NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Towards Trustworthy Federated Learning

TrustFUL

Trustworthy Federated Ubiquitous Learning

Han Yu

Nanyang Assistant Professor
School of Computer Science and Engineering
Nanyang Technological University

Self-Introduction

Han Yu

Nanyang Assistant Professor
School of Computer Science and Engineering
Nanyang Technological University, Singapore

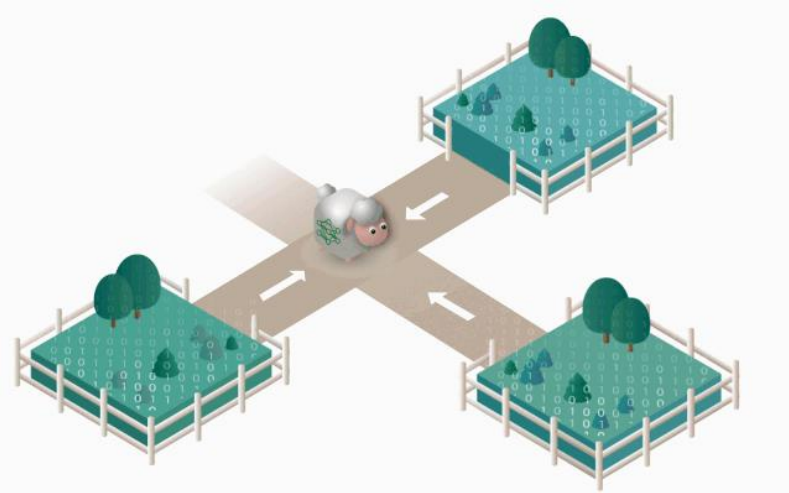
http://hanyu.sg/

han.yu@ntu.edu.sg

Research Areas:

- Federated Learning
- Multi-Agent Systems

Federated Learning – Privacy-Preserving Machine Learning

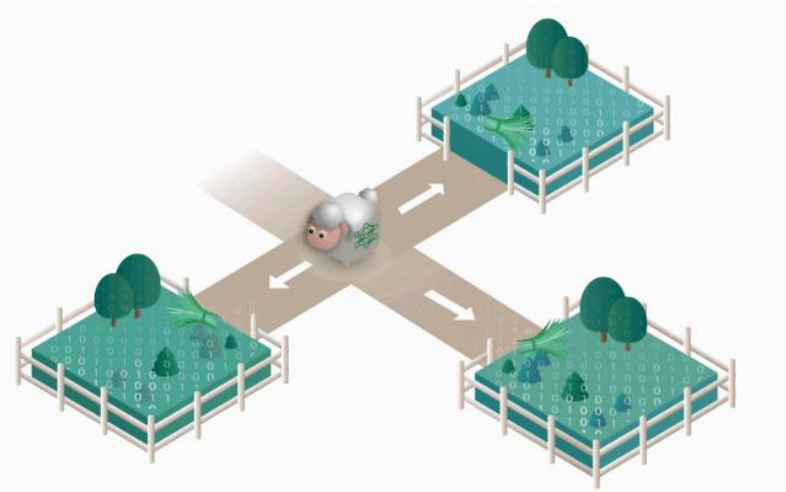


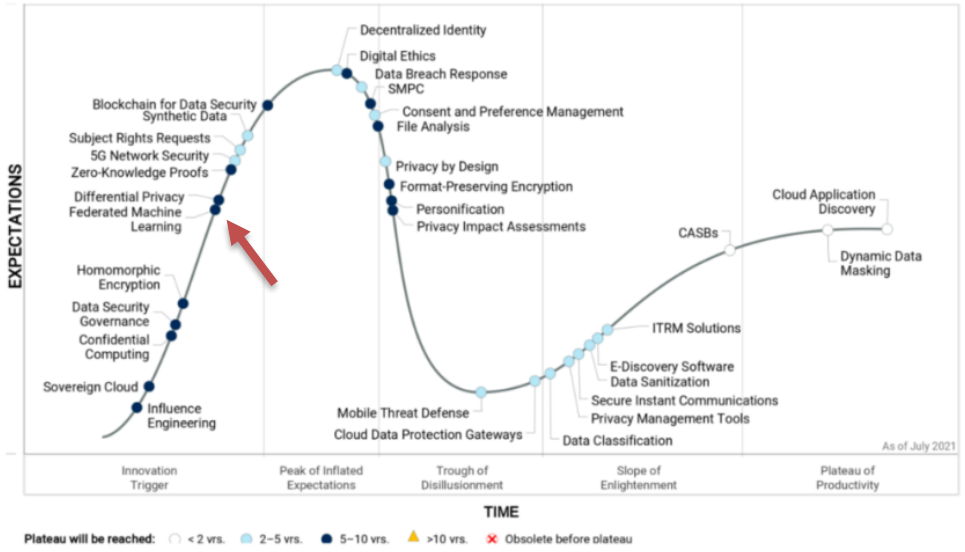
Traditional Machine Learning:

- Moving data to a centralized entity for model training
- Privacy often exposed

Federated Learning:

- Moving model training to where data originate
- Privacy is preserved





Agenda

1: Theoretical Research in Trustworthy Ubiquitous Federated Learning

2: Translational Research in Trustworthy Ubiquitous Federated Learning

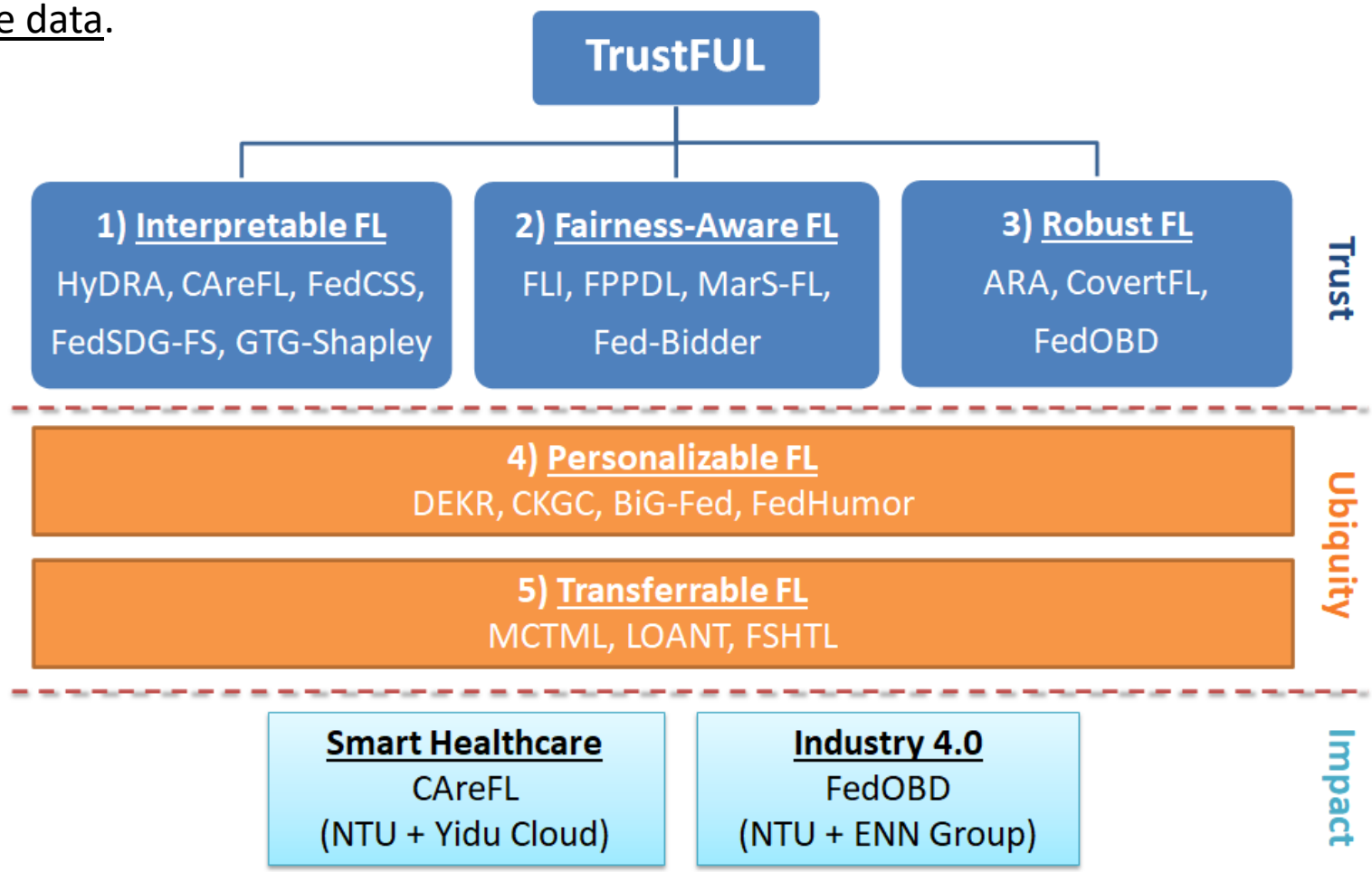
An Overview of TrustFUL

https://trustful.federated-learning.org/

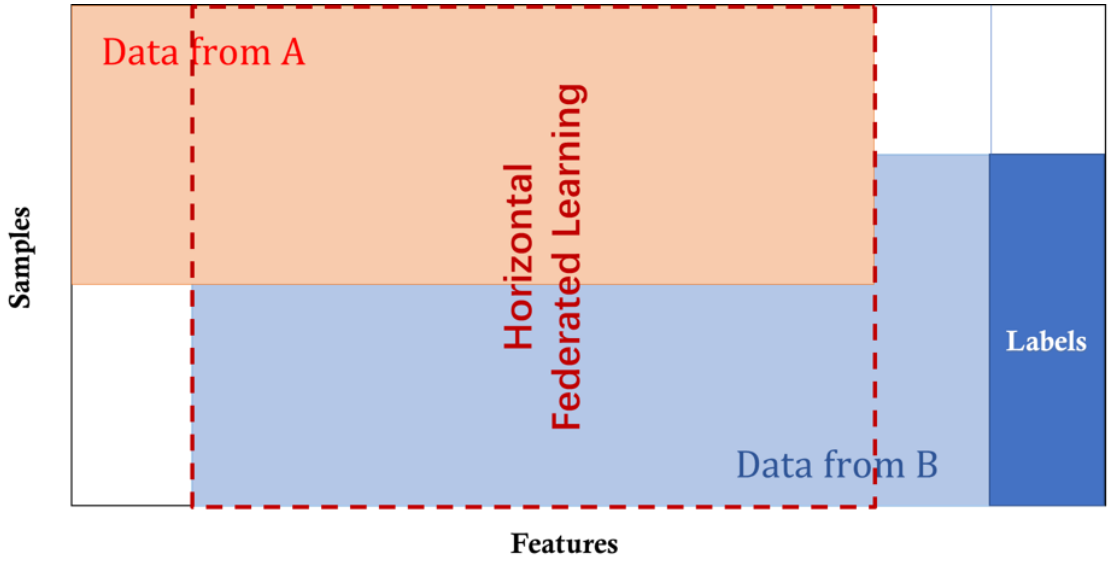
Trustworthy Federated Ubiquitous Learning (TrustFUL) – building trust to enable data providers to participate in AI model co-creation, while protecting their sensitive data.

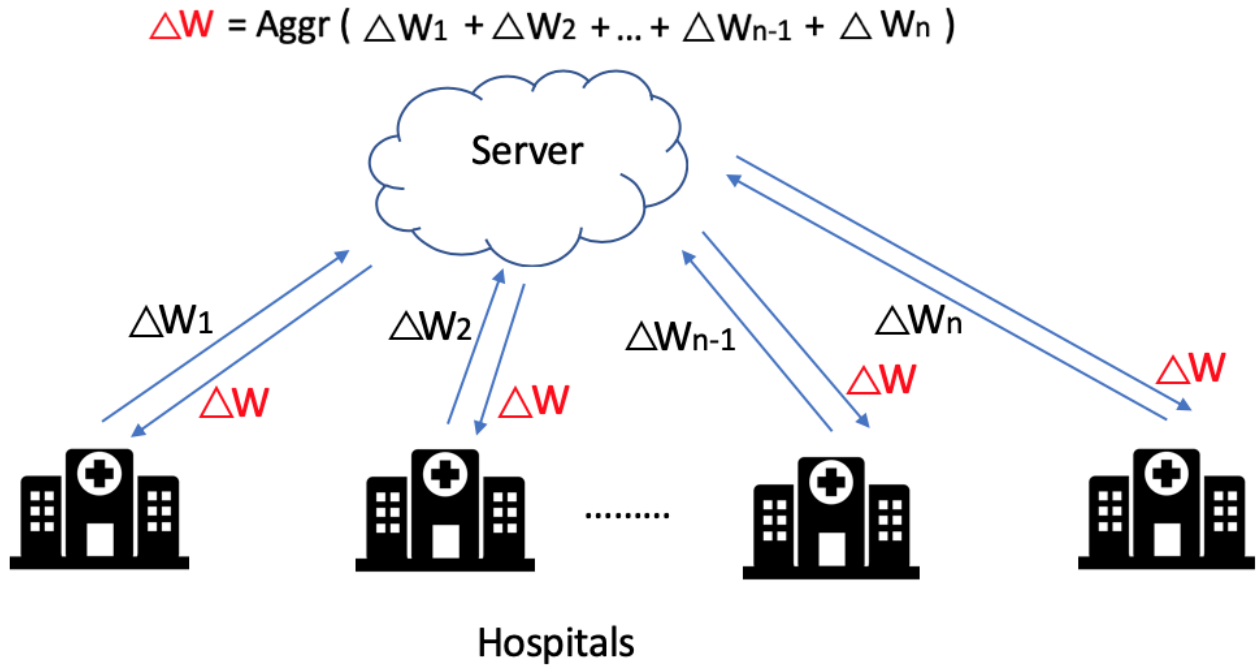
Achieving Trust through:
- Interpretability
  - Data, features, models
- Fairness
  - Opportunities, payoffs
- Robustness
  - Security, scalability

Achieving Ubiquity through:
- Personalizability of models
  - Resource & data heterogeneity
- Transferrability of knowledge
  - Cross country, cross sector, cross tasks

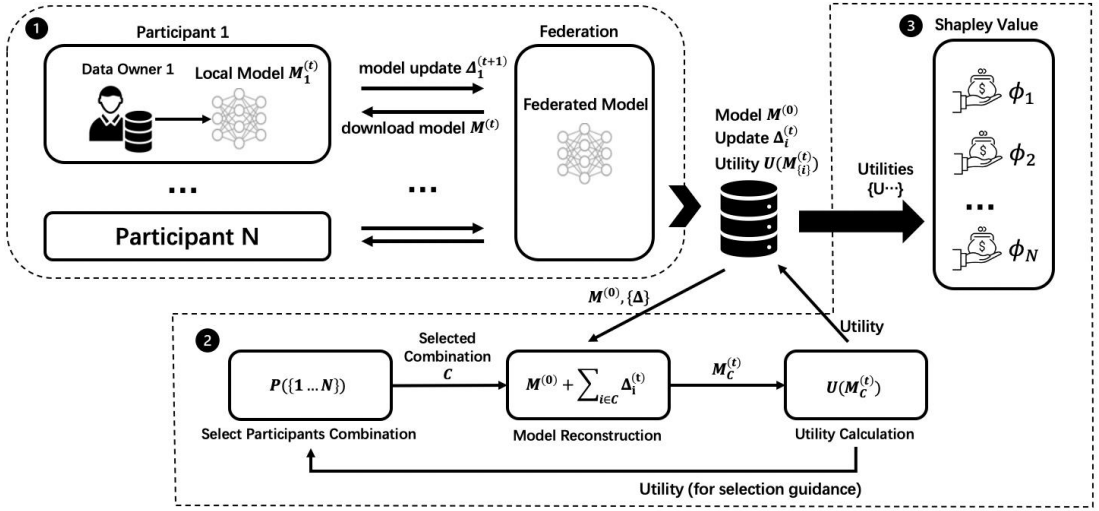


Horizontal Federated Learning (HFL)





Interpretable FL (HFL)

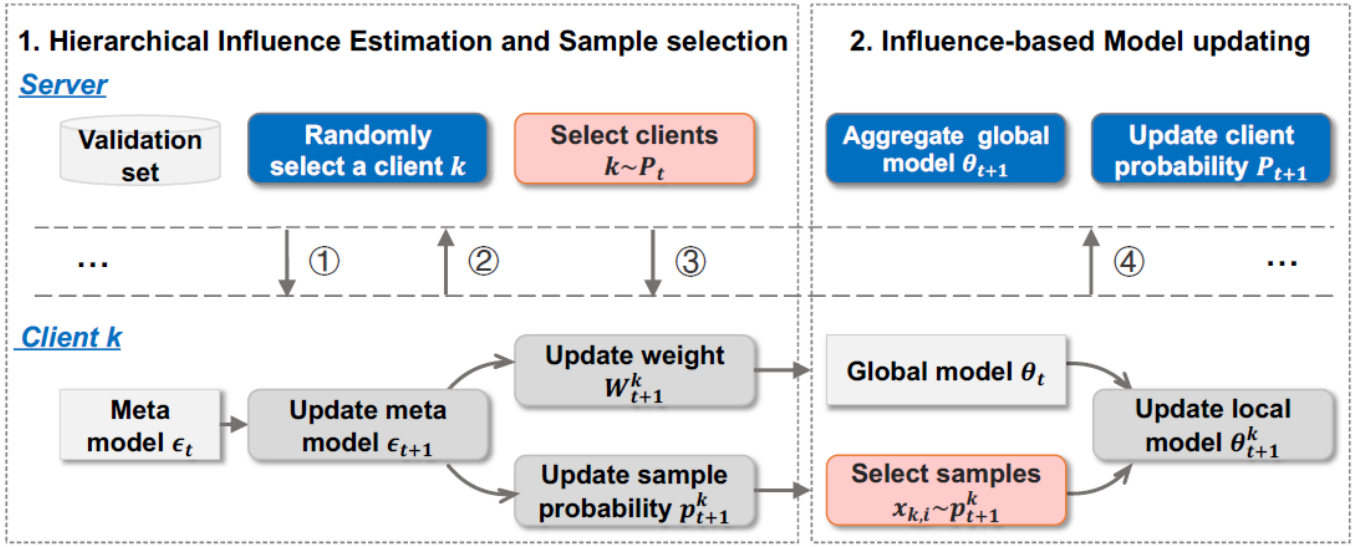


Joint Federated Client and Sample Selection

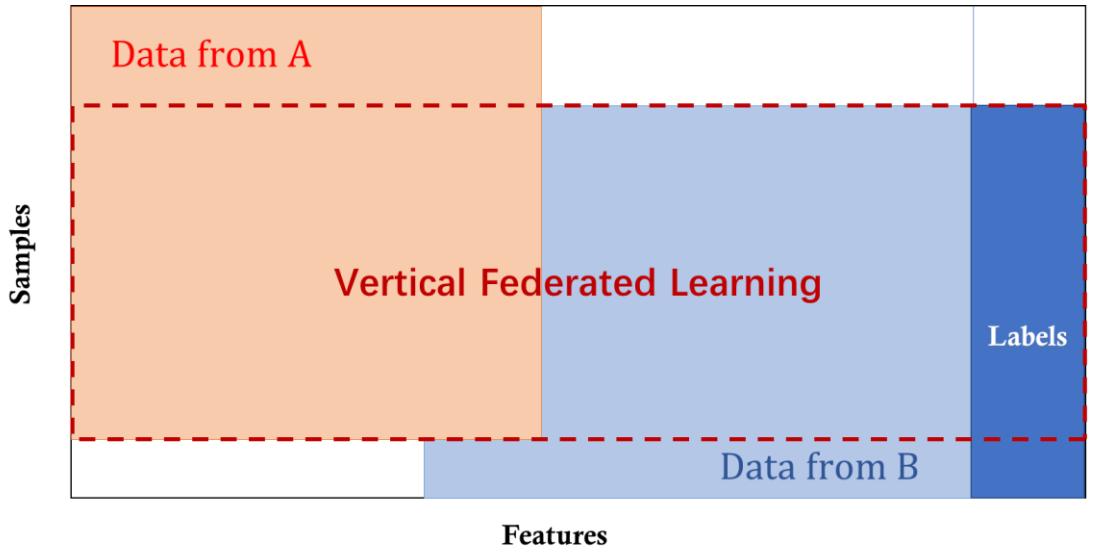
- A bi-level optimization-based approach to jointly select high quality FL clients and subsets of high quality local data for given FL training tasks.
- A client's quality depends on the sum of the influence function values of its selected local samples.
- First work to distinguish hard samples from noisy samples in FL.

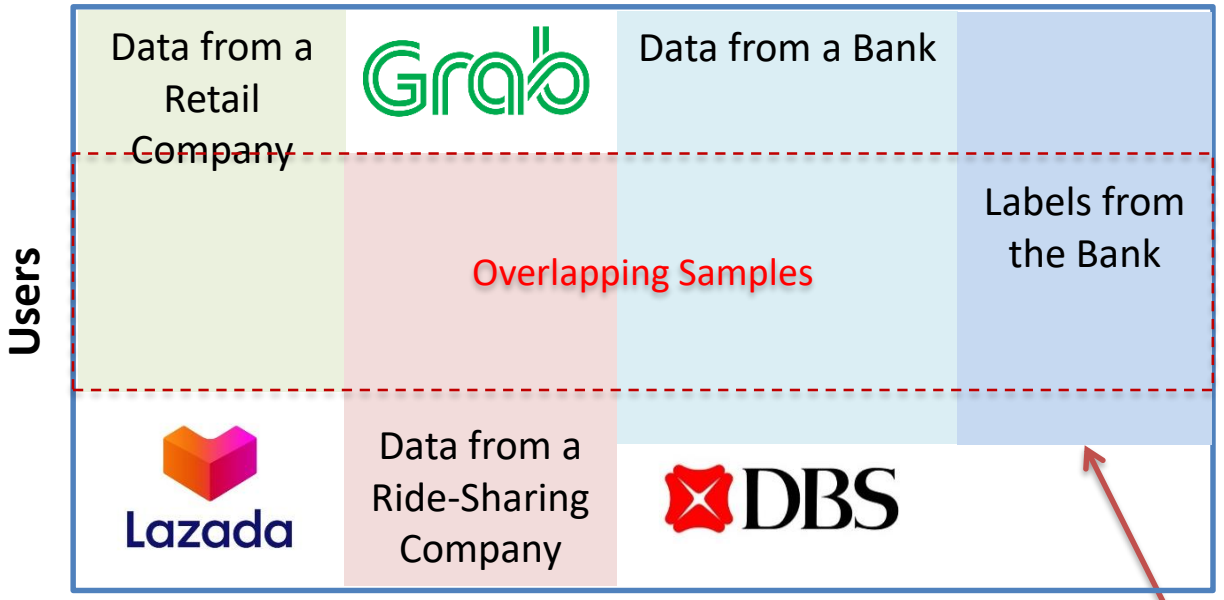
Fair and Efficient FL Participant Contribution Evaluation

- Developed a fair and efficient algorithm to evaluation FL data owner contributions.
- Significantly enhanced the scalability of Shapley value-based data valuation.
- Zelei Liu, Yuanyuan Chen, Han Yu, Yang Liu & Lizhen Cui. GTG-Shapley: Efficient and accurate participant contribution evaluation in federated learning. *ACM Transactions on Intelligent Systems and Technology*, vol. 13, no. 4, pp. 60:1-60:21, ACM (2022).



Interpretable FL (VFL)





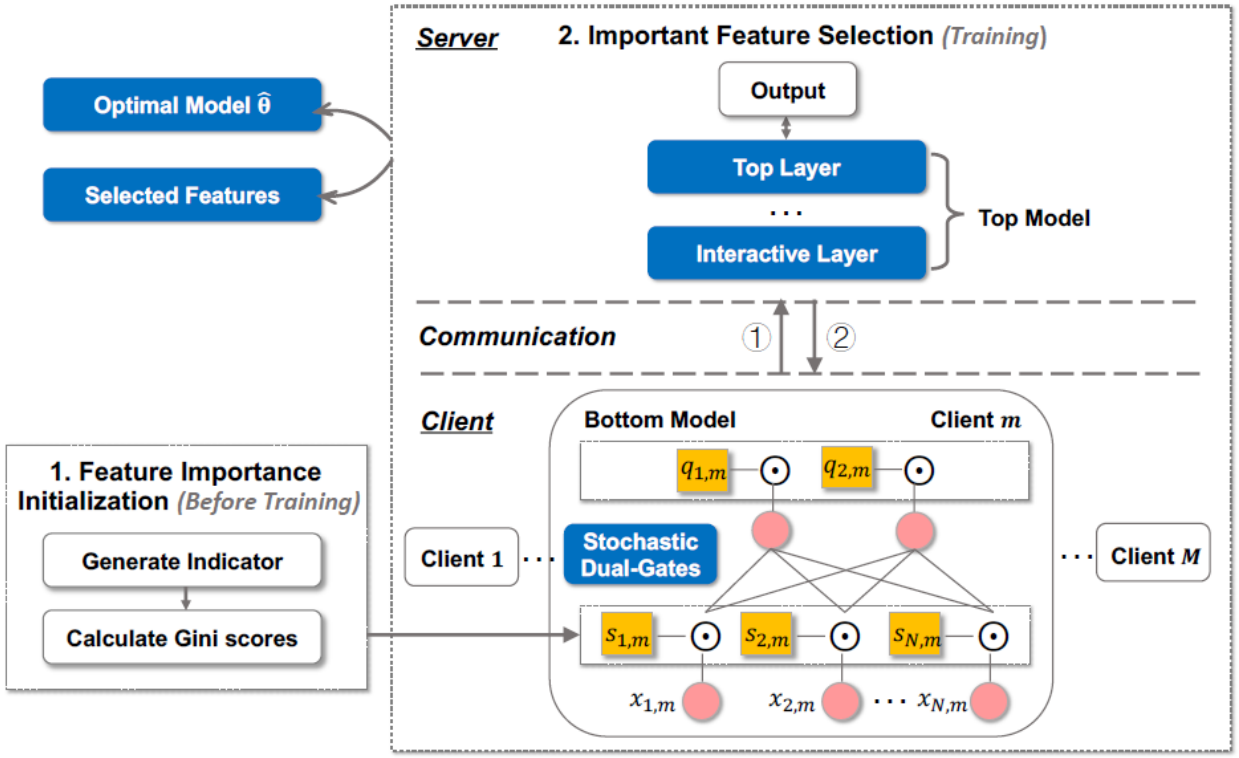
Online shopping behaviours

Mobility patterns

Banking service usage patterns

Learning task: find creditworthy users from other companies interested in bank loans

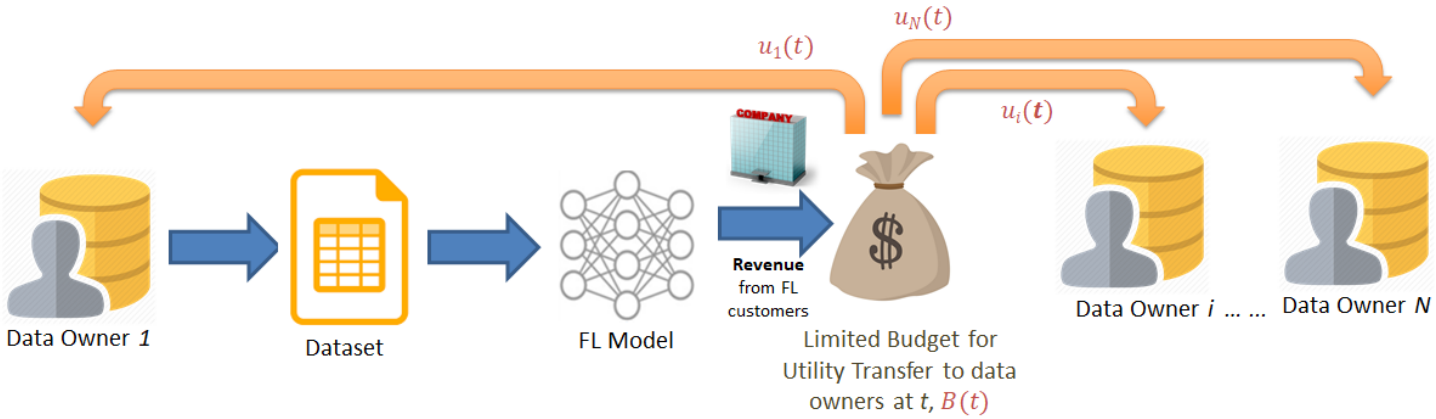
Interpretable FL (VFL)



Federated Stochastic Dual-Gate Feature Selection

- Developed a stochastic dual-gate based VFL feature selection approach.
- Significantly enhanced the accuracy and efficiency of VFL feature selection without exposing privacy.
- Anran Li, Hongyi Peng, Lan Zhang, Jiahui Huang, Qing Guo, Han Yu & Yang Liu, "FedSDG-FS: Efficient and Secure Feature Selection for Vertical Federated Learning," in *Proceedings of the 2023 IEEE International Conference on Computer Communications (INFOCOM'23)*, 2023.

Fairness Towards Early Participation



Han Yu, Zelei Liu, Yang Liu, Tianjian Chen, Mingshu Cong, Xi Weng, Dusit Niyato, Qiang Yang. A sustainable incentive scheme for federated learning. *IEEE Intelligent Systems* **35**(4), 2020.

Han Yu, Zelei Liu, Yang Liu, Tianjian Chen, Mingshu Cong, Xi Weng, Dusit Niyato, Qiang Yang, "A Fairness-aware Incentive Scheme for Federated Learning," in *Proceedings of the 3rd AAAI/ACM Conference on Artificial Intelligence, Ethics, and Society (AIES-20)*, pp. 393–399, 2020.

Individual

Contribution

- $q_i(t)$: Contribution of the dataset towards improving the FL model at t

Data Owner i

Cost

- $c_i(t)$: Cost of contributing a dataset at t
- $Y_i(t)$: A "regret queue" to track payoff due for data owner i at t
- $Q_i(t)$: A "temporal queue" to track how long data owner i has been waiting to receive full payoff from the federation at t

The Data Federation

Collective Utility

$U = \frac{1}{T}\sum_{t=0}^{T-1}\sum_{i=1}^{N} u_{i(t)}q_i(t)$:

Data owners who contribute high quality datasets should receive high payoff

Distribution of "Regret"

$$L(t) = \frac{1}{2}\sum_{i=1}^{N}[Y_i^2(t) + Q_i^2(t)]$$

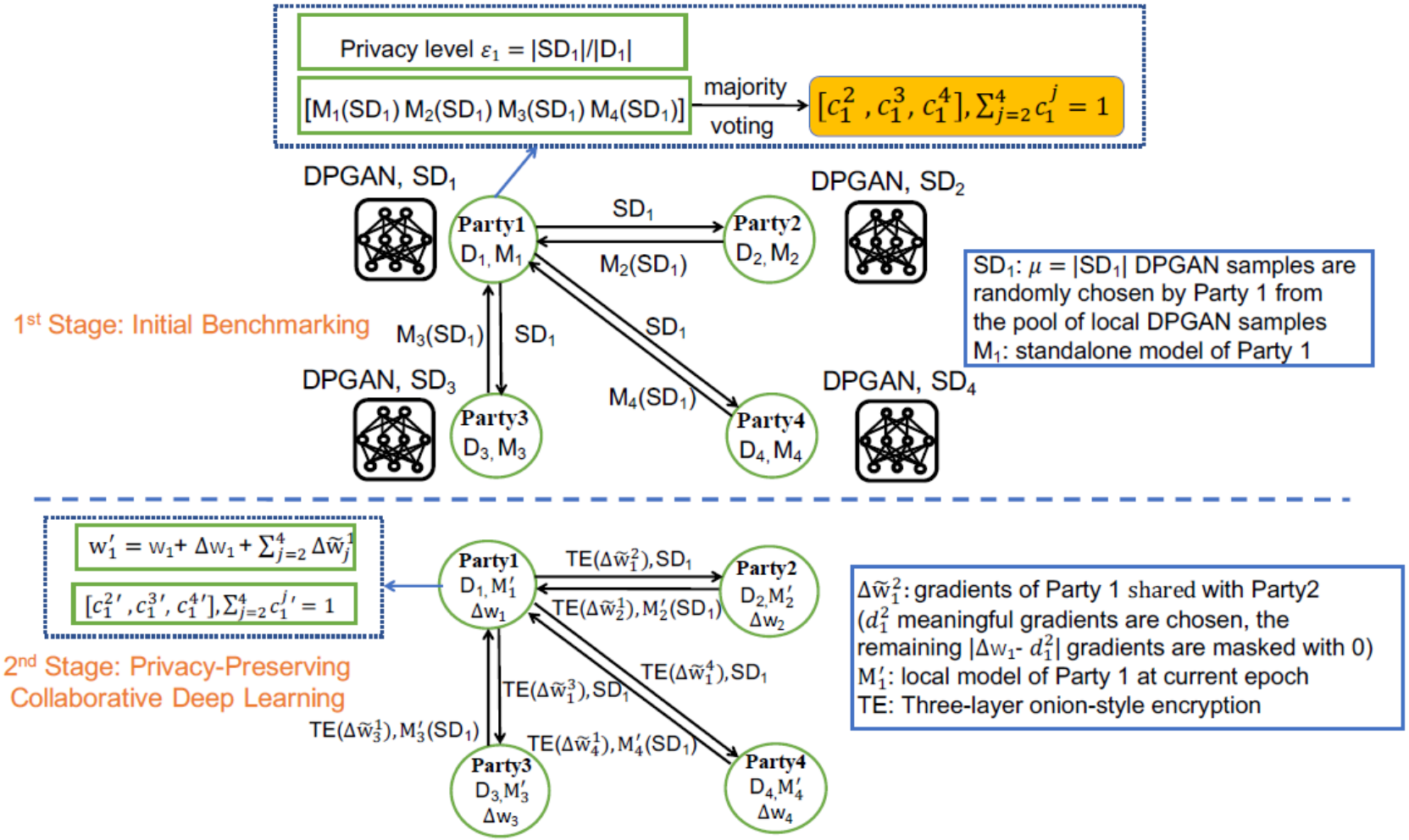
$$\Delta = \frac{1}{T}\sum_{t=0}^{T-1}[L(t+1) - L(t)]$$

Distribution of regret and waiting time among data owners + the change of such distributions over time

- **Contribution Fairness:** a data owner *i*'s payoff shall be positively related to his contribution $q_i(t)$;
- **Regret Distribution Fairness:** the difference of the regret and the temporal regret among data owners shall be minimized; and
- **Expectation Fairness:** the fluctuation of data owners' regret and temporal regret values shall be minimized

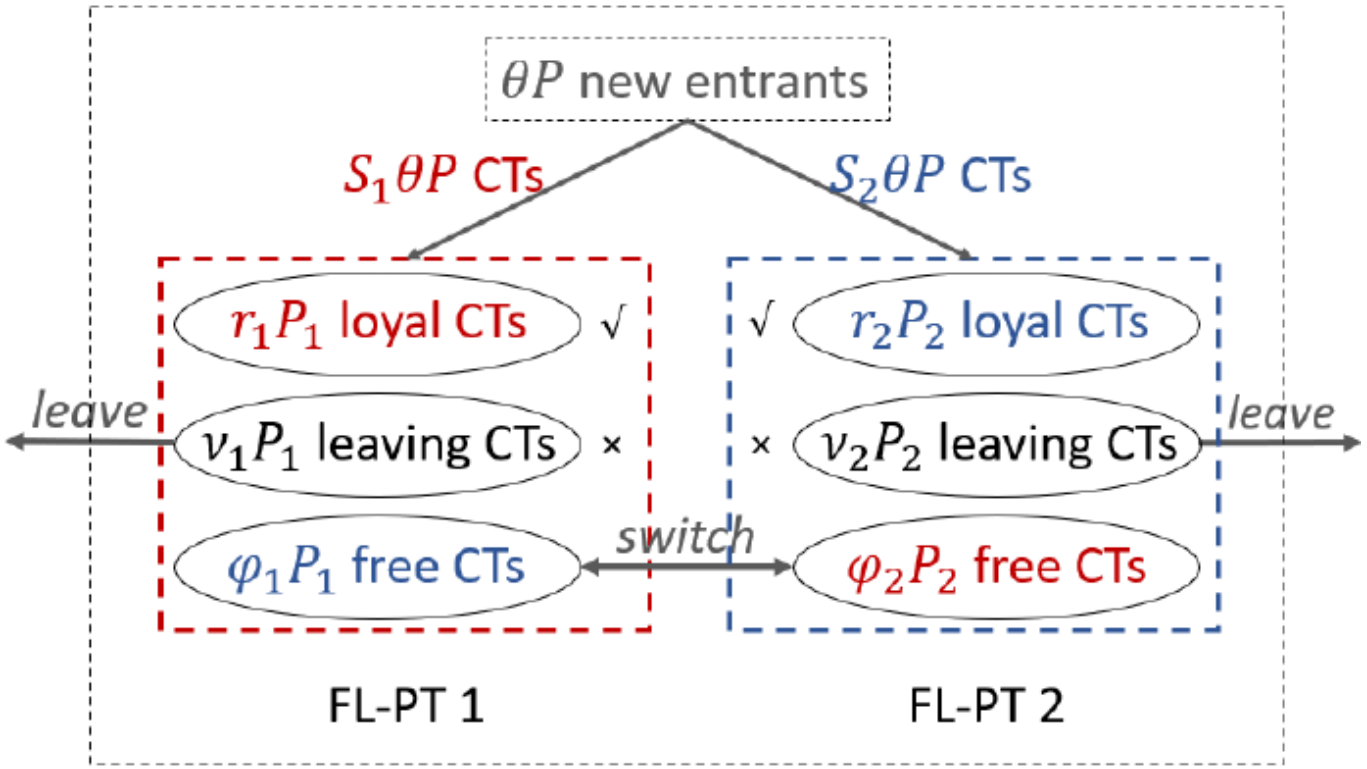
Fairness-Aware FL (Free-Rider Problem)

1. Each client decides the preferred level of sharing
2. Assessing the quality of local training data of each participant via mutual evaluation without looking at the raw data -> *Individual Local Credibility Scores*
3. Each FL client using the local credibility scores to guide the decision on from which other client to download model parameters for model update.



Lingjuan Lyu, Jiangshan Yu, Karthik Nandakumar, Yitong Li, Xingjun Ma, Jiong Jin, Han Yu & Kee Siong Ng. Towards fair and privacy-preserving federated deep models. *IEEE Transactions on Parallel and Distributed Systems* **31**(11), 2524–2541, 2020.

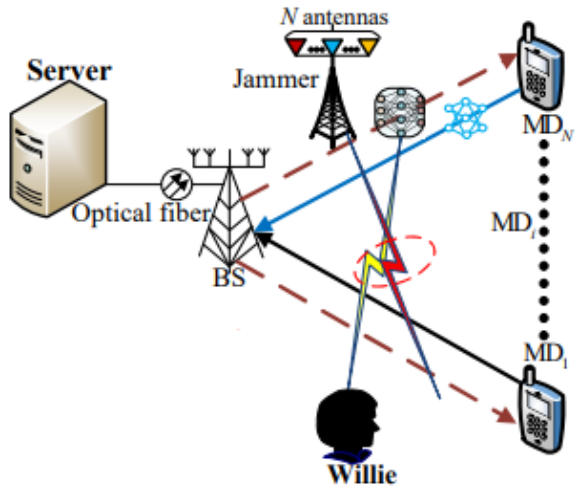
Fairness-Aware FL (Free-Rider Problem)



Xiaohu Wu & Han Yu, MarS-FL: Enabling Competitors to Collaborate in Federated Learning. *IEEE Transactions on Big Data*, 2022.

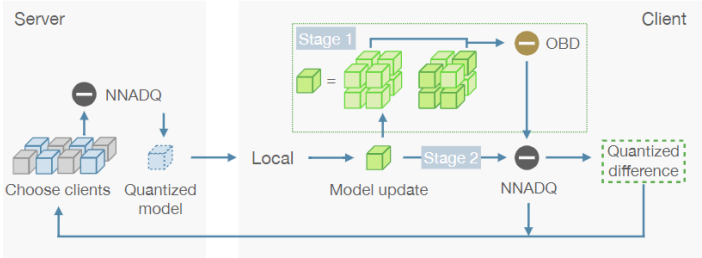
- An analytical framework to help **FL decision-makers** understand the impact of FL on firms' market shares under various market settings.
- For each **FL-PT**, characterize the process by which it joins FL as a non-cooperative game and derive its dominant strategy.
- For an **FL ecosystem manager**, provide a sufficient and necessary condition *Q* for maintaining market stability and quantify how friendly a given market is towards FL.
- Guide non-monetary FL incentive mechanisms to allocate model performance improvements among FL-PTs.
- Encourage larger data owners to overcome their fear of smaller FL-PTs free-riding on them and join FL.

Robust FL (Security & Scalability)



Covert Communication-based FL Defence

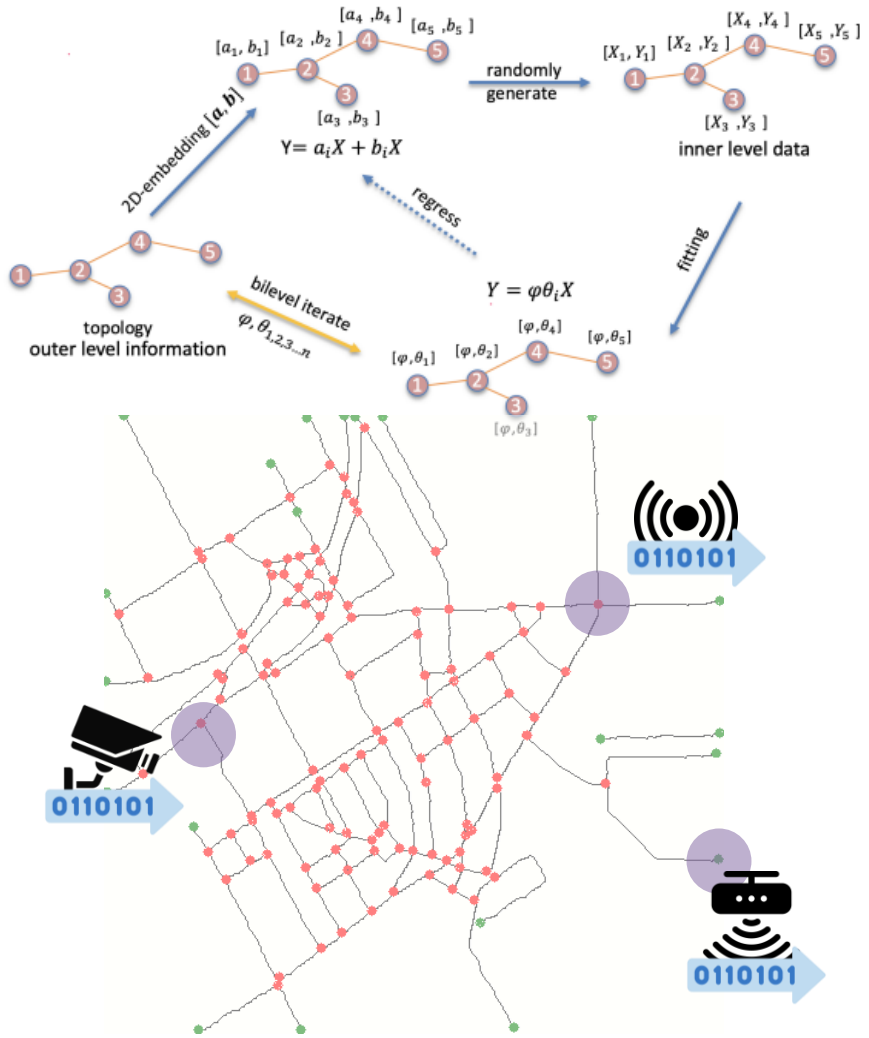
- The first covert communication-based federated learning approach to thwart eavesdropping attackers.
- Turns the problem of engaging a dynamic signal jammer into an economic problem to be optimized.
- Yuan-Ai Xie, Jiawen Kang, Dusit Niyato, Nguyen Thi Thanh Van, Nguyen Cong Luong, Zhixin Liu & Han Yu. Securing federated learning: A covert communication-based approach. *IEEE Network*, 2022.



Opportunistic Block Dropout for Scalable FL

- A unique opportunistic semantic block dropout approach to enable only important model blocks to be transmitted.
- Enables efficient training of high-performance large-scale deep FL models.
- Y. Chen, Z. Chen, P. Wu & H. Yu, "FedOBD: Opportunistic Block Dropout for Efficiently Training Large-scale Neural Networks through Federated Learning," *arXiv preprint arXiv:2208.05174*, 2022.

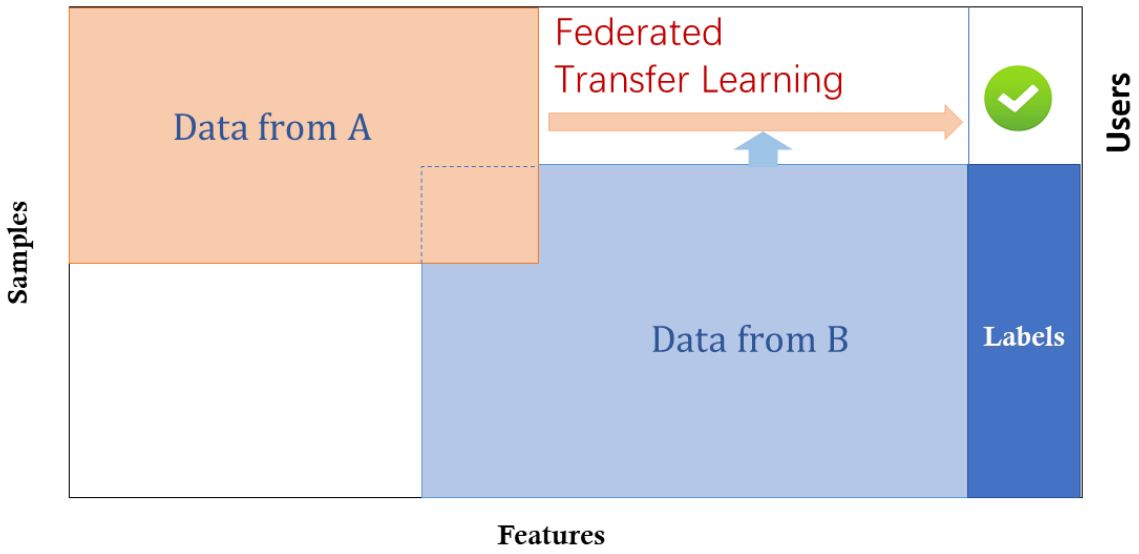
Personalizable FL (highlight)

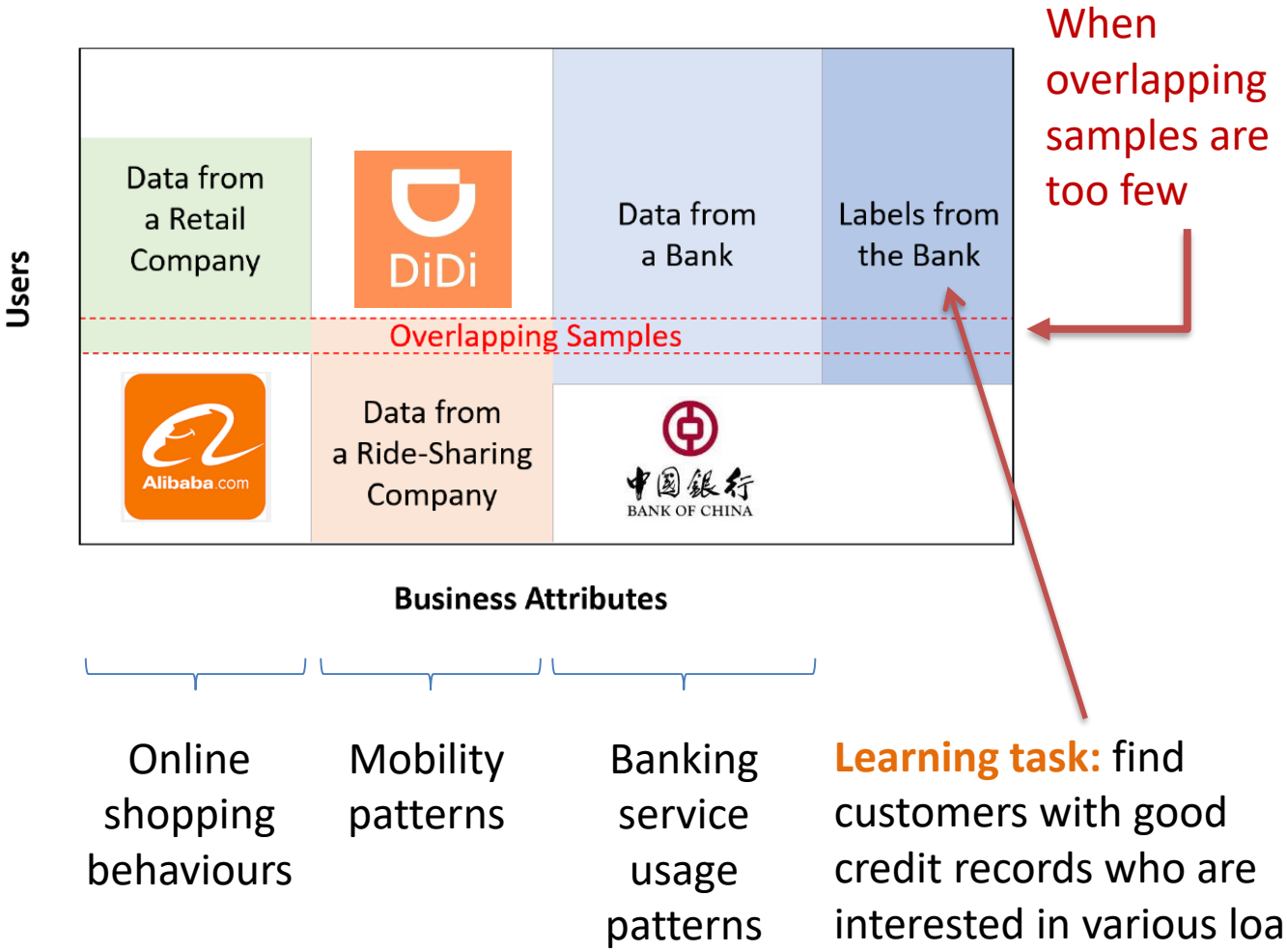


BiG-Fed: Bilevel Optimization Enhanced Graph-Aided Federated Learning

- Developed a one-of-its-kind federated graph neural network model which can be trained through bi-level optimization.
- Capable of performing federated learning on data silos related through a graph topology (FedGNN).
- Pengwei Xing, Songtao Lu, Lingfei Wu & Han Yu. BiG-Fed: Bilevel optimization enhanced graph-aided federated learning. *IEEE Transactions on Big Data*, 2022.

Transferrable FL (highlight)

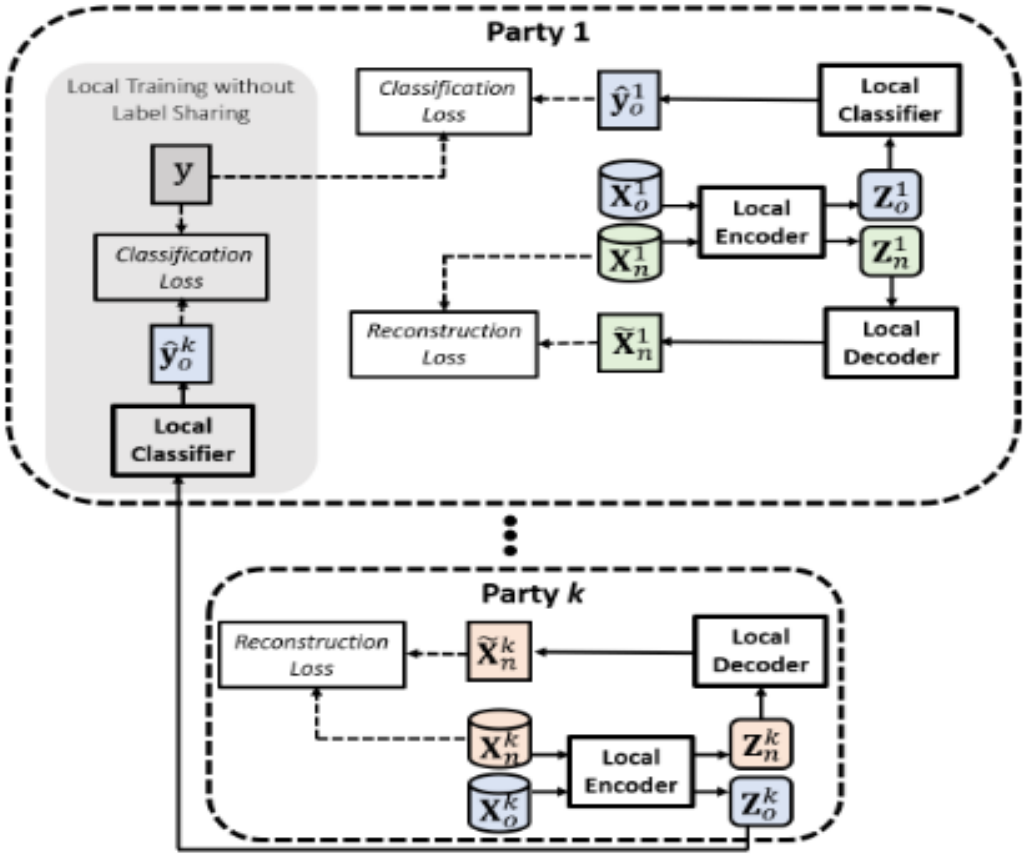




When overlapping samples are too few

Learning task: find customers with good credit records who are interested in various loans

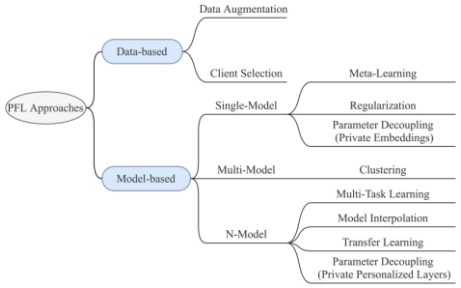
Transferrable FL (highlight)



Semi-Supervised Federated Heterogeneous Transfer Learning

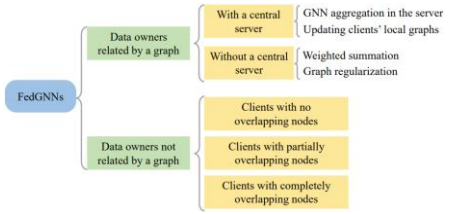
- Federated transfer learning (FTL) methods cannot be applied in practice due to insufficient overlapping data.
- SFHTL leverages unlabeled-non-overlapping samples to reduce FTL model overfitting.
- Siwei Feng, Boyang Li, Han Yu, Yang Liu & Qiang Yang. Semi-supervised federated heterogeneous transfer learning. *Knowledge-Based Systems* **252**, 2022.

Literature Surveys



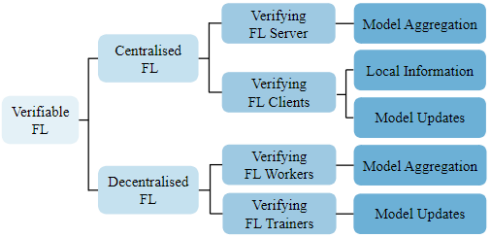
Personalized Federated Learning

- Alysa Ziying Tan, Han Yu, Lizhen Cui & Qiang Yang. Towards personalized federated learning. *IEEE Transactions on Neural Networks and Learning Systems*, 2022.



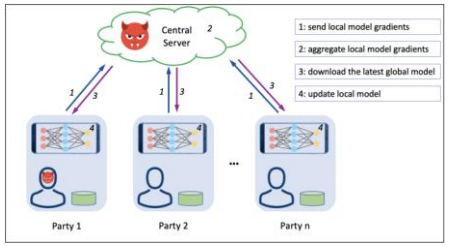
Federated Graph Neural Networks

- Rui Liu & Han Yu, "Federated Graph Neural Networks: Overview, Techniques and Challenges," *arXiv preprint arXiv:2202.07256*, 2022.



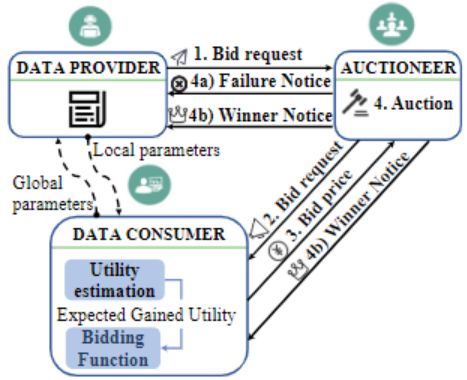
Verifiable Federated Learning

- Yanci Zhang & Han Yu, "Towards Verifiable Federated Learning," in *Proceedings of the 31st International Joint Conference on Artificial Intelligence (IJCAI'22)*, pp. 5686-5693, 2022.



Privacy and Robustness in Federated Learning

- Lingjuan Lyu, Han Yu, Xingjun Ma, Lichao Sun, Jun Zhao, Qiang Yang & Philip S. Yu, "Privacy and Robustness in Federated Learning: Attacks and Defenses," *IEEE Transactions on Neural Networks and Learning Systems*, 2022.



Trustworthy Real-time Bidding & Auctioning

- Xiaoli Tang & Han Yu, "Towards Trustworthy AI-Empowered Real-Time Bidding for Online Advertisement Auctioning," *arXiv preprint arXiv:2210.07770*, 2022

Fairness-Aware Federated Learning

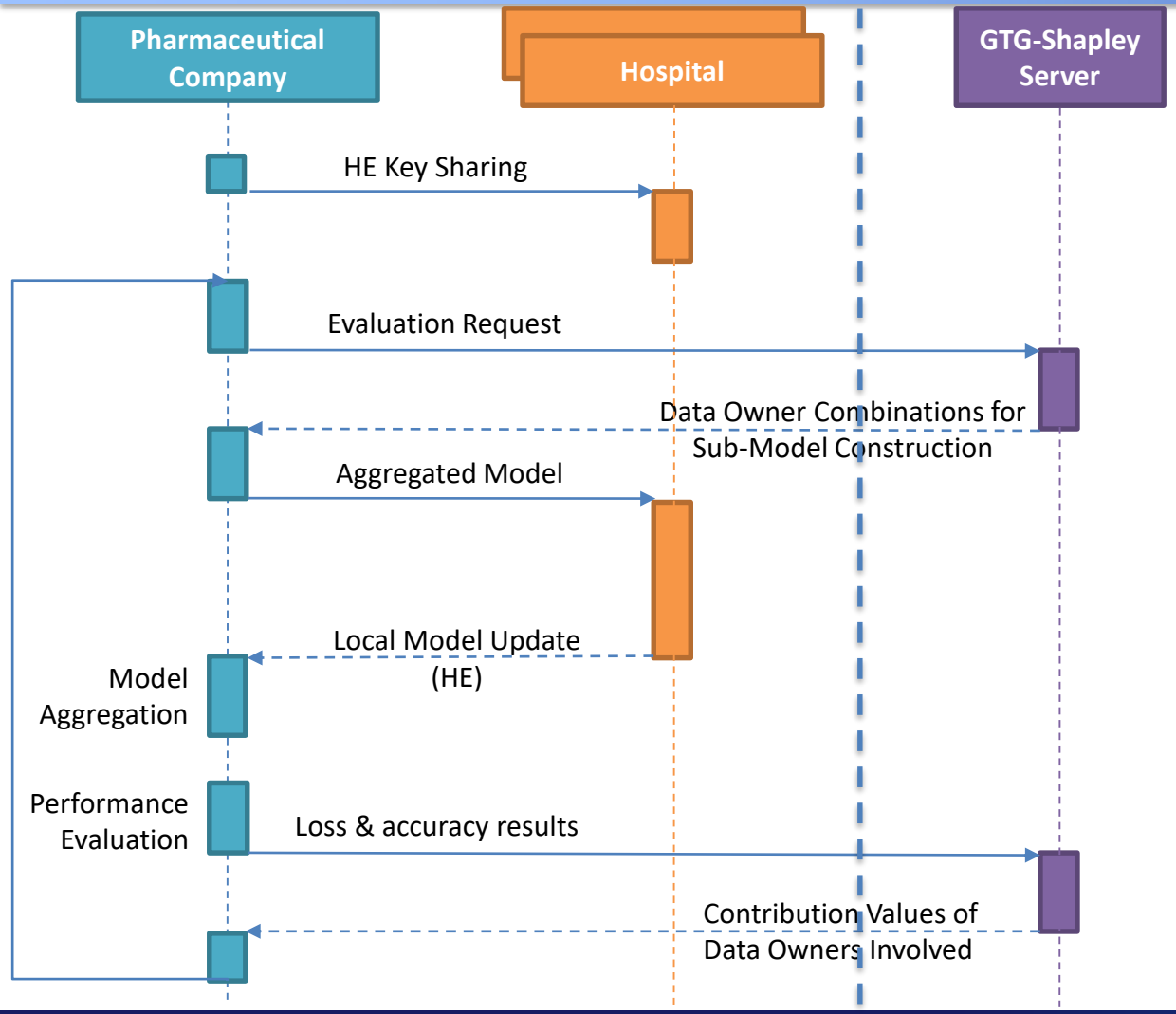
- Yuxin Shi, Han Yu & Cyril Leung, "Towards Fairness-Aware Federated Learning," *arXiv preprint arXiv:2111.01872*, 2021.

Agenda

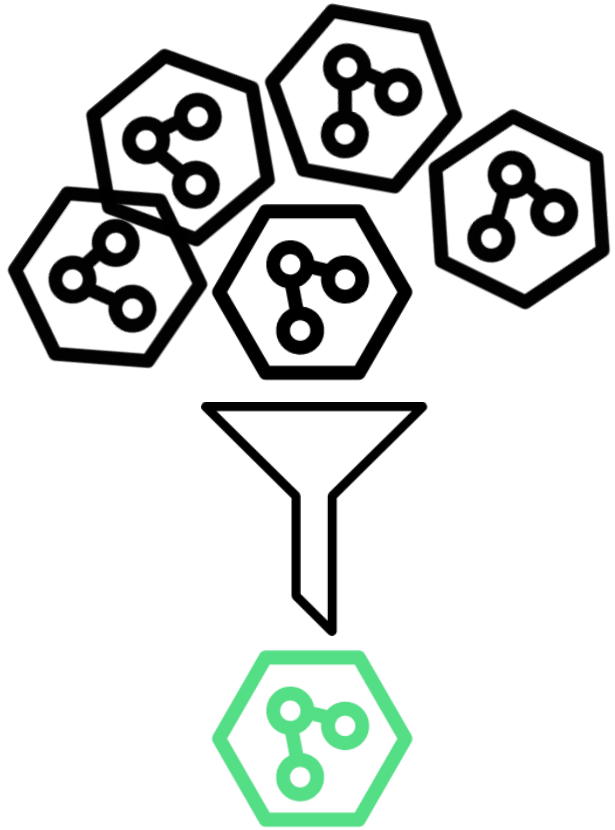
1: Theoretical Research in Trustworthy Ubiquitous Federated Learning

2: Translational Research in Trustworthy Ubiquitous Federated Learning

CAreFL – Contribution-Aware Federated Learning

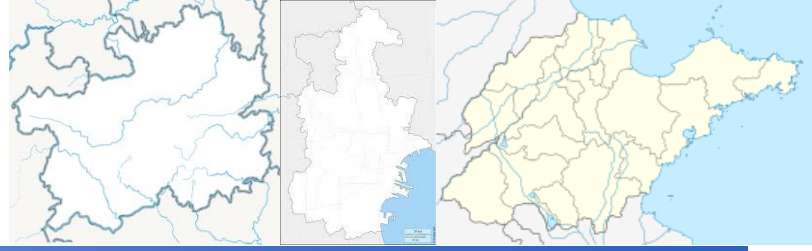


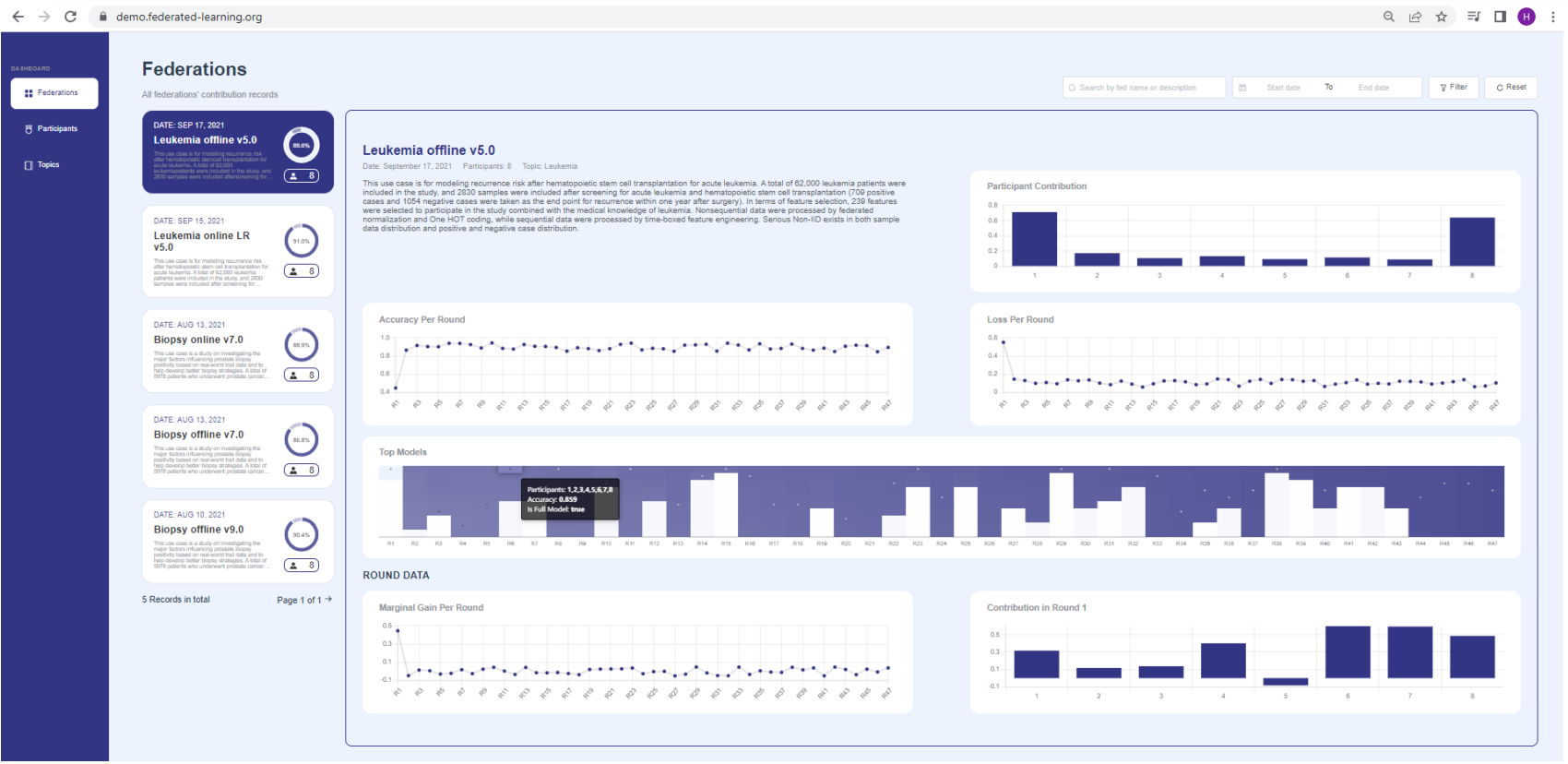
FL sub-models



"Best Subset" FL Model

Deployment in the Healthcare Industry

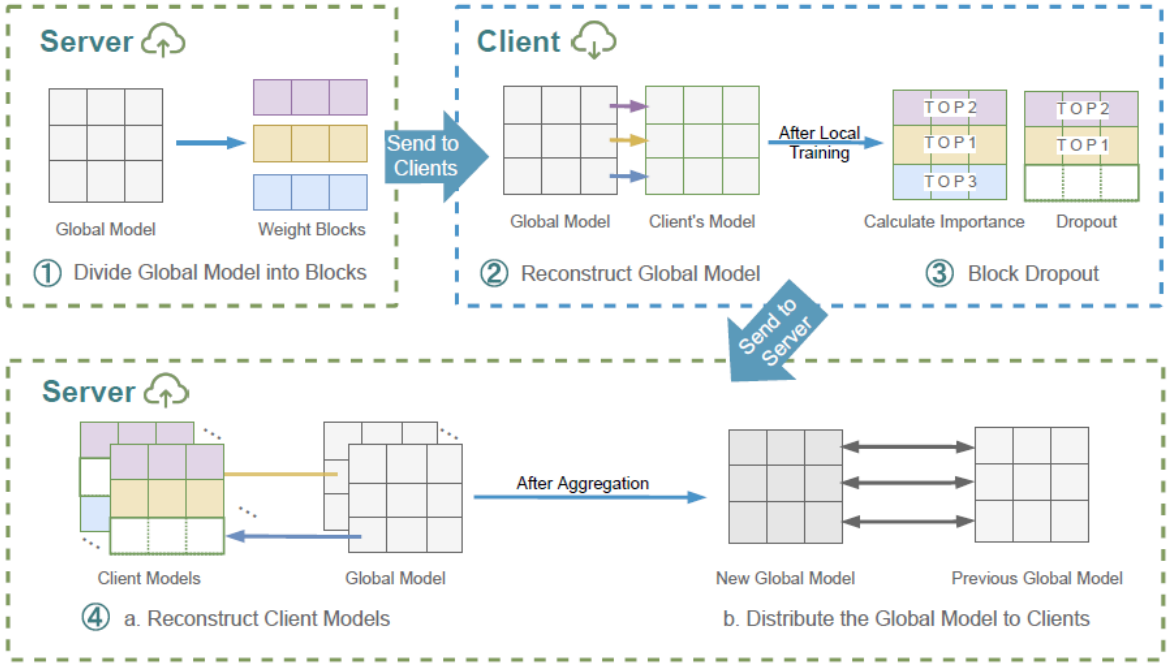


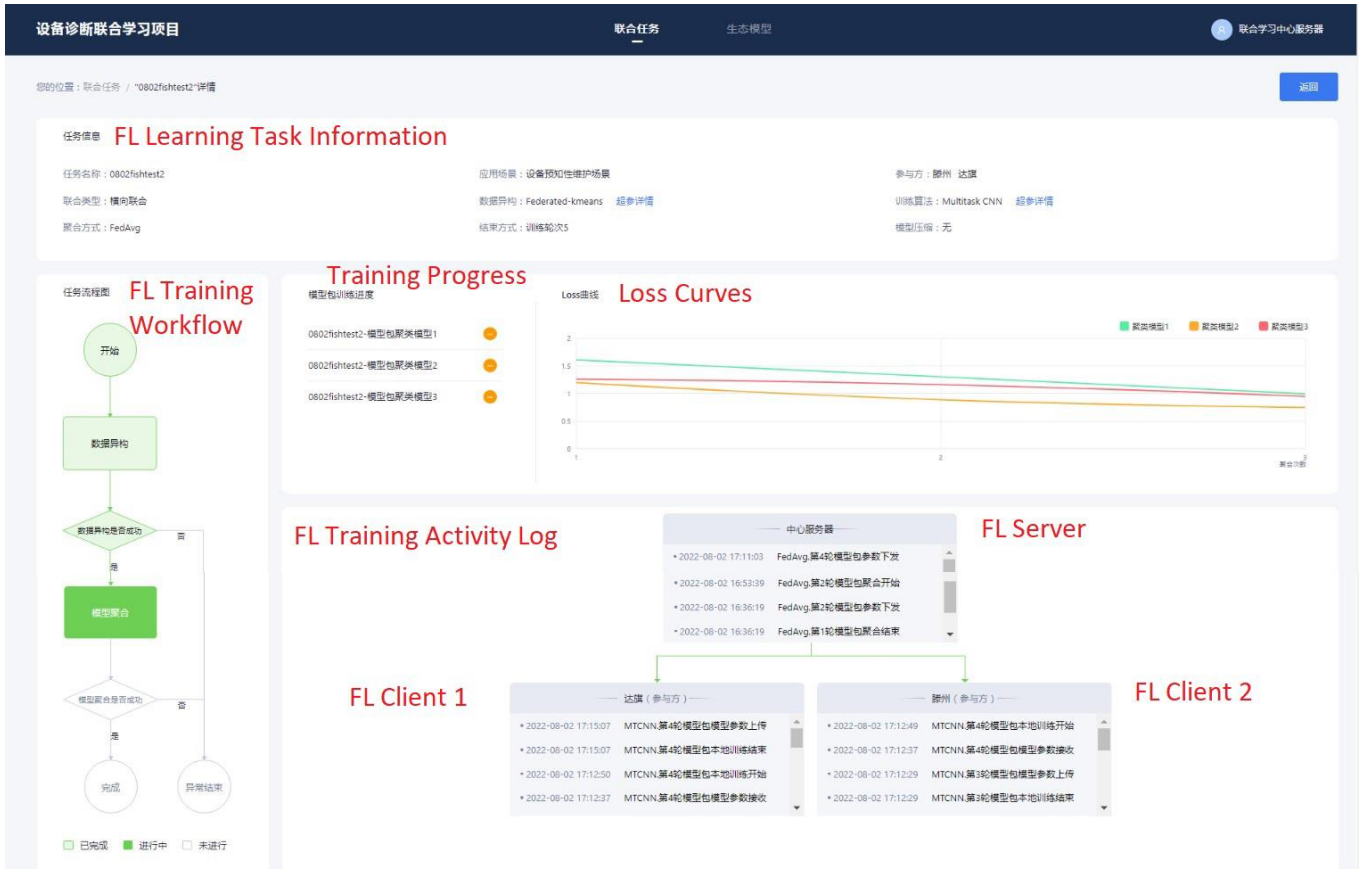


https://demo.federated-learning.org/

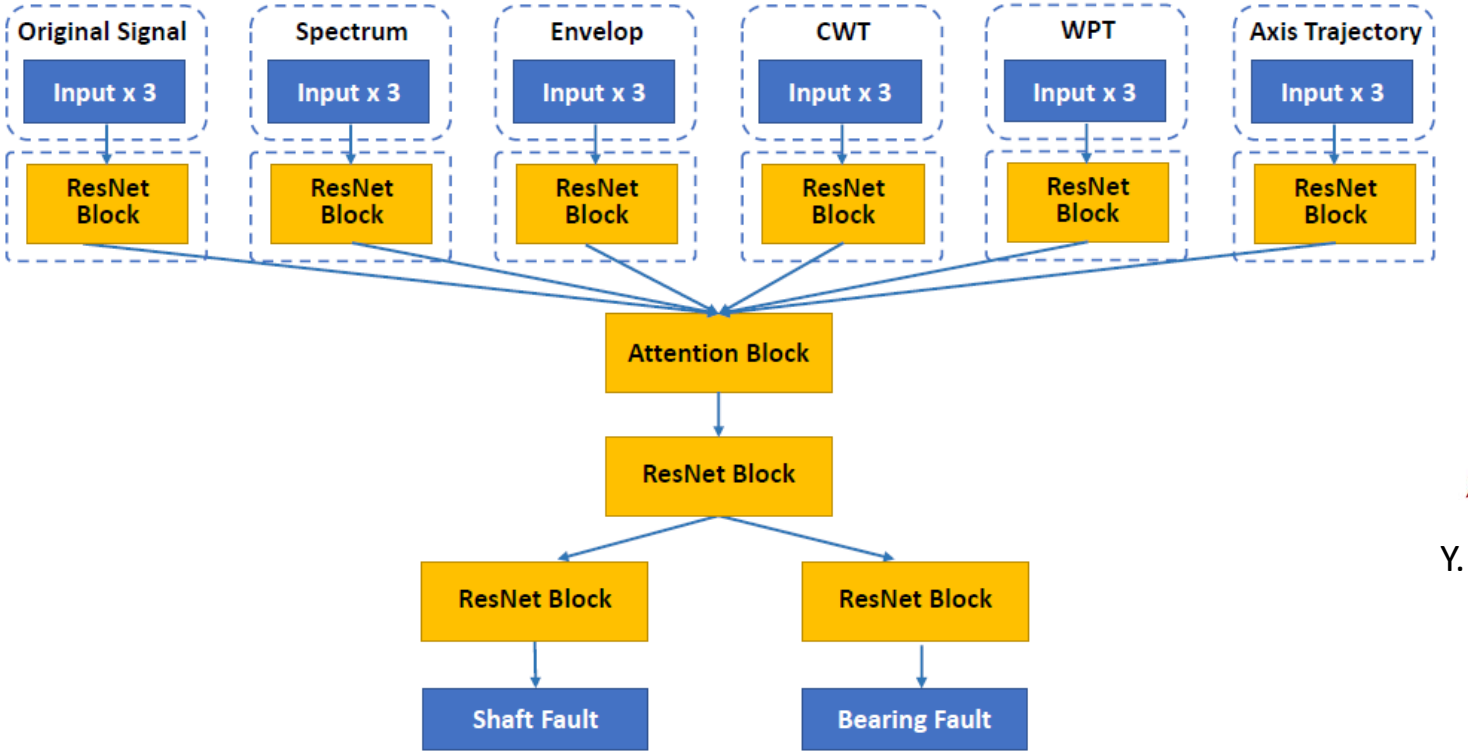
Z. Liu, Y. Chen, Y. Zhao, H. Yu, Y. Liu, R. Bao, J. Jiang, Z. Nie, Q. Xu & Q. Yang, "Contribution-Aware Federated Learning for Smart Healthcare," in *Proceedings of the 34th Annual Conference on Innovative Applications of Artificial Intelligence (IAAI-22)*, pp. 12396-12404, 2022. (**Innovative Application of AI Award**)

Federated Opportunistic Block Dropout for Industry 4.0





Deployment with ENN Group

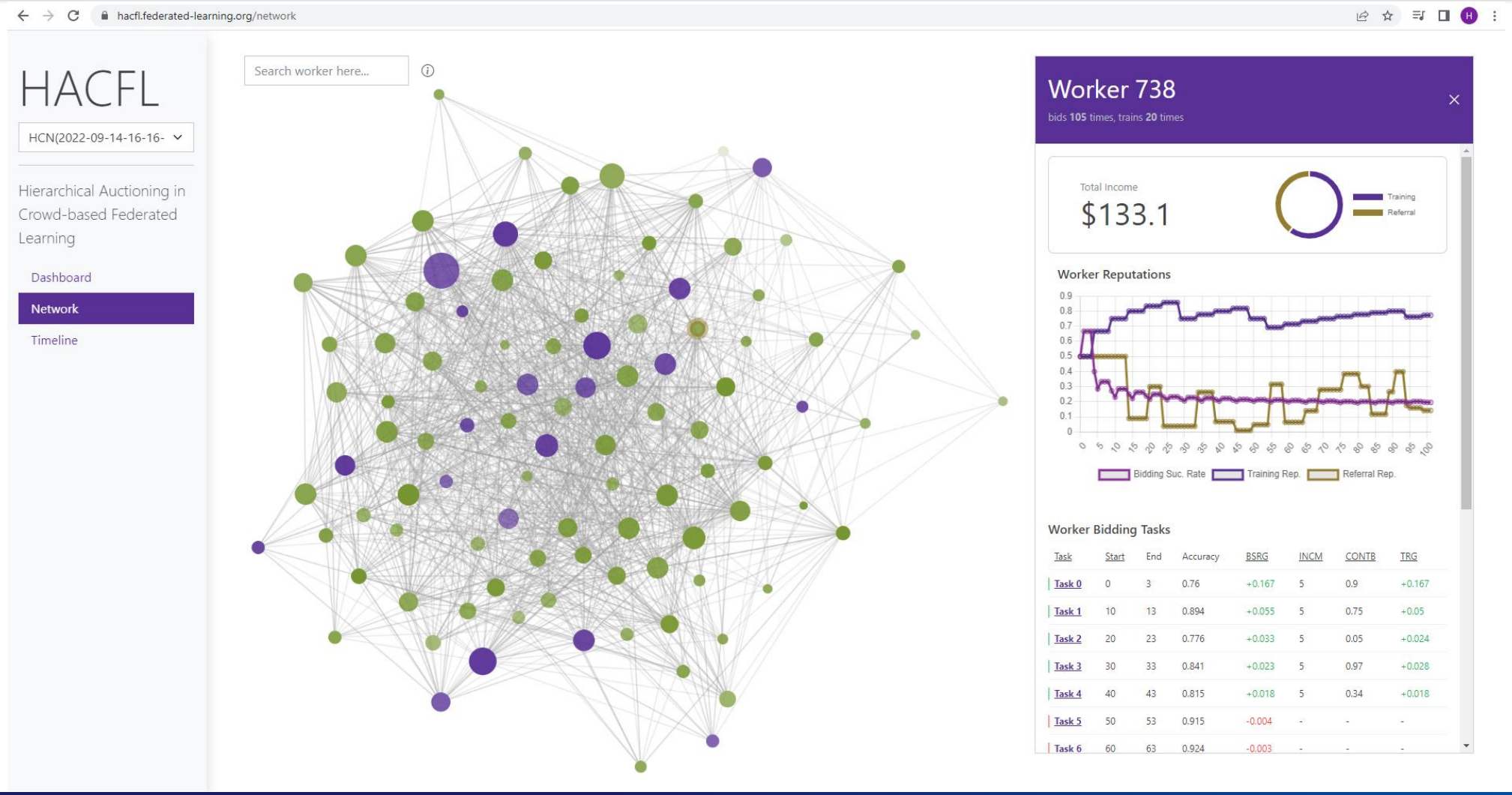


- Training a model with **29 million** parameters.
- Reduced total communication cost from **368 GB** to **104 GB**, while maintaining model performance at 85% F1 Score.
- Reduced model retraining time from **52 hours** to **14.5 hours** (at a limit of 2MB/sec bandwidth allowable for FL training).

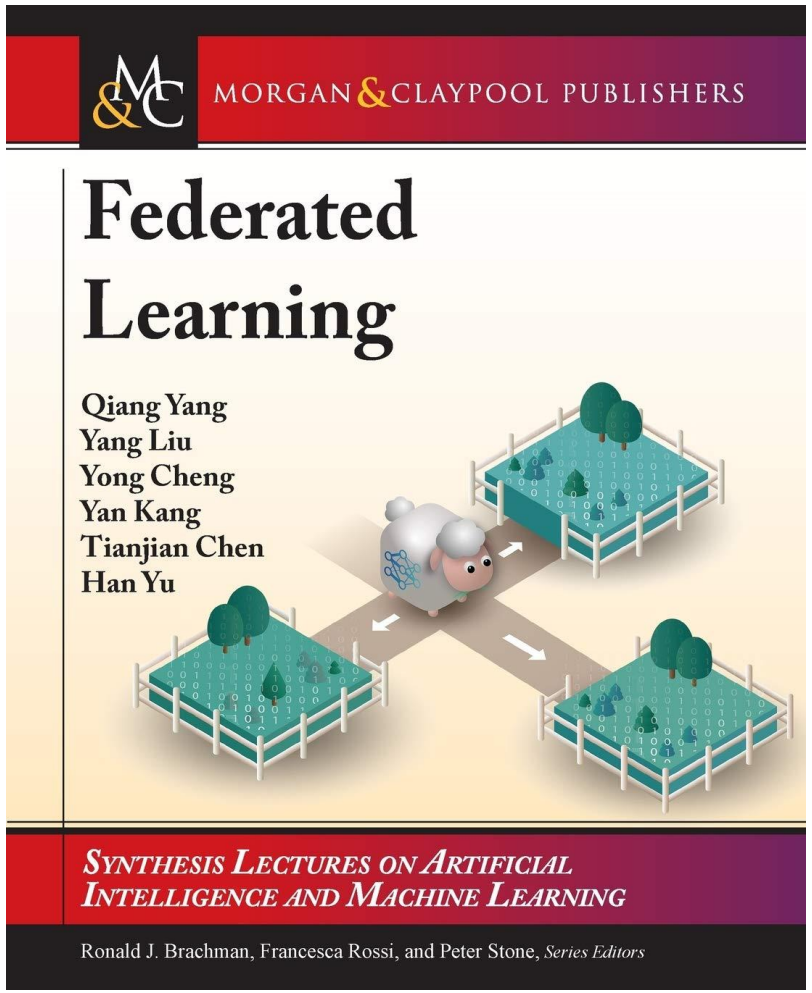
Y. Chen, Z. Chen, S. Guo, Y. Zhao, Z. Liu, P. Wu, C. Yang, Z. Li & H. Yu, "Efficient Training of Large-scale Industrial Fault Diagnostic Models through Federated Opportunistic Block Dropout," in *Proceedings of the 35th Annual Conference on Innovative Applications of Artificial Intelligence (IAAI-23)*, 2023. (**Innovative Application of AI Award**)

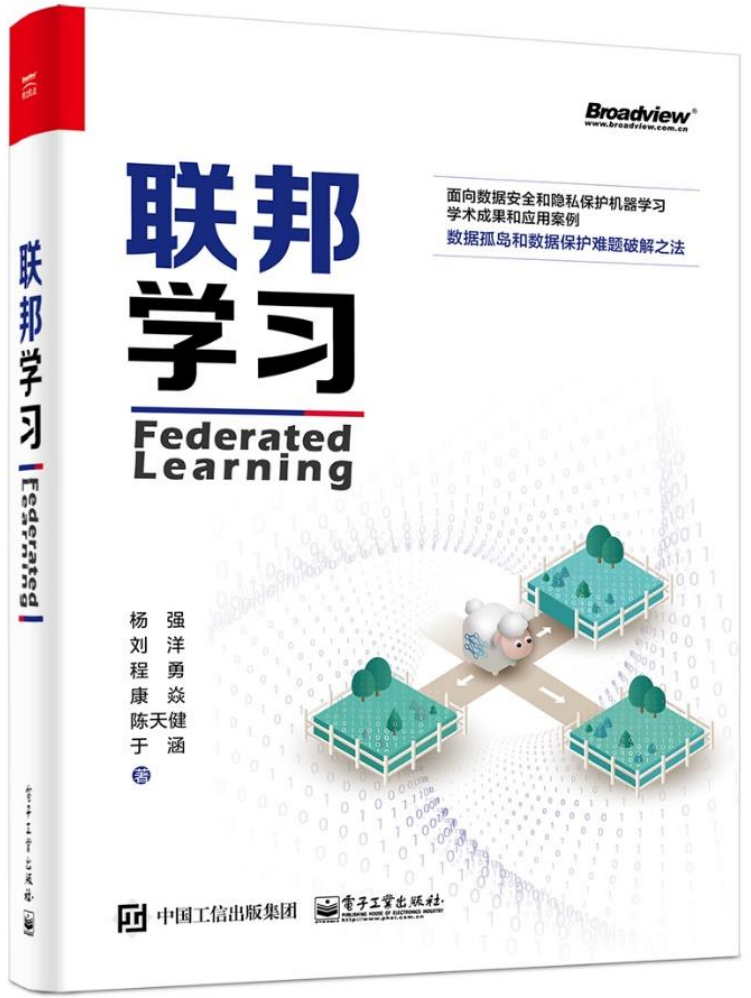
Auction-based Open Collaborative Hierarchical FL Network

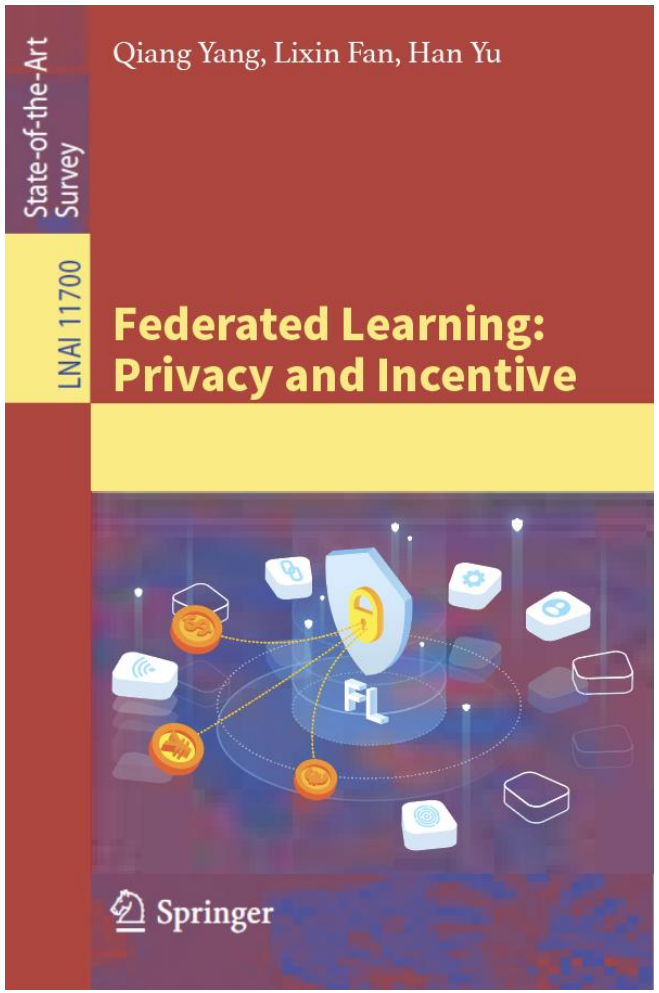
Demo System: https://hacfl.federated-learning.org/, Demo Video: https://youtu.be/qa90Qda3KBQ



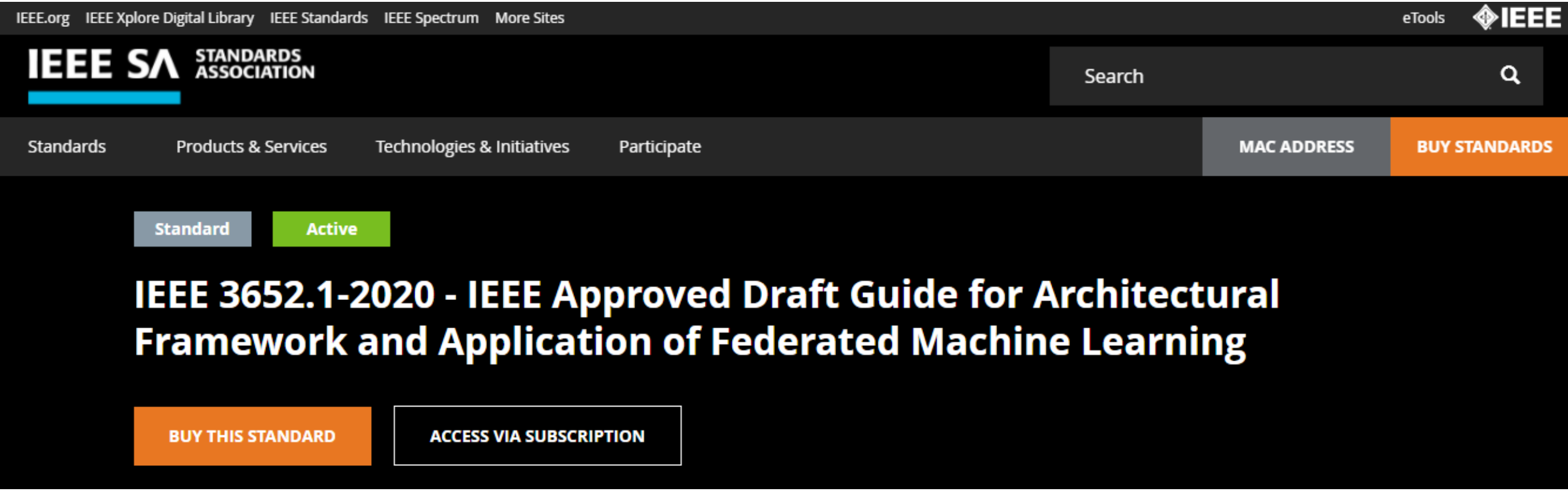
Books on the Topic of FL







IEEE P3652 Federated Machine Learning Standard



FL-Series Workshops

Past FL Special Sessions/Issues

Special Issue on Federated Machine Learning (2020)

Special Issue on Federated Learning: Algorithms, Systems, and Applications (2021)

Special Issue on Trustable, Verifiable, and Auditable Federated Learning (2022)

Upcoming FL Special Sessions/Issues

IEEE ICME 2023 Special Session Call for Papers
Trustworthy Federated Learning for Multimedia

- Submission link: https://cmt3.research.microsoft.com/ICME2023, please select "**SS2: Trustworthy Federated Learning for Multimedia**" in the Subject Areas section.
- Submission deadline: **15 Dec, 2022**.

IEEE TRANSACTIONS ON

NEURAL NETWORKS AND LEARNING SYSTEMS

A PUBLICATION OF THE IEEE COMPUTATIONAL INTELLIGENCE SOCIETY

www.ieee-cis.org/pubs/tnnls

14.255	0.05097	2.999	20.8
Impact Factor	Eigenfactor	Article Influence Score	CiteScore Powered by Scopus

Special Issue on **Trustworthy Federated Learning**

- Submission deadline: **01 Jun, 2023**.
- CFP and Submission Link: **TBA**

Thank you!

http://trustful.federated-learning.org/