Privacy-preserving decentralized learning methods for biomedical applications

Mohammad Tajabadi, Roman Martin, and Dominik Heider

Philip Frese

Advanced Artificial Intelligence in Biomedicine Seminar

January 9, 2025

Outline

Outline

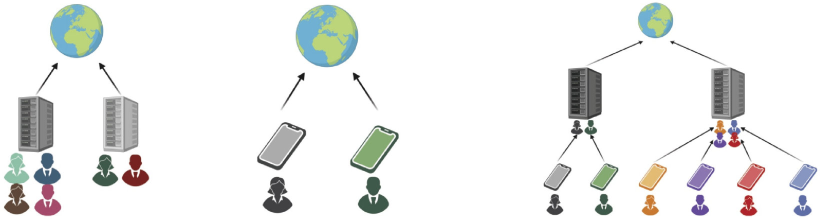
Motivation

- Great potential for artificial intelligence methods in biomedical field
  - Development and repurposing of drugs
  - Epidemiological modeling
  - New treatments, prognostics, and monitoring methods
- Traditional learning methods require massive amounts of data
  - Often not available at a single site, e.g., hospital
  - Regulations like GDPR limit sharing of medical patient data
- Decentralized learning methods allow for training new models without sharing data
- Common procedure: Multiple participants independently train models on their local datasets and share model parameters

Tajabadi et al. [10]

Outline

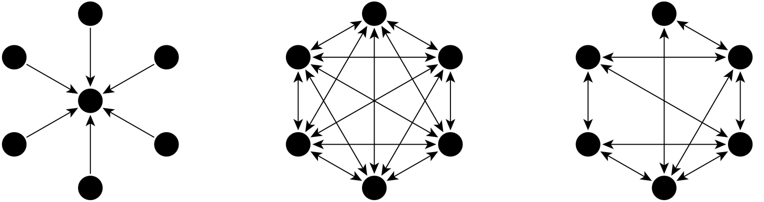
Decentralized Learning Settings



(a) Cross-silo learning (b) Cross-device learning (c) Cross-device forming ad hoc silos

Figure: Tajabadi et al. [10]

Network Topologies



(a) Centralized learning network (b) Fully meshed peer-to-peer network (c) Partially meshed peer-to-peer network

Figure: Tajabadi et al. [10]

Outline

Gossip Learning

- Partially meshed peer-to-peer network, entirely decentralized
- Each peer trains a model using local data
- Perform random walks over partial network to share models with other peers
- Peers merge models and update them using local data (online learning)
- All peers have the same model parameters at convergence

Ormándi et al. [8], Tajabadi et al. [10]

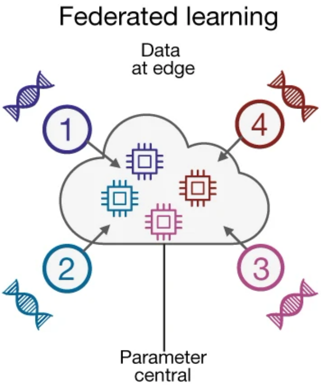
Gossip Learning: Applications

- Pros/Cons:
  - \+ No single point of failure, better robustness and scalability
  - − High data transfer, less efficient than federated learning in some experiments
- Brain tumor segmentation on multi-parametric MRI [1]
  - Introduce Gossip Mutual Learning (GML) for aggregating models in peers
  - Performance is higher than local models, comparable to federated learning (although 25% communication overhead), and lower than pooled model

Chen and Yuan [1], Hegedűs et al. [4]

Federated Learning

- Centralized learning network with one server and multiple clients
- Each client trains a local model with the local dataset
- Model parameters are sent to the server
- Server aggregates the local models, resulting in a global model which is distributed to clients



McMahan et al. [6], Tajabadi et al. [10], Figure: Warnat-Herresthal et al. [11]

Federated Learning: Applications

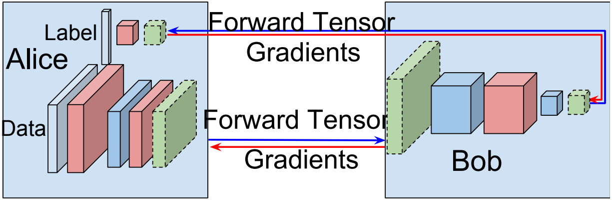
- Pros/Cons:
  - \+ Less data traffic than in gossip learning
  - − Potential single point of failure
- Federated Random Forest (FRF) models for disease prediction and classification [3]
  - Examined diseases: Liver disease, hepatocellular carcinoma, breast cancer, lung tumors
  - Performance comparable to centralized model, outperform local models
  - More stable for imbalanced datasets, no significant performance decrease when increasing number of datasets and decreasing their size

---

Hauschild et al. [3], Hegedűs et al. [4]

Split Learning

- Deep neural network is split between nodes and server
- Node performs forward pass and sends output (*smashed data*) to server for completion of forward pass, inverse for back propagation
- Loss computation can optionally be performed by node to avoid sharing labels (wrapped network)
- Multiple nodes: Round robin; server (centralized mode) or previous node (peer-to-peer mode) sends parameters to next node



Gupta and Raskar [2], Tajabadi et al. [10], Figure: [2]

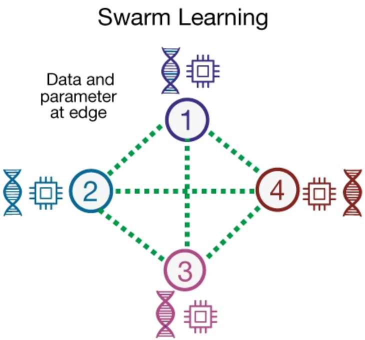
Split Learning: Applications

- Pros/Cons:
  - \+ Training is partially offloaded to server (reduced computation in nodes), configurable privacy-efficiency trade-off
  - – Nodes are processed sequentially (improved in variant *SplitFed*), only suitable for deep neural networks
- Split learning for biomedical image classification and clinical concept predictions on electronic health record (EHR) datasets [5]
  - Convolutional neural network for image classification, transformer (nodes) and fully connected network (server) for EHR data
  - Performance similar to federated learning and centralized learning

Li et al. [5]

Swarm Learning

- Decentralized form of collaborative learning
- Fully meshed peer-to-peer network, mainly for cross-silo settings
- Nodes train models using local data
- Parameters are exchanged via Swarm API and nodes merge models
- New nodes enroll via blockchain smart contract for enhanced security



Tajabadi et al. [10], Warnat-Herresthal et al. [11], Figure: [11]

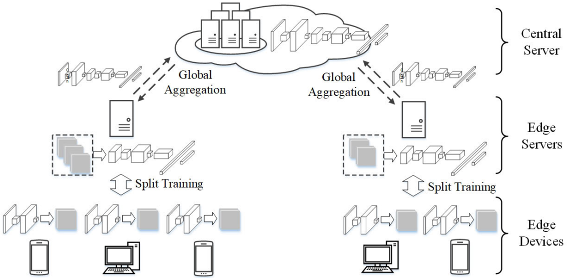
Swarm Learning: Applications

- Pros/Cons
  - \+ No central entity, enhanced security
  - − High data transfer including redundant data
- Disease diagnosis in human nails [7]
  - Image classification using transfer learning (from VGG16 and InceptionV3)
  - Results comparable to central model, slight improvement when data is split unevenly

Mohammed et al. [7]

Edge Learning

- *Edge* refers to edge devices (data collection) and edge servers (one step away from edge devices)
- Edge computing: Perform computations near the data, Fog computing: Computations on edge servers
- Example architecture EdgeFed:



Tajabadi et al. [10], Ye et al. [12], Figure: [12]

Edge Learning: Applications

- Pros/Cons:
  - \+ Increased privacy (depending on architecture), reduced communication cost
  - − Limited processing power in edge devices
- DeepFog healthcare monitoring system [9]
  - Three-layer architecture: physical (data collection), fog (data processing), and cloud layers
  - Tasks: Prediction of diabetes and hypertension attacks, stress type classification

Priyadarshini et al. [9]

Outline

Categories of Decentralized Learning Systems

Categories	**Systems with a centralized authority**	**Peer-to-peer systems**
Learning methods	federated learning, split learning, edge learning	gossip learning, swarm learning
Collaboration	all nodes connect to a central server	direct communication between nodes
Advantages	facilitated collaboration	enhanced fault tolerance
Disadvantages	server has sole authority over training process, single point of failure	higher data transfer
Settings	cross-device & cross-silo	cross-device (GL), cross-silo (SL)

Tajabadi et al. [10]

Privacy Limitations

- Privacy preservation is not inherently guaranteed and depends on architecture and models
- Model parameters may leak training data (and thereby sensitive information)
- Additional security measures to be considered:
  - Secure multi-party computation
  - Homomorphic encryption
  - Differential privacy

Tajabadi et al. [10]

Conclusion

- Decentralized learning methods often match performance of traditional methods
- Factors for selecting a learning method:
  - Model type
  - Network capacity
  - Network stability
  - Computational power
  - Desired level of control
- Methods could be combined in hybrid architectures
- Significant role in growing potential to connect institutions for, e.g., studying rare diseases

Tajabadi et al. [10]

Thank you for your attention!

Questions?

References I

[1] Jingyun Chen and Yading Yuan.
Decentralized Gossip Mutual Learning (GML) for brain tumor segmentation on multi-parametric MRI.
In *2023 IEEE EMBS Special Topic Conference on Data Science and Engineering in Healthcare, Medicine and Biology*, pages 63–64, Malta, December 2023. IEEE.

[2] Otkrist Gupta and Ramesh Raskar.
Distributed learning of deep neural network over multiple agents, 2018.
arXiv preprint arXiv:1810.06060v1.

References II

[3] Anne-Christin Hauschild, Marta Lemanczyk, Julian Matschinske, Tobias Frisch, Olga Zolotareva, Andreas Holzinger, Jan Baumbach, and Dominik Heider.
Federated Random Forests can improve local performance of predictive models for various healthcare applications.
Bioinformatics, 38(8):2278–2286, April 2022.

[4] István Hegedűs, Gábor Danner, and Márk Jelasity.
Decentralized learning works: An empirical comparison of gossip learning and federated learning.
Journal of Parallel and Distributed Computing, 148:109–124, February 2021.

References III

[5] Zhuohang Li, Chao Yan, Xinmeng Zhang, Gharib Gharibi, Zhijun Yin, Xiaoqian Jiang, and Bradley A. Malin.
Split Learning for Distributed Collaborative Training of Deep Learning Models in Health Informatics.
AMIA ... Annual Symposium proceedings. AMIA Symposium, 2023:1047–1056, 2023.

[6] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas.
Communication-Efficient Learning of Deep Networks from Decentralized Data.
In Aarti Singh and Jerry Zhu, editors, *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, volume 54 of *Proceedings of Machine Learning Research*, pages 1273–1282. PMLR, April 2017.

References IV

[7] Aasim Mohammed, P. S. Shrikanth Karthik, Razik Fatin Shariff, Tankala Sunaina, Arti Arya, and Pooja Agarwal.
Privacy Preserving Early Disease Diagnosis in Human Nails Using Swarm Learning.
In Jyoti Choudrie, Parikshit N. Mahalle, Thinagaran Perumal, and Amit Joshi, editors, *ICT for Intelligent Systems*, volume 361, pages 117–130, Singapore, 2023. Springer Nature Singapore.
Series Title: Smart Innovation, Systems and Technologies.

[8] Róbert Ormándi, István Hegedűs, and Márk Jelasity.
Gossip learning with linear models on fully distributed data.
Concurrency and Computation: Practice and Experience, 25(4):556–571, February 2013.

References V

[9] Rojalina Priyadarshini, Rabindra Kumar Barik, and Harishchandra Dubey.
DeepFog: Fog Computing-Based Deep Neural Architecture for Prediction of Stress Types, Diabetes and Hypertension Attacks.
Computation, 6(4):62, December 2018.

[10] Mohammad Tajabadi, Roman Martin, and Dominik Heider.
Privacy-preserving decentralized learning methods for biomedical applications.
Computational and Structural Biotechnology Journal, 23:3281–3287, December 2024.

References VI

[11] Stefanie Warnat-Herresthal, Hartmut Schultze, Krishnaprasad Lingadahalli Shastry, Sathyanarayanan Manamohan, Saikat Mukherjee, Vishesh Garg, Ravi Sarveswara, et al.
Swarm Learning for decentralized and confidential clinical machine learning.
Nature, 594(7862):265–270, June 2021.

[12] Yunfan Ye, Shen Li, Fang Liu, Yonghao Tang, and Wanting Hu.
EdgeFed: Optimized Federated Learning Based on Edge Computing.
IEEE Access, 8:209191–209198, 2020.