
Awesome Federated Learning

A list of resources related to federated learning and privacy in machine learning.

Related Awesome Lists

- [tushar-semwal/awesome-federated-computing](#)

Papers

Introduction & Survey

- Towards Efficient Synchronous Federated Training: A Survey on System Optimization Strategies <https://ieeexplore.ieee.org/document/9780218>
- The Internet of Federated Things (IoFT) <https://ieeexplore.ieee.org/document/9611259>
- Advances and Open Problems in Federated Learning <https://arxiv.org/pdf/1912.04977.pdf>
- Federated Machine Learning: Concept and Applications <https://arxiv.org/pdf/1902.04885>
- Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection <https://arxiv.org/abs/1907.09693>
- Demystifying Parallel and Distributed Deep Learning: An In-Depth Concurrency Analysis <https://arxiv.org/abs/1802.09941>
- EdgeAI: A Vision for Deep Learning in IoT Era <https://arxiv.org/abs/1910.10356>
- Machine Learning Systems for Highly-Distributed and Rapidly-Growing Data <https://arxiv.org/abs/1910.08663>
- No Peek: A Survey of private distributed deep learning <https://arxiv.org/pdf/1812.03288>
- Federated Learning in Mobile Edge Networks: A Comprehensive Survey <https://arxiv.org/abs/1909.11875>

Privacy and Security

- Federated Learning with Formal Differential Privacy Guarantees <https://ai.googleblog.com/2022/02/federated-learning-with-formal.html>
- Applying Differential Privacy to Large Scale Image Classification <https://ai.googleblog.com/2022/02/applying-differential-privacy-to-large.html>

-
- Towards Causal Federated Learning For Enhanced Robustness And Privacy <https://arxiv.org/pdf/2104.06557.pdf>
ICLR DPML 2021
 - FedAUX: Leveraging Unlabeled Auxiliary Data in Federated Learning <https://arxiv.org/abs/2102.02514>
 - OpenFL: An open-source framework for Federated Learning <https://arxiv.org/abs/2105.06413>
 - A Bayesian Federated Learning Framework with Multivariate Gaussian Product <https://arxiv.org/abs/2102.01936>
 - Communication-Efficient Learning of Deep Networks from Decentralized Data <https://arxiv.org/pdf/1602.05629>
 - Practical Secure Aggregation for Federated Learning on User-Held Data <https://arxiv.org/abs/1611.04482>
 - Practical Secure Aggregation for Privacy-Preserving Machine Learning <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/ae87385258d90b9e48377ed49d83d467b45d5776.pdf>
 - A Hybrid Approach to Privacy-Preserving Federated Learning <https://arxiv.org/abs/1812.03224>
 - Analyzing Federated Learning through an Adversarial Lens <https://arxiv.org/pdf/1811.12470>
 - How To Backdoor Federated Learning <https://arxiv.org/abs/1807.00459>
 - Comprehensive Privacy Analysis of Deep Learning: Stand-alone and Federated Learning under Passive and Active White-box Inference Attack <https://arxiv.org/abs/1812.00910>
 - Beyond Inferring Class Representatives: User-Level Privacy Leakage From Federated Learning <https://arxiv.org/pdf/1812.00535>
 - Exploiting Unintended Feature Leakage in Collaborative Learning <https://arxiv.org/abs/1805.04049>
 - Analyzing Federated Learning through an Adversarial Lens <https://arxiv.org/abs/1811.12470>
 - Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning <https://arxiv.org/abs/1702.07464>
 - Protection Against Reconstruction and Its Applications in Private Federated Learning <https://arxiv.org/pdf/1812.00984>
 - Boosting Privately: Privacy-Preserving Federated Extreme Boosting for Mobile Crowdsensing <https://arxiv.org/abs/1907.10218>
 - Differentially Private Data Generative Models <https://arxiv.org/pdf/1812.02274>
 - Differentially Private Federated Learning: A Client Level Perspective <https://arxiv.org/abs/1712.07557>
 - Privacy-Preserving Collaborative Deep Learning with Unreliable Participants <https://arxiv.org/abs/1812.10113>
 - Scalable Private Learning with PATE <https://arxiv.org/abs/1802.08908>
 - Reducing leakage in distributed deep learning for sensitive health data <https://www.media.mit.edu/publication/leakage-in-distributed-deep-learning-for-sensitive-health-data-accepted-to-iclr-2019-workshop-on-ai-for-social-good-2019/>

-
- Deep Leakage from Gradients <http://papers.nips.cc/paper/9617-deep-leakage-from-gradients.pdf>
 - Gradient-Leaks: Understanding and Controlling Deanonimization in Federated Learning <https://arxiv.org/abs/1805.05838>

System and Application

- Pisces: Efficient Federated Learning via Guided Asynchronous Training <https://dl.acm.org/doi/abs/10.1145/3542>
- Record and Reward Federated Learning Contributions with Blockchain <https://mblocklab.com/RecordandReward>
- Flower: A Friendly Federated Learning Framework <https://arxiv.org/pdf/2007.14390.pdf>
- Learning Private Neural Language Modeling with Attentive Aggregation <https://arxiv.org/pdf/1812.07108>
- Dynamic Sampling and Selective Masking for Communication-Efficient Federated Learning <https://arxiv.org/abs/2003.09603>
- Decentralized Knowledge Acquisition for Mobile Internet Applications <https://link.springer.com/article/10.1007/978-3-319-00775-w>
- A generic framework for privacy preserving deep learning <https://arxiv.org/pdf/1811.04017.pdf>
- Federated Learning of N-gram Language Models <https://arxiv.org/pdf/1910.03432.pdf>
- Towards Federated Learning at Scale: System Design <https://arxiv.org/pdf/1902.01046.pdf>
- Federated Learning for Keyword Spotting <https://arxiv.org/abs/1810.05512>
- Federated Learning in Distributed Medical Databases: Meta-Analysis of Large-Scale Subcortical Brain Data <https://arxiv.org/abs/1810.08553>
- Federated Collaborative Filtering for Privacy-Preserving Personalized Recommendation System <https://arxiv.org/pdf/1901.09888>
- Confederated Machine Learning on Horizontally and Vertically Separated Medical Data for Large-Scale Health System Intelligence <https://arxiv.org/abs/1910.02109>
- Privacy-Preserving Deep Learning Computation for Geo-Distributed Medical Big-Data Platform <http://www.cs.ucf.edu/~mohaisen/doc/dsn19b.pdf>
- Institutionally Distributed Deep Learning Networks <https://arxiv.org/abs/1709.05929>
- Multi-Institutional Deep Learning Modeling Without Sharing Patient Data: A Feasibility Study on Brain Tumor Segmentation <https://arxiv.org/abs/1810.04304>
- Split learning for health: Distributed deep learning without sharing raw patient data <https://www.media.mit.edu/publications/split-learning-for-health-distributed-deep-learning-without-sharing-raw-patient-data/>

-
- Continuous Delivery for Machine Learning <https://martinfowler.com/articles/cd4ml.html#EvolvingIntelligentSy>
 - Ease.ml/ci & Ease.ml/meter Towards Data Management for Statistical Generalization <http://ease.ml/>
 - VisionAir: Using Federated Learning to estimate Air Quality using the Tensorflow API for Java <https://blog.tensorflow.org/2020/02/visionair-using-federated-learning-to-estimate-airquality-tensorflow-api-java.html>
 - Federated Optimization in Heterogeneous Networks <https://arxiv.org/abs/1812.06127>

Un-org

- FedProf: Optimizing Federated Learning with Dynamic Data Profiling <https://arxiv.org/abs/2102.01733>
- FedBN: Federated Learning on Non-IID Features via Local Batch Normalization <https://arxiv.org/abs/2102.07623>
- A Scalable Approach for Partially Local Federated Learning <https://ai.googleblog.com/2021/12/a-scalable-approach-for-partially-local.html?m=1>
- Federated Visual Classification with Real-World Data Distribution <https://arxiv.org/abs/2003.08082>
- Measuring the Effects of Non-Identical Data Distribution for Federated Visual Classification <https://arxiv.org/abs/1909.06335>
- LEAF: A Benchmark for Federated Settings <https://arxiv.org/abs/1812.01097>
- On the Convergence of FedAvg on Non-IID Data <https://arxiv.org/abs/1907.02189>
- Privacy-preserving Federated Brain Tumour Segmentation. <https://arxiv.org/pdf/1910.00962.pdf>
- ExpertMatcher: Automating ML Model Selection for Users in Resource Constrained Countries <https://www.media.mit.edu/publications/ExpertMatcher/>
- Detailed comparison of communication efficiency of split learning and federated learning <https://www.media.mit.edu/publications/detailed-comparison-of-communication-efficiency-of-split-learning-and-federated-learning-1/>
- Split Learning: Distributed and collaborative learning <https://aiforsocialgood.github.io/iclr2019/accepted/track>
- Asynchronous Federated Optimization <https://arxiv.org/pdf/1903.03934>
- Robust and Communication-Efficient Federated Learning from Non-IID Data <https://arxiv.org/pdf/1903.02891>
- One-Shot Federated Learning <https://arxiv.org/pdf/1902.11175>
- High Dimensional Restrictive Federated Model Selection with multi-objective Bayesian Optimization over shifted distributions <https://arxiv.org/pdf/1902.08999>

-
- Agnostic Federated Learning <https://arxiv.org/pdf/1902.00146v2.pdf>
 - Peer-to-peer Federated Learning on Graphs <https://arxiv.org/pdf/1901.11173>
 - SecureBoost: A Lossless Federated Learning Framework <https://arxiv.org/pdf/1901.08755>
 - Federated Reinforcement Learning <https://arxiv.org/pdf/1901.08277>
 - Lifelong Federated Reinforcement Learning: A Learning Architecture for Navigation in Cloud Robotic Systems <https://arxiv.org/pdf/1901.06455>
 - Federated Learning via Over-the-Air Computation <https://arxiv.org/pdf/1812.11750>
 - Broadband Analog Aggregation for Low-Latency Federated Edge Learning (Extended Version) <https://arxiv.org/pdf/1812.11494>
 - Multi-objective Evolutionary Federated Learning <https://arxiv.org/pdf/1812.07478>
 - Efficient Training Management for Mobile Crowd-Machine Learning: A Deep Reinforcement Learning Approach <https://arxiv.org/pdf/1812.03633>
 - A Hybrid Approach to Privacy-Preserving Federated Learning <https://arxiv.org/pdf/1812.03224>
 - Applied Federated Learning: Improving Google Keyboard Query Suggestions <https://arxiv.org/pdf/1812.02903>
 - Differentially Private Data Generative Models <https://arxiv.org/pdf/1812.02274>
 - Protection Against Reconstruction and Its Applications in Private Federated Learning <https://arxiv.org/pdf/1812.00984>
 - Split learning for health: Distributed deep learning without sharing raw patient data <https://arxiv.org/pdf/1812.00564>
 - Beyond Inferring Class Representatives: User-Level Privacy Leakage From Federated Learning <https://arxiv.org/pdf/1812.00535>
 - LoAdaBoost: Loss-Based AdaBoost Federated Machine Learning on medical Data <https://arxiv.org/pdf/1811.12624>
 - Communication-Efficient On-Device Machine Learning: Federated Distillation and Augmentation under Non-IID Private Data <https://arxiv.org/pdf/1811.11479>
 - Biscotti: A Ledger for Private and Secure Peer-to-Peer Machine Learning <https://arxiv.org/pdf/1811.09904>
 - Dancing in the Dark: Private Multi-Party Machine Learning in an Untrusted Setting <https://arxiv.org/pdf/1811.09712>
 - Federated Learning Approach for Mobile Packet Classification <https://arxiv.org/abs/1907.13113>
 - Collaborative Learning on the Edges: A Case Study on Connected Vehicles <https://www.usenix.org/conference/hotedge19/presentation/chen>
 - Federated Learning for Time Series Forecasting Using Hybrid Model <http://www.diva-portal.se/smash/get/diva2:1334629/FULLTEXT01.pdf>

-
- Federated Learning: Challenges, Methods, and Future Directions <https://arxiv.org/pdf/1908.07873.pdf>
 - Federated Learning with Matched Averaging <https://openreview.net/forum?id=BkluqlSFDS>

Code

- OpenFL: An open-source framework for Federated Learning - <https://github.com/intel/openfl>
- Flower <https://flower.dev/>
- PySyft <https://github.com/OpenMined/PySyft>
- Tensorflow Federated <https://www.tensorflow.org/federated>
- CrypTen <https://github.com/facebookresearch/CrypTen>
- FATE <https://fate.fedai.org/>
- DVC <https://dvc.org/>
- LEAF <https://leaf.cmu.edu/>
- Federated iNaturalist/Landmarkds <https://github.com/google-research/google-research/tree/master/federated>
- FedML: A Research Library and Benchmark for Federated Machine Learning <https://github.com/FedML-AI/FedML>
- XayNet: Open source framework for federated learning in Rust <https://xaynet.webflow.io/>
- EnvisEdge: <https://github.com/NimbleEdge/EnvisEdge>

Use-cases

MIT CSAIL/Harvard Medical/Tsinghua University's Academy of Arts and Design

- <https://arxiv.org/ftp/arxiv/papers/1903/1903.09296.pdf>
- <https://venturebeat.com/2019/03/25/federated-learning-technique-predicts-hospital-stay-and-patient-mortality/>

Microsoft research/University of Chinese Academy of Sciences, Beijing, China

- <https://arxiv.org/pdf/1907.09173.pdf>

Boston University/Massachusetts General Hospital

- <https://www.ncbi.nlm.nih.gov/pubmed/29500022>

Google

-
- <https://ai.googleblog.com/2017/04/federated-learning-collaborative.html>
 - <https://www.statnews.com/2019/09/10/google-mayo-clinic-partnership-patient-data/>

Tencent WeBank

- <https://www.digfingroup.com/webank-clustar/>

Nvidia/King's College London, American College of Radiology, MGH and BWH Center for Clinical Data Science, and UCLA Health... etc

- <https://venturebeat.com/2019/10/13/nvidia-uses-federated-learning-to-create-medical-imaging-ai/>
- <https://blogs.nvidia.com/blog/2019/12/01/clara-federated-learning/>

Company

- integrate.ai <https://integrate.ai>
 - IntegrateFL: A SaaS platform for Federated Learning <https://integrate.ai/integratefl/>
- Adap <https://adap.com/en>
- Snips
 - <https://snips.ai/>
 - <https://www.theverge.com/2019/11/21/20975607/sonos-buys-snips-ai-voice-assistant-privacy>
- Privacy.ai <https://privacy.ai/>
- OpenMined <https://www.openmined.org/>
- Arkhn <https://arkhn.org/en/>
- Scaleout <https://scaleoutsystems.com/>
- MELLODDY <https://www.melloddy.eu/>
- DataFleets <https://www.datafleets.com/>
- Xayn AG <https://www.xayn.com/>
- NimbleEdge <https://www.nimbleedge.ai/>