White Paper on Federated Learning V2.0

WeBank AI Department

Peng Cheng Laboratory

Tencent Research Institute

CAICT Cloud Computing & Big Data Research Institute

Ping An Technology

CMG Fintech

China UnionPay National Engineering Laboratory of E-Commerce and E-Payment

Jointly Issued by

March 2020

Table of Contents

Chapter I. Background and Importance of Federated Learning

1.1 The State of AI Development

Since the Dartmouth Conference in 1955, AI has experienced two series of springs and winters. More recently, the sector has entered its third spring. The first spring was created by increased expectations on AI, more specifically the desire for automated algorithms that improved efficiency. The following winter was the result of limited algorithmic capabilities as machines proved unable to complete large-scale data training and complex tasks. The second spring started with the proposal of the Hopfield network and the breakthrough of backpropagation, which made large-scale neural network training possible. However, it was found that computing power and data were insufficient and that the design of expert systems was unable to keep up with the growth of industry demand, thus leading to the second winter. The third spring was ushered in by the proposal of deep learning (DL) neural networks in 2006, great improvements to algorithmic and computing power and the emergence of big data in recent years. In 2016, AlphaGo managed to defeat two professional Go players after being trained on a total of 300,000 games. From this, we can see the huge potential of AI and the desire for greater utilization in more extensive, complex, cutting-edge fields such as autonomous driving, medicine and finance.

While the great success of AlphaGo has inspired many with the idea that big data-driven AI can be implemented to improve all walks of life, the reality has been disappointing. With the exception of a few industries, fields are hindered by the limited data volume and quality, which has led to the middling adoption of AI technology. The misconception of the "pervasive availability of AI" may lead to serious commercial consequences. One case is IBM Watson, a very famous Question Answering (QA) system that can find an accurate answer (A) when given a question (Q). Watson can express the Q with a high-dimensional representation, comparable to a spectrum in physics, which is formed of a beam of light broken up into different frequencies by a prism. Such a spectrum needs to be matched with entries in the answer library. The highest matched entry is the most probable answer. While this is a very simple process, the key lies in constructing a very sound answer library. After the success of its appearances on Jeopardy, IBM Watson was applied to what felt like promising applications, such as medicine. Recently, however, the application of IBM Watson to a cancer treatment center in the United States was found to be so unsatisfactory that the project failed. By taking a closer look at the medical field, we can figure out where the questions and answers come from. For example, by using input data such as diseases, gene sequences, pathology reports, and various tests and papers, IBM Watson was expected to make diagnoses that could help doctors. However, after a period of discovery, it was found that the data sources were far from adequate, resulting in poor system performance. Though the medical field requires a huge amount of annotated data,

doctors' time is very precious. Another issue is that unlike certain other computer vision applications, data annotation in the medical field cannot be carried out by laypersons. As such, there is a very limited amount of annotated data available in professional fields such as medicine. It is estimated that if the annotation of medical data was offload to third-party companies, the collection of valid data would require over 100,000 personnel for a period as long as 10 years. This suggests that even if a large amount of manpower was allocated for annotation in these fields, the resulting data would still be insufficient. That is the issue we are facing today.

Additionally, there are certain barriers that are difficult to break between data sources. In general, the data required by AI involves many fields. Take AI product recommendation systems for example, which have the seller's product and sales data, but no data on the purchasing power and payment habits of users. In most industries, data exists in silos. Due to competition, privacy and security, cumbersome administrative procedures and other factors, the integration data between various departments of the same company faces many obstacles. It tends to be very costly, if not unrealistic, to integrate the data scattered throughout such organizations.

1.2 The Challenges Faced by AI

With the further development of big data, increased focus on the privacy and security of data has become a global trend. Every leak data leak leads to a great deal of concern from both the media and the public. For example, the recent Facebook data leak resulted in widespread backlash. In the meantime, countries are strengthening the protection of data security and privacy, as evidenced by the strict guidelines of the EU's *General Data Protection Regulation (GDPR)* formally implemented in 2018. These trends have brought unprecedented challenges to the field of AI. The current state of affairs in both research and business applications is that the party responsible for collecting the data is usually not the one that uses it. For example, data may be collected by Party A, transferred to Party B for cleansing, transferred to Party C for modeling, then finally sold to Party D for use. Such transfer, exchange and transaction of data between entities violates the GDPR and are subject to severe penalties. Similarly, in the *Cybersecurity Law of the People's Republic of China*[1] implemented in 2017 and the *Civil Code of the People's Republic of China - General Part* state that no network operator shall disclose, tamper with or destroy personal information they collected, and shall guarantee that the scope of the data to be traded and the obligations for data protection are clearly defined in the contract prepared for data transaction with a third party. The establishment of these laws and regulations poses new challenges to the traditional manner in which is processing for AI to a variety of extents. At present, there has been no solution proposed from academia or business to meet the challenges of this issue in a satisfactory manner.

1.3 Feasible Solutions to Data Privacy

Resorting to traditional methods to solve the big data dilemma has hit a bottleneck. The simple exchange of data between two entities is not allowed under many laws and regulations, including the GDPR. Users are the owners of their raw data, meaning that it cannot be exchanged between entities without their permission. Additionally, the purpose of data modeling cannot be altered without user consent. In order to ensure compliance, many previous methods such as data exchange have undergone dramatic changes. On the other hand, data owned by commercial enterprises are often of great potential value. When exchanging data, companies and even inter-company departments have to consider the cost and benefits. As such, departments typically do not simply aggregate their data with others, resulting in silos, even within the same company.

A key issue in AI development is designing a machine learning (ML) framework that enables AI systems to use their own data in a more efficient and accurate manner while meeting data privacy, security and regulatory requirements. We advocate a shift in research toward solving the problem of data silos. In light of the above, we propose federated learning [2-4] as a feasible solution that satisfies the requirements of both data privacy and security.

Federated Learning

- Data of all parties is stored locally, ensuring that data privacy and compliance with laws and regulations.
- Multiple parties contribute data to develop a global model from which they can mutually benefit.
- All parties are of equal status.
- The modeling performance of federated learning is the same as, or (in case of user alignment or feature alignment of data) slightly different from, the modeling result achieved through aggregation of all datasets.
- Transfer learning ensures that knowledge transfer can also be achieved through the exchange of encryption parameters between data, even when users or features are not aligned.

Federated learning enables two or more parties to engage in machine learning in a manner that solves data siloing, all while ensuring data privacy and compliance with laws and regulations.

Chapter II. Definition and Value Analysis of Federated Learning

2.1 Overview of Federated Learning

What is federated learning? Let's say there are two different enterprises, A and B, each with its own unique data. Specifically, A has user feature data, while B has product features and annotated data. The two enterprises cannot simply merge their data without violating the GDPR, as the original providers of the data (the respective users) have not been given the chance to consent to such an action. Provided that each enterprise has created a job model in which each job can be classified or forecasted and all jobs have been confirmed by their respective users at the time the data was obtained, the question becomes how to build a high-quality model at the A and B ends respectively. However, as the data may be incomplete (e.g., enterprise A is short of labeled data and enterprise B lacks feature data) or inadequate (e.g., there is not enough data volume to build a sound model), the parties may find it difficult to establish models, or models may not perform to a satisfactory degree. Federated learning aims to address the problem. With the expectation that each enterprise stores its own data locally, federated learning systems can create a global model through parameter exchange under an encryption mechanism while ensuring compliance with data privacy laws and regulations. The model provides optimal performance, comparable to a model built through the aggregation A and B's data. The difference is that the data does not move during the construction of the global model, ensuring data privacy and compliance. In this manner, the constructed model only serves local targets in their respective areas. Parties in a federated learning system can cooperate in a mutually beneficial manner and are of equal status. This is why the system is called federated learning.

The example in this section illustrates the basic idea behind federated learning. The following section will standardize the definition of federated learning, introduce its social and commercial value, and elaborate on the relationship between federated learning and existing research.

2.2 Definition of Federated Learning

Over the course of machine learning, each party can use the data of the other parties for joint modeling. All participants can, without sharing data resources (meaning that data remains local), engage in joint data modeling to establish a global ML model.

The constraints of the federated learning system are:

|V_FED-V_SUM |<δ

where:

V_FED: Performance of the federated learning model;

V_SUM: Performance of models built by traditional methods (i.e., data aggregation); and

δ: Bounded positive numbers.

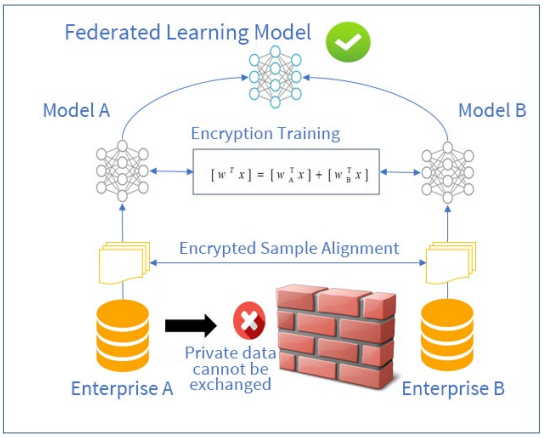


Fig. 1 Federated Learning Architecture

2.3 The Public Value of Federated Learning

There is no doubt that we are currently experiencing the fourth information revolution, with the scale of information and data rapidly increasing. This data, when interpreted through AI, has the potential to revolutionize our daily lives.

As the underlying technology of future AI development, federated learning will continuously take AI to new levels through the connection of data silos under secure and reliable data protection measures. As it sees further penetration and application across a broad range of industry scenarios, federated learning will exert greater influence on all kinds of people, organizations, industries and society. The social value provided by federated learning is outlined below:

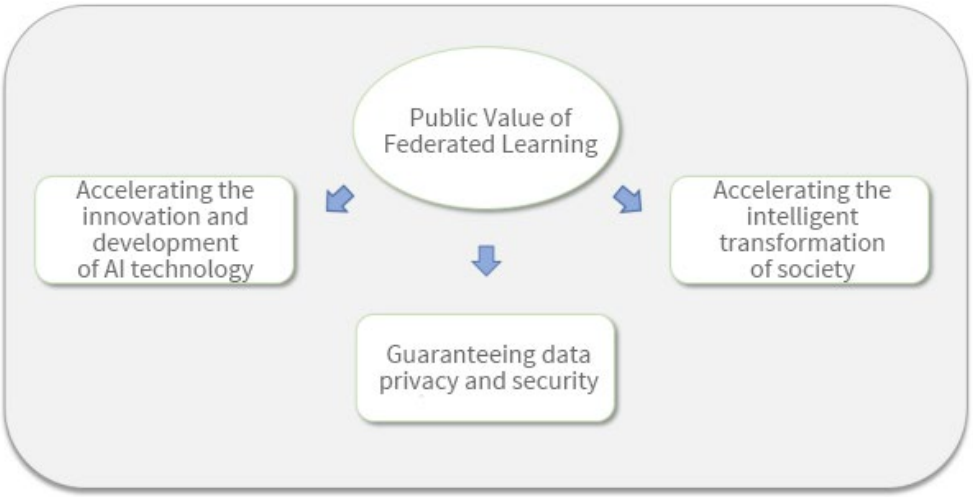


Fig. 2 Public Value of Federated Learning

- Accelerating the innovation and development of AI technology

AI technology has formed an industry ecosystem that integrates diversified resources such as global technology, capital, talent and influence. As an essential core technology of AI modeling, federated learning helps achieve the value of big data and deepens the integration of AI sectors across various localized industries. This enables AI technology to eliminate data bottlenecks and continuously grow and innovate.

- Guaranteeing data privacy and security

Federated learning systems allow parties to store their data locally and allows the creation of a global model through parameter exchange under an encryption mechanism while ensuring compliance with data privacy laws and regulations. Data does not move during the construction of the global model, and consequently data privacy and compliance are ensured.

- Accelerating the intelligent transformation of society

AI technology based on federated learning will be integrated into social infrastructure and life more safely. In addition to assisting human tasks and enhancing daily life, AI will gradually change our models of cognition while stimulating development and the social economy.

2.4 The Commercial Value of Federated Learning

Federated learning technology is a mutually beneficial, highly valuable model for commercial interests. Parties in a federated learning system can cooperate in a mutually beneficial manner and are of equal status. This is why the system is called federated learning. The commercial value provided by federated learning is outlined below:

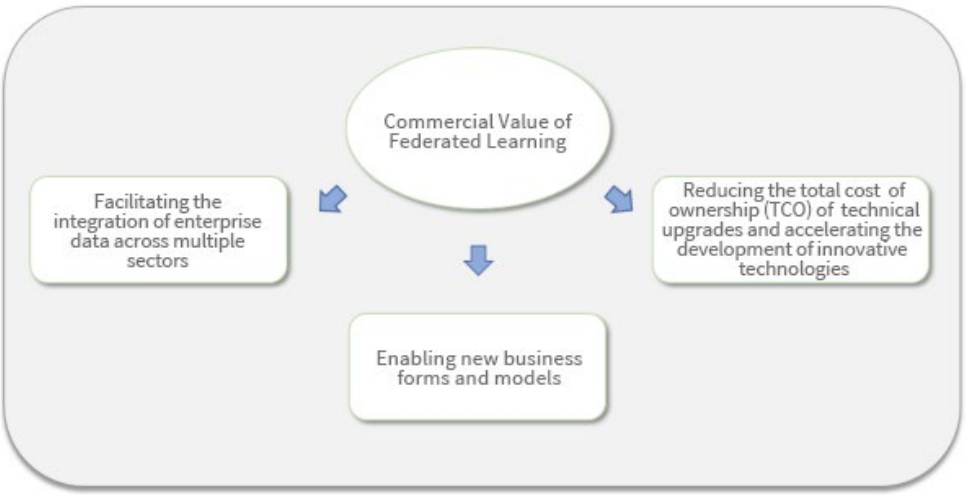


Fig. 3 Commercial Value of Federated Learning

- Facilitating the integration of enterprise data across multiple sectors while enhancing market layouts and competitiveness through intelligent strategies

As an underlying technology of AI development, federated learning enables enterprises to join global and cross-industry federated ecosystems. Through such cooperation enterprises can train models to assist market layouts and optimize strategies more competitively. Federated learning allows enterprises to establish better cooperation and more competitive strategies at the technical level. The model creates a unique ecosystem and promotes the healthy development of enterprises.

- Enabling new business forms and models

The application and expansion of federated ecosystems and federated learning systems across more sectors will continuously influence and transform the collaborative relationship between supply and demand. It will redefine the status, service models and profit models of all parties, and it will facilitate new forms.

- Reducing the total cost of ownership (TCO) of technical upgrades and accelerating the development of innovative technologies

The reusable solutions offered by federated learning systems can reduce the threshold while expanding the scope and breadth of technical applications, thereby allowing enterprises across multiple industries to provide a larger variety of products and services to different customers. The federated learning ecosystem eliminates concerns of data security and empowers breakthroughs in innovative technology while improving efficiency.

2.5 Federated Learning and Existing Research

As federated learning is a brand-new technology, incorporates aspects from other, more mature technologies into its own innovations. In this section, we will outline the relationship between federated learning and related concepts from multiple perspectives.

Differences Between Federated Learning and Differential Privacy

The characteristics of federated learning enable the protection of data privacy, albeit in a different manner from the methods commonly used in big data and data mining, such as differential privacy,[5] k-anonymity,[6] l-diversity[7] and others. The principle of federated learning differs from traditional data privacy methods. In federated learning, data privacy is protected through parameter exchange under a homomorphic [8-12] or other encryption mechanisms. Unlike differential privacy, federated learning data and models are not transmitted. This means that there is no possibility of a leak at the data level and that more stringent data protection regulations such as the GDPR will not be violated. In differential privacy, k-anonymity, l-diversity, and similar methods, privacy is protected by adding noise to data or blurring certain sensitive properties through generalization. This is done until a third party cannot distinguish between individuals, and it ensures that data cannot be restored at a

high probability. In essence however, these methods still engage in the transmission of raw data. It also has the inherent potential of an attack, and consequently it may no longer be viable under the more stringent data-protection regulations such as the GDPR. Federated learning, however, provides a more powerful means to protect the privacy of user data.

Differences Between Federated Learning and Distributed Machine Learning

In terms of federated training between multiple parties, horizontal federated learning is similar to distributed machine learning. Distributed machine learning covers many aspects, including the distributed storage of training data, distributed execution of computing jobs, the distributed release of model results, etc. Parameter servers [13] are a typical example of Distributed Machine Learning. Parameter servers accelerate the training of machine learning models, store data on distributed work nodes, and distribute data and allocate compute resources through a central scheduling node. Thus, the final training model is created more efficiently. In horizontal federated learning, the work node represents the owner of the data being trained in the model. It has full autonomy over local data and can independently decide when to allow federated learning modeling, unlike the central node in parameter servers, which always plays the dominant role. Naturally, this means that federated learning faces a more complex environment. Federated learning emphasizes data privacy in the course of model training, meaning that it can better respond to the increasingly strict regulations on data privacy and security.

Relationship Between Federated Learning and Federated Database Systems

Federated database systems [14] work by integrating multiple databases and managing the integrated whole. The purpose of such systems is to achieve the coordinated operation of multiple independent databases. In the federated database system, individual databases are often stored in a distributed and (in practice) heterogeneous manner. The system is similar to federated learning in terms of data types and storage model. Federated database systems differ in that the interaction among individual databases does not include any data privacy mechanism, meaning that all databases are completely visible to the management system. Moreover, the system focuses on basic database operations (insert, delete, search and merge). Contrastingly, federated learning focuses on establishing a global model that ensures data privacy so as to facilitate better utilization of data models and rules.

Relationship Between Federated Learning and the Blockchain

Blockchain is a distributed ledger based on cryptographic security. The blockchain is easy to verify and impossible to tamper with. Blockchain 2.0 is a decentralized application that uses open-source code and distributed storage to ensure extremely high levels of transparency and security while protecting data from tampering. Examples of blockchain applications include Bitcoin (BTC) and Ethereum (ETH). Blockchain and federated learning are decentralized networks. The difference is that blockchain is a complete peer-to-peer (P2P) network structure, while in federated learning a third party assumes model aggregation, management and other responsibilities. Federated learning and blockchain involve cryptography, encryption algorithms and other basic technologies. Blockchain uses algorithms such as hashing and

asymmetric encryption, while federated learning relies on homomorphic encryption, etc. On the blockchain, all data is recorded on each node through encryption. In federated learning, the data of each party is only stored locally. In terms of incentive mechanisms, different nodes on the blockchain gain rewards by contributing to the ledger. In federated learning, two or more parties cooperate to improve model training results, with rewards distributed according to contribution.

Relationship Between Federated Learning and Secure Multi-Party Computation

In federated learning, user privacy and security are the top priorities. To protect user privacy and prevent applications from being attacked by malicious parties, secure multiparty computation technology can be applied as a part of federated learning technical frameworks. Research into enhancing the security of federated learning through secure multiparty computation has already started. McMahan [15] noted that federated learning could provide higher levels of security through technologies such as differential privacy, secure multiparty computation or a combination of both. Bonawitz [16] proposed that federated learning could use secure multiparty computation to compute the sum of model parameter updates from user devices in a secure manner. Truex [17] proposed a more private federated learning method that used both differential privacy and secure multiparty computation. Liu [18] proposed the application of additive homomorphic encryption (AHE) to the multiparty computation of neural networks. FATE [19], an open-source federated learning framework proposed by WeBank, uses relevant operators that facilitate the efficient development of secure multiparty computation applications.

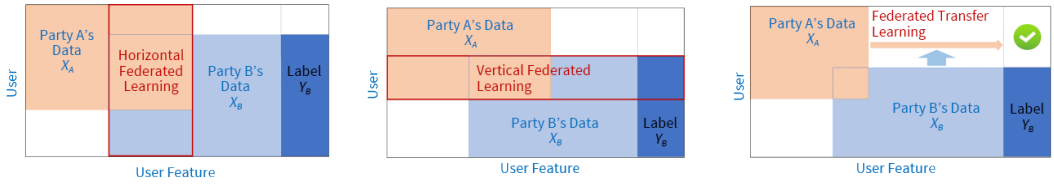
Chapter III. Federated Learning Classifications

The definition of federated learning provided above did not outline how to specifically design an implementation scheme. In practice, siloed data have different distribution features, from which we can propose corresponding federated learning schemes. This chapter focuses on the classification of federated learning scenarios based on the distribution features of siloed data.

Given that there are more than one data owner, the dataset D_i held by each data owner can be represented by a matrix. Each row in the matrix represents a user, while each column represents a user feature. Some datasets may also contain labeled data, which is required in the construction of predictive user-behavior models. We will refer to user features as "X" and label features as "Y". Y is a user's credit score in finance, their consumer desire in marketing, or their mastery of a given field in education. X and Y constitute a complete set of training data (X, Y). In practical terms, we often encounter situations in which user datasets or features are not exactly the same. For example, in a federated learning scenario with two data owners, the distribution can fall into the situations outlined below:

- The user features (X1, X2, ...) of the two datasets overlap to a large extent, while the users (U1, U2, ...) overlap to a small extent;
- The users (U1, U2, ...) of the two datasets overlap to a large extent, while the user features (X1, X2, ...) overlap to a small extent;
- Both the users (U1, U2, ...) and user features (X1, X2, ...) of the two datasets overlap to a small extent.

To better handle these distribution scenarios, we classify federated learning into horizontal federated learning, vertical federated learning and federated transfer learning (Fig. 4).



Horizontal Federated Learning (HFL) Vertical Federated Learning (VTL) Federated Transfer Learning (FTL)

Fig. 4 Federated Learning Classifications

3.1 Horizontal Federated Learning

When the user features of two datasets overlap to a large extent and users overlap to a small extent, we segment the datasets horizontally (by user) and remove data in which the user features are the same but users are not exactly the same from the training process. This method is known as "horizontal federated learning". For example, consider two banks operating in different regions. Their user base largely comes from their respective regions, meaning that there is little overlap. However, their businesses are similar, meaning that recorded user features are the same. In such cases, we can use horizontal federated learning to construct a global model. Google proposed a federation data modeling scheme for Android updates [15,20] in 2017. The proposal outlined a federated learning scheme in which model parameters are continuously updated locally when a user uses an Android, then uploaded to the Android cloud. This allows all data owners with the same features to establish a global model.

3.2 Vertical Federated Learning

When the users of two datasets overlap to a large extent and user features overlap to a small extent, we segment the datasets vertically (by feature) and remove data in which the users are the same but user features are not exactly the same from the training process. This method is known as "vertical federated learning". As an example, consider two different organizations in the same region. One is a bank, while the other is an e-commerce company. Their userbases are made up of most the residents of the region, meaning there is a large overlap. However, the bank only records the user's income, expenditure and credit score; while the e-commerce company records user browsing and purchase history. This means that their user features only overlap to a small degree. Vertical federated learning aggregates the different features in an encrypted state to enhance model performance. As of time of writing, it has been confirmed that many machine learning models such as logistic regression, tree structures and neural networks can be built on the federated learning system.

3.3 Federated Transfer Learning

When both the users and user features of two datasets overlap to a small extent, we do not segment the data but instead use transfer learning [21] to overcome the insufficiency of data or labels. This method is known as "federated transfer learning" [22].

As an example, consider two different organizations. One is a bank in China, while the other is an e-commerce company in the United States. Due to the geographical differences, their userbase has a very small overlap. Additionally, the differences in their operations means that there is a small overlap in their data features as well. To ensure effective federated learning in this scenario, it is necessary to introduce transfer learning to solve the issues caused by lack of data overlap and labeled samples.

Chapter IV. Federated Learning Frameworks

4.1 Introduction to Open-Source Federated Learning Frameworks

As of current, the primary federated learning frameworks in the industry are FATE,[23] TensorFlow Federated,[24] PaddleFL,[25] and Pysyft[26].

In February 2019, WeBank moved its FATE framework to open-source. FATE v1.2 was released in December 2019, whereby it covered horizontal federated learning, vertical federated learning and federated transfer learning. The framework has received widespread attention from and adoption by the community. FATE provides over 20 federated learning algorithm components, covering LR, GBDT, DNN and other mainstream algorithms to satisfy the modeling requirements of conventional commercial applications. FATE serves as a one-stop federated learning model solution, covering feature engineering, ML model training, model evaluation and online inference. In comparison with other open-source frameworks, FATE offers significant advantages in industrial applications.

OpenMined's open-source Pysyft framework supports horizontal federated learning to an adequate degree. The framework also provides many choices for users to get started quickly through support for Tensorflow, Keras and Pytorch. Pysyft provides encryption operators, arithmetic operators and federated learning algorithms. The framework also allows users to build their own federated learning algorithms efficiently. In comparison with FATE, Pysyft has not yet offered any efficient deployment or service solution. The framework is more suitable for efficient academic research and prototyping than it is for industrial applications.

Google's open-source TensorFlow Federated framework has supported horizontal federated learning since the release of version 0.11 in December 2019. The framework's Federated Learning (FL) API can be integrated with TensorFlow or Keras in order to complete classification, regression and other jobs. Users can also use its Federated Core (FC) API to economically express new federation algorithms by combining TensorFlow with distributed communication operators in a strongly typed functional programming environment. As of present, TensorFlow Federated lacks both an open implementation of encryption operators and sound support for online production.

In November 2019, Baidu announced it would move its PaddleFL framework to open-source. PaddleFL contains security operators such as DiffieHellman, along with machine learning algorithms such as LR. It lags behind the other frameworks in terms of operator availability due to its comparatively shorter time in open-source. PaddleFL has advantages in attracting related ecosystem developers, owing to integration with Baidu's PaddlePaddle open-source ML framework.

A comparison of open-source federated learning frameworks is provided below:

Open-Source Framework	**FATE**	**TensorFlow Federated**	**PaddleFL**	**Pysyft**
Application Scenario	Industry/academic research	Academic research	Academic research	Academic research
Developer	WeBank	Google	Baidu	OpenMined
Federated Learning Type	Horizontal federated learning, vertical federated learning and federated transfer learning	Horizontal federated learning	Horizontal federated learning and vertical federated learning	Horizontal federated learning
Feature Engineering Algorithm	Feature binning, feature selection and feature correlation analysis	Not supported	Not supported	Not supported
	Supported	Not supported	Not supported	Not supported
Machine Learning Algorithm	LR, GBDT, DNN, etc.	LR, DNN, etc.	LR, DNN, etc.	LR, DNN, etc.
Security Protocol	Homomorphic encryption, SecretShare, RSA and DiffieHellman	DP	DP	Homomorphic encryption and SecretShare
Online Federated Inference	Supported	Not supported	Not supported	Not supported
Kubernetes	Supported	Not supported	Not supported	Not supported
Host Platform	GitHub (https://github.com/FederatedAI/FATE)	GitHub (https://github.com/tensorflow/federated)	GitHub (https://github.com/PaddlePaddle/PaddleFL)	GitHub (https://github.com/OpenMined/PySyft)

4.2 FATE: Enterprise Federated Learning Architecture

In February 2019, WeBank's AI Department moved its proprietary FATE (Federated AI Technology Enabler) framework to open-source. FATE was the first anywhere to provide a secure computing framework for federated AI ecosystems.

FATE provides a distributed secure computing framework that focuses on data privacy; provides high-performance and secure compute support for machine learning, deep learning and transfer learning algorithms; supports homomorphic encryption, SecretShare, DiffieHellman and other secure multi-party computation protocols. The platform also provides a set of user-friendly cross-sector interactive data management solutions to help federated learning algorithms pass data security audits. FATE enables data cooperation between multiple entities protecting data privacy and security in compliance with the laws and regulations.

As of current, FATE has been used to facilitate implementation in credit-risk management, customer equity pricing, governance technology and other areas.

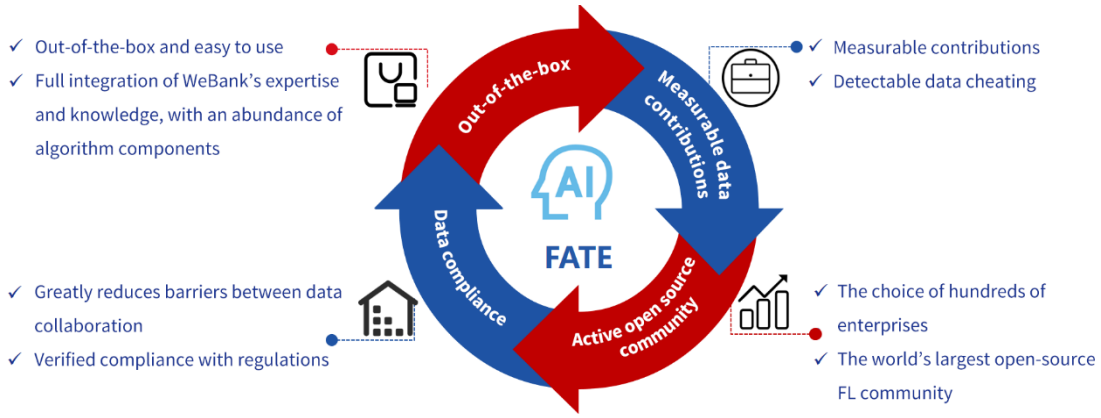


Fig. 5 Advantages of the FATE Framework

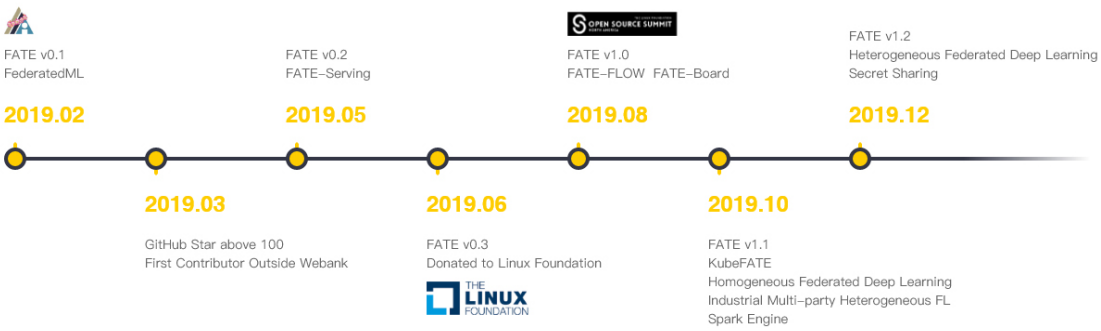


Fig. 6 FATE Milestones in 2019

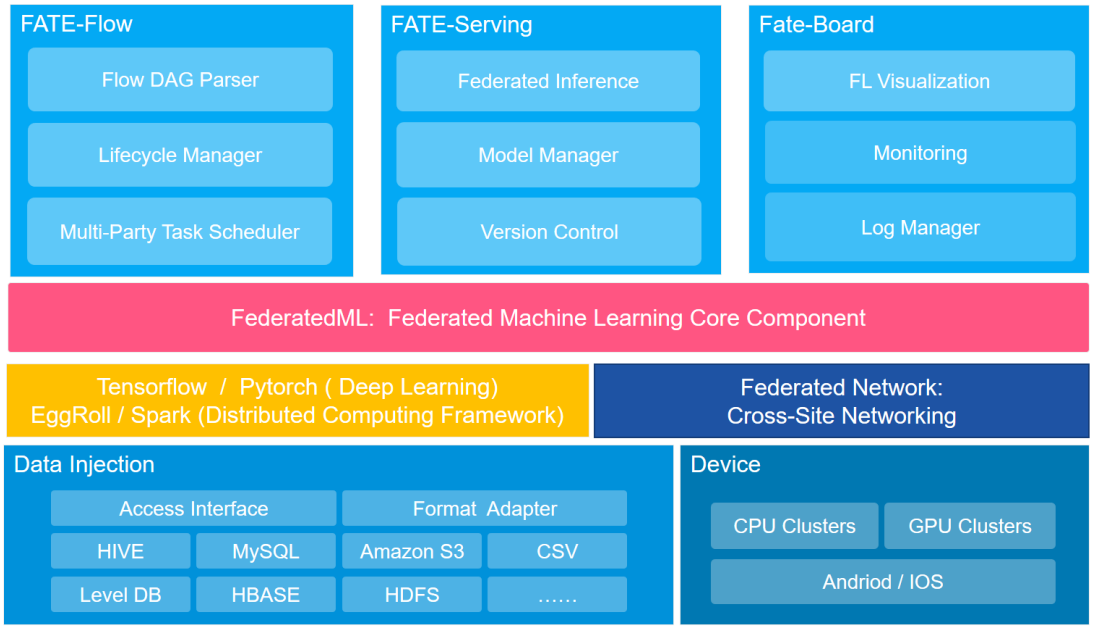


Fig. 7 FATE Technical Framework

FederatedML

A functional component of the federated learning algorithm. Includes the federated implementation of many common ML algorithms. All modules are developed in a modular and decoupled manner to enhance scalability.

Primary Functions

- Federated sample alignment: Vertical sample ID alignment, including alignment based on RSA+hash, etc.
- Federated feature engineering: Sampling, feature binning, feature selection, correlation, statistics, etc.
- Federated machine learning: Logistic regression, linear regression, Poisson regression, SecureBoost, DNN, FTL, etc.
- Secure multi-party computation protocol: Homomorphic encryption, SecretShare, RSA, DiffieHellman, etc.

FATE-Flow

The scheduling and lifecycle management tool used to build end-to-end FL pipeline production services for users.

Primary Functions

- DAG Parser for FL modeling pipelines
- Lifecycle management of FL modeling jobs
- Multi-party collaborative scheduling of FL modeling jobs
- Federated multiparty model and model version management
- Real-time tracking of data, indicator, model and other I/Os in FL modeling processes

FATE-Board

An FL modeling tool used to visualize and measure the entire model training process for end users. Supports tracking, statistics, monitoring and other features throughout the entire model training process, and provides rich visualization of model execution status, model output, log tracking and more. FATE-Board helps users explore and understand models in a simple, efficient, in-depth manner.

Primary Functions

- Visualization of FL modeling jobs throughout their lifecycle
- Visualization of FL models
- Visualization of evaluation reports

FATE-Serving

A high-performance and scalable online FL model service.

Primary Functions

- High-performance online FL model inference algorithm
- Online FL model management
- Online FL inference pipeline

KubeFATE

A tool that deploys FATE on Docker Compose or Kubernetes (Helm Charts) through containerizing all FATE components. Modern applications are developed through DevOps way. Containerization provides advantages in that applications can run on any platform with container support and flexibly achieve multi-instance horizontal scaling on demand. KubeFATE enables developers to easily deploy FATE projects in public or private clouds.

Chapter V. Examples of Federated Learning Applications

The value of federated learning depends on its key application scenarios. It is only through the instantiation of FL applications that we can identify the challenges and opportunities in its development. The following sections introduce seven typical application scenarios for federated learning.

5.1 FL Auto Insurance Pricing

Background and Demand

China's insurance industry has entered a rapid stage of development. Increasingly fierce market competition and rapidly growing product varieties have created higher demands for risk identification and accurate pricing. Traditional methods of risk identification have proved to be inadequate with regard to operational requirements and have started to have a negative effect on profitability.

Using auto insurance as an example, traditional pricing models are determined in accordance with the quality of the vehicle, meaning that the premium for a luxury car is far higher than that of an ordinary one. Despite this, key factors that influence risk during the insurance period such as vehicle servicing conditions, driving environment and others also have a critical influence on insurance pricing. As such, the consumer market has been transitioning from vehicle-based to consumer-based pricing. As the insurance industry is highly regulated, the data that influences pricing accuracy if fairly scattered. Transaction data is only available for vertical scenarios, there is comparatively little customer data and there is no effective mechanism to integrate data links. This makes it difficult to achieve accurate pricing.

The insurance industry has also suffered serious product homogenization, along with difficulties in precisely reaching customers through marketing. Both these issues affect the future development prospects of insurance enterprises.

FL Solutions

Given the fact that consumer, vehicle and behavioral auto insurance pricing data was scattered across different companies; data could not be exported; and aggregation and modeling could not be performed directly, an FL mechanism was introduced to access data sources from multiple parties and break down barriers between data during modeling, all while ensuring the privacy of local user data provided by cooperating parties.

To resolve the issue of sticky pricing caused by serious product homogenization, multidimensional and multi-label Internet behavioral data was introduced so as to refine user profiles, render personalized pricing services and empower marketing intelligence decision-making. To prevent the negative effects of hazards to public morality, big data was used to identify malicious users and insurance fraud.

Advantages of FL Solutions

The FL data model includes a rich variety of risk management features to effectively identify risks, predict insurance costs and provide personalized pricing services. As a result, pricing accuracy in the industry has been greatly improved to over 90%.

By using a big data model compliant with data regulations, the solutions help enhance the marketing intelligence service system, improve precise and customized integrated financial service capabilities and accurately identify high-value targets to improve customer acquisition.

Industry Prospects

Data helps empower the ability of insurance companies to read the user market. Smart finance based on federated learning ensures data privacy, breaks barriers between data, and deeply integrates upstream and downstream insurance scenarios. The solution solves issues such as data siloing and poor customer experiences in insurance companies, intermediary organizations and agents by reducing marketing costs, enhancing data service efficiency, improving quality throughout the entire process and facilitating the healthy and orderly digital transformation of the insurance market.

5.2 FL Credit-Risk Management

Background and Demand

In credit risk management, the cost of a credit review for a single customer is relatively high. This is due to the need to call different data APIs throughout the process. For example, for businesses of consumer finance and micro and small enterprise (MSE) credit, the cost of calling APIs for identity verification, credit checks, etc. is extremely high.

When faced with MSE credit requests, banks and other financial organizations are often short of useful data about enterprise operations, resulting in difficult, slow, costly financing. Similarly in regard to risk management, consumer finance organizations lack effective Internet behavioral profiles and other data. The credit qualifications of lower-tier loan customers also tend to vary more considerably.

Integrating AI with the traditional financial industry to comprehensively judge the qualification and credit of MSEs in areas such as profitability, income fluctuation and growth potential; and users in areas such as consumer behavior, consumer power, interests, and preferences from multisource data in a legal and compliant manner has become an important issue. Ensuring the financial inclusion of MSEs and shortening the distance between consumer finance companies, and payment-and-consumption scenarios are other critical concerns.

FL Solutions

By using a federated data network, the solution helps tighten credit risk management to facilitate pre-approval procedures. Starting from risk sources, the solutions help companies filter out blacklisted or clearly ineligible customers to further reduce credit review costs in the later stages of the loan approval process.

For problems faced by financial institutions such as low Y sample volume, poor distinction between good and bad samples, and deviation of sample distribution from the normal distribution, the solutions provide long-term data accumulation and help obtain more high-similarity Y data from relevant cooperating parties such as credit organizations. During the sampling process, repeated screening and re-sampling ensures that data is synchronized between all parties in real time. This prevents data misalignment (e.g., X in 2018 corresponding to Y in 2019) and ensures that complete data remains within normal distributions at all times. Specifically, the solution digitizes projects by performing a cold boot of operations through the FL cloud service, small sample modeling through the establishment of closed-loop operational and AI models, followed by iterative optimization of models in later stages. This enables consumer finance and credit institutions to continuously accumulate business data and optimize their FL models.

To solve issues such as scarce and incomplete credit review and historical MSE data, the solutions establish a multisource data fusion mechanism to includes transaction data, taxation, industrial and commercial data, and other MSE data to assist financial institutions in obtaining X in more dimensions to enrich their feature systems. In the process of constructing the feature system, the solutions aim to ensure the security and privacy of the data providers while improving model effectiveness. Specifically, the solutions enable cooperating parties to observe the effectiveness of their own data in optimizing the FL model through sample alignment by the FL cloud service and VFL modeling and parameter output.

Advantages of FL Solutions

Through legal and compliant multi-dimensional FL data modeling, the performance of the risk management model was improved by around 12%, reducing the expected credit review costs of consumer finance institutions by 5% to 10% while enhancing risk management through greater volume and quality of data samples. Cooperating parties also greatly improved their credit risk management capabilities. Expected API call costs were reduced by 20% to 30% during pre-approval through the elimination of blacklisted or clearly ineligible customers.

By using FL data modeling, financial and credit institutions can connect data siloes to maximize the value of their data in a legal and compliant manner. Financial institutions can scale these benefits to payment-and-consumption scenarios, while credit institutions enhance their core competitiveness.

Industry Prospects

Smart risk management based on federated learning accelerates the implementation of security-first AI technology, enhances value creation in the consumer finance industry, and improves the ability of relevant industries to manage risk. In addition, federated learning improves the ability of fintech companies to serve financial institutions.

Federated learning has already seen application in all aspects of the risk management process, including fraud prevention, preliminary screening, pre-approval, early warning during and after a loan, and more. Multi-dimensional cooperation can be carried out in accordance with the specific needs of enterprises and organizations. In the future, through deeper penetration into primary credit risk management and review processes, and further utilization of FL modeling in all steps of credit review, federated learning will achieve data interconnection and cooperation while ensuring privacy.

5.3 FL Sales Forecasting

Background and Demand

The development of China's economy has brought with it the acceleration of consumption upgrades. As consumption structures are constantly optimized and demand for services rapidly increases, the growth rate of retail sales has been slowing down accordingly. Data from the National Bureau of Statistics shows that the retail sales of social consumer goods in 2018 totaled CNY 38.09 trillion, up 4.02% and down 6.19% respectively in growth and growth rate from the previous year, where the year-on-year growth rate has decreased for five consecutive years.

The physical retail industry has suffered from ever-growing inventories, slowdowns in growth and the challenge of new retail. To better control for increasing labor costs, decreasing gross profits and mitigating the high losses suffered by the increasingly critical fresh produce business, digital transformation in a legally compliant manner has become an important tool for retail enterprises.

FL Solutions

In regard to losses suffered by the fresh produce business, the solutions provide dynamic inventory counting, product organization for timely sales, forecasting and recommendations for hot-selling products, and other functions to achieve the smart management of retail locations, perform real-time adjustments and pricing strategies in accordance with product freshness, and provide timely feedback to control for losses. Big data is used to forecast hot-selling products and provide retail enterprises with relevant information. This allows the rapid optimization of marketing strategies and enhanced sales conversion.

In the smart retail business scenarios, the data features involved primarily include user purchasing power, user preferences and product characteristics. In practical applications however, these features are likely to be scattered across different departments or enterprises.

For example, banks have user purchasing power features, social networking sites have user preference features, and shopping sites have product characteristics. This creates two key difficulties. First is that it is almost impossible to break the barriers between bank, social networking site, and shopping site data while ensuring user privacy and the protection of enterprise data, meaning that there is no way for smart retail departments to aggregate and model data. Second is that the user feature data is typically heterogeneous, meaning that traditional ML models cannot directly use them for training.

Federated learning allows all parties to construct a machine learning model without exporting their own enterprise data. This ensures user privacy and data security while providing personalized product recommendations, marketing strategies and targeted services to benefit all involved parties.

Advantages of FL Solutions

Technology empowers the management of fresh produce to help enterprises achieve refined operations and sales forecasting of over 85% accuracy. After sufficient project optimization, accuracy can reach over 95%. As a result, retail enterprises reduced losses and greatly increased sales. Through the digital transformation of labor, enterprises were able to flexibly reallocate personnel across multiple tasks, make efficient use of idle time both on- and off-site, fully mobilize personnel and enhance production efficiency. The implementation of a smart labor allocation platform improves personnel efficiency by roughly 27%.

By implementing digital transformation strategies driven by FL modeling, retail enterprises can provide personalized product services in a legal and compliant manner to expand sales channels. In addition to improving the user experience, the solutions lay a foundation for precision marketing. The result is a retail model that caters more to user needs, controlled labor costs, and improved personnel and floor efficiency.

Industry Prospects

The FL smart labor allocation system provides a complete platform that covers the entire labor allocation process and solves the problem of data asymmetry between the supply and demand of labor. Combined with the diversified scenarios of labor-intensive industries and the capabilities of AI, banking and finance, the system provides both parties with high flexibility and freedom in on seamless platform with bank-level clearing and settlement, credit accumulation, and other value-added services.

The system also provides enterprises with AI-empowered digital transformation in planning, purchasing, warehousing, manufacturing, and E2E sales to enhance offline operation models and achieve a truly demand-oriented smart operations system.

In the future, the FL implementation models can further diversify into industries such as manufacturing, warehousing and logistics, import/export and other verticals. In this manner, AI, big data, engineering product functionality, etc., can be applied to all areas of the national economy while ensuring the privacy and security of data.

5.4 FL Smart Security

Background and Demand

As of present, the Chinese cities have developed naturally through 40 years from rural to urban. Over the next decades, the creation of "smart" cities will become the new driving force for urban development.

In China, 83% of prefecture-level cities, representing 500 cities in total, have explicitly proposed or are already in the process of transforming into a smart city. Smart security serves as an essential component in the smart city. In traditional security scenarios, cameras are used to collect basic data, and IT systems and multiprocessors are used to process the data. Control rooms are established to engage in monitoring, supplemented by manual detection of dangerous behaviors. These processes are lengthy, carry high labor costs, and provide low community management efficiency.

Traditional security scenarios are also unable to predict the people flow of community residents, the anomalies of specific groups (such as the elderly, drug addicts and criminals) and are typically too slow to enable rapid response. Existing anomaly definitions rely on subjective considerations, which may lead to errors and misjudgments in the early warning process. Though a large amount of data about user traffic in communities are collected by cameras, access cards, and other means, they tend to not correlated with each other. This means that many communities have fragmented information silos, which makes it difficult for them to tap into the value of data.

FL Solutions

The development of smart cities cannot be separated from a foundation of security, which serves as a core module.

The preset algorithm training model provides early warning, real-time and high-precision tracking shoots, location judgment, action recognition, behavioral analysis, and travel trajectory and abnormal pathing detection to improve community security and management efficiency. By using federated learning and multi-community data to build the security model, data can interconnect and intercommunication across multiple communities for smart security networks with overlapping dimensions.

Based on cloud computing and big data analysis, smart security systems engage in continuous post-incident summary and self-learning. Like a police officer that never tires or retires, the system continuously accumulates experience and improves its early warning capability.

Advantages of FL Solutions

In daily scenario applications, a flood of data from videos, sensors, and information software is collected, sorted and analyzed to provide more secure, accurate, expansive risk prediction services to communities.

In consideration of data security, centralized data modeling is unavailable for the time being. FL models based on data collected from 10 communities have been shown to be better than single-community models in all aspects. Even when applied to just two communities with less sample data available, the accuracy of the FL model was about 3% higher than that of a single-community model.

Industry Prospects

FL smart security ensures data privacy while integrating user traffic and other data across multiple communities. The solutions deliver all-weather monitoring of public and secure areas, early prediction, timely detection, along with early warning and post-incident tracing to enhance community security in all aspects. They provide a reliable and powerful guarantee of community security, public security, policing and public management.

5.5 FL-Assisted Diagnosis

Background and Demand

Medical care, education and pensions are the key areas of concern for most Chinese citizens. In recent years, shortages in medical resources, disparities between doctor income and workload, and doctor-patient disputes have occurred with greater frequency. Furthermore, in a hierarchical medical system with giant hospitals such as West China Hospital and First Affiliated Hospital of Zhengzhou University on top and a variety of township clinics and community hospitals with few patients on the bottom, the quality of care offered by hospitals at different levels varies greatly. Leading hospitals are able to provide better infrastructure and competitive remuneration for staff, which in turn attract more patients and further improves medical research. Hospitals already lagging behind are unable to acquire many patients, which makes it difficult for them to attract high-quality doctors and nurses. The lack of quality personnel further reduces the desire for patients to seek medical treatment at the hospital, leading to a vicious cycle. The centralization of resources in a major area such as healthcare has an adverse impact on public welfare.

The digitization of medical treatment and informatization of cases and treatment data has made AI-assisted medical treatment based on big data possible. For example, with fundus photographs, AI can detect diseases such as diabetic retinopathy at levels similar to that of professional doctors [27]. Such medical data contains a large amount of private patient information. The protection of such highly sensitive data is a significant responsibility of hospitals, AI companies and relevant regulators.

FL Solutions

Hospitals in China are divided into 10 grades and three tiers, and different hospitals vary greatly in terms of patient cases. The results of certain standardized tests and examinations conducted before patients are diagnosed are less affected by operators and can be standardized by equipment and standardized procedures. By taking advantage of standardized

data, horizontal federated learning models based on patient health, test, and examination data ensure that patient data stays in hospital systems and improves diagnosis accuracy.

In addition to improving the ability of lower-tier hospitals to provide higher-quality test results and attract more patients, FL smart medical care also helps doctors diagnose patients to reduce their workload. With the help of smart medical care, patients can seek treatment in their locales, reducing an enormous amount of transportation, accommodation and other costs incurred from travel from smaller cities to provincial capitals or other provinces. This allows patients to spend money on treatment more efficiently, and it relieves a significant burden on both patients and their families.

Advantages of FL Solutions

Using stroke detection as example, the application of horizontal federated learning to a hospital with a small number of cases increases detection accuracy by 10% to 20% over scenarios that only use the hospital's own cases as training samples. Model accuracy is further improved as case samples from more hospitals are added to the FL training process.

Additionally, FL disease prediction carries no risk of patient data leaking. Based on the fact that nearly 2 million patients in China seek medical treatment in locales away from their hometowns (restricted to cross-provincial medical treatment) every year, if FL disease prediction covers only 10% of these patients, roughly CNY 200 million can be saved in the early diagnosis stage each year.

Industry Prospects

As AI gradually enters the medical industry, institutions will accumulate more and higher quality medical data through electronization, informatization and structuring so as to lay a stronger foundation for AI-assisted medical care. FL smart medical care empowers the treatment in clinical diagnosis and other subfields while protecting patient privacy. The applications of federated learning for smart medical care scenarios develop high-quality medical resources shared by regions with fewer resources, and improve the capacity and quality of medical services in Central China, West China, and community-level medical organizations at a very low cost.

5.6 FL Smart Advertising

Background and Demand

The upstream and downstream of the online advertising industry includes advertisers, ad providers and advertising data-exchange platforms. Over a long period, online ads have served as the primary source of income for many top Internet companies. For both foreign companies such as Google and Facebook or Chinese companies such as Tencent, Alibaba, Toutiao, and Baidu, advertising constitutes a significant portion of revenue. In terms of demand, most companies or brand owners allocated a significant portion of their yearly budget to online advertising in order to promote their products and grow revenue. For example, banks hope to

find acquire credit card users through online ads. When macro-economic growth slows down, advertisers experience a decrease in revenue, meaning that they have to cut the advertising budget accordingly and pursue a higher return on investment (ROI). This creates an urgent demand for smart ads that offer higher efficiency at a lower cost.

FL Solutions

The core technologies behind online ads include user targeting and bidding. FL smart advertising helps reduce the cost of customer acquisition. Federated transfer learning enables the enhanced integration of multi-party data to develop user insight and targeting strategies. Real-time APIs (RTAs) constitute a key technology that helps advertisers acquire customers efficiently by preventing the waste of resources from repeated delivery. When applied to RTAs, FL technologies help further improve data security while effectively reducing cost. FL technology randomly encrypts the user features and labels of both advertisers and ad providers to ensure that neither party knows whether individual users have undergone backend conversions or what their specific risk labels are. The use of differential privacy technology in federated learning obfuscates data in a manner that other parties can only view a generalized summary, and cannot identify any individual in the data. WeBank's FL ad solutions effectively filter out invalid traffic through scoring and blacklist system, reducing backend conversion costs and improving ROI.

Advantages of FL Solutions

In comparison with traditional advertising solutions that only focus on frontend data optimization, FL ad solutions use encrypted backend data, cover conversion-end data in addition to the traditional display, click and arrival steps, and strictly ensure the privacy of platform and user data in high-value loan, credit card, insurance, online education and home improvement industries. Using FL advertising frontend and backend integration solutions for the financial industry as an example, conversion cheating was reduced by 2% in the pre-loan stage, achieved directly through RTA, meaning that customer operations were not required. In the post-loan stage, this is improved to about 5% through traffic grading, which filters out high-risk users that are not eligible for credit.

Industry Prospects

Federated learning, differential privacy and secure multi-party computation help manage traffic risks, optimize online traffic, filter unwanted traffic in advance and optimize delivery efficiency while ensuring data privacy and security under increasingly strict regulations. FL advertising technology reduces delivery costs, improves advertiser ROI, and enables the utilization of funds for product innovation and R&D. For ad providers, it improves user click-through rate (CTR) and conversion rate and optimizes link efficiency to achieve mutually beneficial cooperation between all parties.

5.7 FL Autonomous Driving

Background and Demand

The complexity and diversity of China's urban road scenarios pose great challenges to autonomous driving. However, typical traffic scenarios such as highways, docks and pedestrian-free zones are also suitable for implementation due to the simple road environment, fewer pedestrians and vehicle incidents. Logistics and similar industries that require large numbers of drivers to traverse long distances on highways every year have found it harder and harder to recruit younger generations. To make matters worse, they are constantly under the shadow of a high rate of traffic accidents. It is reported that one out of every seven truck drivers has been involved in a traffic accident, and the annual mortality rate of truck drivers is as high as 5% [28]. Autonomous driving will free people from high-stress and high-risk jobs in the logistics industry. Autonomous trucks can transport goods 24/7, which improves asset utilization and reduces costs.

The autonomous driving industry is experiencing an unprecedented boom. Google launched an autonomous vehicle project (Waymo [29]), Tesla launched an autonomous driving system (Autopilot[30]), Baidu launched Apollo,[31] and the leading ride-sharing companies such as Uber and DiDi have begun implementing autonomous driving applications. As major auto companies begin competitive differentiation by focusing on driver assistance and technologies such as the Internet of Vehicles (IoV) and Internet of Roads (IoR) continue to develop, autonomous driving technology will continue to offer extremely high social and economic value in the future.

FL Solutions

Due to the restriction of driving region and time, the sensor data obtained by ordinary vehicles tends to be usually limited. Using horizontal federated learning to integrate the data from the cameras, ultrasonic sensors, radars (e.g., mmWave and LIDAR) and other devices of different vehicles accelerates the deployment of scenario data and improves the model robustness.

In recent years, the field has gradually achieved that autonomous driving should not simply learn from or copy human driving but also interact with the IoV, cooperative vehicle infrastructure systems (CVIS) and even full traffic systems to create a better driving environment. Interactive learning between vehicles and system environments assisted by other urban data such as cameras, traffic lights and smart roads can, when used with VFL, enhance the integration of data from different sources while ensuring privacy and improving the autonomous driving experience.

Advantages of FL Solutions

Perception, planning (decision-making) and control are three core modules of autonomous driving. The perception of input data from sensors such as LIDAR and cameras (monocular, binocular and omnidirectional cameras), as with the human eye, provides basic input for the subsequent planning stage. It serves as the foundation of autonomous driving. The data generated by a single vehicle is usually limited by time and region. Another issue is that a large amount of sensor data is generated

while a vehicle is in motion. The resulting raw data may cause privacy issues, meaning that multicar data in traditional centralized ML processes may lead to new ethical and technical challenges.

By using data from different vehicles data, ensuring data privacy and reducing communication bandwidth, FL modeling on a NVIDIA Jetson RC experimental vehicle performed significantly better than single-vehicle ML in obstacle avoidance, route planning, and other aspects. Particularly, experimental vehicles using federated learning performed 48% better than ordinary vehicles in terms of obstacle avoidance.

Industry Prospects

While auto industry is a pillar of the Chinese economy, it urgently needs new technologies to deliver further industry growth. According to the National Bureau of Statistics, China's labor force decreased for the first time in 2018. As the population continues to age and the social economy becomes more sophisticated, the labor costs of the transportation industry will continue to increase in the future. The high-risk nature and limited career opportunities of the transportation industry will make it difficult to attract young workers. Autonomous driving will serve as a critical technology in ensuring the sound development of society over the next two decades. HFL autonomous driving technologies accelerate perception training while protecting the privacy of drivers and passengers. In the future, VFL will integrate with IoT, CVIS, 5G and other new technologies so as to constitute a smart traffic ecosystem that is efficient, secure and low-cost.

Chapter VI. The Development of Federated Learning

Taking into account the development environment of AI and big data along with practical industry pain points and demands, it is suggested that the four developmental stages of federated learning outlined below should be followed.

6.1 Cultivate an Open-Source Development Ecosystem

The construction of a good open-source environment is the foundation for the sustainable development of federated learning. Proper support for open-source software will expand the influence of federated learning technology, attract research and business implementation, and further link the upstream and downstream of the entire industry to actively participate in open-source development.

An open-source ecosystem can be cultivated through the considerations outlined below.

As the management and operation of open-source communities require the investment of much capital and labor, they are usually reliant on companies, foundations, or alliances. Relying on GitHub, the Linux Foundation, the Apache Software Foundation or a similar group helps FL frameworks attract relevant personnel from all over the world to drive rapid development. In practical applications, companies, organizations and individuals from around the world can provide first-hand feedback, while developers can set efficient and practical short- and long-term research goals. As open-source communities work with project maintainers, a virtuous cycle is formed, benefiting the ecosystem as a whole.

Establishing a domestic open-source environment that encourages fair competition will be the foundation FL autonomous applications. China has a huge potential market and a large pool of expert researchers and technicians. The development of a sound open-source federated learning environment in China will help relevant personnel communicate and implement FL technology more efficiently, while also reducing technical dependence as the geopolitical and economic environment fluctuates. Currently, OpenI-Zongheng, which integrates the FL compute toolset, has been donated to the OpenI Platform as a completed project. OpenI-Zongheng provides rich, one-stop FL modeling components that facilitate rapid experimentation and iterative algorithms to meet the demands of most FL modeling jobs.

6.2 Establish Domestic and International Standards

The construction of AI and other relevant standard systems is accelerating both at home and abroad. The International Organization for Standardization (ISO) established the ISO/IEC JTC 1/SC 42 in October 2017. The United States, Germany, and other countries have also submitted AI terminology and reference model standard proposals. In January 2018, supported by the Standardization Administration of China (SAC) and the Ministry of Industry and Information Technology (MIIT), the National AI General Working Group was established to gather key domestic enterprises and research institutes in AI to promote the construction of China's AI standard system.

Developing and establishing domestic standards (such as group standards and national standards) and international standards (such as IEEE enterprise standards) for federated learning and formulating framework norms, use models and usage specifications can help different institutions engage in legal, compliant, and mutually beneficial multi-data collaboration. This in turn establishes more accurate data models, ensures data privacy and security, and provides a feasible solution for problems that have been or will be encountered during the practical implementation of AI in different industries. The Big Data Technology Standard Promotion Committee of the China Communications Standards Association (CCSA TC601) is also developing industry and group standards related to federated learning. The committee will soon launch the standard compliance testing for FL products. The *Technical Specification for Financial Applications of Secure Multi-party Computation* industry standard of the China Financial Standardization Technical Committee (CFSTC), initiated by the Science and Technology Department of the People's Bank of China is currently in the feedback stage. This year, the National Internet Finance Association of China (NIFA) will also start the development of group standards related to the federated learning data collaboration under the same framework. The NIFA standards emphasize ease of implementation and provide reference opinions based on security requirements in different scenarios.

6.3 Establish Application Examples in Industry Verticals

The actual implementation of federated learning in industry scenarios will provide practical and effective support for research into algorithms. Application scenarios can be divided into homogeneous and heterogeneous scenarios. Homogeneous scenarios refer to situations in which two enterprises in the same or similar fields have similar data properties and features, but different samples. For example, banks and financial institutions have different user samples. In this scenario, horizontal federated learning achieves high model performance through the integration of their samples. Heterogeneous scenarios refer to situations in which two enterprises in different fields have different data properties and features, with a certain overlap in sample IDs. For example, banks and Internet companies both have a degree of overlap in user IDs, but different user feature data. Specifically, the bank has data on user income and transaction behaviors, while the Internet company has data of user activity and travel behavior. In this scenario, vertical federated learning improves feature efficiency in

models. The applications in each of these scenarios show that FL modeling is an improvement on local modeling based on a single party's data.

Promoting the application of federated learning in industry verticals, particularly in heterogeneous scenarios, will help establish a new operational model and a big data ecosystem of mutual growth.

6.4 Establish a Comprehensive Data Alliances

The development of federated learning can generally be divided into three stages. The first is point-to-point development, which includes the creation of open-source FL models and the establishment of FL standards; the second is application implementation and case accumulation; and the third is the establishment of FL data alliances. Federated learning is expected to bring the real knowledge and value behind data to the table, and it is hoped that all parties will work together to build FL data alliances. An FL data alliance should, far beyond traditional knowledge value networks based on knowledge graphs, deliver practical data value and industry knowledge on a grand scale. Through incentive mechanisms, existing members are encouraged to open up the true value behind their data in a legal and compliant manner. In addition to benefiting the members themselves, this will attract more companies and institutions in the field to join as new nodes for extensive integration and the dynamic flow of valuable data. With the establishment of FL data alliances, data will accelerate the growth of industry revenues at low costs, the incentive mechanism will integrate verticals more closely, and FL technology will ensure healthy development. Thousands of industries, including finance, medicine, retail, transportation, express delivery and tourism, have already established their own FL data networks. In the future, different networks will interact with each other, which will unlock an endless way of possibilities.

Chapter VII. Conclusion and Outlook

In recent years, the siloed distribution of data and the tightening of data privacy regulations have become the next challenge for AI. The emergence of federated learning provides new ideas for AI to break down barriers between data and move to the next stage of development. Federated learning enables multiple data owners to establish a mutually beneficial global model while ensuring the and privacy security of local data. This paper briefly introduces the basic concept, architecture and technical principles behind federated learning, and explores the great contributions of federated learning to AI development in certain application scenarios. It is hoped that in the near future, federated learning can help break down barriers between data in all industries and sectors, create an ecosystem of shared data and knowledge while protecting data privacy and security, and implement a consensus mechanism from which alliance contributors are rewarded so that AI may deliver the maximum possible benefit to every corner of society.

7.1 Future Direction of Federated Learning Research

7.1.1 Security

The following components of the federated learning systems might be attacked.

Client: A party with administrator privileges can launch malicious attacks through the client device. A compromised client can check all messages (including models) received from the server in involved iterations as part of an effort to tamper with the training process. A neutral client can check all messages received from the server without tampering with the training process.

Server: A compromised server can check all messages (including gradient descent) sent to it in all iterations so as to tamper with the training process. A neutral server can check all messages sent to it without tampering with the training process.

The process of model output and deployment may also be subject to attacks. Strictly ensuring privacy in these circumstances poses a great challenge.

Attack methods primarily include model update poisoning, data poisoning attack and evasion attack. Based on their position in the lifecycle, attacks can be roughly divided into training attacks (model update poisoning and data poisoning attacks) and inference attacks (evasion attacks).

Model update poisoning attack: An attacker takes direct control of certain clients and changes their output to a model biased toward the attacker. When an attacker controls the client to produce an arbitrary output, this is called a "Byzantine attack"[32]. In such attacks, the compromised client(s) send any value instead of the locally updated model to the server. This may lead to convergence toward a suboptimal model, or even model divergence. In

comparison with untargeted attacks such as Byzantine attacks, targeted model attacks are typically less costly. Literature [33] shows that when 10% of devices in federated learning are controlled by a malicious attacker, backdoors may be introduced through attacking the model of the server. Centralized ML guards against model update poisoning attacks through controlling training data or processes. However, this method cannot be directly applied to federated learning.

Data poisoning attack: Unlike in model update poisoning attacks, data poisoning attacks do not give the attacker the ability to directly alter the model of the central node. Attacks can instead tamper with the data, features, or labels of the client to achieve an untargeted or targeted attack. Similar to model update poisoning attacks, it is difficult to detect the existence of data poisoning attacks with only indicators such as global accuracy or single-client training accuracy.

Evasion attack: During the model inference stage, an attacker can cheat a target system by constructing specific input samples without altering the ML system itself. By adding noise or through other methods, the attack produces inputs that look almost indistinguishable to the original test inputs to deceive the trained model. In image and audio applications, adversarial samples are usually constructed by adding norm-bounded disturbance to the test samples. Adversarial training (i.e., training a robust model with adversarial samples) is usually robust enough to prevent white-box evasion attacks. However, it usually only improves the robustness of specific types of samples (such as adversarial samples) in the training process. The trained model is still vulnerable to other forms of adversarial noise. Additionally, preventing evasion attacks through adversarial training may encounter several problems in federated learning. As adversarial training is primarily used for independent and identically distributed data, performance is not guaranteed in non-independent and identically distributed environments. In federated learning, data cannot be checked before training, making it difficult to configure suitable disturbance norm bounds. As such, new robustness optimization technologies may be required to prevent evasion attacks in federated learning scenarios.

Differential privacy and similar technologies are the key methods used to prevent attacks. Many challenges in federated learning systems can be seen are a requirement for robustness — clean data is destroyed or otherwise tampered with, maliciously or otherwise. Differential privacy (DP) [34] defines privacy from the perspective of robustness. In short, the impact on specific data points can be reduced by adding random noise during training or testing.

In addition to attacks, federated learning may also be affected by non-malicious failures from unreliable clients outside the control of service providers. Though non-malicious failures are usually less destructive than attacks, they may be more common, and share a similar root cause and complexity with malicious attacks. As such, future research on security will involve not only preventing attacks, but also reducing the impact of non-malicious failures on privacy and security.

7.1.2 Incentive Mechanism

The value of federated learning lies in breaking data silos and, by encouraging structures with similar data (HFL) and different data (VFL) to train together, improving overall model performance. Throughout the entire process, the design of an effective incentive mechanism can be used to motivate endpoint users or different enterprises and institutions to participate in federated learning. The introduction of concepts such as game theory and contract theory can improve the design of an incentive mechanism. As different endpoints and organizations participate in FL, it is necessary to effectively measure the contributions of each party to fairly allocate rewards and further incentivize contribution, thus forming a virtuous cycle. The design of an effective reward, punishment, and allocation mechanism is an important area of research.

7.1.3 Efficiency

Non-independent and identically distributed data

A lot of real-world data is non-independent and identically distributed (non-IID). For example, people in different geographical areas have different preferences and tendencies. In a certain time periods, an individual may make choices that differ from usual. Different clients may also have data of vastly different sizes.

While centralized machine learning can obtain all current or previously generated samples to ensure optimized global model training, federated learning requires that data must stay local. This means that many centralized ML techniques such as data shuffling cannot be applied directly. Compared with centralized ML, the impact of such data distribution has a greater adverse effect on the training model.

Improving objective functions or making finite assumptions will be an important area of research to reduce the impact of non-IID data. To address the impact caused by data distribution, the FedProx [35] algorithm attempts to add a proximal term to each local objective function with the idea of making the algorithm more robust to the inhomogeneity of local objectives. Under the assumption that all clients are involved, Ahmed Khaled [36] uses batch gradient descent to help client random gradients converge faster.

Another area of research is improving optimization functions to solve the problem of non-IID data. In the deep learning process, optimization functions have undergone SGD, Adagrad, Adam and other forms of development, where the introduction of momentum delivers faster convergence speed and accuracy. The introduction of momentum and variance in the first-order optimization method of federated learning functions is an effective way to improve optimization and generalization performance. However, there has yet to be a consensus on how to incorporate momentum or variance technology into local SGD and federation averaging in regard to federated learning. SCAFFOLD [37] uses control variables to explicitly model the difference in client updates to the reduction of performance variance, which allows rapid convergence without limiting the distribution difference of client data. In regards to momentum, Yu et al. [38] suggest maintaining a local momentum buffer on each client, then

averaging these local buffers and local model parameters in each communication round. While this method improved the accuracy of local SGD in testing, it requires doubled communication costs. Wang et al. [39] proposed the SlowMo momentum solution to significantly improve the optimization and generalization performance of local SGD without sacrificing throughput. Hsu et al. [40] proposed a momentum solution similar to SlowMo. While the momentum variable of local SGD can converge to the stationary point of the non-convex objective function at the same rate as synchronous small-batch SGD, it is still theoretically difficult to prove that the momentum accelerates the convergence rate in federated learning environments[38,39].

Fine-tuning, transfer learning, meta-learning and other technologies are also constantly being introduced to federated learning to address the impact of non-IID data.

Parameter adjustment with limited resources

In addition to optimization function selection (such as in DL and ML) in areas such as learning rate, batch size and regularization, federated learning requires consideration of parameter selection such as aggregation rules, clients per iteration and local iterations per round. Parties participating in federated learning may be data center servers with many compute and storage resources, or edge devices that are not always online. Some parties may also have limited compute, storage and network resources. Some methods that help adjust model performance in deep learning such as AutoML and NAS (neural architecture search), cannot be directly applied to federated learning as they take up more resources and thus directly reduce communication and compute efficiency. Hyperparameter adjustment with limited resources is thus a challenging and direction of research.

Limited communication bandwidth and device unreliability

In comparison with core nodes in data centers or on data center links, end users that access via wireless networks or close to Internet endpoints usually have lower network bandwidth and communication efficiency. Such connections may be more costly, or otherwise prove unable to guarantee stability. For example, a mobile endpoint may access federated learning training systems only when it is fully charged and connected to a wireless network. This has led to research on how to best reduce the communication bandwidth required for federated learning. There is room for data compression in gradient, model propagation, local computing, and similar areas. It has been proven that combining FL averaging with sparsification or quantification model updating significantly reduces communication costs with little impact on training accuracy. However, it is not clear whether communication costs can be further reduced at present, or whether these methods (or a combination thereof) can provide the best balance between communication efficiency and model accuracy.

References

[1] Xinhuanet. (publication authorized) Cybersecurity Law of the People's Republic of China [OL]. [2020-02-17]. http://www.xinhuanet.com/politics/2016-11/07/c_1119867015.htm

[2] Huang S. Will "federated learning" serve as a breakthrough to the problem of "data silos" hindering AI development? [OL]. [2020-02-17]. https://www.leiphone.com/news/201902/5bLTrPeA6XwkwelR.html

[3] Cong M. How can AI-assisted big data be inclusive and shared with consideration for data privacy? CCF TF's "Federated Learning" seminar provides the answer [OL]. [2019-08-15]. https://www.leiphone.com/news/201903/qk0nnX5iC0G6bPaK.html

[4] Yang Q., Yang L., Chen T., et al. Federated Learning [J]. China Computer Federation Newsletter (CCCF), 2018, 11 (14): 49-55.

[5] Dwork C. Differential Privacy: A survey of results[C]//International Conference on Theory and Applications of Models of Computation. Springer, Berlin, Heidelberg, 2008: 1-19.

[6] Sweeney L. k-anonymity: A model for protecting privacy [J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10 (05): 557-570.

[7] Li N., Li T., Venkatasubramanian S. t-closeness: Privacy beyond k-anonymity and l-diversity [C]//Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on Intelligent Transportation Systems. IEEE, 2007: 106-115.

[8] Gentry C., et al. Fully homomorphic encryption using ideal lattices. In Stoc, volume 9, pages 169-178, 2009.

[9] Brakerski Z. Fully homomorphic encryption without modulus switching from classical gapsvp. In CRYPTO, volume 7417 of Lecture Notes in Computer Science, pages 868-886. Springer, 2012.

[10] Fan J. and Vercauteren F. Somewhat practical fully homomorphic encryption. IACR Cryptology ePrint Archive, 2012:144, 2012.

[11] Brakerski Z., Gentry C. and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In ITCS, pages 309-325. ACM, 2012.

[12] Coron J. S., Lepoint T. and Tibouchi M. Scale-invariant fully homomorphic encryption over the integers. In Public Key Cryptography, volume 8383 of Lecture Notes in Computer Science, pages 311-328. Springer, 2014.

[13] Ho Q., Cipar J., Cui H., et al. More effective distributed ml via a stale synchronous parallel parameter server [C]//Advances in neural information processing systems. 2013: 1223-1231.

[14] Sheth A. P. and Larson J. A. Federated database systems for managing distributed, heterogeneous, and autonomous databases [J]. ACM Computing Surveys (CSUR), 1990, 22(3): 183-236.

[15] Konečný J., McMahan H. B., Yu F. X., et al. Federated learning: Strategies for improving communication efficiency [J]. arXiv preprint arXiv: 1610.05492, 2016.

[16] Bonawitz K., Ivanov V., Kreuter B., et al. Practical secure aggregation for federated learning on user-held data [J]. arXiv preprint arXiv: 1611.04482, 2016.

[17] Truex S., Baracaldo N., Anwar A, et al. A hybrid approach to privacy-preserving federated learning [J]. arXiv preprint arXiv: 1812.03224, 2018.

[18] Liu Y., Chen T. and Yang Q. Secure Federated Transfer Learning [J]. arXiv preprint arXiv: 1812.03337, 2018.

[19] WeBank. FATE Open-Source Federated Learning Platform [CP/OL]. [2020-02-17]. https://github.com/FederatedAI/FATE

[20] McMahan H. B., Moore E., Ramage D., et al. Communication-efficient learning of deep networks from decentralized data [J]. arXiv preprint arXiv: 1602.05629, 2016.

[21] Pan S. J. and Yang Q. A survey on transfer learning [J]. IEEE Transactions on Knowledge and Data Engineering, 2010, 22(10): 1345-1359.

[22] Liu Y., Chen T., and Yang Q. Secure Federated Transfer Learning [J]. arXiv preprint, arXiv: 1812.03337, 2018.

[23] WeBank. Industry Federated Learning Framework [OL]. [2020-02-17]. https://fate.fedai.org/

[24] Google. TensorFlow Federated: machine learning based on distributed data [OL]. [2020-02-17]. https://tensorflow.google.cn/federated

[25] Baidu PaddlePaddle. Baidu PaddlePaddle release note [OL]. [2020-02-17]. https://www.paddlepaddle.org.cn/

[26] Openmined. syft [OL]. [2020-02-17] https://pypi.org/project/syft/

[27] Gulshan V., Peng L., Coram M., et al. Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs [J]. Jama, 2016, 316(22): 2402-2410.

[28] Sina Finance. Survival rate among truck drivers: the desperation of those left behind [OL]. [2020-02-17]. http://finance.sina.com.cn/china/gncj/2018-10-08/doc-ifxeuwws2145661.shtml

[29] Waymo. Waymo official website [OL]. [2020-02-17]. https://waymo.com

[30] Tesla. Autopilot system introduction [OL]. [2020-02-17]. https://www.tesla.com

[31] Baidu. Apollo autonomous driving solution [OL]. [2020-02-17]. https://apollo.auto/index.html

[32] Lamport L., Shostak R. and Pease M. The Byzantine generals problem [M]//Concurrency: the Works of Leslie Lamport. 2019: 203-226.

[33] Bhagoji A. N., Chakraborty S., Mittal P., et al. Analyzing federated learning through an adversarial lens [J]. arXiv preprint arXiv: 1811.12470, 2018.

[34] Dwork C., McSherry F., Nissim K., et al. Calibrating noise to sensitivity in private data analysis[C]//Theory of cryptography conference. Springer, Berlin, Heidelberg, 2006: 265-284.

[35] Li T., Sahu A. K., Zaheer M., et al. Federated optimization in heterogeneous networks [J]. arXiv preprint arXiv: 1812.06127, 2018.

[36] Khaled A., Mishchenko K. and Richtárik P. First analysis of local GD on heterogeneous data [J]. arXiv preprint arXiv: 1909.04715, 2019.

[37] Karimireddy S. P., Kale S., Mohri M., et al. SCAFFOLD: Stochastic controlled averaging for on-device federated learning [J]. arXiv preprint arXiv: 1910.06378, 2019.

[38] Yu H., Jin R. and Yang S. On the linear speedup analysis of communication efficient momentum SGD for distributed non-convex optimization [J]. arXiv preprint arXiv: 1905.03817, 2019.

[39] Wang J., Tantia V., Ballas N., et al. SlowMo: Improving communication-efficient distributed SGD with slow momentum [J]. arXiv preprint arXiv: 1910.00643, 2019.

[40] Hsu T. M. H., Qi H. and Brown M. Measuring the effects of non-identical data distribution for federated visual classification [J]. arXiv preprint arXiv: 1909.06335, 2019.