A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection

Qinbin Li[1], Zeyi Wen[2], Zhaomin Wu[1], Sixu Hu[1],
Naibo Wang[1], Yuan Li[1], Xu Liu[1], Bingsheng He[1]

[1]National University of Singapore
[2]The University of Western Australia
[1]{qinbin, zhaomin, sixuhu, naibowang, liyuan, liuxu, hebs}@comp.nus.edu.sg
[2]zeyi.wen@uwa.edu.au

Abstract

Federated learning has been a hot research topic in enabling the collaborative training of machine learning models among different organizations under the privacy restrictions. As researchers try to support more machine learning models with different privacy-preserving approaches, there is a requirement in developing systems and infrastructures to ease the development of various federated learning algorithms. Similar to deep learning systems such as PyTorch and TensorFlow that boost the development of deep learning, federated learning systems (FLSs) are equivalently important, and face challenges from various aspects such as effectiveness, efficiency, and privacy. In this survey, we conduct a comprehensive review on federated learning systems. To achieve smooth flow and guide future research, we introduce the definition of federated learning systems and analyze the system components. Moreover, we provide a thorough categorization for federated learning systems according to six different aspects, including data distribution, machine learning model, privacy mechanism, communication architecture, scale of federation and motivation of federation. The categorization can help the design of federated learning systems as shown in our case studies. By systematically summarizing the existing federated learning systems, we present the design factors, case studies, and future research opportunities.

1 Introduction

Many machine learning algorithms are data hungry, and in reality, data are dispersed over different organizations under the protection of privacy restrictions. Due to these factors, federated learning (FL) [129, 207, 85] has become a hot research topic in machine learning. For example, data of different hospitals are isolated and become "data islands". Since each data island has limitations in size and approximating real distributions, a single hospital may not be able to train a high-quality model that has a good predictive accuracy for a specific task. Ideally, hospitals can benefit more if they can collaboratively train a machine learning model on the union of their data. However, the data cannot simply be shared among the hospitals due to various policies and regulations. Such phenomena on "data islands" are commonly seen in many areas such as finance, government, and supply chains. Policies such as General Data Protection Regulation (GDPR) [10] stipulate rules on data sharing among different organizations. Thus, it is challenging to develop a federated learning system which has a good predictive accuracy while obeying policies and regulations to protect privacy.

Many efforts have recently been devoted to implementing federated learning algorithms to support effective machine learning models. Specifically, researchers try to support more machine learning models with different privacy-preserving approaches, including deep neural networks (NNs) [119, 213, 24, 158, 129], gradient boosted decision trees (GBDTs) [217, 38, 104], logistics regression [141, 36] and support vector machines (SVMs) [169]. For instance, Nikolaenko et al. [141] and Chen et al. [36] propose

联邦学习系统综述：数据隐私与保护的愿景、炒作与现实

Qinbin Li, Zeyi Wen , Zhaomin Wu , Sixu Hu , Naibo Wang , Yuan Li, Xu Liu, Bingsheng He
[1]新加坡大学
[2]西澳大利亚大学
[1]{qinbin , zhaomin , sixuhu , naibowang , liyuan , liuxu , hebs }@comp .nus .edu .sg
[2]zeyi .wen @uwa .edu .au

摘要

联邦学习是一个研究热点，它可以在隐私限制下实现不同组织之间的机器学习模型的协同训练。随着研究人员试图用不同的隐私保护方法支持更多的机器学习模型，开发系统和基础设施需要简化各种联邦学习算法的开发。与促进深度学习发展的PyTorch 和TensorFlow 等深度学习系统类似，联邦学习系统（FLS）同样重要，并面临来自有效性，效率和隐私等各个方面的挑战。在这次调查中，我们对联邦学习系统进行了全面的回顾。为了实现流畅的流程和指导未来的研究，我们介绍了联邦学习系统的定义和分析系统的组成部分。 此外，我们提供了一个完整的分类联邦学习系统根据六个不同的方面，包括数据分布，机器学习模型，隐私机制，通信架构，联邦规模和联邦的动机。正如我们的案例研究所示，分类可以帮助设计联邦学习系统。通过系统总结现有的联邦学习系统，我们提出了设计因素，案例研究，和未来的研究机会。

1引言

许多机器学习算法都是数据饥渴型的，实际上，数据在隐私限制的保护下分散在不同的组织中。由于这些因素，联邦学习（FL）[129，207，85]已成为机器学习中的热门研究课题。比如，不同医院的数据相互隔离，成为“ 数据孤岛” 。由于每个数据岛在大小和近似真实的分布方面都有限制，因此单个医院可能无法训练出针对特定任务具有良好预测准确性的高质量模型。理想情况下，如果医院能够在其数据的联合上协作训练机器学习模型，那么他们可以受益更多。然而，由于各种政策和法规，这些数据不能简单地在医院之间共享。这种“ 数据孤岛” 现象在金融、政府、供应链等多个领域都很常见。《通用数据保护条例》（GDPR）[10]等政策规定了不同组织之间数据共享的规则。因此，开发一个具有良好预测准确性，同时遵守政策和法规以保护隐私的联邦学习系统是具有挑战性的。

最近，许多努力致力于实现联邦学习算法，以支持有效的机器学习模型。具体来说，研究人员试图用不同的隐私保护方法支持更多的机器学习模型，包括深度神经网络（NN）[119，213，24，158，129]，梯度提升决策树（GBDTs）[217，38，104]，逻辑回归[141，36]和支持向量机（SVM）[169]。例如，Nikolaenko 等人[141]和Chen 等人[36]提出

approaches to conduct FL based on linear regression. Since GBDTs have become very successful in recent years [34, 200], the corresponding Federated Learning Systems (FLSs) have also been proposed by Zhao et al. [217], Cheng et al. [38], Li et al. [104]. Moreover, there are many FLSs supporting the training of NNs. Google proposes a scalable production system which enables tens of millions of devices to train a deep neural network [24].

As there are common methods and building blocks (e.g., privacy mechanisms such as differential privacy) for building FL algorithms, it makes sense to develop systems and infrastructures to ease the development of various FL algorithms. Systems and infrastructures allow algorithm developers to reuse the common building blocks, and avoid building algorithms every time from scratch. Similar to deep learning systems such as PyTorch [148, 149] and TensorFlow [7] that boost the development of deep learning algorithms, FLSs are equivalently important for the success of FL. However, building a successful FLS is challenging, which needs to consider multiple aspects such as effectiveness, efficiency, privacy, and autonomy.

In this paper, we take a survey on the existing FLSs from a system view. First, we show the definition of FLSs, and compare it with conventional federated systems. Second, we analyze the system components of FLSs, including the parties, the manager, and the computation-communication framework. Third, we categorize FLSs based on six different aspects: data distribution, machine learning model, privacy mechanism, communication architecture, scale of federation, and motivation of federation. These aspects can direct the design of an FLS as common building blocks and system abstractions. Fourth, based on these aspects, we systematically summarize the existing studies, which can be used to direct the design of FLSs. Last, to make FL more practical and powerful, we present future research directions to work on. We believe that systems and infrastructures are essential for the success of FL. More work has to be carried out to address the system research issues in effectiveness, efficiency, privacy, and autonomy.

1.1 Related Surveys

There have been several surveys on FL. A seminal survey written by Yang et al. [207] introduces the basics and concepts in FL, and further proposes a comprehensive secure FL framework. The paper mainly target at a relatively small number of parties which are typically enterprise data owners. Li et al. [109] summarize challenges and future directions of FL in massive networks of mobile and edge devices. Recently, Kairouz et al. [85] have a comprehensive description about the characteristics and challenges on FL from different research topics. However, they mainly focus on cross-device FL, where the participants are a very large number of mobile or IoT devices. More recently, another survey [11] summarizes the platforms, protocols and applications of federated learning. Some surveys only focus on an aspect of federated learning. For example, Lim et al. [113] conduct a survey of FL specific to mobile edge computing, while [125] focuses on the threats to federated learning.

1.2 Our Contribution

To the best of our knowledge, there lacks a survey on reviewing existing systems and infrastructure of FLSs and on boosting the attention of creating systems for FL (Similar to prosperous system research in deep learning). In comparison with the previous surveys, the main contributions of this paper are as follows. (1) Our survey is the first one to provide a comprehensive analysis on FL from a system's point of view, including system components, taxonomy, summary, design, and vision. (2) We provide a comprehensive taxonomy against FLSs on six different aspects, including data distribution, machine learning model, privacy mechanism, communication architecture, scale of federation, and motivation of federation, which can be used as common building blocks and system abstractions of FLSs. (3) We summarize existing typical and state-of-the-art studies according to their domains, which is convenient for researchers and developers to refer to. (4) We present the design factors for a successful FLS and comprehensively review solutions for each scenario. (5) We propose interesting research directions and challenges for future generations of FLSs.

[36]提出了基于线性回归的FL实施方法。由于GBDTs近年来已经非常成功[34，200]，因此Zhao 等人[217]，Cheng 等人[38]，L等人[104]也提出了相应的联邦学习系统（FLS）。此外，有许多FLS支持NN的训练。谷歌提出了一个可扩展的生产系统，使数千万台设备能够训练深度神经网络[24]。

由于存在常见的方法和构建块（例如，隐私机制，例如差分隐私），因此开发系统和基础设施以简化各种FL算法的开发是有意义的。系统和基础设施允许算法开发人员重用公共构建块，并避免每次从头开始构建算法。与PyTorch [148，149]和TensorFlow [7]等深度学习系统类似，FLS对FL的成功同样重要。然而，构建成功的FLS具有挑战性，需要考虑有效性，效率，隐私和自治等多个方面。

在本文中，我们采取了现有的FLS从系统的观点。首先，我们展示了FLS的定义，并将其与传统的联邦系统进行了比较。其次，我们分析了FLS的系统组件，包括当事人，管理者和计算通信框架。第三，我们根据六个不同的方面对FLS进行分类：数据分布，机器学习模型，隐私机制，通信架构，联邦规模和联邦动机。这些方面可以指导FLS的设计，作为公共构建块和系统抽象。第四，在此基础上，系统地总结了现有的研究成果，为今后的外语学习系统的设计提供指导。最后，为了使FL更加实用和强大，我们提出了未来的研究方向，我们认为系统和基础设施是FL成功的关键。 在有效性、效率、隐私性和自主性方面的系统研究问题还需要进行更多的工作。

1.1 相关调查

关于FL已经有几个调查。Yang等人撰写的开创性调查。[207]介绍了FL的基础知识和概念，并进一步提出了一个全面的安全FL框架。本文主要针对相对较少的方，这些方通常是企业数据所有者。L等人[109]总结了FL在移动的和边缘设备的大规模网络中的挑战和未来方向。最近，Kairouz 等人[85]从不同的研究主题对外语的特点和挑战进行了全面的描述。然而，它们主要关注跨设备FL，其中参与者是非常大量的移动的或IoT设备。最近，另一项调查[11]总结了联邦学习的平台，协议和应用。一些调查只关注联邦学习的一个方面。例如，Lim等人。[113]对特定于移动的边缘计算的FL进行了调查，而[125]则专注于联邦学习的威胁。

1.2 我们的贡献

据我们所知，缺乏对FLS现有系统和基础设施的审查以及对创建FL系统的关注（类似于深度学习中繁荣的系统研究）的调查。与以往的调查相比，本文的主要贡献如下。(1)我们的调查是第一个从系统的角度对外语进行全面分析的调查，包括系统组件、分类、摘要、设计和愿景。(2)本文从数据分布、机器学习模型、隐私机制、通信架构、联邦规模和联邦动机等六个方面对FLS进行了全面的分类，并将其作为FLS的通用构建块和系统抽象。(3)根据研究领域的不同，对已有的典型研究和最新研究成果进行了总结，以便于研究者和开发者参考。 (4)我们提出了一个成功的FLS的设计因素，并全面审查每个场景的解决方案。(5)我们提出了有趣的研究方向和未来几代FLS的挑战。

The rest of the paper is organized as follows. In Section 2, we introduce the concept and the system components of FLSs. In Section 3, we propose six aspects to classify FLSs. In Section 4, we summary existing studies and systems on FL. We then present the design factors and solutions for an FLS in Section 5. Last, we propose possible future directions on FL in Section 7 and conclude our paper in Section 8.

2 An Overview of Federated Learning Systems

2.1 Background

As data breach becomes a major concern, more and more governments establish regulations to protect users' data, such as GDPR in European Union [185], PDPA in Singapore [39], and CCPA [1] in the US. The cost of breaching these policies is pretty high for companies. In a breach of 600,000 drivers' personal information in 2016, Uber had to pay $148 million to settle the investigation [3]. SingHealth was fined $750,000 by the Singapore government for a breach of PDPA [5]. Google was fined $57 million for a breach of GDPR [4], which is the largest penalty as of March 18, 2020 under the European Union privacy law.

Under the above circumstances, federated learning, a collaborative learning without exchanging users' original data, has drawn increasingly attention nowadays. While machine learning, especially deep learning, has attracted many attentions again recently, the combination of federation and machine learning is emerging as a new and hot research topic.

2.2 Definition

FL enables multiple parties jointly train a machine learning model without exchanging the local data. It covers the techniques from multiple research areas such as distributed system, machine learning, and privacy. Inspired by the definition of FL given by other studies [85, 207], here we give a definition of FLSs.

In a federated learning system, multiple parties collaboratively train machine learning models without exchanging their raw data. The output of the system is a machine learning model for each party (which can be same or different). A practical federated learning system has the following constraint: given an evaluation metric such as test accuracy, the performance of the model learned by federated learning should be better than the model learned by local training with the same model architecture.

2.3 Compare with Conventional Federated Systems

The concept of federation can be found with its counterparts in the real world such as business and sports. The main characteristic of federation is cooperation. Federation not only commonly appears in society, but also plays an important role in computing. In computer science, federated computing systems have been an attractive area of research under different contexts.

Around 1990, there were many studies on federated database systems (FDBSs) [166]. An FDBS is a collection of autonomous databases cooperating for mutual benefits. As pointed out in a previous study [166], three important components of an FDBS are autonomy, heterogeneity, and distribution.

- *Autonomy*. A database system (DBS) that participates in an FDBS is autonomous, which means it is under separate and independent control. The parties can still manage the data without the FDBS.
- *Heterogeneity*. The database management systems can be different inside an FDBS. For example, the difference can lie in the data structures, query languages, system software requirements, and communication capabilities.
- *Distribution*. Due to the existence of multiple DBSs before an FDBS is built, the data distribution may differ in different DBSs. A data record can be horizontally or vertically partitioned into different DBSs, and can also be duplicated in multiple DBSs to increase the reliability.

本文的其余部分组织如下。在第二节中，我们介绍了FLS的概念和系统组成。在第三节中，我们提出了六个方面来分类FLS。在第4节中，我们总结了现有的研究和系统的FL。然后，我们提出了设计因素和解决方案的FLS在第5节。最后，我们在第7节提出了外语未来可能的发展方向，并在第8节总结了我们的论文。

2联邦学习系统概述

2.1 背景

随着数据泄露成为一个主要问题，越来越多的政府制定法规来保护用户的数据，例如欧盟的GDPR [185]，新加坡的PDPA [39]和美国的CCPA [1]。违反这些政策的成本对公司来说相当高。在2016 年60 万名司机的个人信息泄露事件中，Uber 不得不支付1.48 亿美元来解决调查[3]。SingHealth 因违反PDPA而被新加坡政府罚款75 万美元[5]。谷歌因违反GDPR被罚款5700 万美元[4]，这是截至2020 年3月18 日欧盟隐私法规定的最大罚单。

在这种情况下，联邦学习作为一种无需交换用户原始数据的协作学习方式，受到了越来越多的关注。近年来，机器学习，特别是深度学习再次引起了人们的关注，联邦与机器学习的结合正在成为一个新的研究热点。

2.2 定义

FL使多方能够联合训练机器学习模型，而无需交换本地数据。它涵盖了多个研究领域的技术，如分布式系统，机器学习和隐私。受其他研究[85，207]给出的FL定义的启发，本文给出了FLS的定义。

在联合学习系统中，多方协作训练机器学习模型，而无需交换原始数据。系统的输出是每一方的机器学习模型（可以相同或不同）。一个实际的联邦学习系统有以下约束：给定一个评估指标，如测试精度，联邦学习学习的模型的性能应该优于本地训练学习的模型具有相同的模型架构。

2.3 与传统联邦系统比较

联邦的概念可以在真实的世界中找到对应的东西，如商业和体育。联邦的主要特征是合作。联邦不仅在社会中普遍存在，而且在计算领域也扮演着重要的角色。在计算机科学中，联邦计算系统在不同的背景下一直是一个有吸引力的研究领域。

在1990 年左右，有许多关于联邦数据库系统（FDBS）的研究[166]。FDBS是一个自治数据库的集合，它们为了共同的利益而合作。正如以前的研究所指出的，FDBS的三个重要组成部分是自治性，异质性和分布性。

- 自治参与FDBS的数据库系统（DBS）是自治的，这意味着它处于单独和独立的控制之下。各方仍然可以在没有FDBS的情况下管理数据。
- 异源在FDBS中，数据库管理系统可以是不同的。例如，差异可能在于数据结构、查询语言、系统软件要求和通信能力。
- 分布由于在FDBS构建之前存在多个DBS，因此数据分布在不同的DBS中可能不同。数据记录可以水平或垂直地划分到不同的DBS中，并且也可以在多个DBS中复制以增加可靠性。

More recently, with the development of cloud computing, many studies have been done for federated cloud computing [97]. A federated cloud (FC) is the deployment and management of multiple external and internal cloud computing services. The concept of cloud federation enables further reduction of costs due to partial outsourcing to more cost-efficient regions. Resource migration and resource redundancy are two basic features of federated clouds [97]. First, resources may be transferred from one cloud provider to another. Migration enables the relocation of resources. Second, redundancy allows concurrent usage of similar service features in different domains. For example, the data can be partitioned and processed at different providers following the same computation logic. Overall, the scheduling of different resources is a key factor in the design of a federated cloud system.

There are some similarities and differences between FLSs and conventional federated systems. First, the concept of federation still applies. The common and basic idea is about the cooperation of multiple independent parties. Therefore, the perspective of considering heterogeneity and autonomy among the parties can still be applied to FLSs. Second, some factors in the design of distributed systems are still important for FLSs. For example, how the data are shared between the parties can influence the efficiency of the systems. For the differences, these federated systems have different emphasis on collaboration and constraints. While FDBSs focus on the management of distributed data and FCs focus on the scheduling of the resources, FLSs care more about the secure computation among multiple parties. FLSs induce new challenges such as the algorithm designs of the distributed training and the data protection under the privacy restrictions.

Figure 1 shows the number of papers in each year for these three research areas. Here we count the papers by searching keywords "federated database", "federated cloud", and "federated learning" in Google Scholar[1]. Although federated database was proposed 30 years ago, there are still about 400 papers that mentioned it in recent years. The popularity of federated cloud grows more quickly than federated database at the beginning, while it appears to decrease in recent years probably because cloud computing becomes more mature and the incentives of federation diminish. For FL, the number of related papers is increasing rapidly and has achieved about 4,400 last year. Nowadays, the "data island" phenomena are common and have increasingly become an important issue in machine learning. Also, there is a increasing privacy concern and social awareness from the general public. Thus, we expect the popularity of FL will keep increasing for at least five years until there may be mature FLSs.

2.4 System Components

There are three major components in an FLS: parties (e.g., clients), the manager (e.g., server), and the communication-computation framework to train the machine learning model.

2.4.1 Parties

In FLSs, the parties are the data owners and the beneficiaries of FL. They can be organizations or mobile devices, named cross-silo or cross-device settings [85], respectively. We consider the following properties of the parties that affect the design of FLSs.

First, what is the hardware capacity of the parties? The hardware capacity includes the computation power and storage. If the parties are mobile phones, the capacity is weak and the parties cannot perform much computation and train a large model. For example, Wang et al. [192] consider a resource constrained setting in FL. They design an objective to include the resource budget and proposed an algorithm to determine the rounds of local updates.

Second, what is the scale and stability of the parties? For organizations, the scale is relative small compared with the mobile devices. Also, the stability of the cross-silo setting is better than the cross-device setting. Thus, in the cross-silo setting, we can expect that every party can continuously conduct computation and communication tasks in the entire federated process, which is a common setting in many studies [104, 38, 169]. If the parties are mobile devices, the system has to handle possible issues such

[1] https://scholar.google.com/

最近，随着云计算的发展，许多研究已经完成了联合云计算[97]。联合云（FC）是对多个外部和内部云计算服务的部署和管理。云联合的概念可以进一步降低成本，因为部分外包给更具成本效益的地区。资源迁移和资源冗余是联合云的两个基本特征[97]。首先，资源可以从一个云提供商转移到另一个云提供商。迁移可实现资源的重新定位。第二，冗余允许在不同域中并发使用类似的服务功能。例如，数据可以在不同的提供程序中按照相同的计算逻辑进行分区和处理。总的来说，不同资源的调度是联邦云系统设计中的一个关键因素。

FLS和传统的联邦系统有一些相似之处和不同之处。首先，联邦的概念仍然适用。其共同和基本的思想是关于多个独立方的合作。因此，考虑各方异质性和自治性的视角仍然适用于FLS。其次，分布式系统设计中的一些因素对FLS仍然很重要。例如，各方之间如何共享数据可能会影响系统的效率。由于这些联邦系统的不同，它们对协作和约束的重视程度也不同。FDBS侧重于分布式数据的管理，FC侧重于资源的调度，FLS更关心多方之间的安全计算。FLS给分布式训练的算法设计和隐私限制下的数据保护带来了新的挑战。

图1显示了这三个研究领域每年的论文数量。在这里，我们通过在Google Scholar 中搜索关键词“ 联邦数据库” ，“ 联邦云” 和“ 联邦学习” 来统计论文。联邦数据库的提出已有30 多年的历史，但近几年来仍有近400 篇论文提及。联邦云的普及在一开始比联邦数据库增长得更快，但近年来似乎有所下降，可能是因为云计算变得更加成熟，联邦的激励机制减弱。对于FL来说，相关论文的数量正在迅速增加，去年已经达到了4,400 篇左右。如今，“ 数据孤岛” 现象普遍存在，并日益成为机器学习中的一个重要问题。此外，公众对隐私的关注和社会意识也越来越强。因此，我们预计在未来至少五年内，外语学习的受欢迎程度将继续上升，直至有成熟的外语学习系统出现。

2.4 系统组件

财务和后勤系统有三个主要组成部分：缔约方（例如，客户端），管理器（例如，服务器），以及用于训练机器学习模型的通信计算框架。

2.4.1 缔约方

在FLS中，各方是数据所有者和FL的受益者。它们可以是组织或移动的设备，分别称为跨筒仓或跨设备设置[85]。我们考虑影响FLS设计的各方的以下属性。

一是各方硬件能力如何？硬件能力包括计算能力和存储能力。如果参与方是移动的电话，则能力较弱，并且参与方不能执行大量计算并训练大型模型。例如，Wang 等人。[192]考虑FL中的资源受限设置。他们设计了一个包含资源预算的目标，并提出了一种算法来确定局部更新的轮次。

第二，各方的规模和稳定性如何？对于组织来说，与移动的设备相比，规模相对较小。此外，跨思洛存储器设置的稳定性优于跨设备设置。因此，在跨筒仓设置中，我们可以预期每一方都可以在整个联邦过程中持续进行计算和通信任务，这是许多研究中的常见设置[104，38，169]。如果参与方是移动的设备，则系统必须处理可能的问题，

[1] https ://scholar .google .com /

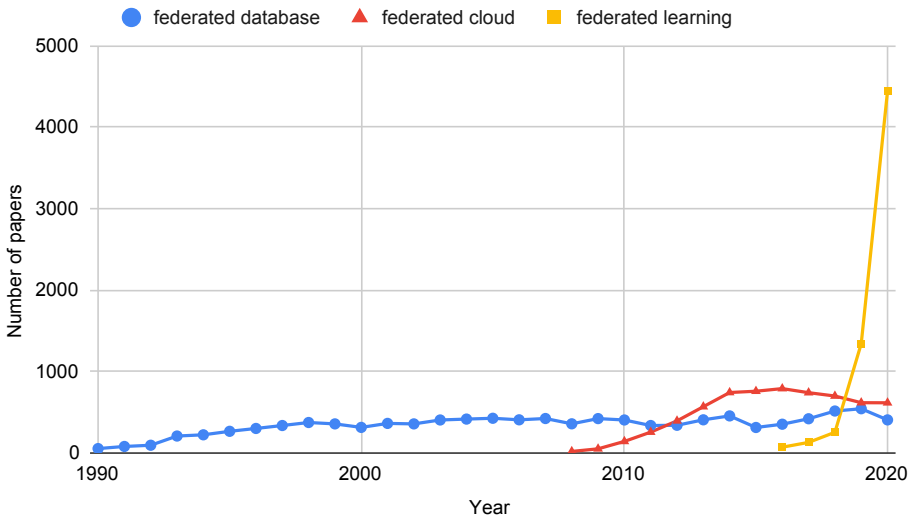


Figure 1: The number of related papers on "federated database", "federated cloud", and "federated learning"

as connection lost [24]. Moreover, since the number of devices can be very large (e.g., millions), it is unpractical to assume all the devices to participate every round in FL. The widely used setting is to choose a fraction of devices to perform computation in each round [129, 24].

Last, what are the data distributions among the parties? Usually, no matter cross-device or cross-silo setting, the non-IID (identically and independently distributed) data distribution is considered a practical and challenging setting in federated learning [85], which is evaluated in the experiments of recent work [104, 213, 111, 189]. Such non-IID data distribution may be more obvious among the organizations. For example, a bank and an insurance company can conduct FL to improve their predictions (e.g., whether a person can repay the loan and whether the person will buy the insurance products), while even the features can vary a lot in these organizations. Techniques in transfer learning [147], meta-learning [55], and multi-task learning [157] may be useful to combine the knowledge of various kinds of parties.

2.4.2 Manager

In the cross-device setting, the manager is usually a powerful central server. It conducts the training of the global machine learning model and manages the communication between the parties and the server. The stability and reliability of the server are quite important. Once the server fails to provide the accurate computation results, the FLS may produce a bad model. To address these potential issues, blockchain [176] may be a possible technique to offer a decentralized solution in order to increase the system reliability. For example, Kim et al. [93] leverage the blockchain in lieu of the central server in their system, where the blockchain enables exchanging the devices' updates and providing rewards to them.

In the cross-silo setting, since the organizations are expected to have powerful machines, the manager can also be one of the organizations who dominates the FL process. This is particularly used in the vertical FL [207], which we will introduce in Section 3.1 in detail. In a vertical FL setting by Liu et al. [119], the features of data are vertically partitioned across the parties and only one party has the labels. The party that owns the labels is naturally considered as the FL manager.

One challenge can be that it is hard to find a trusted server or party as the manager, especially in the cross-silo setting. Then, a fully-decentralized setting can be a good choice, where the parties communicate with each other directly and almost equally contribute to the global machine learning model training. These parties jointly set a FL task and deploy the FLS. Li et al. [104] propose a federated gradient

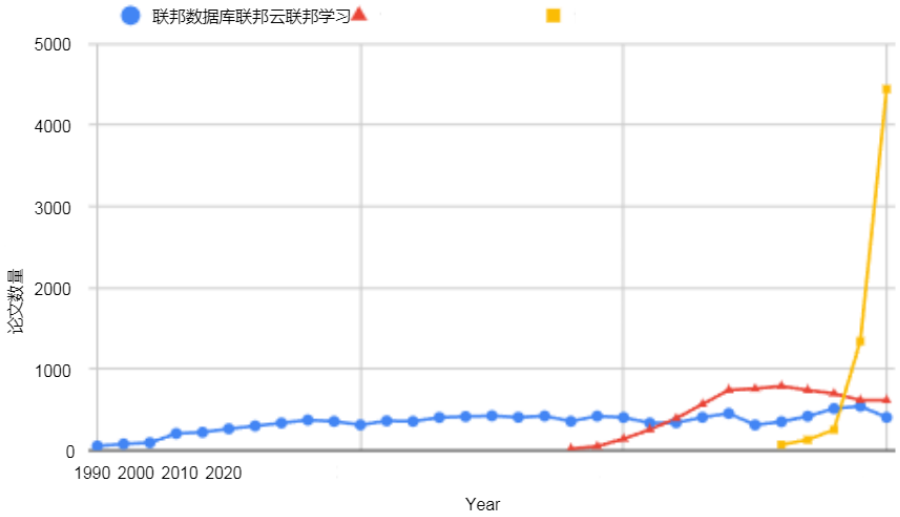


图1：关于“联邦数据库”、“联邦云”和“联邦学习”的相关论文数量

失去联系[24]。此外，由于设备的数量可能非常大（例如，数百万），假设所有设备都参与FL中的每一轮是不切实际的。广泛使用的设置是选择一小部分设备在每一轮中执行计算[129，24]。

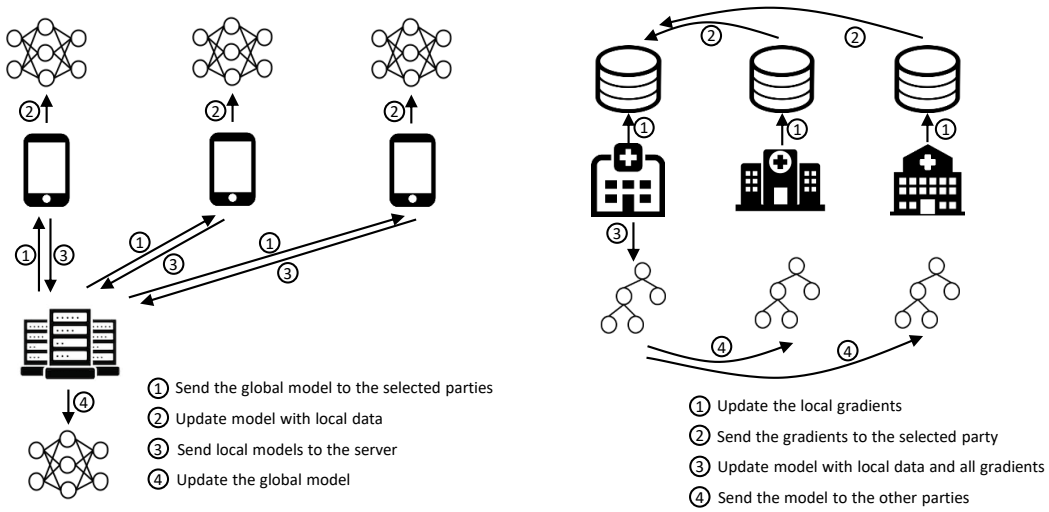
最后，各方之间的数据分布情况如何？通常，无论是跨设备还是跨筒仓设置，非IID（相同和独立分布）数据分布都被认为是联邦学习中实用且具有挑战性的设置[85]，在最近的工作[104，213，111，189]的实验中进行了评估。这种非IID数据分布在各组织中可能更为明显。例如，银行和保险公司可以进行FL以改进其预测（例如，一个人是否能够偿还贷款，以及这个人是否会购买保险产品），而在这些组织中，甚至特征也可以有很大不同。迁移学习[147]、元学习[55]和多任务学习[157]中的技术可能有助于联合收割机组合各种参与方的知识。

2.4.2 管理者

在跨设备设置中，管理器通常是一个强大的中央服务器。它进行全局机器学习模型的训练，并管理各方与服务器之间的通信。服务器的稳定性和可靠性非常重要。一旦服务器不能提供准确的计算结果，FLS可能会产生一个坏的模型。为了解决这些潜在的问题，区块链[176]可能是一种提供去中心化解决方案以提高系统可靠性的可能技术。例如，Kim等人。[93]利用区块链代替他们系统中的中央服务器，区块链可以交换设备的更新并向它们提供奖励。

在跨筒仓设置中，由于组织被期望具有强大的机器，因此经理也可以是主导FL过程的组织之一。这特别用于垂直FL [207]，我们将在第3.1 节详细介绍。在Liu等人的垂直FL设置中。[119]，数据的特征在各方之间垂直分区，只有一方具有标签。拥有标签的一方自然被认为是FL经理。

一个挑战可能是很难找到一个受信任的服务器或一方作为管理器，特别是在跨竖井设置中。然后，完全去中心化的设置可能是一个很好的选择，其中各方直接相互通信，并且几乎平等地为全局机器学习模型训练做出贡献。这些当事方共同确定前线任务并部署前线登陆系统。L等人。[104]提出了一种联邦梯度



(a) FedAvg (b) SimFL

Figure 2: Federated learning frameworks

boosting decision trees framework, where each party trains decision trees sequentially and the final model is the combination of all trees. It is challenging to design a fully-decentralized FLS with reasonable communication overhead.

2.4.3 Communication-Computation Framework

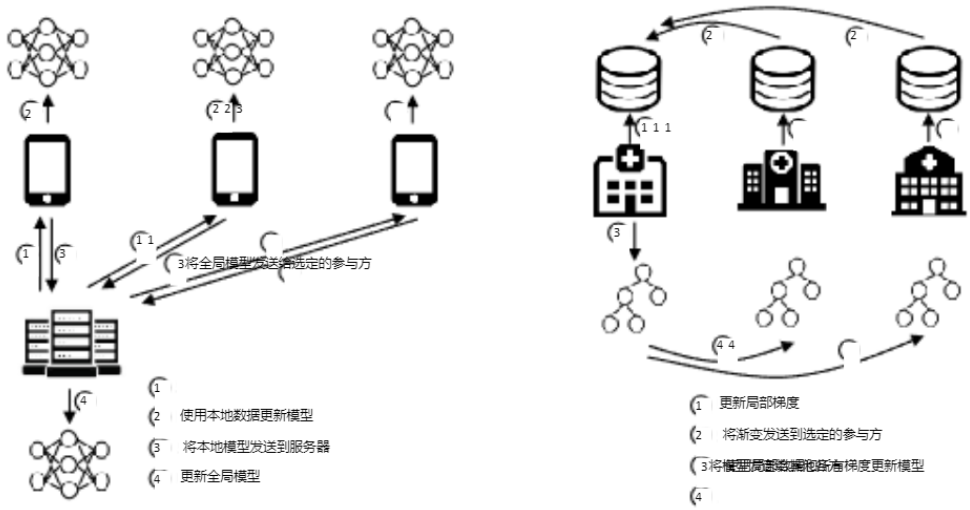
In FLSs, the computation happens on the parties and the manager, while the communication happens between the parties and the manager. Usually, the aim of the computation is for the model training and the aim of the communication is for exchanging the model parameters.

A basic and widely used framework is Federated Averaging (FedAvg) [129] proposed in 2016, as shown in Figure 2a. In each iteration, the server first sends the current global model to the selected parties. Then, the selected parties update the global model with their local data. Next, the updated models are sent back to the server. Last, the server averages all the received local models to get a new global model. FedAvg repeats the above process until reaching the specified number of iterations. The global model of the server is the final output.

While FedAvg is a centralized FL framework, SimFL, proposed by Li et al. [109], represents a decentralized FL framework. In SimFL, no trusted server is needed. In each iteration, the parties first update the gradients of their local data. Then, the gradients are sent to a selected party. Next, the selected party use its local data and the gradients to update the model. Last, the model is sent to all the other parties. To ensure fairness and utilize the data from different parties, every party is selected for updating the model for about the same number of rounds. SimFL repeats a specified number of iterations and outputs the final model.

3 Taxonomy

Considering the common system abstractions and building blocks for different FLSs, we classify FLSs by six aspects: data partitioning, machine learning model, privacy mechanism, communication architecture, scale of federation, and motivation of federation. These aspects include common factors (e.g., data partitioning, communication architecture) in previous FLSs [166, 97] and unique consideration (e.g., machine learning model and privacy mechanism) for FLSs. Furthermore, these aspects can be used to guide the design of FLSs. Figure 3 shows the summary of the taxonomy of FLSs.



(a)FedAvg (b)SimFL

图2：联邦学习框架

[104]提出了一个联合梯度提升决策树框架，其中每一方顺序训练决策树，最终模型是所有树的组合。设计具有合理通信开销的完全分散的FLS是具有挑战性的。

2.4.3 通信-计算框架

在FLS中，计算发生在参与方和管理者身上，而通信发生在参与方和管理者之间。通常，计算的目的是为了模型训练，而通信的目的是为了交换模型参数。

一个基本且广泛使用的框架是2016 年提出的联邦平均（FedAvg ）[129]，如图2a 所示。在每次迭代中，服务器首先将当前全局模型发送给选定的各方。然后，选定的各方使用其本地数据更新全局模型。接下来，更新的模型被发送回服务器。最后，服务器对所有接收到的局部模型进行平均以获得新的全局模型。FedAvg 重复上述过程，直到达到指定的迭代次数。服务器的全局模型是最终输出。

虽然FedAvg 是一个集中的FL框架，但L.等人提出的SimFL代表了一个分散的FL框架。在SimFL中，不需要可信服务器。在每次迭代中，各方首先更新其本地数据的梯度。然后，梯度被发送到选定的一方。接下来，选定方使用其本地数据和梯度来更新模型。最后，将模型发送给所有其他方。为了确保公平性并利用来自不同方的数据，选择每一方对模型进行大约相同轮数的更新。SimFL重复指定次数的迭代并输出最终模型。

3分类学

考虑到不同FLS的共同系统抽象和构建块，我们从六个方面对FLS进行分类：数据划分，机器学习模型，隐私机制，通信架构，联邦规模和联邦动机。这些方面包括共同因素（例如，数据划分，通信体系结构）在以前的FLS [166，97]和独特的考虑（例如，机器学习模型和隐私机制）。此外，这些方面可以用来指导FLSS的设计。图3 显示了FLS分类的总结。

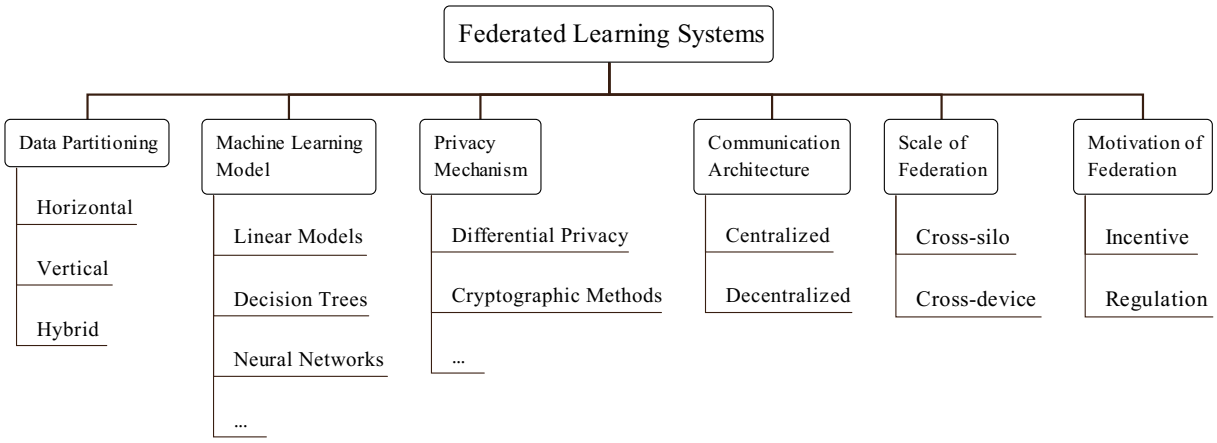


Figure 3: Taxonomy of federated learning systems

In Table 1 of [85], they consider different characteristics to distinguish distributed learning, cross-device federated learning, and cross-silo federated learning, including setting, data distribution, communication, etc. Our taxonomy is used to distinguish different federated learning systems from a deployment view, and aspects like machine learning models and motivation of federation are not considered in [85].

3.1 Data Partitioning

Based on how data are distributed over the sample and feature spaces, FLSs can be typically categorized in horizontal, vertical, and hybrid FLSs [207].

In horizontal FL, the datasets of different parties have the same feature space but little intersection on the sample space. This is a natural data partitioning especially for the cross-device setting, where different users try to improve their model performance on the same task using FL. Also, the majority of FL studies adopt horizontal partitioning. Since the local data are in the same feature space, the parties can train the local models using their local data with the same model architecture. The global model can simply be updated by averaging all the local models. A basic and popular framework of horizontal federated learning is FedAvg, as shown in Figure 2. Wake-word recognition [98], such as 'Hey Siri' and 'OK Google', is a typical application of horizontal partition because each user speaks the same sentence with a different voice.

In vertical FL, the datasets of different parties have the same or similar sample space but differ in the feature space. For the vertical FLS, it usually adopts *entity alignment* techniques [206, 41] to collect the overlapped samples of the parties. Then the overlapped data are used to train the machine learning model using encryption methods. Cheng et al. [38] propose a lossless vertical FLS to enable parties to collaboratively train gradient boosting decision trees. They use privacy-preserving entity alignment to find common users among two parties, whose gradients are used to jointly train the decision trees. Cooperation among different companies usually can be treated as a situation of vertical partition.

In many other applications, while existing FLSs mostly focus on one kind of partition, the partition of data among the parties may be a hybrid of horizontal partition and vertical partition. Let us take cancer diagnosis system as an example. A group of hospitals wants to build an FLS for cancer diagnosis but each hospital has different patients as well as different kinds of medical examination results. Transfer learning [147] is a possible solution for such scenarios. Liu et al. [119] propose a secure federated transfer learning system which can learn a representation among the features of parties using common instances.

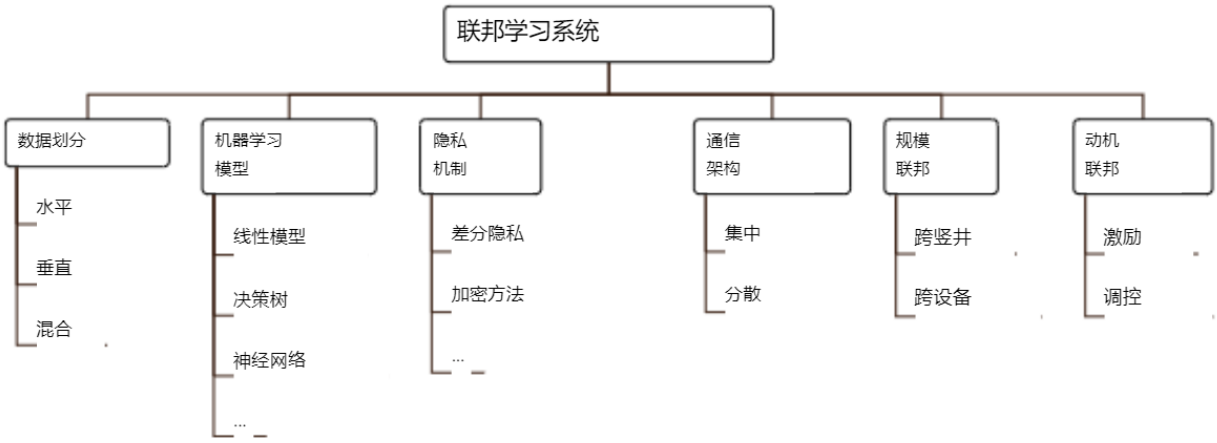


图3：联邦学习系统的分类

在[85]的表1中，他们考虑了不同的特征来区分分布式学习，跨设备联合学习和跨筒仓联合学习，包括设置，数据分布，通信等。我们的分类法用于从部署视图中区分不同的联合学习系统，[85]中没有考虑机器学习模型和联合动机等方面。

3.1 数据划分

根据数据在样本和特征空间中的分布方式，FLS通常可以分为水平、垂直和混合FLS [207]。

在水平FL中，不同方的数据集具有相同的特征空间，但在样本空间上几乎没有交集。这是一种自然的数据分区，特别是对于跨设备设置，其中不同的用户尝试使用FL在同一任务上提高其模型性能。此外，大多数FL研究采用水平分区。由于本地数据位于相同的特征空间中，因此各方可以使用具有相同模型架构的本地数据来训练本地模型。全局模型可以简单地通过平均所有局部模型来更新。水平联邦学习的一个基本和流行的框架是FedAvg ，如图2所示。唤醒词识别[98]，例如“ Hey Siri”和“ OK Google ”，是水平分区的典型应用，因为每个用户都用不同的声音说出相同的句子。

在垂直FL中，不同方的数据集具有相同或相似的样本空间，但在特征空间中不同。对于垂直FLS，它通常采用实体对齐技术[206，41]来收集各方的重叠样本。然后，重叠的数据被用来训练机器学习模型，使用加密方法。Cheng 等人[38]提出了一种无损垂直FLS，使各方能够协作训练梯度提升决策树。他们使用隐私保护实体对齐来找到双方之间的共同用户，其梯度用于联合训练决策树。不同公司之间的合作通常可以被视为一种垂直分割的情况。

在许多其他应用中，虽然现有的FLS主要集中在一种类型的分区上，但是各方之间的数据分区可以是水平分区和垂直分区的混合。让我们以癌症诊断系统为例。一组医院希望建立一个用于癌症诊断的FLS，但每家医院都有不同的患者以及不同的医疗检查结果。迁移学习[147]是这种情况下的一种可能的解决方案。Liu等人。[119]提出了一种安全的联邦迁移学习系统，可以使用公共实例学习各方特征之间的表示。

3.2 Machine Learning Models

Since FL is used to solve machine learning problems, the parties usually want to train a state-of-the-art machine learning model on a specified task. There have been many efforts in developing new models or reinventing current models to the federated setting. Here, we consider the widely-used models nowadays. The most popular machine learning model now is neural network (NN), which achieves state-of-the-art results in many tasks such as image classification and word prediction [96, 175]. There are many federated learning studies based on stochastic gradient descent [129, 189, 24], which can be used to train NNs.

Another widely used model is decision tree, which is highly efficient to train and easy to interpret compared with NNs. A tree-based FLS is designed for the federated training of single or multiple decision trees (e.g., gradient boosting decision trees (GBDTs) and random forests). GBDTs are especially popular recently and it has a very good performance in many classification and regression tasks. Li et al. [104] and Cheng et al. [38] propose FLSs for GBDTs on horizontally and vertically partitioned data, respectively.

Besides NNs and trees, linear models (e.g., linear regression, logistic regression, SVM) are classic and easy-to-use models. There are some well developed systems for linear regression and logistic regression [141, 72]. These linear models are easy to learn compared with other complex models (e.g., NNs).

While a single machine learning model may be weak, ensemble methods [150] such as stacking and voting can be applied in the federated setting. Each party trains a local model and sends it to the server, which aggregates all the models as an ensemble. The ensemble can directly be used for prediction by max voting or be used to train a meta-model by stacking. A benefit of federated ensemble learning is that each party can train heterogeneous models as there is no averaging of model parameters. As shown in previous studies [213, 103], federated ensemble learning can also achieve a good accuracy in a single communication round.

Currently, many FL frameworks [129, 94, 192, 108] are proposed based on stochastic gradient descent, which is a typical optimization algorithm for many models including neural networks and logistic regression. However, to increase the effectiveness of FL, we may have to exploit the model architecture [189]. Since the research of FL is still at an early stage, there is still a gap for FLSs to better support the state-of-the-art models.

3.3 Privacy Mechanisms

Although the local data are not exposed in FL, the exchanged model parameters may still leak sensitive information about the data. There have been many attacks against machine learning models [56, 167, 137, 131], such as model inversion attack [56] and membership inference attack [167], which can potentially infer the raw data by accessing to the model. Moreover, there are many privacy mechanisms such as differential privacy [48] and k-anonymity [50], which provide different privacy guarantees. The characteristics of existing privacy mechanisms are summarized in the survey [186]. Here we introduce two major approaches that are adopted in the current FLSs for data protection: cryptographic methods and differential privacy.

Cryptographic methods such as homomorphic encryption [15, 72, 28, 156, 116], and secure multi-party computation (SMC) [165, 32, 22, 23] are widely used in privacy-preserving machine learning algorithms. Basically, the parties have to encrypt their messages before sending, operate on the encrypted messages, and decrypt the encrypted output to get the final result. Applying the above methods, the user privacy of FLSs can usually be well protected [89, 211, 91, 144]. For example, SMC [63] guarantees that all the parties cannot learn anything except the output, which can be used to securely aggregate the transferred gradients. However, SMC does not provide privacy guarantees for the final model, which is still vulnerable to the inference attacks and model inversion attacks [167, 56]. Also, due to the additional encryption and decryption operations, such systems suffer from the extremely high computation overhead.

Differential privacy [48, 49] guarantees that one single record does not influence much on the output of a function. Many studies adopt differential privacy [31, 8, 105, 180, 220, 112] for data privacy protection to ensure the parties cannot know whether an individual record participates in the learning or not. By

3.2 机器学习模型

由于FL用于解决机器学习问题，因此各方通常希望在指定任务上训练最先进的机器学习模型。在开发新模型或将当前模型改造为联邦设置方面已经做了很多努力。在这里，我们考虑目前广泛使用的模型。现在最流行的机器学习模型是神经网络（NN），它在许多任务中实现了最先进的结果，如图像分类和单词预测[96，175]。有许多基于随机梯度下降的联邦学习研究[129，189，24]，可用于训练NN。

另一种广泛使用的模型是决策树，与NN相比，它具有训练效率高，易于解释的优点。基于树的FLS被设计用于单个或多个决策树的联合训练（例如，梯度提升决策树（GBDTs）和随机森林）。GBDTs是近年来比较流行的一种分类和回归算法，在许多分类和回归任务中表现出了很好的性能。L等人。[104]和Cheng 等人。[38]分别提出了水平和垂直分区数据上GBDTs的FLS。

除了NN和树之外，线性模型（例如，线性回归、逻辑回归、SVM）是经典且易于使用的模型。线性回归和逻辑回归有一些成熟的系统[141，72]。与其他复杂模型（例如，NN）。

虽然单个机器学习模型可能很弱，但集成方法[150]，如堆叠和投票可以应用于联合设置。每一方训练一个本地模型并将其发送到服务器，服务器将所有模型聚合为一个整体。集成可以直接用于通过最大投票进行预测，或者用于通过堆叠来训练元模型。联邦集成学习的一个好处是，每一方都可以训练异构模型，因为没有模型参数的平均值。如以前的研究所示[213，103]，联邦集成学习也可以在单次通信中实现良好的准确性。

目前，许多FL框架[129，94，192，108]都是基于随机梯度下降提出的，随机梯度下降是许多模型（包括神经网络和逻辑回归）的典型优化算法。然而，为了提高FL的有效性，我们可能必须利用模型架构[189]。由于外语学习的研究还处于起步阶段，外语学习系统要更好地支持最新的外语学习模型还存在一定的差距。

3.3 隐私机制

虽然本地数据没有暴露在FL中，但是交换的模型参数仍然可能泄漏关于数据的敏感信息。已经有许多针对机器学习模型的攻击[56，167，137，131]，例如模型反演攻击[56]和成员推断攻击[167]，它们可以通过访问模型来推断原始数据。此外，还有许多隐私机制，如差分隐私[48]和k-匿名[50]，它们提供不同的隐私保证。现有隐私机制的特征在调查中进行了总结[186]。在这里，我们介绍了两个主要的方法，采用在当前的FLS数据保护：加密方法和差分隐私。

同态加密[15，72，28，156，116]和安全多方计算（SMC）[165，32，22，23]等加密方法广泛用于隐私保护机器学习算法。基本上，各方必须在发送之前加密他们的消息，对加密的消息进行操作，并解密加密的输出以获得最终结果。应用上述方法，FLS的用户隐私通常可以得到很好的保护[89，211，91，144]。例如，SMC [63]保证除了输出之外，所有各方都无法学习任何东西，输出可用于安全地聚合传输的梯度。然而，SMC不为最终模型提供隐私保证，最终模型仍然容易受到推理攻击和模型反转攻击[167，56]。此外，由于附加的加密和解密操作，这样的系统遭受极高的计算开销。

差分隐私[48，49]保证了一个记录不会对函数的输出产生太大影响。许多研究采用差异隐私[31，8，105，180，220，112]进行数据隐私保护，以确保各方无法知道个人记录是否参与学习。通过

injecting random noises to the data or model parameters [8, 105, 170, 202], differential privacy provides statistical privacy guarantees for individual records and protection against the inference attack on the model. Due to the noises in the learning process, such systems tend to produce less accurate models.

Note that the above methods are independent of each other, and an FLS can adopt multiple methods to enhance the privacy guarantees [64, 205, 86]. There are also other approaches to protect the user privacy. An interesting hardware-based approach is to use trusted execution environment (TEE) such as Intel SGX processors [159, 145], which can guarantee that the code and data loaded inside are protected. Such environment can be used inside the central server to increase its credibility.

Related to privacy level, the threat models also vary in FLSs [125]. The attacks can come from any stage of the process of FL, including inputs, the learning process, and the learnt model.

- *Inputs* The malicious parties can conduct data poisoning attacks [35, 99, 12] on FL. For example, the parties can modify the labels of training samples with a specific class, so that the final model performs badly on this class.

- *Learning process* During the learning process, the parties can perform model poisoning attacks [16, 203] to upload designed model parameters. Like data poisoning attacks, the global model can have a very low accuracy due to the poisoned local updating. Besides model poisoning attacks, the Byzantine fault [27, 21, 173] is also a common issue in distributed learning, where the parties may behave arbitrarily badly and upload random updates.

- *The learnt model*. If the learnt model is published, the inference attacks [56, 167, 131, 137] can be conducted on it. The server can infer sensitive information about the training data from the exchanged model parameters. For example, membership inference attacks [167, 137] can infer whether a specific data record is used in the training. Note that the inference attacks may also be conducted in the learning process by the FL manager, who has access to the local updates of the parties.

3.4 Communication Architecture

There are two major ways of communication in FLSs: centralized design and decentralized design. In the centralized design, the data flow is often asymmetric, which means the manager aggregates the information (e.g., local models) from parties and sends back training results [24]. The parameter updates on the global model are always done in this manager. The communication between the manager and the local parties can be synchronous [129] or asynchronous [204, 171]. In a decentralized design, the communications are performed among the parties [217, 104] and every party is able to update the global parameters directly.

Google Keyboard [71] is a case of centralized architecture. The server collects local model updates from users' devices and trains a global model, which is sent back to the users for inference, as shown in Figure 2a. The scalability and stability are two important factors in the system design of the centralized FL.

While the centralized design is widely used in existing studies, the decentralized design is preferred at some aspects since concentrating information on one server may bring potential risks or unfairness. However, the design of the decentralized communication architecture is challenging, which should take fairness and communication overhead into consideration. There are currently three different decentralized designs: P2P [104, 217], graph [128] or blockchain [191, 219]. In a P2P design, the parties are equally privileged and treated during federated learning. An example is SimFL [104], where each party trains a tree sequentially and sends the tree to all the other parties. The communication architecture can also be modeled as a graph with the additional constrains such as latency and computation time. Marfoq et al. [128] propose an algorithm to find a throughput-optimal topology design. Recently, blockchain [223] is a popular decentralized platform for consideration. It can be used to store the information of parties in federated learning and ensure the transparency of federated learning [191].

通过向数据或模型参数注入随机噪声[8，105，170，202]，差分隐私为个人记录提供统计隐私保证，并保护模型免受推理攻击。由于学习过程中的噪声，这样的系统往往产生不太准确的模型。

请注意，上述方法相互独立，FLS可以采用多种方法来增强隐私保证[64，205，86]。还有其他方法来保护用户隐私。一个有趣的基于硬件的方法是使用可信执行环境（TEE），如英特尔SGX处理器[159，145]，它可以保证加载的代码和数据受到保护。这样的环境可以在中央服务器内部使用，以增加其可信度。

与隐私级别相关，FLS中的威胁模型也各不相同[125]。攻击可以来自FL过程的任何阶段，包括输入，学习过程和学习模型。

- 输入恶意方可以对FL进行数据中毒攻击[35，99，12]。例如，各方可以修改具有特定类别的训练样本的标签，因此最终模型在此类上表现不佳。

- 学习过程在学习过程中，各方可以执行模型中毒攻击[16，203]以上传设计的模型参数。与数据中毒攻击一样，全局模型由于中毒的局部更新而具有非常低的准确性。除了模型中毒攻击之外，拜占庭故障[27，21，173]也是分布式学习中的常见问题，其中各方可能表现得任意糟糕并上传随机更新。

- 学习模型。如果学习的模型被发布，则可以对其进行推理攻击[56，167，131，137]。服务器可以从交换的模型参数中推断出有关训练数据的敏感信息。例如，成员推断攻击[167，137]可以推断特定数据记录是否用于训练。注意，推断攻击也可以由FL管理器在学习过程中进行，FL管理器可以访问各方的本地更新。

3.4 通信架构

在FLS中有两种主要的通信方式：集中式设计和分散式设计。在集中式设计中，数据流通常是不对称的，这意味着管理员聚集信息（例如，地方模型），并发回培训结果[24]。全局模型上的参数更新始终在此管理器中完成。管理器和本地方之间的通信可以是同步的[129]或异步的[204，171]。在去中心化设计中，通信在各方之间进行[217，104]，并且每一方都能够直接更新全局参数。

Google Keyboard [71]是集中式架构的一个例子。服务器从用户的设备收集本地模型更新并训练全局模型，该全局模型被发送回用户以进行推理，如图2a 所示。可扩展性和稳定性是集中式FL系统设计的两个重要因素。

虽然集中式设计在现有的研究中被广泛使用，但分散式设计在某些方面更受欢迎，因为将信息集中在一台服务器上可能会带来潜在的风险或不公平。然而，分散式通信架构的设计是具有挑战性的，它需要考虑公平性和通信开销。目前有三种不同的去中心化设计：P2P [104，217]，图[128]或区块链[191，219]。在P2P 设计中，各方在联邦学习期间享有同等的特权和待遇。一个例子是SimFL [104]，其中每一方顺序地训练一棵树，并将树发送给所有其他方。通信架构也可以被建模为具有诸如延迟和计算时间之类的附加约束的图。Marfoq 等人。[128]提出了一种算法来找到吞吐量最优的拓扑设计。最近，区块链[223]是一个受欢迎的去中心化平台。 它可以用于存储联邦学习中各方的信息，并确保联邦学习的透明度[191]。

3.5 Scale of Federation

The FLSs can be categorized into two typical types by the scale of federation: cross-silo FLSs and cross-device FLSs [85]. The differences between them lie on the number of parties and the amount of data stored in each party.

In cross-silo FLS, the parties are organizations or data centers. There are usually a relatively small number of parties and each of them has a relatively large amount of data as well as computational power. For example, Amazon wants to recommend items for users by training the shopping data collected from hundreds of data centers around the world. Each data center possesses a huge amount of data as well as sufficient computational resources. Another example is that federated learning can be used among medical institutions. Different hospitals can use federated learning to train a CNN for chest radiography classification while keeping their chest X-ray images locally [86]. With federated learning, the accuracy of the model can be significantly improved. One challenge that such FLS faces is how to efficiently distribute computation to data centers under the constraint of privacy models [224].

In cross-device FLS, on the contrary, the number of parties is relatively large and each party has a relatively small amount of data as well as computational power. The parties are usually mobile devices. Google Keyboard [208] is an example of cross-device FLSs. The query suggestions of Google Keyboard can be improved with the help of FL. Due to the energy consumption concern, the devices cannot be asked to conduct complex training tasks. Under this occasion, the system should be powerful enough to manage a large number of parties and deal with possible issues such as the unstable connection between the device and the server.

3.6 Motivation of Federation

In real-world applications of FL, individual parties need the motivation to get involved in the FLS. The motivation can be regulations or incentives. FL inside a company or an organization is usually motivated by regulations (e.g., FL across different departments of a company). For example, the department which has the transaction records of users can help another department to predict user credit by federated learning. In many cases, parties cannot be forced to provide their data by regulations. However, parties that choose to participate in federated learning can benefit from it, e.g., higher model accuracy. For example, hospitals can conduct federated learning to train a machine learning model for chest radiography classification [86] or COVID-19 detection [152]. Then, the hospitals can get a good model which has a higher accuracy than human experts and the model trained locally without federation. Another example is Google Keyboard [208]. While users have the choice to prevent Google Keyboard from utilizing their data, those who agree to upload input data may enjoy a higher accuracy of word prediction. Users may be willing to participate in federated learning for their convenience.

A challenging problem is how to design a fair incentive mechanism, such that the party that contributes more can also benefit more from federated learning. There have been some successful cases for incentive designs in blockchain [228, 51]. The parties inside the system can be collaborators as well as competitors. Other incentive designs like [88, 87] are proposed to attract participants with high-quality data for FL. We expect game theory models [163, 84, 136] and their equilibrium designs should be revisited under the FLSs. Even in the case of Google Keyboard, the users need to be motivated to participate this collaborative learning process.

4 Summary of Existing Studies

In this section[2], we summarize and compare the existing studies on FLSs according to the aspects considered in Section 3.

[2]Last updated on December 7, 2021. We will periodically update this section to include the state-of-the-art and valuable FL studies. Please check out our latest version at this URL: https://arxiv.org/abs/1907.09693. Also, if you have any reference that you want to add into this survey, kindly drop Dr. Bingsheng He an email (hebs@comp.nus.edu.sg).

3.5 联邦规模

FLS可以根据联合的规模分为两种典型类型：跨竖井FLS和跨设备FLS [85]。它们之间的差异在于参与方的数量和存储在每个参与方中的数据量。

在跨思洛FLS中，参与方是组织或数据中心。通常有相对较少的参与方，并且每个参与方都有相对大量的数据和计算能力。例如，亚马逊希望通过训练从全球数百个数据中心收集的购物数据来为用户推荐商品。每个数据中心都拥有大量的数据和足够的计算资源。另一个例子是，联邦学习可以在医疗机构中使用。不同的医院可以使用联邦学习来训练CNN 进行胸部X射线摄影分类，同时将其胸部X射线图像保存在本地[86]。通过联邦学习，可以显著提高模型的准确性。这种FLS面临的一个挑战是如何在隐私模型的约束下有效地将计算分发到数据中心[224]。

相反，在跨设备FLS中，参与方的数量相对较大，并且每一方具有相对较小的数据量以及计算能力。参与方通常是移动的设备。Google Keyboard [208]是跨设备FLS的一个例子。Google Keyboard 的查询建议可以在FL的帮助下进行改进。由于能耗问题，无法要求设备执行复杂的训练任务。在这种情况下，系统应该足够强大，以管理大量的参与者，并处理可能出现的问题，例如设备和服务器之间的连接不稳定。

3.6 联邦的动机

在现实世界的FL应用中，个体需要动机来参与FLS。动机可以是法规或激励措施。公司或组织内部的FL通常是由法规（例如，公司不同部门的FL）。例如，拥有用户交易记录的部门可以通过联邦学习帮助其他部门预测用户信用。在许多情况下，法规不能强制当事方提供数据。然而，选择参与联合学习的各方可以从中受益，例如，更高的模型精度。例如，医院可以进行联合学习来训练机器学习模型，用于胸部X线摄影分类[86]或COVID-19 检测[152]。然后，医院可以得到一个很好的模型，具有更高的准确性比人类专家和本地训练的模型没有联邦。另一个例子是Google Keyboard [208]。 虽然用户可以选择阻止Google Keyboard 使用他们的数据，但同意上传输入数据的用户可能会享受更高的单词预测准确性。用户可能愿意参与联邦学习，以方便他们。

一个具有挑战性的问题是如何设计一个公平的激励机制，使得贡献更多的一方也可以从联邦学习中受益更多。在区块链中有一些成功的激励设计案例[228，51]。系统内的各方可以是合作者，也可以是竞争者。其他激励设计，如[88，87]，建议用高质量的FL数据吸引参与者。我们希望在FLS下重新审视博弈论模型[163，84，136]及其均衡设计。即使在谷歌键盘的情况下，用户也需要有动力参与这种协作学习过程。

4现有研究综述

在本节中，我们总结和比较现有的研究FLS根据第3节考虑的方面。

2最后更新于2021 年12 月7日。我们将定期更新本节，以包括最先进的和有价值的FL研究。请在此URL查看我们的最新版本：https ://arxiv .org /abs /1907.09693 。此外，如果您有任何参考资料，您想添加到这个调查，请给博士Bingsheng 何一个电子邮件（hebs @comp .nus .edu .sg ）.

4.1 Methodology

To discover the existing studies on FL, we search keyword "Federated Learning" in Google Scholar. Here we only consider the published studies in the computer science community.

Since the scale of federation and the motivation of federation are problem dependent, we do not compare the existing studies by these two aspects. For ease of presentation, we use "NN", "DT" and "LM" to denote neural networks, decision trees and linear models, respectively. Moreover, we use "CM" and "DP" to denote cryptographic methods and differential privacy, respectively. Note that the algorithms (e.g., federated stochastic gradient descent) in some studies can be used to learn many machine learning models (e.g., logistic regression and neural networks). Thus, in the "model implementation" column, we present the models implemented in the experiments of corresponding papers. Moreover, in the "main area" column, we indicate the major area that the papers study on.

4.2 Individual Studies

We summarize existing popular and state-of-the-art research work, as shown in Table 1. From Table 1, we have the following four key findings.

First, most of the existing studies consider a horizontal data partitioning. We conjecture a part of the reason is that the experimental studies and benchmarks in horizontal data partitioning are relatively ready than vertical data partitioning. However, vertical FL is also common in real world, especially between different organizations. Vertical FL can enable more collaboration between diverse parties. Thus, more efforts should be paid to vertical FL to fill the gap.

Second, most studies consider exchanging the raw model parameters without any privacy guarantees. This may not be right if more powerful attacks on machine learning models are discovered in the future. Currently, the mainstream methods to provide privacy guarantees are differential privacy and cryptographic methods (e.g., secure multi-party computation and homomorphic encryption). Differential privacy may influence the final model quality a lot. Moreover, the cryptographic methods bring much computation and communication overhead and may be the bottleneck of FLSs. We look forward to a cheap way with reasonable privacy guarantees to satisfy the regulations.

Third, the centralized design is the mainstream of current implementations. A trusted server is needed in their settings. However, it may be hard to find a trusted server especially in the cross-silo setting. One naive approach to remove the central server is that the parties share the model parameters with all the other parties and each party also maintains the same global model locally. This method bring more communication and computation cost compared with the centralized setting. More studies should be done for practical FL with the decentralized architecture.

Last, the main research directions (also the main challenge) of FL are to improve the effectiveness, efficiency, and privacy, which are also three important metrics to evaluate an FLS. Meanwhile, there are many other research topics on FL such as fairness and incentive mechanisms. Since FL is related to many research areas, we believe that FL will attract more researchers and we can see more interesting studies in the near future.

4.2.1 Effectiveness Improvement

While some algorithms are based on SGD, the other algorithms are specially designed for one or several kinds of model architectures. Thus, we classify them into SGD-based algorithms and model specialized algorithms accordingly.

SGD-Based

If we consider the local data on a party as a single batch, SGD can be easily implemented in a federated setting by performing a single batch gradient calculation each round (i.e., FedSGD [129]). However, such method may require a large number of communication rounds to converge. To reduce the number of communication rounds, FedAvg [129], as introduced in Section 2.3.3 and Figure 1a of the main paper,

4.1 方法

为了发现现有的研究，我们在谷歌学术搜索关键字“ 联邦学习” 。在这里，我们只考虑计算机科学界发表的研究。

由于联盟的规模和联盟的动机是问题依赖性的，我们没有从这两个方面来比较现有的研究。为了便于演示，我们使用“ NN ” ，“ DT” 和“ LM” 分别表示神经网络，决策树和线性模型。此外，我们使用“ CM” 和“ DP” 分别表示加密方法和差分隐私。注意，算法（例如，联合随机梯度下降）在某些研究中可用于学习许多机器学习模型（例如，逻辑回归和神经网络）。因此，在“ 模型实现” 一栏中，我们展示了在相应论文的实验中实现的模型。此外，在“ 主要领域” ，

列，我们指出了论文研究的主要领域。

4.2 个体研究

我们总结了现有的流行和最先进的研究工作，如表1所示。从表1中，我们有以下四个关键发现。

首先，大多数现有的研究考虑水平数据划分。我们推测部分原因是水平数据分区的实验研究和基准测试比垂直数据分区相对成熟。然而，纵向FL在真实的世界中也很常见，尤其是不同组织之间。垂直FL可以使各方之间进行更多的协作。因此，应加大垂直FL的力度，以填补差距。

其次，大多数研究考虑在没有任何隐私保证的情况下交换原始模型参数。
如果将来发现对机器学习模型的更强大的攻击，这可能是不正确的。目前，提供隐私保证的主流方法是差分隐私和密码方法（例如，安全多方计算和同态加密）。差异隐私可能会对最终模型的质量产生很大影响。此外，加密方法带来了大量的计算和通信开销，可能是FLS的瓶颈。我们期待着一个便宜的方式与合理的隐私保证，以满足规定。

第三，集中式设计是当前实现的主流。在他们的设置中需要一个受信任的服务器。但是，可能很难找到受信任的服务器，特别是在跨竖井设置中。移除中央服务器的一种简单方法是各方与所有其他各方共享模型参数，并且每一方还在本地维护相同的全局模型。与集中式设置相比，这种方式带来了更多的通信和计算开销。对于分散式结构下的实际FL，还需要做更多的研究。

最后，提高FLS的有效性、效率和隐私性是FLS的主要研究方向（也是主要挑战），这也是衡量FLS的三个重要指标。同时，外语学习的公平性、激励机制等方面也有许多研究课题。由于外语与许多研究领域相关，我们相信外语将吸引更多的研究者，在不久的将来，我们可以看到更多有趣的研究。

4.2.1 有效性改进

有些算法是基于SGD的，有些算法是针对一种或几种模型结构而设计的。因此，我们将它们分为基于SGD的算法和相应的模型专用算法。

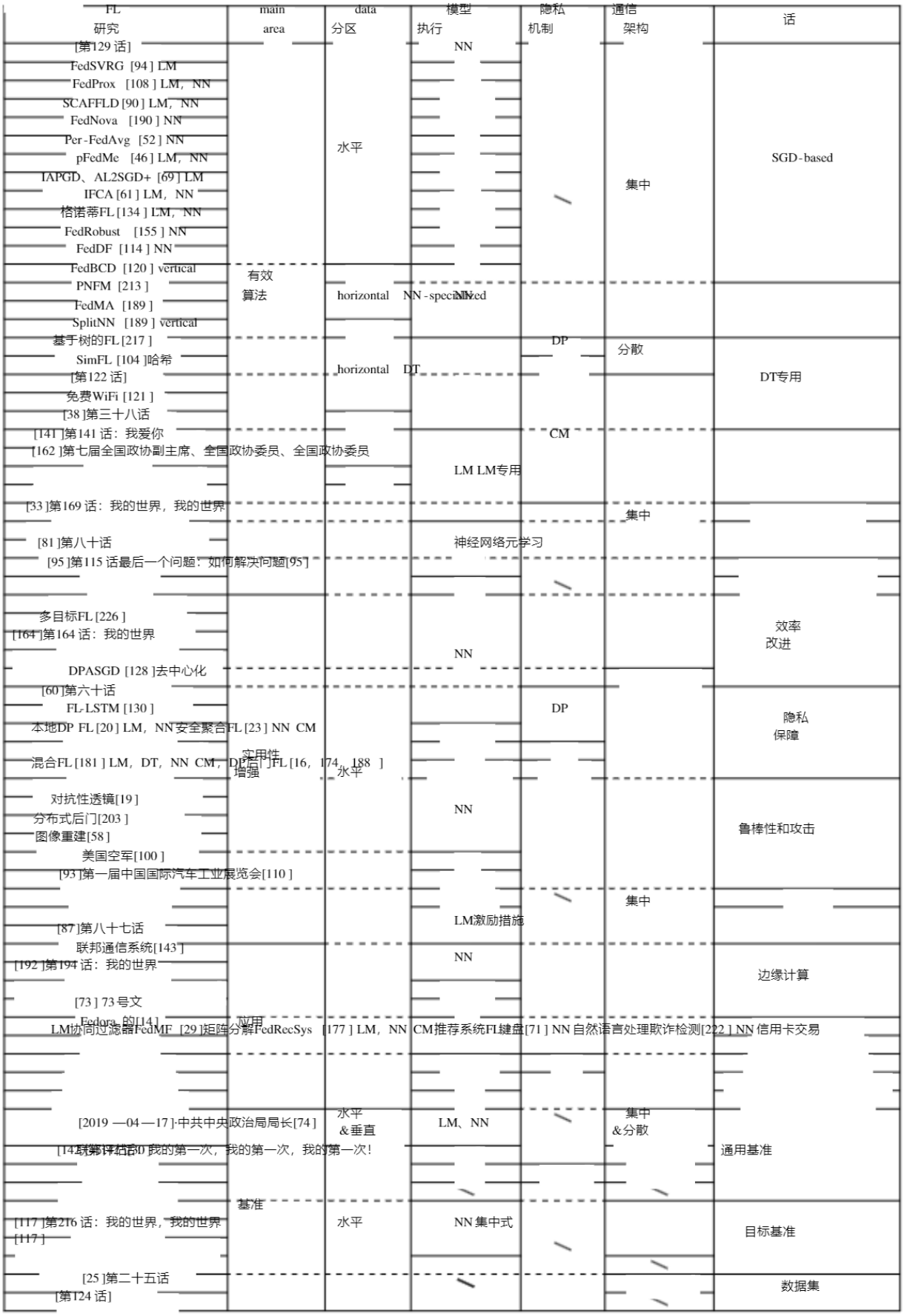
基于**SGD**

如果我们将一方的本地数据视为单个批次，则SGD可以通过每轮执行单个批次梯度计算（即，FedSGD [129]）。然而，这种方法可能需要大量的通信回合来收敛。为了减少沟通回合的数量，FedAvg [129]，如主论文的第2.3.3 节和图1a 所介绍的，

Table 1: Comparison among existing published studies. LM denotes Linear Models. DM denotes Decision Trees. NN denotes Neural Networks. CM denotes Cryptographic Methods. DP denotes Differential Privacy.

FL Studies	main area	data partitioning	model implementation	privacy mechanism	communication architecture	remark
FedAvg [129]	Effective Algorithms	horizontal	NN	⟍	centralized	SGD-based
FedSVRG [94]			LM			
FedProx [108]			LM, NN			
SCAFFOLD [90]			LM, NN			
FedNova [190]			NN			
Per-FedAvg [52]			NN			
pFedMe [46]			LM, NN			
IAPGD, AL2SGD+ [69]			LM			
IFCA [61]			LM, NN			
Agnostic FL [134]			LM, NN			
FedRobust [155]			NN			
FedDF [114]			NN			
FedBCD [120]		vertical				
PNFM [213]		horizontal	NN			NN-specialized
FedMA [189]						
SplitNN [189]		vertical				
Tree-based FL [217]		horizontal	DT	DP	decentralized	DT-specialized
SimFL [104]				hashing		
FedXGB [122]						
FedForest [121]						
SecureBoost [38]		vertical				
Ridge Regression FL [141]		horizontal	LM	CM		LM-specialized
PPRR [36]						
Linear Regression FL [162]		vertical				
Logistic Regression FL [72]						
Federated MTL [169]					centralized	multi-task learning
Federated Meta-Learning [33]			NN			meta-learning
Personalized FedAvg [81]						
LFRL [115]						reinforcement learning
FBO [44]			LM	⟍		Bayesian optimization
Structure Updates [95]	Practicality Enhancement	horizontal	NN			efficiency improvement
Multi-Objective FL [226]						
On-Device ML [79]						
Sparse Ternary Compression [164]						
DPASGD [128]					decentralized	
Client-Level DP FL [60]				DP		privacy guarantees
FL-LSTM [130]						
Local DP FL [20]			LM, NN			
Secure Aggregation FL [23]			NN	CM		
Hybrid FL [181]			LM, DT, NN	CM, DP		
Backdoor FL [16, 174, 188]			NN			robustness and attacks
Adversarial Lens [19]						
Distributed Backdoor [203]						
Image Reconstruction [58]						
RSA [100]			LM			
Model Poison [53]			LM, NN			
q-FedAvg [110]			LM, NN	⟍	centralized	fairness
BlockFL [93]			LM			incentives
Reputation FL [87]						
FedCS [143]	Applications		NN			edge computing
DRL-MEC [194]						
Resource-Constrained MEC [192]			LM, NN			
FedGKT [73]			NN			
FedCF [14]			LM			collaborative filter
FedMF [29]						matrix factorization
FedRecSys [177]			LM, NN	CM		recommender system
FL Keyboard [71]			NN			natural language processing
Fraud detection [222]			NN			credit card transaction
FedML [74]	Benchmarks	horizontal &vertical	LM, NN	⟍	centralized &decentralized	general purpose benchmarks
FedEval [30]		horizontal	NN		centralized	
OARF [77]			NN	CM,DP	centralized	
Edge AIBench [70]			⟍		⟍	
PerfEval [142]			NN	⟍	centralized	targeted benchmarks
FedReID [227]						
semi-supervised benchmark [216]						
non-IID benchmark [117]					⟍	
LEAF [25]			⟍		centralized	datasets
Street Dataset [124]					⟍	

表1：现有已发表研究的比较。LM表示线性模型。DM表示决策树。NN表示神经网络。CM表示加密方法。DP表示差分隐私。



is now a typical and practical FL framework based on SGD. In FedAvg, each party conducts multiple training rounds with SGD on its local model. Then, the weights of the global model are updated as the mean of weights of the local models. The global model is sent back to the parties to finish a global iteration. By averaging the weights, the local parties can take multiple steps of gradient descent on their local models, so that the number of communication rounds can be reduced compared with FedSGD.

Konečnỳ et al. [94] propose federated SVRG (FSVRG). The major difference between federated SVRG and federated averaging is the way to update parameters of the local model and global model (i.e., step 2 and step 4). The formulas to update the model weights are based on stochastic variance reduced gradient (SVRG) [82] and distributed approximate newton algorithm (DANE) in federated SVRG. They compare their algorithm with the other baselines like CoCoA+ [126] and simple distributed gradient descent. Their method can achieve better accuracy with the same communication rounds for the logistic regression model. There is no comparison between federated averaging and federated SVRG.

A key challenge in federated learning is the heterogeneity of local data (i.e., non-IID data) [106], which can degrade the performance of federated learning a lot [108, 90, 111]. Since the local models are updated towards their local optima, which are far from each other due to non-IID data, the averaged global model may also far from the global optima. To address the challenge, Li et al. [108] propose FedProx. Since too many local updates may lead the averaged model far from the global optima, FedProx introduces an additional proximal term in the local objective to limit the amount of local changes. Instead of directly limiting the size of local updates, SCAFFOLD [90] applies the variance reduction technique to correct the local updates. While FedProx and SCAFFOLD improve the local training stage of FedAvg, FedNova [190] improves the aggregation stage of FedAvg. It takes the heterogeneous local updates of each party into consideration and normalizes the local models according to the local updates before averaging.

The above studies' objective is to minimize the loss on the whole training dataset under the non-IID data setting. Another solution is to design personalized federated learning algorithms, where the aim is that each party learns a personalized model which can perform well on its local data. Per-FedAvg [52] applies the idea of model-agnostic meta-learning [55] framework in FedAvg. pFedMe [46] uses Moreau envelope to help decompose the personalized model optimization. Hanzely et al. [69] establish the lower bound for the communication complexity and local oracle complexity of the personalized federated learning optimization. Moreover, they apply accelerated proximal gradient descent (APGD) and accelerated L2SGD+ [68], which can achieve optimal complexity bound. IFCA [61] assumes that the parties are partitioned into clusters by the local objectives. The idea is to alternatively minimize the loss functions while estimating the cluster identities.

Another research direction related to the non-IID data setting is to design robust federated learning against possible combinations of the local distributions. Mohri et al. [134] propose a new framework named agnostic FL. Instead of minimizing the loss with respect to the average distribution among the data distributions from local clients, they try to train a centralized model optimized for any possible target distribution formed by a mixture of the client distributions. FedRobust [155] considers a structured affine distribution shifts. It proposes gradient descent ascent method to solve the distributed minimax optimization problem.

While the above studies consider the heterogeneity of data, the heterogeneity of the local models may also exist in federated learning. The parties can train models with different architectures. FedDF [114] utilizes knowledge distillation [75] to aggregate the local models. It assumes a public dataset exists on the server-side, which can be used to extract the knowledge of the local models and update the global model.

There are few studies on SGD-based vertical federated learning. [120] propose the Federated Stochastic Block Coordinate Descent (FedBCD) for vertical FL. By applying coordinate descent, each party updates its local parameter for multiple rounds before communicating the intermediate results. They also provide convergence analysis for FedBCD. Hu et al. [78] propose FDML for vertical FL assuming all parties have the labels. Instead of exchanging the intermediate results, it aggregates the local prediction from each of the participated party.

是一个典型的、实用的基于SGD的外语教学框架。在FedAvg 中，每一方都在其本地模型上与SGD进行多轮培训。然后，全局模型的权重被更新为局部模型的权重的平均值。全局模型被发送回各方以完成全局迭代。通过平均权重，本地各方可以在其本地模型上采取多个梯度下降步骤，从而与FedSGD 相比可以减少通信轮数。

Kone B.C. n `y等人[94]提出了联邦SVRG（FSVRG）。联合SVRG和联合平均之间的主要区别是更新局部模型和全局模型的参数的方式（即，步骤2和步骤4）。更新模型权重的公式基于随机方差约简梯度（SVRG）[82]和联邦SVRG中的分布式近似牛顿算法（DANE）。他们将其算法与其他基线（如可可+ [126]和简单分布式梯度下降）进行了比较。他们的方法可以在逻辑回归模型的相同通信轮次下实现更好的准确性。联邦平均和联邦SVRG之间没有比较。

联邦学习中的一个关键挑战是本地数据的异构性（即，非IID数据）[106]，这会大大降低联邦学习的性能[108，90，111]。由于局部模型朝向其局部最优值更新，由于非IID数据，局部最优值彼此远离，因此平均全局模型也可能远离全局最优值。为了应对这一挑战，L等人[108]提出了FedProx 。由于太多的局部更新可能会导致平均模型远离全局最优值，FedProx 在局部目标中引入了一个额外的近似项来限制局部变化的数量。SCAFFOLD [90]没有直接限制局部更新的大小，而是应用方差减小技术来校正局部更新。FedProx 和SCAFFOLD改进了FedAvg 的本地训练阶段，FedNova [190]改进了FedAvg 的聚合阶段。 该方法考虑了各参与方的异构局部更新，并在平均之前根据局部更新对局部模型进行归一化。

上述研究的目标是在非IID数据设置下最小化整个训练数据集的损失。另一种解决方案是设计个性化的联邦学习算法，其目标是每一方学习一个个性化的模型，该模型可以在其本地数据上表现良好。Per - FedAvg [52]在FedAvg 中应用了与模型无关的元学习[55]框架。pFedMe [46]使用Moreau 包络来帮助分解个性化模型优化。Hanzely 等人。[69]建立了个性化联邦学习优化的通信复杂度和本地Oracle 复杂度的下限。此外，他们应用了加速近端梯度下降（APGD）和加速L2 SGD + [68]，可以实现最佳复杂度界限。IFCA [61]假设各方根据当地目标划分为集群。我们的想法是交替最小化损失函数，同时估计集群身份。

与非IID数据设置相关的另一个研究方向是针对局部分布的可能组合设计鲁棒的联邦学习。Mohri 等人。[134]提出了一个名为不可知FL的新框架。他们试图训练一个集中式模型，该模型针对由客户端分布混合形成的任何可能的目标分布进行优化，而不是最小化本地客户端数据分布之间的平均分布的损失。FedRobust [155]考虑了结构化仿射分布移位。提出了梯度下降上升法来求解分布式极小极大优化问题。

虽然上述研究考虑了数据的异质性，但在联邦学习中也可能存在局部模型的异质性。各方可以用不同的架构训练模型。FedDF [114]利用知识蒸馏[75]来聚合本地模型。它假设服务器端存在一个公共数据集，可以用来提取本地模型的知识并更新全局模型。

基于SGD的垂直联邦学习的研究很少。[120 提出了垂直FL的联邦随机块坐标下降（FedBCD ）。通过应用坐标下降，每一方在交流中间结果之前更新其多轮局部参数。它们还提供了FedBCD 的收敛性分析。Hu 等人。[78]提出了垂直FL的FDML，假设所有各方都有标签。它不是交换中间结果，而是聚合来自每个参与方的本地预测。

Neural Networks

Although neural networks can be trained using the SGD optimizer, we can potentially increase the model utility if the model architecture can also be exploited. Yurochkin et al. [213] develop probabilistic federated neural matching (PFNM) for multilayer perceptrons by applying Bayesian nonparametric machinery [59]. They use an Beta-Bernoulli process informed matching procedure to combine the local models into a federated global model. The experiments show that their approach can outperform FedAvg on both IID and non-IID data partitioning.

Wang et al. [189] show how to apply PFNM to CNNs (convolutional neural networks) and LSTMs (long short-term memory networks). Moreover, they propose Federated Matched Averaging (FedMA) with a layer-wise matching scheme by exploting the model architecture. Specifically, they use matched averaging to update a layer of the global model each time, which also reduces the communication size. The experiments show that FedMA performs better than FedAvg and FedProx [108] on CNNs and LSTMs.

Another study for vertical federated learning on neural networks is split learning [184]. Vepakomma et al. [184] propose a novel paradigm named SplitNN, where a neural network is divided into two parts. Each participated party just need to train a few layers of the network, then the output at the cut layer are transmitted to the party who has label and completes the rest of the training.

Trees

Besides neural networks, decision trees are also widely used in the academic and industry [34, 92, 54, 105]. Compared with NNs, the training and inference of trees are highly efficient. However, the tree parameters cannot be directly optimized by SGD, which means that SGD-based FL frameworks are not applicable to learn trees. We need specialized frameworks for trees. Among the tree models, the Gradient Boosting Decision Tree (GBDT) model [34] is quite popular. There are several studies on federated GBDT.

There are some studies on horizontal federated GBDTs. Zhao et al. [217] propose the first FLS for GBDTs. In their framework, each decision tree is trained locally without the communications between parties. The trees trained in a party are sent to the next party to continuous train a number of trees. Differential privacy is used to protect the decision trees. Li et al. [104] exploit similarity information in the building of federated GBDTs by using locality-sensitive hashing [45]. They utilize the data distribution of local parties by aggregating gradients of similar instances. Within a weaker privacy model compared with secure multi-party computation, their approach is effective and efficient. Liu et al. [122] propose a federated extreme boosting learning framework for mobile crowdsensing. They adopted secret sharing to achieve privacy-preserving learning of GBDTs.

Liu et al. [121] propose Federated Forest, which enables training random forests in the vertical FL setting. In the building of each node, the party with the corresponding split feature is responsible for splitting the samples and sharing the results. They encrypt the communicated data to protect privacy. Their approach is as accurate as the non-federated version.

Cheng et al. [38] propose SecureBoost, a framework for GBDTs in the vertical FL setting. In their assumption, only one party has the label information. They used the entity alignment technique to get the common data and then build the decision trees. Additively homomorphic encryption is used to protect the gradients.

Linear/Logistic Regression

Linear/logistic regression can be achieved using SGD. Here we show the studies that are not SGD-based and specially designed for linear/logistic regression.

In the horizontal FL setting, Nikolaenko et al. [141] propose a system for privacy-preserving ridge regression. Their approaches combine both homomorphic encryption and Yao's garbled circuit to achieve privacy requirements. An extra evaluator is needed to run the algorithm. Chen et al. [36] propose a system for privacy-preserving ridge regression. Their approaches combine both secure summation and homomorphic encryption to achieve privacy requirements. They provided a complete communication and computation overhead comparison among their approach and the previous state-of-the-art approaches.

神经网络

虽然神经网络可以使用SGD优化器进行训练，但如果模型架构也可以利用，我们可以潜在地提高模型的实用性。Yurochkin 等人。[213]通过应用贝叶斯非参数机制[59]为多层感知器开发了概率联邦神经匹配（PFNM ）。它们使用Beta -Bernoulli 过程通知匹配过程来将局部模型联合收割机组合成联合全局模型。实验表明，他们的方法可以优于FedAvg IID和非IID数据分区。

Wang 等人。[189]展示了如何将PFNM 应用于CNN （卷积神经网络）和LSTM（长短期记忆网络）。此外，他们提出了联邦匹配平均（FedMA ）与逐层匹配计划，通过开发模型架构。具体来说，他们使用匹配平均来每次更新全局模型的一层，这也减少了通信大小。实验表明，FedMA 在CNN 和LSTM上的表现优于FedAvg 和FedProx [108]。

另一项关于神经网络垂直联邦学习的研究是分裂学习[184]。Vepakomma 等人。[184]提出了一种名为SplitNN 的新范式，其中神经网络分为两部分。每个参与方只需要训练网络的几层，然后将切割层的输出传输给具有标签的一方，并完成其余的训练。

树木

除了神经网络，决策树也广泛应用于学术和工业[34，92，54，105]。与神经网络相比，树的训练和推理效率很高。然而，树参数不能直接由SGD优化，这意味着基于SGD的FL框架不适用于学习树。我们需要专门的树框架。在树模型中，梯度提升决策树（GBDT）模型[34]非常流行。有几项关于联邦GBDT的研究。

有一些关于水平联邦GBDTs的研究。Zhao 等人[217]提出了GBDTs的第一个FLS。在他们的框架中，每个决策树都是在本地训练的，没有各方之间的通信。在一个团队中训练的树被发送到下一个团队，以连续训练多棵树。差分隐私被用来保护决策树。L等人。[104]通过使用位置敏感哈希[45]在构建联邦GBDTs时利用相似性信息。它们通过聚合相似实例的梯度来利用本地各方的数据分布。在一个较弱的隐私模型与安全多方计算相比，他们的方法是有效的和高效的。Liu等人。[122]提出了一种用于移动的人群感知的联合极端提升学习框架。他们采用秘密共享来实现GBDTs的隐私保护学习。

Liu等人。[121]提出了联邦森林，它可以在垂直FL设置中训练随机森林。在每个节点的构建中，具有相应拆分特征的一方负责拆分样本并共享结果。他们加密通信数据以保护隐私。

他们的方法和非联邦版本一样准确。
Cheng 等人。[38]提出了SecureBoost ，这是垂直FL设置中GBDTs的框架。在他们的假设中，只有一方拥有标签信息。他们使用实体对齐技术来获取公共数据，然后构建决策树。加性同态加密用于保护梯度。

线性/逻辑回归

可以使用SGD实现线性/逻辑回归。在这里，我们展示了不是基于SGD的研究，而是专门为线性/逻辑回归设计的研究。

在水平FL设置中，Nikolaenko 等人。[141]提出了一种隐私保护岭回归系统。他们的方法结合了联合收割机和同态加密和姚的乱码电路来实现隐私要求。需要一个额外的计算器来运行算法。Chen 等人。[36]提出了一个保护隐私的岭回归系统。他们的方法结合了联合收割机安全求和和同态加密，以实现隐私要求。他们提供了一个完整的通信和计算开销之间的比较，他们的方法和以前的国家的最先进的方法。

In the vertical FL setting, Sanil et al. [162] present a secure regression model. They focus on the linear regression model and secret sharing is applied to ensure privacy in their solution. Hardy et al. [72] present a solution for two-party vertical federated logistic regression. They apply entity resolution and additively homomorphic encryption.

Others

There are many studies that combine FL with other machine learning techniques such as multi-task learning [157], meta-learning [55], reinforcement learning [133], and transfer learning [147].

Smith et al. [169] combine FL with multi-task learning [26, 215]. Their method considers the issues of high communication cost, stragglers, and fault tolerance for MTL in the federated environment. Corinzia and Buhmann [43] propose a federated MTL method with non-convex models. They treated the central server and the local parties as a Bayesian network and the inference is performed using variational methods.

Chen et al. [33] adopt meta-learning in the learning process of FedAvg. Instead of training the local NNs and exchanging the model parameters, the parties adopt the Model-Agnostic Meta-Learning (MAML) [55] algorithm in the local training and exchange the gradients of MAML. Jiang et al. [81] interpret FedAvg in the light of existing MAML algorithms. Furthermore, they apply Reptile algorithm [139] to fine-tune the global model trained by FedAvg. Their experiments show that the meta-learning algorithm can improve the effectiveness of the global model.

Liu et al. [115] propose a lifelong federated reinforcement learning framework. Adopting transfer learning techniques, a global model is trained to effectively remember what the robots have learned in reinforcement learning.

Dai et al. [44] considers Bayesian optimization in FL. They propose federated Thompson sampling to address the communication efficiency and heterogeneity of the clients. Their approach can potentially be used in the parameter search in federated learning.

Another issue in FL is the package loss or party disconnection during FL process, which usually happens on mobile devices. When the number of failed messages is small, the server can simply ignore them as they have a small weight on the updating of the global model. If the party failure is significant, the server can restart from the results of the previous round [24]. We look forward to more novel solutions to deal with the disconnection issue for effectiveness improvement.

Summary

We summarize the above studies as follows.

- As the SGD-based framework has been widely studied and used, more studies focus on model specialized FL recently. We expect to achieve better model accuracy by using model specialized methods. Moreover, we encourage researchers to study on federated decision trees models. The tree models have a small model size and are easy to train compared with neural networks, which can result in a low communication and computation overhead in FL.

- The study on FL is still on a early stage. Few studies have been done on appling FL to train the state-of-the-art neural networks such as ResNeXt [127] and EfficientNet [178]. How to design an effective and practical algorithm to train a complex machine learning model is still a challenging and on-going research direction.

- While most studies focus on horizontal FL, there is still no well developed algorithm for vertical FL. However, the vertical federated setting is common in real world applications where multiple organizations are involved. We look forward to more studies on this promising area.

在垂直FL设置中，Sanil 等人[162]提出了一种安全的回归模型。他们专注于线性回归模型，并在解决方案中应用秘密共享来确保隐私。哈代等人。[72]提出了一种两方垂直联邦逻辑回归的解决方案。它们应用实体解析和加法同态加密。

别人

有许多研究将联合收割机FL与其他机器学习技术相结合，如多任务学习[157]，元学习[55]，强化学习[133]和迁移学习[147]。

Smith 等人。[169]将联合收割机FL与多任务学习结合起来[26，215]。他们的方法考虑了联邦环境中MTL的高通信成本、落伍者和容错问题。Corinzia 和Buhmann [43]提出了一种具有非凸模型的联邦MTL方法。他们将中央服务器和本地方视为贝叶斯网络，并使用变分方法进行推理。

Chen 等人[33]在FedAvg 的学习过程中采用了元学习。双方在本地训练中采用模型不可知元学习（MAML）[55]算法，并交换MAML的梯度，而不是训练本地NN 和交换模型参数。Jiang 等人。[81]根据现有的MAML算法解释FedAvg 。此外，他们应用Reptile 算法[139]来微调FedAvg 训练的全局模型。他们的实验表明，元学习算法可以提高全局模型的有效性。

Liu等人[115]提出了一个终身联邦强化学习框架。采用迁移学习技术，训练一个全局模型，以有效地记住机器人在强化学习中学到的东西。

Dai等人。[44]考虑了FL中的贝叶斯优化。他们提出联邦汤普森采样来解决客户端的通信效率和异质性。他们的方法可以潜在地用于联邦学习中的参数搜索。

FL中的另一个问题是FL过程中的包丢失或方断开连接，这通常发生在移动的设备上。当失败消息的数量较少时，服务器可以简单地忽略它们，因为它们对全局模型的更新具有较小的权重。如果参与方失败很严重，服务器可以从上一轮的结果重新启动[24]。我们期待更多新颖的解决方案来处理断开问题，以提高效率。

总结

我们将上述研究总结如下。

- 随着SGD框架的广泛研究和应用，近年来对模型化外语的研究也越来越多。我们希望通过使用模型专用方法来实现更好的模型精度。此外，我们鼓励研究人员研究联邦决策树模型。与神经网络相比，树模型具有较小的模型大小并且易于训练，这可以导致FL中的低通信和计算开销。

- 对外语的研究还处于起步阶段。很少有研究将FL应用于训练最先进的神经网络，如ResNeXt [127]和EfficientNet [178]。如何设计一种有效的、实用的算法来训练复杂的机器学习模型仍然是一个具有挑战性的研究方向。

- 虽然大多数研究集中在水平FL，仍然没有很好的算法垂直FL。然而，垂直联邦设置是常见的真实的世界的应用程序中，涉及多个组织。我们期待着对这一前景广阔的领域进行更多的研究。

4.2.2 Communication Efficiency

While the computation of FL can be accelerated using modern hardware and techniques [123, 101, 102] in high performance computing community [197, 199], the FL studies mainly work on reducing the communication size during the FL process.

Konečnỳ et al. [95] propose two ways, structured updates and sketched updates, to reduce the communication costs in federated averaging. The first approach restricts the structure of local updates and transforms it to the multiplication of two smaller matrices. Only one small matrix is sent during the learning process. The second approach uses a lossy compression method to compress the updates. Their method can reduce the communication cost by two orders of magnitude with a slight degradation in convergence speed. Zhu and Jin [226] design a multi-objective evolutionary algorithm to minimize the communication costs and global model test errors simultaneously. Considering the minimization of the communication cost and the maximization of the global learning accuracy as two objectives, they formulated FL as a bi-objective optimization problem and solve it by the multi-objective evolutionary algorithm. Jeong et al. [79] propose a FL framework for devices with non-IID local data. They design federated distillation, whose communication size depends on the output dimension but not on the model size. Also, they propose a data augmentation scheme using a generative adversarial network (GAN) to make the training dataset become IID. Many other studies also design specialize approach for non-IID data [221, 111, 118, 210]. Sattler et al. [164] propose a new compression framework named sparse ternary compression (STC). Specifically, STC compresses the communication using sparsification, ternarization, error accumulation, and optimal Golomb encoding. Their method is robust to non-IID data and large numbers of parties.

Beside the communication size, the communication architecture can also be improved to increase the training efficiency. Marfoq et al. [128] consider the topology design for cross-silo federated learning. They propose an approach to find a throughput-optimal topology, which can significantly reduce the training time.

4.2.3 Privacy, Robustness and Attacks

Although the original data is not exchanged in FL, the model parameters can also leak sensitive information about the training data [167, 137, 196]. Thus, it is important to provide privacy guarantees for the exchanged local updates.

Differential privacy is a popular method to provide privacy guarantees. Geyer et al. [60] apply differential privacy in federated averaging from a client-level perspective. They use the Gaussian mechanism to distort the sum of updates of gradients to protect a whole client's dataset instead of a single data point. McMahan et al. [130] deploy federated averaging in the training of LSTM. They also use client-level differential privacy to protect the parameters. Bhowmick et al. [20] apply local differential privacy to protect the parameters in FL. To increase the model quality, they consider a practical threat model that wishes to decode individuals' data but has little prior information on them. Within this assumption, they can better utilize the privacy budget.

Bonawitz et al. [23] apply secure multi-party computation to protect the local parameters on the basis of federated averaging. Specifically, they present a secure aggregation protocol to securely compute the sum of vectors based on secret sharing [165]. They also discuss how to combine differential privacy with secure aggregation.

Truex et al. [181] combine both secure multiparty computation and differential privacy for privacy-preserving FL. They use differential privacy to inject noises to the local updates. Then the noisy updates will be encrypted using the Paillier cryptosystem [146] before sent to the central server.

For the attacks on FL, one kind of popular attack is backdoor attack, which aims to achieve a bad global model by exchanging malicious local updates.

Bagdasaryan et al. [16] conduct model poisoning attack on FL. The malicious parties commit the attack models to the server so that the global model may overfit with the poisoned data. The secure multi-party computation cannot prevent such attack since it aims to protect the confidentiality of the

4.2.2 沟通效率

虽然FL的计算可以使用高性能计算社区[197，199]中的现代硬件和技术[123，101，102]来加速，但FL研究主要致力于减少FL过程中的通信大小。

Kone Escn'y 等人[95]提出了两种方法，结构化更新和草图更新，以减少联邦平均中的通信成本。第一种方法限制了局部更新的结构，并将其转换为两个较小矩阵的乘法。在学习过程中只发送一个小矩阵。第二种方法使用有损压缩方法来压缩更新。他们的方法可以将通信成本降低两个数量级，收敛速度略有下降。Zhu 和Jin [226]设计了一种多目标进化算法，以同时最小化通信成本和全局模型测试误差。将通信代价最小化和全局学习精度最大化作为两个目标，将FL问题转化为一个双目标优化问题，并采用多目标进化算法进行求解。Jeong 等人。[79]提出了一种用于具有非IID本地数据的设备的FL框架。 他们设计了联邦蒸馏，其通信大小取决于输出维度，而不是模型大小。此外，他们提出了一种使用生成对抗网络（GAN）的数据增强方案，使训练数据集成为IID。许多其他研究也为非IID数据设计了专门的方法[221，111，118，210]。Sattler 等人。[164]提出了一种新的压缩框架，称为稀疏三进制压缩（STC）。具体地，STC使用稀疏化、三值化、误差累积和最优Golomb 编码来压缩通信。他们的方法对非IID数据和大量参与者具有鲁棒性。

除了通信规模之外，还可以改进通信架构以提高训练效率。Marfoq 等人。[128]考虑了跨竖井联邦学习的拓扑设计。他们提出了一种寻找吞吐量最优拓扑的方法，可以显着减少训练时间。

4.2.3 隐私、鲁棒性和攻击

虽然原始数据不在FL中交换，但模型参数也可能泄漏有关训练数据的敏感信息[167，137，196]。因此，重要的是为交换的本地更新提供隐私保证。

差分隐私是提供隐私保证的一种流行方法。盖耶等人。[60]从客户端级别的角度将差分隐私应用于联邦平均。它们使用高斯机制来扭曲梯度更新的总和，以保护整个客户端的数据集，而不是单个数据点。McMahan 等人。[130]在LSTM的训练中部署联邦平均。他们还使用客户端级别的差异隐私来保护参数。Bhowmick 等人。[20]应用局部差分隐私来保护FL中的参数。为了提高模型质量，他们考虑了一种实用的威胁模型，该模型希望解码个人的数据，但几乎没有先验信息。在这个假设下，他们可以更好地利用隐私预算。

Bonawitz 等人。[23]应用安全多方计算来保护基于联邦平均的局部参数。具体来说，他们提出了一个安全的聚合协议，以安全地计算基于秘密共享的向量之和[165]。他们还讨论了如何将联合收割机差异隐私与安全聚合相结合。

Truex 等人。[181]联合收割机将安全多方计算和差分隐私结合起来用于隐私保护FL。他们使用差分隐私向本地更新注入噪声。然后，在发送到中央服务器之前，噪声更新将使用Paillier 密码系统[146]进行加密。

对于FL的攻击，一种流行的攻击是后门攻击，其目的是通过交换恶意的局部更新来实现坏的全局模型。Bagdasaryan 等人[16]对FL进行模型中毒攻击。恶意方将攻击模型提交给服务器，以便全局模型可能与中毒数据过拟合。安全多方计算不能防止这种攻击，因为它旨在保护

model parameters. Bhagoji et al. [19] also study the model poisoning attack on FL. Since the averaging step will reduce the effect of the malicious model, it adopts an explicit boosting way to increase the committed weight update. Sun et al. [174] conduct experiments to evaluate backdoor attacks and defenses for federated learning on federated EMNIST dataset to see what factors can affect the performance of adversary. They find that in the absence of defenses, the performance of the attack largely depends on the fraction of adversaries presented and the "complexity" of the targeted task. The more backdoor tasks we have, the harder it is to backdoor a fixed-capacity model while maintaining its performance on the main task. Wang et al. [188] discuss the backdoor attack from a theoretical view and prove that it is feasible in FL. They also propose a new class of backdoor attacks named edge-case backdoors, which are resistant to the current defending methods. Xie et al. [203] propose a distributed backdoor attack on FL. They decompose the global trigger pattern into local patterns. Each adversarial party only employs one local pattern. The experiments show that their distributed backdoor attack outperforms the central backdoor attack.

Another kind of attack is the *Byzantine*-attacks, where adversaries fully control some authenticated devices and behave arbitrarily to disrupt the network. There have been some existing robust aggregation rules in distributed learning such as $Krum$ [21] and Bulyan [132]. These rules can be directly applied in federated learning. However, since each party conduct multiple local update steps in federated learning, it is interesting to investigate the Byzantine attacks and defenses in federated learning. Li et al. [100] propose RSA, a Byzantine-robust stochastic aggregation method for federated learning on non-IID data setting. Fang et al. [53] propose model poison attacks for byzantine-robust federated learning approaches. The goal of their approach is to modify the local models such that the global model deviates the most towards the inverse of the correct update direction.

Another line of study about FL attack are the inference attacks. There are existing studies for the inferences attack [56, 167, 137] on the machine learning model trained in a centralized setting. For the federated setting, Geiping et al. [58] show that it is possible to reconstruct the training images from the knowledge of the exchanged gradients.

4.2.4 Fairness and Incentive Mechanisms

By taking fairness into consideration based on FedAvg, Li et al. [110] propose q-FedAvg. Specifically, they define the fairness according to the variance of the performance of the model on the parties. If such variance is smaller, then the model is more fair. Thus, they design a new objective inspired by α-fairness [13]. Based on federated averaging, they propose q-FedAvg to solve their new objective. The major difference between q-FedAvg with FedAvg is in the formulas to update model parameters.

Kim et al. [93] combine blockchain architecture with FL. On the basis of federated averaging, they use a blockchain network to exchange the devices' local model updates, which is more stable than a central server and can provide the rewards for the devices. Kang et al. [87] designed a reputation-based worker selection scheme for reliable FL by using a multi-weight subjective logic model. They also leverage the blockchain to achieve secure reputation management for workers with non-repudiation and tamper-resistance properties in a decentralized manner.

Summary

According to the review above, we summarize the studies in Section 4.2.2 to Section 4.2.4 as follows.

- Besides effectiveness, efficiency and privacy are the other two important factors of an FLS. Compared with these three areas, there are fewer studies on fairness and incentive mechanisms. We look forward to more studies on fairness and incentive mechanisms, which can encourage the usage of FL in the real world.

- For the efficiency improvement of FLSs, the communication overhead is still the main challenge. Most studies [95, 79, 164] try to reduce the communication size of each iteration. How to reasonably

模型参数Bhagoji 等人[19]还研究了对FL的模型中毒攻击，由于平均步骤会降低恶意模型的影响，因此采用显式提升的方式来增加提交的权重更新。Sun 等人。[174]进行实验，以评估联邦EMNIST数据集上联邦学习的后门攻击和防御，以了解哪些因素会影响对手的性能。他们发现，在没有防御的情况下，攻击的性能在很大程度上取决于对手的比例和目标任务的“ 复杂性” 。我们拥有的后门任务越多，就越难在保持主任务性能的同时后门固定容量模型。Wang 等人[188]从理论上讨论了后门攻击，证明了它在FL中是可行的，他们还提出了一类新的后门攻击，称为边缘情况后门，它可以抵抗当前的防御方法。Xie等人[203]提出了一种分布式后门攻击方法，将全局触发模式分解为局部模式。每个敌对方只使用一种局部模式。实验结果表明，分布式后门攻击的性能优于集中式后门攻击。

另一种攻击是拜占庭攻击，其中对手完全控制一些经过身份验证的设备，并任意破坏网络。在分布式学习中已经存在一些现有的鲁棒聚合规则，例如克鲁姆[21]和Bulyan [132]。这些规则可以直接应用于联邦学习。然而，由于联邦学习中的每一方都进行多个局部更新步骤，因此研究联邦学习中的拜占庭攻击和防御是很有趣的。L等人。[100]提出了RSA，这是一种用于非IID数据设置的联邦学习的拜占庭鲁棒随机聚合方法。Fang 等人。[53]提出了用于拜占庭鲁棒联邦学习方法的模型毒药攻击。他们的方法的目标是修改局部模型，使得全局模型朝着正确更新方向的逆方向偏离最多。

FL攻击的另一个研究方向是推理攻击。现有的研究针对在集中式环境中训练的机器学习模型的推理攻击[56，167，137]。对于联邦设置，Geiping 等人。[58]表明可以根据交换梯度的知识重建训练图像。

4.2.4 公平和激励机制

通过基于FedAvg 考虑公平性，L等人。[110]提出了q-FedAvg 。具体而言，他们根据模型对各方的表现的方差来定义公平性。如果这种方差较小，则模型更公平。因此，他们设计了一个受α公平启发的新目标[13]。基于联邦平均，他们提出了q-FedAvg 来解决他们的新目标。q-FedAvg 与FedAvg 之间的主要区别在于更新模型参数的公式。

Kim等人[93]将联合收割机区块链架构与FL相结合，在联邦平均的基础上，他们使用区块链网络来交换设备的本地模型更新，这比中央服务器更稳定，并且可以为设备提供奖励。Kang 等人。[87]通过使用多权重主观逻辑模型设计了一种基于声誉的可靠FL工人选择方案。他们还利用区块链以分散的方式为具有不可否认性和防篡改性的工作人员实现安全的声誉管理。

总结

根据上述综述，我们将第4.2.2 节至第4.2.4 节中的研究总结如下。

- 除了有效性之外，效率和隐私是FLS的另外两个重要因素。与这三个领域相比，对公平和激励机制的研究较少。我们期待着更多关于公平性和激励机制的研究，以鼓励外语在真实的世界中的使用。

- 对于FLS的效率提高，通信开销仍然是主要的挑战。大多数研究[95，79，164]试图减少每次迭代的通信大小。如何合理

set the number of communication rounds is also promising [226]. The trade-off between the computation and communication still needs to be further investigated.

- For the privacy guarantees, differential privacy and secure multi-party computation are two popular techniques. However, differential privacy may impact the model quality significantly and secure multi-party computation may be very time-consuming. It is still challenging to design a practical FLS with strong privacy guarantees. Also, the effective robust algorithms against poisoning attacks are not widely adopted yet.

4.2.5 Applications

One related area with FL is edge computing [140, 212, 153, 47, 218], where the parties are edge devices. Many studies try to integrate FL with the mobile edge systems. FL also shows promising results in recommender system [14, 29, 225], natural language processing [71] and transaction fraud detection [222].

Edge Computing

Nishio and Yonetani [143] implement federated averaging in practical mobile edge computing (MEC) frameworks. They use an operator of MEC framworks to manage the resources of heterogeneous clients. Wang et al. [194] adopt both distributed deep reinforcement learning (DRL) and federatd learning in mobile edge computing system. The usage of DRL and FL can effectively optimize the mobile edge computing, caching, and communication. Wang et al. [192] perform FL on resource-constrained MEC systems. They address the problem of how to efficiently utilize the limited computation and communication resources at the edge. Using federated averaging, they implement many machine learning algorithms including linear regression, SVM, and CNN. He et al. [73] also consider the limited computing resources in the edge devices. They propose FedGKT, where each device only trains a small part of a whole ResNet to reduce the computation overhead.

Recommender System

Ammad-ud din et al. [14] formulate the first federated collaborative filter method. Based on a stochastic gradient approach, the item-factor matrix is trained in a global server by aggregating the local updates. They empirically show that the federated method has almost no accuracy loss compared with the centralized method. Chai et al. [29] design a federated matrix factorization framework. They use federated SGD to learn the matrices. Moreover, they adopt homomorphic encryption to protect the communicated gradients. Tan et al. [177] build a federated recommender system (FedRecSys) based on FATE. FedRecSys has implemented popular recommendation algorithms with SMC protocols. The algorithms include matrix factorization, singular value decomposition, factorization machine, and deep learning.

Natural Language Processing

Hard et al. [71] apply FL in mobile keyboard next-word prediction. They adopt the federated averaging method to learn a variant of LSTM called Coupled Input and Forget Gate (CIFG) [65]. The FL method can achieve better precision recall than the server-based training with log data.

Transaction Fraud Detection

Zheng et al. [222] introduce FL into the field of fraud detection on credit card transaction. They design a novel meta-learning based federated learning framework, named deep K-tuplet network, which not only guarantees data privacy but also achieves a significantly higher performance compared with the existing approaches.

设置通信轮数也是有希望的[226]。计算和通信之间的权衡仍然需要进一步研究。

- 在隐私保证方面，差分隐私和安全多方计算是两种比较流行的技术。然而，差异隐私可能会影响模型的质量显着和安全的多方计算可能是非常耗时的。设计一个具有强隐私保证的实用FLS仍然具有挑战性。另外，针对中毒攻击的有效鲁棒算法还没有被广泛采用。

4.2.5 应用

与FL相关的一个领域是边缘计算[140，212，153，47，218]，其中各方是边缘设备。许多研究试图将FL与移动的边缘系统集成。FL还在推荐系统[14，29，225]，自然语言处理[71]和交易欺诈检测[222]中显示出有希望的结果。

边缘计算

西尾和Yonetani [143]在实际的移动的边缘计算（MEC）框架中实现了联合平均。它们使用MEC框架的操作符来管理异构客户端的资源。Wang 等人。[194]在移动的边缘计算系统中采用分布式深度强化学习（DRL）和联邦学习。DRL和FL的使用可以有效地优化移动的边缘计算、缓存和通信。Wang 等人。[192]在资源受限的MEC系统上执行FL。它们解决了如何有效利用边缘有限的计算和通信资源的问题。使用联邦平均，他们实现了许多机器学习算法，包括线性回归，SVM和CNN 。He 等人[73]还考虑了边缘设备中有限的计算资源。他们提出了FedGKT，其中每个设备只训练整个ResNet 的一小部分，以减少计算开销。

推荐系统

Ammad -ud din 等人[14]提出了第一个联合协作过滤方法。基于随机梯度方法，通过聚集局部更新在全局服务器中训练项目因子矩阵。他们的经验表明，联邦方法几乎没有精度损失相比，集中式方法。Chai 等人[29]设计了一个联邦矩阵分解框架。他们使用联邦SGD来学习矩阵。此外，它们采用同态加密来保护所传送的梯度。Tan等人。[177]基于FATE构建了一个联邦推荐系统（FedRecSys ）。FedRecSys 已经使用SMC协议实现了流行的推荐算法。这些算法包括矩阵分解、奇异值分解、分解机和深度学习。

自然语言处理

Hard 等人。[71]将FL应用于移动的键盘下一个单词预测。他们采用联邦平均方法来学习LSTM的一种变体，称为耦合输入和遗忘门（CIFG）[65]。FL方法可以实现比基于服务器的日志数据训练更好的查准率。

交易欺诈检测

Zheng 等人[222]将FL引入信用卡交易欺诈检测领域。他们设计了一种新的基于元学习的联邦学习框架，称为深度K-tuplet 网络，它不仅保证了数据隐私，而且与现有方法相比，性能显着提高。

Summary

According to the above studies, we have the following summaries.

- Edge computing naturally fits the cross-device federated setting. A nontrivial issue of applying FL to edge computing is how to effectively utilize and manage the edge resources. The usage of FL can bring benefits to users, especially for improving mobile device services.
- FL can solve many traditional machine learning tasks such as image classification and work prediction. Due to the regulations and "data islands", the federated setting may be a common setting in the next years. With the fast development of FL, we believe that there will be more applications in computer vision, natural language processing, and healthcare.

4.2.6 Benchmark

Benchmark is important for directing the development of FLSs. Multiple benchmark-related works have been conducted recently, and several benchmark frameworks are available online. We categorize them into three types: 1) *General purpose benchmark systems* aim at comprehensively evaluate FLSs and give a detailed characterization of different aspects of FLSs; 2) *Targeted benchmarks* aim at one or more aspects that concentrated in a small domain and tries to optimize the performance of the system in that domain; 3) *Dataset benchmarks* aim at providing dedicated datasets for federated learning.

General Purpose Benchmark Systems

FedML [74] is a research library that provides both frameworks for federated learning and benchmark functionalities. As a benchmark, it provides comprehensive baseline implementations for multiple ML models and FL algorithms, including FedAvg, FedNAS, Vertical FL, and split learning. Moreover, it supports three computing paradigms, namely distributed training, mobile on-device training, and standalone simulation. Although some of its experiment results are currently still at a preliminary stage, it is one of the most comprehensive benchmark frameworks concerning its functionalities.

FedEval [30] is another evaluation model for federated learning. It features the "ACTPR" model, i.e., using accuracy, communication, time consumption, privacy and robustness as its evaluation targets. It utilizes Docker containers to provide an isolated evaluation environment to work around the hardware resource limitation problem, and simulated up to 100 clients in the implementation. Currently, two horizontal algorithms are supported: FedSGD and FedAvg, and the models including MLP and LeNet are tested.

OARF [77] provides a set of utilities and reference implementations for FL benchmarks. It features the measurement of different components in FLSs, including FL algorithms, encryption mechanisms, privacy mechanisms, and communication methods. In addition, it also features realistic partitioning of datasets, which utilizes public datasets collected from different sources to reflect real-world data distributions. Both horizontal vertical algorithms are tested.

Edge AIBench [70] provides a testbed for federated learning applications, and models four application scenarios as reference implementations: ICU patients monitor, surveillance camera, smart home, and autonomous vehicles. The implementation is open sourced, but no experiment result has been reported currently.

Targeted Benchmarks

Nilsson et al. [142] propose a method utilizing correlated t-test to compare between different types of federated learning algorithms while bypassing the influence of data distributions. Three FL algorithms, FedAvg, FedSVRG [95] and CO-OP [195] are compared in both IID and non-IID setup in their work, and the result shows that FedAvg achieves the highest accuracy among the three algorithms regardless of how data is partitioned.

总结

根据以上研究，我们有以下几点总结。

- 边缘计算自然适合跨设备联合设置。将FL应用于边缘计算的一个重要问题是如何有效地利用和管理边缘资源。FL的使用可以给用户带来好处，特别是对于改善移动终端服务。

- FL可以解决许多传统的机器学习任务，如图像分类和工作预测。由于法规和“ 数据孤岛” ，联合设置可能是未来几年的常见设置。随着FL的快速发展，我们相信在计算机视觉，自然语言处理和医疗保健方面会有更多的应用。

4.2.6 基准

基准测试对于指导FLS的发展具有重要意义。最近进行了多项与基准有关的工作，并在网上提供了几个基准框架。我们将其分为三种类型：1）通用基准系统旨在全面评估FLS，并对FLS的不同方面进行给予详细描述; 2）针对性基准系统针对集中在一个小领域的一个或多个方面，并试图优化该领域的系统性能; 3）数据集基准系统旨在为联邦学习提供专用数据集。

通用基准系统

FedML [74]是一个研究库，提供了联邦学习和基准测试功能的框架。作为基准，它为多种ML模型和FL算法提供了全面的基线实现，包括FedAvg ，FedNAS ，Vertical FL和split learning 。此外，它还支持三种计算模式，即分布式训练、移动的设备上训练和独立模拟。虽然其一些实验结果目前仍处于初步阶段，但它是就其功能而言最全面的基准框架之一。

FedEval [30]是联邦学习的另一个评估模型。它以“ ACTPR” 模式为特色，即，以准确性、通信性、耗时性、隐私性和鲁棒性为评价指标。它利用Docker 容器提供一个隔离的评估环境来解决硬件资源限制问题，并在实现中模拟了多达100 个客户端。目前支持两种水平算法：FedSGD 和FedAvg ，并测试了包括MLP和LeNet 在内的模型。

OARF [77]为FL基准提供了一组实用程序和参考实现。它的特点是在FLS中的不同组件的测量，包括FL算法，加密机制，隐私机制和通信方法。此外，它还具有现实的数据集分区，利用从不同来源收集的公共数据集来反映真实世界的数据分布。两个水平垂直算法进行了测试。

Edge AIBench [70]为联邦学习应用程序提供了一个测试平台，并将四种应用场景建模为参考实现：ICU患者监护仪，监控摄像头，智能家居和自动驾驶汽车。该实现是开源的，但目前还没有实验结果报告。

目标基准

Nilsson 等人。[142]提出了一种利用相关t检验来比较不同类型的联邦学习算法的方法，同时绕过数据分布的影响。三种FL算法，FedAvg ，FedSVRG [95]和CO-OP [195]在他们的工作中在IID和非IID设置中进行了比较，结果表明FedAvg 在三种算法中实现了最高的准确性，无论数据如何划分。

Zhuang et al. [227] utilize benchmark analysis to improve the performance of federated person re-identification. The benchmark part uses 9 different datasets to simulate real-world situations and uses federated partial averaging, an algorithm that allows the aggregation of partially different models, as the reference implementations.

Zhang et al. [216] present a benchmark targeted at semi-supervised federated learning setting, where users only have unlabelled data, and the server only has a small amount of labelled data, and explore the relation between final model accuracy and multiple metrics, including the distribution of the data, the algorithm and communication settings, and the number of clients. Utilizing the experiment results, their semi-supervised learning improved method achieves better generalization performance.

Liu et al. [117] focus on the non-IID problem, where datasets are distributed unevenly across the participating parties. Their work explores methods for quantitatively describing the skewness of the data distribution, and propose several non-IID dataset generation approaches.

Datasets

LEAF [25] is one of the earliest dataset proposals for federated learning. It contains six datasets covering different domains, including image classification, sentiment analysis, and next-character prediction. A set of utilities is provided to divide datasets into different parties in an IID or non-IID way. For each dataset, a reference implementation is also provided to demonstrate the usage of that dataset in the training process.

Luo et al. [124] present real-world image datasets which are collected from 26 different street cameras. Images in that dataset contain objects of 7 different categories and are suitable for the object detection task. Implementations with federated averaging running YOLOv3 model and Faster R-CNN model are provided as references.

Summary

Summarizing the studies above, we have the following discoveries

- Benchmarks serve an important role in the development of federated learning. Through different types of benchmarks, we can quantitatively characterize the different components and aspects of federated learning. Benchmarks regarding the security and privacy issues in federated learning are still at an early stage and require further development.
- Currently no comprehensive enough benchmark system has been implemented to cover all the algorithms or application types in FLSs. Even the most comprehensive benchmark systems lack supports for certain algorithms and evaluation metrics for each level of the system. Further development of comprehensive benchmark systems requires the support of extensive FL frameworks.
- Most benchmark researches are using datasets which are split from a single dataset, and there is no consensus on what type of splitting method should be used. Similarly, regarding the non-IID problem, there is no consensus on the metric of non-IID-ness. Using realistic partitioning method, as proposed in FedML [74] and OARF [77] may mitigate this issue, but for federated learning at a large-scale, realistic partitioning is not suitable due to the difficulty of collecting data from different sources.

4.3 Open Source Systems

In this section, we introduce five open source FLSs: Federated AI Technology Enabler (FATE)[3], Google TensorFlow Federated (TFF)[4], OpenMined PySyft[5], Baidu PaddleFL[6], and FedML[7].

[3] https://github.com/FederatedAI/FATE
[4] https://github.com/tensorflow/federated
[5] https://github.com/OpenMined/PySyft
[6] https://github.com/PaddlePaddle/PaddleFL
[7] https://github.com/FedML-AI/FedML

Zhuang 等人。[227]利用基准分析来提高联邦人员重新识别的性能。基准测试部分使用9个不同的数据集来模拟真实世界的情况，并使用联邦部分平均，这是一种允许聚合部分不同模型的算法，作为参考实现。

Zhang et al. [216]提出了一个针对半监督联邦学习设置的基准测试，其中用户只有未标记的数据，服务器只有少量的标记数据，并探索最终模型准确性与多个指标之间的关系，包括数据的分布，算法和通信设置以及客户端的数量。利用实验结果，他们的半监督学习改进方法取得了更好的泛化性能。

Liu等人。[117]关注非IID问题，其中数据集在参与方之间分布不均匀。他们的工作探索了定量描述数据分布偏度的方法，并提出了几种非IID数据集生成方法。

数据集

LEAF[25]是联邦学习最早的数据集提案之一。它包含六个涵盖不同领域的数据集，包括图像分类，情感分析和下一个字符预测。提供了一组实用程序，用于以IID或非IID方式将数据集划分为不同的各方。对于每个数据集，还提供了一个参考实现，以演示该数据集在训练过程中的使用。

Luo 等人。[124]展示了从26 个不同街道摄像机收集的真实图像数据集。该数据集中的图像包含7个不同类别的对象，适用于对象检测任务。提供了运行YOLOv 3模型和Faster R-CNN 模型的联邦平均实现作为参考。

总结

总结以上研究，我们有以下发现

- 基准在联邦学习的发展中发挥着重要作用。通过不同类型的基准测试，我们可以定量地描述联邦学习的不同组件和方面。关于联合学习中安全和隐私问题的基准仍处于早期阶段，需要进一步发展。

- 目前还没有一个全面的基准测试系统能够覆盖FLS中的所有算法或应用类型。即使是最全面的基准测试系统也缺乏对系统每个级别的某些算法和评估指标的支持。全面的基准系统的进一步发展需要广泛的FL框架的支持。

- 大多数基准研究使用的数据集是从单个数据集中分离出来的，并且对于应该使用什么类型的分离方法没有达成共识。同样，关于非IID问题，对非IID性的度量也没有共识。使用FedML [74]和OARF [77]中提出的现实分区方法可以缓解这个问题，但是对于大规模的联邦学习，由于难以从不同来源收集数据，因此现实分区并不适合。

4.3 开源系统

在本节中，我们将介绍五种开源FLS：Federated AI Technology Enabler （FATE）[3]，Google TensorFlow Federated （TFF）[4]，OpenMined PySyft [5]，Baidu PaddleFL [6]和FedML [7]。

[3] https://github.com/FederatedAI/FATE

[4] https://github.com/tensorflow/federated

[5] https://github.com/OpenMined/PySyft

[6] https://github.com/PaddlePaddle/PaddleFL

[7] https://github.com/FedML-AI/FedML

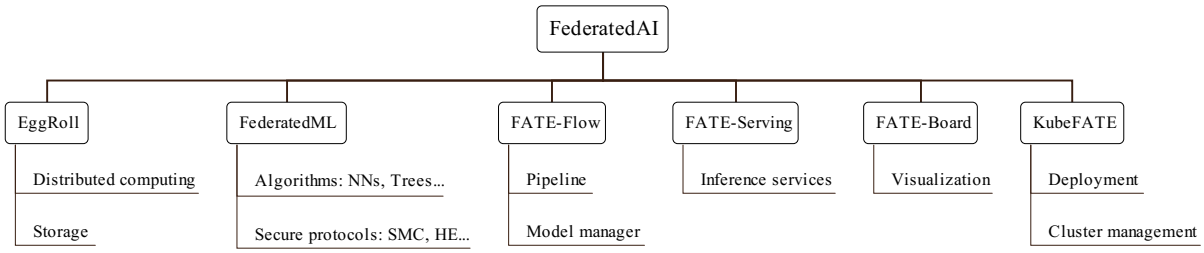


Figure 4: The FATE system structure

4.3.1 FATE

FATE is an industrial level FL framework developed by WeBank, which aims to provide FL services between different organizations. FATE is based on Python and can be installed on Linux or Mac. It has attracted about 3.2k stars and 900 forks on GitHub. The overall structure of FATE is shown in Figure 4. It has six major modules: EggRoll, FederatedML, FATE-Flow, FATE-Serving, FATE-Board, and KubeFATE. EggRoll manages the distributed computing and storage. It provides computing and storage AIPs for the other modules. FederatedML includes the federated algorithms and secure protocols. Currently, it supports training many kinds of machine learning models under both horizontal and vertical federated setting, including NNs, GBDTs, and logistic regression. FATE assumes that the parties are honest-but-curious. Thus, it uses secure multi-party computation and homomorphic encryption to protect the communicated messages. However, it does not support differential privacy to protect the final model. FATE-Flow is a platform for the users to define their pipeline of the FL process. The pipeline can include the data preprocessing, federated training, federated evaluation, model management, and model publishing. FATE-Serving provides inference services for the users. It supports loading the FL models and conducting online inference on them. FATE-Board is a visualization tool for FATE. It provides a visual way to track the job execution and model performance. Last, KubeFATE helps deploy FATE on clusters by using Docker or Kubernetes. It provides customized deployment and cluster management services. In general, FATE is a powerful and easy-to-use FLS. Users can simply set the parameters to run a FL algorithm. Moreover, FATE provides detailed documents on its deployment and usage. However, since FATE provides algorithm-level interfaces, practitioners have to modify the source code of FATE to implement their own federated algorithms. This is not easy for non-expert users.

4.3.2 TFF

TFF, developed by Google, provides the building blocks for FL based on TensorFlow. It has attracted about 1.5k stars and 380 forks on GitHub. TFF provides a Python package which can be easily installed and imported. As shown in Figure 5, it provides two APIs of different layers: FL API and Federated Core (FC) API. FL API offers high-level interfaces. It includes three key parts, which are models, federated computation builders, and datasets. FL API allows users to define the models or simply load the Keras [66] model. The federated computation builders include the typical federated averaging algorithm. Also, FL API provides simulated federated datasets and functions to access and enumerate the local datasets for FL. Besides high-level interfaces, FC API also includes lower-level interfaces as the foundation of the FL process. Developers can implement their functions and interfaces inside the federated core. Finally, FC provides the building blocks for FL. It support multiple federated operators such as federated sum, federated reduce, and federated broadcast. Developers can define their own operators to implement the FL algorithm. Overall, TFF is a lightweight system for developers to design and implement new FL algorithms. Currently, TFF does not consider consider any adversaries during FL training. It does not provide privacy mechanisms. TFF can only deploy on a single machine now, where the federated setting is implemented by simulation.

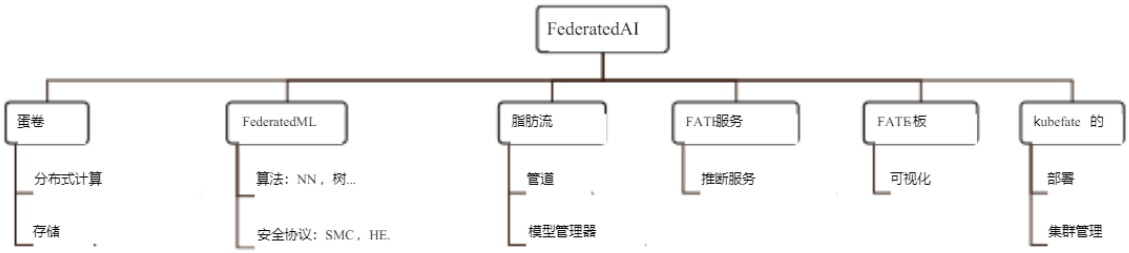


图4：FATE系统结构

4.3.1 FATE

FATE是微众银行开发的行业级FL框架，旨在为不同组织之间提供FL服务。FATE基于Python ，可以安装在Linux 或Mac 上。它在GitHub 上吸引了大约3.2k 颗星星和900 个分叉。FATE的总体结构如图4所示。它有六个主要模块：EggRoll ， FederatedML ， FATE-Flow ， FATE-Serving ， FATE-Board 和KubeFATE。EggRoll 管理分布式计算和存储。它为其他模块提供计算和存储AIP。FederatedML 包括联邦算法和安全协议。目前，它支持在水平和垂直联邦设置下训练多种机器学习模型，包括NN ，GBDTs和logistic 回归。命运假设当事人诚实但好奇。因此，它使用安全多方计算和同态加密来保护通信消息。但是，它不支持差分隐私来保护最终模型。 FATE-Flow 是一个用户定义FL流程管道的平台。管道可以包括数据预处理、联邦训练、联邦评估、模型管理和模型发布。FATE-Serving 为用户提供推理服务。它支持加载FL模型并对其进行在线推理。FATE-Board 是FATE的可视化工具。它提供了一种可视化的方式来跟踪作业执行和模型性能。最后，KubeFATE通过使用Docker 或Kubernetes 帮助在集群上部署FATE。它提供定制的部署和集群管理服务。总的来说，FATE是一个功能强大且易于使用的FLS。用户可以简单地设置参数来运行FL算法。此外，FATE还提供了有关其部署和使用的详细文档。然而，由于FATE提供算法级接口，从业者必须修改FATE的源代码来实现自己的联邦算法。这对于非专业用户来说并不容易。

4.3.2 TFF

TFF由Google 开发，提供了基于TensorFlow 的FL构建块。它在GitHub 上吸引了大约1.5k 个星星和380 个分叉。TFF提供了一个Python 包，可以很容易地安装和导入。如图5所示，它提供了两个不同层的API：FL API和Federated Core （FC）API。FL API提供高级接口。它包括三个关键部分，即模型、联邦计算构建器和数据集。FL API允许用户定义模型或简单地加载Keras [66]模型。联邦计算构建器包括典型的联邦平均算法。此外，FL API还提供了模拟的联邦数据集和函数来访问和枚举FL的本地数据集。除了高层接口外，FC API还包括作为FL过程基础的低层接口。开发人员可以在联邦核心内实现他们的函数和接口。最后，FC为FL提供构建块。 它支持多个联邦运算符，如联邦求和、联邦缩减和联邦广播。开发人员可以定义自己的运算符来实现FL算法。总的来说，TFF是一个轻量级的系统，供开发人员设计和实现新的FL算法。目前，TFF在FL训练中不考虑任何对手。它不提供隐私机制。TFF现在只能部署在一台机器上，其中联邦设置是通过模拟实现的。

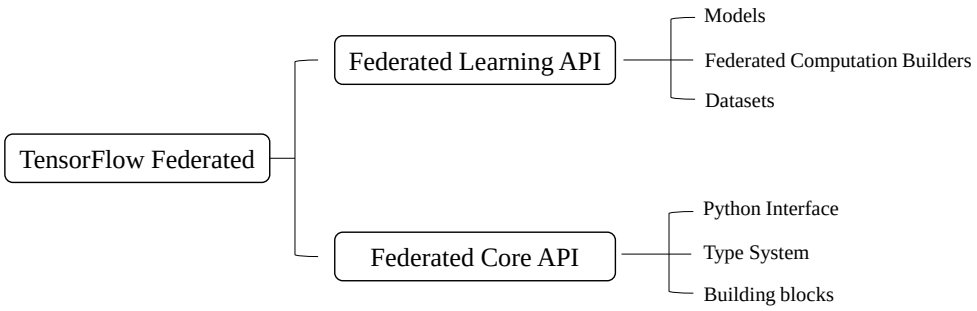


Figure 5: The TFF system structure

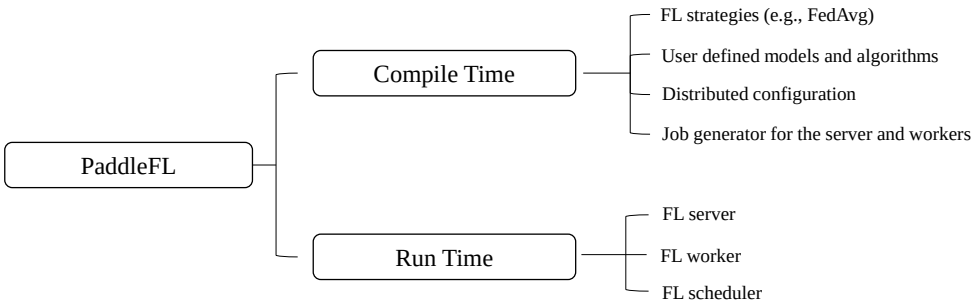


Figure 6: The PaddleFL system structure

4.3.3 PySyft

PySyft, first proposed by Ryffel et al. [158] and developed by OpenMined, is a python library that provides interfaces for developers to implement their training algorithm. It has attracted about 7.3k stars and 1.7k forks on GitHub. While TFF is based on TensorFlow, PySyft can work well with both PyTorch and TensorFlow. PySyft provides multiple optional privacy mechanisms including secure multi-party computation and differential privacy. Thus, it can support running on honest-but-curious parties. Moreover, it can be deployed on a single machine or multiple machines, where the communication between different clients is through the websocket API [168]. However, while PySyft provides a set of tutorials, there is no detailed document on its interfaces and system architecture.

4.3.4 PaddleFL

PaddleFL is a FLS based on PaddlePaddle[8], which is a deep learning platform developed by Baidu. It is implemented on C++ and Python. It has attracted about 260 stars and 60 forks on GitHub. Like PySyft, PaddleFL supports both differential privacy and secure multi-party computation and can work on honest-but-curious parties. The system structure of PaddleFL is shown in Figure 6. In the compile time, there are four components including FL strategies, user defined models and algorithms, distributed training configuration, and FL job generator. The FL strategies include the horizontal FL algorithms such as FedAvg. Vertical FL algorithms will be integrated in the future. Besides the provided FL strategies, users can also define their own models and training algorithms. The distributed training configuration defines the training node information in the distributed setting. FL job generator generates the jobs for federated server and workers. In the run time, there are three components including FL server, FL worker, and FL scheduler. The server and worker are the manager and parties in FL, respectively. The scheduler selects the workers that participate in the training in each round. Currently, the development of PaddleFL is still in a early stage and the documents and examples are not clear enough.

[8]https://github.com/PaddlePaddle/Paddle

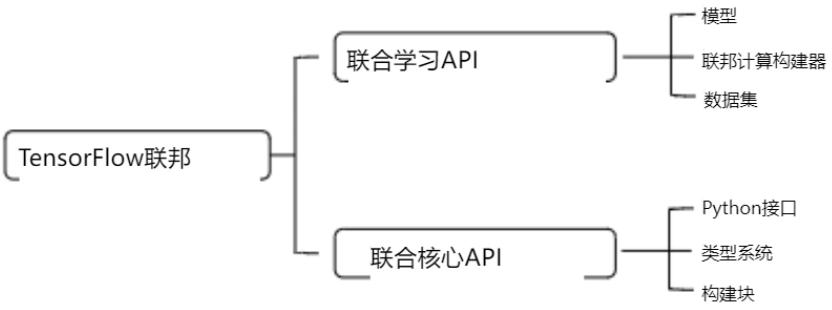


图5： TFF系统结构

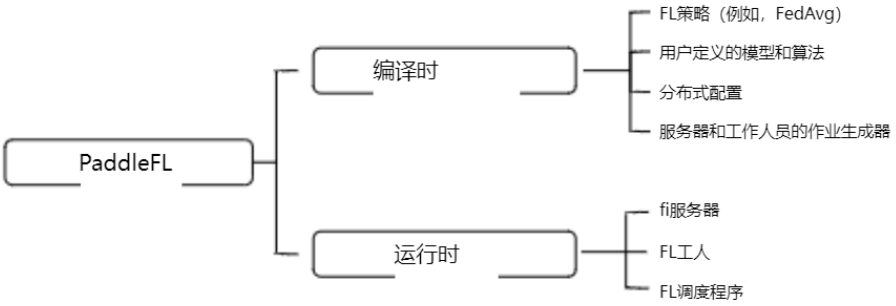


图6： PaddleFL 系统结构

4.3.3 PySyft

PySyft，由Ryanson 等人首先提出[158]，由OpenMined 开发，是一个Python 库，为开发人员提供接口来实现他们的训练算法。它在GitHub 上吸引了大约7.3k 颗星和1.7k 个分叉。虽然TFF基于TensorFlow ，但PySyft 可以很好地与PyTorch 和TensorFlow 一起工作。PySyft 提供了多种可选的隐私机制，包括安全多方计算和差分隐私。因此，它可以支持诚实但好奇的政党。此外，它可以部署在单个机器或多个机器上，其中不同客户端之间的通信是通过WebSocket API [168]。然而，虽然PySyft 提供了一组教程，但没有关于其接口和系统架构的详细文档。

4.3.4 PaddleFL

PaddleFL 是基于百度开发的深度学习平台PaddlePaddle 的FLS。它在C++和Python 上实现。它在GitHub 上吸引了大约260 颗星星和60 个分叉。像PySyft 一样，PaddleFL 支持差分隐私和安全多方计算，并且可以在诚实但好奇的各方上工作。PaddleFL 的系统结构如图6所示。在编译时，有四个组成部分，包括FL策略，用户定义的模型和算法，分布式训练配置，FL作业生成器。FL策略包括水平FL算法，如FedAvg 。未来将整合垂直FL算法。除了提供的FL策略，用户还可以定义自己的模型和训练算法。分布式训练配置定义分布式设置中的训练节点信息。FL作业生成器为联邦服务器和工作者生成作业。 在运行时，有三个组件，包括FL服务器，FL工作者和FL调度器。服务器和工作者分别是FL中的管理者和参与方。调度器选择参与每一轮训练的工作者。目前，PaddleFL 的开发还处于早期阶段，文档和示例不够清晰。

8https ： github .com / PaddlePaddle / Paddle

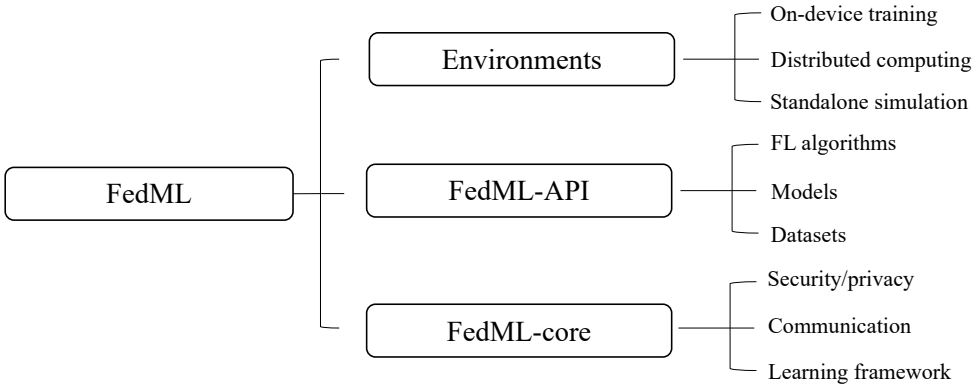


Figure 7: The FedML system structure

4.3.5 FedML

FedML provides both a framework for federated learning and a platform for FL benchmark. It is developed by a team from University of Southern California [74] based on PyTorch. FedML has attracted about 660 stars and 180 forks on GitHub. As an FL framework, It's core structure is divided into two levels, as shown in Figure 7. In the low-level FedML-core, training engine and distributed communication infrastructures are implemented. The high-level FedML-API is built on top of them and provides training models, datasets, and FL algorithms. Reference application/benchmark implementations are further built on top of the FedML-API. While most algorithms implemented on FedML does not consider any adversaries, it supports applying differential privacy when aggregating the messages from the parties. FedML supports three computing paradigms, namely standalone simulation, distributed computing and on-device training, which provides a simulation environment for a broad spectrum of hardware requirements. Reference implementations for all supported FL algorithms are provided. Although there are still gaps between some of the experiment results and the optimal results, they provide useful information for further development.

4.3.6 Others

There are other closed source federated learning systems. NVIDIA Clara [9] has enabled FL. It adopts a centralized architecture and encrypted communication channel. The targeted users of Clara FL is hospitals and medical institutions. Ping An Technology aims to build a federated learning system named Hive [2], which targets at the financial industries. While Clara FL provides APIs and documents, we cannot find the official documents of Hive.

4.3.7 Summary

Overall, FATE, PaddleFL, and FedML try to provide algorithm-level APIs for users to use directly, while TFF and PySyft try to provide more detailed building blocks so that the developers can easily implement their FL process. Table 2 shows the comparison between the open-source systems. In the algorithm level, FATE is the most comprehensive system that supports many machine learning models under both horizontal and vertical settings. TFF and PySyft only implement FedAvg, which is a basic framework in FL as shown in Section 4.2. PaddleFL supports several horizontal FL algorithms currently on NNs and logistic regression. FedML integrates several state-of-the-art FL algorithms such as FedOpt [154] and FedNova [190]. Compared with FATE, TFF, and FedML, PySyft and PaddleFL provide more privacy mechanisms. PySyft covers all the listed features that TFF supports, while TFF is based on TensorFlow and PySyft works better on PyTorch. Based on the popularity on GitHub, PySyft is currently the most impactful federated learning system in the machine learning community.

[9] https://developer.nvidia.com/clara

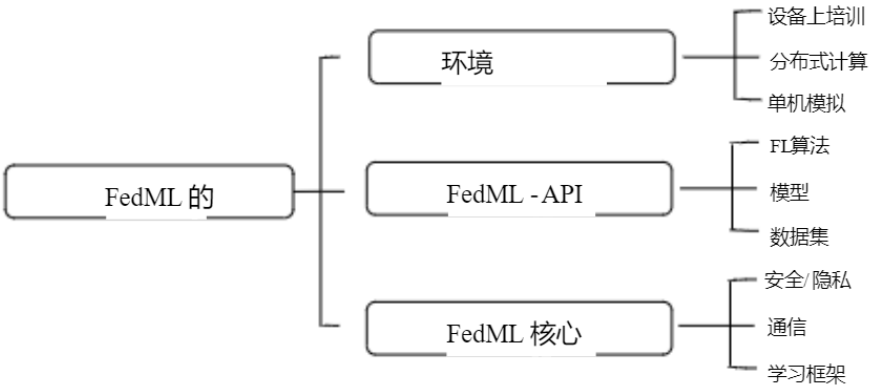


图7： FedML 系统结构

4.3.5 FedML的

FedML 提供了一个联邦学习的框架和FL基准测试的平台。它是由南加州大学的一个团队基于PyTorch 开发的。FedML 已经在GitHub 上吸引了大约660 颗星星和180 个分叉。作为一个FL框架，它的核心结构分为两个层次，如图7所示。在底层FedML 核心中，实现了训练引擎和分布式通信基础设施。高级FedML - API构建在它们之上，并提供训练模型，数据集和FL算法。参考应用程序/ 基准实现进一步构建在FedML - API之上。虽然FedML 上实现的大多数算法不考虑任何对手，但它支持在聚合来自各方的消息时应用差异隐私。FedML 支持三种计算范式，即独立仿真、分布式计算和设备上培训，为广泛的硬件需求提供了仿真环境。提供了所有支持的FL算法的参考实现。虽然一些实验结果与最优结果之间仍有差距，但它们为进一步发展提供了有用的信息。

4.3.6 其他

还有其他闭源的联邦学习系统。NVIDIA Clara 已启用FL，采用集中式架构和加密通信通道。Clara FL的目标用户是医院和医疗机构。平安科技的目标是建立一个名为Hive 的联邦学习系统[2]，该系统针对金融行业。虽然Clara FL提供了API和文档，但我们无法找到Hive 的官方文档。

4.3.7 总结

总体而言，FATE、PaddleFL 和FedML 试图提供算法级API供用户直接使用，而TFF和PySyft 试图提供更详细的构建块，以便开发人员可以轻松实现其FL过程。表2显示了开源系统之间的比较。在算法层面，FATE是最全面的系统，在水平和垂直设置下支持许多机器学习模型。TFF和PySyft 只实现了FedAvg ，这是FL中的一个基本框架，如4.2 节所示。PaddleFL 支持目前NN 和逻辑回归上的几种水平FL算法。FedML 集成了几种最先进的FL算法，如FedOpt [154]和FedNova [190]。与FATE、TFF和FedML 相比，PySyft 和PaddleFL 提供了更多的隐私机制。PySyft 涵盖了TFF支持的所有列出的功能，而TFF基于TensorFlow ，PySyft 在PyTorch 上工作得更好。 基于GitHub 上的流行度，PySyft 是目前机器学习社区中最具影响力的联邦学习系统。

9https : developer .nvidia .com / clara

Table 2: The comparison among some existing FLSs. The notations used in this table are the same as Table 1. The cell is left empty if the system does not support the corresponding feature. There is no release version for FedML.

Supported features		FATE 1.5.0	TFF 0.17.0	PySyft 0.3.0	PaddleFL 1.1.0	FedML
Operation systems	Mac	✓	✓	✓	✓	✓
	Linux	✓	✓	✓	✓	✓
	Windows			✓	✓	✓
	iOS					✓
	Android					✓
Data partitioning	horizontal	✓	✓	✓	✓	✓
	vertical	✓			✓	✓
Models	NN	✓	✓	✓	✓	✓
	DT	✓				
	LM	✓	✓	✓	✓	✓
Privacy Mechanisms	DP		✓	✓	✓	✓
	CM	✓		✓	✓	
Communication	simulated	✓	✓	✓	✓	✓
	distributed	✓		✓	✓	✓
Hardwares	CPUs	✓	✓	✓	✓	✓
	GPUs		✓	✓		✓

5 System Design

Figure 8 shows the factors that need to be considered in the design of an FLS. Here effectiveness, efficiency, and privacy are three important metrics of FLSs, which are also main research directions of federated learning. Inspired by federated database [166], we also consider autonomy, which is necessary to make FLSs practical. Next, we explain these factors in detail.

5.1 Effectiveness

The core of an FLS is an (multiple) effective algorithm (algorithms). To determine the algorithm to be implemented from lots of existing studies as shown in Table 1, we should first check the data partitioning of the parties. If the parties have the same features but different samples, one can use FedAvg [129] for NNs and SimFL [104] for trees. If the parties have the same sample space but different features, one can use FedBCD [120] for NNs and SecureBoost [38] for trees.

5.2 Privacy

An important requirement of FLSs is to protect the user privacy. Here we analyze the reliability of the manager. If the manager is honest and not curious, then we do not need to adopt any additional technique, since the FL framework ensures that the raw data is not exchanged. If the manager is honest but curious, then we have to take possible inference attacks into consideration. The model parameters may also expose sensitive information about the training data. One can adopt differential privacy [60, 40, 130] to inject random noises into the parameters or use SMC [22, 72, 23] to exchanged encrypted parameters. If the manager cannot be trusted at all, then we can use trusted execution environments [37] to execute the code in the manager. Blockchain is also an option to play the role as a manager [93].

5.3 Efficiency

Efficiency is an important factor in the success of many existing systems such as XGBoost [34] and ThunderSVM [198]. Since federated learning involves multi-rounds training and communication, the computation and communication costs may be large, which increases the threshold of usage of FLSs. To

表2：现有FLS之间的比较。本表中使用的符号与表1相同。如果系统不支持相应的功能，则该单元格为空。FedML 没有发布版本。

		FATE1.5.0	TFF 0.17.0	PySyft 0.3.0	PaddleFL 1.1.0	FedML
操作系统	Mac	✓	✓	✓	✓	✓
	Linux	3	3	3	3	
	Windows	3	3	3		
	iOS	3				
	Android	3				
数据划分	水平	3	3	3	3	3
	垂直	3	3	3		
模型	NN	✓	✓	✓	✓	
	DT	3				
	LM	✓	✓	✓	✓	
隐私机制	DP	✓	✓	✓		
	CM	✓	✓	✓		
通信	模拟	3	3	3	3	
	分布	3	3	3	3	
HARDWARE	CPU	✓	✓	✓	✓	
	GPU	3	3	3		

5 系统设计

图8显示了FLS设计中需要考虑的因素。有效性、效率和隐私性是联邦学习系统的三个重要指标，也是联邦学习的主要研究方向。受联邦数据库[166]的启发，我们还考虑了自治，这是使FLS实用所必需的。接下来，我们将详细解释这些因素。

5.1 有效性

FLS的核心是一个（多个）有效的算法（算法）。为了从表1所示的大量现有研究中确定要实现的算法，我们应该首先检查各方的数据划分。如果各方具有相同的特征但样本不同，则可以使用FedAvg [129]用于NN，SimFL [104]用于树。如果各方具有相同的样本空间但具有不同的特征，则可以使用FedBCD [120]用于NN，并使用SecureBoost [38]用于树。

5.2 隐私

FLS的一个重要要求是保护用户隐私。在这里，我们分析经理的可靠性。如果经理是诚实的，不好奇，那么我们不需要采用任何额外的技术，因为FL框架确保原始数据不会被交换。如果管理者诚实但好奇，那么我们必须考虑可能的推理攻击。模型参数还可以暴露关于训练数据的敏感信息。可以采用差分隐私[60，40，130]来向参数中注入随机噪声，或者使用SMC [22，72，23]来交换加密参数。如果管理器根本不可信，那么我们可以使用可信执行环境[37]来执行管理器中的代码。区块链也是扮演管理者角色的一种选择[93]。

5.3 效率

效率是许多现有系统（如XGBoost [34]和ThunderSVM [198]）成功的重要因素。由于联邦学习涉及多轮训练和通信，计算和通信成本可能很大，这增加了FLS的使用阈值。到

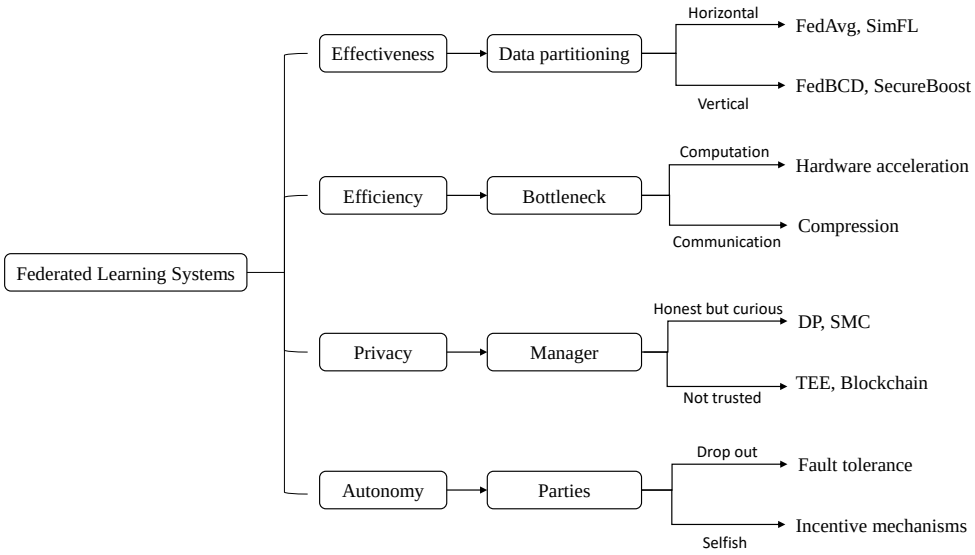


Figure 8: The design factors of FLSs

increase the efficiency, the most effective way is to deal with the bottleneck. If the bottleneck lies in the computation, we can use powerful hardware such as GPUs [42] and TPUs [83]. If the bottleneck lies in the communication, the compression techniques [18, 95, 164] can be applied to reduce the communication size.

5.4 Autonomy

Like federated databases [166], a practical FLS has to consider the autonomy of the parties. The parties may drop out (e.g., network failure) during the FL process, especially in the cross-device setting where the scale is large and the parties are unreliable [85]. Thus, the FLS should be robust and stable, which can tolerate the failure of parties or reduce the number of failure cases. Google has developed a practical FLS [24]. In their system, they monitor devices' health statistics to avoid wasting devices' battery or bandwidth. Also, the system will complete the current round or restart from the results of the previously committed round if there are failures. Zhang et al. [214] propose a blockchain-based approach to detect the device disconnection. Robust secure aggregation [17] is applicable to protect the communicated message in case of party drop out. Besides the disconnection issues, the parties may be selfish and are not willing to share the model with good quality. Incentive mechanisms [87, 88] can encourage the participation of the parties and improve the final model quality.

5.5 The Design Reference

Based on our taxonomy shown in Section 3 and the design factors shown in Figure 8, we derive a simple design reference for developing an FLS.

The first step is to identity the participated entities and the task, which significantly influence the system design. The participated entities determines the communication architecture, the data partitioning and the scale of federation. The task determines the suitable machine learning models to train. Then, we can choose or design a suitable FL algorithm according to the above attributes and Table 1. After fixing the FL algorithm, to satisfy the privacy requirements, we may determine the privacy mechanisms to protect the communicated messages. DP is preferred if efficiency is more important than model performance compared with SMC. Last, incentive mechanism can be considered to enhance the system. Existing systems [74, 24] usually do not support incentive mechanisms. However, incentive mechanisms can encourage the parties to participate and contribute in the system and make the system more attractive. Shapley value [193, 187] is a fair approach that can be considered.

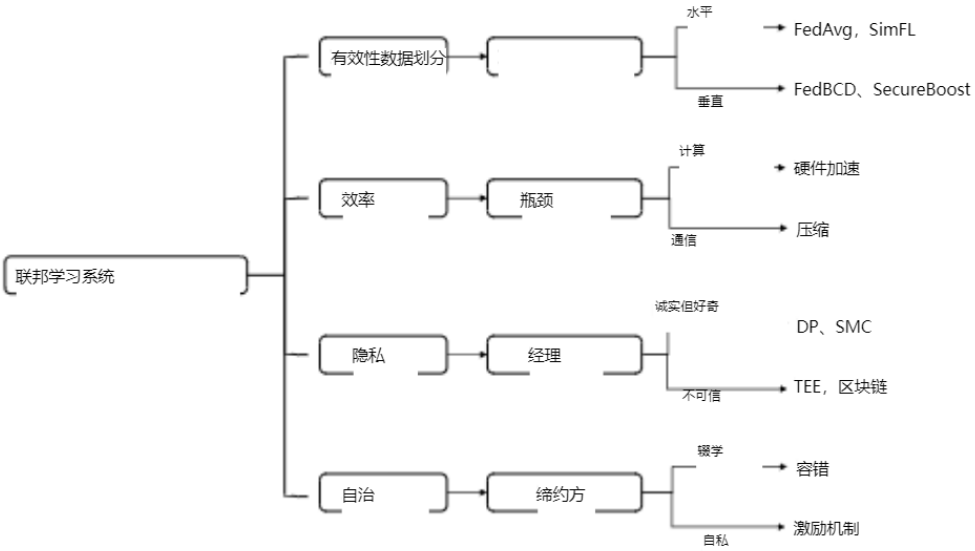


图8： FLS的设计因素

要提高效率，最有效的办法就是解决瓶颈。如果瓶颈在于计算，我们可以使用强大的硬件，如GPU [42]和TPU [83]。如果瓶颈在于通信，则可以应用压缩技术[18，95，164]来减小通信大小。

5.4 自治

像联邦数据库[166]一样，实际的FLS必须考虑各方的自治。当事人可以退出（例如，网络故障），特别是在规模大且各方不可靠的跨设备设置中[85]。因此，FLS应该是健壮和稳定的，可以容忍各方的失败或减少失败的情况下的数量。Google 开发了一个实用的FLS [24]。在他们的系统中，他们监控设备的健康统计数据，以避免浪费设备的电池或带宽。此外，系统将完成当前回合，或者如果存在失败，则从先前提交的回合的结果重新启动。Zhang 等人。[214]提出了一种基于区块链的方法来检测设备断开。鲁棒安全聚合[17]适用于在一方退出的情况下保护所传递的消息。除了断开连接的问题，各方可能是自私的，不愿意共享高质量的模型。 激励机制[87，88]可以鼓励各方参与，提高最终模型质量。

5.5 设计基准

基于第3节中所示的分类法和图8中所示的设计因素，我们推导出一个用于开发FLS的简单设计参考。

第一步是识别参与实体和任务，这对系统设计有重要影响。参与的实体决定了通信结构、数据划分和联邦规模。该任务确定要训练的合适的机器学习模型。然后，我们可以根据上述属性和表1选择或设计合适的FL算法。在修正FL算法后，为了满足隐私要求，我们可以确定隐私机制来保护通信消息。与SMC相比，如果效率比模型性能更重要，则首选DP。最后，可以考虑建立激励机制来完善这一制度。现有的系统[74，24]通常不支持激励机制。然而，激励机制可以鼓励各方参与该系统并作出贡献，使该系统更具吸引力。

Shapley 值[193，187]是一种可以考虑的公平方法。

Table 3: Requirements of the real-world federated systems

System Aspect	Mobile Service	Healthcare	Financial
Data Partitioning	Horizontal Partitioning	Hybrid Partitioning	Vertical Partitioning
Machine Learning Model	No specific Models	No specific Models	No specific Models
Scale of Federations	Cross-device	Cross-silo	Cross-silo
Communication Architecture	Centralized	Distributed	Distributed
Privacy Mechanism	DP	DP/SMC	DP/SMC
Motivation of Federation	Incentive Motivated	Policy Motivated	Interest Motivated

For real-world applications of federated learning systems, please refer to Section 4 of the supplementary material.

5.6 Evaluation

The evaluation of FLSs is very challenging. According to our studied system factors, it has to cover the following aspects: (1) model performance, (2) system security, (3) system efficiency, and (4) system robustness.

For the evaluation of the model, there are two different settings. One is to evaluate the performance (e.g., prediction accuracy) of the final global model on a global dataset. The other one is to evaluate the performance of the final local models on the corresponding non-IID local datasets. The evaluation setting depends on the objective of FL, i.e., learn a global model or learn personalized local models.

While theoretical security/privacy guarantee is a good evaluation metric for system security, another way is to conduct membership inference attacks [167] or model inversion attacks [56] to test the system security. These attacks can be conducted in two ways: (1) white-box attack: the attacker has access to all the exchanged models during the FL process. (2) black-box attack: the attacker only has access to the final output model. The attack success ratio can be an evaluation metric for the system security.

The efficiency of the system includes two parts: computation efficiency and communication efficiency. An intuitive metric is the training time, including the computation and communication time. Note that FL is usually a multi-round process. Thus, for a fair comparison, one approach is to use time per round as a metric. Another approach is to record the time or round to achieve the same target performance [90, 107].

It is challenging to quantifying the robustness of an FLS. A possible solution is to use a similar metric as robust secure aggregation, i.e., the maximum number of disconnected parties that can tolerate during the FL process.

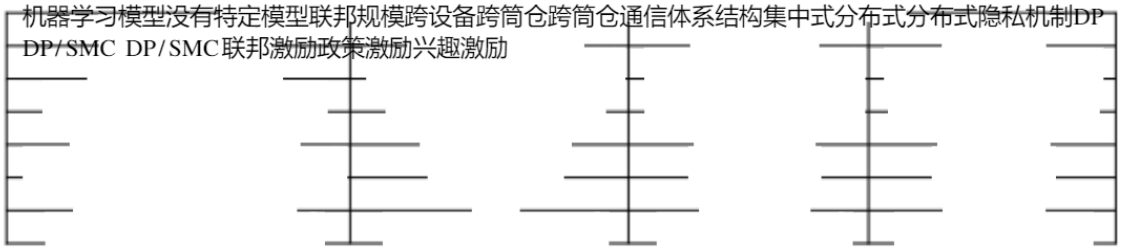
6 Case Study

In this section, we present several real-world applications of FL according to our taxonomy, as summarized in Table 3.

6.1 Mobile Service

There are many corporations providing predicting service to their mobile users, such as Google Keyboard [208], Apple's emoji suggestion and QuickType [179]. These services bring much convenience to the users. However, the training data come from users' edge devices, like smartphones. If the company collects data from all users and trains a global model, it might potentially cause privacy leakage. On the other hand, the data of each single user are insufficient to train an accurate prediction model. FL enables these companies to train an accuracy prediction model without accessing users' original data, which means protecting users' privacy. In the framework of FLSs, the users calculate and send their local models instead of their original data. That means a Google Keyboard user can enjoy an accurate prediction for the next word while not sharing his/her input history. If FLS can be widely applied to such prediction services, there will be much less data leakage since data are always stored in the edge.

表三：真实世界联邦系统的要求系统方面移动的服务医疗保健财务数据划分水平划分混合划分垂直划分机器学习模型没有特定模型联邦规模跨设备跨筒仓跨筒仓通信体系结构集中式分布式分布式隐私机制DP DP/SMC DP/SMC联邦激励政策激励兴趣激励



对于联邦学习系统的实际应用，请参阅补充材料的第4节。

5.6 评价

FLS的评价是非常具有挑战性的。根据我们所研究的系统因素，它必须涵盖以下几个方面：（1）模型性能，（2）系统安全性，（3）系统效率，（4）系统鲁棒性。

对于模型的评估，有两种不同的设置。一种是评估性能（例如，预测精度）。另一个是在相应的非IID局部数据集上评估最终局部模型的性能。评估设置取决于FL的目标，即，学习全局模型或学习个性化的局部模型。

虽然理论上的安全/隐私保证是系统安全性的一个很好的评估指标，但另一种方法是进行成员推断攻击[167]或模型反转攻击[56]来测试系统安全性。这些攻击可以通过两种方式进行：（1）白盒攻击：攻击者可以在FL过程中访问所有交换的模型。(2)黑盒攻击：攻击者只能访问最终的输出模型。攻击成功率可以作为系统安全性的评价指标。

系统的效率包括计算效率和通信效率两部分。一个直观的指标是训练时间，包括计算和通信时间。请注意，FL通常是一个多轮过程。因此，为了进行公平的比较，一种方法是使用每轮时间作为度量。另一种方法是记录达到相同目标性能的时间或轮次[90，107]。

量化FLS的鲁棒性具有挑战性。一种可能的解决方案是使用与鲁棒安全聚合类似的度量，即，在FL过程期间可以容忍的断开连接的方的最大数量。

6 案例研究

在本节中，我们将根据我们的分类法介绍FL的几个实际应用，如表3所示。

6.1 移动的服务

有许多公司为他们的移动的用户提供预测服务，例如Google Keyboard [208]，Apple 的emoji 建议和QuickType [179]。这些服务给用户带来了极大的方便。然而，训练数据来自用户的边缘设备，如智能手机。如果该公司收集所有用户的数据并训练一个全球模型，可能会导致隐私泄露。另一方面，单个用户的数据不足以训练准确的预测模型。FL使这些公司能够在不访问用户原始数据的情况下训练准确性预测模型，这意味着保护用户的隐私。在FLS框架中，用户计算并发送他们的本地模型，而不是他们的原始数据。这意味着谷歌键盘用户可以享受下一个单词的准确预测，而不分享他/她的输入历史。 如果FLS可以广泛应用于这样的预测服务，将有更少的数据泄漏，因为数据总是存储在边缘。

In such a scenario, data are usually horizontally split into millions of devices. Hence, the limitation of single device computational resource and the bandwidth are two major problems. Besides, the robustness of the system should also be considered since a user could join or leave the system at anytime. In other words, a centralized, cross-device FLS on horizontal data should be designed for such prediction services.

Although the basic framework of an FLS can have somehow protected individuals' privacy, it may not be secure against inference attacks [167]. Some additional privacy mechanisms like differential privacy should be leveraged to ensure the indistinguishability of individuals. Here secure multi-party computation may not be appropriate since each device has a weak computation capacity and cannot afford expensive encryption operations. Apart from guaranteeing users' privacy, some incentive mechanisms should be developed to encourage users to contribute their data. In reality, these incentives could be vouchers or additional service.

6.2 Healthcare

Modern health systems require cooperation among research institutes, hospitals, and federal agencies to improve health care of the nation [57]. Moreover, collaborative research among countries is vital when facing global health emergencies, like COVID-19 [6]. These health systems mostly aim to train a model for the diagnosis of a disease. These models for diagnosis should be as accurate as possible. However, the information of patients are not allowed to transfer under some regulations such as GDPR [10]. The privacy of data is even more concerned in international collaboration. Without solving the privacy issue, the collaborative research could be stagnated, threatening the public health. The data privacy in such collaboration is largely based on confidentiality agreement. However, this solution is based on "trust", which is not reliable. FL makes the cooperation possible because it can ensure the privacy theoretically, which is provable and reliable. In this way, every hospital or institute only has to share local models to get an accurate model for diagnosis.

In such a scenario, the health care data is partitioned both horizontally and vertically: each party contains health data of residents for a specific purpose (e.g., patient treatment), but the features used in each party are diverse. The number of parties is limited and each party usually has plenty of computational resource. In other words, a private FLS on hybrid partitioned data is required. One of the most challenging problems is how to train the hybrid partitioned data. The design of the FLS could be more complicated than a simple horizontal system. In a federation of healthcare, there is probably no central server. So, another challenging part is the design of a decentralized FLS, which should also be robust against some dishonest or malicious parties. Moreover, the privacy concern can be solved by additional mechanisms like secure multi-party computation and differential privacy. The collaboration is largely motivated by regulations.

6.3 Finance

A federation of financial consists of banks, insurance companies, etc. They often hope to cooperate in daily financial operations. For example, some 'bad' users might pack back a loan in one back with the money borrowed from another bank. All the banks want to avoid such malicious behavior while not revealing other customers' information. Also, insurance companies also want to learn from the banks about the reputation of customers. However, a leakage of 'good' customers' information may cause loss of interest or some legal issues.

This kind of cooperation can happen if we have a trusted third party, like the government. However, in many cases, the government is not involved in the federation or the government is not always trusted. So, an FLS with privacy mechanisms can be introduced. In the FLS, the privacy of each bank can be guaranteed by theoretical proved privacy mechanisms.

In such a scenario, financial data are often vertically partitioned, linked by user ID. Training a classifier in vertically partitioned data is quite challenging. Generally, the training process can be divided into two parts: privacy-preserving record linkage [183] and vertical federated training. The first part aims to find links between vertical partitioned data, and it has been well studied. The second part aims to train the

在这种情况下，数据通常被水平拆分到数百万台设备中。因此，单台设备计算资源和带宽的限制是两个主要问题。此外，由于用户可以随时加入或离开系统，因此还应考虑系统的鲁棒性。换句话说，应该为这样的预测服务设计水平数据上的集中式跨设备FLS。

虽然FLS的基本框架可以以某种方式保护个人隐私，但它可能无法抵御推理攻击[167]。应该利用一些额外的隐私机制，如差异隐私，以确保个人的不可侵犯性。这里，安全多方计算可能不合适，因为每个设备具有弱计算能力并且不能负担昂贵的加密操作。除了保障用户的隐私外，还应制定一些激励机制，鼓励用户贡献其数据。实际上，这些激励措施可以是代金券或额外服务。

6.2医疗保健

现代卫生系统需要研究机构、医院和联邦机构之间的合作，以改善国家的卫生保健[57]。此外，在面临全球卫生紧急情况（如COVID-19）时，各国之间的合作研究至关重要[6]。这些卫生系统的主要目标是训练一个诊断疾病的模型。这些诊断模型应尽可能准确。然而，根据GDPR等法规，患者的信息不允许转移[10]。在国际合作中，数据的隐私性更受关注。如果不解决隐私问题，合作研究可能会停滞不前，威胁公众健康。这种合作中的数据隐私在很大程度上基于保密协议。但是，这种解决方案是建立在“信任”的基础上的，并不可靠。模糊逻辑在理论上可以保证用户的隐私，这是可证明的，也是可靠的。 通过这种方式，每个医院或研究所只需共享本地模型即可获得准确的诊断模型。

在这样的场景中，健康护理数据被水平地和垂直地分区：每一方包含用于特定目的的居民的健康数据（例如，患者治疗），但各方使用的功能各不相同。参与方的数量是有限的，而且每一方通常都有足够的计算资源。换句话说，需要混合分区数据上的私有FLS。其中最具挑战性的问题之一是如何训练混合分区数据。FLS的设计可能比简单的水平系统更复杂。在医疗保健联盟中，可能没有中央服务器。因此，另一个具有挑战性的部分是去中心化FLS的设计，它也应该对一些不诚实或恶意的方具有鲁棒性。此外，隐私问题可以通过安全多方计算和差分隐私等其他机制来解决。这种合作在很大程度上是由法规推动的。

6.3金融

金融联盟由银行、保险公司等组成，他们往往希望在日常金融业务中进行合作。例如，一些“坏”用户可能会将从另一家银行借来的钱打包回一笔贷款。所有银行都希望在不泄露其他客户信息的同时避免此类恶意行为。此外，保险公司也希望从银行了解客户的声誉。然而，“好”客户信息的泄露可能会导致利益损失或一些法律的问题。

如果我们有一个值得信赖的第三方，比如政府，这种合作就可能发生。然而，在许多情况下，政府并不参与联邦，或者政府并不总是受到信任。因此，可以引入具有隐私机制的FLS。在FLS中，每个银行的隐私可以通过理论上证明的隐私机制来保证。

在这种情况下，财务数据通常是垂直分区的，通过用户ID链接。在垂直分区的数据中训练分类器是非常具有挑战性的。通常，训练过程可以分为两部分：隐私保护记录链接[183]和垂直联邦训练。第一部分的目的是找到垂直分区数据之间的联系，它已经得到了很好的研究。第二部分旨在培养

linked data without sharing the original data of each party, which still remains a challenge. The cross-silo and decentralized setting are applied in this federation. Also, some privacy mechanisms should be adopted in this scenario and the participant can be motivated by interest.

7 Vision

In this section, we show interesting directions to work on in the future. Although some directions are already covered in existing studies introduced in Section 4, we believe they are important and provide more insights on them.

7.1 Heterogeneity

The heterogeneity of the parties is an important characteristic in FLSs. Basically, the parties can differ in the accessibility, privacy requirements, contribution to the federation, and reliability. Thus, it is important to consider such practical issues in FLSs.

Dynamic scheduling Due to the instability of the parties, the number of parties may not be fixed during the learning process. However, the number of parties is fixed in many existing studies and they do not consider the situations where there are entries of new parties or departures of the current parties. The system should support dynamic scheduling and have the ability to adjust its strategy when there is a change in the number of parties. There are some studies addressing this issue. For example, Google's system [24] can tolerate the drop-out of the devices. Also, the emergence of blockchain [223] can be an ideal and transparent platform for multi-party learning. However, to the best of our knowledge, there is no work that study a increasing number of parties during FL. In such a case, more attention may be paid to the later parties, as the current global model may have been welled trained on existing parties.

Diverse privacy restrictions Little work has considered the privacy heterogeneity of FLSs, where the parties have different privacy requirements. The existing systems adopt techniques to protect the model parameters or gradients for all the parties on the same level. However, the privacy restrictions of the parties usually differ in reality. It would be interesting to design an FLS which treats the parties differently according to their privacy restrictions. The learned model should have a better performance if we can maximize the utilization of data of each party while not violating their privacy restrictions. The heterogeneous differential privacy [9] may be useful in such settings, where users have different privacy attitudes and expectations.

Intelligent benefits

Intuitively, one party should gain more from the FLS if it contributes more information. Existing incentive mechanisms are mostly based on Shapley values [193, 187], the computation overhead is a major concern. A computation-efficient and fair incentive mechanism needs to be developed.

7.2 System Development

To boost the development of FLSs, besides the detailed algorithm design, we need to study from a high-level view.

System architecture Like the parameter server [76] in deep learning which controls the parameter synchronization, some common system architectures are needed to be investigated for FL. Although FedAvg is a widely used framework, the applicable scenarios are still limited. For example, while unsupervised learning [129, 107, 108] still adopt model averaging as the model aggregation method, which cannot work if the parties want to train heterogeneous models. We want a general system architecture, which provides many aggregation methods and learning algorithms for different settings.

Model market Model market [182] is a promising platform for model storing, sharing, and selling. An interesting idea is to use the model market for federated learning. The party can buy the models to conduct model aggregation locally. Moreover, it can contribute its models to the market with additional information such as the target task. Such a design introduces more flexibility to the federation and is

在不共享各方原始数据的情况下链接数据，这仍然是一个挑战。在此联邦中应用了跨竖井和分散式设置。此外，在这种情况下，应该采取一些隐私机制，参与者可以由利益驱动。

7愿景

在本节中，我们将展示未来工作的有趣方向。虽然第4节介绍的现有研究已经涵盖了一些方向，但我们认为它们很重要，并提供了更多的见解。

7.1异质性

参与方的异质性是FLS的一个重要特征。基本上，各方可以在可访问性、隐私要求、对联盟的贡献和可靠性方面有所不同。因此，在FLS中考虑这些实际问题很重要。

动态调度由于参与方的不稳定性，在学习过程中参与方的数量可能不是固定的。然而，在许多现有的研究中，缔约方的数量是固定的，它们没有考虑到新缔约方加入或现有缔约方离开的情况。该系统应该支持动态调度，并有能力调整其策略时，有一个在党的数量变化。有一些研究涉及这一问题。例如，Google的系统[24]可以容忍设备的丢失。此外，区块链的出现[223]可以成为多方学习的理想和透明的平台。然而，据我们所知，在FL期间没有研究越来越多的政党的工作。在这种情况下，可能会更多地关注后来的政党，因为当前的全球模型可能已经对现有政党进行了良好的训练。

多样的隐私限制很少有工作考虑FLS的隐私异质性，各方有不同的隐私要求。现有的系统采用技术来保护同一级别上的所有参与方的模型参数或梯度。然而，当事人的隐私限制在现实中通常是不同的。设计一个根据当事人的隐私限制对他们进行不同处理的财务和后勤系统将是很有意思的。如果我们能够最大限度地利用各方的数据，同时不违反他们的隐私限制，学习模型应该有更好的性能。异构差异隐私[9]可能在这样的设置中有用，其中用户具有不同的隐私态度和期望。

智能优势
直觉上，如果一方提供更多的信息，它将从FLS中获得更多的收益。现有的激励机制大多基于Shapley值[193，187]，计算开销是一个主要问题。需要开发一种计算效率高且公平的激励机制。

7.2系统开发

为了促进FLS的发展，除了详细的算法设计外，还需要从高层次的角度进行研究。系统架构与深度学习中控制参数同步的参数服务器[76]一样，FL需要研究一些常见的系统架构。虽然FedAvg是一个广泛使用的框架，但适用的场景仍然有限。例如，虽然无监督学习[129，107，108]仍然采用模型平均作为模型聚合方法，但如果各方想要训练异构模型，则无法工作。我们想要一个通用的系统架构，它为不同的设置提供了许多聚合方法和学习算法。

模型市场模型市场[182]是一个很有前途的模型存储、共享和销售平台。一个有趣的想法是使用模型市场进行联邦学习。该方可以购买模型以在本地进行模型聚合。此外，它可以将其模型与目标任务等其他信息一起贡献给市场。这种设计为联邦引入了更多的灵活性，

more acceptable for the organizations, since the FL just like several transactions. A well evaluation of the models is important in such systems. The incentive mechanisms may be helpful [201, 87, 88].

Benchmark As more FLSs are being developed, a benchmark with representative data sets and workloads is quite important to evaluate the existing systems and direct future development. Although there have been quite a few benchmarks [25, 77, 74], no benchmark has been widely used in the experiments of federated learning studies. We need a robust benchmark which has representative datasets and strict privacy evaluation. Also, comprehensive evaluation metric including model performance, system efficiency, system security, and system robustness is often ignored in existing benchmarks. The evaluation of model performance on non-IID datasets and system security under data pollution needs more investigation.

Data life cycles Learning is simply one aspects of a federated system. A data life cycle [151] consists of multiple stages including data creation, storage, use, share, archive and destroy. For the data security and privacy of the entire application, we need to invent new data life cycles under FL context. Although data sharing is clearly one of the focused stage, the design of FLSs also affects other stages. For example, data creation may help to prepare the data and features that are suitable for FL.

7.3 FL in Domains

Internet-of-thing Security and privacy issues have been a hot research area in fog computing and edge computing, due to the increasing deployment of Internet-of-thing applications. For more details, readers can refer to some recent surveys [172, 209, 135]. FL can be one potential approach in addressing the data privacy issues, while still offering reasonably good machine learning models [113, 138]. The additional key challenges come from the computation and energy constraints. The mechanisms of privacy and security introduces runtime overhead. For example, Jiang et al. [80] apply independent Gaussian random projection to improve the data privacy, and then the training of a deep network can be too costly. The authors need to develop a new resource scheduling algorithm to move the workload to the nodes with more computation power. Similar issues happen in other environments such as vehicle-to-vehicle networks [160].

Regulations While FL enables collaborative learning without exposing the raw data, it is still not clear how FL comply with the existing regulations. For example, GDPR proposes limitations on data transfer. Since the model and gradients are actually not safe enough, is such limitation still apply to the model or gradients? Also, the "right to explainability" is hard to execute since the global model is an averaging of the local models. The explainability of the FL models is an open problem [67, 161]. Moreover, if a user wants to delete its data, should the global model be retrained without the data [62]? There is still a gap between the FL techniques and the regulations in reality. We may expect the cooperation between the computer science community and the law community.

8 Conclusion

Many efforts have been devoted to developing federated learning systems (FLSs). A complete overview and summary for existing FLSs is important and meaningful. Inspired by the previous federated systems, we have shown that heterogeneity and autonomy are two important factors in the design of practical FLSs. Moreover, with six different aspects, we provide a comprehensive categorization for FLSs. Based on these aspects, we also present the comparison on features and designs among existing FLSs. More importantly, we have pointed out a number of opportunities, ranging from more benchmarks to integration of emerging platforms such as blockchain. FLSs will be an exciting research direction, which calls for the effort from machine learning, system and data privacy communities.

Acknowledgement

This work is supported by a MoE AcRF Tier 1 grant (T1 251RES1824), an SenseTime Young Scholars Research Fund, and a MOE Tier 2 grant (MOE2017-T2-1-122) in Singapore.

更容易被组织接受，因为FL就像几个交易。在这样的系统中，对模型的良好评价是重要的。激励机制可能会有所帮助[201，87，88]。基准测试随着越来越多的FLS正在开发中，具有代表性的数据集和工作负载的基准测试对于评估现有系统和指导未来的开发非常重要。虽然有相当多的基准[25，77，74]，但没有基准广泛用于联邦学习研究的实验中。我们需要一个强大的基准，具有代表性的数据集和严格的隐私评估。现有的基准测试往往忽略了模型性能、系统效率、系统安全性和系统鲁棒性等综合评价指标。模型在非IID数据集上的性能评估和数据污染下的系统安全性需要进一步研究。数据生命周期学习只是联邦系统的一个方面。 数据生命周期[151]由多个阶段组成，包括数据创建、存储、使用、共享、存档和销毁。为了整个应用程序的数据安全和隐私，我们需要在FL上下文下发明新的数据生命周期。虽然数据共享显然是重点阶段之一，但FLS的设计也会影响其他阶段。例如，数据创建可以帮助准备适合FL的数据和特征。

7.3域中的FL

随着物联网应用的日益普及，安全和隐私问题成为雾计算和边缘计算领域的研究热点。有关更多详细信息，读者可以参考最近的一些调查[172，209，135]。FL可以成为解决数据隐私问题的一种潜在方法，同时仍然提供相当好的机器学习模型[113，138]。额外的关键挑战来自计算和能源限制。隐私和安全机制引入了运行时开销。例如，Jiang等人。[80]应用独立高斯随机投影来提高数据隐私，然后深度网络的训练成本太高。作者需要开发一种新的资源调度算法，将工作负载转移到具有更多计算能力的节点。类似的问题也发生在其他环境中，例如车对车网络[160]。

虽然FL可以在不暴露原始数据的情况下实现协作学习，但目前尚不清楚FL如何遵守现有法规。例如，GDPR提出了对数据传输的限制。由于模型和梯度实际上不够安全，这种限制是否仍然适用于模型或梯度？此外，“解释权”很难执行，因为全球模型是对局部模型的平均。FL模型的可解释性是一个悬而未决的问题[67，161]。此外，如果用户想要删除其数据，是否应该在没有数据的情况下重新训练全局模型[62]？外语教学技术与现实中的法规还存在一定的差距。我们可以期待计算机科学界和法律界之间的合作。

8结论

联邦学习系统（FLS）的开发已经投入了大量的努力。对现有的FLS进行全面的概述和总结是重要和有意义的。受以前联邦系统的启发，我们已经表明，异构性和自治性是两个重要的因素，在实际的FLS的设计。此外，从六个不同的方面，我们提供了一个全面的分类FLS。在此基础上，对现有的FLS在功能和设计上进行了比较.更重要的是，我们指出了一些机会，从更多的基准到区块链等新兴平台的整合。FLS将是一个令人兴奋的研究方向，需要机器学习，系统和数据隐私社区的努力。

确认

这项工作得到了莫伊AcRF Tier 1资助（T1 251 RES 1824）、商汤科技青年学者研究基金和新加坡MoE Tier 2资助（MOE 2017-T2-1-122）的支持。

References

[1] California Consumer Privacy Act Home Page. https://www.caprivacy.org/.

[2] URL https://www.intel.com/content/www/us/en/customer-spotlight/stories/ping-an-sgx-customer-story.html.

[3] Uber settles data breach investigation for $148 million, 2018. URL https://www.nytimes.com/2018/09/26/technology/uber-data-breach.html.

[4] Google is fined $57 million under europe's data privacy law, 2019. URL https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

[5] 2019 is a 'fine' year: Pdpc has fined s'pore firms a record $1.29m for data breaches, 2019. URL https://vulcanpost.com/676006/pdpc-data-breach-singapore-2019/.

[6] Rolling updates on coronavirus disease (covid-19), 2020. URL https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen.

[7] Martín Abadi, Paul Barham, Jianmin Chen, Zhifeng Chen, Andy Davis, Jeffrey Dean, Matthieu Devin, Sanjay Ghemawat, Geoffrey Irving, Michael Isard, et al. Tensorflow: A system for large-scale machine learning. In *12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16)*, pages 265–283, 2016.

[8] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 308–318. ACM, 2016.

[9] Mohammad Alaggan, Sébastien Gambs, and Anne-Marie Kermarrec. Heterogeneous differential privacy. *arXiv preprint arXiv:1504.06998*, 2015.

[10] Jan Philipp Albrecht. How the gdpr will change the world. *Eur. Data Prot. L. Rev.*, 2:287, 2016.

[11] Mohammed Aledhari, Rehma Razzak, Reza M Parizi, and Fahad Saeed. Federated learning: A survey on enabling technologies, protocols, and applications. *IEEE Access*, 8:140699–140725, 2020.

[12] Scott Alfeld, Xiaojin Zhu, and Paul Barford. Data poisoning attacks against autoregressive models. In *Thirtieth AAAI Conference on Artificial Intelligence*, 2016.

[13] Eitan Altman, Konstantin Avrachenkov, and Andrey Garnaev. Generalized α-fair resource allocation in wireless networks. In *2008 47th IEEE Conference on Decision and Control*, pages 2414–2419. IEEE, 2008.

[14] Muhammad Ammad-ud din, Elena Ivannikova, Suleiman A Khan, Were Oyomno, Qiang Fu, Kuan Eeik Tan, and Adrian Flanagan. Federated collaborative filtering for privacy-preserving personalized recommendation system. *arXiv preprint arXiv:1901.09888*, 2019.

[15] Yoshinori Aono, Takuya Hayashi, Lihua Wang, Shiho Moriai, et al. Privacy-preserving deep learning via additively homomorphic encryption. *IEEE Transactions on Information Forensics and Security*, 13(5):1333–1345, 2018.

[16] Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. How to backdoor federated learning. In *International Conference on Artificial Intelligence and Statistics*, pages 2938–2948. PMLR, 2020.

[17] James Henry Bell, Kallista A Bonawitz, Adrià Gascón, Tancrède Lepoint, and Mariana Raykova. Secure single-server aggregation with (poly) logarithmic overhead. In *CCS*, 2020.

引用

[1]加州消费者隐私法主页。https://www.caprivacy.org/.

[2]网址https://www.intel.com/content/www/us/en/customer-spotlight/stories/ ping-an-sgx-customer-story.html。

[3]2018年，Uber以1.48亿美元的价格解决了数据泄露调查。网址：https://www.nytimes.com/2018/ 09/26/technology/uber-data-breach.html。

[4]根据2019年欧洲数据隐私法，谷歌被罚款5700万美元。网址https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html。

[5]2019年是“罚款”的一年：Pdpc已对2019年数据泄露的公司处以创纪录的129万美元罚款。网址https://vulcanpost.com/676006/pdpc-data-breach-singapore-2019/。

[6]2020年冠状病毒病（COVID-19）滚动更新。网址https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen.

[7]Mart 'ın Abadi，Paul Barham，Jianmin Chen，Zhifeng Chen，Andy Davis，Jeffrey Dean，Matthieu迪文，Sanjay Ghemawat，Geoffrey欧文，Michael Isard，et al. Tensorflow：A system for

大规模机器学习在第12届{USENIX}操作系统设计和实现研讨会（{OSDI} 16），第265-283页，2016年。

[8]Martin Abadi、Andy Chu、Ian Goodfellow、H Brendan McMahan、Ilya Mironov、Kunal Talwar和Li Zhang。深度学习与差分隐私2016年ACM SIGSAC计算机和通信安全会议论文集，第308-318页。ACM，2016.

[9]Mohammad Alaggan、S'ebastien Gambs和Anne-Marie Kermarrec。异构差异隐私。arXiv预印本arXiv：1504.06998，2015年。

[10]简·菲利普·阿尔布莱希特。gdpr将如何改变世界。EUR.数据保护L.版本号：2：287，2016.

[11]Mohammed Aledhari，Rezma Razzak，Reza M Parizi，and Fahad Saeed.联邦学习：A调查使能技术、协议和应用。IEEE Access，8：140699-140725，2020。

[12]Scott Alfeld，Xiaojin Zhu，and Paul Barford.针对自回归模型的数据中毒攻击。在2016年第三十届AAAI人工智能会议上。

[13]Eitan Altman，Konstantin Avrachenkov，and Andrey Garnaev.广义α-公平资源分配在无线网络中。2008年第47届IEEE决策与控制会议，第2414-2419页。IEEE，2008年。

[14]Muhammad Ammad-ud din、Elena Ivannikova、Suleiman A Khan、Were Oyomno、强富、Kuan Eeik Tan和Adrian Flanagan。隐私保护个性化推荐系统中的联邦协同过滤。arXiv预印本arXiv：1901.09888，2019。

[15]Yoshinori Aono，Takuya Hayashi，Lihua Wang，Shiho Moriai，et al.通过加法同态加密学习。IEEE Transactions on Information Forensics and Security，13（5）：1333-1345，2018。

[16]尤金·巴格达萨良、安德烈亚斯·维特、华毅青、黛博拉·埃斯特林和维塔利·什马提科夫。如何后门联邦学习在人工智能和统计国际会议上，第2938-2948页。PMLR，2020年。

[17]詹姆斯亨利贝尔，卡利斯塔A博纳维茨，阿德里阿加森，坦克尔德莱波因特和玛丽安娜雷科娃。安全的单服务器聚合与（聚）对数开销。在CCS，2020年。

[18] Jeremy Bernstein, Yu-Xiang Wang, Kamyar Azizzadenesheli, and Anima Anandkumar. signsgd: Compressed optimisation for non-convex problems. *arXiv preprint arXiv:1802.04434*, 2018.

[19] Arjun Nitin Bhagoji, Supriyo Chakraborty, Prateek Mittal, and Seraphin Calo. Analyzing federated learning through an adversarial lens, 2018.

[20] Abhishek Bhowmick, John Duchi, Julien Freudiger, Gaurav Kapoor, and Ryan Rogers. Protection against reconstruction and its applications in private federated learning. *arXiv preprint arXiv:1812.00984*, 2018.

[21] Peva Blanchard, Rachid Guerraoui, Julien Stainer, et al. Machine learning with adversaries: Byzantine tolerant gradient descent. In *Advances in Neural Information Processing Systems*, pages 119–129, 2017.

[22] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. Practical secure aggregation for federated learning on user-held data. *arXiv preprint arXiv:1611.04482*, 2016.

[23] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. Practical secure aggregation for privacy-preserving machine learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1175–1191. ACM, 2017.

[24] Keith Bonawitz, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingerman, Vladimir Ivanov, Chloe Kiddon, Jakub Konecny, Stefano Mazzocchi, H Brendan McMahan, et al. Towards federated learning at scale: System design. *arXiv preprint arXiv:1902.01046*, 2019.

[25] Sebastian Caldas, Peter Wu, Tian Li, Jakub Konečnỳ, H Brendan McMahan, Virginia Smith, and Ameet Talwalkar. Leaf: A benchmark for federated settings. *arXiv preprint arXiv:1812.01097*, 2018.

[26] Rich Caruana. Multitask learning. *Machine learning*, 28(1):41–75, 1997.

[27] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In *OSDI*, volume 99, pages 173–186, 1999.

[28] Hervé Chabanne, Amaury de Wargny, Jonathan Milgram, Constance Morel, and Emmanuel Prouff. Privacy-preserving classification on deep neural network. *IACR Cryptology ePrint Archive*, 2017: 35, 2017.

[29] Di Chai, Leye Wang, Kai Chen, and Qiang Yang. Secure federated matrix factorization. *arXiv preprint arXiv:1906.05108*, 2019.

[30] Di Chai, Leye Wang, Kai Chen, and Qiang Yang. Fedeval: A benchmark system with a comprehensive evaluation model for federated learning. *arXiv preprint arXiv:2011.09655*, 2020.

[31] Kamalika Chaudhuri, Claire Monteleoni, and Anand D Sarwate. Differentially private empirical risk minimization. *Journal of Machine Learning Research*, 12(Mar):1069–1109, 2011.

[32] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of cryptology*, 1(1):65–75, 1988.

[33] Fei Chen, Zhenhua Dong, Zhenguo Li, and Xiuqiang He. Federated meta-learning for recommendation. *arXiv preprint arXiv:1802.07876*, 2018.

[34] Tianqi Chen and Carlos Guestrin. Xgboost: A scalable tree boosting system. In *KDD*, pages 785–794. ACM, 2016.

[18]Jeremy伯恩斯坦，Yu-Xiang Wang，Kamyar Azizzadenesheli和Anima Anandkumar。signsgd：非凸问题的压缩优化。arXiv预印本arXiv：1802.04434，2018。

[19]Arjun Nitin Bhagoji，Supriyo Chakraborty，Prateek Mittal和Seraphin Calo。通过对抗透镜分析联邦学习，2018年。

[20]Abhishek Bhowmick，John Duchi，Julien Freudiger，Gaurav Kapoor，and Ryan Rogers.亲-防止重构及其在私有联邦学习中的应用。arXiv预印本arXiv：1812.00984，2018。

[21]Peva Blanchard，Rachid Guerraoui，Julien Stainer等人。拜占庭容忍梯度下降。神经信息处理系统的进展，第119-129页，2017年。

[22]基思博纳维茨，弗拉基米尔伊万诺夫，本克罗伊特，安东尼奥Marcedone，H布伦丹McMahan，萨瓦尔帕特尔、丹尼尔·拉梅奇、亚伦·西格尔和卡恩·赛斯。对用户持有的数据进行联邦学习的实用安全聚合。arXiv预印本arXiv：1611.04482，2016。

[23]基思博纳维茨，弗拉基米尔伊万诺夫，本克罗伊特，安东尼奥Marcedone，H布伦丹McMahan，萨瓦尔帕特尔、丹尼尔·拉梅奇、亚伦·西格尔和卡恩·赛斯。实用的安全聚合隐私-保留机器学习。2017年ACM SIGSAC计算机和通信安全会议论文集，第1175-1191页。ACM，2017年。

[24]基思博纳维茨、休伯特·艾希纳、沃尔夫冈·格里斯坎普、德米特里·胡巴、亚历克斯·英格曼、弗拉基米尔Ivanov，Chloe Kiddon，Jakub Konecny，Stefano Mazzocchi，H Brendan McMahan，et al. Towards federated learning at scale：System design. arXiv预印本arXiv：1902.01046，2019。

[25]塞巴斯蒂安卡尔达斯，吴彼得，李田，雅各布Kone Eschercn'y，H布伦丹McMahan，弗吉尼亚史密斯，和阿梅特·塔尔沃卡Leaf：联邦设置的基准。arXiv预印本arXiv：1812.01097，2018。

[26]瑞奇·卡鲁阿纳多任务学习。机器学习，28（1）：41-75，1997年。

[27]Miguel Castro，Barbara Liskov，et al. Practical Byzantine Fault Tolerance. OSDI，第99卷，第173-186页，1999年。

[28]Herv 'e Chabanne，Amaury de Wargny，Jonathan Milgram，Constance Morel和Emmanuel Prouff。深度神经网络上的隐私保护分类。IACR Cryptology ePrint Archive，2017：35，2017.

[29]柴迪，王乐也，陈凯，杨强。安全联邦矩阵分解。arXiv预印本arXiv：1906.05108，2019。

[30]柴迪，王乐也，陈凯，杨强。Fedeval：一个具有联邦学习综合评估模型的基准系统。arXiv预印本arXiv：2011.09655，2020。

[31]Kamalika Chaudhuri，Claire Monteleoni和Anand D Sarwate。微分私人经验风险最小化。Journal of Machine Learning Research，12（Mar）：1069-1109，2011。

[32]大卫·乔姆。用餐密码问题：无条件发送者和接收者不可追踪性。Journal of cryptology，1（1）：65-75，1988.

[33]陈飞，董振华，李振国，何秀强。用于推荐的联邦元学习。arXiv预印本arXiv：1802.07876，2018。

[34]陈天奇和卡洛斯. Xgboost：一个可扩展的树提升系统。在KDD中，第785-794页。ACM，2016.

[35] Xinyun Chen, Chang Liu, Bo Li, Kimberly Lu, and Dawn Song. Targeted backdoor attacks on deep learning systems using data poisoning. *arXiv preprint arXiv:1712.05526*, 2017.

[36] Yi-Ruei Chen, Amir Rezapour, and Wen-Guey Tzeng. Privacy-preserving ridge regression on distributed data. *Information Sciences*, 451:34–49, 2018.

[37] Yu Chen, Fang Luo, Tong Li, Tao Xiang, Zheli Liu, and Jin Li. A training-integrity privacy-preserving federated learning scheme with trusted execution environment. *Information Sciences*, 522:69–79, 2020.

[38] Kewei Cheng, Tao Fan, Yilun Jin, Yang Liu, Tianjian Chen, and Qiang Yang. Secureboost: A lossless federated learning framework. *arXiv preprint arXiv:1901.08755*, 2019.

[39] Warren B Chik. The singapore personal data protection act and an assessment of future trends in data privacy reform. *Computer Law & Security Review*, 29(5):554–575, 2013.

[40] Olivia Choudhury, Aris Gkoulalas-Divanis, Theodoros Salonidis, Issa Sylla, Yoonyoung Park, Grace Hsu, and Amar Das. Differential privacy-enabled federated learning for sensitive health data. *arXiv preprint arXiv:1910.02578*, 2019.

[41] Peter Christen. *Data matching: concepts and techniques for record linkage, entity resolution, and duplicate detection*. Springer Science & Business Media, 2012.

[42] Shane Cook. *CUDA programming: a developer's guide to parallel computing with GPUs*. Newnes, 2012.

[43] Luca Corinzia and Joachim M Buhmann. Variational federated multi-task learning. *arXiv preprint arXiv:1906.06268*, 2019.

[44] Zhongxiang Dai, Kian Hsiang Low, and Patrick Jaillet. Federated bayesian optimization via thompson sampling. *NeurIPS*, 2020.

[45] Mayur Datar, Nicole Immorlica, Piotr Indyk, and Vahab S Mirrokni. Locality-sensitive hashing scheme based on p-stable distributions. In *Proceedings of the twentieth annual symposium on Computational geometry*, pages 253–262. ACM, 2004.

[46] Canh T Dinh, Nguyen H Tran, and Tuan Dung Nguyen. Personalized federated learning with moreau envelopes. *arXiv preprint arXiv:2006.08848*, 2020.

[47] Moming Duan. Astraea: Self-balancing federated learning for improving classification accuracy of mobile deep learning applications. *arXiv preprint arXiv:1907.01132*, 2019.

[48] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*, pages 265–284. Springer, 2006.

[49] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.

[50] Khaled El Emam and Fida Kamal Dankar. Protecting privacy using k-anonymity. *Journal of the American Medical Informatics Association*, 15(5):627–637, 2008.

[51] Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer, and Robbert Van Renesse. Bitcoin-ng: A scalable blockchain protocol. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pages 45–59, Santa Clara, CA, March 2016. USENIX Association. ISBN 978-1-931971-29-4. URL https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal.

[35]陈欣云，刘畅，李波，陆君怡，宋黎明。使用数据中毒对深度学习系统进行针对性后门攻击。arXiv预印本arXiv：1712.05526，2017。

[36]Yi-Ruei Chen，Amir Rezapour，and Wen-Guey Tzeng.分布式数据上的隐私保护岭回归。信息科学，451：34-49，2018。

[37]雨晨，方罗，佟丽，陶香，刘哲利，金丽。一个培训-完整性隐私-
在可信的执行环境中维护联邦学习方案。信息科学，522：69-79，2020。

[38]程科伟，范涛，靳一伦，刘洋，陈天健，杨强。Secureboost：无损联邦学习框架。arXiv预印本arXiv：1901.08755，2019。

[39]沃伦B奇克。新加坡个人资料保护法及资料私隐改革未来趋势评估。Computer Law & Security Review，29（5）：554-575，2013.

[40]Olivia Choudhury，阿里斯Gkoulalas-Divanis，Theodoros Salonyoung，Issa Sylla，Yoonyoung Park，Grace Hsu，and Amar Das.针对敏感健康数据的差异隐私支持的联合学习。
arXiv预印本arXiv：1910.02578，2019。

[41]彼得·克里斯顿。数据匹配：记录链接、实体解析和重复检测的概念和技术。Springer Science & Business Media，2012.

[42]肖恩·库克CUDA编程：GPU并行计算开发者指南。纽恩斯，
2012.

[43]Luca Corinzia和Joachim M Buhmann.变分联邦多任务学习。arXiv预印本arXiv：1906.06268，2019。

[44]戴忠祥，刘建祥，帕特里克。基于汤普森抽样的联邦贝叶斯优化。NeurIPS，2020年。

[45]Mayur Datar，Nicole Immorlica，Piotr Indyk，and Vahab S Mirrokni.局部敏感哈希法

基于p-稳定分布。在第二十届计算几何年会论文集，第253-262页。ACM，2004年。

[46]Canh T Dinh，Nguyen H Tran，and Tuan Dung Nguyen.使用莫罗信封的个性化联邦学习。arXiv预印本arXiv：2006.08848，2020。

[47]段默明。Astraea：自平衡联邦学习，用于提高移动的深度学习应用程序的分类准确性。arXiv预印本arXiv：1907.01132，2019。

[48]Cynthia Dwork，Frank McSherry，Kobbi Nissim，and Adam Smith.在私人数据分析中校准噪声敏感度。密码学理论会议，第265-284页。施普林格，2006年。

[49]Cynthia Dwork，Aaron Roth，et al.《差分隐私的算法基础》。Foundations and Trends® in Theoretical Computer Science，9（3-4）：211-407，2014。

[50]Khaled El Emam和Fida Kamal Dankar使用k-anonymity保护隐私。Journal of the American Medical Informatics Association，15（5）：627-637，2008.

[51]Ittay Eyal，Adem Efe Gencer，Emin Gun Sirer，and Robbert货车Renesse. Bitcoin-ng：一个可扩展的

区块链协议。在第13届USENIX网络系统设计和实施研讨会（NSDI 16），第45-59页，圣克拉拉，加利福尼亚州，2016年3月。USENIX协会。ISBN 978-1931971-29-4。网址 https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal。

[52] Alireza Fallah, Aryan Mokhtari, and Asuman Ozdaglar. Personalized federated learning with theoretical guarantees: A model-agnostic meta-learning approach. *Advances in Neural Information Processing Systems*, 33, 2020.

[53] Minghong Fang, Xiaoyu Cao, Jinyuan Jia, and Neil Gong. Local model poisoning attacks to byzantine-robust federated learning. In *USENIX*, 2020.

[54] Ji Feng, Yang Yu, and Zhi-Hua Zhou. Multi-layered gradient boosting decision trees. In *Advances in neural information processing systems*, pages 3551–3561, 2018.

[55] Chelsea Finn, Pieter Abbeel, and Sergey Levine. Model-agnostic meta-learning for fast adaptation of deep networks. In *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pages 1126–1135. JMLR. org, 2017.

[56] Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1322–1333. ACM, 2015.

[57] Charles P Friedman, Adam K Wong, and David Blumenthal. Achieving a nationwide learning health system. *Science translational medicine*, 2(57):57cm29–57cm29, 2010.

[58] Jonas Geiping, Hartmut Bauermeister, Hannah Dröge, and Michael Moeller. Inverting gradients–how easy is it to break privacy in federated learning? *arXiv preprint arXiv:2003.14053*, 2020.

[59] Samuel J Gershman and David M Blei. A tutorial on bayesian nonparametric models. *Journal of Mathematical Psychology*, 56(1):1–12, 2012.

[60] Robin C Geyer, Tassilo Klein, and Moin Nabi. Differentially private federated learning: A client level perspective. *arXiv preprint arXiv:1712.07557*, 2017.

[61] Avishek Ghosh, Jichan Chung, Dong Yin, and Kannan Ramchandran. An efficient framework for clustered federated learning. *arXiv preprint arXiv:2006.04088*, 2020.

[62] Antonio Ginart, Melody Guan, Gregory Valiant, and James Y Zou. Making ai forget you: Data deletion in machine learning. In *Advances in Neural Information Processing Systems*, pages 3513–3526, 2019.

[63] Oded Goldreich. Secure multi-party computation. *Manuscript. Preliminary version*, 78, 1998.

[64] Slawomir Goryczka and Li Xiong. A comprehensive comparison of multiparty secure additions with differential privacy. *IEEE transactions on dependable and secure computing*, 14(5):463–477, 2015.

[65] Klaus Greff, Rupesh K Srivastava, Jan Koutník, Bas R Steunebrink, and Jürgen Schmidhuber. Lstm: A search space odyssey. *IEEE transactions on neural networks and learning systems*, 28 (10):2222–2232, 2016.

[66] Antonio Gulli and Sujit Pal. *Deep learning with Keras*. Packt Publishing Ltd, 2017.

[67] David Gunning. Explainable artificial intelligence (xai). *Defense Advanced Research Projects Agency (DARPA), nd Web*, 2, 2017.

[68] Filip Hanzely and Peter Richtárik. Federated learning of a mixture of global and local models. *arXiv preprint arXiv:2002.05516*, 2020.

[69] Filip Hanzely, Slavomír Hanzely, Samuel Horváth, and Peter Richtárik. Lower bounds and optimal algorithms for personalized federated learning. *arXiv preprint arXiv:2010.02372*, 2020.

[52]Alireza Fallah，Aryan Mokhtari，and Asuman Ozdaglar.个性化联邦学习，
理论保证：模型不可知的元学习方法。神经信息处理系统的进展，33，2020。

[53]Minghong Fang，Xiaoyu Cao，Jinyuan Jia，and Neil Gong.局部模型中毒攻击对拜占庭联邦学习的鲁棒性。在USENIX，2020年。

[54]季风，杨宇，周志华。多层梯度提升决策树。神经信息处理系统的进展，第3551-3561页，2018年。

[55]Chelsea Finn Pieter Abbeel和Sergey Levine用于快速适应的模型不可知元学习

深度网络。第34届国际机器学习会议论文集第70卷，第1126-1135页。JMLR。org，2017.

[56]Matt Fredrikson，Somesh Jha，和托马斯Ristenpart.模型反转攻击利用
信心信息和基本对策。第22届ACM SIGSAC计算机和通信安全会议论文集，第1322-1333页。ACM，2015.

[57]查尔斯·P·弗里德曼亚当·K·王和大卫布卢门塔尔。建立一个全国性的学习保健系统。Science translational medicine，2（57）：57cm29-57cm29，2010.

[58]Jonas Geiping，Hartmut Bauermeister，Hannah Dr？oge，and Michael Moeller.反向梯度-在联邦学习中打破隐私有多容易？arXiv预印本arXiv：2003.14053，2020。

[59]Samuel J Gershman和大卫M Blei。一个关于baidu非参数模型的教程。Journal of Mathematical Psychology，56（1）：1-12，2012.

[60]Robin C盖耶，Tassilo Klein和Moin Nabi。差异化私有联邦学习：客户端层面的视角。arXiv预印本arXiv：1712.07557，2017。

[61]Avishek Ghosh，Jichan Chung，Dong Yin，and Kannan Ramchandran.一个有效的集群联邦学习框架。arXiv预印本arXiv：2006.04088，2020。

[62]Antonio Ginart，Melody Guan，Gregory Valiant和James Y Zou。Making ai forget you：2013

机器学习中的删除神经信息处理系统的进展，第3513-3526页，2019年。

[63]奥德·戈德赖希安全多方计算。曼恩角初版，78，1998年。

[64]Slawomir Goryczka和李雄。多方安全添加的全面比较
不同的隐私。IEEE Transactions on Reliable and Secure Computing，14（5）：463-477，2015。

[65]Klaus Greff，Rupesh K Srivastava，Jan Koutn 'ık，Bas R Steunebrink和J urgen Schmidhuber。Lstm：搜索空间奥德赛。IEEE transactions on neural networks and learning systems，28（10）：2222-2232，2016。

[66]Antonio Gulli和Sujit使用Keras进行深度学习。Packt Publishing Ltd，2017.

[67]大卫甘宁。可解释人工智能（XAI）。国防高级研究计划局（DARPA），nd Web，2017年2月。

[68]菲利普·汉兹利和彼得·里希特·阿里克。联合学习全局和局部模型的混合。
arXiv预印本arXiv：2002.05516，2020。

[69]菲利普·汉泽利、斯拉夫姆·汉泽利、塞缪尔·霍瓦特和彼得·里希特·阿里克。个性化联邦学习的下界和最优算法。arXiv预印本arXiv：2010.02372，2020。

[70] Tianshu Hao, Yunyou Huang, Xu Wen, Wanling Gao, Fan Zhang, Chen Zheng, Lei Wang, Hainan Ye, Kai Hwang, Zujie Ren, et al. Edge aibench: Towards comprehensive end-to-end edge computing benchmarking. *arXiv preprint arXiv:1908.01924*, 2019.

[71] Andrew Hard, Kanishka Rao, Rajiv Mathews, Françoise Beaufays, Sean Augenstein, Hubert Eichner, Chloé Kiddon, and Daniel Ramage. Federated learning for mobile keyboard prediction. *arXiv preprint arXiv:1811.03604*, 2018.

[72] Stephen Hardy, Wilko Henecka, Hamish Ivey-Law, Richard Nock, Giorgio Patrini, Guillaume Smith, and Brian Thorne. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. *arXiv preprint arXiv:1711.10677*, 2017.

[73] Chaoyang He, Murali Annavaram, and Salman Avestimehr. Group knowledge transfer: Federated learning of large cnns at the edge. *Advances in Neural Information Processing Systems*, 33, 2020.

[74] Chaoyang He, Songze Li, Jinhyun So, Mi Zhang, Hongyi Wang, Xiaoyang Wang, Praneeth Vepakomma, Abhishek Singh, Hang Qiu, Li Shen, et al. Fedml: A research library and benchmark for federated machine learning. *arXiv preprint arXiv:2007.13518*, 2020.

[75] Geoffrey Hinton, Oriol Vinyals, and Jeff Dean. Distilling the knowledge in a neural network. *arXiv preprint arXiv:1503.02531*, 2015.

[76] Qirong Ho, James Cipar, Henggang Cui, Seunghak Lee, Jin Kyu Kim, Phillip B Gibbons, Garth A Gibson, Greg Ganger, and Eric P Xing. More effective distributed ml via a stale synchronous parallel parameter server. In *Advances in neural information processing systems*, pages 1223–1231, 2013.

[77] Sixu Hu, Yuan Li, Xu Liu, Qinbin Li, Zhaomin Wu, and Bingsheng He. The oarf benchmark suite: Characterization and implications for federated learning systems. *arXiv preprint arXiv:2006.07856*, 2020.

[78] Yaochen Hu, Di Niu, Jianming Yang, and Shengping Zhou. Fdml: A collaborative machine learning framework for distributed features. In *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, pages 2232–2240, 2019.

[79] Eunjeong Jeong, Seungeun Oh, Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. Communication-efficient on-device machine learning: Federated distillation and augmentation under non-iid private data. *arXiv preprint arXiv:1811.11479*, 2018.

[80] Linshan Jiang, Rui Tan, Xin Lou, and Guosheng Lin. On lightweight privacy-preserving collaborative learning for internet-of-things objects. In *Proceedings of the International Conference on Internet of Things Design and Implementation*, IoTDI '19, pages 70–81, New York, NY, USA, 2019. ACM. ISBN 978-1-4503-6283-2. doi: 10.1145/3302505.3310070. URL http://doi.acm.org/10.1145/3302505.3310070.

[81] Yihan Jiang, Jakub Konečnỳ, Keith Rush, and Sreeram Kannan. Improving federated learning personalization via model agnostic meta learning. *arXiv preprint arXiv:1909.12488*, 2019.

[82] Rie Johnson and Tong Zhang. Accelerating stochastic gradient descent using predictive variance reduction. In *Advances in neural information processing systems*, pages 315–323, 2013.

[83] Norman P Jouppi, Cliff Young, Nishant Patil, David Patterson, Gaurav Agrawal, Raminder Bajwa, Sarah Bates, Suresh Bhatia, Nan Boden, Al Borchers, et al. In-datacenter performance analysis of a tensor processing unit. In *Proceedings of the 44th Annual International Symposium on Computer Architecture*, pages 1–12, 2017.

[70]Tianshu Hao，Yunyou Huang，Xu Wen，Wanling Gao，Fan Zhang，Chen Zheng，Lei Wang，Hainan Ye，Kai Hwang，Zujie Ren，et al. Edge aibench：Towards comprehensive end-to-end edge computing benchmarking. arXiv预印本arXiv：1908.01924，2019。

[71]Andrew Hard，Kanishka Rao，Rajiv马修斯，Franc Pastoise Beaufays，Sean Augenstein，Hubert 艾希纳，克洛伊·基登和丹尼尔·拉米奇。用于移动的键盘预测的联邦学习。arXiv预印本arXiv：1811.03604，2018。

[72]斯蒂芬哈代，威尔科·亨内卡，哈米什·艾维-劳，理查德·诺克，乔治·帕特里尼，纪尧姆史密斯和布莱恩·索恩。通过实体解析和加法同态加密对垂直分区数据进行私有联邦学习。arXiv预印本arXiv：1711.10677，2017。

[73]Chaoyang He，Murali Annavaram，and Salman Avestimehr.小组知识转移：联合在边缘学习大的cnn。神经信息处理系统的进展，33，2020。

[74]Chaoyang He，Songze Li，Jinhyun So，Mi Zhang，Hongyi Wang，Xiaoyang Wang，Praneeth Vepakomma，Abhishek Singh，Hang Qiu，Li Shen，et al. Fedml：A research library and benchmark for federated machine learning. arXiv预印本arXiv：2007.13518，2020。

[75]杰弗里欣顿，奥里尔Vinyals，和杰夫迪恩。在神经网络中提取知识。arXiv预印本arXiv：1503.02531，2015年。

[76]何启荣、James Cipar、Chenggang Cui、Seunhak Lee、Jin Kyu Kim、Phillip B Gibbons、Garth A.吉布森、格雷格·冈格尔和埃里克·P·邢。更有效的分布式ml通过陈旧的同步并行参数服务器。神经信息处理系统的进展，第1223-1231页，2013年。

[77]Sixu Hu，Yuan Li，Xu Liu，Qinbin Li，Zhaomin Wu，and Bingsheng He. oarf基准套件：联邦学习系统的特征和含义。arXiv预印本arXiv：2006.07856，2020。

[78]胡耀晨，牛迪，杨建明，周升平。FDML：一台协作机器分布式特征的学习框架。第25届ACM SIGKDD知识发现和数据挖掘国际会议论文集，第2232-2240页，2019年。

[79]Eunjeong Jeong、Heungeun Oh、Hyesung Kim、Jihong Park、Mehdi Bennis和Seong-Lyun Kim。通信高效的设备上机器学习：非iid私有数据下的联邦蒸馏和增强。arXiv预印本arXiv：1811.11479，2018。

[80]姜林山，谭锐，楼欣，林国胜。在轻量级隐私保护的col上，物联网对象的实验性学习。在物联网设计和实施国际会议论文集，IoTDI '19，第70-81页，纽约，纽约，美国，2019年。ACM。ISBN 978-1-4503-6283-2。doi：10.1145/3302505.3310070。网址http://doi.acm.org/10.1145/3302505.3310070。

[81]Yihan Jiang，Jakub Kone Ruscn `y，基思拉什，和Sreeram Kannan.通过模型不可知Meta学习改进联邦学习个性化。arXiv预印本arXiv：1909.12488，2019。

[82]李约翰逊和张彤。使用预测方差减少加速随机梯度下降。神经信息处理系统的进展，第315-323页，2013年。

[83]Norman P Jouwal，Cliff Young，Nishant Patil，大卫帕特森，Gaurav Agrawal，Raminder Bajwa，Sarah Bates，Suresh Bhatia，Nan博登，Al Borchers等人，张量处理单元的数据中心内性能分析。在Proceedings of the 44 th Annual International Symposium on Computer Architecture，第1-12页，2017年。

[84] R. Jurca and B. Faltings. An incentive compatible reputation mechanism. In *EEE International Conference on E-Commerce, 2003. CEC 2003.*, pages 285–292, June 2003. doi: 10.1109/COEC.2003.1210263.

[85] Peter Kairouz, H Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Keith Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, et al. Advances and open problems in federated learning. *arXiv preprint arXiv:1912.04977*, 2019.

[86] Georgios Kaissis, Alexander Ziller, Jonathan Passerat-Palmbach, Théo Ryffel, Dmitrii Usynin, Andrew Trask, Ionésio Lima, Jason Mancuso, Friederike Jungmann, Marc-Matthias Steinborn, et al. End-to-end privacy preserving deep learning on multi-institutional medical imaging. *Nature Machine Intelligence*, pages 1–12, 2021.

[87] Jiawen Kang, Zehui Xiong, Dusit Niyato, Shengli Xie, and Junshan Zhang. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. *IEEE Internet of Things Journal*, 2019.

[88] Jiawen Kang, Zehui Xiong, Dusit Niyato, Han Yu, Ying-Chang Liang, and Dong In Kim. Incentive design for efficient federated learning in mobile networks: A contract theory approach. *arXiv preprint arXiv:1905.07479*, 2019.

[89] Murat Kantarcioglu and Chris Clifton. Privacy-preserving distributed mining of association rules on horizontally partitioned data. *IEEE Transactions on Knowledge & Data Engineering*, (9): 1026–1037, 2004.

[90] Sai Praneeth Karimireddy, Satyen Kale, Mehryar Mohri, Sashank Reddi, Sebastian Stich, and Ananda Theertha Suresh. Scaffold: Stochastic controlled averaging for federated learning. In *International Conference on Machine Learning*, pages 5132–5143. PMLR, 2020.

[91] Alan F Karr, Xiaodong Lin, Ashish P Sanil, and Jerome P Reiter. Privacy-preserving analysis of vertically partitioned data using secure matrix products. *Journal of Official Statistics*, 25(1):125, 2009.

[92] Guolin Ke, Qi Meng, Thomas Finley, Taifeng Wang, Wei Chen, Weidong Ma, Qiwei Ye, and Tie-Yan Liu. Lightgbm: A highly efficient gradient boosting decision tree. In *NIPS*, 2017.

[93] Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. On-device federated learning via blockchain and its latency analysis. *arXiv preprint arXiv:1808.03949*, 2018.

[94] Jakub Konečnỳ, H Brendan McMahan, Daniel Ramage, and Peter Richtárik. Federated optimization: Distributed machine learning for on-device intelligence. *arXiv preprint arXiv:1610.02527*, 2016.

[95] Jakub Konečnỳ, H Brendan McMahan, Felix X Yu, Peter Richtárik, Ananda Theertha Suresh, and Dave Bacon. Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*, 2016.

[96] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. In *Advances in neural information processing systems*, pages 1097–1105, 2012.

[97] Tobias Kurze, Markus Klems, David Bermbach, Alexander Lenk, Stefan Tai, and Marcel Kunze. Cloud federation. *Cloud Computing*, 2011:32–38, 2011.

[98] David Leroy, Alice Coucke, Thibaut Lavril, Thibault Gisselbrecht, and Joseph Dureau. Federated learning for keyword spotting. In *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 6341–6345. IEEE, 2019.

[84]R. Jurca和B。费廷斯激励相容的声誉机制。国际贸易
电子商务会议，2003年。CEC 2003年，第285-292页，2003年6月。doi：10.1109/COEC。
2003.1210263.

[85]Peter Kairouz，H Brendan McMahan，Brendan Avent，Aur elien Bellet，Mehdi Bennis，Arjun Nitin Bhagoji，基思Bonawitz，Zachary Charles，Graham Cormode，Rachel Cummings等人，联邦学习的进展和开放问题。arXiv预印本arXiv：1912.04977，2019。

[86]Georgios Kaissis，Alexander Ziller，Jonathan Passerat—Palmbach，Th 'eo Ryffel，Dmitrii Usynin，Andrew Trask，Ion 'esio Lima，Jason Mancuso，Friederike Jungmann，Marc-Matthias Steinborn等人。多机构医学成像的端到端隐私保护深度学习。Nature Machine Intelligence，第1-12页，2021年。

[87]Jiawen Kang，Zehui Xiong，杜西特Niyato，Shengli Xie，and Junshan Zhang.激励机制
可靠的联邦学习：联合优化方法结合声誉和合同理论。IEEE Internet of Things Journal，2019。

[88]Jiawen Kang，Zehui Xiong，杜西特Niyato，Han Yu，Ying-Chang Liang，and Dong In Kim.激励移动的网络中高效联邦学习的设计：契约理论方法。arXiv预印本arXiv：1905.07479，2019。

[89]穆拉特坎塔奇奥卢和克里斯克利夫顿。隐私保护的分布式关联规则挖掘
水平分区的数据。IEEE Transactions on Knowledge & Data Engineering，（9）：1026-1037，2004.

[90]Sai Praneeth Karimireddy、Satyen Kale、Mehryar Mohri、Sashank Reddi、塞巴斯蒂安斯蒂奇和阿南达·瑟莎·苏雷什Scaffold：用于联邦学习的随机控制平均。国际机器学习会议，第5132-5143页。PMLR，2020年。

[91]Alan F Karr，Xiaodong Lin，Ashish P Sanil，and杰罗姆P Reiter.隐私保护分析
垂直分区的数据使用安全矩阵产品。官方统计杂志，25（1）：125，2009。

[92]Guolin Ke，Qi Meng，托马斯芬利，Taifeng Wang，Wei Chen，Weidong Ma，Qiwei Ye，and Tie-Yan Liu. Lightgbm：一个高效的梯度提升决策树。在NIPS，2017年。

[93]Hyesung Kim，Jihong Park，Mehdi Bennis，and Seong-Lyun Kim.通过区块链及其延迟分析的设备上联邦学习。arXiv预印本arXiv：1808.03949，2018。

[94]Jakub Kone Roccn 'y，H Brendan McMahan，丹尼尔Ramage和Peter Richt' arik。联邦优化：分布式机器学习，用于设备上的智能。arXiv预印本arXiv：1610.02527，2016。

[95]Jakub Kone Zagcn'y，H Brendan McMahan，Felix X Yu，Peter Richt 'arik，Ananda Theertha Suresh.
戴夫·培根联邦学习：提高沟通效率的策略。arXiv预印本arXiv：1610.05492，2016年。

[96]Alex Krizhevsky，Ilya Sutskever，and Geoffrey E欣顿. Imagenet分类与深
卷积神经网络神经信息处理系统的进展，第1097-1105页，2012年。

[97]Tobias Kurze，Markus Klems，David Bermbach，Alexander Lenk，Stefan Tai和Marcel Kunze。Cloud联邦云计算，2011：32—38，2011。

[98]大卫勒罗伊，爱丽丝Coucke，Thibaut Lavril，Thibault Gisselbrecht和约瑟夫Dureau。联邦学习关键词识别。在ICASSP 2019-2019 IEEE声学，语音和信号处理国际会议（ICASSP），第6341-6345页。IEEE，2019年。

[99] Bo Li, Yining Wang, Aarti Singh, and Yevgeniy Vorobeychik. Data poisoning attacks on factorization-based collaborative filtering. In *Advances in neural information processing systems*, pages 1885–1893, 2016.

[100] Liping Li, Wei Xu, Tianyi Chen, Georgios B Giannakis, and Qing Ling. Rsa: Byzantine-robust stochastic aggregation methods for distributed learning from heterogeneous datasets. In *AAAI*, 2019.

[101] Peilong Li, Yan Luo, Ning Zhang, and Yu Cao. Heterospark: A heterogeneous cpu/gpu spark platform for machine learning algorithms. In *2015 IEEE International Conference on Networking, Architecture and Storage (NAS)*, pages 347–348. IEEE, 2015.

[102] Qinbin Li, Zeyi Wen, and Bingsheng He. Adaptive kernel value caching for svm training. *IEEE transactions on neural networks and learning systems*, 2019.

[103] Qinbin Li, Bingsheng He, and Dawn Song. Model-agnostic round-optimal federated learning via knowledge transfer. *arXiv preprint arXiv:2010.01017*, 2020.

[104] Qinbin Li, Zeyi Wen, and Bingsheng He. Practical federated gradient boosting decision trees. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 34, pages 4642–4649, 2020.

[105] Qinbin Li, Zhaomin Wu, Zeyi Wen, and Bingsheng He. Privacy-preserving gradient boosting decision trees. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 34, pages 784–791, 2020.

[106] Qinbin Li, Yiqun Diao, Quan Chen, and Bingsheng He. Federated learning on non-iid data silos: An experimental study. *arXiv preprint arXiv:2102.02079*, 2021.

[107] Qinbin Li, Bingsheng He, and Dawn Song. Model-contrastive federated learning. In *CVPR*, 2021.

[108] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith. Federated optimization in heterogeneous networks. *arXiv preprint arXiv:1812.06127*, 2018.

[109] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. Federated learning: Challenges, methods, and future directions, 2019.

[110] Tian Li, Maziar Sanjabi, and Virginia Smith. Fair resource allocation in federated learning. *arXiv preprint arXiv:1905.10497*, 2019.

[111] Xiang Li, Kaixuan Huang, Wenhao Yang, Shusen Wang, and Zhihua Zhang. On the convergence of fedavg on non-iid data. *arXiv preprint arXiv:1907.02189*, 2019.

[112] Hans Albert Lianto, Yang Zhao, and Jun Zhao. Attacks to federated learning: Responsive web user interface to recover training data from user gradients. In *The ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2020.

[113] Wei Yang Bryan Lim, Nguyen Cong Luong, Dinh Thai Hoang, Yutao Jiao, Ying-Chang Liang, Qiang Yang, Dusit Niyato, and Chunyan Miao. Federated learning in mobile edge networks: A comprehensive survey, 2019.

[114] Tao Lin, Lingjing Kong, Sebastian U Stich, and Martin Jaggi. Ensemble distillation for robust model fusion in federated learning. *arXiv preprint arXiv:2006.07242*, 2020.

[115] Boyi Liu, Lujia Wang, Ming Liu, and Chengzhong Xu. Lifelong federated reinforcement learning: a learning architecture for navigation in cloud robotic systems. *arXiv preprint arXiv:1901.06455*, 2019.

[99]Bo Li，Yining Wang，Aarti Singh，and Yevgeniy Vorobeychik.数据中毒攻击
基于因子分解的协同过滤神经信息处理系统的进展，第1885-1893页，2016年。

[100]李丽萍，徐伟，陈天一，Georgios B Giannakis和Qing Ling。Rsa：拜占庭-鲁棒
从异构数据集进行分布式学习的随机聚合方法。在AAAI，2019年。

[101]李沛龙，罗燕，张凝，曹玉。Heterospark：一个异构的CPU/GPU火花
机器学习算法的平台。2015年IEEE网络、架构和存储国际会议（NAS），第347-348页。IEEE，
2015年。

[102]Qinbin Li，Zeyi Wen，and Bingsheng He.支持向量机训练的自适应核值缓存。IEEE
transactions on neural networks and learning systems，2019。

[103]Qinbin Li，Bingsheng He，and Dawn Song.通过知识转移的模型不可知轮最优联邦学习。arXiv
预印本arXiv：2010.01017，2020。

[104]Qinbin Li，Zeyi Wen，and Bingsheng He.实用的联邦梯度提升决策树。在
AAAI人工智能会议论文集，第34卷，第4642-4649页，2020年。

[105]Qinbin Li，Zhaomin Wu，Zeyi Wen，and Bingsheng He.隐私保护梯度提升
决策树在AAAI人工智能会议论文集，第34卷，第784-791页，2020年。

[106]Qinbin Li，Yiqun Diao，Quan Chen，and Bingsheng He.非iid数据孤岛上的联邦学习：一项实
验研究。arXiv预印本arXiv：2102.02079，2021。

[107]Qinbin Li，Bingsheng He，and Dawn Song.模型对比联邦学习。在CVPR，2021年。

[108]Tian Li，Anit Kumar Sahu，Manzil Zaheer，Maziar Sanjabi，Ameet Talwalkar，and Virginia
Smith.
异构网络中的联邦优化。arXiv预印本arXiv：1812.06127，2018。

[109]Tian Li，Anit Kumar Sahu，Ameet Talwalkar，and Virginia Smith.联邦学习：挑战，方法和未来
方向，2019年。

[110]Tian Li，Maziar Sanjabi，and Virginia Smith.联邦学习中的公平资源分配。arXiv预印本arXiv：
1905.10497，2019。

[111]Xiang Li，Kaixuan Huang，Wenhao Yang，Shusen Wang，and Zhihua Zhang.非独立同分布
数据下fedavg的收敛性。arXiv预印本arXiv：1907.02189，2019。

[112]Hans Albert Lianto，Yang Zhao，and Jun Zhao.对联邦学习的攻击：响应式Web用户
接口从用户梯度中恢复训练数据。2020年ACM亚洲计算机与通信安全会议（ASIACCS）

[113]Wei Yang Bryan Lim，Nguyen Cong Luong，Dinh Thai Hoang，Yutao Jiao，Ying-Chang Liang，
杨强、杜西特·尼亚托和苗春燕。移动的边缘网络中的联邦学习：2019年综合调查。

[114]林涛，孔玲静，塞巴斯蒂安U斯蒂奇和马丁·贾吉。联邦学习中鲁棒模型融合的包围蒸馏。arXiv预印
本arXiv：2006.07242，2020。

[115]Boyi Liu，Lujia Wang，Ming Liu，and Chengzhong Xu.终身联邦强化学习：
云机器人系统导航的学习架构。arXiv预印本arXiv：1901.06455，
2019.

[116] Jian Liu, Mika Juuti, Yao Lu, and Nadarajah Asokan. Oblivious neural network predictions via minionn transformations. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 619–631. ACM, 2017.

[117] Lifeng Liu, Fengda Zhang, Jun Xiao, and Chao Wu. Evaluation framework for large-scale federated learning. *arXiv preprint arXiv:2003.01575*, 2020.

[118] Lumin Liu, Jun Zhang, SH Song, and Khaled B Letaief. Edge-assisted hierarchical federated learning with non-iid data. *arXiv preprint arXiv:1905.06641*, 2019.

[119] Yang Liu, Tianjian Chen, and Qiang Yang. Secure federated transfer learning. *arXiv preprint arXiv:1812.03337*, 2018.

[120] Yang Liu, Yan Kang, Xinwei Zhang, Liping Li, Yong Cheng, Tianjian Chen, Mingyi Hong, and Qiang Yang. A communication efficient vertical federated learning framework. *arXiv preprint arXiv:1912.11187*, 2019.

[121] Yang Liu, Yingting Liu, Zhijie Liu, Junbo Zhang, Chuishi Meng, and Yu Zheng. Federated forest. *arXiv preprint arXiv:1905.10053*, 2019.

[122] Yang Liu, Zhuo Ma, Ximeng Liu, Siqi Ma, Surya Nepal, and Robert Deng. Boosting privately: Privacy-preserving federated extreme boosting for mobile crowdsensing. *arXiv preprint arXiv:1907.10218*, 2019.

[123] Noel Lopes and Bernardete Ribeiro. Gpumlib: An efficient open-source gpu machine learning library. *International Journal of Computer Information Systems and Industrial Management Applications*, 3:355–362, 2011.

[124] Jiahuan Luo, Xueyang Wu, Yun Luo, Anbu Huang, Yunfeng Huang, Yang Liu, and Qiang Yang. Real-world image datasets for federated learning. *arXiv preprint arXiv:1910.11089*, 2019.

[125] Lingjuan Lyu, Han Yu, and Qiang Yang. Threats to federated learning: A survey. *arXiv preprint arXiv:2003.02133*, 2020.

[126] Chenxin Ma, Jakub Konečnỳ, Martin Jaggi, Virginia Smith, Michael I Jordan, Peter Richtárik, and Martin Takáč. Distributed optimization with arbitrary local solvers. *optimization Methods and Software*, 32(4):813–848, 2017.

[127] Dhruv Mahajan, Ross Girshick, Vignesh Ramanathan, Kaiming He, Manohar Paluri, Yixuan Li, Ashwin Bharambe, and Laurens van der Maaten. Exploring the limits of weakly supervised pretraining. In *Proceedings of the European Conference on Computer Vision (ECCV)*, pages 181–196, 2018.

[128] Othmane Marfoq, Chuan Xu, Giovanni Neglia, and Richard Vidal. Throughput-optimal topology design for cross-silo federated learning. *arXiv preprint arXiv:2010.12229*, 2020.

[129] H Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, et al. Communication-efficient learning of deep networks from decentralized data. *arXiv preprint arXiv:1602.05629*, 2016.

[130] H Brendan McMahan, Daniel Ramage, Kunal Talwar, and Li Zhang. Learning differentially private recurrent language models. *arXiv preprint arXiv:1710.06963*, 2017.

[131] Luca Melis, Congzheng Song, Emiliano De Cristofaro, and Vitaly Shmatikov. Exploiting unintended feature leakage in collaborative learning. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 691–706. IEEE, 2019.

[132] El Mahdi El Mhamdi, Rachid Guerraoui, and Sébastien Rouault. The hidden vulnerability of distributed learning in byzantium. *arXiv preprint arXiv:1802.07927*, 2018.

[116]Jian Liu，Mika Juuti，Yao Lu，and Nadarajah Asokan.不经意的神经网络预测，minionn变换2017年ACM SIGSAC计算机和通信安全会议论文集，第619-631页。ACM，2017年。

[117]刘立峰，张丰达，肖军，吴超。大规模联邦学习的评估框架。arXiv预印本arXiv：2003.01575，2020。

[118]Lumin Liu，Jun Zhang，SH Song，and Khaled B Letaief.基于非iid数据的边辅助分层联邦学习。arXiv预印本arXiv：1905.06641，2019。

[119]杨柳、陈天健、杨强。安全联合迁移学习。arXiv预印arXiv：1812.03337，2018。

[120]杨柳、颜康、张新伟、李丽萍、勇成、陈天健、洪铭义、以及

杨强。一个通信高效的垂直联邦学习框架。arXiv预印本arXiv：1912.11187，2019。

[121]Yang Liu，Yingting Liu，Zhijie Liu，Junbo Zhang，Chuishi Meng，and Yu Zheng.联邦森林arXiv预印本arXiv：1905.10053，2019。

[122]Yang Liu，Zhuo Ma，Ximeng Liu，Siqi Ma，Surya Nepal，and Robert Deng.提升优先级-vately：用于移动的人群感知的隐私保护联合极端提升。arXiv预印本arXiv：1907.10218，2019。

[123]诺埃尔·洛佩斯和伯纳黛特·里贝罗Gpumlib：一个高效的开源GPU机器学习图书馆International Journal of Computer Information Systems and Industrial Management Applications，3：355-362，2011.

[124]嘉欢罗、雪阳吴、云罗、安布黄、云峰黄、杨柳、强阳。用于联邦学习的真实世界图像数据集。arXiv预印本arXiv：1910.11089，2019。

[125]Lingjuan Lyu，Han Yu，and Qiang Yang.联邦学习的威胁：一项调查。arXiv预印本arXiv：2003.02133，2020。

[126]Chenxin Ma，Jakub Kone Jagcn'y，Martin Jaggi，Virginia Smith，Michael I Jordan，Peter Richt 'arik，and

马丁·塔卡克。使用任意局部求解器的分布式优化。优化方法和软件，32（4）：813-848，2017。

[127]Dhruv Mahajan，Ross Girshick，Vignesh Ramanathan，Kaiming He，Manohar Paluri，Yixuan Li，Ashwin Bharambe，and Laurens货车der Maaten.探索弱监督预训练的局限性。在欧洲计算机视觉会议（ECCV）的会议记录中，第181-196页，2018年。

[128]Othmane Marfoq，Chuan Xu，Giovanni Neglia，and Richard Vidal.跨竖井联邦学习的最优拓扑设计。arXiv预印本arXiv：2010.12229，2020。

[129]H Brendan McMahan，Eider摩尔，丹尼尔Ramage，Seth Hampson等人。arXiv预印本arXiv：1602.05629，2016。

[130]H Brendan McMahan，丹尼尔Ramage，Kunal Talwar，和Li Zhang.学习差分私有递归语言模型。arXiv预印本arXiv：1710.06963，2017。

[131]Luca Melis，Congzheng Song，Emiliano De Cristofaro，and Vitaly Shmatikov.剥削工会-在协作学习中倾向于特征泄漏。2019年IEEE安全与隐私研讨会（SP），第691-706页。IEEE，2019年。

[132]El Mahdi El Mhamdi，Rachid Guerraoui和S'ebastien Rouault。拜占庭分布式学习中隐藏的脆弱性。arXiv预印本arXiv：1802.07927，2018。

[133] Volodymyr Mnih, Koray Kavukcuoglu, David Silver, Andrei A Rusu, Joel Veness, Marc G Bellemare, Alex Graves, Martin Riedmiller, Andreas K Fidjeland, Georg Ostrovski, et al. Human-level control through deep reinforcement learning. *Nature*, 518(7540):529–533, 2015.

[134] Mehryar Mohri, Gary Sivek, and Ananda Theertha Suresh. Agnostic federated learning. *arXiv preprint arXiv:1902.00146*, 2019.

[135] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar. Security and privacy in fog computing: Challenges. *IEEE Access*, 5:19293–19304, 2017. doi: 10.1109/ACCESS.2017.2749422.

[136] Moni Naor, Benny Pinkas, and Reuban Sumner. Privacy preserving auctions and mechanism design. In *Proceedings of the 1st ACM Conference on Electronic Commerce*, EC '99, pages 129–139, New York, NY, USA, 1999. ACM. ISBN 1-58113-176-3. doi: 10.1145/336992.337028. URL http://doi.acm.org/10.1145/336992.337028.

[137] Milad Nasr, Reza Shokri, and Amir Houmansadr. Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. In *Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks against Centralized and Federated Learning*, page 0. IEEE, 2019.

[138] Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, Hossein Fereidooni, N. Asokan, and Ahmad-Reza Sadeghi. DÏot: A federated self-learning anomaly detection system for iot, 2018.

[139] Alex Nichol and John Schulman. Reptile: a scalable metalearning algorithm. *arXiv preprint arXiv:1803.02999*, 2:2, 2018.

[140] Solmaz Niknam, Harpreet S Dhillon, and Jeffery H Reed. Federated learning for wireless communications: Motivation, opportunities and challenges. *arXiv preprint arXiv:1908.06847*, 2019.

[141] Valeria Nikolaenko, Udi Weinsberg, Stratis Ioannidis, Marc Joye, Dan Boneh, and Nina Taft. Privacy-preserving ridge regression on hundreds of millions of records. In *2013 IEEE Symposium on Security and Privacy*, pages 334–348. IEEE, 2013.

[142] Adrian Nilsson, Simon Smith, Gregor Ulm, Emil Gustavsson, and Mats Jirstrand. A performance evaluation of federated learning algorithms. In *Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning*, pages 1–8. ACM, 2018.

[143] Takayuki Nishio and Ryo Yonetani. Client selection for federated learning with heterogeneous resources in mobile edge. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pages 1–7. IEEE, 2019.

[144] Richard Nock, Stephen Hardy, Wilko Henecka, Hamish Ivey-Law, Giorgio Patrini, Guillaume Smith, and Brian Thorne. Entity resolution and federated learning get a federated resolution. *arXiv preprint arXiv:1803.04035*, 2018.

[145] Olga Ohrimenko, Felix Schuster, Cédric Fournet, Aastha Mehta, Sebastian Nowozin, Kapil Vaswani, and Manuel Costa. Oblivious multi-party machine learning on trusted processors. In *25th {USENIX} Security Symposium ({USENIX} Security 16)*, pages 619–636, 2016.

[146] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 223–238. Springer, 1999.

[147] Sinno Jialin Pan and Qiang Yang. A survey on transfer learning. *IEEE Transactions on knowledge and data engineering*, 22(10):1345–1359, 2010.

[133]Volodymyr Mnih，Koray Kavukcuoglu，大卫银，Andrei A Rusu，Joel Veness，Marc G Bellemare，Alex Graves，Martin Riedmiller，Andreas K Fidjeland，Georg Ostrovski等人通过深度强化学习进行人类水平控制。Nature，518（7540）：529-533，2015.

[134]Mehryar Mohri，加里Sivek，和Ananda Theertha Suresh。不可知的联邦学习。arXiv预印本arXiv：1902.00146，2019。

[135]M.穆克吉河马塔姆湖舒湖，加-地马格拉拉斯湾A. Ferrag，N. Choudhury，and V. Kumar. 雾计算中的安全和隐私：挑战。IEEE Access，5：19293-19304，2017。doi：10.1109/ACCESS.2017.2749422.

[136]莫妮·诺尔本尼·平卡斯和萨班·萨姆纳。隐私保护拍卖与机制设计。在第一届ACM电子商务会议的会议录，EC '99，第129-139页中，美国纽约州纽约，1999年。ACM。ISBN 1-58113-176-3。doi：10.1145/336992.337028。网址http://doi.acm.org/10.1145/336992.337028。

[137]Milad Nasr，Reza Shokri，and Amir Houmansadr.深度学习的全面隐私分析：针对集中式和联邦学习的被动和主动白盒推理攻击。在深度学习的全面隐私分析：针对集中式和联邦学习的被动和主动白盒推理攻击，第0页。IEEE，2019年。

[138]Thien Duc Nguyen，Samuel Marchal，Markus Miettinen，Hossein Fereidooni，N. Asokan和Ahmad-Reza Sadeghi。DÏot：物联网联合自学习异常检测系统，2018年。

[139]亚历克斯·尼科尔和约翰·舒尔曼爬虫：可扩展的元学习算法。arXiv预印本arXiv：1803.02999，2：2，2018。

[140]Solmaz Niknam，Harpreet S Dhillon，and Jeffery H Reed.无线通信的联合学习：动机、机遇和挑战。arXiv预印本arXiv：1908.06847，2019。

[141]Valeria Nikolaenko，Udi Weinsberg，Stratis Ioannyoung，Marc Joye，Dan Boneh，and Nina塔夫脱。隐私保护岭回归数亿条记录。2013年IEEE安全与隐私研讨会，第334-348页。IEEE，2013年。

[142]艾德里安·尼尔森、西蒙·史密斯、格雷戈尔·乌尔姆、埃米尔·古斯塔夫松和马茨·吉尔斯特兰。性能评估联邦学习算法。在第二届深度学习分布式结构研讨会论文集，第1-8页。ACM，2018年。

[143]西尾隆之和米谷亮。异构环境下联邦学习的客户端选择移动的边缘中的资源。在ICC 2019-2019 IEEE国际通信会议（ICC），第1-7页。IEEE，2019年。

[144]Richard Nock，Stephen哈代，Wilko Henecka，Hamish Ivey-Law，Giorgio Patrini，Guillaume史密斯和布莱恩·索恩。实体解析和联邦学习得到联邦解析。arXiv预印本arXiv：1803.04035，2018。

[145]Olga Ohrimenko，Felix Schuster，C edric Fournet，Aastha Mehta，Sebastian Nowozin，Kapil，1999年瓦斯瓦尼和曼努埃尔·科斯塔。可信处理器上的不经意多方机器学习。第25届{USENIX}安全研讨会（{USENIX} Security 16），第619-636页，2016年。

[146]帕斯卡尔·派利耶基于复合度剩余类的公钥密码系统。在密码技术理论与应用国际会议，第223-238页。Springer，1999年。

[147]Sinno Jialin Pan和Qiang Yang。迁移学习研究综述。IEEE Transactions on Knowledge and Data Engineering，22（10）：1345-1359，2010。

[148] Adam Paszke, Sam Gross, Soumith Chintala, Gregory Chanan, Edward Yang, Zachary DeVito, Zeming Lin, Alban Desmaison, Luca Antiga, and Adam Lerer. Automatic differentiation in pytorch. 2017.

[149] Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, et al. Pytorch: An imperative style, high-performance deep learning library. In *Advances in Neural Information Processing Systems*, pages 8024–8035, 2019.

[150] Robi Polikar. Ensemble learning. In *Ensemble machine learning*. Springer, 2012.

[151] Neoklis Polyzotis, Sudip Roy, Steven Euijong Whang, and Martin Zinkevich. Data lifecycle challenges in production machine learning: a survey. *ACM SIGMOD Record*, 47(2):17–28, 2018.

[152] Adnan Qayyum, Kashif Ahmad, Muhammad Ahtazaz Ahsan, Ala Al-Fuqaha, and Junaid Qadir. Collaborative federated learning for healthcare: Multi-modal covid-19 diagnosis at the edge, 2021.

[153] Yongfeng Qian, Long Hu, Jing Chen, Xin Guan, Mohammad Mehedi Hassan, and Abdulhameed Alelaiwi. Privacy-aware service placement for mobile edge computing via federated learning. *Information Sciences*, 505:562–570, 2019.

[154] Sashank Reddi, Zachary Charles, Manzil Zaheer, Zachary Garrett, Keith Rush, Jakub Konečnỳ, Sanjiv Kumar, and H Brendan McMahan. Adaptive federated optimization. *arXiv preprint arXiv:2003.00295*, 2020.

[155] Amirhossein Reisizadeh, Farzan Farnia, Ramtin Pedarsani, and Ali Jadbabaie. Robust federated learning: The case of affine distribution shifts. *arXiv preprint arXiv:2006.08907*, 2020.

[156] M Sadegh Riazi, Christian Weinert, Oleksandr Tkachenko, Ebrahim M Songhori, Thomas Schneider, and Farinaz Koushanfar. Chameleon: A hybrid secure computation framework for machine learning applications. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 707–721. ACM, 2018.

[157] Sebastian Ruder. An overview of multi-task learning in deep neural networks. *arXiv preprint arXiv:1706.05098*, 2017.

[158] Theo Ryffel, Andrew Trask, Morten Dahl, Bobby Wagner, Jason Mancuso, Daniel Rueckert, and Jonathan Passerat-Palmbach. A generic framework for privacy preserving deep learning. *arXiv preprint arXiv:1811.04017*, 2018.

[159] Mohamed Sabt, Mohammed Achemlal, and Abdelmadjid Bouabdallah. Trusted execution environment: what it is, and what it is not. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 57–64. IEEE, 2015.

[160] Sumudu Samarakoon, Mehdi Bennis, Walid Saad, and Merouane Debbah. Federated learning for ultra-reliable low-latency v2v communications, 2018.

[161] Wojciech Samek, Thomas Wiegand, and Klaus-Robert Müller. Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models. *arXiv preprint arXiv:1708.08296*, 2017.

[162] Ashish P Sanil, Alan F Karr, Xiaodong Lin, and Jerome P Reiter. Privacy preserving regression modelling via distributed computation. In *Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 677–682. ACM, 2004.

[163] Yunus Sarikaya and Ozgur Ercetin. Motivating workers in federated learning: A stackelberg game perspective, 2019.

[148]Adam Paszke、Sam Gross、Soumith Chintala、Gregory Chanan、Edward Yang、Zachary DeVito、Zeming Lin、Alban Desmaison、Luca Antiga和Adam Lerer。pytorch中的自动微分。2017.

[149]亚当-帕斯克，萨姆-格罗斯，弗朗西斯科马萨，亚当-莱勒，詹姆斯-布拉德伯里，格雷戈里-查南，特雷弗基林，林泽明，娜塔莉亚Gimelshein，卢卡Antiga，等. Pytorch：一种命令式风格，高性能深度学习库。神经信息处理系统的进展，第8024-8035页，2019年。

[150]罗比·波利卡包围学习。在Encourage机器学习中。Springer，2012.

[151]Neoklis Polyzotis，Sudip Roy，Steven Euijong Whang，and Martin Zinkevich.生产机器学习中的数据生命周期挑战：调查。ACM SIGMOD记录，47（2）：17-28，2018。

[152]Adnan Qayyum，Kashif Ahmad，Muhammad Ahtazaz Ahsan，Ala Al-Fuqaha，and Junaid Qadir.医疗保健的协作联邦学习：2021年边缘的多模式COVID-19诊断。

[153]Yongfeng Qian，Long Hu，Jing Chen，Xin Guan，Mohammad Mehedi哈桑，Abdulhameed阿莱莱维通过联邦学习实现移动的边缘计算的隐私感知服务放置。信息科学，505：562-570，2019。

[154]Sashank Reddi，Zachary Charles，Manzil Zaheer，Zachary加勒特，基思拉什，Jakub Kone Rush，Sanjiv Kumar和H Brendan McMahan。自适应联邦优化。arXiv预印本arXiv：2003.00295，2020。

[155]Amirhossein Reisizadeh、Farzan Farnia、Ramtin Pedarsani和Ali Jadbabaie。鲁棒的联邦学习：仿射分布移位的情况。arXiv预印本arXiv：2006.08907，2020。

[156]M Sadegh Riazi，Christian Weinert，Oleksandr Tkachenko，Ebrahim M Songhori，Thomas Schnei—der和Farinaz Koushanfar。Chameleon：一个机器混合安全计算框架学习应用。在2018年亚洲计算机和通信安全会议上，第707-721页。ACM，2018年。

[157]塞巴斯蒂安鲁德。深度神经网络中的多任务学习概述。arXiv预印本arXiv：1706.05098，2017。

[158]西奥·赖恩，安德鲁·特拉斯克，莫滕·达尔，鲍比·瓦格纳，杰森·曼库索，丹尼尔·鲁科特，乔纳森·帕瑟拉特-帕姆巴赫隐私保护深度学习的通用框架。arXiv预印本arXiv：1811.04017，2018。

[159]Mohamed Sabt，Mohammed Achemlal和Abdelmadjid Bouabdallah。可信执行环境它是什么，它不是什么。2015年IEEE Trustcom/BigDataSE/ISPA，第1卷，第57-64页。IEEE，2015年。

[160]Sumudu Samarakoon，Mehdi Bennis，Walid Saad，and Merouane Debbah.超可靠低延迟v2v通信的联合学习，2018年。

[161]Wojciech Samek，托马斯Wiegand，Klaus-Robert Müuller。可解释的人工智能：理解、可视化和解释深度学习模型。arXiv预印本arXiv：1708.08296，2017。

[162]Ashish P Sanil，Alan F Karr，Xiaodong Lin，and杰罗姆P Reiter.隐私保护回归通过分布式计算建模。在第十届ACM SIGKDD知识发现和数据挖掘国际会议上，第677-682页。ACM，2004年。

[163]Yunus Sarikaya和Ozgur Ercetin。联邦学习中的激励工作者：Stackelberg游戏视角，2019。

[164] Felix Sattler, Simon Wiedemann, Klaus-Robert Müller, and Wojciech Samek. Robust and communication-efficient federated learning from non-iid data. *arXiv preprint arXiv:1903.02891*, 2019.

[165] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[166] Amit P Sheth and James A Larson. Federated database systems for managing distributed, heterogeneous, and autonomous databases. *ACM Computing Surveys (CSUR)*, 22(3):183–236, 1990.

[167] Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 3–18. IEEE, 2017.

[168] Dejan Skvorc, Matija Horvat, and Sinisa Srbljic. Performance evaluation of websocket protocol for implementation of full-duplex web streams. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1003–1008. IEEE, 2014.

[169] Virginia Smith, Chao-Kai Chiang, Maziar Sanjabi, and Ameet S Talwalkar. Federated multi-task learning. In *Advances in Neural Information Processing Systems*, pages 4424–4434, 2017.

[170] Shuang Song, Kamalika Chaudhuri, and Anand D Sarwate. Stochastic gradient descent with differentially private updates. In *2013 IEEE Global Conference on Signal and Information Processing*, pages 245–248. IEEE, 2013.

[171] Michael R Sprague, Amir Jalalirad, Marco Scavuzzo, Catalin Capota, Moritz Neun, Lyman Do, and Michael Kopp. Asynchronous federated learning for geospatial applications. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, pages 21–28. Springer, 2018.

[172] Ivan Stojmenovic, Sheng Wen, Xinyi Huang, and Hao Luan. An overview of fog computing and its security issues. *Concurr. Comput. : Pract. Exper.*, 28(10):2991–3005, July 2016. ISSN 1532-0626. doi: 10.1002/cpe.3485. URL https://doi.org/10.1002/cpe.3485.

[173] Lili Su and Jiaming Xu. Securing distributed machine learning in high dimensions. *arXiv preprint arXiv:1804.10140*, 2018.

[174] Ziteng Sun, Peter Kairouz, Ananda Theertha Suresh, and H Brendan McMahan. Can you really backdoor federated learning? *arXiv preprint arXiv:1911.07963*, 2019.

[175] Martin Sundermeyer, Ralf Schlüter, and Hermann Ney. Lstm neural networks for language modeling. In *Thirteenth annual conference of the international speech communication association*, 2012.

[176] Melanie Swan. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[177] Ben Tan, Bo Liu, Vincent Zheng, and Qiang Yang. A federated recommender system for online services. In *Fourteenth ACM Conference on Recommender Systems*, pages 579–581, 2020.

[178] Mingxing Tan and Quoc V Le. Efficientnet: Rethinking model scaling for convolutional neural networks. *arXiv preprint arXiv:1905.11946*, 2019.

[179] ADP Team et al. Learning with privacy at scale. *Apple Machine Learning Journal*, 1(8), 2017.

[180] Om Thakkar, Galen Andrew, and H Brendan McMahan. Differentially private learning with adaptive clipping. *arXiv preprint arXiv:1905.03871*, 2019.

[164]Felix Sattler，Simon Wiedemann，Klaus—Robert M 'uller和Wojciech Samek。强劲和来自非IID数据的通信高效的联邦学习。arXiv预印本arXiv：1903.02891，2019。

[165]阿迪·沙米尔如何分享秘密。美国计算机学会通讯，22（11）：612-613，1979年。

[166]Amit P Sheth和James A Larson。用于管理分布式、异构和自治数据库的联邦数据库系统。ACM Computing Surveys（CSUR），22（3）：183-236，1990.

[167]Reza Shokri，Marco Stronati，Congzheng Song，and Vitaly Shmatikov.隶属度推理攻击机器学习模型。2017年IEEE安全与隐私研讨会（SP），第3-18页。IEEE，2017年。

[168]Dejan Skvorc，Matija Horvat和Sinisa Srbljic。基于WebSocket的WebSocket协议性能分析实现全双工网络流。2014年第37届信息和通信技术、电子和微电子国际会议（MIPRO），第1003-1008页。
IEEE，2014年。

[169]Virginia Smith，Chao-Kai Chiang，Maziar Sanjabi，and Ameet S Talwalkar.联邦多任务学习。神经信息处理系统的进展，第4424-4434页，2017年。

[170]Shuang Song，Kamalika Chaudhuri，and Anand D Sarwate.随机梯度下降

差异私有更新。2013年IEEE全球信号与信息处理会议，第245-248页。IEEE，2013年。

[171]Michael R Sprague，Amir Jalalirad，Marco Scavuzzo，Catalin Capota，莫里茨Neun，莱曼多，和迈克尔·科普地理空间应用程序的异步联邦学习。在联合欧洲
数据库中的机器学习和知识发现会议，第21-28页。Springer，2018年。

[172]伊万·斯托伊梅诺维奇，盛文，黄心怡，郝鸾。雾计算及其应用
安全问题同意Comput.：执业专家，28（10）：2991-3005，2016年7月。ISSN 1532-0626。doi：10.1002/cpe.3485。网址https://doi.org/10.1002/cpe.3485。

[173]苏丽丽和徐家明。在高维度中保护分布式机器学习。arXiv预印本arXiv：1804.10140，2018。

[174]Ziteng Sun，Peter Kairouz，Ananda Theertha Suresh，and H Brendan McMahan.你真的可以后门联邦学习吗？arXiv预印本arXiv：1911.07963，2019。

[175]Martin Sundermeyer，Ralf Schlüuter，and Hermann Ney. LSTM语言神经网络

建模2012年国际语音通信协会第十三届年会。

[176]梅兰妮·斯旺区块链：新经济的蓝图。 “O'Reilly Media，Inc." 2015.

[177]Ben Tan，Bo Liu，Vincent Zheng，and Qiang Yang.一种用于在线服务的联合推荐系统。第十四届ACM推荐系统会议，第579-581页，2020年。

[178]Mingxing Tan and Quoc V Le. Efficientnet：重新思考卷积神经网络的模型缩放。arXiv预印本arXiv：1905.11946，2019。

[179]ADP团队等人，大规模学习隐私。Apple Machine Learning Journal，1（8），2017。

[180]Om Thakkar，Galen Andrew，and H Brendan McMahan.具有自适应裁剪的差分私有学习。arXiv预印本arXiv：1905.03871，2019。

[181] Stacey Truex, Nathalie Baracaldo, Ali Anwar, Thomas Steinke, Heiko Ludwig, Rui Zhang, and Yi Zhou. A hybrid approach to privacy-preserving federated learning. In *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*, pages 1–11. ACM, 2019.

[182] Manasi Vartak, Harihar Subramanyam, Wei-En Lee, Srinidhi Viswanathan, Saadiyah Husnoo, Samuel Madden, and Matei Zaharia. Modeldb: a system for machine learning model management. In *Proceedings of the Workshop on Human-In-the-Loop Data Analytics*, pages 1–3, 2016.

[183] Dinusha Vatsalan, Ziad Sehili, Peter Christen, and Erhard Rahm. Privacy-preserving record linkage for big data: Current approaches and research challenges. In *Handbook of Big Data Technologies*, pages 851–895. Springer, 2017.

[184] Praneeth Vepakomma, Otkrist Gupta, Tristan Swedish, and Ramesh Raskar. Split learning for health: Distributed deep learning without sharing raw patient data. *arXiv preprint arXiv:1812.00564*, 2018.

[185] Paul Voigt and Axel Von dem Bussche. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.

[186] Isabel Wagner and David Eckhoff. Technical privacy metrics: a systematic survey. *ACM Computing Surveys (CSUR)*, 51(3):57, 2018.

[187] Guan Wang, Charlie Xiaoqian Dang, and Ziye Zhou. Measure contribution of participants in federated learning. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 2597–2604. IEEE, 2019.

[188] Hongyi Wang, Kartik Sreenivasan, Shashank Rajput, Harit Vishwakarma, Saurabh Agarwal, Jy-yong Sohn, Kangwook Lee, and Dimitris Papailiopoulos. Attack of the tails: Yes, you really can backdoor federated learning. *Advances in Neural Information Processing Systems*, 33, 2020.

[189] Hongyi Wang, Mikhail Yurochkin, Yuekai Sun, Dimitris Papailiopoulos, and Yasaman Khazaeni. Federated learning with matched averaging. *arXiv preprint arXiv:2002.06440*, 2020.

[190] Jianyu Wang, Qinghua Liu, Hao Liang, Gauri Joshi, and H Vincent Poor. Tackling the objective inconsistency problem in heterogeneous federated optimization. *Advances in Neural Information Processing Systems*, 2020.

[191] Rui Wang, Heju Li, and Erwu Liu. Blockchain-based federated learning in mobile edge networks with application in internet of vehicles. *arXiv preprint arXiv:2103.01116*, 2021.

[192] Shiqiang Wang, Tiffany Tuor, Theodoros Salonidis, Kin K Leung, Christian Makaya, Ting He, and Kevin Chan. Adaptive federated learning in resource constrained edge computing systems. *IEEE Journal on Selected Areas in Communications*, 37(6):1205–1221, 2019.

[193] Tianhao Wang, Johannes Rausch, Ce Zhang, Ruoxi Jia, and Dawn Song. A principled approach to data valuation for federated learning. In *Federated Learning*, pages 153–167. Springer, 2020.

[194] Xiaofei Wang, Yiwen Han, Chenyang Wang, Qiyang Zhao, Xu Chen, and Min Chen. In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning. *IEEE Network*, 2019.

[195] Yushi Wang. Co-op: Cooperative machine learning from mobile devices. 2017.

[196] Zhibo Wang, Mengkai Song, Zhifei Zhang, Yang Song, Qian Wang, and Hairong Qi. Beyond inferring class representatives: User-level privacy leakage from federated learning. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pages 2512–2520. IEEE, 2019.

[181]Stacey Truex，Nathalie Baracaldo，Ali Anwar，Thomas Steinke，Heiko Ludwig，Rui Zhang，和易舟。隐私保护联邦学习的混合方法。第12届ACM人工智能与安全研讨会论文集，第1-11页。ACM，2019年。

[182]马纳西·瓦尔塔克、Harihar Subramanyam、Wei-En Lee、Srinidhi Viswanathan、Saadiyah Husnoo、Samuel Madden和Matei Zaharia。Modeldb：一个机器学习模型管理的系统。在人类在环数据分析研讨会的会议记录中，第1-3页，2016年。

[183]Dinusha Vatsalan，Ziad Sehili，Peter Christen和埃哈德拉姆。隐私保护记录链接大数据：当前的方法和研究挑战。大数据技术手册，第851-895页。Springer，2017.

[184]Praneeth Vepakomma，Otkrist Gupta，Tristan Swedish，and Ramesh Raskar.健康分割学习：分布式深度学习，无需共享原始患者数据。arXiv预印本arXiv：1812.00564，2018。

[185]保罗·沃伊特和阿克塞尔·冯·登·布舍。欧盟通用数据保护条例（gdpr）。实用指南，第1版，陈：施普林格国际出版社，2017年。

[186]伊莎贝尔瓦格纳和大卫·埃克霍夫。技术隐私指标：系统调查。ACM计算调查（CSUR），51（3）：57，2018。

[187]王观，党晓倩，周子烨。衡量参与者的贡献

联邦学习在2019年IEEE大数据国际会议（大数据），第2597- 2604页。IEEE，2019年。

[188]Hongyi Wang、Kartik Sreenivasan、Shashank Rajput、Harit Vishwakarma、Saurabh Agarwal、Jy-孙勇，李康旭，迪米特里斯·帕帕里奥普洛斯。尾部攻击：是的，你真的可以后门联邦学习。神经信息处理系统的进展，33，2020。

[189]Hongyi Wang，Mikhail Yurochkin，Yuekai Sun，Dimitris Papailiopoulos，and Yasaman Khazaeni.联合学习与匹配平均。arXiv预印本arXiv：2002.06440，2020。

[190]Jianyu Wang，Qinghua Liu，Hao Liang，Gauri Joshi，and H Vincent Poor.解决目标异构联邦优化中不一致性问题神经信息处理系统的进展，2020。

[191]王瑞，李和菊，刘二武。移动的边缘网络中基于区块链的联邦学习及其在车联网中的应用。arXiv预印本arXiv：2103.01116，2021。

[192]王世强、Tiffany Tuor、Theodoros Salonidis、Kin K Liang、Christian Makaya、Ting He和

凯文·陈资源受限边缘计算系统中的自适应联邦学习。IEEE Journal on Selected Areas in Communications，37（6）：1205-1221，2019。

[193]王天豪，Johannes Rausch，张策，贾若曦和Dawn Song。联邦学习数据估值的原则性方法。在联邦学习，第153-167页。施普林格，2020年。

[194]Xiaofei Wang，Yiwen Han，Chenyang Wang，Qiyang Zhao，Xu Chen，and Min Chen.边缘内ai：通过联邦学习实现移动的边缘计算、缓存和通信的智能化。IEEE网络，2019年。

[195]王雨诗。Co-op：从移动的设备进行协作机器学习。2017.

[196]Zhibo Wang，Mengkai Song，Zhifei Zhang，Yang Song，Qian Wang，and Hairong Qi.超出推断类代表：来自联邦学习的用户级隐私泄露。在IEEE INFOCOM 2019-IEEE计算机通信会议，第2512-2520页。IEEE，2019年。

[197] Zeyi Wen, Bingsheng He, Ramamohanarao Kotagiri, Shengliang Lu, and Jiashuai Shi. Efficient gradient boosted decision tree training on gpus. In *2018 IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, pages 234–243. IEEE, 2018.

[198] Zeyi Wen, Jiashuai Shi, Qinbin Li, Bingsheng He, and Jian Chen. ThunderSVM: A fast SVM library on GPUs and CPUs. *Journal of Machine Learning Research*, 19:797–801, 2018.

[199] Zeyi Wen, Jiashuai Shi, Bingsheng He, Jian Chen, Kotagiri Ramamohanarao, and Qinbin Li. Exploiting gpus for efficient gradient boosting decision tree training. *IEEE Transactions on Parallel and Distributed Systems*, 2019.

[200] Zeyi Wen, Jiashuai Shi, Qinbin Li, Bingsheng He, and Jian Chen. Thundergbm: Fast gbdts and random forests on gpus. In *https://github.com/Xtra-Computing/thundergbm*, 2019.

[201] Jiasi Weng, Jian Weng, Jilian Zhang, Ming Li, Yue Zhang, and Weiqi Luo. Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Transactions on Dependable and Secure Computing*, 2019.

[202] Xiaokui Xiao, Guozhang Wang, and Johannes Gehrke. Differential privacy via wavelet transforms. *IEEE Transactions on knowledge and data engineering*, 23(8):1200–1214, 2010.

[203] Chulin Xie, Keli Huang, Pin-Yu Chen, and Bo Li. Dba: Distributed backdoor attacks against federated learning. In *International Conference on Learning Representations*, 2019.

[204] Cong Xie, Sanmi Koyejo, and Indranil Gupta. Asynchronous federated optimization. *arXiv preprint arXiv:1903.03934*, 2019.

[205] Runhua Xu, Nathalie Baracaldo, Yi Zhou, Ali Anwar, and Heiko Ludwig. Hybridalpha: An efficient approach for privacy-preserving federated learning. In *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*, pages 13–23, 2019.

[206] Zhuang Yan, Li Guoliang, and Feng Jianhua. A survey on entity alignment of knowledge base. *Journal of Computer Research and Development*, 1:165–192, 2016.

[207] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 10(2):12, 2019.

[208] Timothy Yang, Galen Andrew, Hubert Eichner, Haicheng Sun, Wei Li, Nicholas Kong, Daniel Ramage, and Françoise Beaufays. Applied federated learning: Improving google keyboard query suggestions. *arXiv preprint arXiv:1812.02903*, 2018.

[209] Shanhe Yi, Zhengrui Qin, and Qun Li. Security and privacy issues of fog computing: A survey. In *WASA*, 2015.

[210] Naoya Yoshida, Takayuki Nishio, Masahiro Morikura, Koji Yamamoto, and Ryo Yonetani. Hybrid-fl: Cooperative learning mechanism using non-iid data in wireless networks. *arXiv preprint arXiv:1905.07210*, 2019.

[211] Hwanjo Yu, Xiaoqian Jiang, and Jaideep Vaidya. Privacy-preserving svm using nonlinear kernels on horizontally partitioned data. In *Proceedings of the 2006 ACM symposium on Applied computing*, pages 603–610. ACM, 2006.

[212] Zhengxin Yu, Jia Hu, Geyong Min, Haochuan Lu, Zhiwei Zhao, Haozhe Wang, and Nektarios Georgalas. Federated learning based proactive content caching in edge computing. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2018.

[197]Zeyi Wen，Bingsheng He，Ramamohanarao科塔吉里，Shengliang Lu，and Jiashuai Shi.高效GPU上的梯度提升决策树训练。在2018年IEEE国际并行和分布式处理研讨会（IPDPS），第234-243页。IEEE，2018年。

[198]温泽一，施佳帅，李沁彬，何炳胜，剑尘。ThunderSVM：GPU和CPU上的快速SVM库。Journal of Machine Learning Research，19：797-801，2018。

[199]Zeyi Wen，Jiashuai Shi，Bingsheng He，Jian Chen，科塔吉里Ramamohanarao，和Qinbin Li.利用gpu进行有效的梯度提升决策树训练。IEEE Transactions on Parallel and Distributed Systems，2019。

[200]温泽一，施佳帅，李沁彬，何炳胜，剑尘。Thundergbm：GPU上的快速gbdts和随机森林。在https：//github.com/Xtra-Computing/thundergbm，2019年。

[201]Jiasi Weng，Jian Weng，Jilian Zhang，Ming Li，Yue Zhang，and Weiqi Luo. Deepchain：可审核以及基于区块链激励的隐私保护深度学习。IEEE Transactions on Dependency and Secure Computing，2019。

[202]Xiaokui Xiao，Guozhang Wang，and Johannes Gehrke.基于小波变换的差分隐私。IEEE Transactions on Knowledge and Data Engineering，23（8）：1200-1214，2010。

[203]Chulin Xie，Keli Huang，Pin-Yu Chen，and Bo Li. DBA：分布式后门攻击联邦学习。在2019年国际学习代表会议上。

[204]Cong Xie，Sanmi Koyejo，and Indranil Gupta.异步联邦优化。arXiv预印本arXiv：1903.03934，2019。

[205]Runhua Xu，Nathalie Baracaldo，Yi Zhou，Ali Anwar，and Heiko Ludwig. Hybridalpha：An隐私保护联邦学习的有效方法。在第12届ACM人工智能和安全研讨会的会议记录中，第13-23页，2019年。

[206]庄妍，李国梁，冯建华。知识库实体对齐研究综述。Journal of Computer Research and Development，1：165-192，2016.

[207]杨强，刘扬，陈天健，童永新。联邦机器学习：概念和应用ACM Transactions on Intelligent Systems and Technology（TIST），10（2）：12，2019。

[208]Timothy Yang，Galen Andrew，Hubert Eichner，Haicheng Sun，Wei Li，Nicholas Kong，Daniel（英文）Ramage和Fran C. Beaufays。应用联邦学习：改进谷歌键盘查询建议。arXiv预印本arXiv：1812.02903，2018。

[209]易山河，秦正瑞，李群。雾计算的安全和隐私问题：调查。In WASA，2015.

[210]吉田直哉、西尾隆之、森仓正弘、山本浩司、米谷亮。混合动力-fl：无线网络中使用非iid数据的协作学习机制。arXiv预印本arXiv：1905.07210，2019。

[211]Hwanjo Yu，Xiaoqian Jiang，and Jaideep Vaidya.基于非线性核的隐私保护svm水平分区的数据。2006年ACM应用计算研讨会论文集，第603-610页。ACM，2006年。

[212]Zhengxin Yu，Jia Hu，Geyong Min，Haochuan Lu，Zhiwei Zhao，Haozhe Wang，and Nektarios乔治拉斯边缘计算中基于联合学习的主动内容缓存。2018年IEEE全球通信会议（GLOBECOM），第1-6页。IEEE，2018年。

[213] Mikhail Yurochkin, Mayank Agarwal, Soumya Ghosh, Kristjan Greenewald, Trong Nghia Hoang, and Yasaman Khazaeni. Bayesian nonparametric federated learning of neural networks. *arXiv preprint arXiv:1905.12022*, 2019.

[214] Weishan Zhang, Qinghua Lu, Qiuyu Yu, Zhaotong Li, Yue Liu, Sin Kit Lo, Shiping Chen, Xiwei Xu, and Liming Zhu. Blockchain-based federated learning for device failure detection in industrial iot. *IEEE Internet of Things Journal*, 2020.

[215] Yu Zhang and Qiang Yang. A survey on multi-task learning. *arXiv preprint arXiv:1707.08114*, 2017.

[216] Zhengming Zhang, Zhewei Yao, Yaoqing Yang, Yujun Yan, Joseph E Gonzalez, and Michael W Mahoney. Benchmarking semi-supervised federated learning. *arXiv preprint arXiv:2008.11364*, 2020.

[217] Lingchen Zhao, Lihao Ni, Shengshan Hu, Yaniiao Chen, Pan Zhou, Fu Xiao, and Libing Wu. Inprivate digging: Enabling tree-based distributed data mining with differential privacy. In *INFOCOM*, pages 2087–2095. IEEE, 2018.

[218] Yang Zhao, Jun Zhao, Linshan Jiang, Rui Tan, and Dusit Niyato. Mobile edge computing, blockchain and reputation-based crowdsourcing iot federated learning: A secure, decentralized and privacy-preserving system. *arXiv preprint arXiv:1906.10893*, 2019.

[219] Yang Zhao, Jun Zhao, Linshan Jiang, Rui Tan, Dusit Niyato, Zengxiang Li, Lingjuan Lyu, and Yingbo Liu. Privacy-preserving blockchain-based federated learning for iot devices. *IEEE Internet of Things Journal*, 2020.

[220] Yang Zhao, Jun Zhao, Mengmeng Yang, Teng Wang, Ning Wang, Lingjuan Lyu, Dusit Niyato, and Kwok Yan Lam. Local differential privacy based federated learning for internet of things. *arXiv preprint arXiv:2004.08856*, 2020.

[221] Yue Zhao, Meng Li, Liangzhen Lai, Naveen Suda, Damon Civin, and Vikas Chandra. Federated learning with non-iid data. *arXiv preprint arXiv:1806.00582*, 2018.

[222] Wenbo Zheng, Lan Yan, Chao Gou, and Fei-Yue Wang. Federated meta-learning for fraudulent credit card detection. In *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20)*, 2020.

[223] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4): 352–375, 2018.

[224] Amelie Chi Zhou, Yao Xiao, Bingsheng He, Jidong Zhai, Rui Mao, et al. Privacy regulation aware process mapping in geo-distributed cloud data centers. *IEEE Transactions on Parallel and Distributed Systems*, 2019.

[225] Pan Zhou, Kehao Wang, Linke Guo, Shimin Gong, and Bolong Zheng. A privacy-preserving distributed contextual federated online learning framework with big data support in social recommender systems. *IEEE Transactions on Knowledge and Data Engineering*, 2019.

[226] Hangyu Zhu and Yaochu Jin. Multi-objective evolutionary federated learning. *IEEE transactions on neural networks and learning systems*, 2019.

[227] Weiming Zhuang, Yonggang Wen, Xuesen Zhang, Xin Gan, Daiying Yin, Dongzhan Zhou, Shuai Zhang, and Shuai Yi. Performance optimization of federated person re-identification via benchmark analysis. In *Proceedings of the 28th ACM International Conference on Multimedia*, pages 955–963, 2020.

[213]米哈伊尔·尤罗奇金、马扬克·阿加瓦尔、苏姆亚·戈什、克里斯琴·格林瓦尔德、仲恩吉亚黄、和亚萨曼·哈扎伊尼神经网络的贝叶斯非参数联邦学习。arXiv预印本arXiv：1905.12022，2019。

[214]Weishan Zhang，Qinghua Lu，Qiuyu Yu，Zhaotong Li，Yue Liu，Sin Kit Lo，Shiping Chen，Xiwei Xu，and Liming Zhu.基于区块链的联合学习用于工业物联网设备故障检测。IEEE Internet of Things Journal，2020。

[215]张玉和杨强。多任务学习研究综述。arXiv预印本arXiv：1707.08114，2017.

[216]Zhengming Zhang，Zhewei Yao，Yaoqing Yang，Yujun Yan，Joseph E Gonzalez，and Michael W 马洪尼对半监督联邦学习进行基准测试。arXiv预印本arXiv：2008.11364，2020。

[217]Zhao，Lihao Ni，Shengshan Hu，Yaniiao Chen，Pan Zhou，Fu Xiao，and Libing Wu. Inprivate digging：启用基于树的分布式数据挖掘，并具有差异隐私。见INFOCOM，第2087-2095页。IEEE，2018年。

[218]Yang Zhao，Jun Zhao，Linshan Jiang，Rui Tan，and杜西特Niyato.移动的边缘计算，区块链和基于声誉的众包物联网联合学习：一个安全，分散和隐私保护的系统。arXiv预印本arXiv：1906.10893，2019。

[219]杨钊、赵军、林山姜、瑞谭、杜实尼亚托、李增祥、令娟吕、和刘英波。用于物联网设备的基于隐私保护区块链的联邦学习。IEEE Internet of Things Journal，2020。

[220]杨钊、赵军、杨萌萌、滕王、宁王、令娟·吕、杜实·尼亚托和郭仁林。基于局部差分隐私的物联网联邦学习。arXiv预印本arXiv：2004.08856，2020。

[221]Yue Zhao，Meng Li，Liangzhen Lai，Naveen苏达，Damon Civin，和Vikas Chandra.使用非iid数据的联邦学习。arXiv预印本arXiv：1806.00582，2018。

[222]郑文波，燕岚，苟超，王飞跃。针对欺诈的联邦元学习

信用卡检测在2020年第二十九届国际人工智能联合会议（IJCAI-20）的会议记录中。

[223]Zibin Zheng，Shaoan Xie，Hong-Ning Dai，Xiangping Chen，and Huaimin Wang.区块链挑战和机遇：一项调查。International Journal of Web and Grid Services，14（4）：352-375，2018。

[224]周池，肖耀，何炳生，翟继东，毛锐，等.隐私权保护地理分布的云数据中心中的感知过程映射。IEEE Transactions on Parallel and Distributed Systems，2019。

[225]潘周，王可豪，郭林科，龚世民，郑博龙。隐私保护分布式上下文联合在线学习框架与社会推荐系统中的大数据支持。IEEE Transactions on Knowledge and Data Engineering，2019。

[226]朱航宇和金耀初。多目标进化联邦学习。IEEE transactions on neural networks and learning systems，2019。

[227]Weiming Zhuang，Yonggang Wen，Xuesen Zhang，Xin Gan，Daiying Yin，Dongzhan Zhou，Shuai
张，帅毅。基于基准测试的联邦人员再识别性能优化分析.在第28届ACM多媒体国际会议的会议录中，第955-963页，2020.

[228] G. Zyskind, O. Nathan, and A. '. Pentland. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184, May 2015. doi: 10.1109/SPW.2015.27.

[228]G.济斯金德河，澳-地Nathan和A. '.彭特兰去中心化隐私：使用区块链保护个人数据. 2015年IEEE安全和隐私研讨会，第180-184页，2015年5月。doi：10.1109/SPW.2015.27。