Applications of Federated Learning

Qiang Yang
HKUST/WeBank
Feb 2021
1. Federated Recommendation

Qiang Yang, http://ai.webank.com
Webank and HKUST
Recommender Systems Have Been Widely Used

<table>
<thead>
<tr>
<th>E-commerce</th>
<th>Online Video</th>
<th>Social Network</th>
<th>News Feeds</th>
<th>Online Advertising</th>
</tr>
</thead>
<tbody>
<tr>
<td>amazon</td>
<td>YouTube</td>
<td>facebook</td>
<td></td>
<td>Google</td>
</tr>
<tr>
<td>Taobao.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JD.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

![Diagram of various online platforms and services using recommender systems](image)
Recommender Systems Improve User Engagement

personized services

precision marketing

YouTube Homepage: 60%+ more clicks [Davidson et al. 2010]

Netflix: 80%+ more movie watches [Gomze-Uribe et al. 2016]

Amazon: 30%+ more page views [Smith and Linden, 2017]
Overview of Recommender Systems

**Input:** historical user-item interactions, and optionally additional side information (e.g., user demographic, item attributes)

**Output:** how likely a user would interact with an item (e.g., a movie, a song, a product)
More Data Used in Recommender Systems, Better Performance

Reality in Recommender Systems: Data Silos
Facebook finally rolls out privacy tool for your browsing history

Google strengthens Chrome’s privacy controls

Top Microsoft exec says online privacy has reached ‘a crisis point’
Federated Learning to Bridge Decentralized Data

Lossless performance

- Performance of ‘A fed B’ is close to ‘A+B’

Data protected

- Raw data stays locally
- Only parameters and gradients are securely transmitted
**Assumption:** for easier understanding and system efficiency, we assume the existence of a trustworthy 3rd-party server in the following federated recommendation solution discussion.

In general, such 3rd-party servers can be removed to strengthen the data security.
Key Security Technology in Federated Recommendation

- Secure Multi-party Computation (MPC)
  - Homomorphic Encryption (HE)
  - Yao’s Garbled Circuit
- Secret sharing
  - ...
Secure Multi-Party Computation (MPC)

Overview of MPC:
- Provides security proof in a well-defined simulation framework
- Guarantees complete zero knowledge
- Requires participants’ data to be secretly-shared among non-colluding servers
Homomorphic Encryption

- Full Homomorphic Encryption and Partial Homomorphic Encryption.
- **Paillier** partially homomorphic encryption

**Addition:** $[[u]] + [[v]] = [[u+v]]$

**Scalar multiplication:** $n[[u]] = [[nu]]$

- For public key $pk = n$, the encoded form of $m \in \{0, \ldots, n - 1\}$ is

  $$
  \text{Encode}(m) = r^n (1 + n)^m \mod n^2
  $$

  $r$ is randomly selected from $\{0, \ldots, n - 1\}$.

- For float $q = (s, e)$, encrypt $[[q]] = ([[s]], e)$, here $q = s\beta^e$ is base-$\beta$ exponential representation.

Applying Homomorphic Encryption to Machine Learning

① Polynomial approximation for logarithm function

\[
\log \left( \frac{1}{1 + \exp(u)} \right) \approx \sum_{j=0}^{k} a_j u^j
\]

② Encrypted computation for each term in the polynomial function

\[
\text{loss} = \log 2 - \frac{1}{2} y w^T x + \frac{1}{8} (w^T x)^2
\]

\[
[[\text{loss}]] = [[\log 2]] + \left(-\frac{1}{2}\right) [[y w^T x]] + \frac{1}{8} [[(w^T x)^2]]
\]

- Aono et al. 2016. Scalable and secure logistic regression via homomorphic encryption. CODASPY, Pages 142-144.
Is the Gradient Info Safe to Share?


Algorithm ensures that no information is leaked to the semi-honest server, provided that the underlying additively homomorphic encryption scheme is secure*.

Yang et al. 2018. Federated machine learning: concepts and applications. ACM TIST.
## Federated Learning vs Federated Database vs Blockchain

<table>
<thead>
<tr>
<th></th>
<th>Federated Learning</th>
<th>Federated Database</th>
<th>Blockchain</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consistency (Unique Results)</strong></td>
<td>Training and Inference Results</td>
<td>Query Results</td>
<td>Transaction Information</td>
</tr>
<tr>
<td><strong>Atomicity (Same Status)</strong></td>
<td>True for Models</td>
<td>Partially True</td>
<td>True</td>
</tr>
<tr>
<td><strong>Collective Security (Multi-party Participation, Secure Computation)</strong></td>
<td>True</td>
<td>False</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Summary
- **Federated Learning**: No data transfer, Secure model parameter transfer, Data and model security guarantee.
- **Federated Database**: Interoperability of multiple databases, No security requirement, Possible security leak in the central management system
- **Blockchain**: Distributed ledger, All nodes keeping the same copy of data
Categorization of Federated Recommendation

**Horizontal Federated Recommendation** (a.k.a. Item-based FedRec)

- Large overlap of *items* of the two rating matrices

**Vertical Federated Recommendation** (a.k.a. User-based FedRec)

- Large overlap of *users* of the two rating matrices
Category 1: Horizontal Federated Recommendation

Large overlap of items of the two rating matrices
Horizontal Federated Recommendation: Case 1

Example: movie recommendation with data from individual users
Federated Collaborative Filtering [Ammad et al. 2019]

Intuition: decentralized matrix factorization, each user profile is updated locally, item profiles are aggregated and updated by server.
Server initializes item profiles, parties initializes user profiles;

Sever distributes item profiles to parties;

Parties locally update user profiles with item profiles;

Parties send item profile gradient updates to server;

Server updates item profile.
Horizontal Federated Matrix Factorization [Chai et al. 2019]

Intuition: Item profile gradients are encrypted by HE. Semi-honest server securely aggregates encrypted item profiles gradients, and knows nothing about the profile content.

Training Process:

1. Server initializes and encrypts item profiles;
2. Server distributes encrypted item profiles to parties;
3. Parties locally update user profiles with encrypted item profiles;
4. Parties send encrypted item profile gradient updates to server;
   Server securely aggregates item profile gradients and updates item profiles.

Security of secure aggregation protocol is guaranteed [Bonawitz et al. 2017].

Horizontal Federated Recommendation: Case 2

Example: movie recommendation with data from two different groups of users

Solution to Case 2:
Item profiles are securely aggregated by server, group of user profiles are locally updated by parties.
Category 2: Vertical Federated Recommendation

Large overlap of users of the two rating matrices
Vertical Federated Recommendation: Case 1

Example:
Shared users, different items

Party A

Party B
**Intuition:** User profile gradients are encrypted and securely aggregated by semi-honest server, item profiles are updated locally.

$$\min_{p,q} \sum_{(i,j) \in K_A} (r_{i,j} - \langle p_i, q_j^A \rangle)^2 + \sum_{(i,j) \in K_B} (r_{i,j} - \langle p_i, q_j^B \rangle)^2 + \lambda \|p\|^2_2 + \mu (\|q^A\|^2_2 + \|q^B\|^2_2)$$
Vertical Federated Matrix Factorization [Chai et al. 2019]

Training Process:

1. Server initializes and encrypts user profiles; parties initialize item profiles.
2. Server distributes encrypted user profiles to parties;
3. Parties locally update item profiles with decrypted user profiles; Parties send encrypted user profile gradient to server;
4. Server securely aggregates user profile gradients and update user profiles.

Security of secure aggregation protocol is guaranteed [Bonawitz et al. 2017].

Vertical Federated Recommendation: Case 2

Example:
Shared users
different features

book recommendation  auxiliary data from third-parties

<table>
<thead>
<tr>
<th>Location</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Georgia</td>
<td>2018.5</td>
</tr>
<tr>
<td>Florida</td>
<td>2019.1</td>
</tr>
<tr>
<td>Hawaii</td>
<td>2017.3</td>
</tr>
<tr>
<td>Kansas</td>
<td>2018.5</td>
</tr>
<tr>
<td>Georgia</td>
<td>2018.10</td>
</tr>
<tr>
<td>Florida</td>
<td>2019.9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Party A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sports</td>
</tr>
<tr>
<td>Y</td>
</tr>
<tr>
<td>N</td>
</tr>
<tr>
<td>Y</td>
</tr>
<tr>
<td>Y</td>
</tr>
<tr>
<td>N</td>
</tr>
<tr>
<td>N</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Party B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sports</td>
</tr>
<tr>
<td>Y</td>
</tr>
<tr>
<td>N</td>
</tr>
<tr>
<td>Y</td>
</tr>
<tr>
<td>Y</td>
</tr>
<tr>
<td>N</td>
</tr>
<tr>
<td>N</td>
</tr>
</tbody>
</table>
Federated Factorization Machine [Zheng et al. 2019]

Intuition: cross-features between A and B are useful, but features are sensitive. Federated factorization machine computes these cross-party cross-features and their gradients under encryption.

Cross features between A and B are useful; e.g., “location x sports” can be a strong indicator for predicting Georgia user’s preference to sports movies.

\[
f([x_p^{(A)}; x_q^{(B)}]) = f(x_p^{(A)}) + f(x_q^{(B)}) + \sum \langle v_i^{(A)}, v_j^{(B)} \rangle x_p^{(A)} x_{q,j}^{(B)}
\]

Training Process:

1. Server initializes and encrypts user profiles; parties initialize item profiles.
2. Server distributes encrypted user profiles to parties;
3. Parties locally update item profiles with decrypted user profiles;
4. Parties send encrypted user profile gradient to server;
   Server securely aggregates user profile gradients and update user profiles.

Security of secure aggregation protocol is guaranteed [Bonawitz et al. 2017].

Federated Factorization Machine [Zheng et al. 2019]

Inference Process: encrypted prediction on party A’s features + encrypted prediction on A&B features + encrypted prediction on party B’s features.

1. Party A and B compute encrypted intermediate results
2. Server aggregates the encrypted intermediate results and decrypts
3. Sever sends plain-text prediction to party A
What If Different Users and Items at the Same Time?

Transfer Federated Recommendation
Category 3: Transfer Federated Recommendation

Example: movie and book recommenders with different groups of users
Matrix Tri-factorization [Li et al. 2009]

**Intuition:** similar users/items can be clustered into groups, and there exist group correspondences across parties.

![Diagram showing user and item clusters for Party A and Party B, with dense and sparse matrices, and a codebook mapping.](image)

Li et al. Transfer Learning for Collaborative Filtering via a Rating-Matrix Generative Model, ICML, pp.617-624.
Federated Matrix Tri-factorization [Tan et al. 2019]

Intuition: codebooks as group correspondences are used for transfer, they are encrypted and securely aggregated by semi-honest server, and user/item profiles are updated by parties.

Training Process

1. Server initializes and encrypts codebook; Parties initializes user and item profiles;
2. Server distributes encrypted codebook to parties;
3. Parties update user and item factors by decrypted codebook;
4. Parties compute codebook gradients and send encrypted gradients to server;
   Server securely aggregates encrypted codebook gradients and updates codebook.

Security of secure aggregation protocol is guaranteed [Bonawitz et al. 2017].

Application 1: Horizontal Federated Movie Recommendation

Recommender keeps user data on local devices, protects privacy while achieving lossless performance.

MovieLens

Application 2: Vertical Federated News Feeds Recommendation

Recommender leverages auxiliary user data to address cold start and improve performance.
AutoML with Transfer Learning and Federated Learning

Qiang Yang
WeBank and Hong Kong University of Science and Technology
2020.08
Machine Learning

• [Mitchell, 1997]. A computer program is said to learn from experience $E$ with respect to some classes of task $T$ and performance measure $P$ if its performance can improve with $E$ on $T$ measured by $P$. 

[Mitchell, 1997]
Machine Learning Stages
AutoML – Automated Machine Learning

Problem Definition → Data Collection → Feature Engineering → Model Training → Model Evaluation → Model Application → Real Deployment
AutoML

- A computer program is said to learn from experience $E$ with respect to some classes of task $T$ and performance measure $P$ if its performance can improve with $E$ on $T$ measured by $P$. AutoML tries to construct this computer program without human assistance and within limited computational budgets.
AutoML for Problem Solving

- Parameter Optimization
  - Efficiency?

\[
\max_{c} P(ML(c, E), T)
\]

- Parameter setting
  - How to set?

- Evaluation
  - How to evaluate results?

AutoML: network parameter spaces, evaluation, Optimization strategy?
AutoFL: Automating Federated Learning
Data Partition on Features (Vertical)
Federated Learning

- Feature overlap
- Samples overlap

What can AutoFL (Vertical) do:

1. To determine the learning architecture automatically and locally in a communication-efficient manner with data protection;

Banking Authentication:
1. Upload front camera photo: to judge whether an image is taken from a real person or his photo.
2. Bank A can cooperate with a Secure Face Database with VFL;

A Secure Face Database

Vertically Federated Learning

Bank APP

Image From a real person or his photo?

Bank APP

Net A

Net B

Query(userID)

VFL Framework

①

②

③

④
AutoFL with DARTS

Agent A

1. Agent A update architecture and weights based on $U_B$.

Agent B

2. Agent B update architecture and weights based on gradients of $U_B$.

Protected by Differential Privacy -- adding Gaussian Noise
Communication-efficient AutoFL Framework

For $t$ in 1, 2, ..., n:

$$\partial L(\hat{v}_A^{\text{out}}, \hat{v}_A^{\text{val}})$$

$$\partial L(\hat{v}_B^{\text{out}}, \hat{v}_B^{\text{val}})$$

For $t$ in 1, 2, ..., n:

$$[\hat{v}_A]_t \leftarrow [\hat{v}_A]_{t-1} - \theta \frac{\partial L(\hat{v}_A^{\text{out}}, \hat{v}_A^{\text{val}})}{\partial [\hat{v}_A]_{t-1}}$$

$$[\hat{v}_B]_t \leftarrow [\hat{v}_B]_{t-1} - \theta \frac{\partial L(\hat{v}_B^{\text{out}}, \hat{v}_B^{\text{val}})}{\partial [\hat{v}_B]_{t-1}}$$

For $t$ in 1, 2, ..., n:

$$[\hat{v}_A]_t \leftarrow f_{\hat{w}_A|\hat{v}_A^{\text{out}}}[X_A^{\text{trn}}][U_A^{\text{trn}}]_t$$

$$[\hat{v}_B]_t \leftarrow f_{\hat{w}_B|\hat{v}_B^{\text{out}}}[X_B^{\text{trn}}][U_B^{\text{trn}}]_t$$

For $t$ in 1, 2, ..., n:

$$[\hat{v}_B]_t \leftarrow f_{\hat{w}_B|\hat{v}_B^{\text{out}}}[X_B^{\text{trn}}][U_B^{\text{trn}}]_t$$

$$[\hat{v}_A]_t \leftarrow f_{\hat{w}_A|\hat{v}_A^{\text{out}}}[X_A^{\text{trn}}][U_A^{\text{trn}}]_t$$

For $t$ in 1, 2, ..., n:

$$\partial L(\hat{v}_A^{\text{val}}, \hat{v}_A^{\text{val}})/\partial [U_A^{\text{val}}]_0$$

$$\partial L(\hat{v}_B^{\text{val}}, \hat{v}_B^{\text{val}})/\partial [U_B^{\text{val}}]_0$$

$$\partial L(\hat{v}_A^{\text{out}}, \hat{v}_A^{\text{val}})/\partial [U_A^{\text{out}}]_0$$

$$\partial L(\hat{v}_B^{\text{out}}, \hat{v}_B^{\text{val}})/\partial [U_B^{\text{out}}]_0$$

48
Experimental Results: Accuracy vs DP Noise

**Dataset:** ModelNet40

**VFL settings:**
- two VFL participants
- each holding a single view of one 3D object

---

**Conclusions:**
1. AutoFL can achieve reasonable performance within acceptable time;
2. Trade-off exists between AutoFL performance and privacy;
Summary of AutoFL

• AutoVL enables parties in vertical federated learning to automatically determine their local optimal learning architecture at different privacy level;

• DARTS-based algorithms are computational expensive.

• Future work
  • To further reduce the communication and computation costs with multiple local updates and asynchronization.
  • To explore computational-efficient AutoML algorithms.


Traditional Big Data: Bring Data to Center

Federated Learning: Model parameters encrypted and trained
FATE Case 1: WeBank Serves More SMEs via FATE

**Data Demander (WeBank)**
- ✓ Sample ID, Y (loan performance)
- ✓ Scale of loans: 20 billion
- ✓ Scale of customers: 0.3 million

**Data Provider**
- (a large invoice data company in China)
  - ✓ Sample ID, X (Features)

---

**Challenge**
- Credit Data Shortage
  - SME loans are hampered by a lack of credit data

**Expectation**
- Inclusive Finance
  - Serve more SMEs, especially those usually locked out of the conventional banking system due to their low incomes

**Results**
- Improved Performance
  - Loan Balance: 1 billion ↑, Borrowers: 3K ↑

---

SME: Small and Medium-Sized Enterprise
FATE Case 2: Build up Robust Risk Management via FATE

Data Demander (an internet bank)
- Sample ID, Y (loan performance)
- Scale of loans: 10 billion
- Scale of customers: 1 million

Data Provider (a large social media company in China)
- Sample ID, X (Features)

Privacy Preserving
- Without privacy preserving, data provider won’t cooperate

Robust Risk Management
- Combine more data to improve precision of credit scoring model
- Establish robust risk management mechanism that satisfies local regulatory requirements

Improved Performance
- AUC: 0.73
- Positive feedback: “helpful to satisfy local regulatory requirements”
FATE Case 3: Better Identify Home Mortgage Fraud via FATE

Data Demander (a personal loan company)
✓ Sample ID, Y (loan performance)
✓ Scale of loans: ~ 100million
✓ Scale of customers: ~ 10 thousand

Data Provider (a large social media company in China)
✓ Sample ID, X (Features)

Bottleneck in Fraud Detection
● Difficult to improve fraud detection with credit history

Higher Recall of Fraud
● Combine more data to improve model prediction performance
● Better identify home mortgage fraud

Improved Performance
● AUC: 0.79 (9.29% ↑)

AUC represents the separability measure or degree (how well the classification machine learning model is capable to distinguish between various classes.)
At a top-tier AML conference held in December 2019, a senior leader of Shenzhen Branch, Peoples’ Bank of China, urged financial institutions to “make more use of Federated AI Technology when connecting with external data sources”.


“All institutions can complete the training of artificial intelligence algorithm model without exchanging data by Federated Learning.” Xiao Gang, a senior researcher at the China Finance 40 Forum, the former chief of China’s securities regulator, told a forum in Qingdao.
FATE Case 5: HKMA Recommends Data Collaboration Using Federated Learning

Federated learning, a new trend in AI, was adopted by one bank that we interviewed to securely learn from the encrypted data captured on electronic invoices, also known as ‘e-Fapiao’. These electronic invoices are shared by organizations centrally in China to improve KYC assessment and credit risk measurement of SMEs.

Corporates such as WeBank have expressed interest in the development of federated learning, and WeBank has contributed its Federated AI Technology Enabler (FATE) framework for use by the open source community so as to assist other banks and corporations to onboard the technology.

"Reshaping Banking with Artificial Intelligence", published by The Hong Kong Monetary Authority (HKMA), December, 2019

Federated Learning in Anti Money Laundering

Regulators+ WeBank AI

Through horizontal federal expansion, anti-money laundering samples are enriched, and the basic anti-money laundering model is constructed.

Through vertical federal expansion, customer characteristic dimensions are further optimized, improving the accuracy and efficiency of the anti-money laundering system.

Bank 1

Bank 2

Bank 3

Transactions
✓ 转账
✓ 支付
✓ ......

Interne t Co. 互联网公司

Mobile Payment Data
✓ 电商购物
✓ 地图轨迹
✓ ......
Federated Learning in Risk Management: Load Credit Risk

Multiple Data Sources → Fed Model → Rating

Rating ~ Quality of Assets

反欺诈/贷前评分/贷后监测

反欺诈评分举例
模型效果：AUC=0.70，KS=30，尾部分组坏样本比例是平均样本比例的2.4倍
使用方式：1）单一策略；2）入模变量；3）决策矩阵

MPC and FL on Multiple Data Sources
微众与瑞士再保险探索再保险商业创新

协助再保公司建立承保人（保险公司）的车险索赔概率模型：纵向联邦引入和挖掘互联网大数据“从人因子”，横向联邦扩大承保人传统因子数据集规模，从而实现对车主进行精准画像和风险分析

Data from Internet
- 出行数据
- 消费数据
- 信息偏好
- 车辆违章数据
- ……

Data from insurance
- 承保数据
- 理赔数据
- 车联网数据
- ……
Federated Computer Vision

Object detection techniques are commonly applied to detect abandoned and suspicious objects. But image data on those objects are imbalanced, and they are typically collected and labeled by different companies with different business goals.
FATE Case 6: Federated Learning in IoT

Perception engine
analysis engine
recognition engine

5G

Cloud computing

Client

Active region

Check-out
Federated Computer Vision

Medical care

• Medical data are often stored at different institutions and are too sensitive to be directly shared due to privacy and legal concerns.
• Federated Learning can be applied to collaboratively train a CV model for diagnosis.
Federated Computer Vision

Autonomous Driving

• CV-powered autonomous driving system built based on heterogeneous data scattered among various types of devices.

• Autonomous car needs stable and robust approaches to ensure the safety of drivers in each and every situation.

• FL can unite all kinds of devices to collaboratively build shared and personalized models.
Federated Natural Language Processing

• Step 1: Each mobile device downloads the shared model from the server
• Step 2: Each mobile device trains the shared model based on user-typed content
• Step 3: Each mobile device summarizes the changes as a small focused update and uploads this update to the server through secure protocol
• Step 4: The server gathers the updates from mobile devices, aggregates these updates, and improves the shared model with the aggregated updates
Federated Learning and COVID-19

  - Show to authorities to visit places, cross border, travel, etc.
  - Question: how to ensure privacy while showing no contact with infections?
联邦学习应用于医疗健康 Fed Health

微众银行携手腾讯天衍实验室成立腾讯医疗健康-微众联合实验室
“脑卒中发病风险预测模型”准确率80%以上
小型医院模型预测指标提升了10-20%

研究论文被FL-IJCAI’20收录
Privacy-Preserving Technology to Help Millions of People: Federated Prediction Model for Stroke Prevention
Ce Ju1,*, Ruihui Zhao2,*, Jichao Sun3,*, Xiguang Wei1,*, Bo Zhao4, Yang Liu5, Hongshan Li6, Tianjian Chen1, Xinwei Zhang1, Dashan Gao5,*, Ben Tan1, Han Yu7 and Yuan Jin8

微众银行携手顶尖学术机构
联邦学习技术在脑机接口领域应用
将不同研究机构、不同受试者的脑电图数据在不泄露隐私信息的情况下联合使用，为脑机接口大规模商用保驾护航。

研究论文被IEEE EMBC 2020收录
Federaed Transfer Learning for EEG Signal Classification
Ce Ju, Dashan Gao, Ravikiran Mane, Ben Tan, Yang Liu, Cuntai Guan

The success of deep learning (DL) methods in the Brain-Computer interface (BCI) field for classification of electroencephalographic (EEG) recordings has been restricted by the lack of large datasets. Privacy concerns associated with EEG signals limit the possibility of constructing a large EEG-BCI dataset by the conglomerate of multiple small ones for jointly training machine learning models. Hence, in this paper, we propose a novel privacy-preserving DL architecture named federated transfer learning (FTL) for EEG

GitHub: https://github.com/DashanGao/Federated-Transfer-Learning-for-EEG

联邦学习应用于语音识别引擎 Fed Voice Recognition

微众AI 基于“联邦对抗学习”的解决方案

语音识别联邦学习方案
- 业界常态目前为技术提供方到应用方的单向信息流动
- 我们的方案实现了技术提供方和应用方共生共赢的生态闭环

语音识别对抗学习方案
- 利用群体智能优胜劣汰
- 减少对数据标注的依赖
IEEE Standard P3652.1 – Federated Machine Learning

- **2019.02**: FATE v0.1 LR, SecureBoost, Eggroll | Federated Network
- **201905**: FATE v0.2, FATE-Serving, Feature Eng.
- **201908**: FATE v1.0, FATE-FLOW | FATEBoard
- **201911**: FATE v1.2, Federated Deep Learning, SecretShare

**201903**: GitHubStar 100+, First outside Contributor

**201906**: FATE v0.3, FATE to Linux Foundation

**201910**: FATE v1.1, spark engine

**201912**: FATE v1.3