A principal motivating example for Federated Learning arises when the training data comes from users’ interaction with mobile applications. Federated Learning enables mobile phones to collaboratively learn a shared prediction model while keeping all the training data on device, decoupling the ability to do machine learning from the need to store the data in the cloud.

The training data is kept locally on users’ mobile devices, and the devices are used as nodes performing computation on their local data in order to update a global model

For simplicity, we consider synchronized algorithms for Federated Learning where a typical round consists of the following steps:

1. A subset of existing clients is selected, each of which downloads the current model.

2. Each client in the subset computes an updated model based on their local data.

3. The model updates are sent from the selected clients to the sever.

4. The server aggregates these models (typically by averaging) to construct an improved

global model.

Outline and summary. The goal of increasing communication efficiency of Federated Learning is to reduce the cost of sending to the server, while learning from data stored across large number of devices with limited internet connection and availability for computation. We propose two general classes of approaches, structured updates and sketched updates. In the Experiments section, we evaluate the effect of these methods in training deep neural networks.

Federated Learning is a distributed machine learning approach which enables model training on a large corpus of decentralized data. We have built a scalable production system for Federated Learning in the domain of mobile devices, based on TensorFlow. In this paper, we describe the resulting high-level design, sketch some of the challenges and their solutions, and touch upon the open problems and future directions.

Federated Learning (FL) (McMahan et al., 2017) is a distributed machine learning approach which enables training on a large corpus of decentralized data residing on devices like mobile phones.

“bringing the code to the data, instead of the data to the code"

**. The Federated Averaging algorithm**

In this paper, we report on a system design for such algorithms in the domain of mobile phones (Android). This work

is still in an early stage, and we do not have all problems solved, nor are we able to give a comprehensive discussion of all required components. Rather, we attempt to sketch the major components of the system, describe the challenges, and identify the open issues, in the hope that this will be useful to spark further systems research.

Our system enables one to train a deep neural network, using TensorFlow (Abadi et al., 2016), on data stored on the phone which will never leave the device. The weights are combined in the cloud with Federated Averaging, constructing a global model which is pushed back to phones for inference. An implementation of Secure Aggregation (Bonawitz et al., 2017) ensures that on a global level individual updates from phones are uninspectable. The system has been applied in large scale applications, for instance in the realm of a phone keyboard.

: device availability that correlates with the local data distribution in complex ways (e.g., time zone dependency); unreliable device connectivity and interrupted execution; orchestration of lock-step execution across devices with varying availability; and limited device storage and compute resources. These issues are addressed at the communication protocol, device, and server levels.

We have reached a state of maturity sufficient to deploy the system in production and solve applied learning problems over tens of millions of real-world devices; we anticipate uses where the number of devices reaches billions.

Applications

Current applications of Federated Learning are for supervised learning tasks, typically using labels inferred from user activity (e.g., clicks or typed words)

Content suggestions for on-device keyboards On-device

keyboard implementations can add value to users by suggesting relevant content – for example, search queries that are related to the input text. Federated Learning can be used

to train ML models for triggering the suggestion feature, as well as ranking the items that can be suggested in the current context. This approach has been taken by Google’s Gboard mobile keyboard team, using our FL system (Yang et al., 2018).

Next word prediction Gboard also used our FL platform to train a recurrent neural network (RNN) for next-wordprediction (Hard et al., 2018). This model, which has about 1.4 million parameters, converges in 3000 FL rounds after processing 6e8 sentences from 1.5e6 users over 5 days of training (so each round takes about 2–3 minutes).3 It

improves top-1 recall over a baseline n-gram model from 13.0% to 16.4%, and matches the performance of a servertrained RNN which required 1.2e8 SGD steps. In live A/B experiments, the FL model outperforms both the n-gram and the server-trained RNN models.

Today’s AI still faces two major challenges. One is that in most industries, data exists in the form of isolated islands. The other is the strengthening of data privacy and security. We propose a possible solution to thesechallenges: secure federated learning. Beyond the federated learning framework first proposed by Google in 2016, we introduce a comprehensive secure federated learning framework, which includes horizontal federated

learning, vertical federated learning and federated transfer learning. We provide definitions, architectures and applications for the federated learning framework, and provide a comprehensive survey of existing works on this subject. In addition, we propose building data networks among organizations based on federated mechanisms as an effective solution to allow knowledge to be shared without compromising user privacy

In fact, it is very difficult, if not impossible, in many situations to break the barriers between

data sources. In general, the data required in any AI project involves multiple types. For example, in an AI-driven product recommendation service, the product seller has information about the product, data of the user’s purchase, but not the data that describe user’s purchasing ability and payment habits. In most industries, data exists in the form of isolated islands. Due to industry competition, privacy security, and complicated administrative procedures, even data integration between different departments of the same company faces heavy resistance. It is almost impossible to integrate the data scattered around the country and institutions, or the cost is prohibited. At the same time, with the increasing awareness of large companies compromising on data security and user privacy, the emphasis on data privacy and security has become a worldwide major issue. News about leaks on public data are causing great concerns in public media and governments. For example, the recent data breach by Facebook has caused a wide range of protests [70]. In response, states across the world are strengthening laws in protection of data security

and privacy. An example is the General Data Protection Regulation (GDPR)[19] enforced by the European Union on May 25, 2018. GDPR (Figure 1) aims to protect users’ personal privacy and data security. It requires businesses to use clear and plain languages for their user agreement and grants users the "right to be forgotten", that is, users can have their personal data deleted or withdrawn. Companies violating the bill will face stiff fine. Similar acts of privacy and security are being enacted in the US and China. For example, China’s Cyber Security Law and the General Principles of the Civil Law, enacted in 2017, require that Internet businesses must not leak or tamper with the personal information that they collect and that, when conducting data transactions with third parties, they need to ensure that the proposed contract follow legal data protection obligations. The establishment of these regulations will clearly help build a more civil society, but will also pose new challenges to the data transaction procedures commonly used today in AI. To be more specific, traditional data processing models in AI often involves simple data transactions models, with one party collecting and transferring data to anoanother party, and this other party will be responsible for cleaning and fusing the data. Finally a third party will take the integrated data and build models for still other parties to use. The models are usually the final products that are sold as a service. This traditional procedure face challenges with the above new data regulations and laws. As well, since users may be unclear about the future uses of the models, the transactions violate laws such as the GDPR. As a result, we face a dilemma that our data is in the form of isolated islands, but we are forbidden in many situations to collect, fuse and use the data to different places for AI processing. How to legally solve the problem of data fragmentation and isolation is a majorchallenge for AI researchers and practitioners today.

In this article, we give an overview of a new approach known as federated learning, which is

a possible solution for these challenges. We survey existing works on federated learning, and

propose definitions, categorizations and applications for a comprehensive secure federated learning framework. We discuss how the federated learning framework can be applied to various businesses successfully. In promoting federated learning, we hope to shift the focus of AI development from improving model performance, which is what most of the AI field is currently doing, to investigating methods for data integration that is compliant with data privacy and security laws.

Federated learning enables multiple parties to collaboratively construct a machine learning model while keeping their private training data private. As a novel technology, federated learning has several threads of originality, some of which are rooted on existing fields. Below we explain the relationship between federated learning and other related concepts from multiple perspectives.

3.1 Privacy-preserving machine learning

3.2 Federated Learning vs Distributed Machine Learning

Take the smart retail as an example. Its purpose is to use machine learning techniques to provide customers with personalized services, mainly including product recommendation and sales services. The data features involved in the smart retail business mainly include user purchasing power,user personal preference, and product characteristics. In practical applications, these three data features are likely to be scattered among three different departments or enterprises. For example, a user’s purchasing power can be inferred from her bank savings and her personal preference can be analyzed from her social networks, while the characteristics of products are recorded by an e-shop. In this scenario, we are facing two problems. First, for the protection of data privacy and data security, data barriers between banks, social networking sites, and e-shopping sites are difficult to break. As a result, data cannot be directly aggregated to train a model. Second, the data stored in the three parties are usually heterogeneous, and traditional machine learning models cannot directly work on heterogeneous data. For now, these problems have not been effectively solved with traditional machine learning methods, which hinder the popularization and application of

artificial intelligence in more fields. Federated learning and transfer learning

Federated learning and transfer learning are the key to solving these problems. First, by exploiting the characteristics of federated learning, we can build a machine learning model for the three parties without exporting the enterprise data, which not only fully protects data privacy and data security, but also provides customers with personalized and targeted services and thereby achieves mutual benefits. Meanwhile, we can leverage transfer learning to address the data heterogeneity problem and break through the limitations of traditional artificial intelligence techniques. Therefore federated learning provides a good technical support for us to build a cross-enterprise, cross-data, and cross-domain ecosphere for big data and artificial intelligence.

One can use federated learning framework for multi-party database querying without exposing the data. For example, supposed in a finance application we are interested in detecting multiparty borrowing, which has been a major risk factor in the banking industry. This happens when certain users maliciously borrows from one bank to pay for the loan at another bank. Multi-party borrowing is a threat to financial stability as a large number of such illegal actions may cause the entire financial system to collapse. To find such users without exposing the user list to each other between banks A and B, we can exploit a federated learning framework. In particular, we can use the encryption mechanism of federated learning and encrypt the user list at each party, and then take the intersection of the encrypted list in the federation. The decryption of the final result gives the list of multi-party borrowers, without exposing the other "good" users to the other party. As we will see below, this operation corresponds to the vertical federated learning framework.

Smart healthcare is another domain which we expect will greatly benefit from the rising of

federated learning techniques. Medical data such as disease symptoms, gene sequences, medical reports are very sensitive and private, yet medical data are difficult to collect and they exist in isolated medical centers and hospitals. The insufficiency of data sources and the lack of labels have led to an unsatisfactory performance of machine learning models, which becomes the bottleneck of current smart healthcare. We envisage that if all medical institutions are united and share their data to form a large medical dataset, then the performance of machine learning models trained on that large medical dataset would be significantly improved. Federated learning combining with transfer learning is the main way to achieve this vision. Transfer learning could be applied to fill the missing labels thereby expanding the scale of the available data and further improving the performance of a trained model. Therefore, federated transfer learning would play a pivotal role in the development of smart healthcare and it may be able to take human health care to a whole new level

**Federated learning is not only a technology standard but also a business model. When people realize the effects of big data, the first thought that occurs to them is to aggregate the data together, compute the models through a remote processor and then download the results for further use.Cloud computing comes into being under such demands. However, with the increasing importance of data privacy and data security and a closer relationship between a company’s profits and its data, the cloud computing model has been challenged. However, the business model of federated learning has provided a new paradigm for applications of big data. When the isolated data occupied by each institution fails to produce an ideal model, the mechanism of federated learning makes it possible for institutions and enterprises to share a united model without data exchange. Furthermore, federated learning could make equitable rules for profits allocation with the help of consensus mechanism from blockchain techniques. The data possessors, regardless of the scale of data they have, will be**

**motivated to join in the data alliance and make their own profits. We believe that the establishment of the business model for data alliance and the technical mechanism for federated learning should be carried out together. We would also make standards for federated learning in various fields to put it into use as soon as possible.**

In recent years, the isolation of data and the emphasis on data privacy are becoming the next

challenges for artificial intelligence, but federated learning has brought us new hope. It could

establish a united model for multiple enterprises while the local data is protected, so that enterprises could win together taking the data security as premise. This article generally introduces the basic concept, architecture and techniques of federated learning, and discusses its potential in various applications. It is expected that in the near future, federated learning would break the barriers between industries and establish a community where data and knowledge could be shared together with safety, and the benefits would be fairly distributed according to the contribution of each participant. The bonus of artificial intelligence would finally be brought to every corner of our lives.

**What impact might this bring to the AI community?**

**Federated learning opens up a brand new research field in AI. Today, gigantic amounts of data are generated by consumer devices such as mobile phones on a daily basis. These data contain valuable information about users and their personal preferences: what websites they mostly visited, what social media apps they mostly used, what types of videos they mostly watched, etc. With such valuable information, these data become the key to building better and personalized machine learning models to deliver personalized services to maximally enhance user experiences. Federated learning provides a unique way to build such personalized models without intruding users’ privacy. Such a unique advantage is the key motivation to attract researchers in the AI community to work on this new research direction.**

**Federated learning also opens up a brand new computing paradigm for AI. As compute resources inside end devices such as mobile phones are becoming increasingly powerful, especially with the emergence of AI chipsets, AI is moving from clouds and datacenters to end devices. Federated learning provides a privacy-preserving mechanism to effectively leverage those decentralized compute resources inside end devices to train machine learning models. Considering that there are billions of mobile devices worldwide, the compute resources accumulated from those mobile devices are way beyond the reach of the largest datacenter in the world. In this sense, federated learning has the potential to disrupt cloud computing, the dominant computing paradigm today.**



**TensorFlow Federated will provide distributed machine learning for developers to train models across many mobile devices without data ever leaving those devices. Encryption provides an additional layer of privacy, and weights from models trained on mobile devices are shared with a central model for continuous learning.**