ICLR 2025 oral

Subgraph Federated Learning for Local Generalization

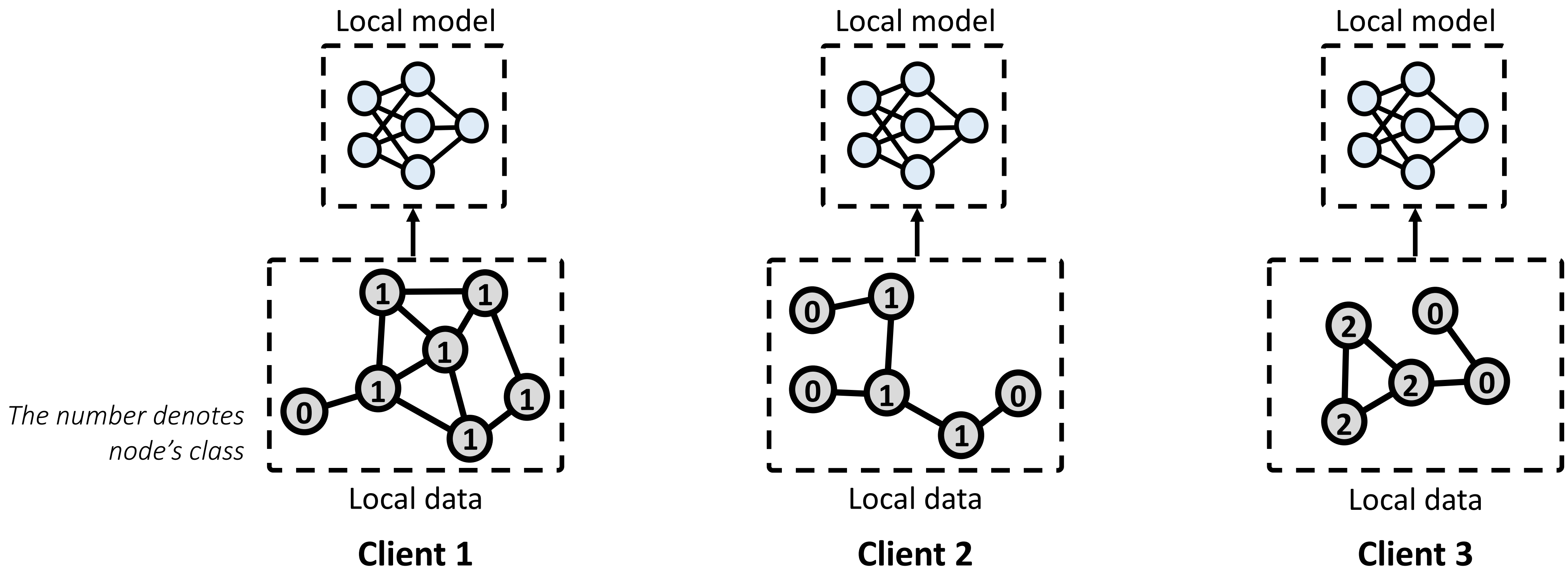
Sungwon Kim, Yoonho Lee, Yunhak Oh, Namkyeong Lee,
Sukwon Yun, Junseok Lee, Sein Kim, Carl Yang & Chanyoung Park

25th Apr. 2025

Presenter : Sungwon Kim

MOTIVATION

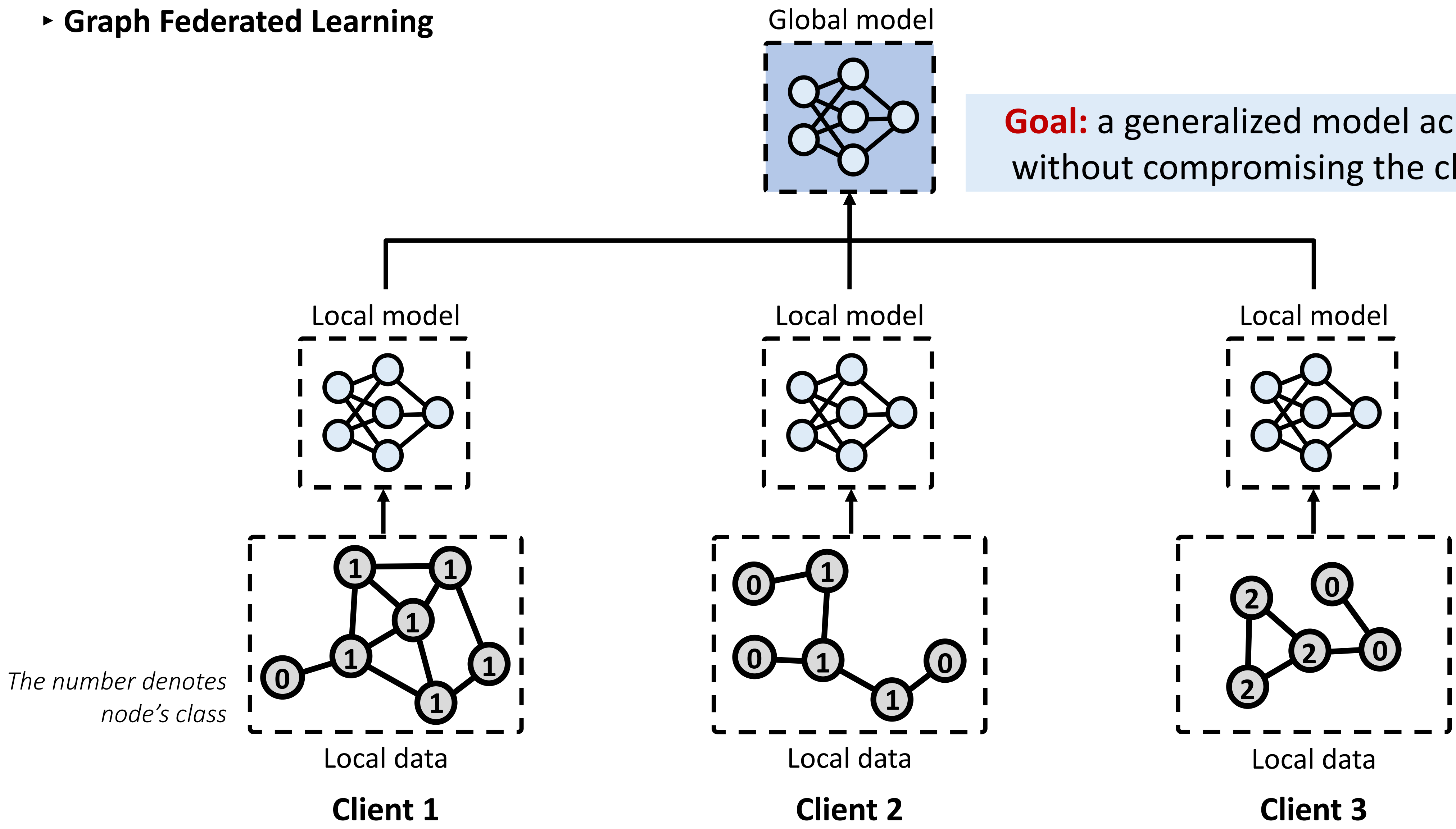
- **Graph Federated Learning**



MOTIVATION

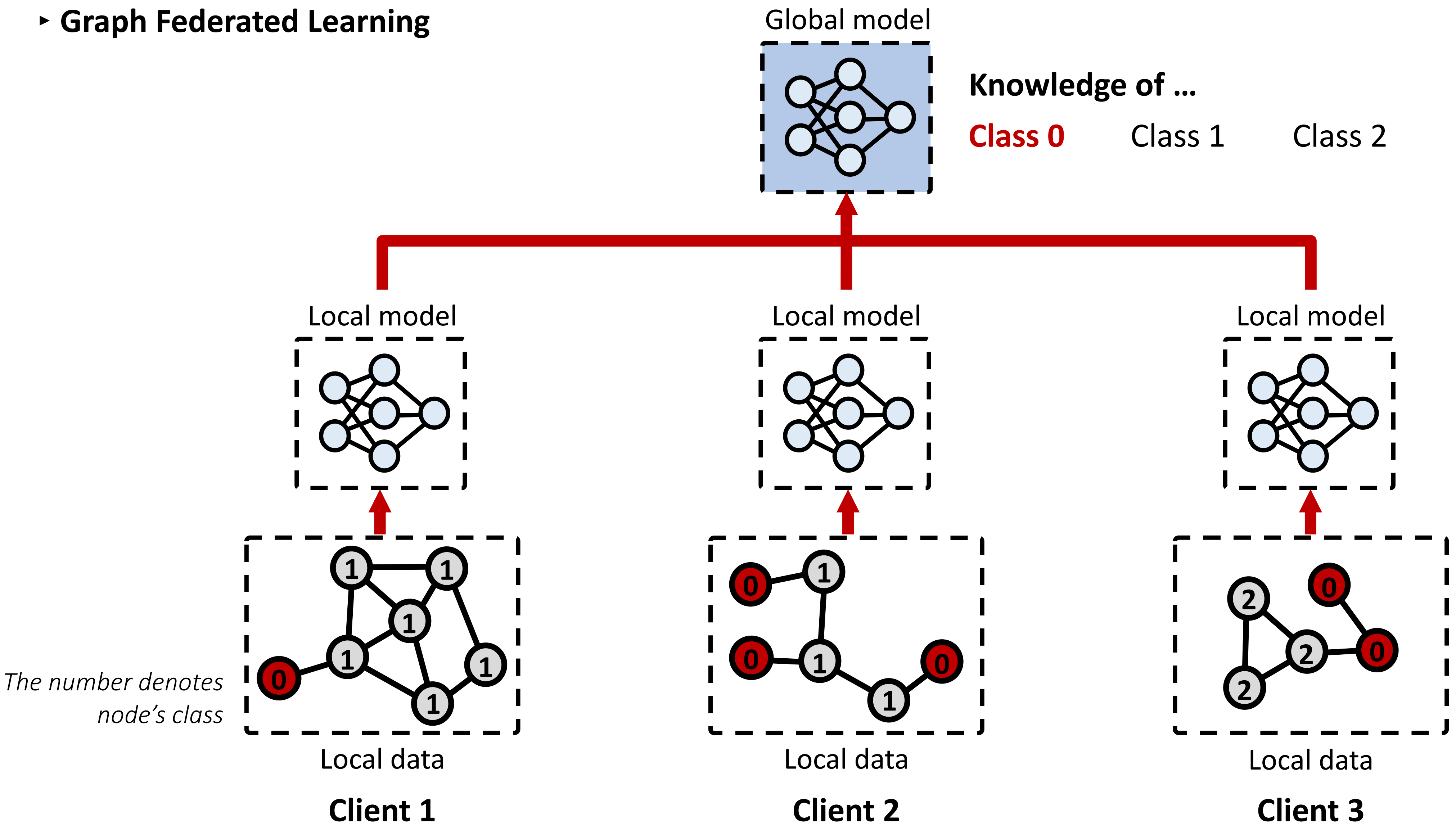
- **Graph Federated Learning**

Goal: a generalized model across all clients without compromising the clients' privacy



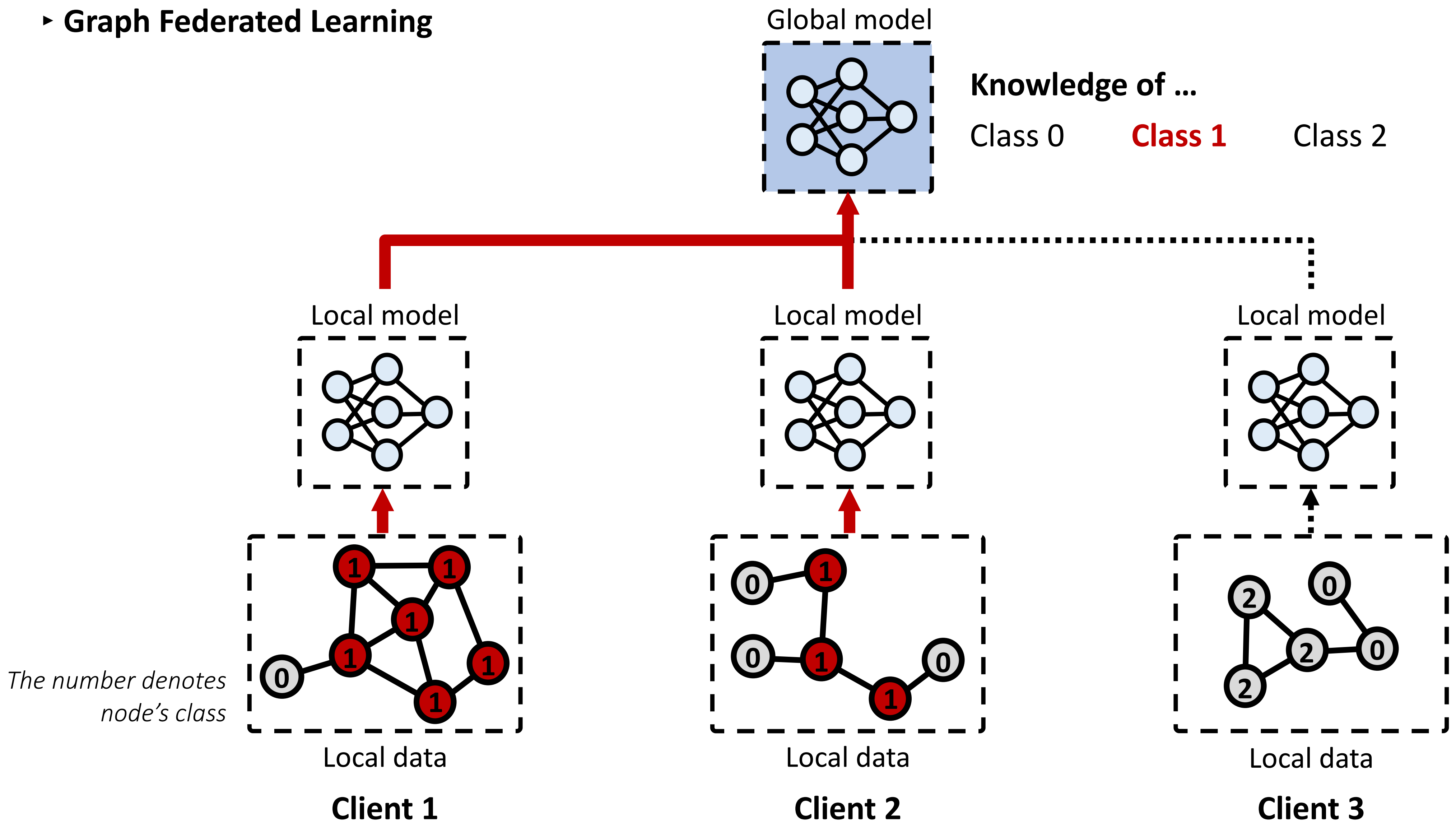
MOTIVATION

- **Graph Federated Learning**



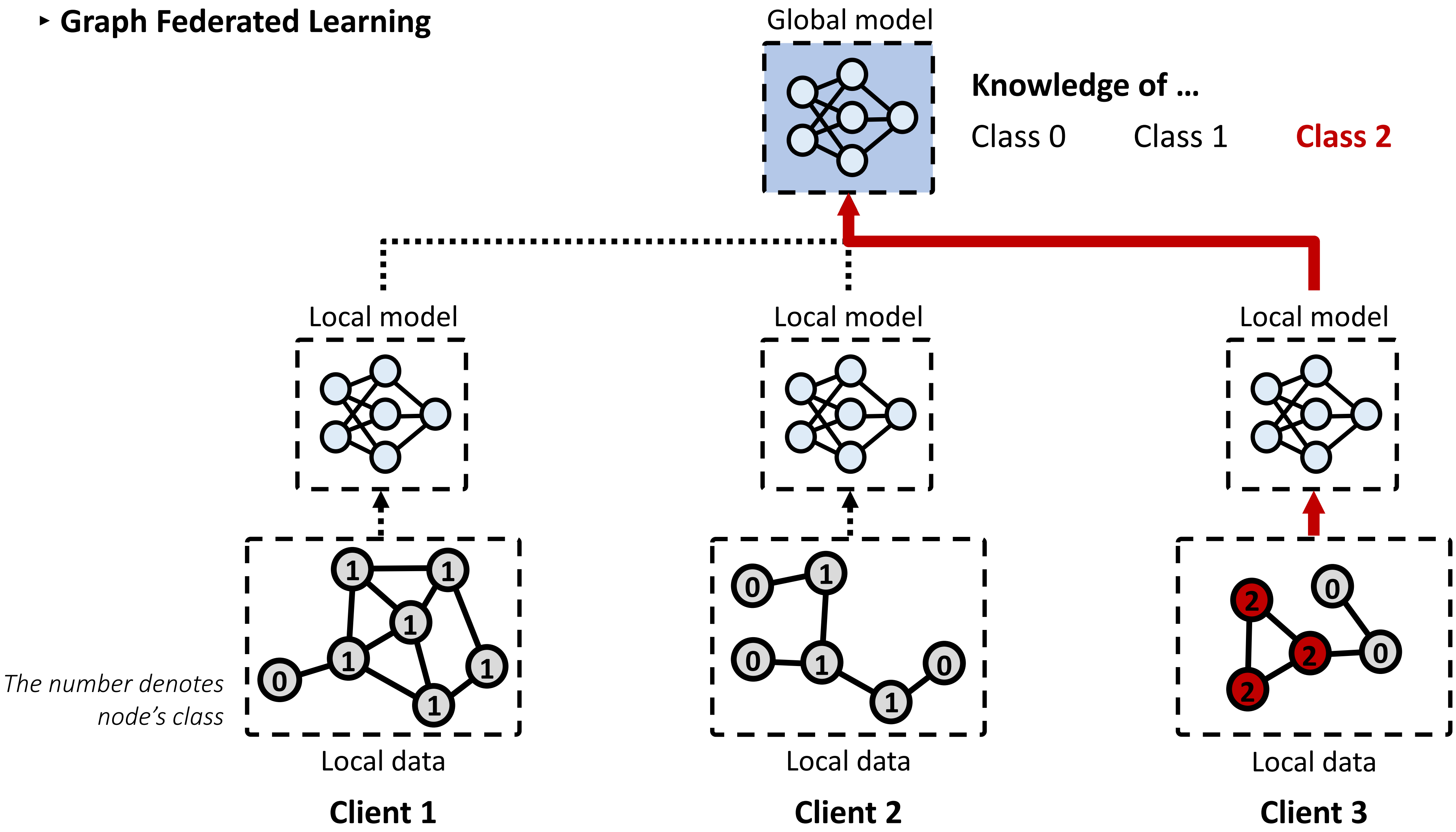
MOTIVATION

- **Graph Federated Learning**



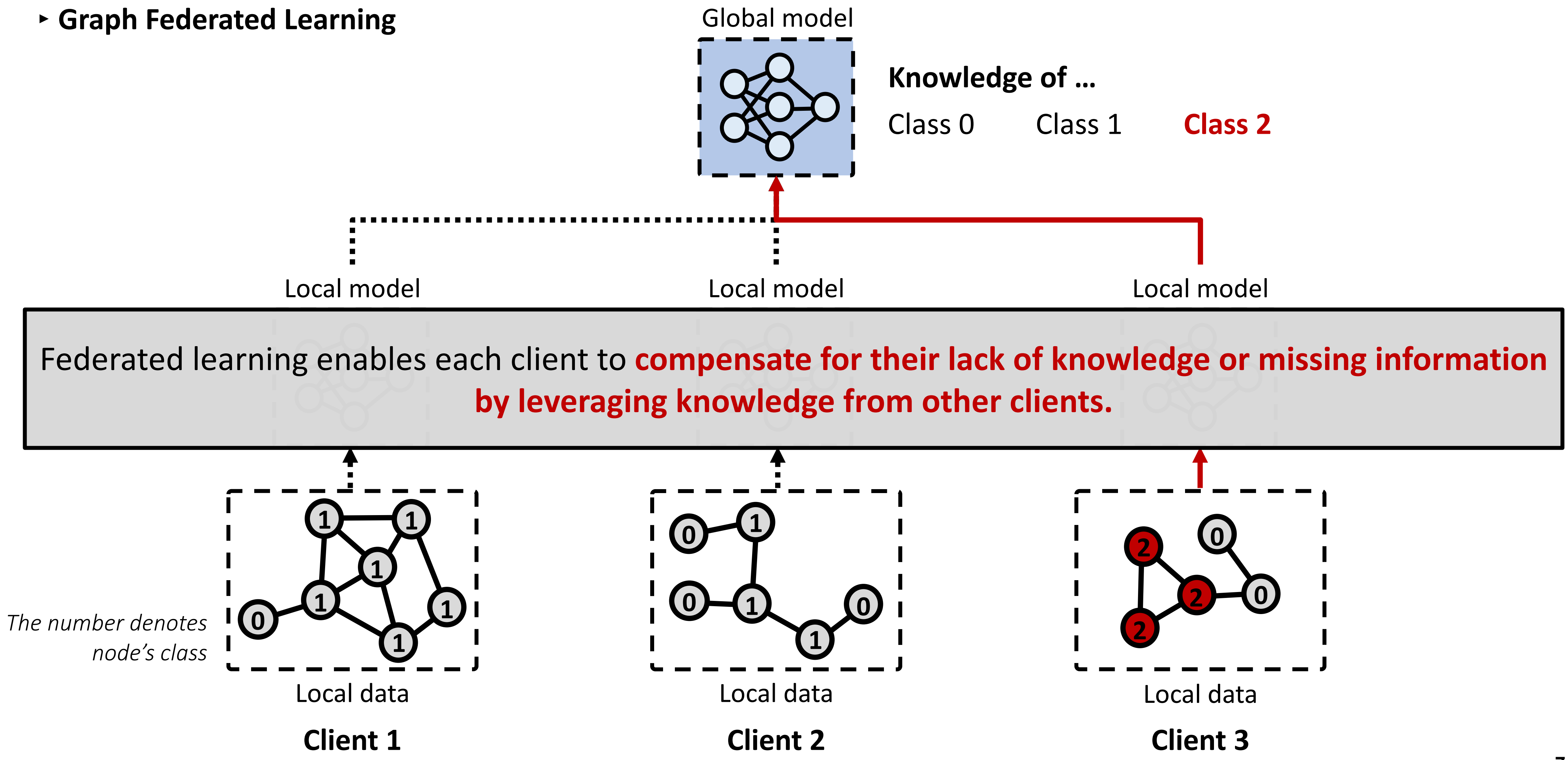
MOTIVATION

- **Graph Federated Learning**



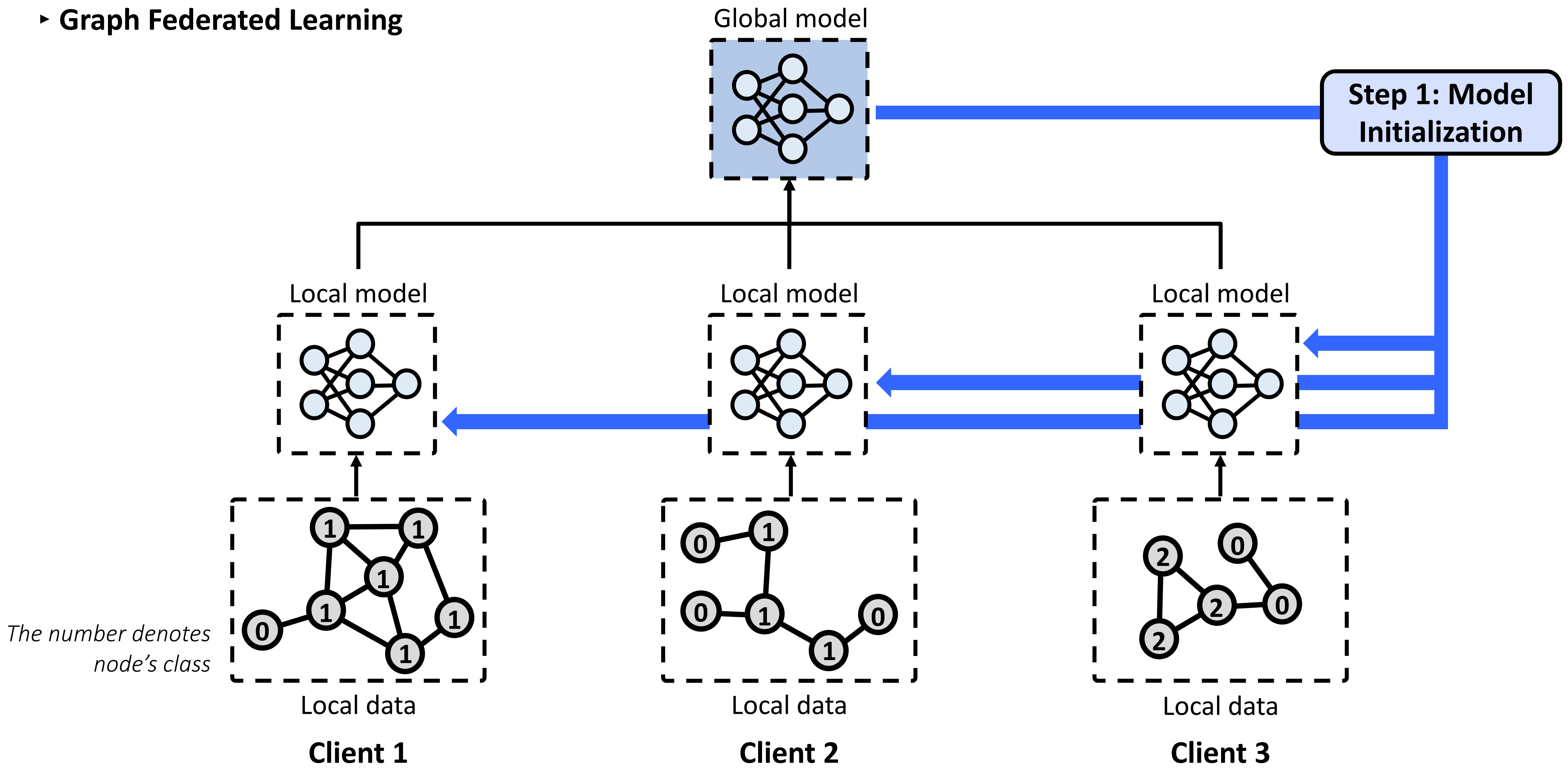
MOTIVATION

- **Graph Federated Learning**



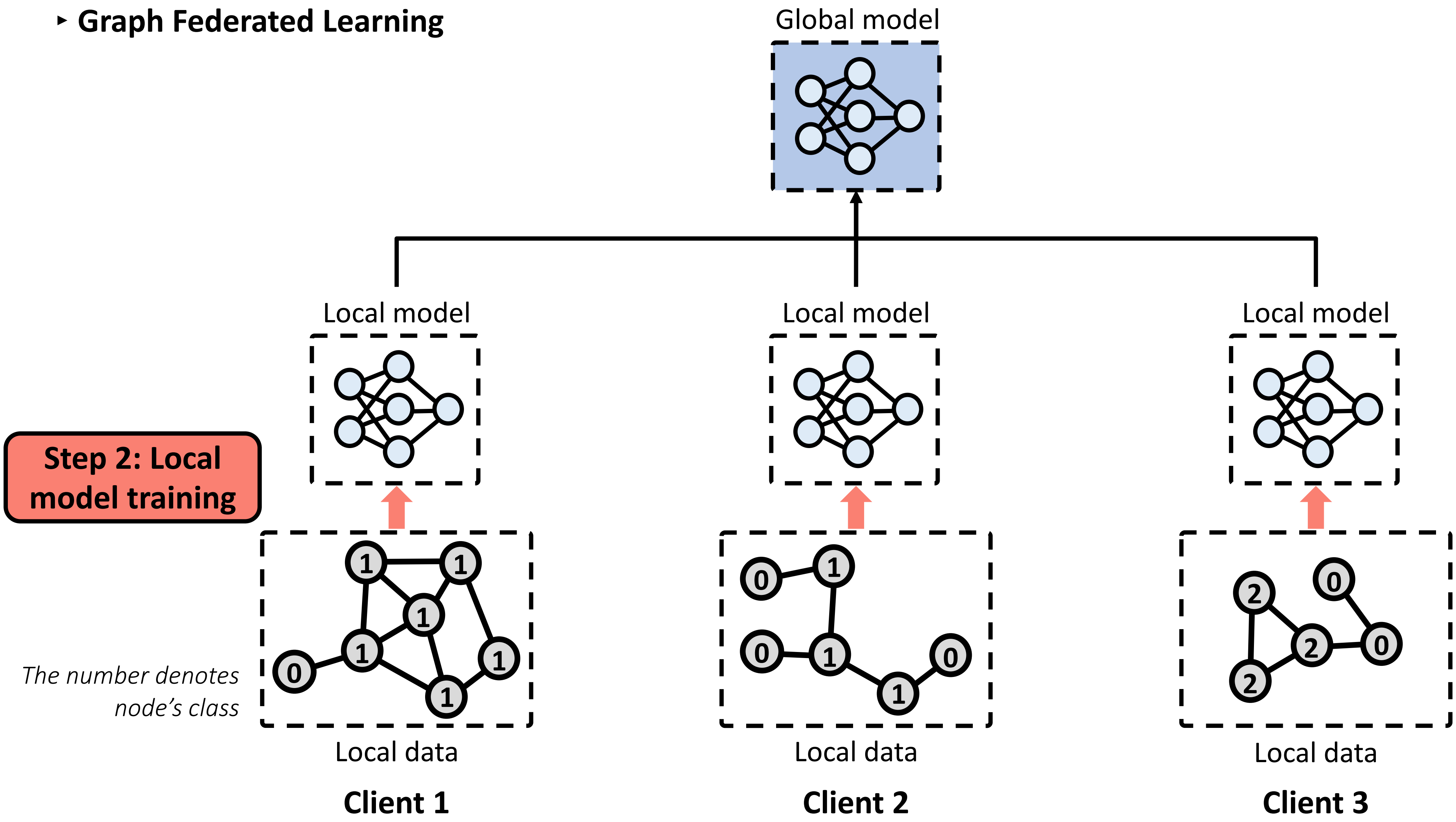
MOTIVATION

- **Graph Federated Learning**



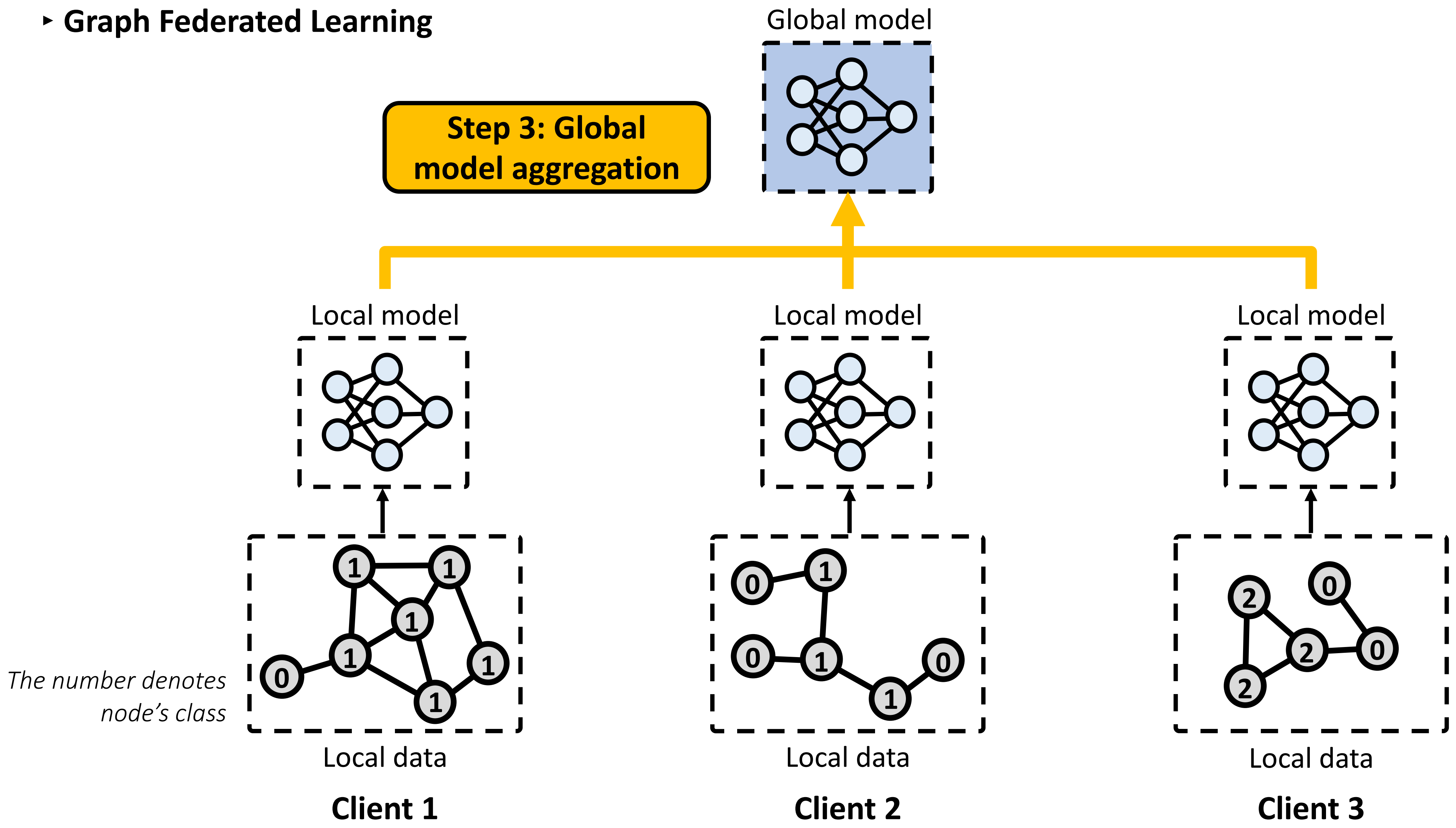
MOTIVATION

- **Graph Federated Learning**



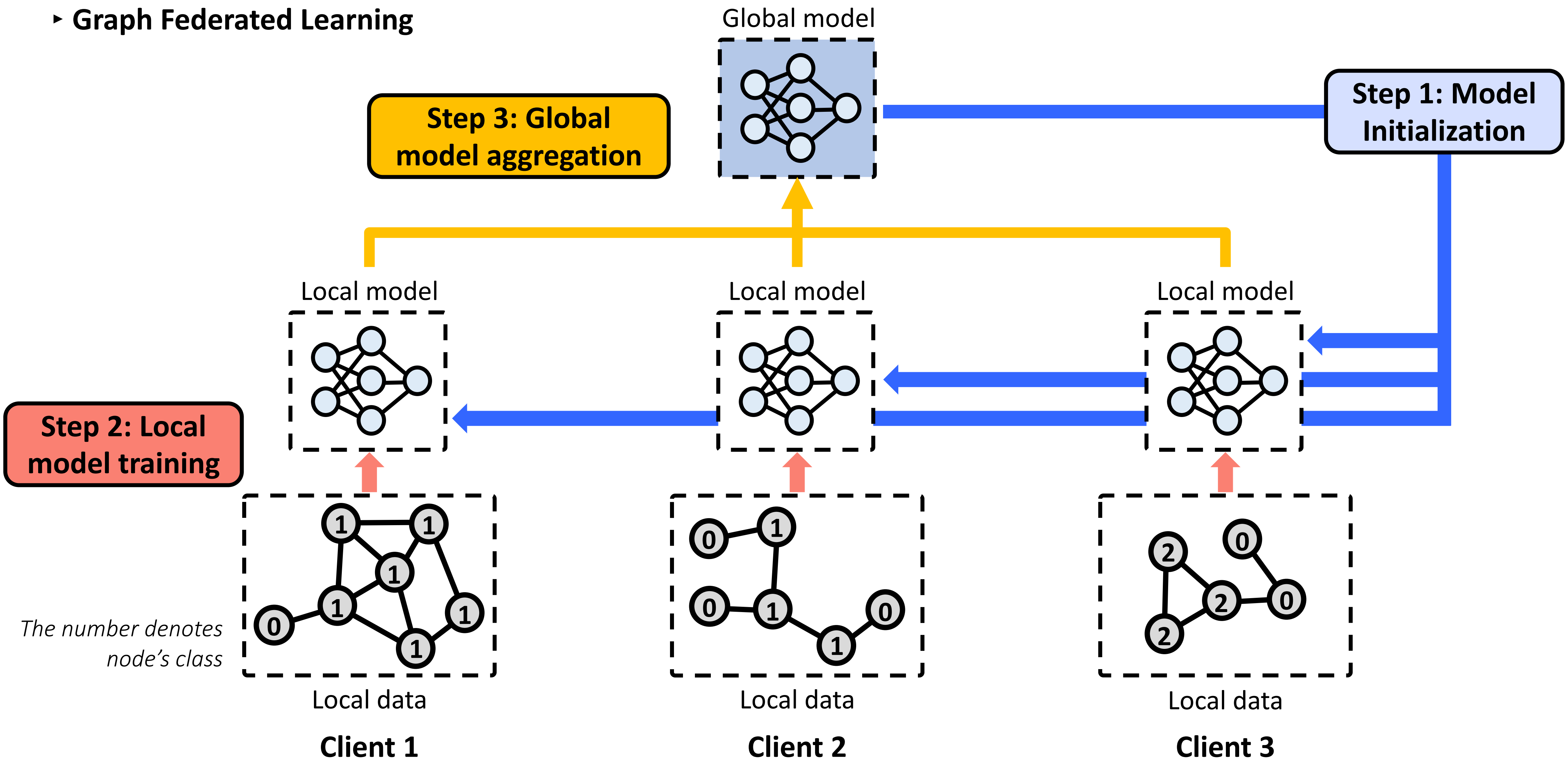
MOTIVATION

- **Graph Federated Learning**



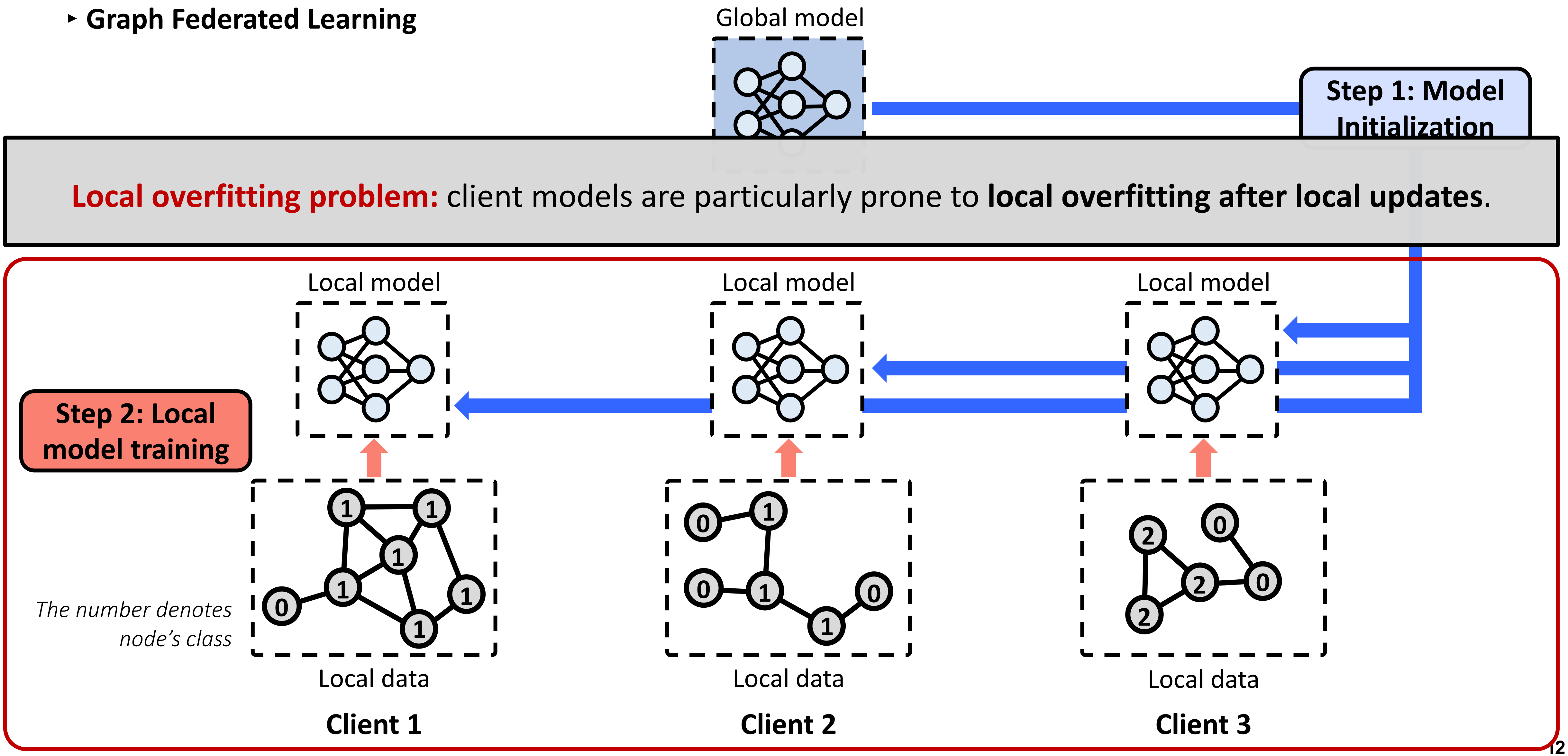
MOTIVATION

- **Graph Federated Learning**



MOTIVATION

- **Graph Federated Learning**

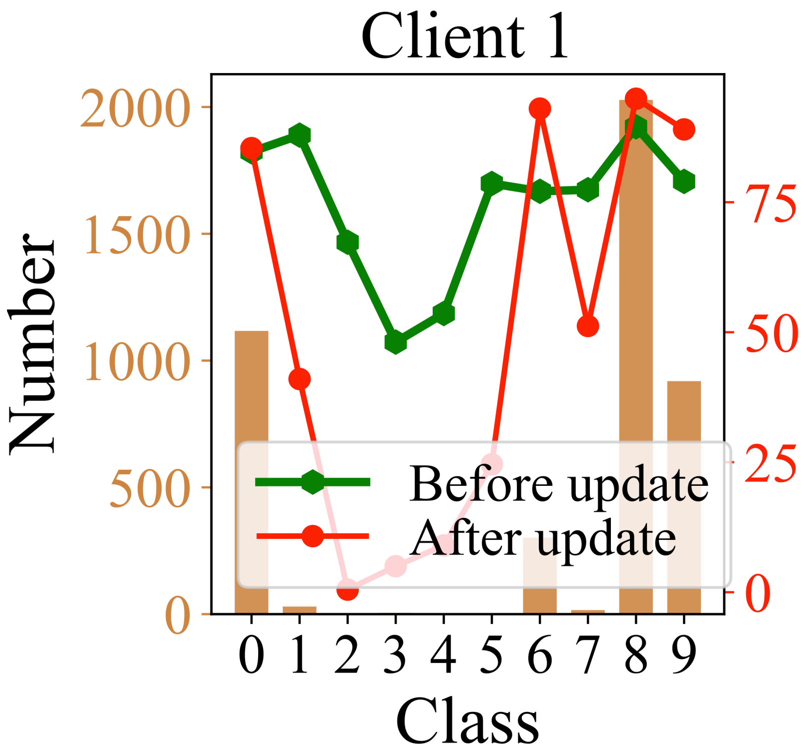


Local overfitting problem: client models are particularly prone to **local overfitting after local updates**.

MOTIVATION

- **Graph Federated Learning**

Local overfitting problem: client models are particularly prone to local overfitting after local updates.



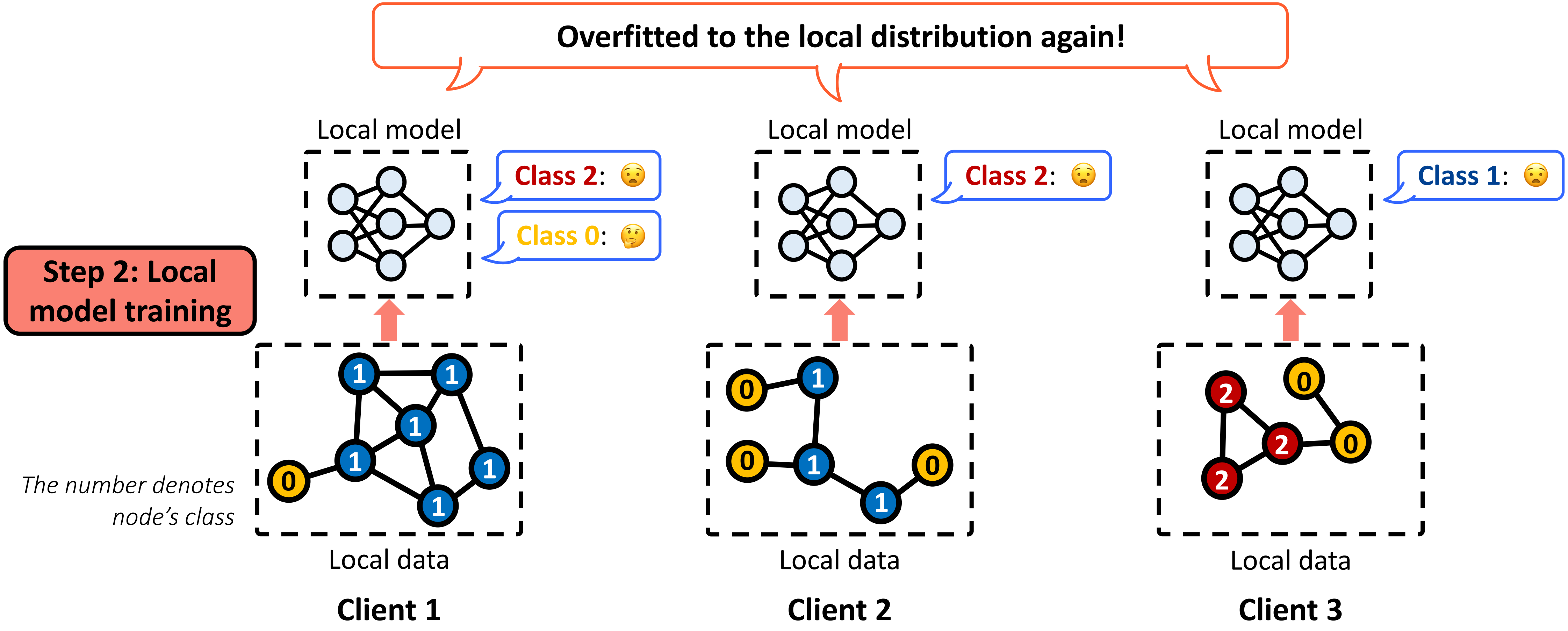
Local Overfitting leads to **significant decrease** in the accuracy of:

1) **Minority classes**
2) **Missing classes:** Unseen classes which are not present in the local graph <u>but exist in others.</u>

Figure: Zhang et al., Federated Learning with Label Distribution Skew via Logits Calibration, ICML'22

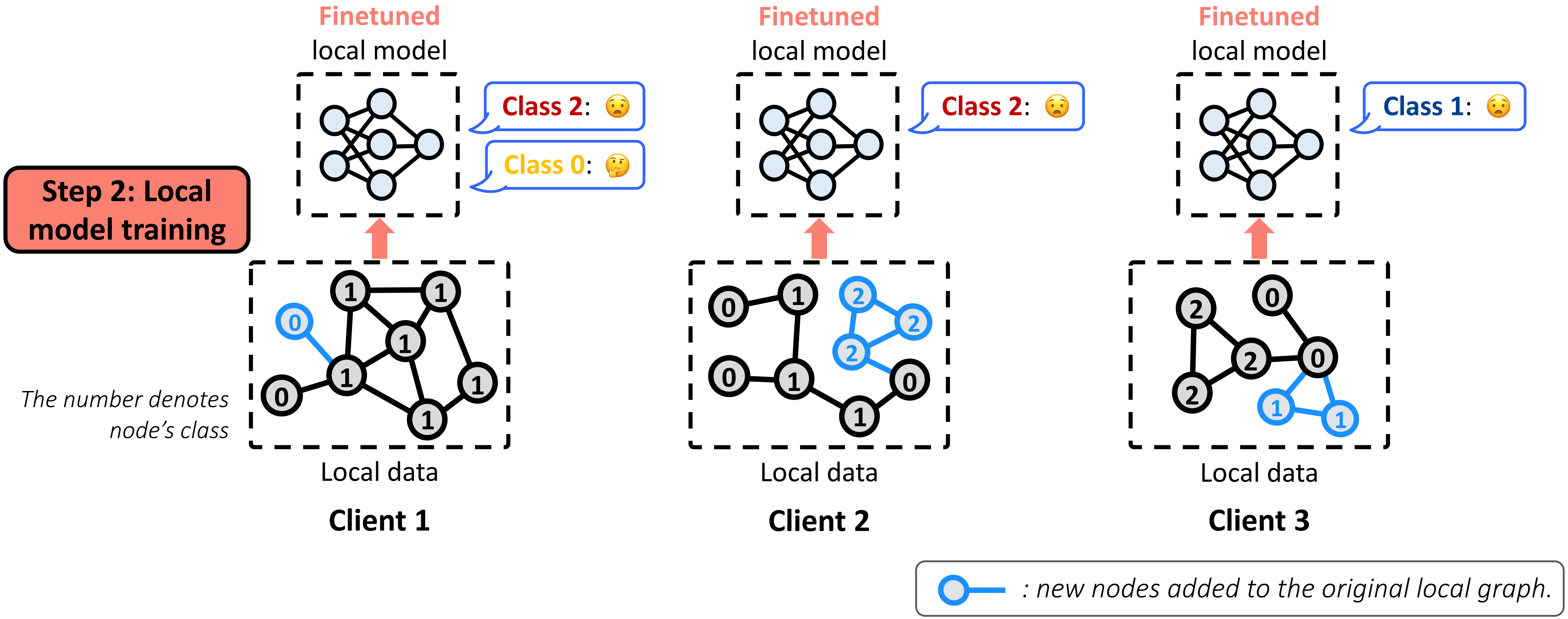
MOTIVATION

- **Graph Federated Learning**



MOTIVATION

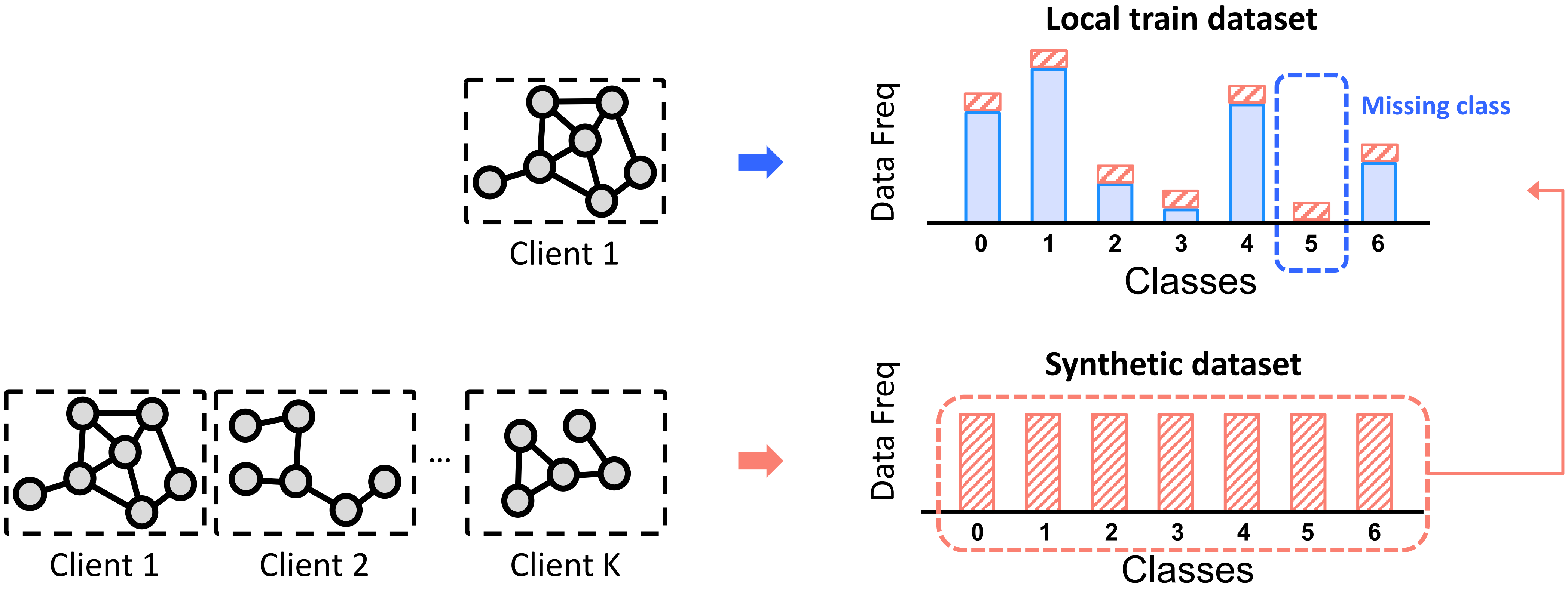
- **Graph Federated Learning**



The mutable nature of graph data easily leads to **shifts in label and structural distribution**

MAIN CHALLENGES

- **Alleviating the Local Overfitting Problem (i.e., Local Generalization)**



1. Generate synthetic training data from **knowledge aggregated from the clients.**
2. Then, **generalize the absent knowledge (e.g., minority class, missing class)** within each local dataset.

MAIN CHALLENGES

- **Alleviating the Local Overfitting Problem (i.e., Local Generalization)**

Local train dataset

Main challenges our work, FedLoG, addresses:

- **C1. Which data across clients should be aggregated** to ensure reliability?
- **C2.** How can data from other clients be utilized **without compromising privacy?**

1. Generate synthetic training data from **knowledge aggregated from the clients.**
2. Then, **generalize the absent knowledge (e.g., minority class, missing class)** within each local dataset.

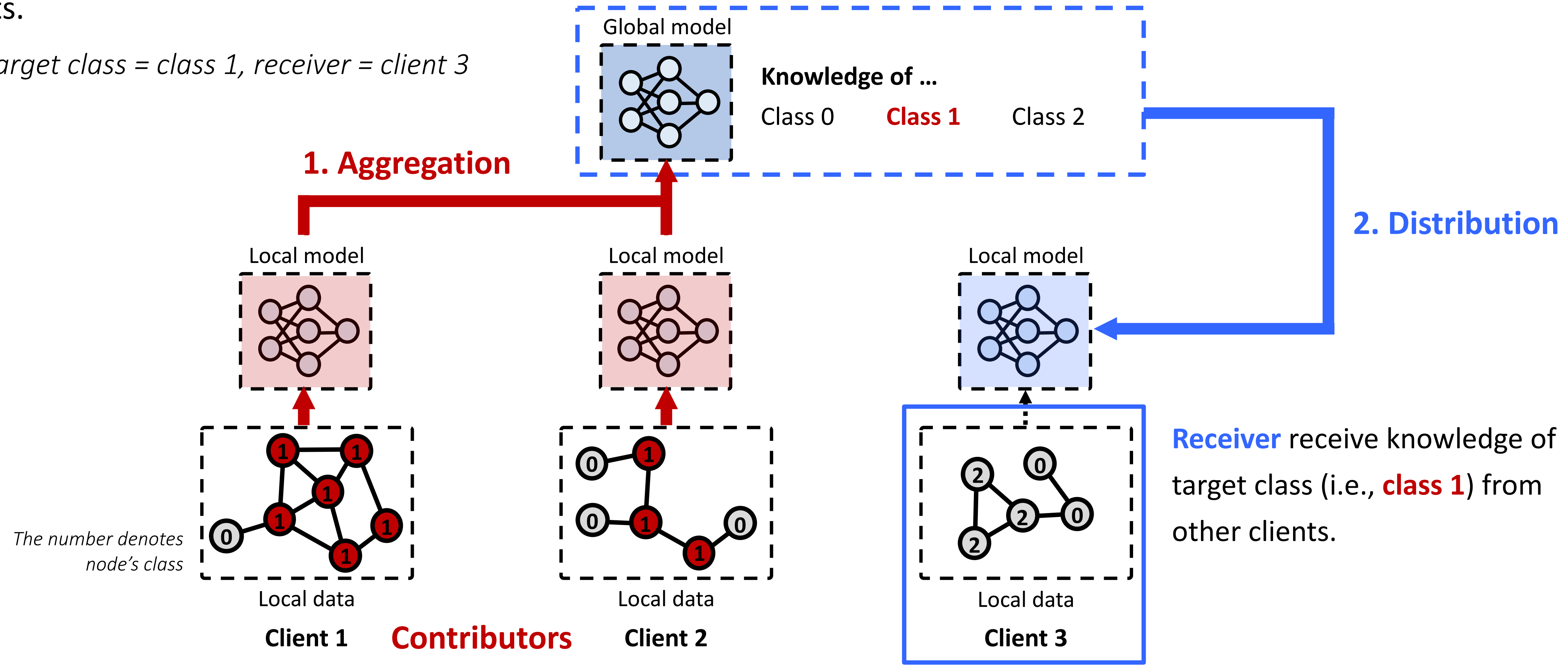
C1. WHICH DATA ARE RELIABLE TO BE AGGREGATED?

- **Performance Influence of Knowledge Acquired from Other Clients**

Data Reliability: The accuracy and consistency of information from decentralized nodes.

→ We measured the target class accuracy of a client (receiver) receiving information (i.e., weights) from other clients.

e.g., target class = class 1, receiver = client 3

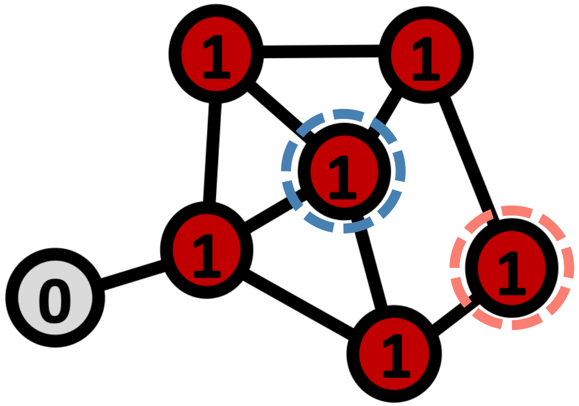


Receiver receive knowledge of target class (i.e., **class 1**) from other clients.

C1. WHICH DATA ARE RELIABLE TO BE AGGREGATED?

- **Performance Influence of Knowledge Acquired from Other Clients**

Contributors’ knowledge acquired from …



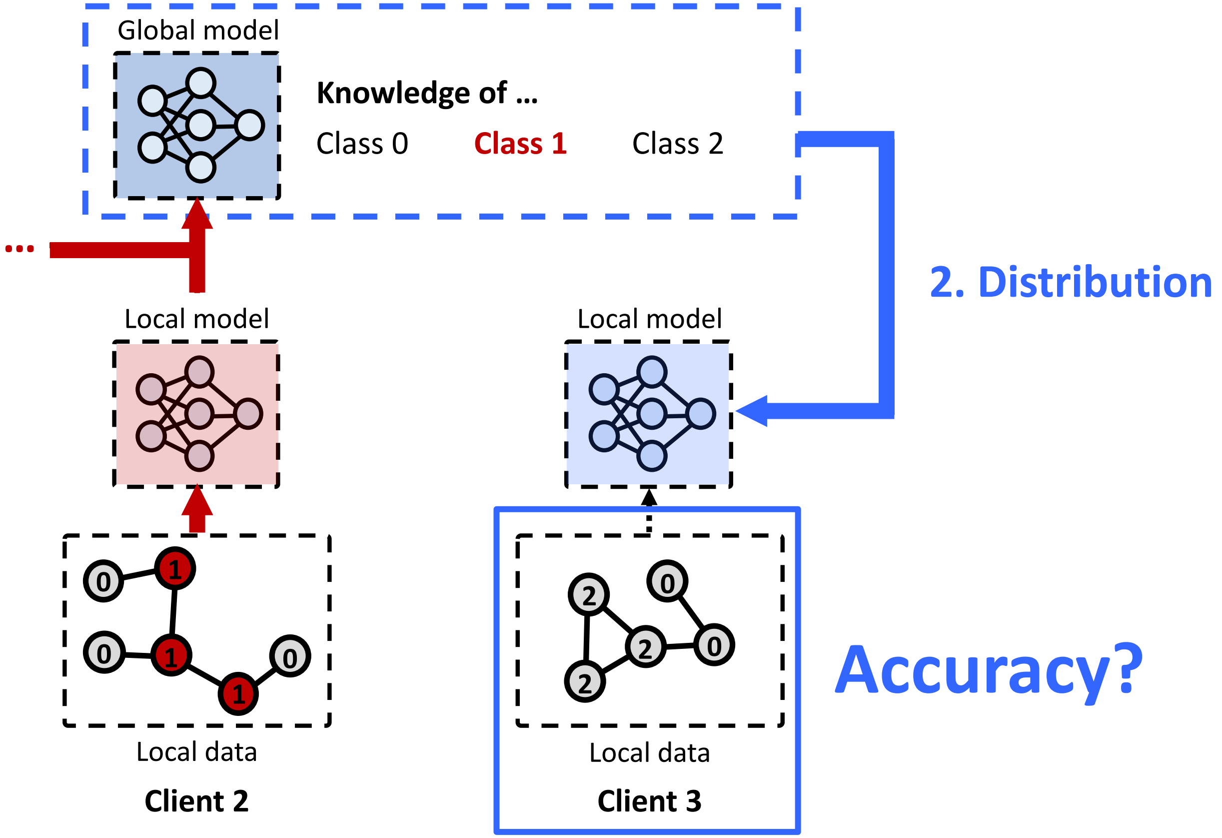
In terms of ‘Node Degree’,

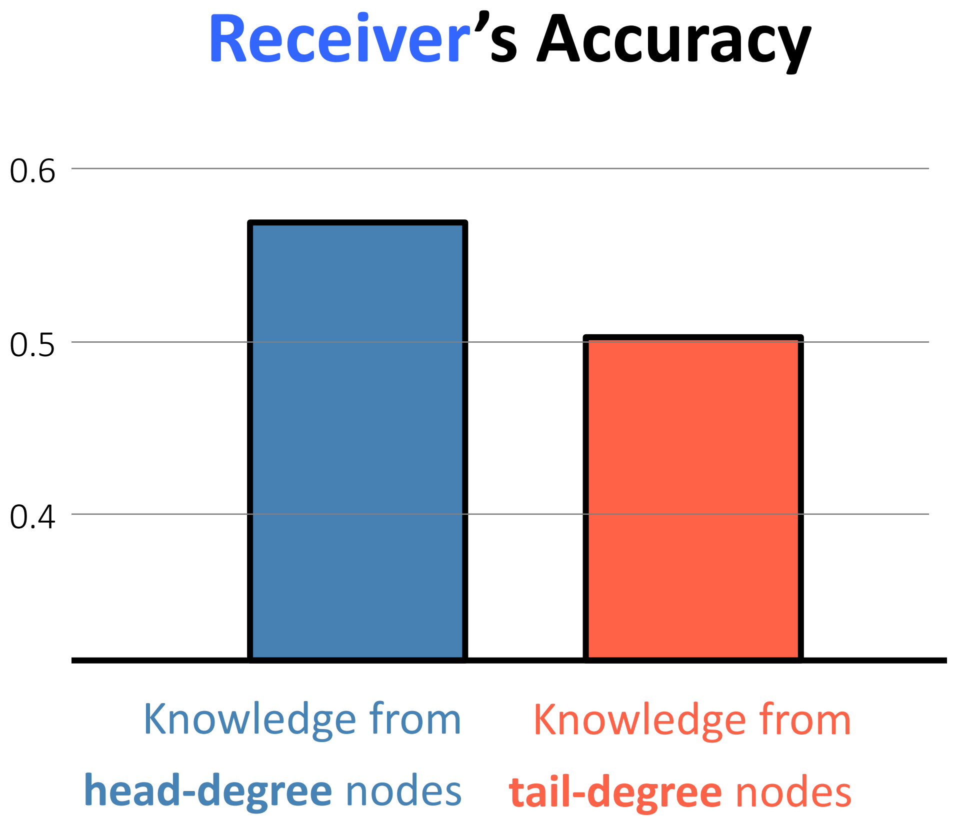
1. Head Degree Nodes

2. Tail Degree Nodes

C1. WHICH DATA ARE RELIABLE TO BE AGGREGATED?

- **Performance Influence of Knowledge Acquired from Other Clients**

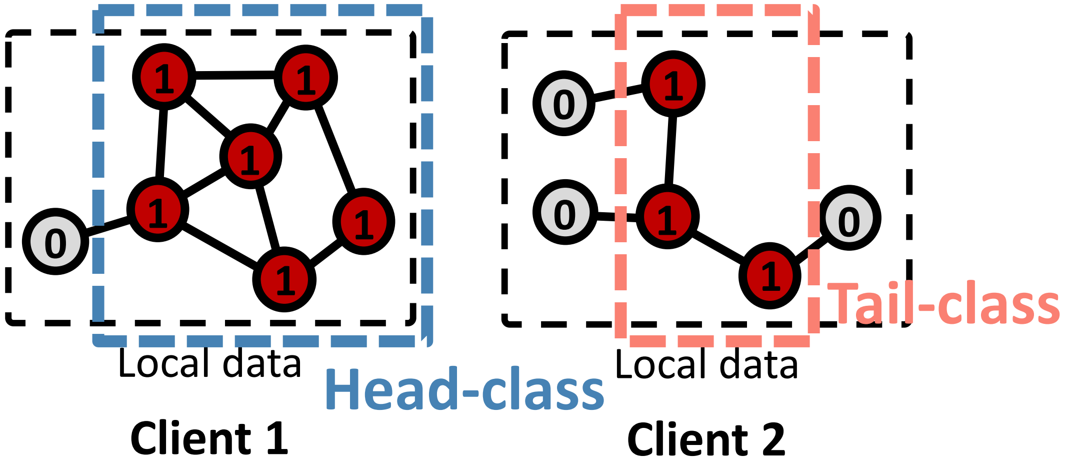




C1. WHICH DATA ARE RELIABLE TO BE AGGREGATED?

- **Performance Influence of Knowledge Acquired from Other Clients**

Contributors' Knowledge acquired from …



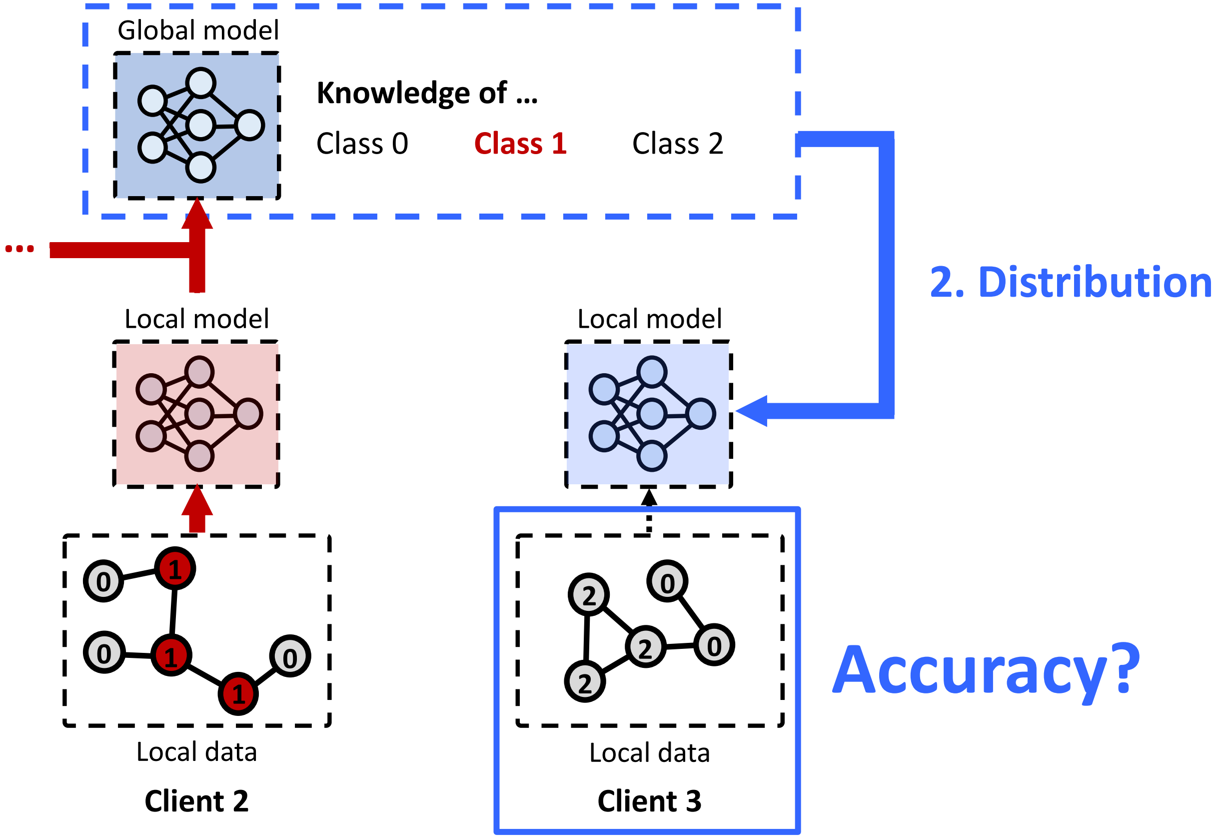
In terms of 'Class',

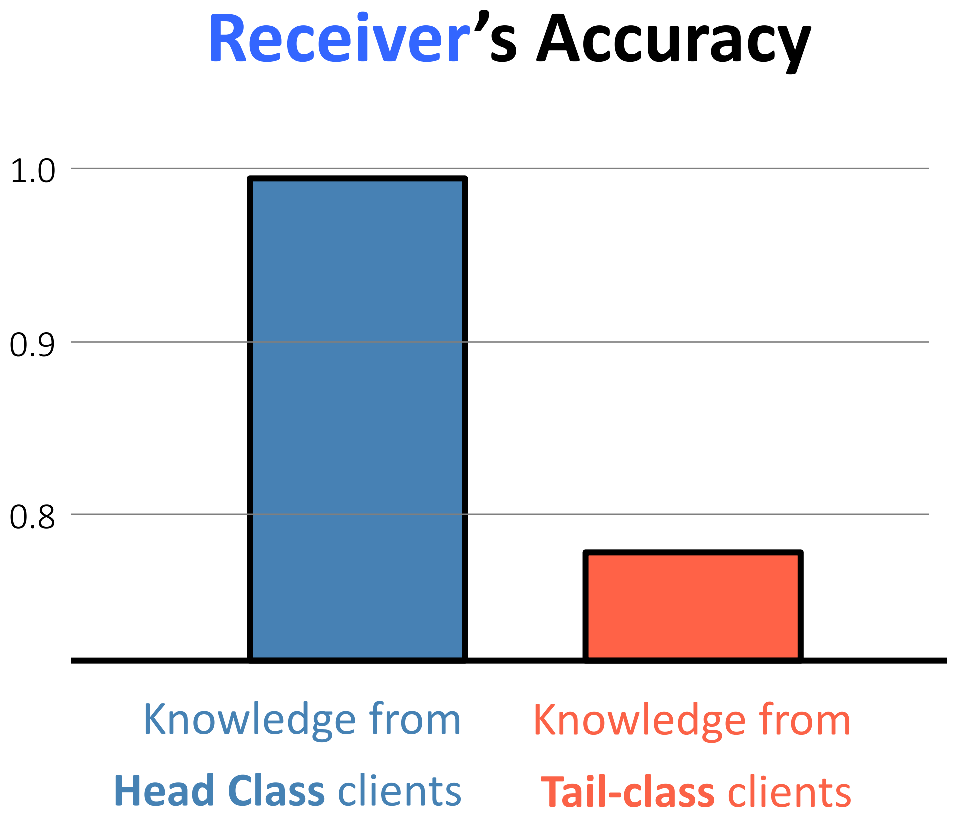
1. Clients possessing the **Head Class**

2. Clients possessing the **Tail Class**

C1. WHICH DATA ARE RELIABLE TO BE AGGREGATED?

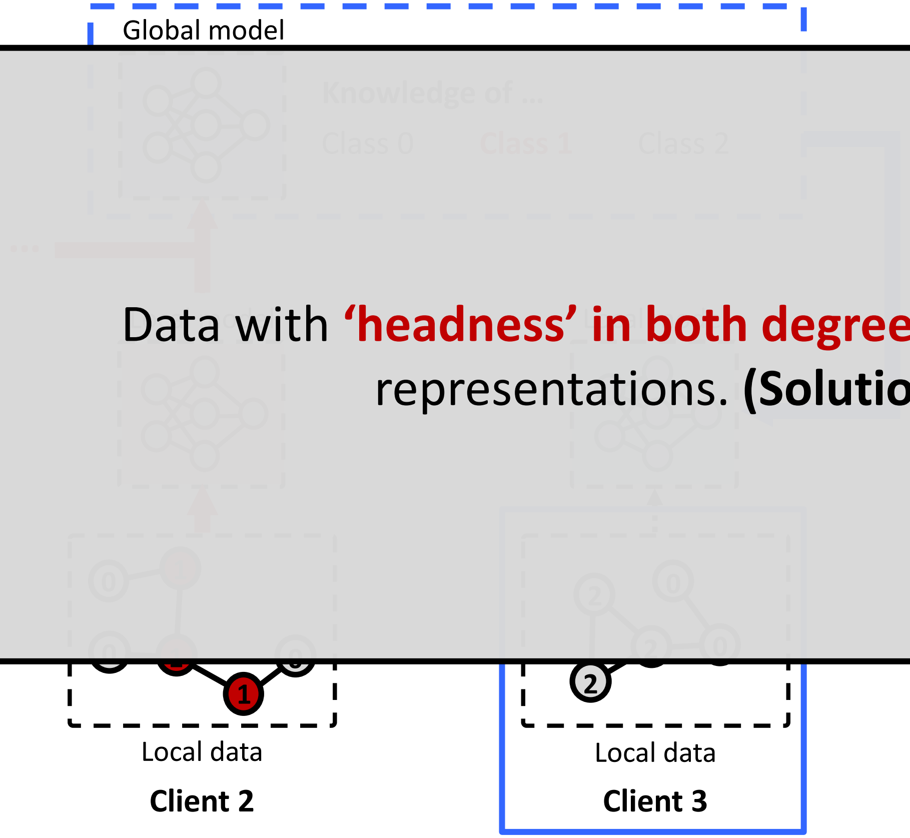
- **Performance Influence of Knowledge Acquired from Other Clients**

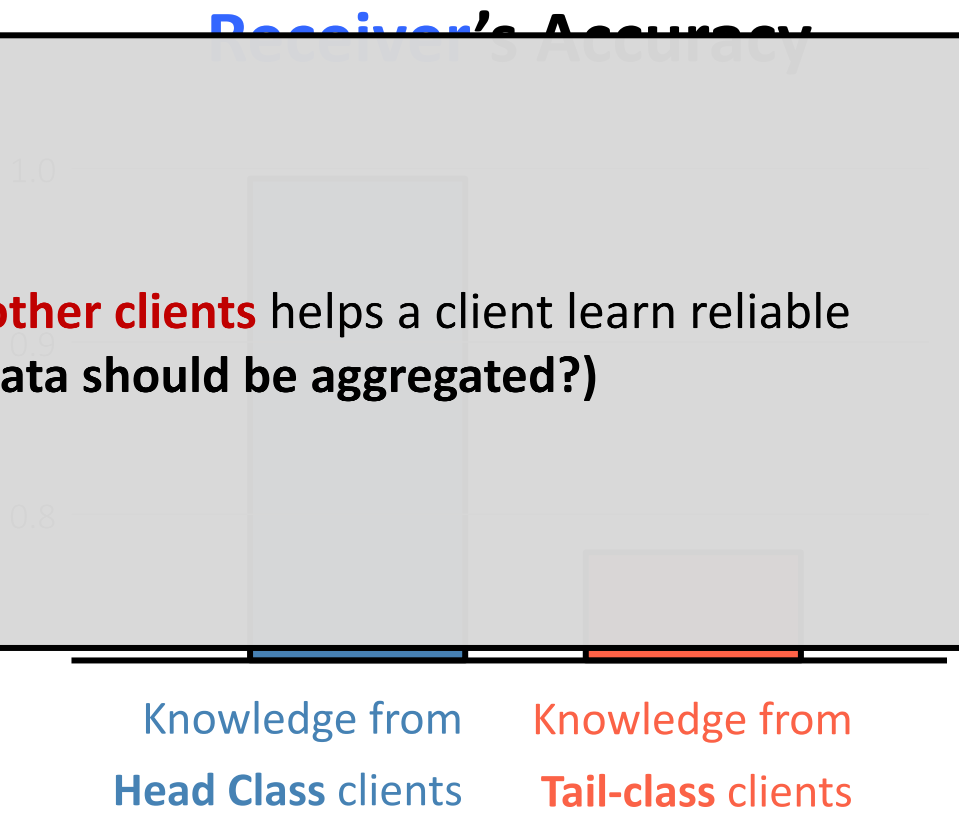




C1. WHICH DATA ARE RELIABLE TO BE AGGREGATED?

- **Performance Influence of Knowledge Acquired from Other Clients**

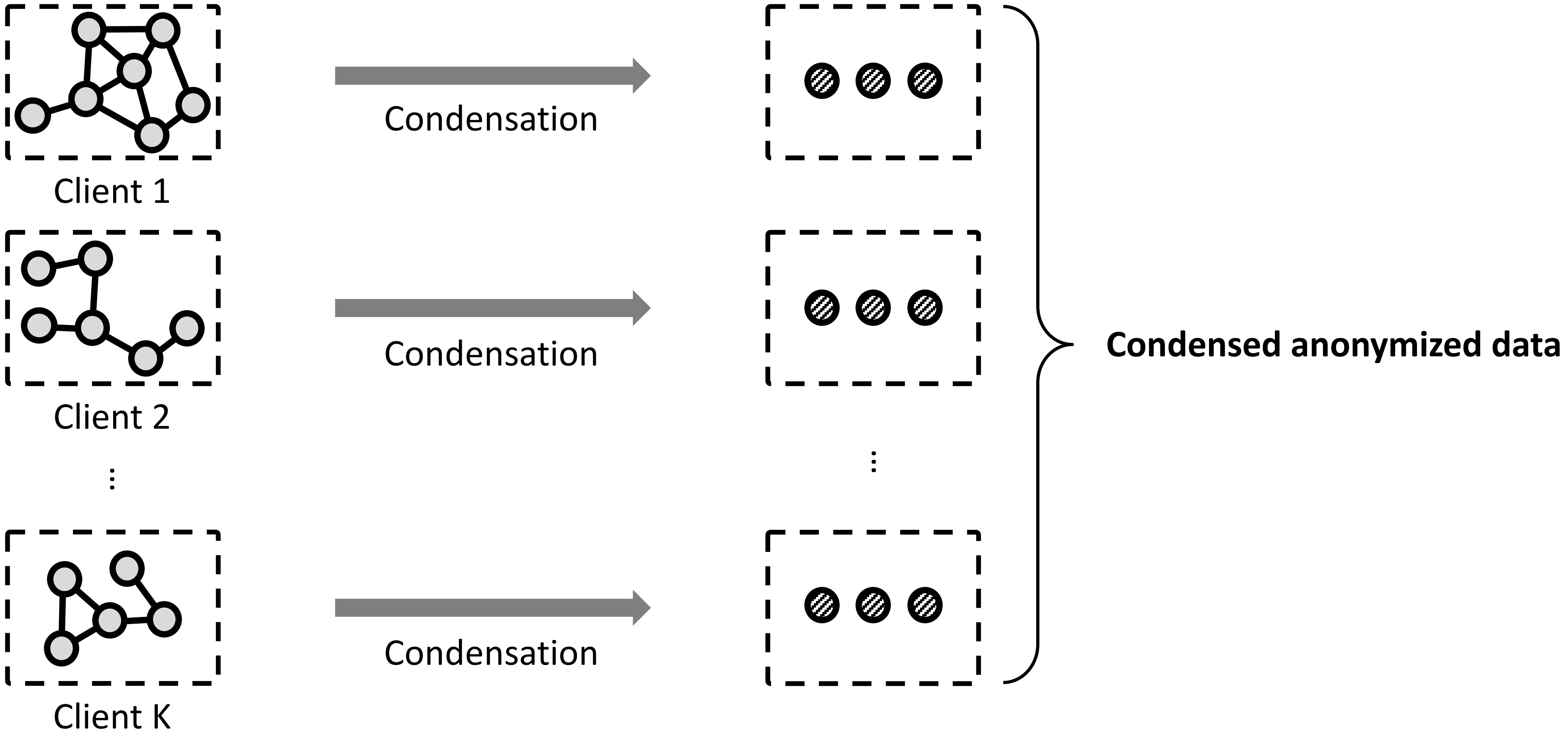




Data with **'headness' in both degree and class from other clients** helps a client learn reliable representations. **(Solution to C1: Which data should be aggregated?)**

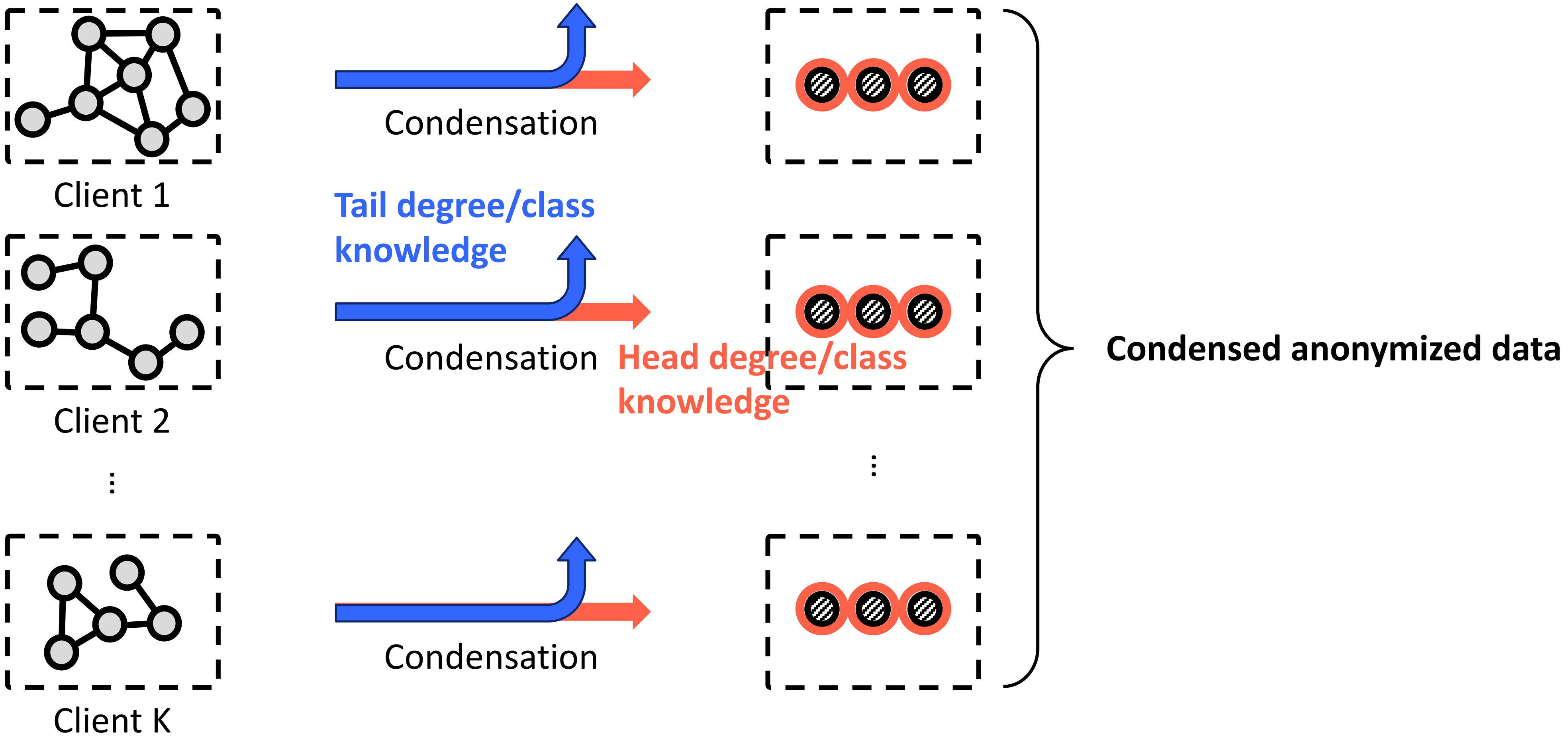
C2. HOW CAN DATA FROM OTHER CLIENTS BE UTILIZED WITHOUT COMPROMISING PRIVACY?

- **Data Condensation for Anonymizing Local Data**



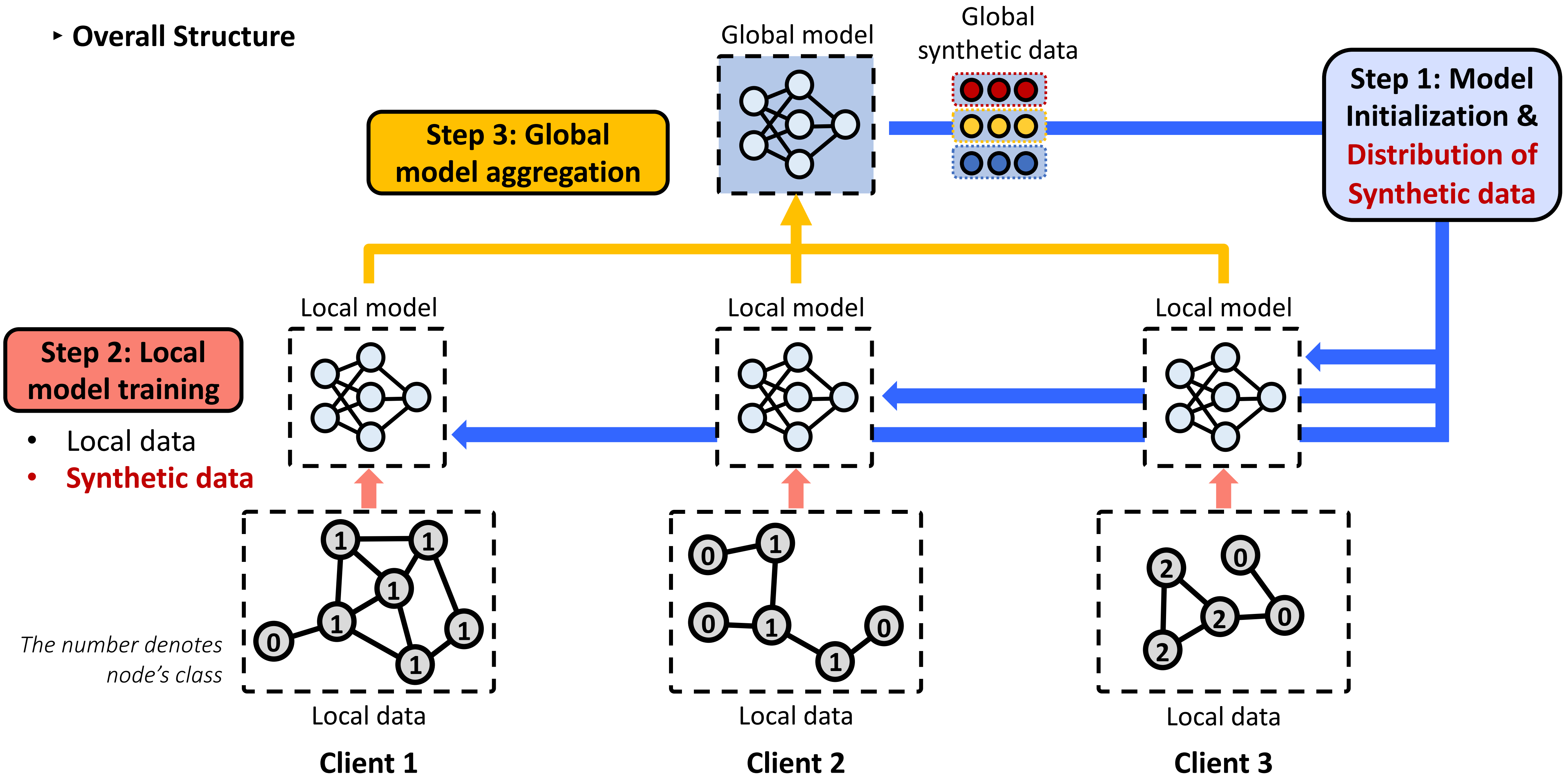
C2. HOW CAN DATA FROM OTHER CLIENTS BE UTILIZED WITHOUT COMPROMISING PRIVACY?

- Data Condensation for Anonymizing Local Data



METHODOLOGY

- Overall Structure

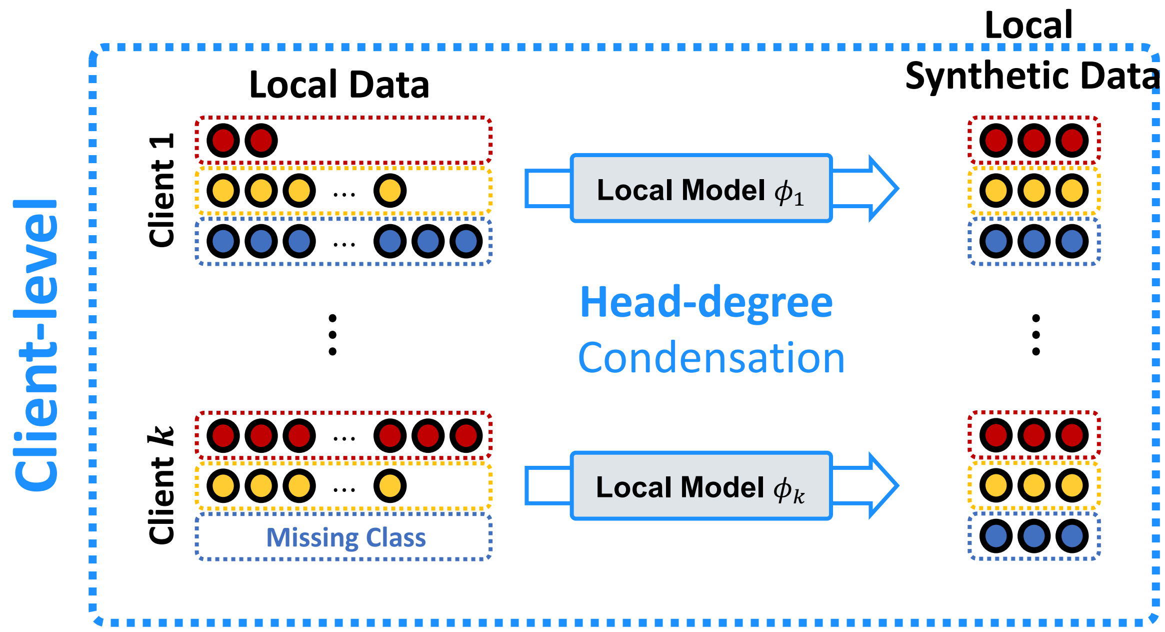


METHODOLOGY

- **Overall Structure**

1. Generating Global Synthetic Data
2. Learning with the Global Synthetic Data (i.e., Local Generalization)

1. Generating Global Synthetic Data

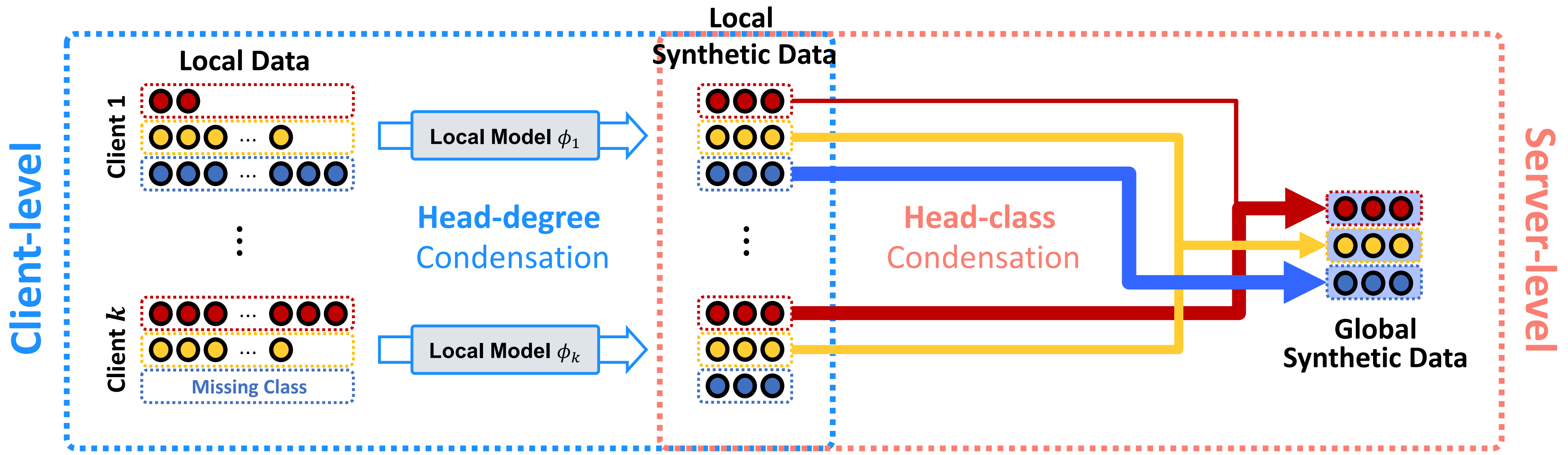


METHODOLOGY

- **Overall Structure**

1. Generating Global Synthetic Data
2. Learning with the Global Synthetic Data (i.e., Local Generalization)

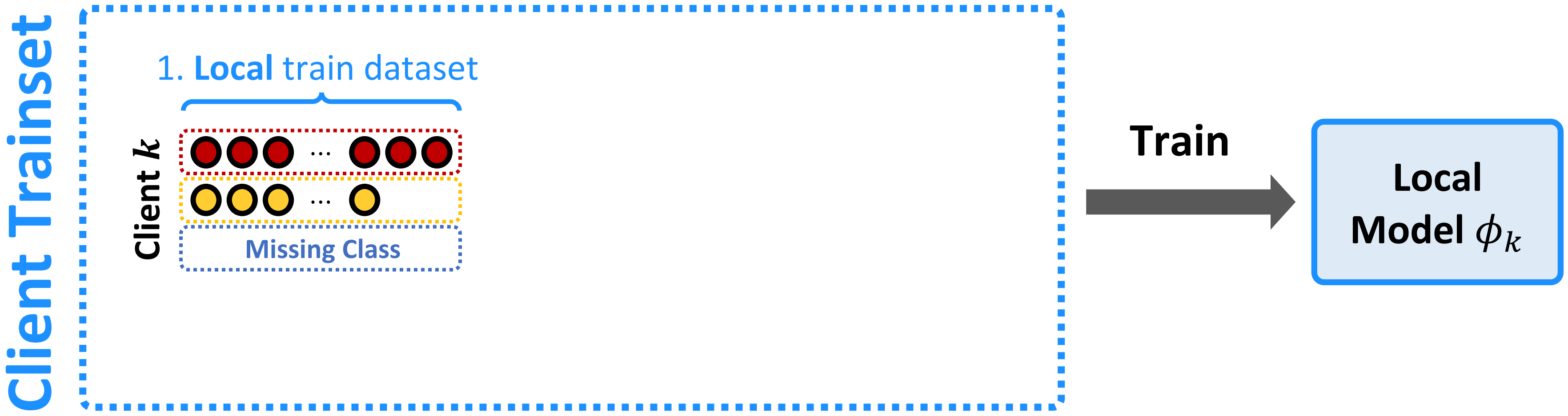
1. Generating Global Synthetic Data



METHODOLOGY

- **Overall Structure**

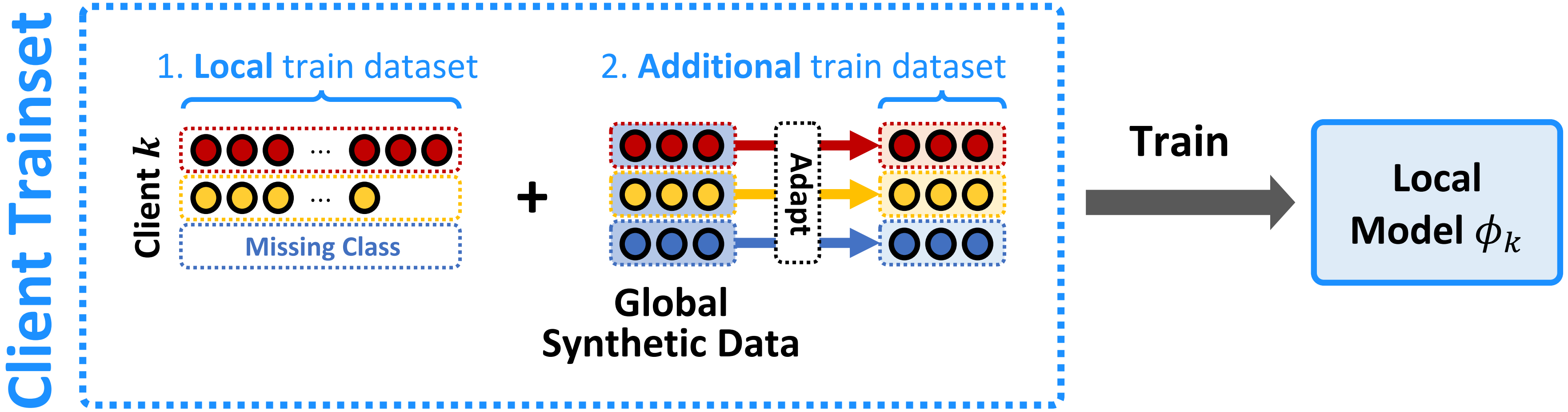
2. Learning with the Global Synthetic Data (i.e., Local Generalization)



METHODOLOGY

- **Overall Structure**

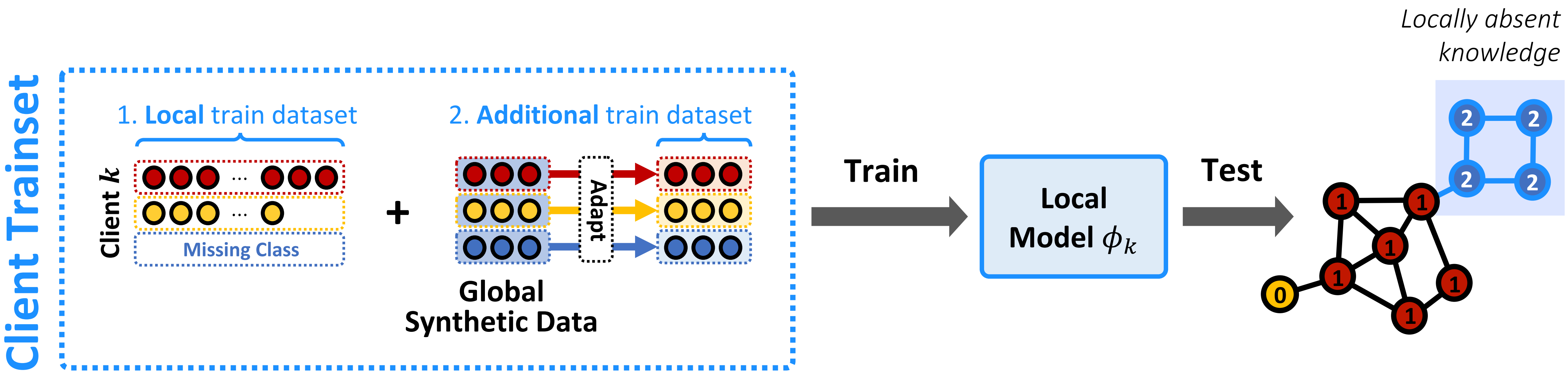
2. Learning with the Global Synthetic Data (i.e., Local Generalization)



METHODOLOGY

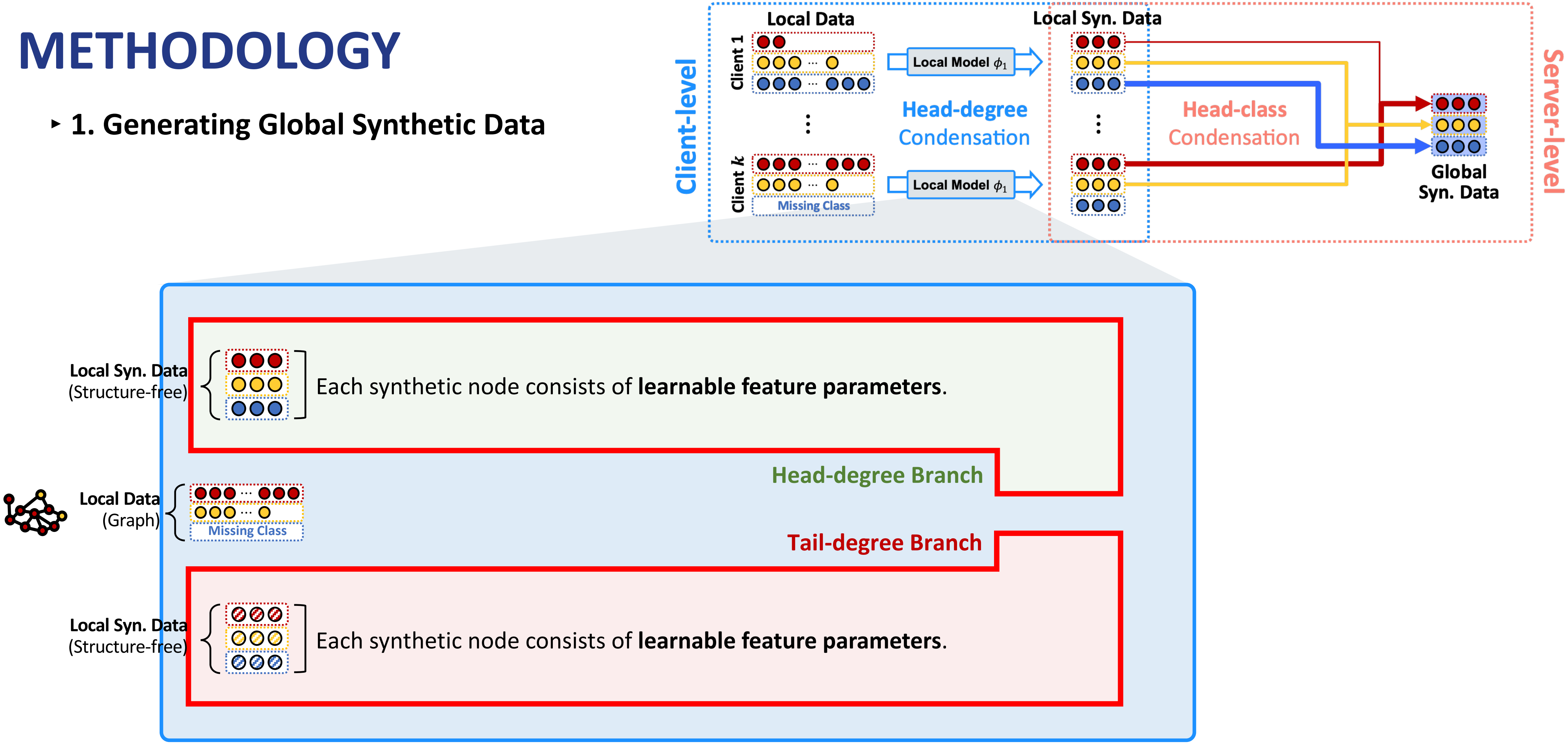
- **Overall Structure**

2. Learning with the Global Synthetic Data (i.e., Local Generalization)



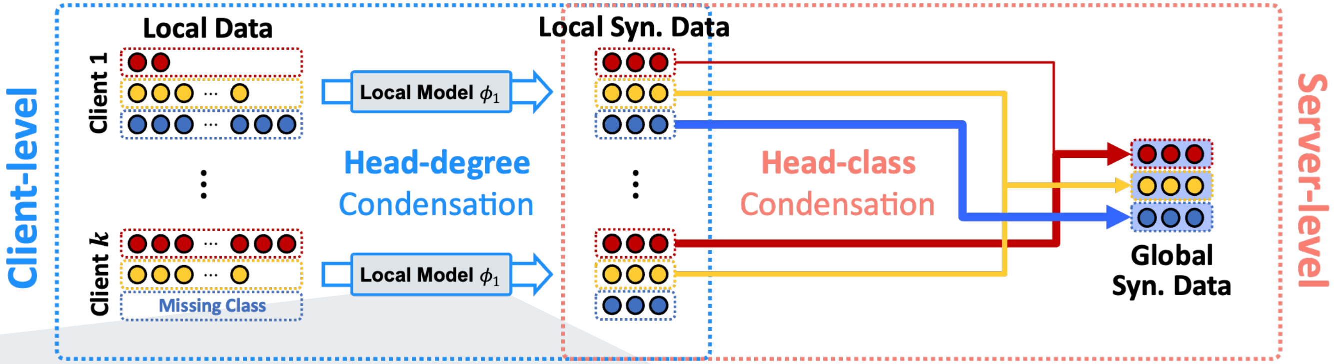
METHODOLOGY

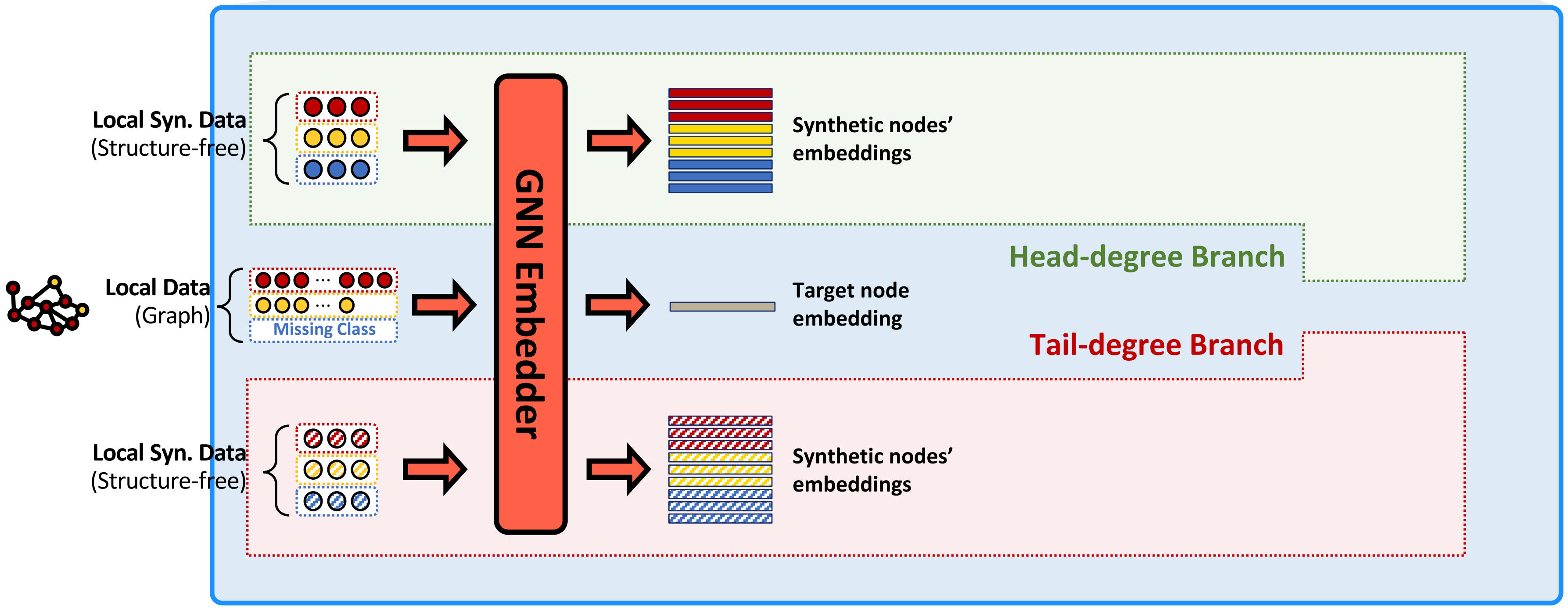
- 1. Generating Global Synthetic Data



METHODOLOGY

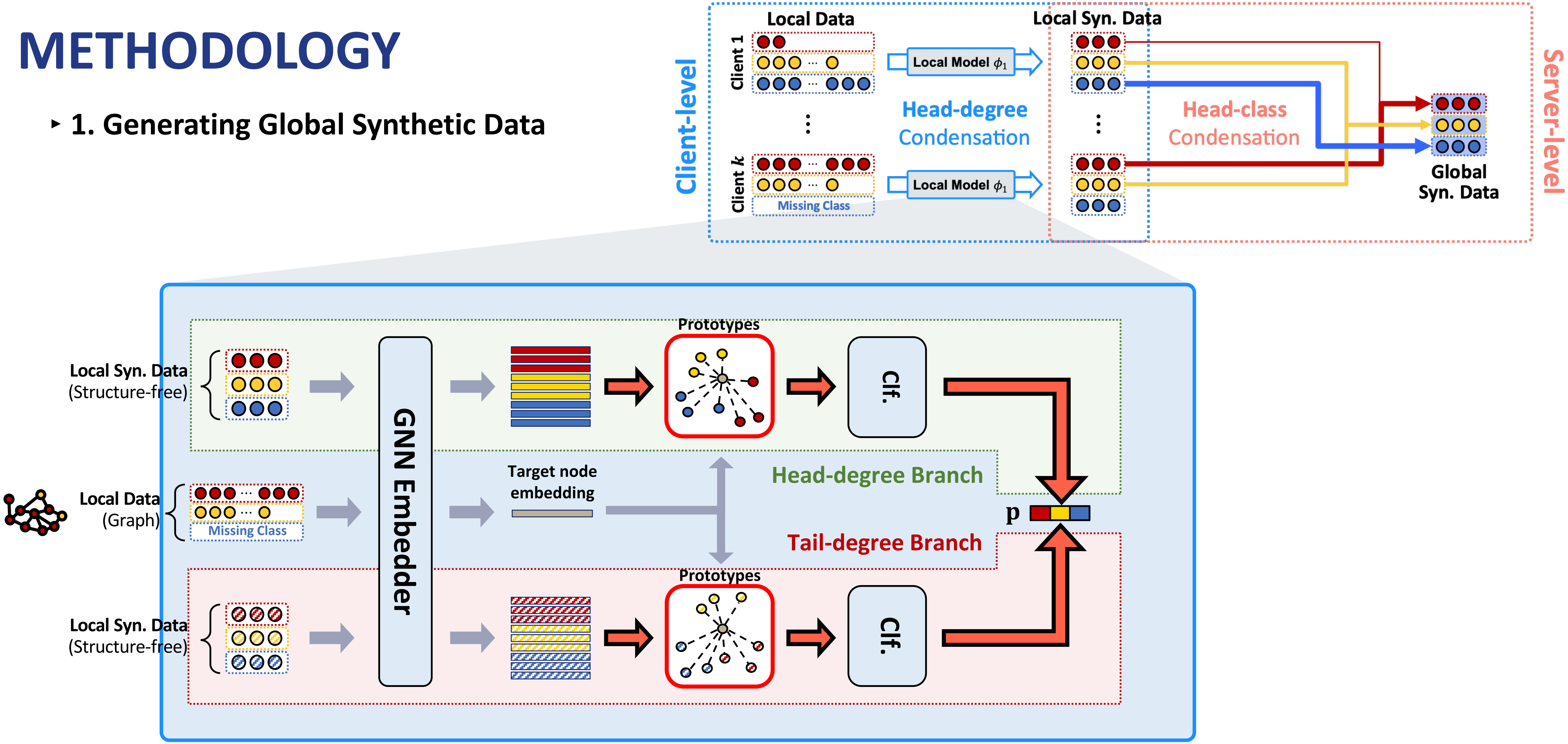
- 1. Generating Global Synthetic Data





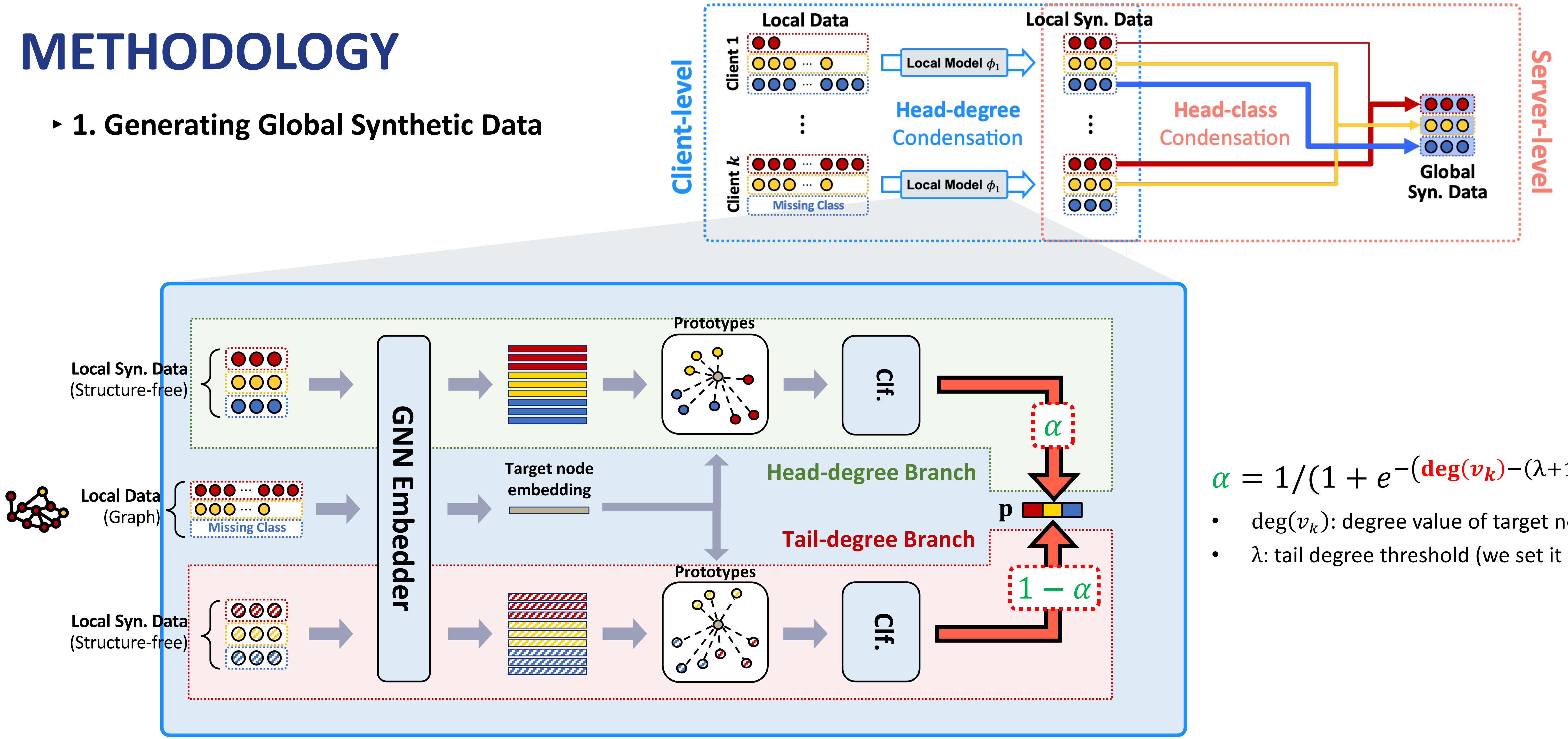
METHODOLOGY

- 1. Generating Global Synthetic Data



METHODOLOGY

- 1. Generating Global Synthetic Data

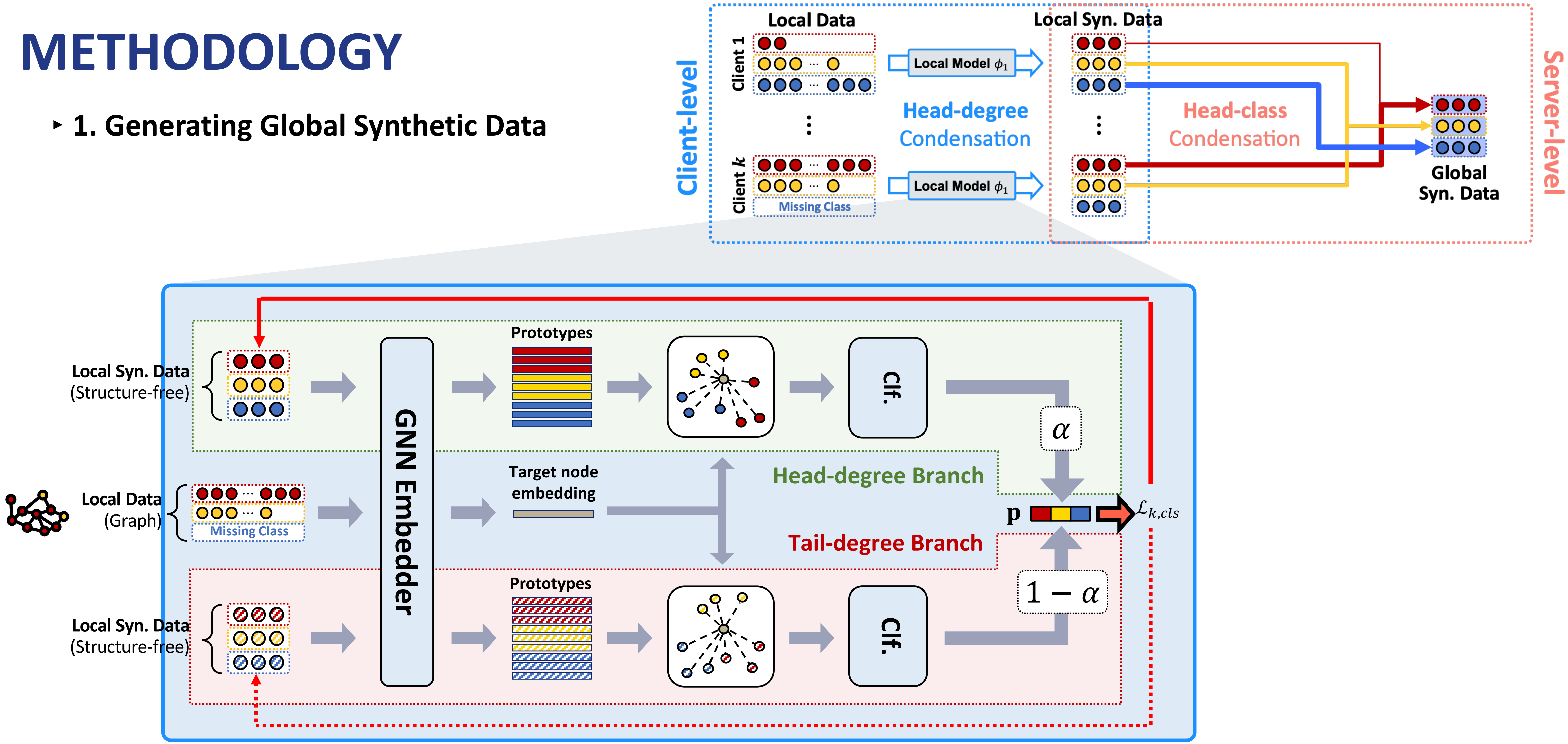


$$\alpha = 1/(1+e^{-(\mathbf{deg}(v_k)-(\lambda+1))})$$

- $\deg(v_k)$: degree value of target node
- λ: tail degree threshold (we set it to 3)

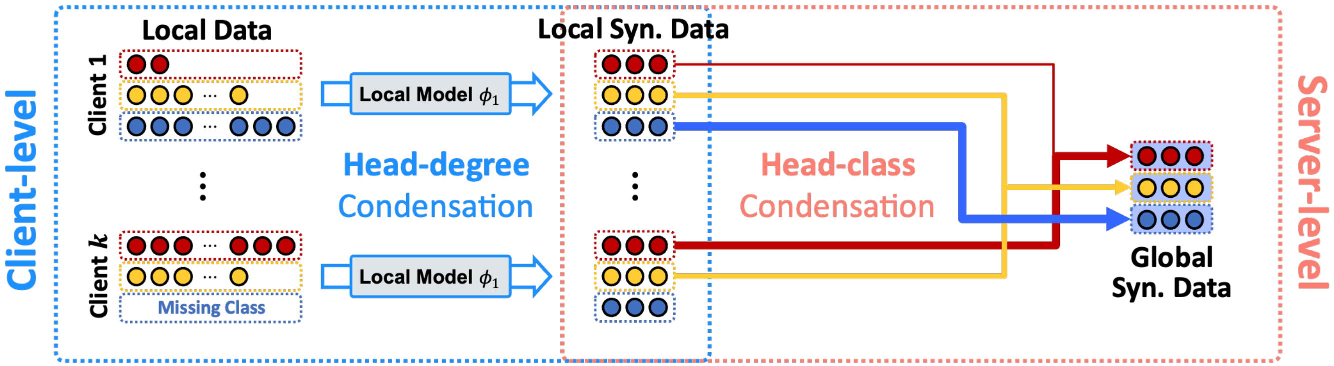
METHODOLOGY

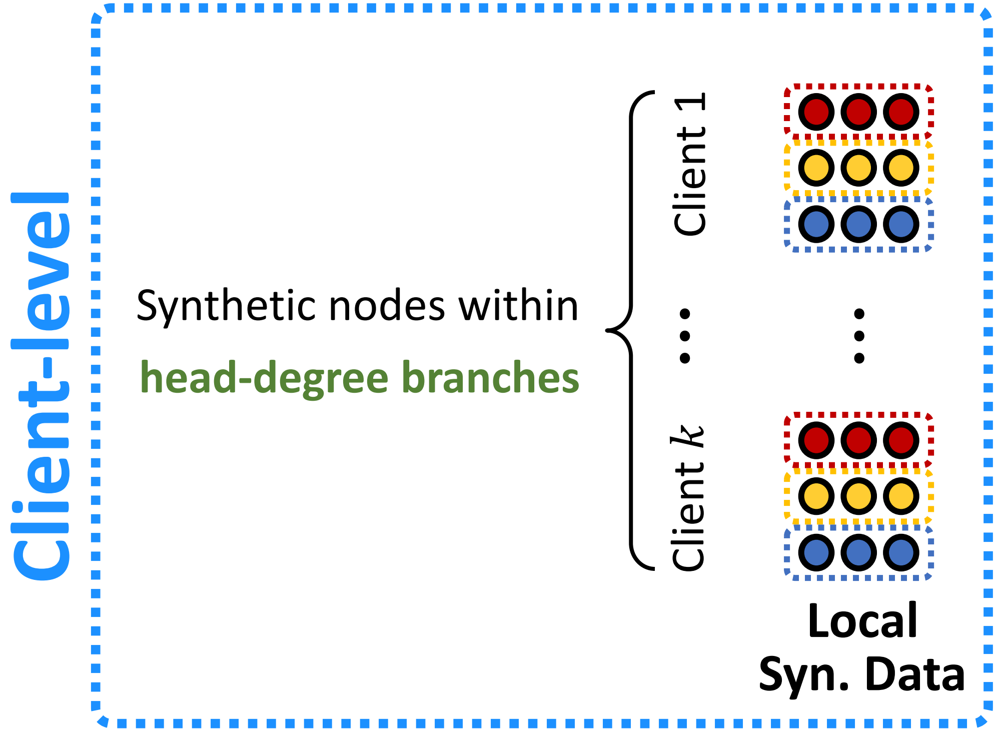
- 1. Generating Global Synthetic Data



METHODOLOGY

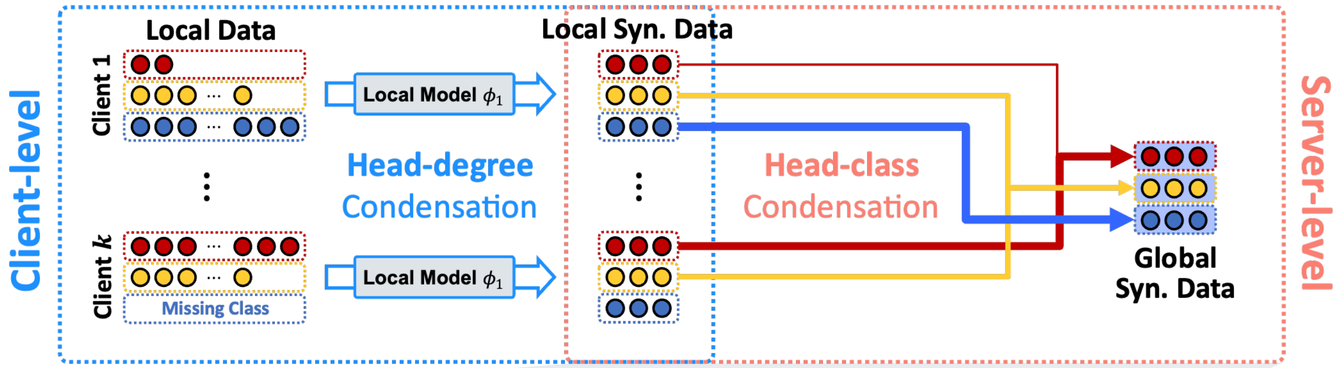
- 1. Generating Global Synthetic Data

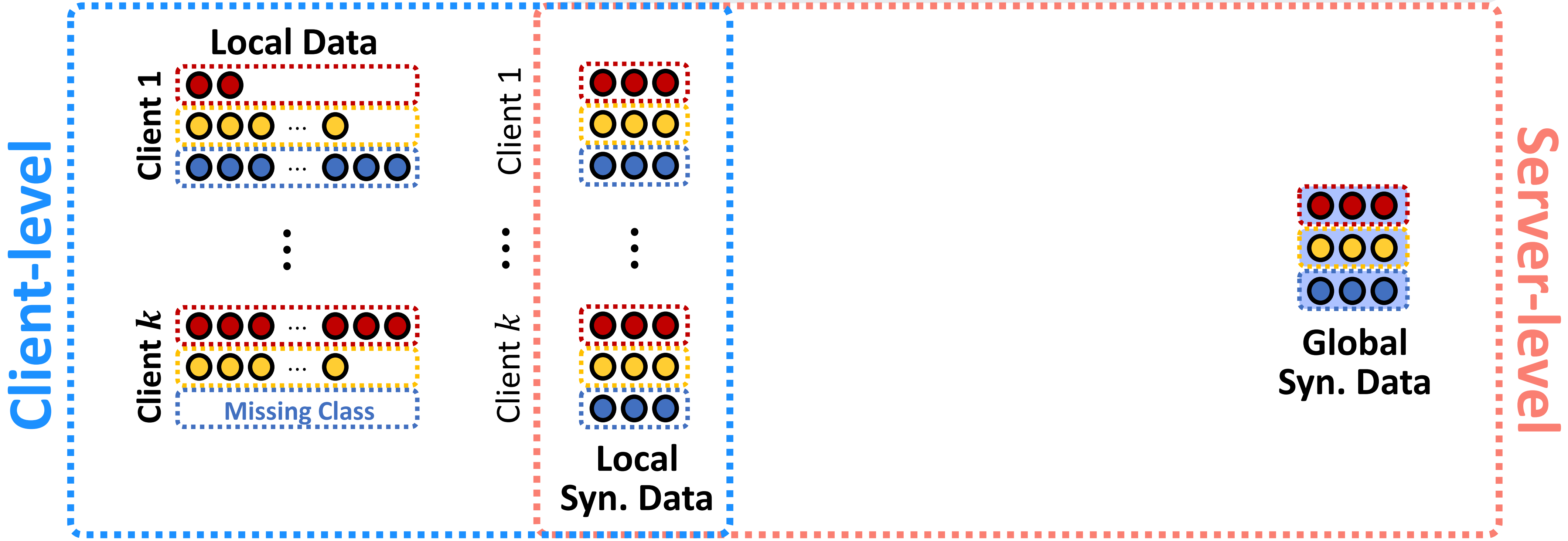




METHODOLOGY

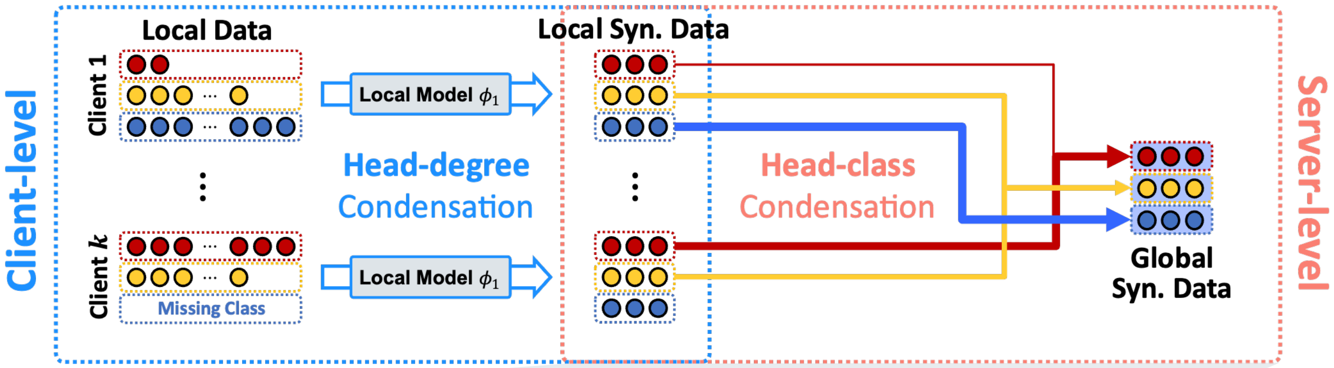
- 1. Generating Global Synthetic Data

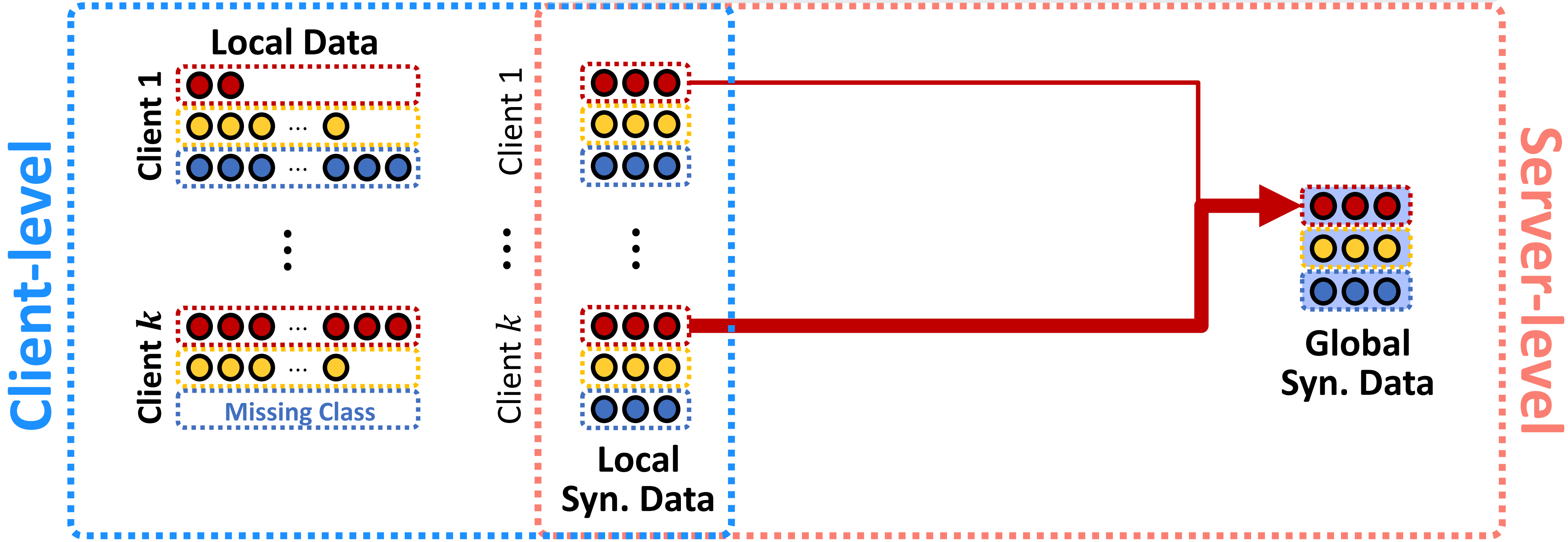




METHODOLOGY

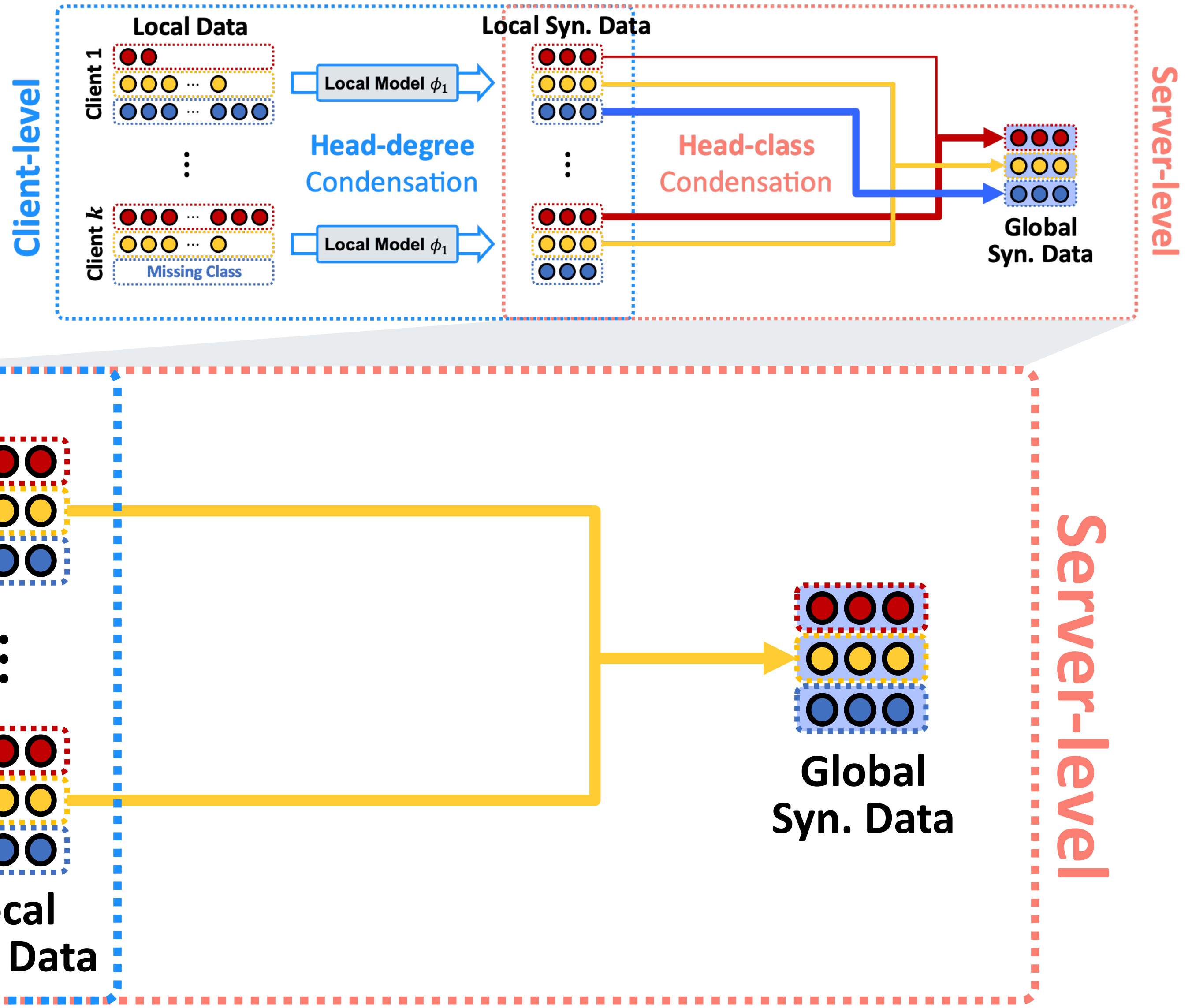
- 1. Generating Global Synthetic Data





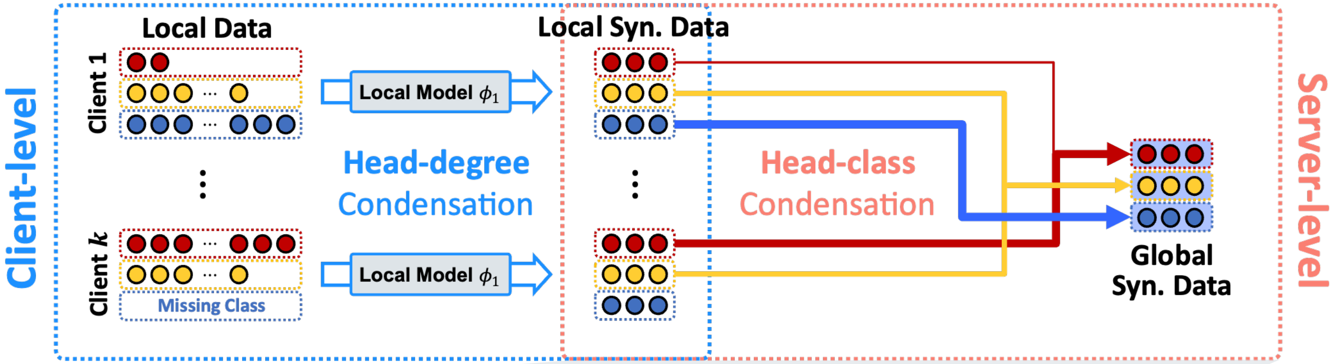
METHODOLOGY

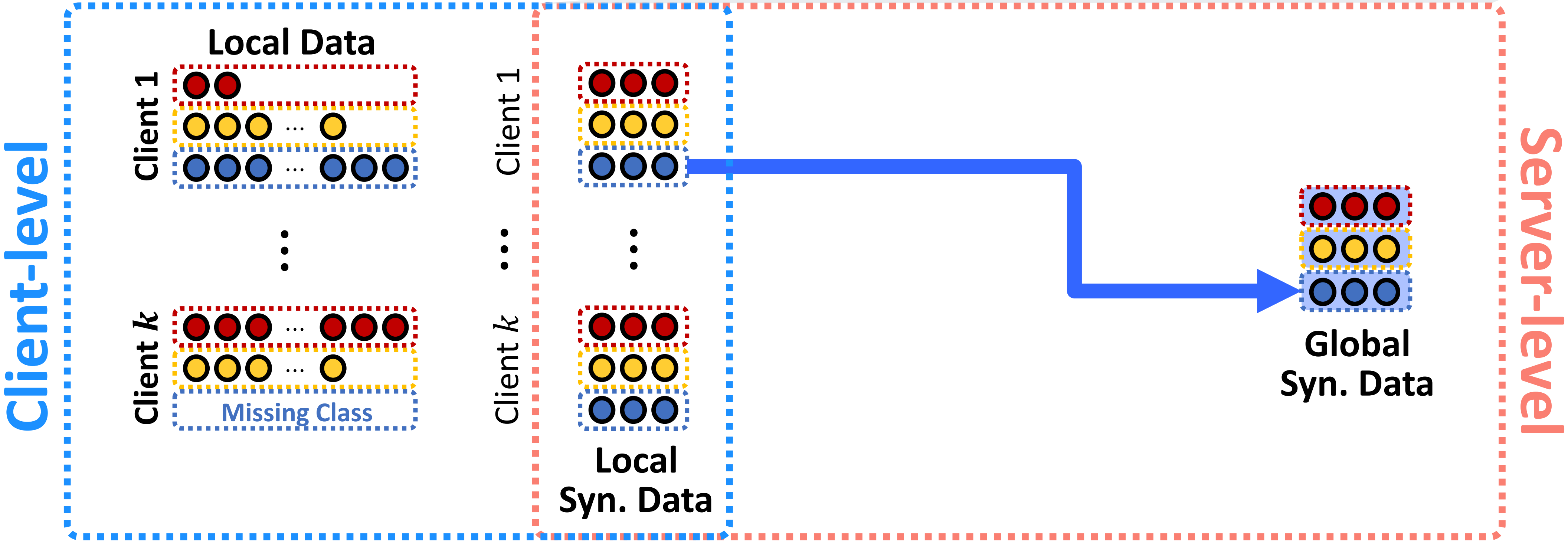
- 1. Generating Global Synthetic Data



METHODOLOGY

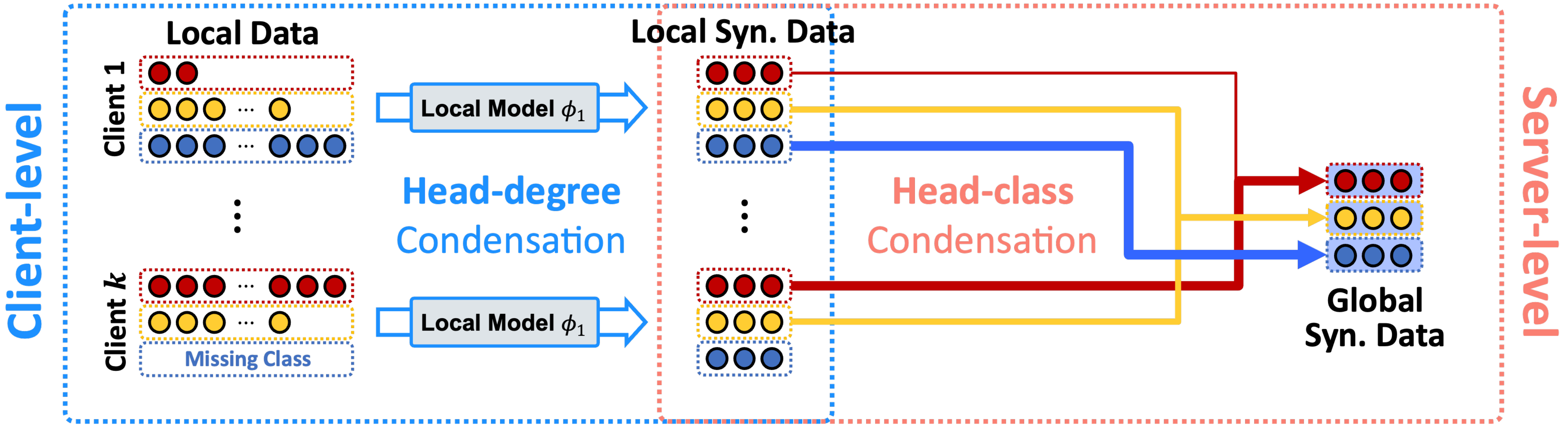
- 1. Generating Global Synthetic Data





METHODOLOGY

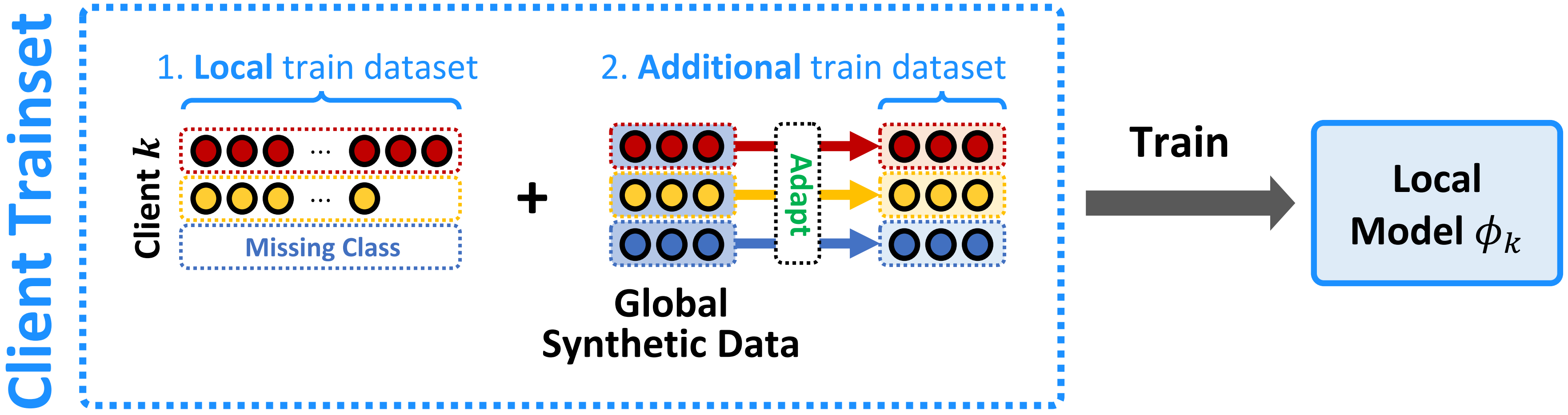
- 1. Generating Global Synthetic Data



As a result, the generated global synthetic data condense
the knowledge of head-degree and head-class nodes across all clients.

METHODOLOGY

- **2. Learning with the Global Synthetic Data (i.e., Local Generalization)**



Since each client has different locally absent knowledge,

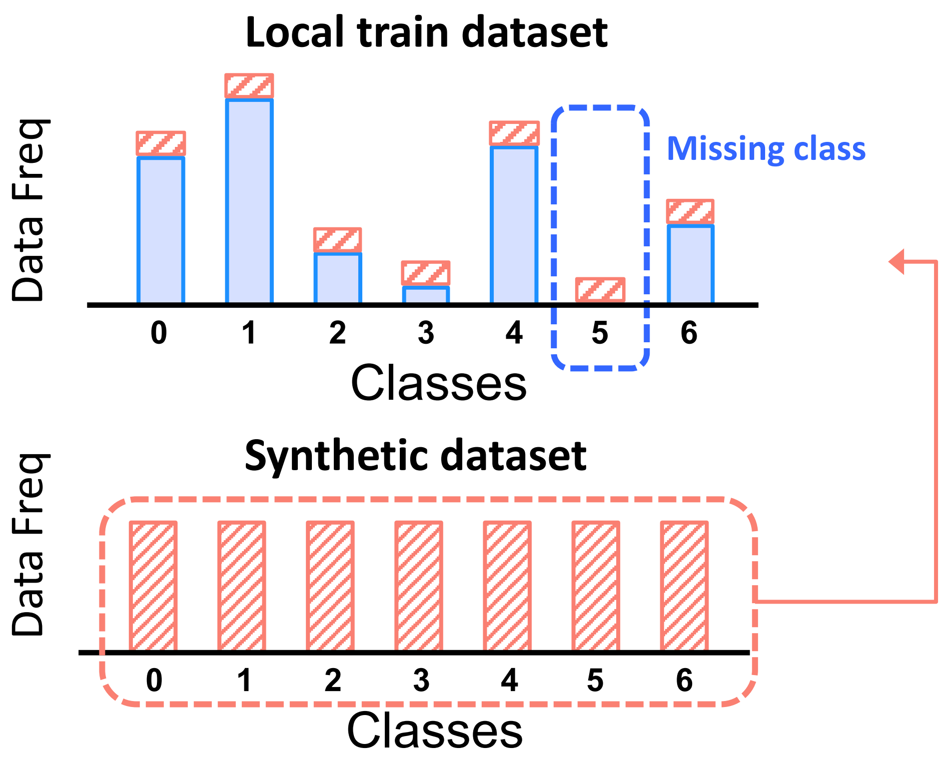
a local model first adaptively customizes **the global synthetic data** to fit the current state.

- Feature scaling
- Prompt generation

METHODOLOGY

- **2. Learning with the Global Synthetic Data (i.e., Local Generalization)**

Feature Scaling



e.g.,

Class 1 *has strong perturbation,*

Class 5 *has weak perturbation*

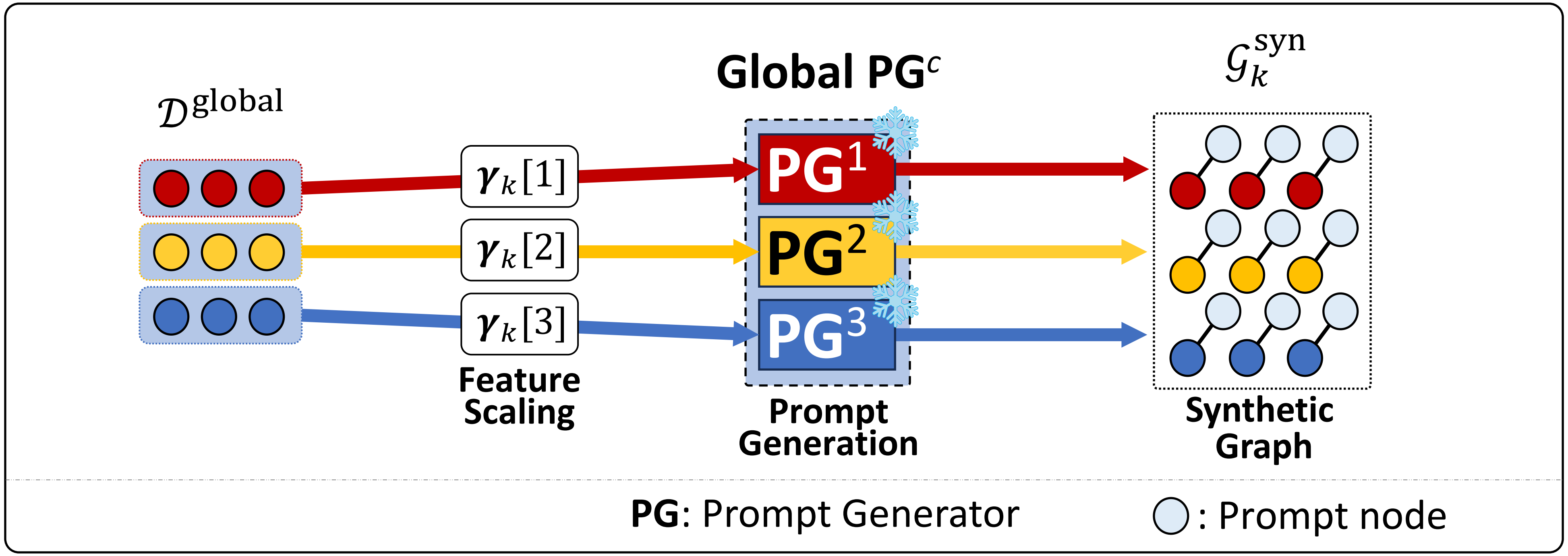
FedLoG amplifies perturbation on the dominant class synthetic data
if the local model’s accuracy for the corresponding class exceeds the threshold.

METHODOLOGY

- **2. Learning with the Global Synthetic Data (i.e., Local Generalization)**

Prompt Generation

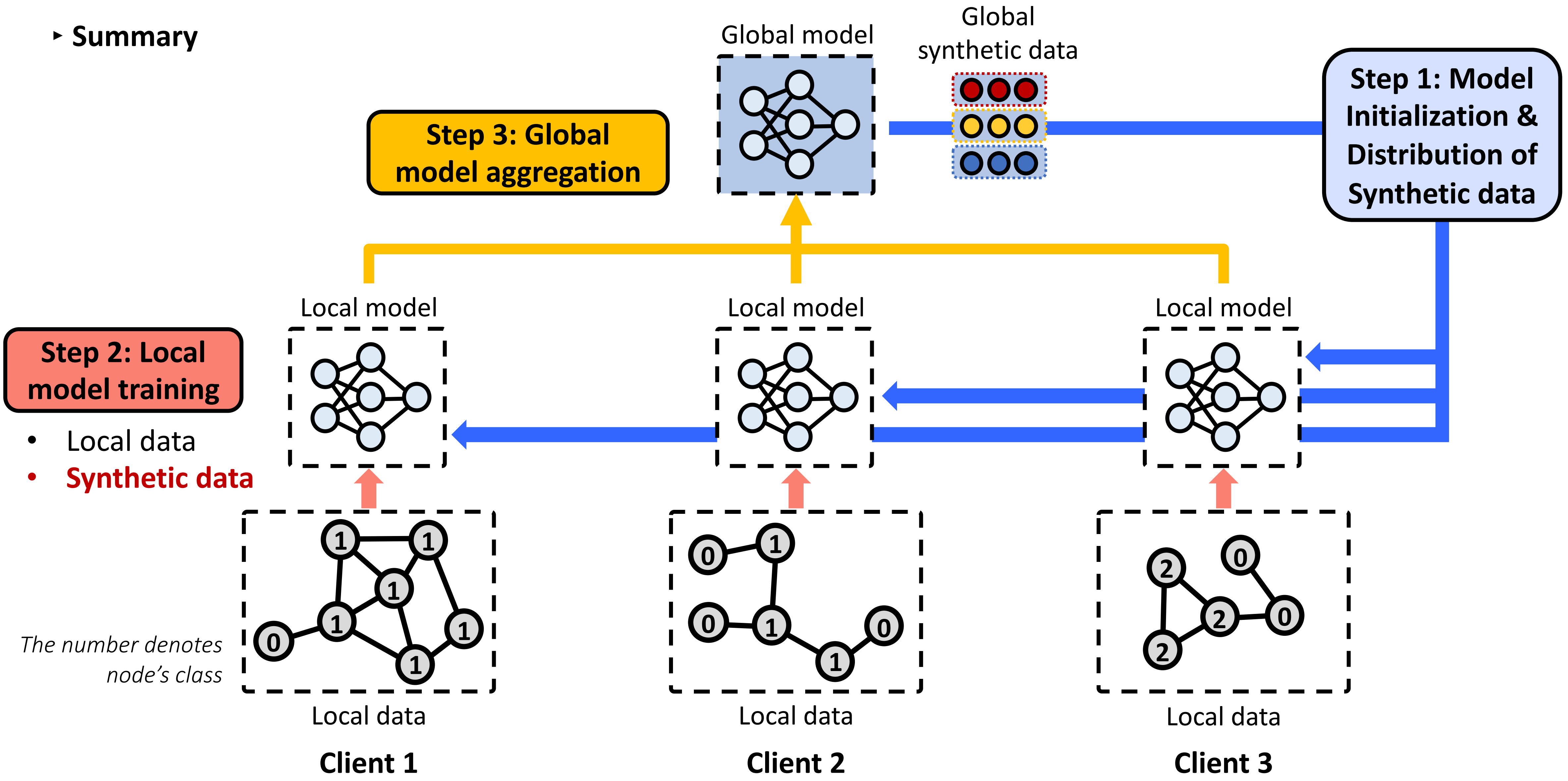
Note that global synthetic nodes have only features and no graph structure.



FedLoG generate a prompt node for each synthetic node to help reduce discrepancies in training effects between synthetic and original nodes within the graph structure.

METHODOLOGY

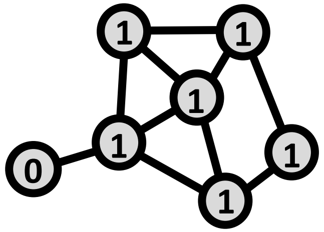
- Summary



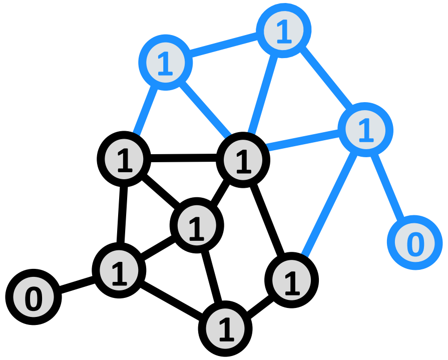
PROPOSED EVALUATION SETTINGS

▸ **Evaluation Settings for Evaluating the Local Generalization Ability**

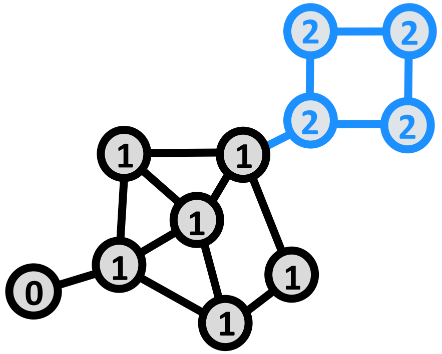
1. Seen Graph



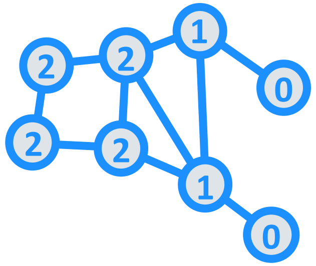
2. Unseen Node



3. Missing Class



4. New Client



* Added during the inference phase

Test nodes from …

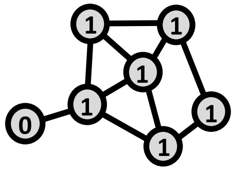
1. Seen Graph	2. Unseen Node	3. Missing Class	4. New Client
· Seen Graph · Seen Class	· Evolved graph · Seen Class	· Evolved graph · Missing Class	· Unseen graph · Seen + Missing Class

We also propose four evaluation settings to test if the model effectively addresses the **local overfitting problem.**

EXPERIMENTS

- **Model Performance Across Proposed Evaluation Settings**

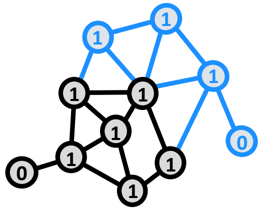
1. Seen Graph



	Cora		
Methods	3 Clients	5 Clients	10 Clients
Local	0.7357 (0.0030)	0.7325 (0.0066)	0.8039 (0.0008)
FedAvg	0.8416 (0.0044)	0.6332 (0.0166)	0.7162 (0.0382)
FedSAGE+	0.7560 (0.0237)	0.4156 (0.0034)	0.3522 (0.1196)
FedGCN	0.8226 (0.0062)	0.8124 (0.0158)	0.7243 (0.0172)
FedPUB	0.8476 (0.0021)	0.8448 (0.0009)	**0.8622** (0.0059)
FedNTD	0.8452 (0.0067)	0.8526 (0.0024)	0.6984 (0.0030)
FedED	0.8542 (0.0084)	0.8398 (0.0024)	0.6779 (0.0343)
FedLoG	**0.8601** (0.0118)	**0.8575** (0.0074)	0.8451 (0.0103)

(a) Seen Graph

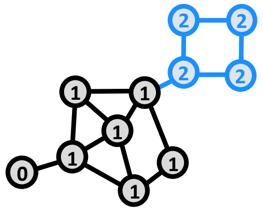
2. Unseen Node



	Cora		
Methods	3 Clients	5 Clients	10 Clients
Local	0.1250 (0.0030)	0.2957 (0.0079)	0.2854 (0.0263)
FedAvg	0.5403 (0.0797)	0.5198 (0.0179)	0.4139 (0.1308)
FedSAGE+	0.5653 (0.0546)	0.4265 (0.0062)	0.3836 (0.0705)
FedGCN	0.3689 (0.0646)	0.5877 (0.0018)	0.5075 (0.0001)
FedPUB	0.5529 (0.0246)	0.5192 (0.0064)	0.4767 (0.0286)
FedNTD	0.6355 (0.0195)	0.5880 (0.0041)	0.3913 (0.1235)
FedED	0.7338 (0.0294)	0.5514 (0.0117)	0.3916 (0.1184)
FedLoG	**0.7341** (0.0273)	**0.7413** (0.0316)	**0.7406** (0.0527)

(b) Unseen Node

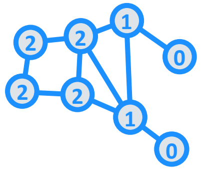
3. Missing Class



	Cora		
Methods	3 Clients	5 Clients	10 Clients
Local	0.0000 (0.0000)	0.0000 (0.0000)	0.0000 (0.0000)
FedAvg	0.3900 (0.1104)	0.1119 (0.0202)	0.0652 (0.0568)
FedSAGE+	0.5000 (0.0457)	0.1393 (0.0317)	0.0287 (0.0111)
FedGCN	0.0702 (0.0713)	0.2123 (0.0197)	0.0549 (0.0091)
FedPUB	0.0000 (0.0000)	0.0000 (0.0000)	0.0000 (0.0000)
FedNTD	0.3714 (0.1273)	0.1895 (0.0098)	0.0336 (0.0317)
FedED	0.5305 (0.1078)	0.1080 (0.0158)	0.0350 (0.0305)
FedLoG	**0.6472** (0.0811)	**0.4948** (0.0930)	**0.4037** (0.0619)

(c) Missing Class

4. New Client



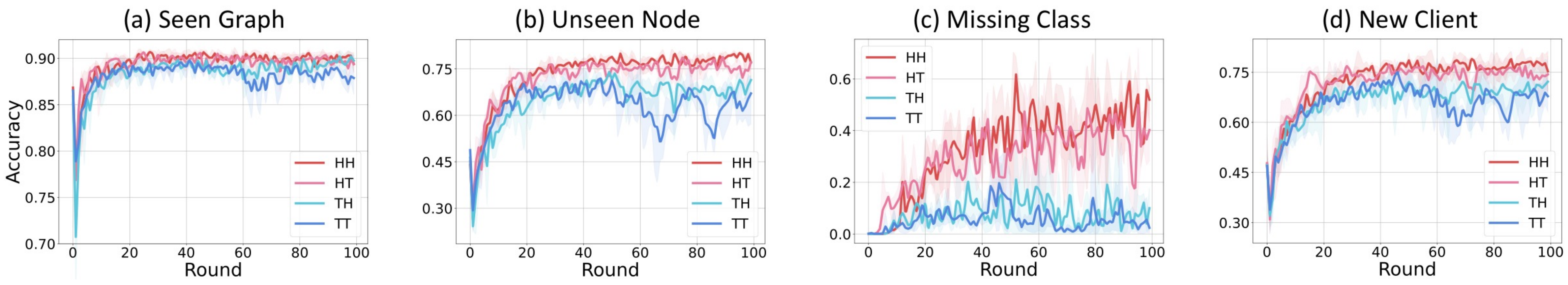
	Cora		
Methods	3 Clients	5 Clients	10 Clients
Local	0.0995 (0.0084)	0.1488 (0.0059)	0.1778 (0.0284)
FedAvg	0.3583 (0.0206)	0.2713 (0.0057)	0.3924 (0.1880)
FedSAGE+	0.2411 (0.0109)	0.3250 (0.0226)	0.4129 (0.1052)
FedGCN	0.3449 (0.0494)	0.3320 (0.0052)	0.4825 (0.0189)
FedPUB	0.3990 (0.0239)	0.2258 (0.0153)	0.4031 (0.0087)
FedNTD	0.3805 (0.0328)	0.3169 (0.0010)	0.3705 (0.1879)
FedED	0.4527 (0.0353)	0.2537 (0.0165)	0.3194 (0.1364)
FedLoG	**0.5047** (0.0884)	**0.4439** (0.0455)	**0.6055** (0.0914)

(d) New Client

FedLoG successfully addresses the locally absent knowledge (i.e., missing class, unseen structure) problem, **alleviating the local overfitting issue in graph FL.**

EXPERIMENTS

- **Do the headness of degree and class really help other clients?**



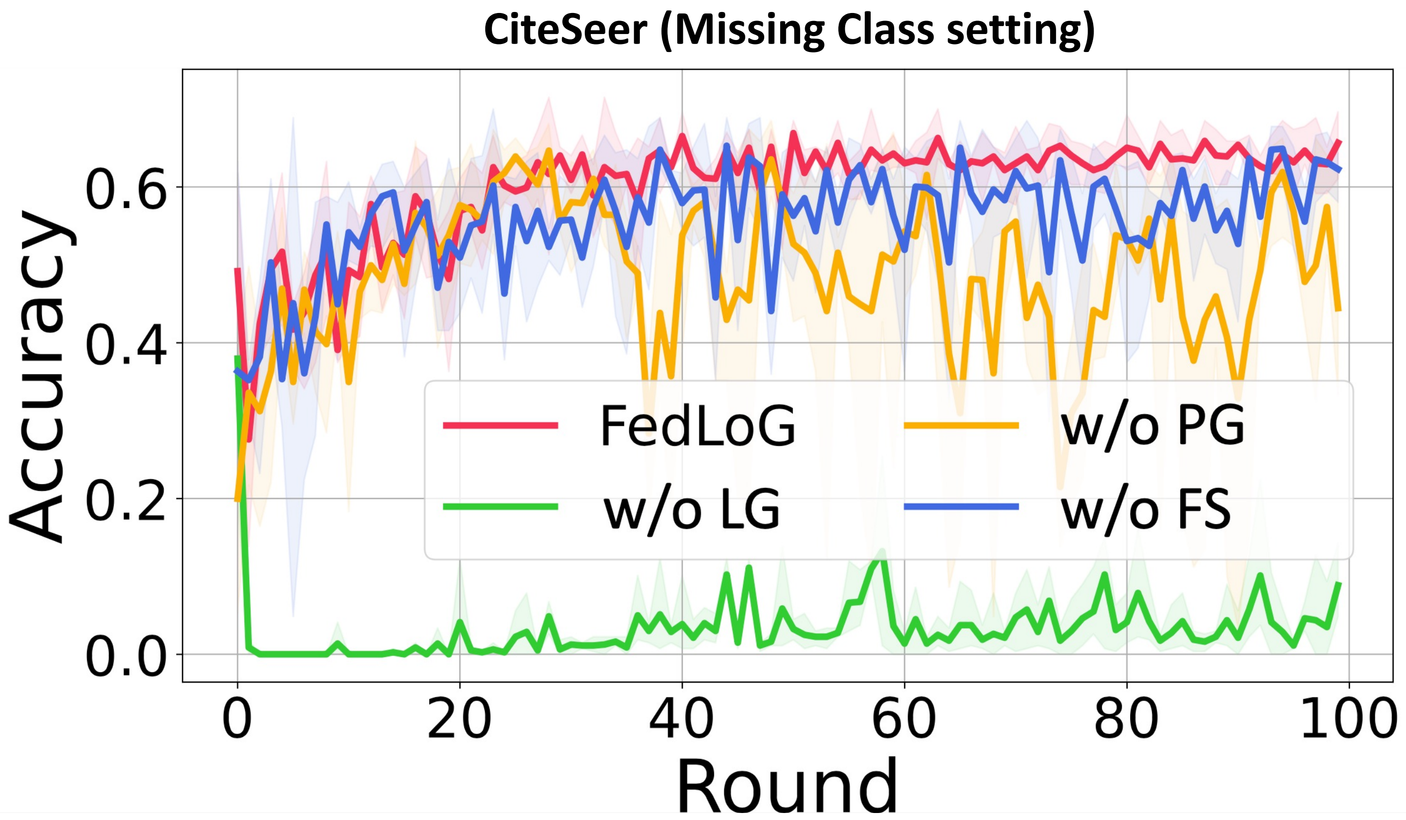
Global synthetic data is generated by condensing the following:

- Head Class + Head Degree Nodes (**HH**)
- Head Class + Tail Degree Nodes (**HT**)
- Tail Class + Head Degree Nodes (**TH**)
- Tail Class + Tail Degree Nodes (**TT**)

Data reliability varies with global synthetic data knowledge, with **HH knowledge being most reliable.**

EXPERIMENTS

- Does each module effectively address the local overfitting problem?

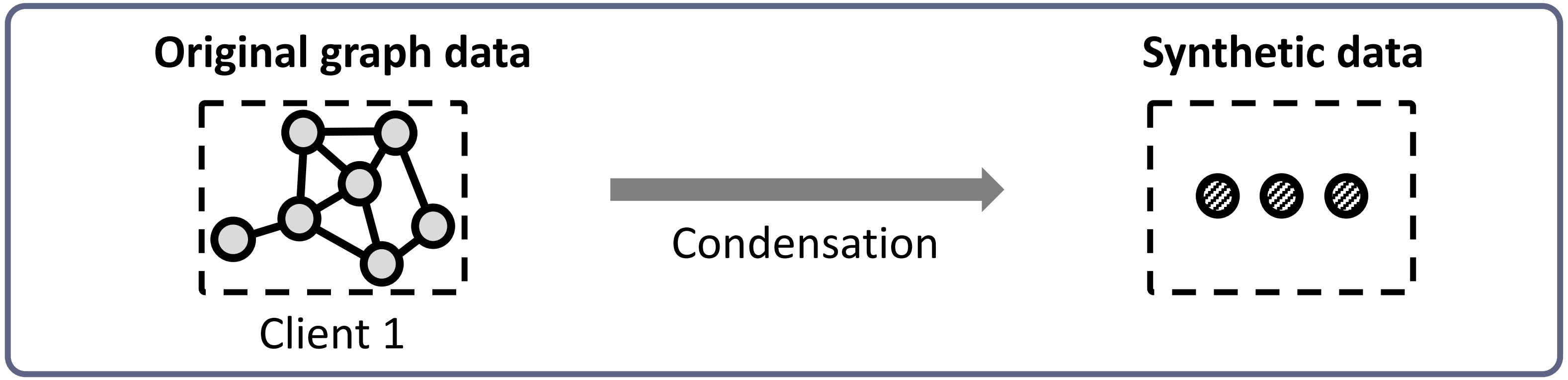


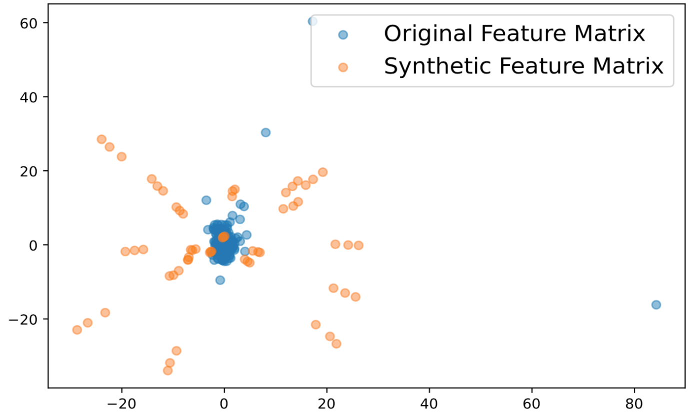
- **w/o PG:** without Prompt Generation
- **w/o FS:** without Feature Scaling
- **w/o LG:** without Local Generation

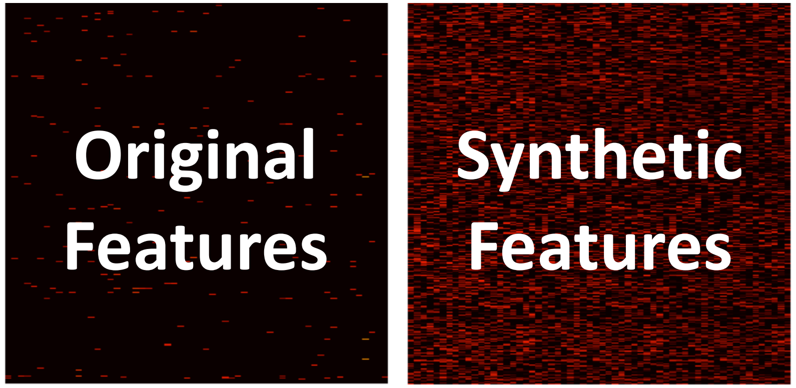
Local Generalization phase is crucial for addressing the absent knowledge

EXPERIMENTS

- **Can synthetic data be specified to match the original data's features?**



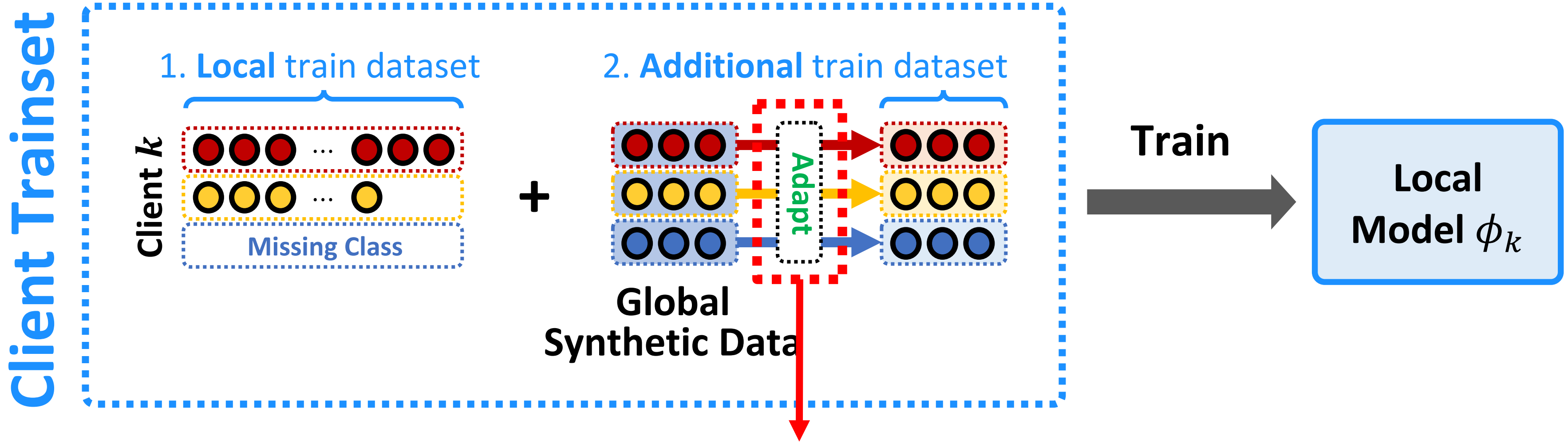




Lacking a graph structure, synthetic nodes distill structural information differently,
forming a distinct distribution

EXPERIMENTS

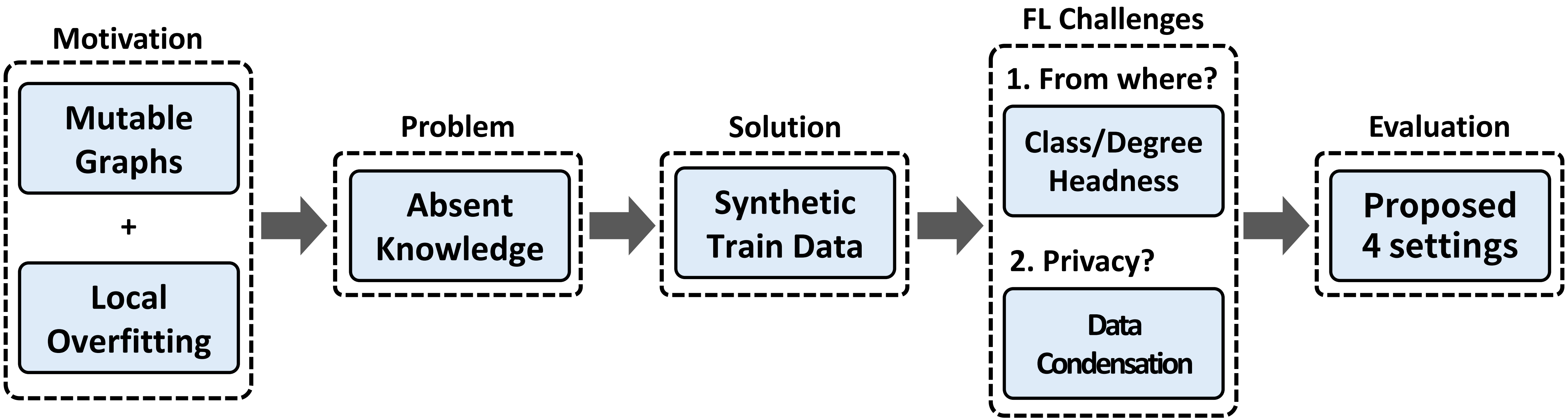
- **How does FedLoG provide protection against gradient inversion attacks?**
  - Each client trains on **both its local data and global synthetic data.**
  - Global synthetic data are adapted uniquely within each local client **without sharing perturbation information.**



How each client adapts to the synthetic data is never shared!

FedLoG enhances protection against adversaries attempting to invert gradients and reconstruct the original data.

CONCLUSIONS



Code

Paper

Subgraph Federated Learning for Local Generalization

Code: https://github.com/sung-won-kim/FedLoG

Paper: https://www.arxiv.org/abs/2503.03995

Email: swkim@kaist.ac.kr

C1. WHICH DATA ARE RELIABLE TO BE AGGREGATED?

- **Performance Influence of Knowledge Acquired from Other Clients**

Data Reliability: The accuracy and consistency of information from decentralized nodes.

→ We measured the target class accuracy of a client (receiver) receiving information (i.e., weights) from other clients.