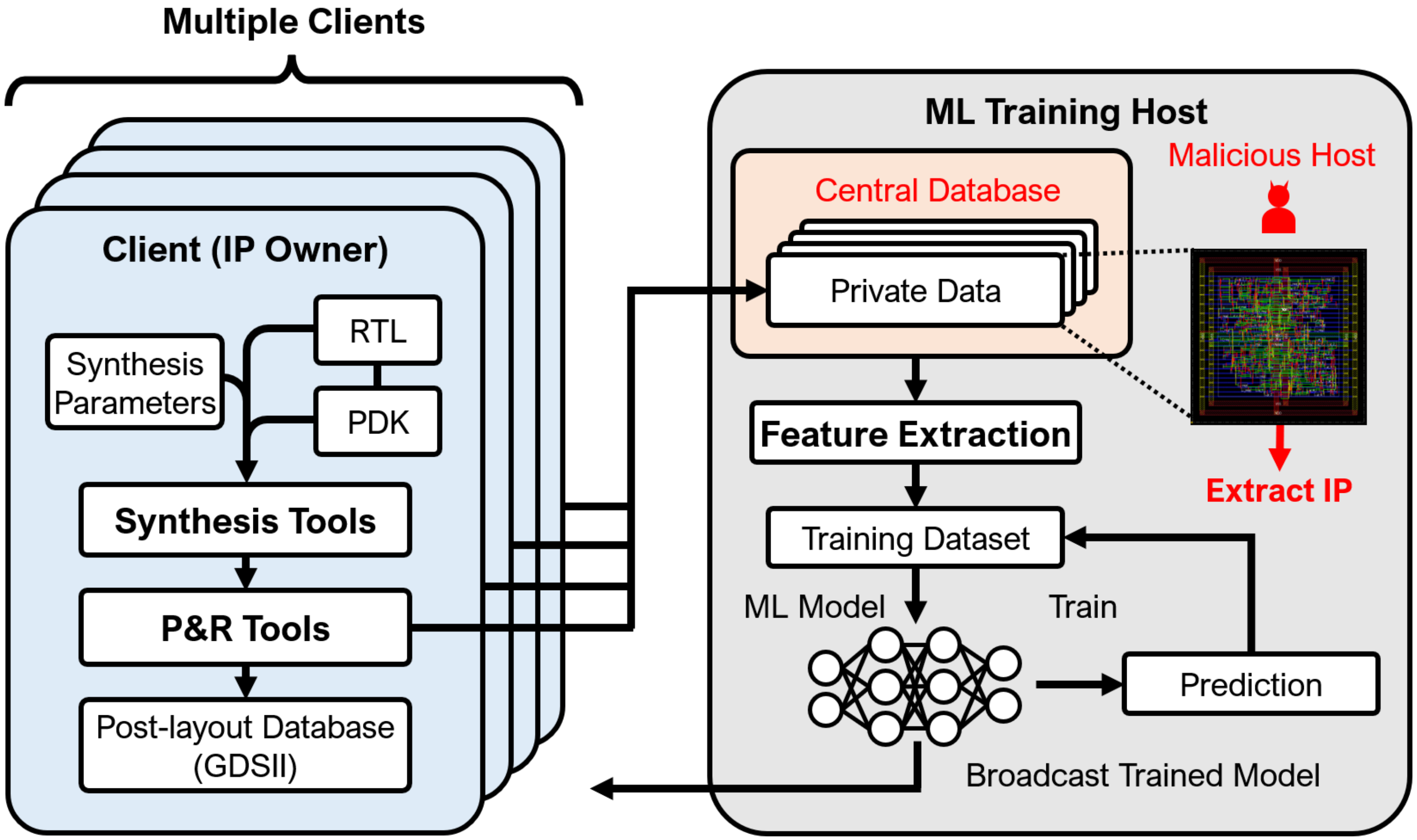
FedEDA: Federated Learning Framework for Privacy-Preserving ML-EDA

Seokhyeong Kang
Department of Electrical Engineering
Pohang University of Science and Technology

Why We Need Security in ML-EDA

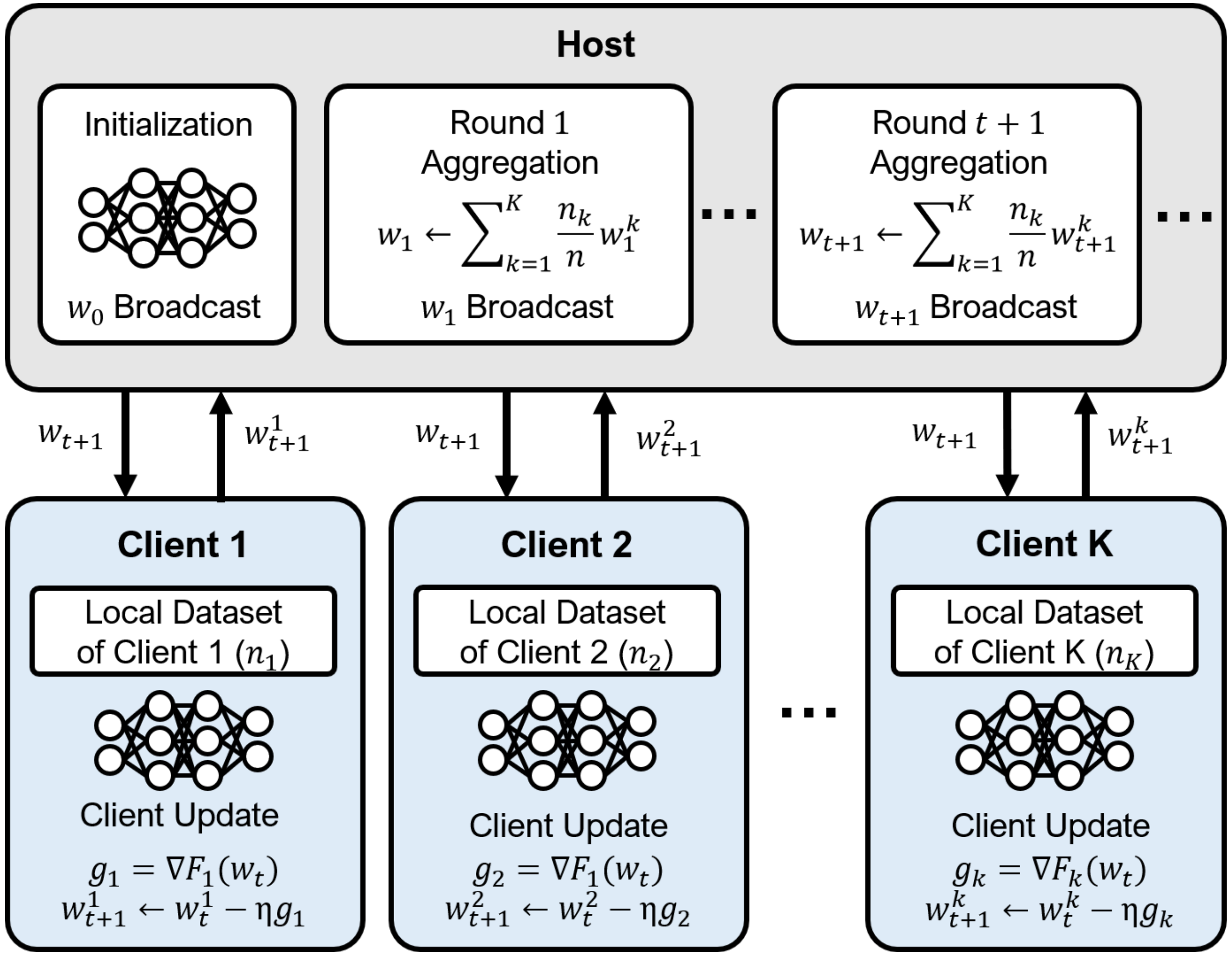


- Problem in ML-EDA
  - Lack of data for training
- Why?
  - Security concerns on IP
  - Large volume of storage

If it is not sharable, need a proxy and federated learning

[1] McMahan, Brendan, et al. "Communication-efficient learning of deep networks from decentralized data." *Artificial intelligence and statistics*. PMLR, 2017.

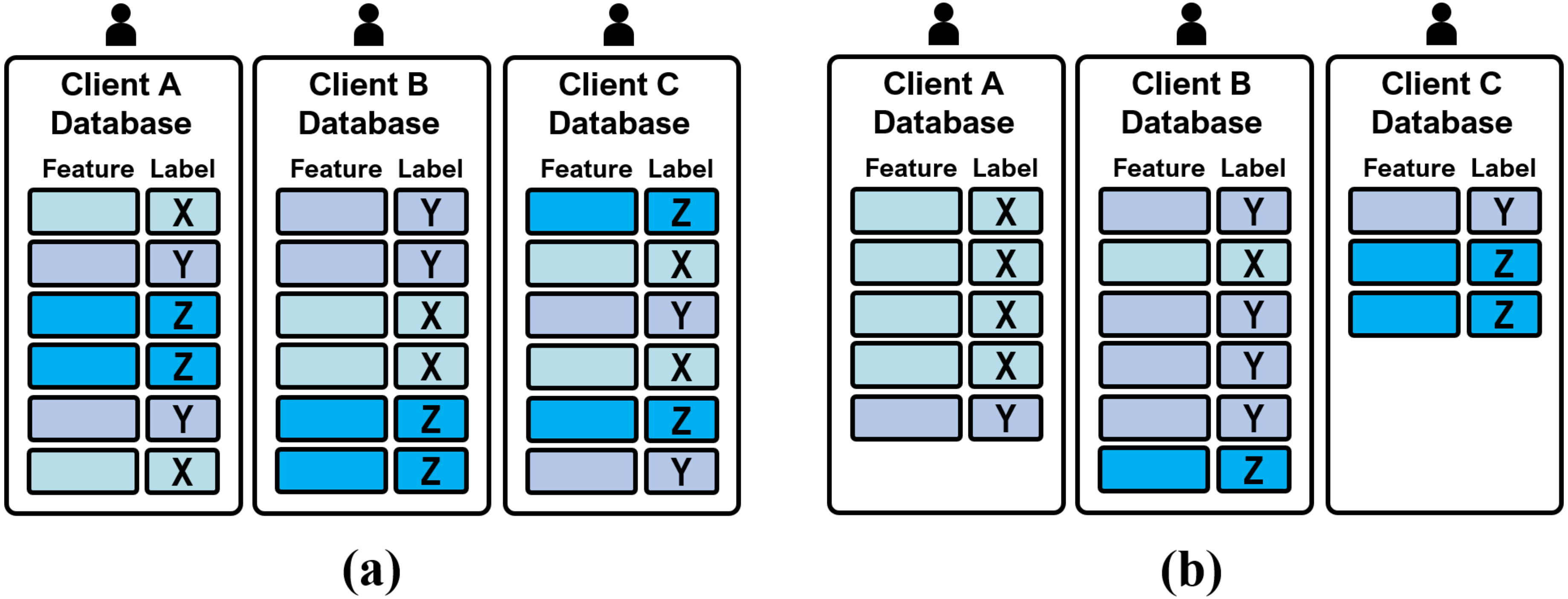
What is Federated Learning[1] (FL)?



- **Model merging scheme : effective aggregation of independently trained models**
- **Clients share locally trained weights with the host**
- **The host aggregated these local weights**
- **Aggregated weights are distributed**
- **Host has no direct access to private data**

[1] McMahan, Brendan, et al. "Communication-efficient learning of deep networks from decentralized data." *Artificial intelligence and statistics*. PMLR, 2017.

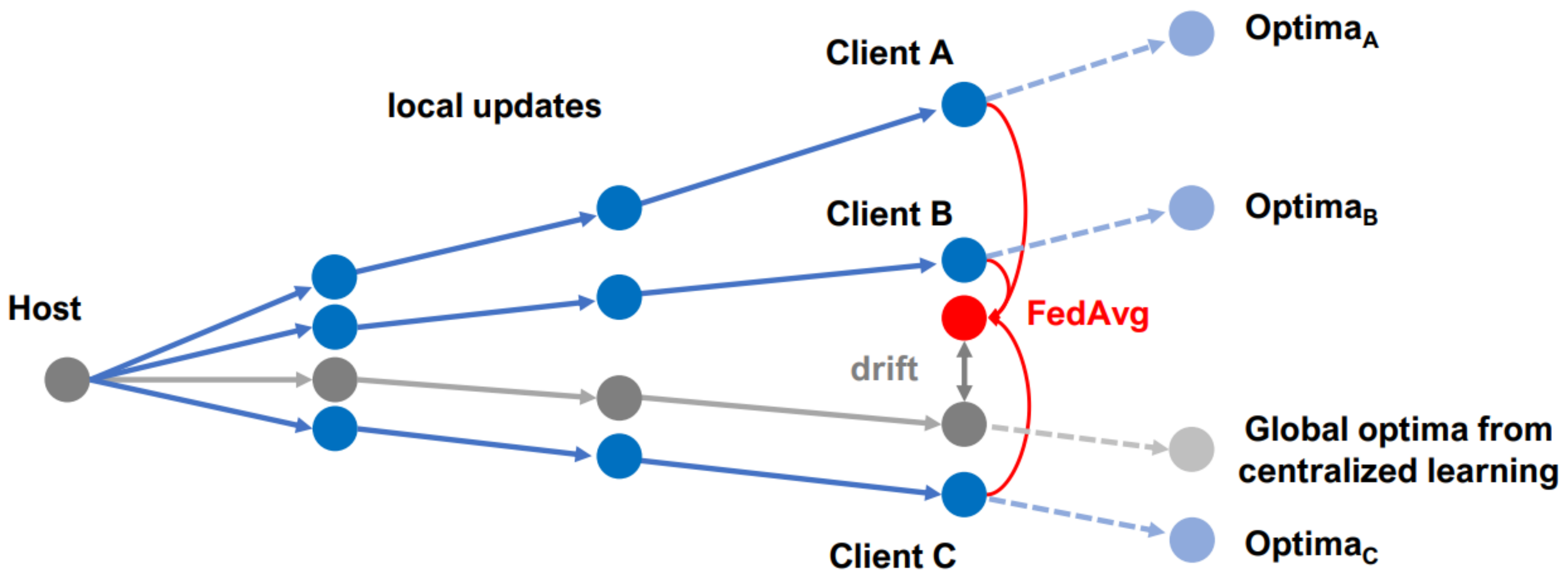
Main Concern of FL – Data Non-IID-ness (1)



- Non-IID : The real-world data distribution is not independent and is unequally distributed.
- Label Skew: Distribution of unique label data per client
- Quantity Skew: Distribution of different quantities of feature data per client

POSTECH

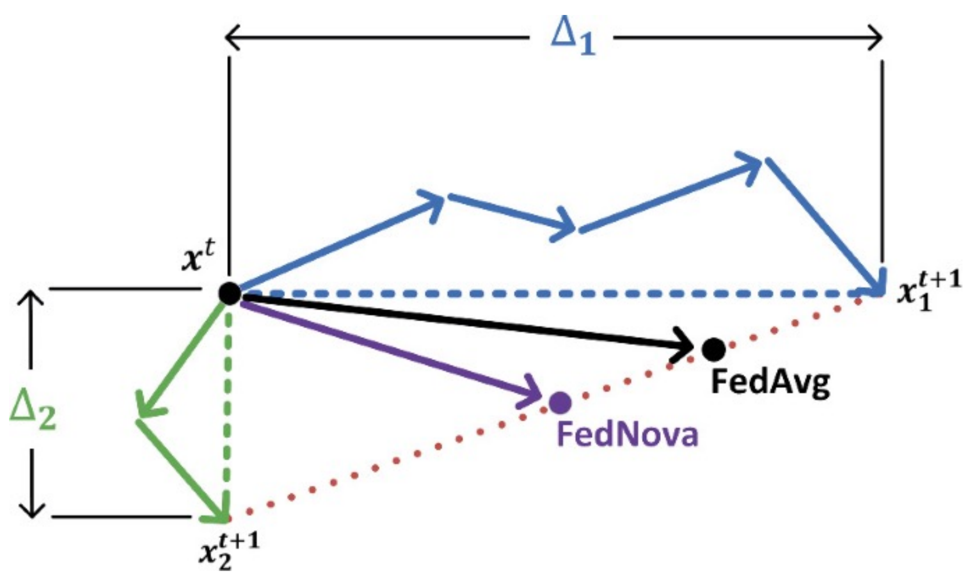
Main Concern of FL – Data Non-IID-ness (2)

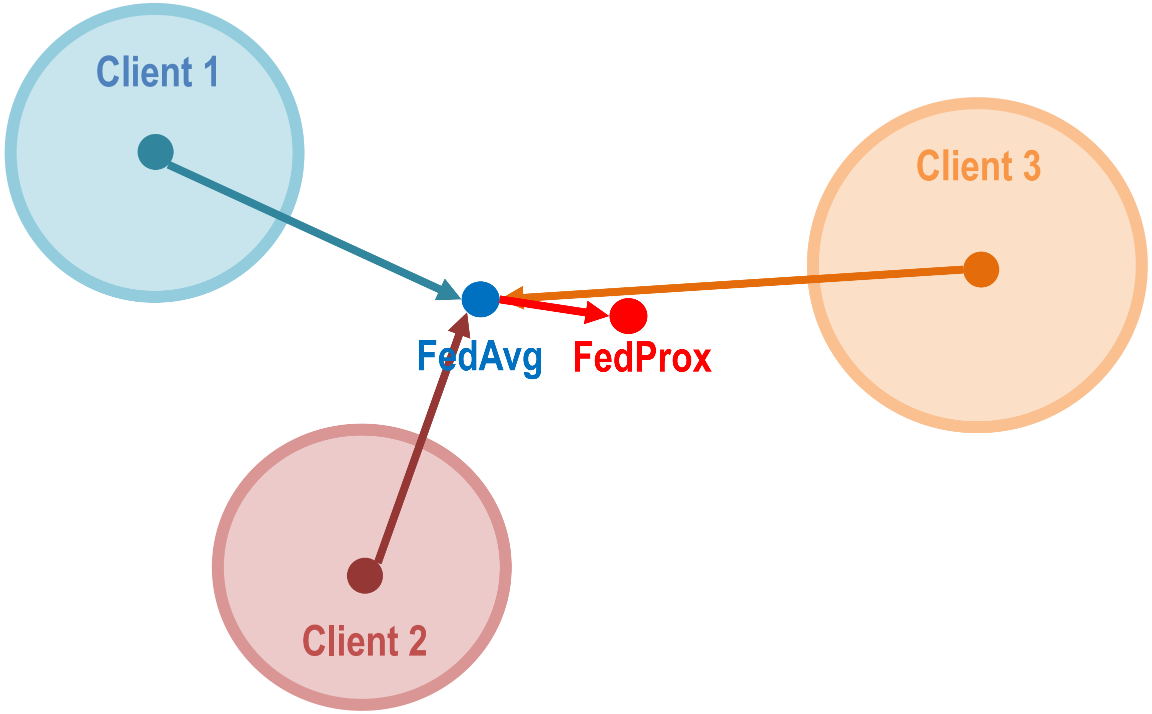


- Federated Averaging[1] : Naïve aggregation algorithm where weights are averaged
- Distribution of local dataset is highly different from the global distribution
- Converged model by FedAvg may be far from global optima → "drift[2]" of local updates
  - Performance degradation of FedAvg in a non-IID data setting

[2] K, Sai Praneeth, et al. "Scaffold: Stochastic controlled averaging for on-device federated learning." *arXiv preprint arXiv:1910.06378* 2.6 (2019).

Existing FL Model Merging Algorithm

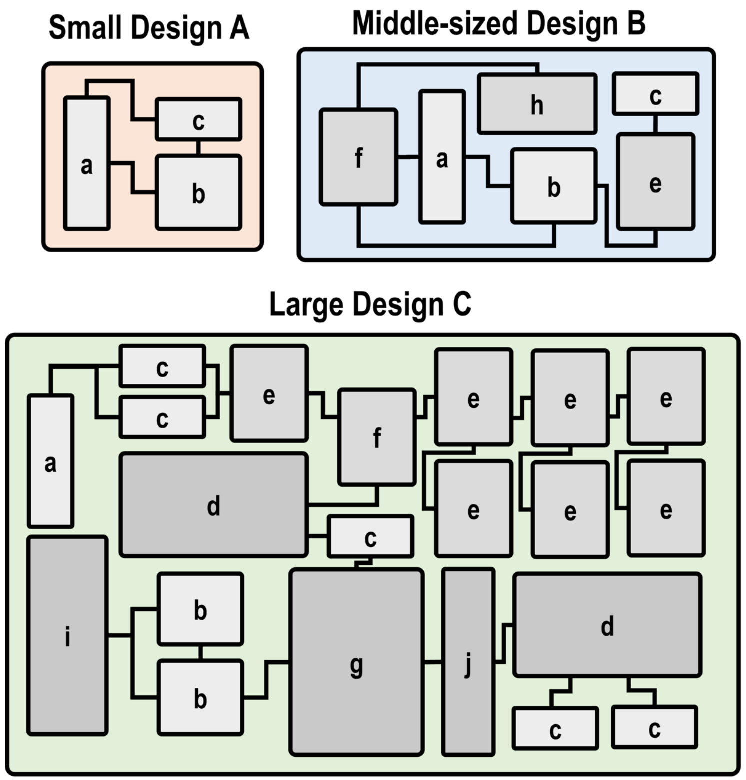


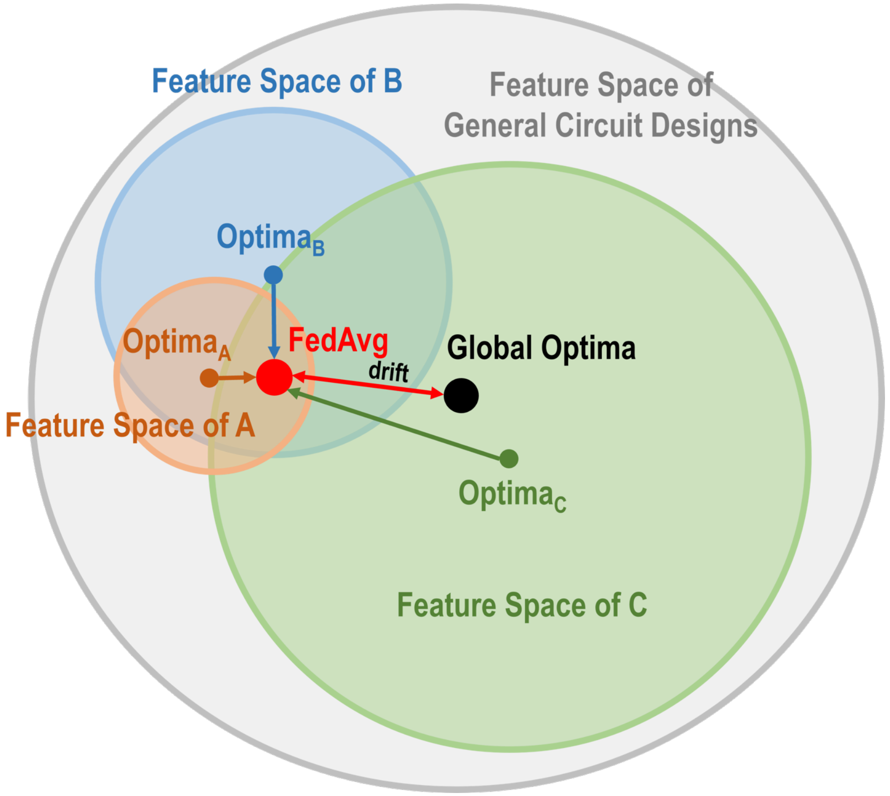


- FedNova[3]: Normalize the number of training steps in model merging
- FedProx[4]: Minimize difference of L2 norm between global and local weights
- These model merging methods are proposed for the image or text data

[3] W, Jianyu, et al. "Tackling the objective inconsistency problem in heterogeneous federated optimization." *Advances in neural information processing systems* 33 (2020): 7611-7623.
[4] Y, Xiaotong, et. al. "On convergence of FedProx: Local dissimilarity invariant bounds, non-smoothness and beyond." *Advances in Neural Information Processing Systems* 35 (2022): 10752-10765.

Non-IID-ness of EDA Data (1)

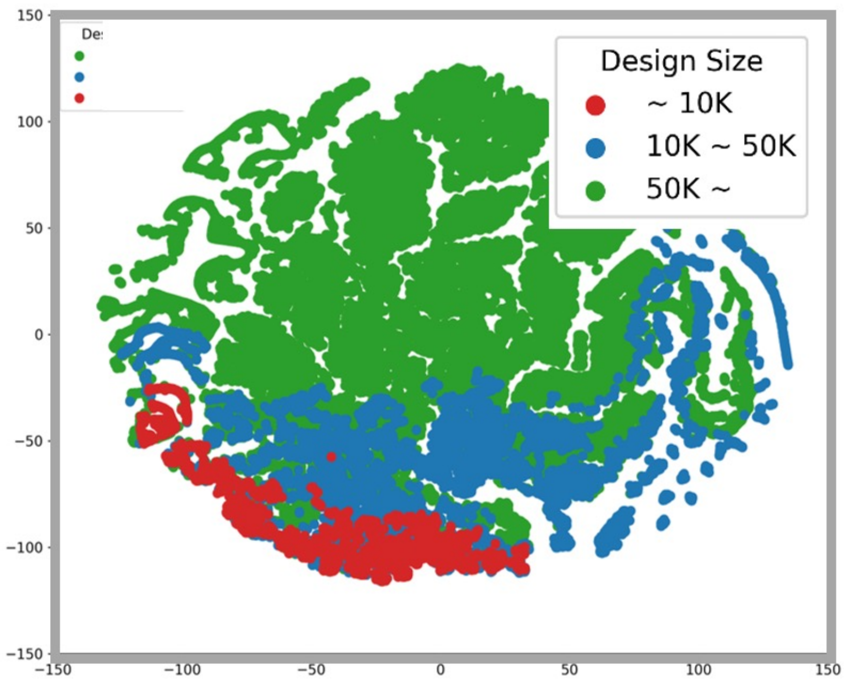


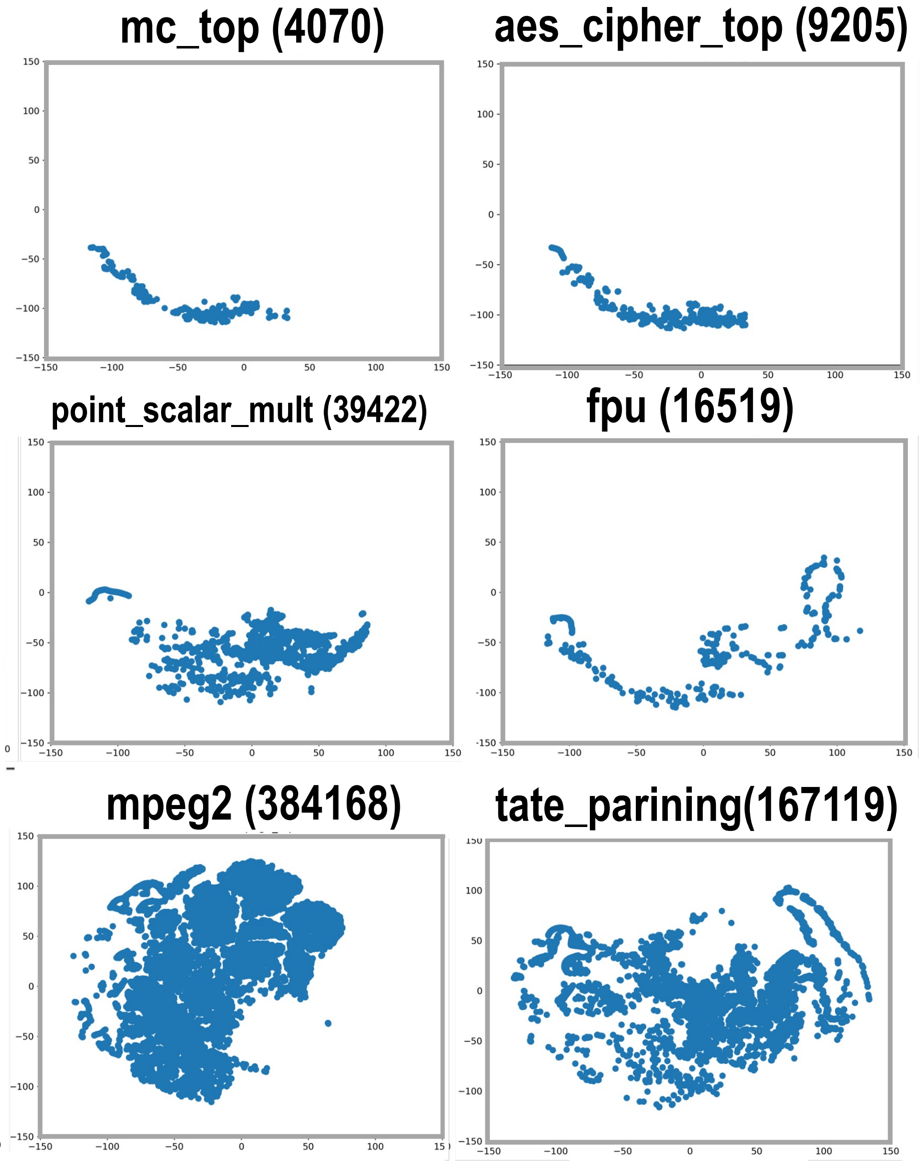


- In EDA data, design size is the main source of data non-IID-ness
- Larger designs have larger feature space compared to smaller designs

Non-IID-ness of EDA Data (2)

Stage	Features
Placement	cell/pin density, F/F ratio, avg terminals, # of insts/nets/terminals, net RUDY, metal channel density
Early Global Routing	wire/channel/via density, net density, WNS, TNS

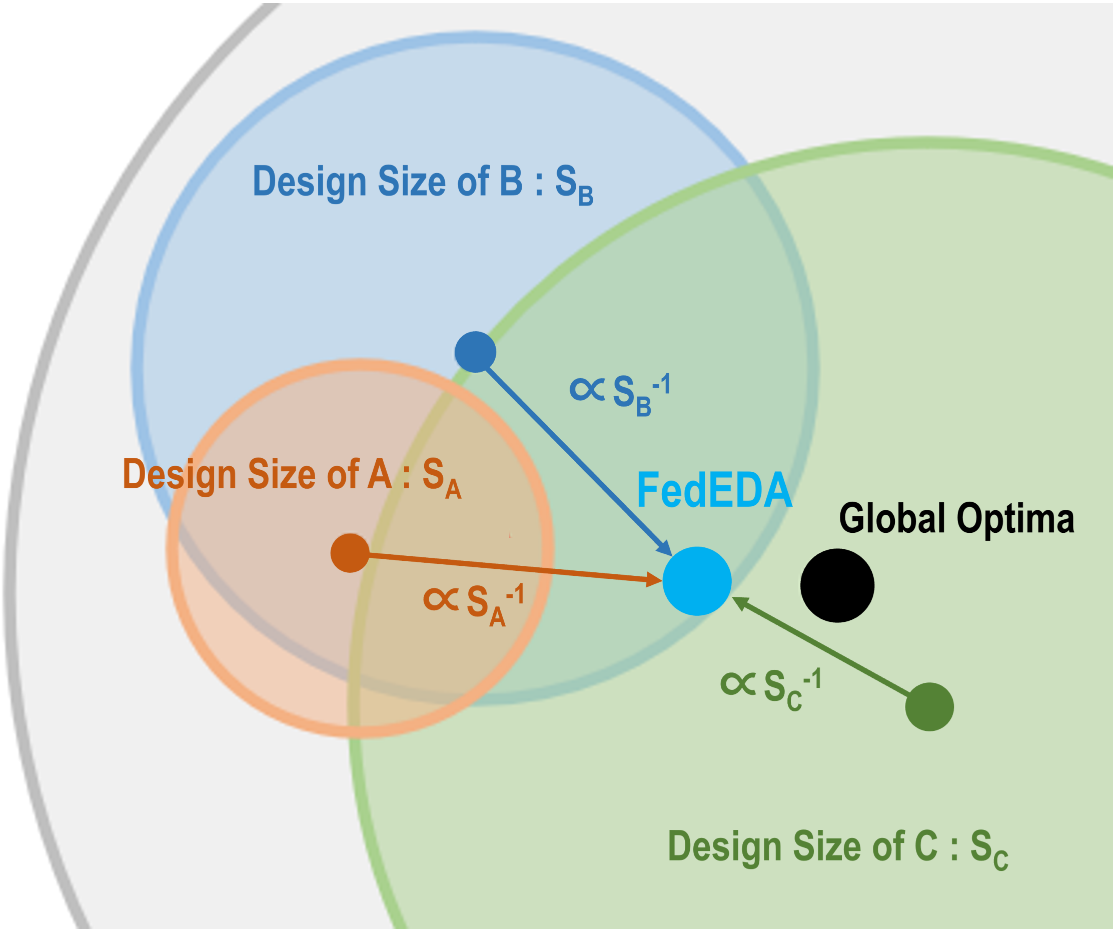




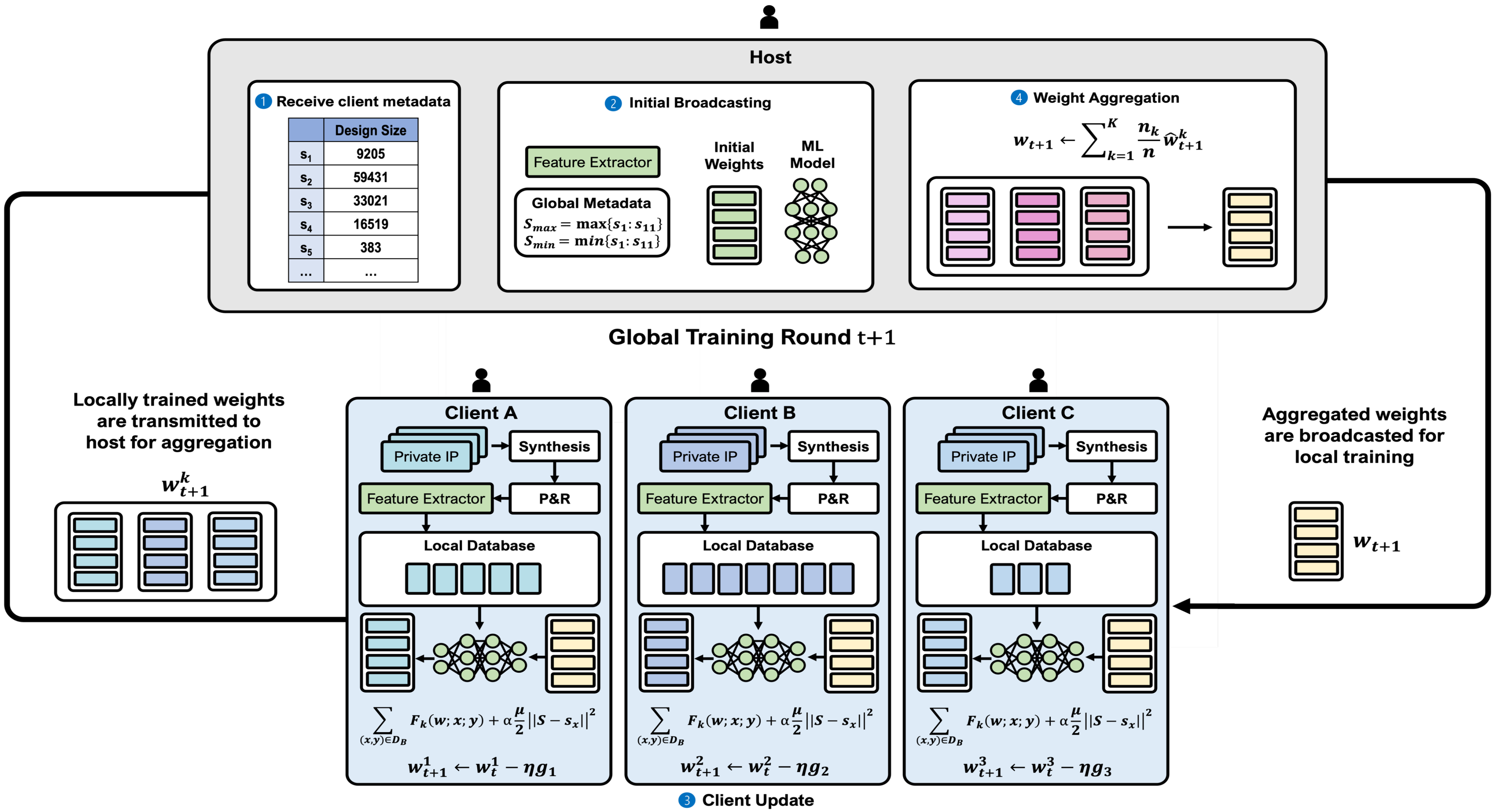
- The feature space of small designs tend to overlap with larger designs

FedEDA – Effectively Handling the Non-IID-ness

- We handle non-IID-ness of EDA data by considering the design size and L2 norm
- So, during aggregation, the influence of smaller designs will be attenuated

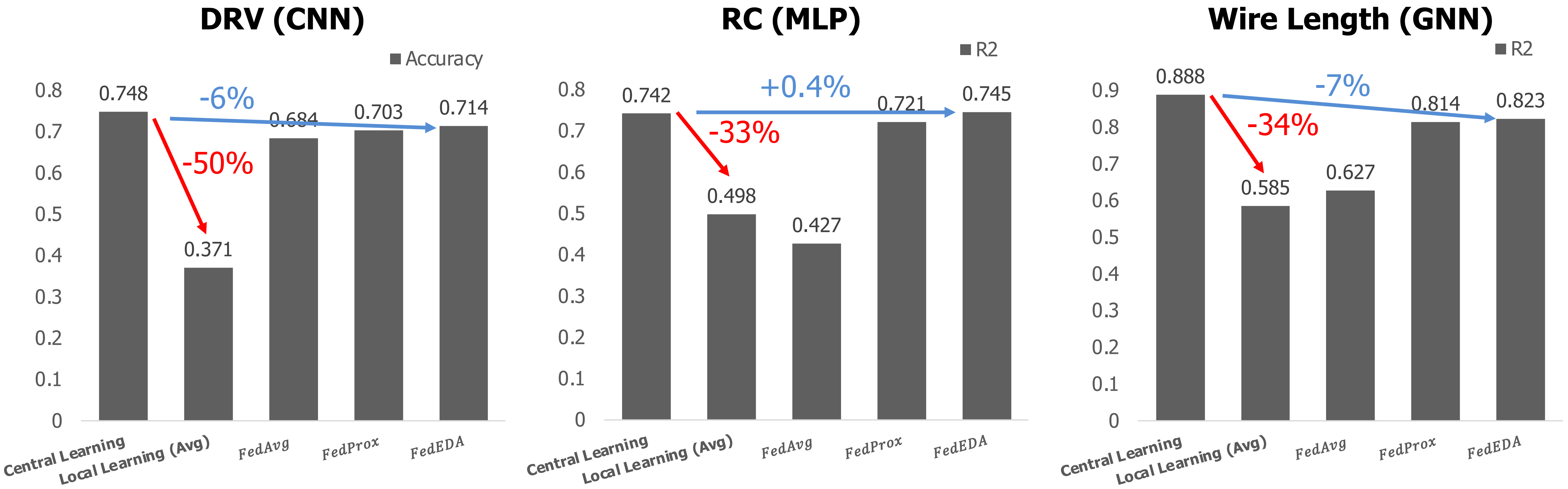


FedEDA – Overall Framework



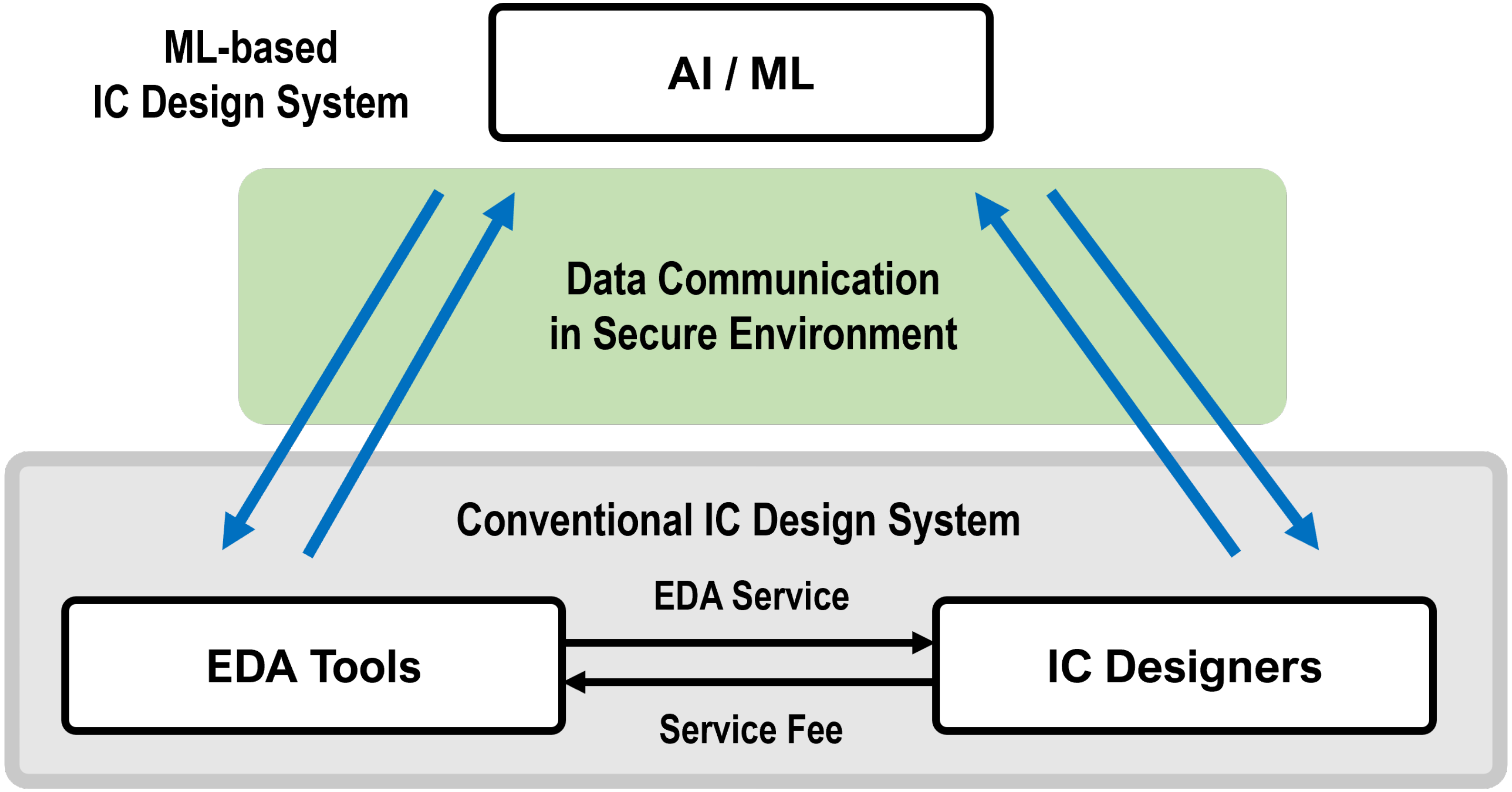
- FedEDA exploits the data size of the circuit and L2 norm into the loss function for EDA applications

Experimental Results



- We validated FedEDA framework on three early-stage prediction tasks
- # of design: 20, # of client: 2, 3, 5, and label skew + quantity skew are included
- Better model performance than traditional FLs

Impact in the EDA Community



- FedEDA can provide a secure FL environment for a collaborative ML-based IC design system
- Active participation in this collaborative environment shall reinforce ML quality and trustworthiness

Future Directions

- Investigating EDA data distributions further
  - There are multiple factors attributing to the varying data distributions in EDA (e.g., tech. library, cell height, utilization, target clock period …)
  - Other sources of non-IID-ness will be considered in our FedEDA framework

- Collaborative ML environment for EDA
  - Secure multi-party computation is crucial in collaborative ML → FedEDA
  - Other techniques besides model merging can be utilized → Model editing
  - Investigation of EDA data and collaboration security for collaborative ML-EDA

Thank You !