Federated Learning – Advances and Open Problems

Yang Liu
Principal Researcher
WeBank AI Department
2020/12/17
Federated Learning’s Explosive Growth

Advances and Open Problems in Federated Learning

Peter Kairouz7, H. Brendan McMahan7x, Brendan Avent21, Aurélien Bellet9
Mehdi Bennis19, Arjun Nitin Bhagoji13, Keith Bonawitz7, Zachary Charles7
Graham Cormode23, Rachel Cummings6, Rafael G.L. D’Oliveira14
Salim El Rouayheb14, David Evans22, Josh Gardner24, Zachary Garrett7
Adrià Gascón7, Badih Ghazi7, Phillip B. Gibbons2, Marco Gruteser7,14
Zaid Harchaoui24, Chaoyang He21, Lie He4, Zhiyuan Liu20
Ben Hutchinson7, Justin Hsu19, Martin Jaggi1, Tara Javidi17, Gauri Joshi12
Mikhail Khodak7, Jakub Konečný7, Aleksandra Korolova21, Farinaz Koushanfar17
Sannies Koyejo7,18, Tancrède Lepoint7, Yang Liu12, Prateek Mittal13
Mehryar Mohri7, Richard Nock2, Ayfer Özgür45, Rasmus Pagh7,10
Marina Radvorova7, Hang Qi7, Daniel Ramage7, Ramesh Raskar11
Dawn Song10, Weikang Song7, Sebastian U. Stich1, Ziteng Sun3
Ananda Theertha Suresh7, Florian Tramèr15, Praneeth Vepakomma11, Jiayu Wang2
Li Xiong5, Zheng Xu7, Qiang Yang8, Felix X. Yu7, Han Yu12, Sen Zhao7

1Australian National University, 2Carnegie Mellon University, 3Cornell University,
4École Polytechnique Fédérale de Lausanne, 5Emory University, 6Georgia Institute of Technology,
7Google Research, 8Hong Kong University of Science and Technology, 9INRIA, 10IT University of Copenhagen,
11Massachusetts Institute of Technology, 12Nanyang Technological University, 13Princeton University,
14Rutgers University, 15Stanford University, 16University of California Berkeley,
17University of California San Diego, 18University of Illinois Urbana-Champaign, 19University of Oulu,
20University of Pittsburgh, 21University of Southern California, 22University of Virginia,
23University of Warwick, 24University of Washington, 25University of Wisconsin–Madison

To appear in foundations and trends in machine learning,
Edited by Michael Jordan
Federated Learning Industrial Landscape
FL Datasets

- WeBank FedVision - Street Dataset, Available: [https://dataset.fedai.org/#/](https://dataset.fedai.org/#/)
  
  A real-world **object detection** dataset that annotates images captured by a set of street cameras based on object present in them, including 7 classes. In this dataset, each or every few cameras serve as a device.

  
  - Federated Extended MNIST (FEMNIST), 62 classes, Image Classification
  - Twitter, Sentiment140, Sentiment Analysis, federated
  - Shakespeare, Next-Character Prediction, federated
  - Celeba, Image Classification (Smiling vs. Not smiling), federated
  - Synthetic Dataset, Classification, federated
FL open-sourced Project

- **WeBank FATE**, supports TensorFlow and PyTorch, [https://github.com/FederatedAI/FATE](https://github.com/FederatedAI/FATE)
- Google TensorFlow Federated (TFF), [https://github.com/tensorflow/federated](https://github.com/tensorflow/federated)
- Google Tensorflow-Encrypted, [https://github.com/tf-encrypted/tf-encrypted](https://github.com/tf-encrypted/tf-encrypted)
- OpenMined PySyft, supports PyTorch, [https://github.com/OpenMined/PySyft](https://github.com/OpenMined/PySyft)
- 平安科技蜂巢平台,是由平安科技开发的一个联邦学习平台, supports TensorFlow, Keras, Pytorch, and MXNet, [https://mp.weixin.qq.com/s/1SXW1N7BaVnyFXFZ-f24TA](https://mp.weixin.qq.com/s/1SXW1N7BaVnyFXFZ-f24TA)
- 百度 MesaTEE, MesaTEE是由百度公司开发的可信安全计算服务框架, [https://mesatee.org/](https://mesatee.org/)
- 百度PaddlePaddle/PaddleFL, [https://github.com/PaddlePaddle/PaddleFL](https://github.com/PaddlePaddle/PaddleFL)
FedML:
A Research Library and Benchmark for Federated Machine Learning

- web: https://fedml.ai/
- github: https://github.com/FedML-AI
2019.2 WeBank initiated the IEEE FL Standard

IEEE Standard P3652.1 – Federated Machine Learning
Federated Learning’s unique challenges

**Heterogeneity and Locality**

![Graph showing IID and non-IID settings for federated learning](image)

Figure 3: Illustration of the weight divergence for federated learning with IID and non-IID data.


**Privacy-Accuracy-Efficiency Triage**

![Graph showing accuracy over communication rounds](image)

Figure 1: Accuracy of digit classification from non-IID MNIST-data held by clients over the course of decentralized training. For differentially private federated optimization, dots at the end of accuracy curves indicate that the $\delta$-threshold was reached and training therefore stopped.

- From 100 to 1,000 clients, model accuracy does not converge and stays significantly below the non-differentially private approach

Other Emerging Scenarios

Decentralized Peer-to-Peer Learning

(a) Centralized Topology

(b) Decentralized Topology


Split learning

(a) Vanilla split learning

(b) U-shaped split learning


WeBank
Addressing Privacy-Accuracy-Efficiency Trilemma over Various heterogeneity
Uninspectable, heterogeneous data and devices

Ligeng Zhu, Zhijian Liu, Song Han, Deep Leakage from Gradients, Neurips 2019
Privacy-Preserving Machine Learning

Security Definition

Honest-but-curious vs Malicious

Zero knowledge vs Some knowledge

Adversarial Server vs Adversarial Client
Privacy-Preserving Technologies

- 多方安全计算 Secure Multi-party Computation (MPC)
- 同态加密 Homomorphic Encryption (HE)
- 姚式混淆电路 Yao’s Garbled Circuit
- 秘密共享 Secret Sharing
- 差分隐私 Differential Privacy (DP)
- TEE (Trusted Execution Environment)

Mix and layering
Privacy in Depth
BatchCrypt: Efficient Homomorphic Encryption for Cross-Silo Federated Learning

- Reducing the encryption overhead and data transfer
  - Quantizing a gradient value into low-bit integer representations
  - Batch encryption: encoding a batch of quantized values to a long integer and encrypting it in one go

- BatchCrypt is implemented in FATE and is evaluated using popular deep learning models
  - Accelerating the training by \(23x-93x\)
  - Reducing the netw. footprint by \(66x-101x\)
  - Almost no accuracy loss (\(<1%\))


C. Zhang, S. Li, J. Xia, W Wang, F Yan, Y. Liu, BatchCrypt: Efficient Homomorphic Encryption for Cross-Silo Federated Learning, USENIX ATC’20
Each Site Hold Own Data

Performance is LOSSLESS

Solution for Common Users

Architecture of Vertical Federated Learning
From FedSGD to FedBCD (Federated Block Coordinate Gradient Descent)

- Communication at every round
- expensive especially when privacy-preserving protocol is applied.

FedSGD

- Party B
- Select mini-batch samples
- local iteration
- Select mini-batch samples
- local iteration
- Select mini-batch samples
- local iteration
- ......

FedBCD

- Party B
- Select mini-batch samples
- local iteration
- Select mini-batch samples
- local iteration
- Select mini-batch samples
- local iteration
- ......

- Each communication round, each party performs multiple local iterations,
- Each local iteration, each party locally computes gradient based on its own data and (staled) intermediate components from other parties in the most recent synchronization.

From FedSGD to FedBCD (Federated Block Coordinate Gradient Descent)

- Reasonably increasing $Q$ leads to 70% reduction in communication rounds

<table>
<thead>
<tr>
<th>Algo.</th>
<th>MIMIC-LR</th>
<th>MNIST-CNN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AUC 84%</td>
<td>AUC 99.7%</td>
</tr>
<tr>
<td>FedSGD</td>
<td>1 334</td>
<td>1 46</td>
</tr>
<tr>
<td>FedBCD-p</td>
<td>5 71</td>
<td>5 16</td>
</tr>
<tr>
<td>FedBCD-s</td>
<td>50 52</td>
<td>5 8</td>
</tr>
<tr>
<td></td>
<td>407 48</td>
<td>4 15</td>
</tr>
<tr>
<td></td>
<td>5 74</td>
<td>5 9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AUC</th>
<th>Algo.</th>
<th>$Q$</th>
<th>Round</th>
<th>Computation (mins)</th>
<th>Communication (mins)</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>80%</td>
<td>FedSGD</td>
<td>1</td>
<td>46</td>
<td>32.20</td>
<td>30.69</td>
<td>62.89</td>
</tr>
<tr>
<td></td>
<td>FedBCD-p</td>
<td>5</td>
<td>13</td>
<td>43.52</td>
<td>9.05</td>
<td>52.57</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>7</td>
<td>41.53</td>
<td>5.12</td>
<td>46.65</td>
</tr>
</tbody>
</table>

Table 1: Number of communication rounds and training time to reach target AUC

- Implemented on FATE with homomorphic encryption

Mixed-protocols

• **ABY**
  
  - It is a mixed-protocol framework that combines various secret sharing schemes in a two-party setting, namely Arithmetic, Boolean and Yao sharing.

• **SPDZ (Smart, Pastro, Damgard, Zakarias 11)**
  
  - It is a family of multi-party computation protocols for arbitrary number of parties
  
  • **Malicious** Setting

---

Differentially Private Federated Learning

For any two datasets $D$ and $D'$ differing in a single item and any output $O$ of function $f$,

$$\Pr\{f(D) \in O\} \leq \exp(\epsilon) \cdot \Pr\{f(D') \in O\}$$


- **Local Differential Privacy**
  - Deployed by Google, Apple, Microsoft, Snap
  - Require large numbers of clients to provide utility

- **Central Differential Privacy**
  - Require a trustworthy central server

- **Distributed DP**
  - Involves an MPC protocol or TEE

- **Hybrid DP**
  - Personalized trust preference
Towards Efficient and Secure FL

- Faster Algorithms to reduce communication overhead
- More efficient HE encryption strategy
- Hybrid Privacy-Preserving Protocols
- Compression and Sparsification
New Trends in Federated Learning
New Research Trends

➢ Robustness to Attacks

➢ Personalized Federated Learning

➢ AutoFL

➢ Incentives, fairness and data valuation

---

Can Federated Learning Save The Planet?

Xinhe Qiu¹, Titouan Parcollet², Daniel J. Beutel¹,³, Taner Topal¹,², Akhil Mathur³, Nicholas D. Lane¹

¹ University of Cambridge, UK ² Avignon Université, France ³University College London, UK ⁴Adap, Germany 
xq227@cam.ac.uk

Abstract

Despite impressive results, deep learning-based technologies also raise severe privacy and environmental concerns induced by the training procedure often conducted in data centers. In response, alternatives to centralized training such as Federated Learning (FL) have emerged. Perhaps unexpectedly, FL in particular is starting to be deployed at a global scale by companies that must adhere to new legal demands and policies originating from governments and the civil society for privacy protection. However, the potential environmental impact related to FL remains unclear and unexplored. This paper offers the first ever systematic study of the carbon footprint of FL. First, we propose a rigorous model to quantify the carbon footprint, hence facilitating the investigation of the relationship between FL design and carbon emissions. Then, we compare the carbon footprint of FL to traditional centralized learning. Our findings show FL, despite being slower to converge, can be a greener technology than data center GPUs. Finally, we highlight and connect the reported results to the future challenges and trends in FL to reduce its environmental impact, including algorithms efficiency, hardware capabilities, and stronger industry transparency.
FL introduces New Backdoor Attacks

Targeted Attacks: The attacker aims to train a model which achieves high performance on both the original task and the targeted back-door task.

Backdoor Attacks in Vertical FL

- **Difficulty**: It has no access to either labels or other passive parties' contributions at every iteration.

- **Infer labels from the intermediate gradients**.

  $$g_{i,j} = \begin{cases} 
  S_j, & j \neq y \\
  S_j - 1, & j = y 
  \end{cases}$$

  where $S_j$ is the softmax function $S_j = \frac{e^{h_j}}{\sum_i e^{h_i}}$ over $H_i$.

- **Gradient-replacement backdoor**
  - Assume that the passive attacker knows at least one clean sample
  - the attacker records the received intermediate gradient of $D_{\text{target}}$ as $g_{\text{rec}}$
  - set the intermediate gradients of the poisoned samples to be $g_{\text{rec}}$
  - update the model parameters using $\gamma g_{\text{rec}} \frac{\partial H_k}{\partial y_k}$, where $\gamma$ is an adjustable amplify ratio.
Backdoor Attacks--Gradient-replacement backdoor

(a) normal(NUS-WIDE)  (b) poisoned(NUS-WIDE)

(c) normal(MNIST)  (d) poisoned(MNIST)
Defense Strategies

- Differential Privacy (DP)
- Gradient Sparsification (GS)
- Fully Connected (FC) Layer for shuffling
- Verification, Consensus and hardware
Defenses

**FC Defense**

- Backdoor task accuracy vs. Number of epochs for backdoor training and normal training.

**DP Defense**

- Gaussian noise defense with varying noise levels (0.1, 0.05, 0.025).

**GS Defense**

- Gradient sparsification with varying sparsity levels (95, 99, 99.9).

**Experimental Sets**

- MNIST
- NUS-WIDE
New Research Trends

➢ Robustness to Attacks

➢ Personalized Federated Learning

➢ AutoFL

➢ Incentives, fairness and data valuation
Personalized Federated Learning

Challenges:
- Heterogenous devices and computing power
- Distributed, non-iid, uninspectable data
- Heterogenous model objectives

Approaches:
- Multi-task learning
- Meta learning
- Clustered federated learning
- Federated transfer learning
Step 1
Party A and B send public keys to each other

Step 2
Parties compute, encrypt and exchange intermediate results

Step 3
Parties compute encrypted gradients, add masks and send to each other

Step 4
Parties decrypt gradients and exchange, unmask and update model locally

Federated Domain Adversarial Training

Sample Space

Features

Label

Party C

$X^{s,c}$

$X^{t,c}$

Domain Shift

align

Party A

$X^{s,a}$

$Y^{s,a}$

$D^{s}$

align

Party B

$X^{t,b}$

$Y^{t,b}$

$D^{t}$
New Research Trends

➢ Robustness to Attacks

➢ Personalized Federated Learning

➢ AutoFL

➢ Incentives, fairness and data valuation
How to choose model, data and hyperparameters when data are uninspectable and private?

Privacy-preserving feature engineering and architecture search.
AutoML + FL = AutoFL

Han Cai et al, Once for All: Train One Network and Specialize it for Efficient Deployment, CVPR 2019

Mengwei Xu et al, Neural Architecture Search over Decentralized Data, 2020

Chaoyang He et al, FedNAS: Federated Deep Learning via Neural Architecture Search, 2020

Federated NAS

Vertical Federated Neural Architecture Search

Xinle Liang, Yang Liu et al, Vertical Federated Neural Architecture Search, in preparation 2020
AutoFL can find optimal model architecture for each party without accessing local data.

AutoFL requires much smaller model size with superior accuracy.

Xinle Liang, Yang Liu et al, Self-supervised Cross-silo Federated Neural Architecture Search, arxiv, 2020
03
Incentive Design for Federated Learning
Federated Learning incentive Definition

Agent/Data Owner
• Individuals or Organizations in Federated Learning

Federation
• Founded by N (N > 1) participants in Federated learning

Federated Model
• The model built by participants in Federation

Utility
• The contribution of one party to the Federation

Payment
• Money paid by parties to the Federation.
Incentives, Fairness and data valuation

- The success of a federation depends on data owner to continue sharing data with the federation
- **Challenge:**
  - How to motivate continued participation by data owners in a federation?

**Research Question:** How to determine $u_i(t)$?

---

Objectives of Incentive mechanism in FL

- Motivate data owners to continue participating in the data federation.
- Distribute profits generated by the data federation to participants in a fair and just manner.
- Dynamically allocate a given budget to each participant in the data federation.
- Serve as an adjustment mechanism that help the data federation resist malicious participants.
Contribution and Revenue

• Three natural and widely used profit sharing rules:
  • **Egalitarian**: any unit of utility produced by a data federation is divided equally among the data owners who helped produce it
  • **Marginal gain**: the payoff a data owner in a data federation is the utility that the team gained when she joined
  • **Marginal loss**: the payoff a data owner in a data federation is the utility that the team would lose if it were to leave

• From a systematic perspective, the **goal** is to maximize the total utility produced:

\[ U = \sum_{t} \sum_{i} u_i(t) \]
Contribution and Revenue

- Profit-Sharing Policy – Equal

\( B(t) \) is equally divided among data owners in this federation (Egalitarian).

Payoff instalment: \( \hat{u}_i(t) = \frac{B(t)}{N} \)
Contribution and Revenue

- Profit-Sharing Policy - Individual

A data owner $i$’s share of $B(t)$ is proportional to his marginal contribution to the revenue of the federation (Marginal gain).

$$u_i(t) = v(\{i\})$$

Payoff instalment: $$\hat{u}_i(t) = \frac{u_i(t)}{\sum_i u_i(t)} B(t)$$
Contribution and Revenue

• Profit-Sharing Policy – Labour Union

A data owner $i$’s share of $B(t)$ follows the Labor Union game scheme and is proportional to his marginal contribution to the revenue of the federation formed by his predecessors (Marginal gain).

\[ u_i(t) = v(F \cup \{i\}) - v(F) \]

- Revenue of a data federation if $i$ joins it
- Revenue of a data federation without $i$

Payoff instalment: \[ \hat{u}_i(t) = \frac{u_i(t)}{\sum_i u_i(t)} B(t) \]
Contribution and Revenue

• Profit-Sharing Policy – Fair-value

A data owner $i$’s share of $B(t)$ is proportional to his marginal loss to the revenue of the federation after his leaving (Marginal loss).

$$u_i(t) = v(F) - v(F \setminus \{i\})$$

Payoff instalment: $\hat{u}_i(t) = \frac{u_i(t)}{\sum_i u_i(t)} B(t)$
Contribution and Revenue

• Profit-Sharing Policy - Shapley

The payment to each data owner $i$ can be viewed as his average payment in the Labor Union payoff scheme, where the average is taken over all possible orderings of the players in the party (Marginal gain).

$$u_i(t) = \sum_{P \subseteq P_j \setminus \{i\}} |P|! \left( \frac{|P_j| - |P| - 1)!}{|P_j|} \right) \left[ v(P \cup \{i\}) - v(P) \right]$$

Payoff instalment: $\hat{u}_i(t) = \frac{u_i(t)}{\sum_i u_i(t)} B(t)$
Shapley

• proposed by Lloyd Shapley in 1953

• Pros:
  • Satisfies a collection of desirable properties
    • Cumulative
    • Equitable
  • Defines a way of distributing the profit generated by the coalition of all players

• Cons:
  • Expensive computation
  • Monte Carlo approximation, Gradient Shapley (Amirata Ghorbani, James Zou., Data Shapley: Equitable Valuation of Data for Machine Learning, ICML, 2019)
Trustworthy Federated Learning

Ecosystem Management Tools
- Robust FL Training for Large AI Models
- Misbehaviour Deterrence Optimization
- Accountable Contribution Assessment
- Fair Monetary FL Incentive
- Fair Non-Monetary FL Incentive
- Interpretable VFL
- Interpretable HFL

Research Platforms
- Testbed for Attacks on FL
- Gamified FL Incentive Testbed
03

Open Problems and Application Outlook
Towards building a data economy via FL

• Data encryption only protects data at rest or in transit, but not data in use
  • MPC, FHE technologies, Secure hardware (e.g. TEE) combined with DP

• How much information does exchanged outputs from FL leak?
  • Security Analysis

• Data can be copied and data usage is difficult to control
  • Distributed Ledger and Blockchain
Blockchain and distributed commerce

- Federated learning provides participants with the capability of collaboratively building powerful machine learning models and employs privacy-preserving mechanisms to protect the privacy of their data.

- Federated learning has been questioned for its vulnerability to backdoor attacks.
  - In order to actively prevent federated learning from malicious attacks instead of just passive defense, a mechanism that can effectively detect malicious attacks and pinpoint malicious participants is needed.

- Blockchain, with its immutability and traceability, can be an effective tool to prevent malicious attacks in federated learning.

- The immediate updates made by each participant to its local model can be chained together on the distributed ledger offered by a blockchain such that those model updates are audited.
  - Every model update, be it either local weights or gradients, can be traced to and associated with an individual participant, which helps the detection of tamper attempts and malicious model substitutes.
  - Model updates can be chained in a cryptographical way such that their integrity and confidentiality can be guaranteed.
Federated learning has also become an active research topic at the intersection of machine learning and wireless networks, and particularly for the fifth generation (5G) mobile network and even beyond.

Federated learning comes as a solution, for addressing not only the data privacy concerns, but also the communication bandwidth, reliability and latency challenges.

Federated learning can also help with building a better wireless network.
Distributed AI + Edge Computing (边缘计算)
Federated Learning is interdisciplinary

Where
- edge computing (边缘计算)
- cloud computing (云平台)

Who
- Value 价值
- Fairness 公平
- (incentive mechanism, game theory)
- Data valuation, AI fairness

Do What
- machine learning
- transfer learning
- multi-task learning
- federated computation

How
- Distributed learning (分布式计算)
- Collaboration and coordination
- (system design and optimization)

preserving user privacy and data confidentiality

数据处理
- Differential Privacy
- Data perturbation/randomization
- Dimension reduction
- Feature Engineering
- DNN encryption (神经网络加密)

模型处理
- Model compression (模型压缩)
- 传递中间计算结果
- 传递模型参数
- 防御攻击(inference attack, GAN, re-identification attack..)

数据加密或隔离
- Homomorphic Encryption (同态加密)
- MPC (多方安全计算)
- Secret Sharing, Yao’s Garbled Circuit
- TEE (可信执行环境)
Thank You

Questions
yangliu@webank.com