized



Federated Supervised Learning

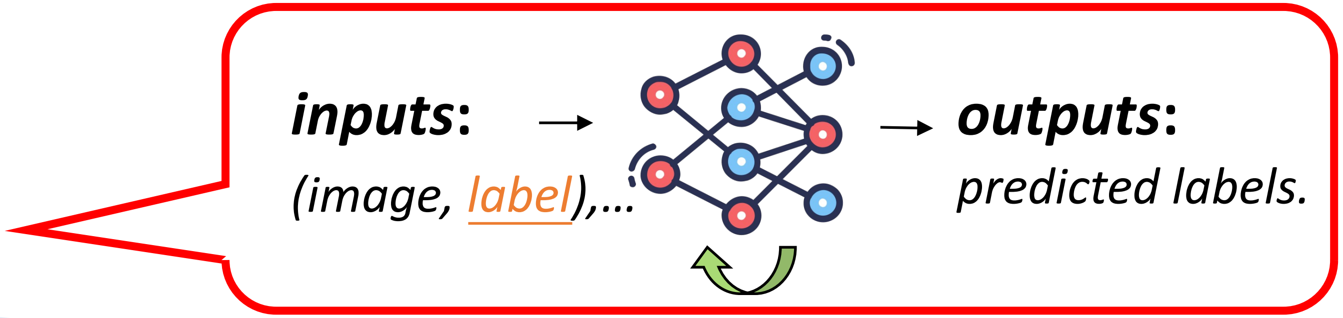
- **Local training**: each model trains the newest global model on local labeled dataset, then, uploading local updates to server
- **Global aggregation**: the server aggregates the updated local models to obtain new global model



Edge Devices

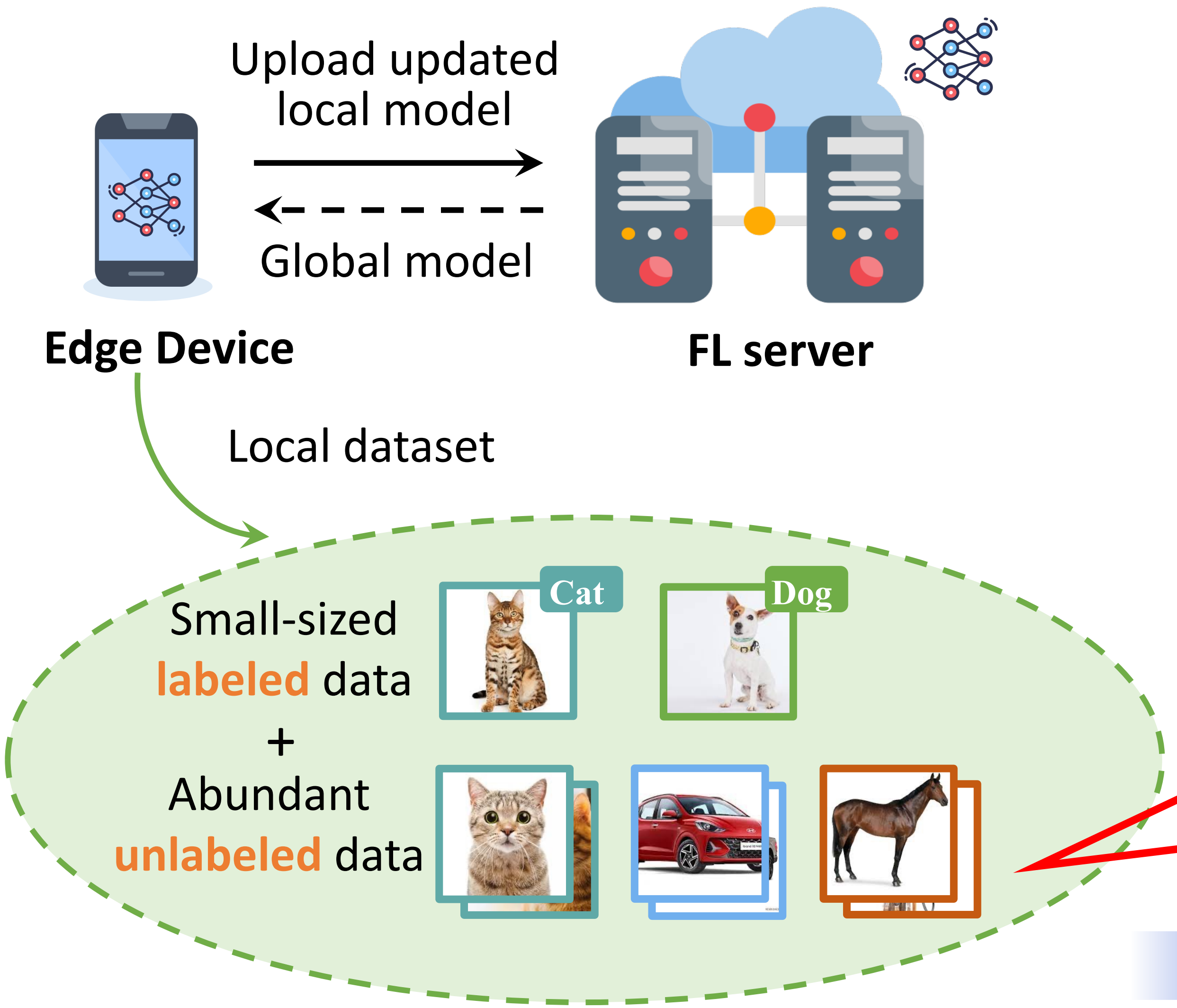
Supervised learning:

- Require all training data are labeled.
- In many real-world applications, labeled data are scarce.



Local Training

Federated Semi-Supervised Learning (FedSSL) [1] [2]



Notations:

- Local dataset on client i: $\mathcal{D}_i = \mathcal{D}_i^l \cup \mathcal{D}_i^u$
- Labeled part on client i: $\mathcal{D}_i^l = \{(x_j, y_j)\}_{j=1}^{n_i^l}$
- Unlabeled part on client i: $\mathcal{D}_i^u = \{(x_j)\}_{j=1}^{n_i^u}$
- The set of classes seen in full labeled data: $\mathcal{C}^l$
- The set of classes in full unlabeled data: $\mathcal{C}^u$

Existing works consider a closed-world setting:

$$\mathcal{C}^l = \mathcal{C}^u$$

Question: how about $\mathcal{C}^l \neq \mathcal{C}^u$?

[1] Lin et al. SemiFL: Semi-Supervised Federated Learning for Unlabeled Clients with Alternate Training, NeurIPS 2022.
[2] Jeong et al. Federated semi-supervised learning with inter-client consistency & disjoint learning. ICLR 2021.

Federated Open-world Semi-Supervised Learning (FedoSSL)

- **Enabling efficient FedoSSL is challenging:**

$$\mathcal{C}^l \neq \mathcal{C}^u$$

➢ Challenge 1: **Internal** heterogeneity in each client

Labeled data

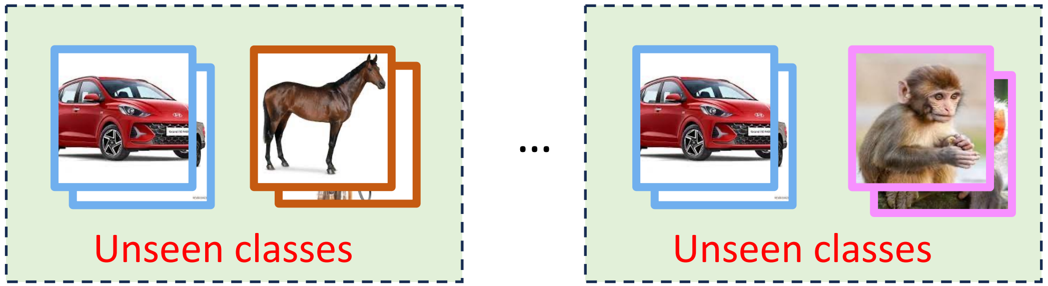
Unlabeled data

$$\mathcal{C}_i^l \neq \mathcal{C}_i^u$$

Unseen classes: unknow classes compared to the set of classes in labeled data.

➢ Challenge 2: **External** heterogeneity across different clients

Unlabeled data on client i



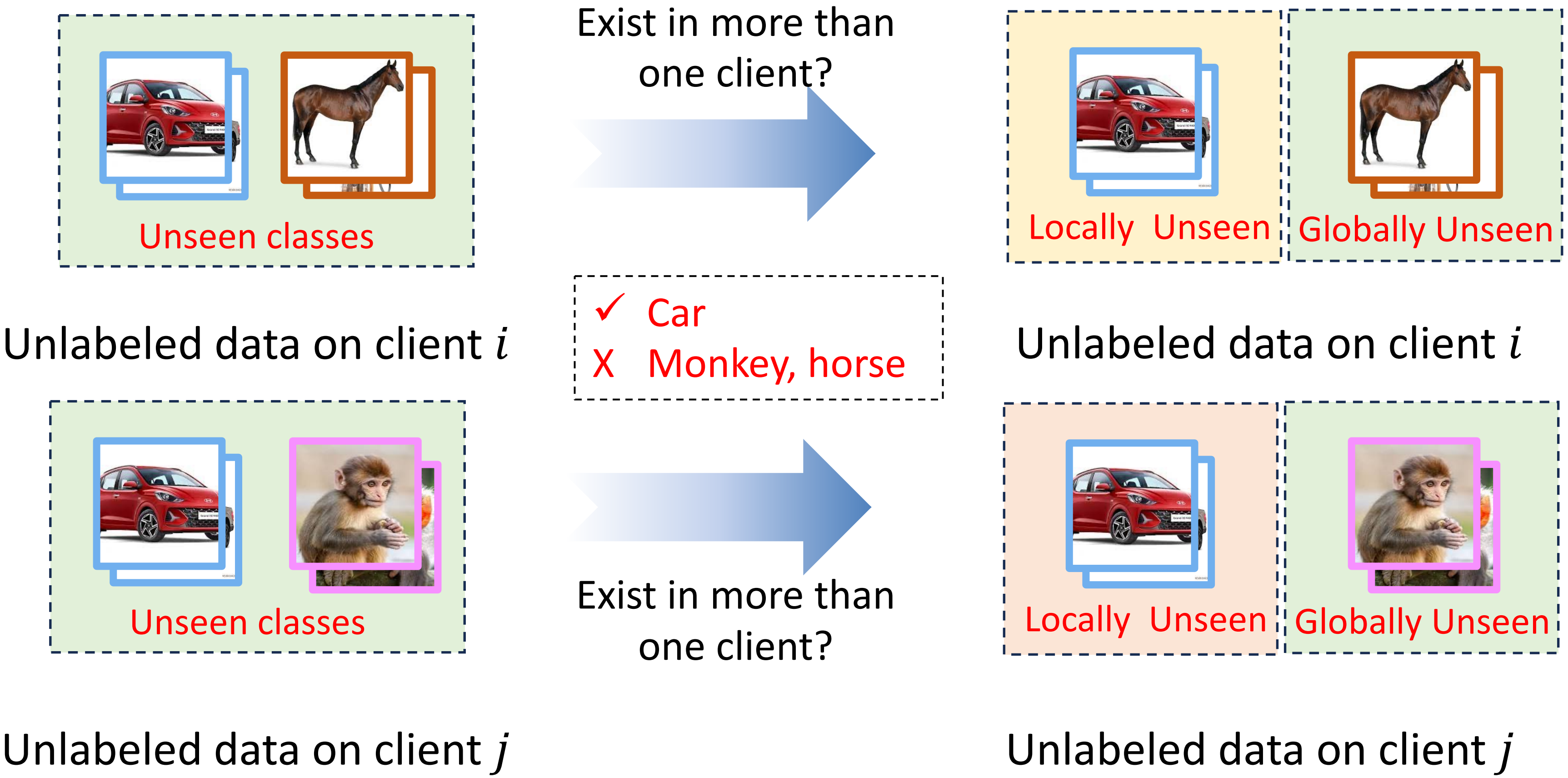
Unlabeled data on client j

$$\mathcal{C}_i^u \neq \mathcal{C}_j^u$$

Goal: Design efficient FedoSSL framework to overcome above two challenges.

Inspiration

- The unseen class can be further divided into two types according to the distribution heterogeneity.



Next Step: how to eliminate biased training among different types of unseen classes?

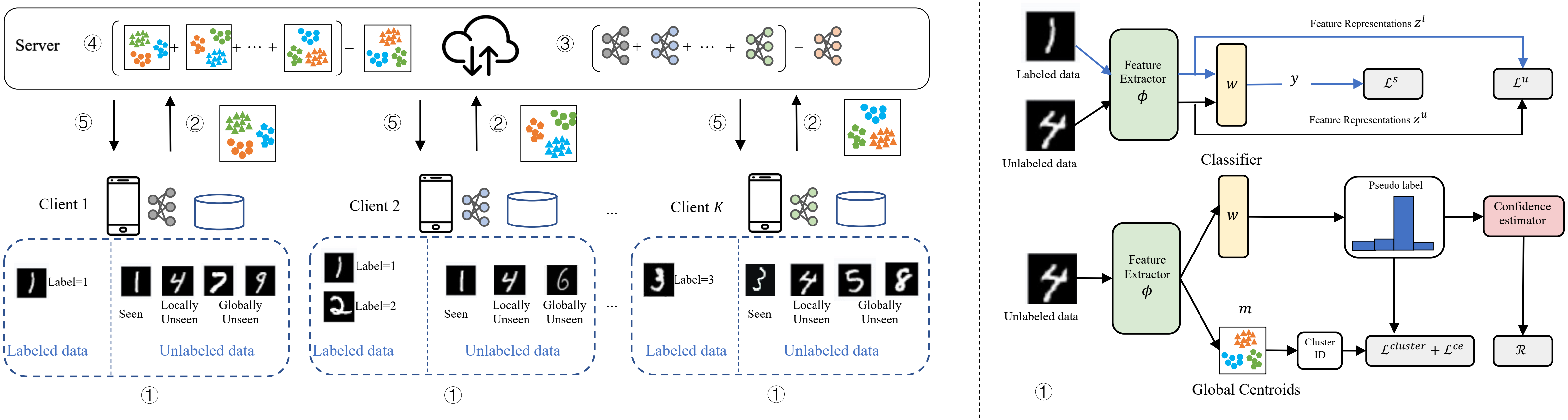
Methodology: FedoSSL

Definition 1 (Locally unseen & globally unseen class): In FedoSSL, the unseen classes $\mathcal{C}_{i,\,unseen}$ on client i can be divided into two types: locally unseen classes $\mathcal{C}_{i,\,lu}$, in which $\mathcal{C}_{i,\,lu} = \mathcal{C}_{1,\,unseen} \cap \cdots \mathcal{C}_{K,\,unseen}$; and globally unseen classes $\mathcal{C}_{i,\,gu}$, in which $\mathcal{C}_{i,\,gu} = \mathcal{C}_{i,\,unseen} \setminus \mathcal{C}_{i,\,lu}$.

Objective: $$\mathcal{L}_i^* = \mathcal{L}_i + \beta \mathcal{R}_i + \gamma \mathcal{L}_i^{cal}$$

- Fundamental semi-supervised loss: $\mathcal{L}_i = \mathcal{L}_i^s + \alpha \mathcal{L}_i^u$, where $\mathcal{L}_i^s$ is the standard cross-entropy loss on labeled data, $\mathcal{L}_i^u$ is the pairwise unsupervised loss on unlabeled data.
- Uncertainty-aware loss: $\mathcal{R}_i = \frac{1}{n_i^u} \sum_{x_j^u \in \mathcal{D}_i^u} \left| \pi(x_j^u) \right|$, where $\pi(\cdot)$ is the data uncertainty function.
- Calibration module: $\mathcal{L}_i^{cal} = \mathcal{L}_i^{ce} + \mathcal{L}_i^{cluster}$, where $\mathcal{L}_i^{ce}$ is global centroids-guided calibration loss, $\mathcal{L}_i^{cluster}$ is the additional loss for promoting clusterability of feature representations.

Workflow of FedoSSL



- **Local training**: 1) training on private dataset; 2) computing local centroids via Sinkhorn-Knopp based clustering algorithm.
- Upload both model parameters and local centroids to the server
- **Global aggregation**: 1) aggregating on local model parameters; 2) computing global centroids by again using Sinkhorn-Knopp clustering.

Evaluation Setup

Dataset:

- CIFAR-10, CIFAR-100, and CINIC-10
- We first divide classes into 60% seen and 40% unseen classes, then select 50% of seen classes as the labeled data and the rest as unlabeled data.

Baselines:

- 1) extending existing open-world SSL methods to FL environments:
  - ➢ Fed-AO, Fed-RO, Fed-AN, Fed-RO
- 2) extending existing FedSSL methods to the open-world scenarios:
  - ➢ *SemiFL

FL environment:

- 1) 10 clients with 50% participation ratio;
- 2) 50 clients with 10% participation ratio

Performance Comparison to SOTA Baselines

- Classification accuracy of compared methods on seen, unseen and all classes with 10 clients over three benchmark datasets.

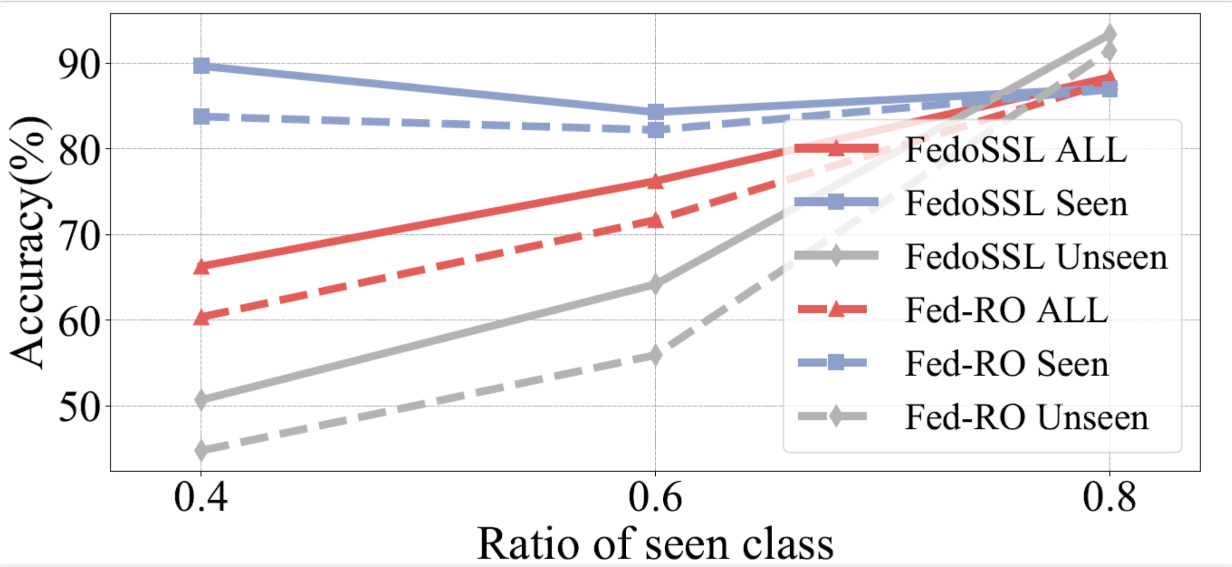
#Method	CIFAR-10 (%)					CIFAR-100 (%)					CINIC-10 (%)				
	All	Seen	Unseen			All	Seen	Unseen			All	Seen	Unseen		
			LU.	GU.	AU.			LU.	GU.	AU.			LU.	GU.	AU.
Cen-O	78.26	86.63	-	-	71.95	56.92	73.68	-	-	44.28	69.32	83.18	-	-	58.86
Cen-N	81.02	89.47	-	-	74.64	58.98	75.10	-	-	46.82	71.89	83.82	-	-	62.89
Local-O	65.98	79.57	-	-	45.60	43.10	54.33	-	-	26.25	55.33	65.23	-	-	40.48
Local-N	67.67	83.95	-	-	43.26	45.28	57.24	-	-	27.34	57.31	65.70	-	-	44.73
Fed-AO	69.46	81.01	89.38	42.03	52.15	47.91	59.67	38.07	29.12	30.26	54.85	63.22	71.31	37.88	42.29
Fed-RO	71.72	82.22	89.84	53.43	55.96	47.72	59.79	44.13	28.86	29.62	57.16	62.26	72.24	42.09	49.50
Fed-AN	66.58	84.18	78.76	37.58	40.15	47.25	58.24	42.11	30.44	30.77	53.49	63.61	66.78	36.06	38.32
Fed-RN	68.83	**85.52**	79.84	41.79	43.81	48.02	59.4	**48.77**	30.36	30.96	58.11	65.97	68.81	39.01	46.33
*SemiFL	64.91	81.57	86.33	31.16	39.92	42.28	54.94	31.68	21.46	23.29	52.27	62.72	64.53	37.21	37.34
FedoSSL	**76.26**	84.29	**90.68**	**59.69**	**64.22**	**51.58**	**61.12**	45.76	**33.82**	**31.13**	**63.82**	**68.40**	**79.79**	**47.78**	**56.96**

FedoSSL vs. SOTA Baselines:

- Over 11.10% performance gain on globally unseen classes.
- Over 14.76% performance gain on overall unseen classes.
- Reduce the performance gap between locally and globally unseen classes.

Environmental Sensitivity and Visualization

Number of Seen Class



Number of Local Centroids

L	All	Seen	Unseen		
			LU.	GU.	AU.
8	74.28	84.26	88.90	54.09	59.29
16	75.76	84.17	89.28	58.36	63.15
32	76.26	84.29	90.68	59.69	64.22

Selection of clustering algorithm

	All	Seen	Unseen		
			LU.	GU.	AU.
No Privacy	77.19	85.95	89.76	58.77	64.05
K-anonymity	76.26	84.29	90.68	59.69	64.22

FedoSSL holds good performance on different environmental settings, i.e., insensitive to the hyperparameters.

Thank you!

Jie-comp.zhang@polyu.edu.hk