计算机工程
Computer Engineering
ISSN 1000-3428,CN 31-1289/TP

《计算机工程》网络首发论文

题目：联邦学习及其安全与隐私保护研究综述
作者：熊世强，何道敬，王振东，杜润萌
DOI：10.19678/j.issn.1000-3428.0067782
网络首发日期：2023-11-23
引用格式：熊世强，何道敬，王振东，杜润萌．联邦学习及其安全与隐私保护研究综述[J/OL]．计算机工程. https://doi.org/10.19678/j.issn.1000-3428.0067782

网络首发时间：2023-11-23 15:47:43
网络首发地址：https://link.cnki.net/urlid/31.1289.TP.20231122.1027.001

计 算 机 工 程
Computer Engineering

联邦学习及其安全与隐私保护研究综述

熊世强[1]，何道敬[2]，王振东[1]，杜润萌[3]

(1. 江西理工大学 信息工程学院，江西 赣州 341000；2. 哈尔滨工业大学 计算机科学与技术学院，广东 深圳 518055；3. 华东师范大学 计算机科学与技术学院，上海 200062)

摘　要：联邦学习是一种新兴的分布式机器学习技术，其无需对数据进行收集，只需将数据留在本地就能通过各方协作来训练一个共有模型，解决了传统机器学习中数据难以采集和数据隐私安全问题，随着该技术的应用和发展，研究发现联邦学习中仍可能受到各类攻击，为确保联邦学习的足够安全，研究联邦学习中的攻击方式和相应的隐私保护技术显得尤为重要。首先对联邦学习的相关背景知识进行了介绍，随后对联邦学习的定义进行了简要介绍，总结概述了联邦学习的发展历程及其分类，接着介绍了联邦学习安全三要素，从基于来源和基于安全三要素两个角度分类概述了联邦学习中的安全问题，并综述了其研究进展，而后对隐私保护技术进行了分类，结合相关研究应用具体综述了联邦学习中安全多方计算、同态加密、差分隐私和可信执行环境四种常用隐私保护技术，最后对联邦学习的未来研究方向进行了展望。

关键词：联邦学习；数据安全；攻击方式；隐私保护；安全三要素

开放科学（资源服务）标志码（OSID）：

A Review of Federated Learning and its Security and Privacy Protection

Xiong Shiqiang[1], He Daojing[2], Wang Zhendong[1], Du Runmeng[3]

(1. School of Information Engineering, Jiangxi University of Technology, Ganzhou,Jiangxi 341000, China; 2. School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen,Guangdong 518055, China; 3. School of Computer Science and Technology, East China normal University, Shanghai 200062, China)

【Abstract】Federated learning is an emerging distributed machine learning technology. It does not need to collect data, but can train a common model through the cooperation of all parties, which solves the problems of difficult data collection and data privacy security in traditional machine learning. With the application and development of this technology, the research finds that federated learning may still be subject to various attacks. In order to ensure enough security of federated learning, it is very important to study the attack mode and the corresponding privacy protection technology in federated learning. First of all, it introduces the relevant background and knowledge of federated learning, and then gives a brief introduction to the definition of federated learning, and summarizes the development process and Classification of federated learning, then introduces the three elements of federated learning security, from the perspective of sourcing-based and security-based three elements of the classification of security issues in federated learning, It also summarizes its research progress, and then classifies the privacy protection technology, combined with relevant research and application, specifically reviews the secure multi-party computing homomorphic encryption in federated learning Differential privacy and trusted execution environment are four common privacy protection technologies. Finally, the future research direction of federated learning is prospected.

【Key words】federated learning; data security; attack mode; privacy protection; security three elements

DOI:10.19678/j.issn.1000-3428.0067782

0　概述

随着人类社会的发展以及信息技术的不断成熟，移

基金项目：国家自然科学基金（62062037）；江西省自然科学基金（20212BAB202014）。

作者简介：熊世强(1997－，通信作者)，男，硕士研究生，信息安全工程师，主研方向为联邦学习、信息安全；何道敬，教授、博士；王振东，副教授、博士；杜润萌，博士研究生。

E-mail：xiongsqiang@qq.com

动物联网设备已逐渐渗透在生活中的方方面面，物联网设备的使用伴随着每天都会产生海量的数据，不言而喻，人类社会已进入到大数据时代[1]。在大数据时代，数据逐渐成为现代社会发展的生产要素，由于业务用途的不同，这些数据通常分散在不同的终端设备、企业或组织中，单方面的小数据往往难以发掘其中的潜在价值，若将这些分散的数据进行整合、分析和处理，往往能够产生意想不到的效益。传统的用人力来处理数据的方式已经过时，机器学习（machine learning，ML）所训练的模型由于能够快速处理海量的数据并能够挖掘离散数据间的隐藏信息而被社会广泛关注。然而，训练一个准确度较高的机器学习模型需要使用大量的高质量数据，以往的方法通常是从各个数据源将数据收集到一起才能满足机器学习模型训练所需的大量数据的需求，但在实际应用过程中却发现收集数据通常都会面临很多阻碍[2]。由于受到用户隐私安全保护、商业利益以及政府法律法规等因素的影响，数据通常无法在各企业与组织之间流通共享，各方所拥有的往往都是各领域所特有的一小部分数据，这与机器学习所需要的大量高质量数据的需求背道而驰，无疑阻碍了人工智能（artificial intelligence，AI）的研究和发展[3]。如何打破数据隐私安全僵局，让人工智能在各领域大展拳脚是人工智能发展所面临的重要挑战。

联邦学习（federated learning，FL）作为一种带有隐私保护技术的分布式机器学习技术[4]为此提供了解决方案，其允许各参与方在不共享各方原始数据的条件下共同训练一个模型，在该范式下，无需将所有分散的数据收集到一个中心节点进行模型训练，而是通过在各自的本地设备上进行模型训练并将结果上传至中心节点来改善模型效果，期间既不会发生隐私泄露的风险也不会违反任何的法律法规。联邦学习技术能够实现设备间的信息共享，可用于在分布式的数据集中构建全局的机器学习模型，相较传统方法不仅能够保持模型具有相差不大的准确度，还能有效保证数据安全[5]。自联邦学习被提出以来，就在学术界和工业界等领域引起了极大地反响，近年来，联邦学习发展迅速，有关联邦学习的应用开始在各行各业落地生根，但同时也随之产生了一系列的安全问题，如数据隐私泄露、恶意节点攻击、模型安全以及参与方是否可信等，这些安全威胁对联邦学习的落地提出了新的挑战。针对这些问题，联邦学习需要采取相应的隐私保护措施，以确保联邦学习系统安全可靠[6]，因此，研究联邦学习中的安全及其隐私保护技术具有重大意义。

本文对联邦学习及其安全与隐私保护进行了综述，介绍了联邦学习的背景、定义以及发展历程，并根据不同的依据对联邦学习进行了分类，阐述了联邦学习中的安全问题，从基于来源和基于安全三要素两个方面对联邦学习安全进行了分类综述，并介绍了近年来有关联邦学习安全方面的研究进展。结合相关研究从基于加密、基于数据绕动以及基于可信硬件三个方面对联邦学习中的隐私保护技术进行了分类阐述，对该领域的未来研究方向进行了展望。

1 联邦学习

1.1 机器学习

机器学习是属于人工智能领域内的一个分支，其主要思想在于希望机器能表现出像人一样的智能行为，通过模仿人的学习过程，对事物不断的认识来获取经验，本质是试图让机器通过某种计算手段，在数据中学习得到某种规律，根据所得出的规律来对新的数据进行预测，从而改善机器系统的自身性能[7]。然而，传统的机器学习训练通常都是将需要进行模型训练的数据收集到一处，通过单一的服务器节点进行模型训练，这对于中央服务器节点的数据处理时效及速度要求极高。随着数据量的持续扩增，模型也随之变得越来越复杂，单独的一个服务器节点由于计算和存储能力受限，逐渐不能满足已有的更为复杂的模型训练，传统的机器学习遇到发展瓶颈，因此就有了分布式机器学习（distributed machine learning，DML），其核心思想在于“分而治之”，将大量的数据及计算资源分散部署在多台服务器节点上[8]，各部分数据在各服务器节点上进行分布式模型训练，具有很强的扩展性，解决了单个服务器节点无法同时处理大批量数据和训练复杂模型的难题。

1.2 联邦学习及其定义

无论是传统的机器学习还是分布式机器学习都是将要用来训练模型的数据收集到服务器节点，在采集数据过程中，各数据提供者需要将原始数据发送或传输至服务器节点，也即发生了原始数据的交换，这就意味着在传输交换过程中有可能遭受到恶意攻击者对数据信息的窃取，从而导致用户隐私信息泄露。

近年来，随着信息技术的高速发展，社会各界对于用户个人数据安全保护的呼声有增无减，用户的隐私意识不断提高，人们越来越关心自己的个人信息是否会被

非法泄露给恶意方利用或是滥用，从而给生活带来不必要的困扰，这无疑给数据采集和获取带来了很大的阻碍。另一方面，为了响应社会呼吁以及减少数据安全事件的刑事纠纷，各个国家或组织陆续制定和颁布了关于保护用户隐私安全的各项法律法规。在国外，欧盟在 2018 年 5 月发布了有着史上最为严格的个人信息保护法之称的《通用数据保护条例》（General Data Protection Regulation，GDPR）[9]，该保护法案明确禁止了数据在不同实体组织或企业间的转移、交换和交易，以此来加强对用户数据隐私安全的保护和管理。在国内，我国早在 2016 年 11 月就发布通过了《中华人民共和国网络安全法》[10]，其中对数据的收集和处理提出了严格的约束和管控要求，明确要求企业或机构不能对其所收集到的用户信息进行泄露、篡改或是毁损，更在 2021 年 6 月和 8 月先后颁布了《中华人民共和国数据安全法》[11]和《中华人民共和国个人信息保护法》[12]，进一步限制了数据的使用。在这样一个日渐严格的法律环境下，收集离散数据将会变得愈加困难，长此以往，各方数据只允许保留在各方自己内部，就会形成一个个只具有一小部分数据的数据孤岛，这无疑可能会导致人工智能的又一个寒冬。

联邦学习正是为了解决数据隐私共享难题而产生，其最大的特点就是不用再从各方去收集数据，而是将原始数据保留在设备本地，各方之间进行协作训练一个共有模型，在这期间不会发生原始数据的传递和交换[13]，联邦学习实际是分布式机器学习的一种特殊形式，二者都是使用分散的数据来进行分布式的模型训练。具体来说，在联邦学习架构下，各提供数据的参与方设备分别使用其本地的数据进行局部的模型训练，训练结束后将所得到的局部模型参数脱敏后发送给中央服务器节点，待服务器节点接收到所有参与方的局部模型之后，将接收到的所有局部模型进行加权聚合，而后再将更新之后加密的全局模型分发给各参与方设备，各参与方收到全局聚合模型后使用该全局模型进行局部的模型训练，之后再将更新的局部模型发送至服务器节点，如此反复，直至模型收敛或达到所设最大的迭代次数，期间所有模型和参数的交换都会被严格设计，任何一方都无法从中获取除自身数据以外的信息。训练结束后，各参与方都能够得到一个相对使用自身数据来进行模型训练更优的机器学习模型[14]。数据对于机器学习来说必不可少，如果将数据比作是智能时代的石油，那联邦学习无疑会是一台蕴含极大潜力的石油挖掘机[15]，其所具备的这些特性为人工智能发展所面临的挑战问题提供了很好地解决办法。

具体联邦学习可作如下定义[16]，假设有n个提供数据参与模型训练的参与方，各参与方用F_i表示，各参与方所拥有的数据为D_i，其中$i=\{1,2,\dots,n-1,n\}$，使用各参与方的数据进行模型训练，传统的方法是将所有数据收集到一个中心节点，使用整合后的所有数据$D=D_1\cup D_2\cup\dots\cup D_{n-1}\cup D_n$进行模型训练，该方式训练所得的模型记为$M_{sum}$，准确率记为$V_{sum}$。在联邦学习中，各参与方$F_1,F_2,\dots,F_{n-1},F_n$分别使用各自的数据$D_1,D_2,\dots,D_{n-1},D_n$在各客户端本地进行局部模型训练，记聚合后的全局模型为M_{fed}，准确率为V_{fed}，期间任意参与方F_i都无法获知除其本身以外的数据D_i。若存在非负实数δ，满足$|V_{sum}-V_{fed}|<\delta$,则称模型M_{fed}的性能损失为δ[17]，其中，δ是一个足够小的浮点数，即表示通过联邦学习方式训练所得的模型应与传统方式将所有数据放在一起进行模型训练的准确率相差不大。

1.3 联邦学习发展历程

2016 年，联邦学习由谷歌公司 Mcmahan 等人在译名为《使用模型平均的深度网络联邦学习》[18]的论文中最先提出，该技术是考虑到传统方法在数据中心进行训练时可能会由于数据量过大或隐私安全问题而影响训练效果所提出的一种替代方案。2017 年 4 月，谷歌研究科学家 Brendan McMahan 和 Daniel Ramage 在谷歌博客中联名发布了译名为《联邦学习：没有集中训练数据的协作机器学习》[19]的博文，该文介绍了联邦学习的相关特性以及技术原理，指出用户可以通过移动设备利用联邦学习训练模型，并在 Gboard 谷歌键盘中测试使用了联邦学习，用以改进查询建议。谷歌的这些工作激发了国内外从业人员对联邦学习的研究热情，2018 年，在中国人工智能大会（CCAI）上，CCAI 的名誉副理事长杨强进行了以《GDPR 对 AI 的挑战和基于联邦迁移学习的对策》为题的一场演讲[20]，引入了谷歌所提出的联邦学习这一概念，指出可以在手机终端上建立模型，联邦学习能够用来解决在安卓设备上进行模型更新时的数据加密问题。2019 年 2 月，Bonawitz 等人发表了译名为《迈向大规模联邦学习：系统设计》[21]的论文，其中介绍了使用 TensorFlow 构建的第一个产品级别并能够进行扩展的联邦学习系统的组成部分，这个系统能支持大规模的移动设备，能够对存储在手机上的数据进行深层神经网络训练，可用来解决数以千万计的现实世界设备的应用学习问题。

联邦学习自提出以来，近年来在该领域内的研究成果持续增长，根据《联邦学习全球研究与应用趋势报告 2022》[22],联邦学习的发展可分为萌芽期、缓慢增长、扩展期和迅猛发展四个周期，从 2016 至 2021 年，研究时

段内的与联邦学习有关的论文数量高达 4576 篇，研究论文数逐年递增，2021 年的复合年增长率更是高达 40.78%，其论文数量分布、技术周期以及研究热词如表 1 所示。

表 1　联邦学习研究发展统计

Table 1　Federated learning research development statistics

技术周期	年份	论文数	研究热词
萌芽期	2016	323	差分隐私、通信效率、深度网络、边缘计算等
缓慢增长	2017	325	差分隐私、数据库、安全聚合、通信效率、多任务学习、云计算、物联网
扩展期	2018	407	医疗保健、物联网、生物医学、安全、效率、区块链
迅猛增长	2019	630	边缘计算、物联网、区块链、隐私保护技术、数据异构、模型压缩
	2020	1105	边缘计算、物联网、医疗保健、数据异构、效率及隐私保护、激励机制
	2021	1786	隐私保护技术、安全可信联邦学习、物联网、区块链、边缘计算

1.4 联邦学习分类

联邦学习是近年来产生的一个全新的概念，随着研究的深入和技术的成熟，在该领域内也随之产生了许多新的名词和定义，关于联邦学习的分类也有多种不同的划分和见解。总体来看，主要有三种划分，从参与到联邦学习训练中参与方数据的分布特点的差异来看，可将联邦学习划分为横向联邦学习、纵向联邦学习以及联邦迁移学习三类，依据在联邦学习训练中网络拓扑结构的差异，即是否存在中央服务器节点，可将联邦学习划分为中心化联邦学习和去中心化联邦学习两类[4]，根据参与到联邦学习中进行联邦训练的设备数量以及设备的性能，又可将联邦学习划分为“cross-device”和“cross-silo”[23]，即跨设备的联邦学习和跨筒仓/跨企业的联邦学习。

其中，横向联邦学习是将参与方数据的属性特征进行堆叠对齐，适用于参与方数据的分布特征有较多的重叠而用户样本分布重叠较少的情形。纵向联邦学习是将参与方的数据的样本进行堆叠对齐，即适用于参与方数据的用户样本有较多的重叠而属性特征重叠相对较少的情形。不同于横向和纵向联邦学习，联邦迁移学习中既不是将数据的属性特征进行对齐也不是将数据用户样本进行对齐，其实际是为了补充横向和纵向联邦学习而所做的一类划分，适用于在每个参与方数据的属性特征和用户样本都重叠较少的情形下使用。

中心化联邦学习是一种中心化机器学习架构，又称客户服务器架构[17]，在该架构下，具有一个中央服务器节点，用来协调各参与方之间的模型训练，负责聚合从各参与方接收过来的局部模型，并进行全局模型分发，其适用于需要中央服务器节点进行协调的应用场景。相对的，去中心化联邦学习无需中央服务器节点来对参与方进行协调，适用于无需中央服务器的场景。其中，去中心化联邦学习又被称为对等网络架构，即各参与方之间是对等关系，由于不存在中央节点，故该方式的安全性能更高，但同时参与方之间的交互需要更多的加解密操作来保证其安全性。

跨设备和跨筒仓联邦学习是由 Kairouz 等人在文献[23]中提出，该分类较为宽泛，其中跨设备联邦学习中的参与方通常是面向移动或物联网设备，如手机终端设备以及穿戴式设备等，这些设备的数量规模庞大，但计算和存储能力有限，只能承载小部分数据的模型训练。跨筒仓联邦学习的参与方通常都是面向一些企业和组织机构的数据中心，这些终端都具有较高的性能和较强的计算能力，能够进行大规模数据的模型训练。

以上三种分类各有针对，其简要概述如下表 2 所示。

表 2　联邦学习分类

Table 2　Classification of federated learning

划分依据	分类	简要描述
数据分布	横向联邦学习	适用于数据特征有较多重叠而数据样本重叠较少的情形
	纵向联邦学习	适用于数据样本有较多重叠而数据特征重叠较少的情形
	联邦迁移学习	适用于数据特征和数据样本均有较少重叠的情形
网络拓扑	中心化联邦学习	适用于需要中央节点进行协调的情形
	去中心化联邦学习	适用于无需中央节点进行协调的情形
设备数和性能	跨设备联邦学习	适用于手机终端等性能较弱的个人边缘设备
	跨筒仓联邦学习	适用于企业等组织机构性能较强的终端设备

2 联邦学习安全

联邦学习在保护用户隐私安全以及解决数据孤岛问题方面具有很大潜力，主要由充当数据提供者的参与方以及用来聚合全局模型的协调方中央服务器节点两大实体组成，除此以外，模型训练结束后，还有模型的使用方参与其中。其能够将各参与方的原始数据保存在本地，

通过交换模型和参数来完成全局模型更新，然而，尽管在联邦学习过程中没有发生原始数据的交换，但仍存在安全威胁问题，本节将对联邦学习的安全性问题进行探讨。

2.1 安全三要素

联邦学习中，数据安全是重中之重，是联邦学习的基础与核心，要想联邦学习的安全性得到保证，必须保证安全的三要素，即机密性、完整性和可用性[24]。其中，机密性是指利用加密手段对数据信息进行加密处理，保护隐私信息避免泄露和非授权查看，联邦学习中即保证训练模型中的参数和数据等敏感信息不会被攻击者窃取，完整性是指利用网络安全技术保障数据的完好无损，不能被非授权修改，联邦学习中即保证模型在训练和预测过程中不受到外界的干扰，能够保障结果的完整和正常输出，可用性是指能够提供正常服务，保证服务不被中断，联邦学习中即保证训练出的模型能够被使用方正常使用。

2.2 联邦学习安全分类

通常来说，联邦学习假设所有参与进来的实体都是诚实并且可信的，然而在实际应用过程中，该假设并不能完全保证[25]，其中极有可能会存在半诚实甚至是恶意方，半诚实参与者能够正常遵守训练协议进行模型训练，但是可能会对其他参与方的隐私数据感到好奇，想要从中获取隐私信息，而恶意方则可能为了达成某种目的完全不遵循联邦学习训练规则，试图获取、篡改甚至破坏数据模型。本节将根据安全威胁的来源和安全三要素对联邦学习中面临的安全问题进行分类论述。

2.2.1 根据安全来源划分

联邦学习的整个过程离不开三大实体，即数据提供方、服务器节点以及模型使用方，因此其安全性保障也关键在于这三者，根据安全威胁的来源不同，可将攻击划分为参与方攻击、服务器攻击、外部攻击以及系统自身漏洞攻击[26~28]。其中，参与方攻击主要是指不诚实的参与方在进行模型训练时利用参与方身份对共享模型中的模型参数进行推理，试图从中获取其他参与方的隐私数据，造成数据泄露，甚至在局部模型训练时加入脏数据，从而影响全局模型效果。服务器攻击主要是指选取了不可信的服务器节点来协调训练模型，当参与方将局部模型参数发送至服务器节点时，其会试图从中获取参与方的隐私信息，而在分发全局模型时刻意将被篡改过的错误模型发送给参与方，从而影响局部模型效果，导致训练失败。外部攻击主要是指在参与方与服务器节点进行模型参数交换时，恶意攻击者从传输通道中窃取训练模型及参数梯度信息，试图从中获取数据隐私信息。系统自身漏洞攻击[29]则是指由于联邦学习系统自身存在设计漏洞，恶意攻击者利用这些漏洞实行攻击，通过对系统中获取的信息进行推断分析，从而获取隐私数据信息。

2.2.2 根据安全三要素划分

根据联邦学习安全的三要素，其对应的攻击可划分为机密性攻击、完整性攻击和可用性攻击[30,31]。其中机密性攻击是指针对数据模型机密性发起的攻击，主要的攻击方式有模型提取、模型反转以及重构攻击，其中模型提取攻击旨在通过向服务器持续发送特定数据来获得响应结果，根据响应结果对原模型中的具体功能和参数进行推测，从而复制重建一个与原模型功能类似的替代模型，即希望通过创建一个替代模型来代替完成目标模型所要完成的任务，其目的是为了窃取模型。模型反转攻击，又称模型逆向攻击，是指先用系统 api 来得到模型的部分信息，根据这些模型信息来逆向分析从而推测模型中的隐私信息，即攻击者通过对模型的预测结果进行分析并试图从中提取出用户隐私信息，根据不同的推测目的，模型反转攻击又可作进一步的划分，其中，以推测某个成员是否参与到训练中为目的的攻击称为成员推理攻击[27]，以推测某些统计信息为目的的攻击称为属性推理攻击。重构攻击是指攻击者试图在模型训练过程中通过获取某种标签属性或特征，使用属性推理等特定方式从中恢复重构部分或全部原始数据[32]。

完整性攻击针对的是模型的完整性，其主要攻击方式有对抗攻击、模型投毒攻击以及后门攻击。其中，对抗攻击[33]是指攻击者向原始数据中加入扰动过的数据样本，该样本又称对抗样本，导致模型不能正确识别样本而做出错误的判断从而影响模型准确度，以高置信度给出错误输出。根据针对的对象不同对抗攻击常分为逃逸攻击与数据中毒，前者主要针对模型通过构造对抗样本逃出模型的预测结果，后者则是针对数据通过在输入模型数据中加入质量差的脏数据或错误数据来扰乱数据分布，从而影响模型质量，破坏模型完整和可用。除此以外，根据扰动范围的不同，对抗攻击还可分为全局像素扰动攻击和部分像素扰动攻击，根据攻击者所得到的目标模型知识的不同，又可将其分为白盒攻击和黑盒攻击，根据是否指定分类类别可分为定向攻击和非定向攻击，根据攻击频次还可分为单次攻击和迭代攻击[34]，不同的场景可选择不同种类的攻击方式。模型投毒攻击与数据投毒类似，是指在参与方与服务器节点进行模型交换时通过发送错误或损坏的模型和参数来影响全局模型质量，

其针对的是模型参数，而不直接操作数据。后门指的是一种通过绕过系统安全控制而获得访问控制权的方法，其目的是为了方便下次秘密进入或控制系统，后门攻击[35]即是通过在模型训练过程中对模型植入带有触发器的秘密后门，当触发器未被激活时，模型训练正常，而一旦激活，模型则会按照攻击者预先设定的某种规则进行训练从而达到攻击目的。

类似的，可用性攻击即针对的是模型的可用性，其主要攻击方式是数据投毒攻击和拜占庭攻击，数据投毒攻击即数据中毒，如前所述，数据中毒不仅能够破坏模型的完整性，还能对模型的可用性造成破坏，而拜占庭攻击是指攻击者能够对多个参与用户进行控制，这些用户能够通过对本地更新后的模型参数进行修改从而可以发送任意参数去干扰和破坏全局模型的准确度，最终导致模型训练失败[36]。

除了上述划分，还可根据攻击在联邦学习过程中所处阶段的不同，将攻击划分在不同的阶段[17, 27]，如属性推理攻击是在数据的发布阶段，重构攻击是在模型的训练阶段，而成员推理攻击则发生在模型的推理阶段等。根据针对的联邦学习类型的不同，可将攻击划分为对横向联邦学习的攻击和对纵向联邦学习的攻击等[37]。对联邦学习安全重点概述的两种划分中的部分攻击图示如图1所示，简述如下表3所示。

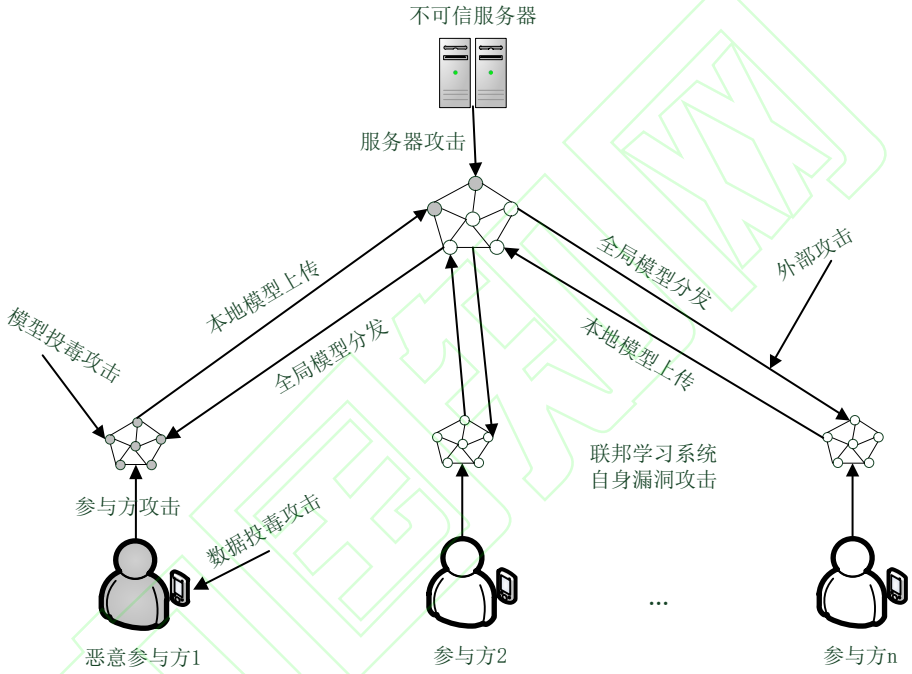

图 1 联邦学习中部分攻击

Fig. 1 Partial attacks in federated learning

表 3 联邦学习安全分类

Table 3 Federated learning security classification

划分依据	分类	描述
安全威胁来源	参与方攻击	不诚实参与方试图从共享模型中获取隐私数据，参与模型训练时加入脏数据破坏全局模型
	服务器攻击	不可信服务器试图从全局模型中获取隐私信息，分发篡改过的错误模型给参与方
	外部攻击	攻击者试图从传输通道中窃取隐私信息
	系统漏洞攻击	攻击者利用联邦学习系统的设计漏洞实行攻击
安全三要素	机密性攻击	针对机密性发起的攻击，攻击方式主要有模型提取攻击、模型反转攻击以及重构攻击，其中模型反转攻击又包含成员推理和属性推理攻击
	完整性攻击	针对完整性发起的攻击，攻击方式主要有对抗攻击、模型投毒攻击以及后门攻击
	可用性攻击	针对可用性发起的攻击，攻击方式有主要有数据投毒攻击和拜占庭攻击

2.3 联邦学习安全研究进展

有关联邦学习的安全问题近年来已有不少研究，针对联邦学习中全局模型容易受到恶意参与方中毒数据的攻击，但已有策略存在计算开销大、健壮性不足及隐私安全等问题，文献[38]提出了恶意参与方检测联邦学习MCDFL 来防御标签翻转攻击，其能够通过恢复潜在特征空间上的分布来识别恶意参与方，以检测各参与方的数据质量，实验表明该方案在不同的条件下检测恶意参与方具有鲁棒性，且不会产生过高的成本。针对联邦学习中异常聚合器或恶意参与方可能在训练阶段发起模型

反演攻击和模型中毒攻击，文献[39]提出了一种双掩码联邦学习框架 DMFL，该框架提倡在聚合过程中上传部分权值，并在终端设备和聚合器端同时使用两种掩码，在基于图像分类基准数据上的实验表明，所提 DMFL 框架性能优于其他基线，能够成功保证权重私密性和保护模型的安全性。针对在异构环境中为实现联邦学习框架的系统性和鲁棒性而不能在全局模型更新过程中删除任何局部模型的问题，文献[40]提出了一种名为 FedEqual 的防御策略来减轻模型中毒攻击，在不排除任何良性模型的情况下保持学习任务的性能，实验表明，FedEqual 在不同异构环境下的性能优于其他最新的中毒攻击模型。针对联邦学习中由于固有分布式和隐私保护特性而产生的后门攻击，文献[41]提出了 RDFL 算法，通过对比 MNIST、FEMNIST 和 CIFAR-10 数据集在非独立同分布情形下的现有基线，评估了 RDFL 的性能，并考虑不同的攻击情景，包括不同数量的恶意攻击、分布式后门攻击、不同毒性比的局部数据和模型中毒攻击，实验表明 RDFL 能够有效减轻后门攻击，性能优于所比较的基线。文献[42]针对联邦学习中的模型替换攻击和后门攻击提出了一种新颖有效的检测和防御技术，实验评估结果表明，与现有技术相比该技术能够有效检测和防御联邦学习中的后门攻击，在保持原有训练模型准确度的条件下使得后门攻击的成功率和持续时间大大降低。针对联邦学习中攻击者仍可通过发起重构攻击和成员推理攻击来利用局部梯度和参数获取本地训练数据，文献[43]提出了一种有效的联邦学习模型扰动方法，以防御好奇参与方发起的重构和成员推理攻击，实验表明所提方法在回归和分类任务中都达到了与非私有方法相同的准确性，且优于最先进的防御方案。

随着联邦学习技术的不断发展和完善，越来越多的数据将被用于联邦学习中，对联邦学习安全技术的研究将有助于提高数据隐私和模型安全的保护能力，促进联邦学习技术在各领域的安全应用和推广，随着对联邦学习研究的深入和技术的不断成熟，相信在不久的将来联邦学习安全领域也将有更多的研究进展和新的突破。

3 隐私保护技术

联邦学习中只有模型和参数在参与方和服务器之间进行交换和传递，而数据保留在参与方本地，在模型参数的传递过程中要用隐私保护技术来对其进行脱敏保护，本节将对常用隐私保护技术进行分类，结合隐私保护技术在联邦学习中的应用对常用的隐私保护技术进行综述。

3.1 隐私保护技术分类

根据保护手段的不同，现阶段常见隐私保护技术大概可分为四类，第一类是基于数据加密的密码学方式对数据进行保护[44]，该方式最为常见，使用的技术方法有对称加密、非对称加密、安全多方计算等，联邦学习中以安全多方计算最为常见，其实现方式有秘密共享、混淆电路、不经意传输和同态加密等。第二类是基于数据扰动的方式对数据进行保护，其常用的技术是差分隐私，主要是通过添加噪音来对原始数据进行干扰和模糊处理。第三类是基于数据匿名的方式对数据进行保护，其常用的技术有 k-匿名、l-多样性以及 t-接近等，采用的匿名化操作主要有抑制、泛化、解剖、扰动和置换[45]。第四类则是一种基于可信硬件的隐私信息保护技术，常用技术是可信执行环境，通过创建一个安全隔离的执行环境来保护数据安全[46]。

近年来，用于联邦学习中的隐私保护技术以基于数据加密、基于数据扰动以及基于可信硬件三类隐私保护技术最为常见，有关基于数据匿名的隐私保护技术研究较少，联邦学习中常用的隐私保护技术分类如下图 2 所示，其详细介绍将在下文论述。

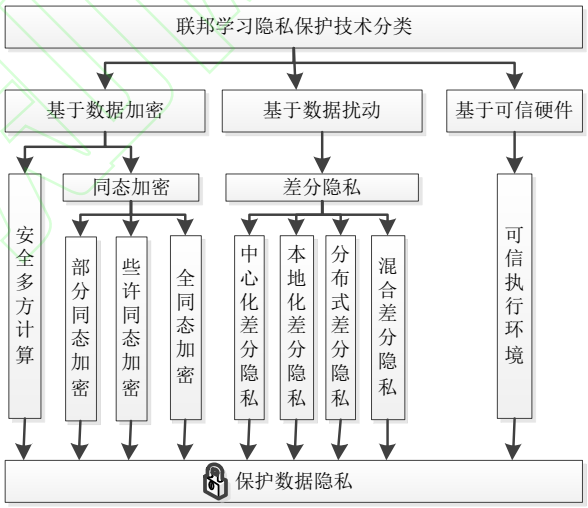

图 2 隐私保护技术分类

Fig. 2 Classification of privacy protection technologies

3.2 基于加密的密码学方法

3.2.1 安全多方计算

安全多方计算(secure multi-party computing，SMC)是为了实现两方之间数据的安全比较于 1982 年由图灵奖获得者姚期智提出[47]，是一种用于多个参与方之间协作计算的分布式计算技术，其目的是为了解决如何在保护各方隐私信息且没有可以信任的第三方的条件下多个互不信任的参与方之间协同一起进行计算的问题。也就是在分布式环境下，由多个参与方对某个特定的函数一起进行计算，各个参与方各自提供对该函数的输入值，

待计算结束后，各参与方得到正确的输出结果[48,49]，其中任意参与方不能得知除其本身以外的任何输入输出信息。具体可作如下定义，假设共有n位参与方，各参与方记为P_i，各参与方输入的隐秘数据记为x_i，输出记为y_i，其中，$i=\{1,2,\dots,n-1,n\}$，则各方协同计算的函数表达式可表示为$y_1,y_2,\dots,y_{n-1},y_n=f(x_1,x_2,\dots,x_{n-1},x_n)$，各参与方$P_i$不能获知除其本身输入$x_i$和输出$y_i$以外的任意值，即只能根据自己的输入$x_i$来得到计算结束后的输出$y_i$，各方对自己的输入输出值严格保密，其计算过程展示为图 3 所示。

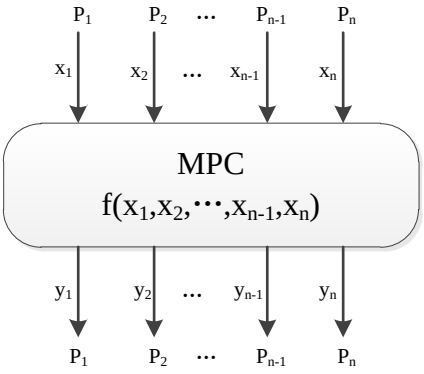

图 3 安全多方计算

Fig. 3 Secure multi-party computing

安全多方计算是联邦学习中常用的一种隐私保护技术，为了消除服务器在一般联邦学习设置中必须是诚实的约束，文献[50]提出了一种增强的安全多方计算方法，在基本信息传输到服务器之前，通过两轮分解对局部模型进行加密，理论分析和实验表明，该方案能够为训练数据的安全性和隐私性提供更强的保护，同时将产生的额外通信和计算成本降至最低。文献[51]使用安全多方计算构建了一个保护隐私的联邦学习框架，用来解决医院间进行协作式模型训练时访问模型参数或梯度会暴露私有训练样本的问题，通过在存储库 The Cancer Genome Atlas(TCGA)上进行实验，并与差分隐私和联邦平均作为基线进行比较，表明该框架能够在防止隐私泄露的前提下得到更高的准确率，但代价就是会产生更高的通信开销。文献[52]为了解决使用安全多方计算保护聚合本地模型时在分散环境中的高通信成本和可扩展性较差的问题，设计了一种通信高效的新型安全多方计算 CE-Fed 来支持联邦学习，并在不同的数据集上证明了 CE-Fed 的有效性，表明其能够在不泄露隐私的情况下实现更高的精度、通信效率和可扩展性。文献[53]为了解决数据共享中的安全和效率问题，提出了一个基于安全多方计算的特征工程框架，该框架能够在确保数据安全的前提下支持多方参与特征工程，与现有方法相比，该框架的核心算法具有更高的计算效率。

3.2.2 同态加密

同态加密（homomorphic encryption，HE）是一种基于数学计算的方式来进行加密的密码学技术，于 1978 年由 Rivest 等人在文献[54]中提出，该技术能够在不用对加密数据解密的情形下就对其直接进行计算，可支持多次加法或乘法运算，经由同态加密的方式处理过的数据能够在解密后与未加密的原始数据做同样的操作保持同样的输出。根据不同的运算种类和运算次数，可以将同态加密划分为部分同态加密、些许同态加密以及全同态加密[15,17,20]。其中，部分同态加密可支持任意次数的运算，但加法和乘法不能同时使用，只允许使用其中一种，些许同态加密仅可以支持有限次数的运算，但允许加法和乘法同时混合使用，全同态加密则能够支持满足任意次数的加法同态和乘法同态之间的混合运算，目前同态加密在联邦学习中的应用以使用加法运算的同态加密最为常见。具体可做如下定义，若将明文数据记为m_1，m_2，其对应密文数据记为c_1，c_2，Enc()记为某种加密函数，f()记为某种运算，可以为加法同态或是乘法同态，则$c_1=Enc(m_1)$，$c_2=Enc(m_2)$，同态加密的基本性质可表示为$Enc\big(f(m_1,m_2)\big)=f(c_1,c_2)$，即对明文数据$m_1$，$m_2$先加密后运算等价于先运算后加密[55]。

近年来，有关同态加密在联邦学习中的应用的研究较多，文献[56]为了防止参与用户在联邦学习过程中退出并可能会破坏用户和参数服务器，提出了一个分布式阈值加法同态加密的抗退出方案，评估表明该方案具有一定安全性，当联邦学习中的参与方数量超过 26 时，具有较低的通信开销。文献[57]为了避免深度学习模型尤其是使用医疗数据的应用程序遭受对抗性攻击，提出了一个使用了同态加密的医疗数据隐私信息保护联邦学习算法，该算法使用安全的多方计算协议来保护深度学习模型免受对手的攻击，并在医学数据集上根据模型性能进行了评估。文献[58]为了防止数据所有者在将中间模型传输到中央服务器的过程中隐私信息遭受侵犯，提出了一种可以使用不同的加密密钥来实现同态操作的算法，该算法能够避免同态加密只有在使用相同加密密钥加密才能计算的限制，安全性有了一定的提升。文献[59]为了解决联邦学习中共享的模型参数安全性较弱存在隐私数据泄露的问题，提出了一种隐私增强联邦平均(PE-FedAvg)的方案来增强模型参数的安全性，该方案实现了与 FedAvg 相同的训练效果，但是增加了额外时间开销，与基于 Paillier 的联邦平均相比，该方案在通信和计算成本方面具有更好的性能，采用 CKKS 同态加密来对模型参数加密，

实验验证了该方法的有效性以及在通信和计算方面的优势。文献[60]为了解决联邦学习中客户端之间数据分布差异和全局分布偏度的统计异质性问题，提出了一种名为 Dubhe 的可插拔系统级客户端选择方法，该方法允许客户端在使用同态加密保护其隐私的情况下参与训练，实验结果表明 Dubhe 在分类精度上与最优贪婪方法不相上下，其中的加密和通信开销可以忽略不计。

3.3 基于数据扰动的方法

3.3.1 差分隐私

差分隐私（differential privacy，DP）是一种通过在敏感数据上添加噪声的方式来对计算过程进行干扰从而保护数据隐私的方法，由 Dwork 等人于 2006 年在文献[61]中首次提出，其主要目的是为了能够隐藏模型参数等隐私信息，使敏感数据失真，从而让参与方无法从中反推原始数据。主要思想是若对某数据集中的单个数据使用其他数据替换，该替换对数据集的影响可以忽略不计，而当恶意方试图从数据集中查询某个单一个体时，无法从查询结果中获取到个体的任何有用信息，则可认为这个数据集中的单个个体的隐私信息得到了保护[15,20]。

具体可作如下定义，对于给出的两个数据集D和D'，其中D和D'两者之间只相差一条数据记录，具备这种特性的数据集又被之称为相邻数据集，数据持有者以某个数据集为输入的随机算法记为A，$A(D)$表示使用A算法从数据集D上进行某个体的查询时处理的输出，A的所有可能子集记为S，即$S \subseteq Range(A)$，$Range(A)$为 A 的一个取值范围[62]，Pr[]为取概率，若存在正实数ε，使得$\Pr[A(D) \in S] \leq e^{\varepsilon} \cdot \Pr[A(D') \in S]$，则称算法$A$能够满足$\varepsilon$-差分隐私，以上不等式说明若在两个给定的相邻数据集D和D'上使用算法A得到的输出结果$A(D)$和$A(D')$的概率相差不大，则该算法可达到差分隐私效果。

差分隐私技术主要有拉普拉斯机制、高斯机制和指数机制三种加噪的机制，其中前二者主要适用于数值型的查询，而第三者则适用于非数值型的查询[63]。根据应用场景的不同，差分隐私通常被化分为中心化差分隐私、本地化差分隐私、分布式差分隐私[64]和混合差分隐私四种，差分隐私被提出之初大多情形下是指中心化差分隐私，即将各方的原始数据收集至一个高度可信第三方进行汇总，通过对整体的计算结果来加噪进行干扰以实现差分隐私。然而，在实际的应用过程中，要找到这种高度可以信任的第三方通常不太容易，因此便有了本地化差分隐私，本地化差分隐私无需将数据进行收集，而是将各方原始数据存放在数据源本地，即认为第三方不可信，其数据完全由各数据提供方掌控，直接在本地数据集上实行差分隐私，然后再传输到第三方进行聚合，保护的是用户将脱敏数据上传至第三方的这个过程。分布式差分隐私中需要用到若干个可信的中间结点，多个参与方先将各自处理过的模糊数据传递至可信的中间结点执行聚合操作后再进一步使用隐私技术，而后再将脱敏后的数据传输至服务端，即需要参与方先在各自的本地使用差分隐私完成简单的扰动，再将结果发送至可信中间节点，借助安全聚合或安全混洗等方式在可信的中间节点上再次的使用隐私技术，最后各中间节点再将所得结果发送给服务端[65]。混合差分隐私是由 Avent 等人[66]在 2017 年提出，其认为本地化差分隐私与中心化差分隐私可以同时共存，通过参与方对服务器信任关系的不同对参与用户分类，各参与用户根据与服务器的信任关系来决定是直接上传原始数据还是在本地使用本地化差分隐私。

联邦学习中将原始数据存放在参与方本地的特质与本地化差分隐私有着极大的相似，近年来有关联邦学习与差分隐私的研究也大多集中在本地化差分隐私。文献[67]为了解决在跨筒仓联邦学习中用户级隐私存在泄露风险的问题，提出了一个利用本地化差分隐私来保护跨筒仓联邦学习的三平面框架，其中本地差分隐私能够在提供强大的数据隐私保护的同时仍保留用户数据统计信息以保持其高实用性，通过在数据集上进行实验验证了所提出的框架是有效的。文献[68]提出了一种新的用于工业环境的本地差分隐私专用的联邦学习协议 LDPFL，该协议能够在不受信任实体的工业环境中运行，相对现有方法具有更强的隐私保证，能在较小的隐私预算如$\varepsilon = 0.5$的情况下表现出高达 98%的联邦学习模型性能。文献[69]为了防止攻击者从传递的模型参数中推断出隐私信息，减少差分隐私保护模型的通信开销，提出了具有局部差分隐私机制的联邦学习通用矢量量化方法，以此来对模型参数进行量化，通过隐私性能分析以及计算日志时刻来跟踪隐私损失，表明即使量化位相对较小，该方法也能在不降低全局模型精度的情况下实现模型压缩。文献[70]为了防止参与客户端串通暴露诚实客户模型参数的攻击，提出了一种基于遗忘分布式差分隐私的机制来缩小这种共谋差距，利用该隐私机制构建了一个改进的联邦学习安全协议，通过在 5000 个分布式网络客户端的真实模型中对两个数据集的协议执行速度、准确率和隐私性进行了实证分析，证明了该协议的安全性。文献[71]为了解决模型训练时隐私保护不佳以及训练准确率不足，提出了一个分布式差分隐私联邦学习框架 Hyades，该框架高效且能灵活适应客户端退出，评估表明，与现有方案相比，Hyades 能够高效处理各种现实场景中的客户端掉线，实现最佳的隐私效用权衡，并将训练速度提

高了 2.1 倍。文献[72]为了解决参与用户对服务器的信任问题，实现不同用户的不同隐私需求，使用混合差分隐私集成到联邦学习中，提出了一种安全且足够可靠的联邦学习算法，通过对所提算法的收敛能力和隐私安全边界做了对应的分析，提出了一种自适应梯度剪裁方案和改进过的合成方法，用来减少噪声和裁剪的影响，评估结果验证了该算法是有效的。

3.4 基于可信硬件的方法

3.4.1 可信执行环境

可信执行环境（trusted execution environment，TEE）指的是一种可以信赖的计算环境，是存在于计算平台上的一个与不可信操作系统相互独立的可信隔离环境，其运用了包括可信计算和虚拟隔离等多种技术在内的技术组合[73]，为需要进行安全保护的隐私数据信息提供一个安全可信的空间，以确保在该环境下的程序和数据的安全和完整，是一种基于硬件环境的安全计算方案，即其安全性由相关硬件机制来保证。常见的可信环境有 Intel 软件防护扩展(software grard extensions，SGX)、Intel 管理引擎(manage-ment engine，ME)以及 AMD 内存加密技术[46,74]等。

联邦学习中需要进行模型的安全聚合等隐私保护操作，研究使用可信执行环境来保证计算环境的安全具有重大意义。文献[75]为了防止在使用受信任的 SGX 处理器保护梯度信息时受到侧信道攻击，提出了一个使用可信 SGX 的梯度保持系统，该系统结合了随机组结构和组内梯度段聚合，分析评估表明其能够有效保证参与者的梯度隐私，并能较好的适用于联邦学习系统。文献[76]为了防止联邦学习中攻击者从中间梯度中逆推私有数据，提出了一种基于可信执行环境的分布式联邦学习框架，从硬件的角度来保护梯度，使用可信 SGX 作为实现联邦学习的实例，提出了 SGX-FL 框架，评估结果表明 SGX-FL 的计算成本比现有方法降低了 19 倍。文献[77]为了防止联邦学习中的隐私泄露，提出并实施了隐私保护联邦学习框架 PPFL，在客户端上使用可信执行环境进行本地训练，并在服务器上使用可信执行环境进行安全聚合，以此更新模型梯度，性能评估表明，PPFL 能够显著改善隐私并在客户端产生较小的系统开销。文献[78]为了防止在联邦学习训练过程中可能存在一些恶意方在模型中加入篡改过的错误结果来破坏模型，提出了一个新型的联邦学习隐私信息保护方法来保证模型在训练时的完整性，使用可信执行环境设计了一种训练协议，通过实验原型实现及性能评估表明所提出的方案是有效的。

联邦学习的根本目的是为了能够充分整合各方数据，使得数据中的价值最大化，要想在不泄露用户隐私数据的条件下使得各方数据得到共享，隐私保护技术的作用至关重要。由上文可知，联邦学习中的隐私安全技术已有不少研究，然而这些研究大多都是将单个隐私保护技术应用在联邦学习上，用来保护联邦学习中的单个方面或是某个环节的数据隐私安全，为了加强对联邦学习中隐私信息的安全防护，近年来已出现将多个隐私保护技术相结合来保护联邦学习中数据的相关研究。文献[79]针对联邦学习中的安全漏洞问题，设计了工业互联网中区块链赋能联邦学习的应用模型，并基于模型制定了数据保护聚合方案，给出了基于差分隐私和同态加密的分布式 K 均值聚类，以及具有差分隐私的分布式随机森林和具有同态加密方法的分布式 AdaBoost 方法，在数据共享和模型共享中实现了多重数据保护，将所提方法与联邦学习结合，实验结果表明该聚合方案和工作机制在所选指标中具有较好的表现。文献[80]为了弥合中心化差分隐私和本地化差分隐私之间缺乏可信服务器而产生的效用差距，提出了一个利用可信执行环境结合中心化差分隐私和本地化差分隐私优点的系统 Olive，在真实数据上的实验结果表明即使在训练中具有数十万个参数模型，该系统也能有效工作，同时能够确保敏感信息完全遗忘从而使联邦学习安全更易于实现。

联邦学习中常用隐私保护技术简述如下表 4 所示，其中，同态加密和差分隐私分类如表 5 所示，联邦学习中隐私保护技术研究进展总结如表 6 所示。

表 4　联邦学习隐私保护分类

Table 4　Federated learning privacy classification

分类	隐私保护技术	描述
基于数据加密	安全多方计算 同态加密	解决互不信任的参与方之间在保护数据隐私且没有可信的第三方的条件下协同计算的问题 能够在无需解密的情况下对加密数据直接进行计算，可支持多次加法或乘法运算，经由同态加密的方式处理过的数据能够在解密后与未加密的原始数据做同样的操作保持同样输出
基于数据扰动	差分隐私	通过以在敏感数据上添加噪声使敏感数据失真的方式来对计算过程进行干扰从而保护数据隐私，目的是为了隐藏信息
基于可信硬件	可信执行环境	一种可以信赖的计算环境，是存在于计算平台上的一个与不可信操作系统相互独立的可信隔离环境，安全性由相关硬件机制保证

表 5　同态加密与差分隐私分类

Table 5　Homomorphic encryption and differential privacy classification

隐私保护技术	分类	描述
同态加密	部分同态加密	支持任意次数加法或乘法运算
	些许同态加密	支持有限次数加法和乘法运算
	全同态加密	支持任意次数加法和乘法运算
差分隐私	中心化差分隐私	将数据收集至一个高度可信第三方，对整体计算结果进行扰动
	本地化差分隐私	将数据存放至本地，在本地进行数据扰动
	分布式差分隐私	先在本地进行简单扰动，再将结果发送至可信中间结点进行进一步隐私保护，最后发送至服务端
	混合差分隐私	根据参与方对服务器的信任关系决定进行本地化差分隐私还是中心化差分隐私

表 6　联邦学习中隐私保护技术研究进展总结

Table 6　Summary of research progress of privacy protection technology in federated learning

分类	文献	提出的方案	拟解决的问题
安全多方计算	[50]	一种增强的安全多方计算方法	消除服务器在一般联邦学习设置中必须是诚实的约束
	[51]	一个保护隐私的 FL 框架	解决协作式模型训练时访问模型参数或梯度暴露私有样本的问题
	[52]	一种通信高效的新型 MPC	解决 MPC 在分散环境中通信成本高和可扩展性差的问题
	[53]	一个基于 MPC 的特征工程框架	解决明文和密文数据共享中的安全和效率问题
同态加密	[56]	一个分布式阈值加法 HE 抗退出方案	防止参与用户中途退出并可能破坏用户和参数服务器
	[57]	一个使用了 HE 的联邦学习算法	避免遭受对抗攻击
	[58]	一种可以实现同态操作的算法	防止本地模型传输到服务器过程中隐私数据遭受侵犯
	[59]	一种隐私增强联邦平均方案	解决共享的模型参数安全性较弱存在隐私泄露问题
	[60]	一种可拔插系统级客户端选择方法	解决数据统计异质性问题
差分隐私	[67]	一个保护跨筒仓 FL 的三平面框架	解决跨筒仓 FL 中用户级隐私存在泄露风险的问题
	[68]	一种新的用于工业环境的 FL 协议	在不受信任的工业环境中提供更强的隐私保证
	[69]	一种 FL 通用矢量量化方法	降低差分隐私保护模型的通信开销
	[70]	一种分布式差分隐私机制	防止参与客户端串通暴露诚实客户模型参数的攻击
	[71]	一个分布式差分隐私 FL 框架	解决模型训练时隐私保护不佳以及训练准确率不足的问题
	[72]	一种安全且足够可靠的 FL 算法	解决参与用户对服务器的信任问题，实现不同用户的不同隐私需求
可信执行环境	[75]	一个可信 SGX 梯度保持系统	防止在使用受信任的 SGX 处理器保护梯度信息时受到侧信道攻击
	[76]	一种基于 TEE 的分布式 FL 框架	防止 FL 中攻击者从中间梯度中逆推私有数据
	[77]	一个隐私保护 FL 框架	防止联邦学习中的隐私泄露
	[78]	一个新型的 FL 隐私信息保护方法	防止 FL 训练过程中恶意参与方在模型中加入篡改过的数据来破坏模型

4 未来研究方向

联邦学习作为一个用来解决数据隐私安全和孤岛问题的可行方案，自从被提出以来就受到了相关从业人员的广泛关注并成为近几年的研究热点，随着研究的深入以及相关技术的日渐成熟，联邦学习也迎来了需要进一步研究和解决新的问题和挑战，本节将对联邦学习中所面临的问题和挑战进行简要概述。

1）激励机制问题。通常来说，在实际应用场景中，大型企业或是组织由于用户数量庞大，其所具备的数据多而完整，对于想要训练一个理想模型，这些巨头企业通常具有较大的优势，而中小型企业由于用户数量较少，其所具备的数据少而残缺从而导致不足以训练一个理想模型，尽管联邦学习能够通过联合各方使用所有参与方的数据训练一个共享模型，但由于各方所具备的数据数量和数据质量各不相同，一些大型企业因为已具备训练理想模型条件往往不愿再参与到联邦学习中，如何创建一种合理的激励机制来评估各方贡献效益以实现激励资金的公平分配从而吸引更多的企业机构加入到联邦生态是联邦学习所面临的重要挑战[15,17]。

2）算力与通信效率问题。联邦学习模型训练过程中，虽然没有原始数据的直接传输，但依然会进行模型和参数的频繁传递和交换，为防止攻击者从模型参数中推断出隐私信息，仍需对这些模型参数进行加密脱敏后再传输，频繁的加解密操作无疑加大了系统的计算开销，这对于参与设备的算力提出了更高的要求[81]。加密脱敏后的模型参数通常具有更大的数据量，且参与设备量大，而多数情况下各参与方设备又与中央服务器距离相距较远，信息传输延迟概率增大，因此也具有更大的通信开销，如何在保护数据隐私安全的前提下解决联邦学习中的算力和通信负担过大的难题是联邦学习所面临的又一挑战[82]。

3）数据异构与设备异质。目前大多数机器学习模型都是使用随机梯度下降算法来进行迭代优化，而用于随机梯度下降算法的数据一般需要满足独立同分布才会表现良好[15,83]，联邦学习中各参与方所提供的数据通常都是在不同的业务场景中产生的，这些数据由于生成存储方式的不同而具备不同的属性特征和结构排列，常表现为非独立同分布的特性[84]，若将这些数据用在以往的机器学习算法上则可能不再适用[85]，研究适用于处理非独立同分布数据的算法是联邦学习面临的重要挑战。除此以外，联邦学习中因为各参与方设备的计算或存储性能、网络状态以及电池电量等的不同会造成设备的异质性，其容易造成参与方设备由于断电、断网等原因在训练过

程中中途退出，从而影响整个训练模型的训练结果，如何解决参与设备异质性问题也是联邦学习所面临一大挑战[86]。

4）其他问题。联邦学习除了面临以上挑战，同时还面临着一些其他的问题。如参与方的筛选问题[87]，通常考虑所有参与方都是诚实可信的，但在实际应用场景中却存在好奇甚至恶意的参与方，选取出诚实积极的参与方对于保护模型隐私安全和提升模型准确率具有重要意义。此外，联邦学习中的隐私保护也还有待完善，还需加强对隐私数据的保护力度[88]。

5 结束语

随着社会的快速发展和人类对生活质量要求的不断提高，人们对于个人隐私信息保护意识的观念有所加强，法律法规的不断出台致使以往的数据收集方式已属违法违规，联邦学习作为一种新兴技术能够在数据不出本地的情形下联合各方数据训练一个共有模型来解决数据孤岛问题而受到从业人员的广泛关注，该技术发展至今，正在逐步改善并不断走向成熟，具有广阔的研究使用前景。本文首先对联邦学习的相关背景做了相关介绍，从为什么会有联邦学习的角度先对机器学习和分布式机器学习进行了简要介绍，之后再引申出联邦学习这一概念，简要介绍了联邦学习的相关定义、发展历程以及常见分类，而后对联邦学习的安全和隐私保护技术进行了综述，最后简述了未来联邦学习研究中需要进一步解决的问题。如今联邦学习已经取得了重大的研究进展，未来的联邦学习研究将可能更多的关注如何更有效的隐藏数据隐私信息，同时保证模型的准确性和效率，并将其扩展到大规模环境中，探索如何更有效的处理大量设备的数据，使联邦学习技术进一步完善。

参考文献

[1] ROH Y J, HEO G, WHANG S E. A survey on data collection for machine learning: a big data - AI integration perspective[J]. IEEE Transactions on Knowledge and Data Engineering, 2021, 33(4): 1328-1347.

[2] ZHANG C, LI S, XIA J, et al. BatchCrypt: efficient homomorphic encryption for cross-silo federated learning[C]//USENIX Annual Technical Conference, 2020.

[3] YUE Z, LI M, LAI L Z, et al. Federated learning with Non-IID data[J]. ArXiv: 1806.00582, 2018.

[4] YANG Q, LIU Y, CHEN T J, et al. Federated machine learning: concept and applications [J]. ACM Transactions on Intelligent Systems and Technology, 2019, 10(2): 12:1-12:19.

[5] PILLUTLA K, MALIK K, MOHAMED A, et al. Federated learning with partial model personalization[J]. ArXiv: 2204.03809, 2022.

[6] MAMOUN A, RM S P, PARIMALA M, et al. Federated learning for cybersecurity: concepts, challenges, and future directions[J]. IEEE Transactions on Industrial Informatics 18, 2022, 3501-3509.

[7] 周志华.机器学习[M]. 清华大学出版社，2016，425.
ZHOU Z H. Machine learning [M], Tsinghua University Press, 2016,425. (in Chinese)

[8] VERBRAEKEN J, WOLTING M, KATZY J, et al. A survey on distributed machine learning[J]. ACM computing surveys, 2021, 53(2): 30.1-30.33.

[9] CUSTERS B H, SEARS A M, DECHESNE F, et al. EU personal data protection in policy and practice[M]. T.M.C. Asser Press, The Hague, 2019.

[10] 中华人民共和国网络安全法[EB/OL]. [2016-11-07]. http://www.cac.gov.cn/2016-11/07/c_1119867116_2.htm.
Cyber security law of the People's Republic of China [EB/OL]. [2016-11-07]. http://www.cac.gov.cn/2016-11/07/c_1119867116_2.htm. (in Chinese)

[11] 中华人民共和国数据安全法[EB/OL]. [2021-06-11]. http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm.
Data security law of the People's Republic of China [EB/OL]. [2021-06-11]. http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm. (in Chinese)

[12] 中华人民共和国个人信息保护法[EB/OL]. [2021-08-20]. http://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm.
Personal information protection law of the People's Republic of China [EB/OL]. [2021-08-20]. http://www.cac.gov.cn/2021-08/20/c_1631050028355286.

htm. (in Chinese)

[13] WANG X D, GARG S, LIN H, et al. Toward accurate anomaly detection in industrial internet of things using hierarchical federated learning[J]. IEEE Internet of Things Journal 9, 2022, 7110-7119.

[14] ANDREW H, RAO K, MATHEWS R, et al. Federated learning for mobile keyboard prediction[J]. ArXiv:1811.03604, 2018.

[15] 王健宗，李泽远，何安珣. 深入浅出联邦学习原理与实践[M]. 北京：机械工业出版社，2021.

WANG J Z, LI Z Y, HE A X. Principles and practice of federated learning in a simple way [M]. Beijing: Mechanical Industry Press, 2021. (in Chinese)

[16] DING J, ERIC W T, ANIT K S, et al. Federated learning challenges and opportunities: an outlook[C]//ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) , 2022, 8752-8756.

[17] 杨强, 刘洋, 程勇等. 联邦学习[M]. 北京: 电子工业出版社, 2020.

YANG Q, LIU Y, CHENG Y, et al. Federated learning[M]. Beijing: Publishing House of Electronics Industry, 2020. (in Chinese)

[18] MCMAHAN H B, MOORE E, RAMAGE D, et al. Federated learning of deep networks using model averaging[J]. CoRR, 2016.

[19] MCMAHAN B, RANAGE D. Federated learning: collaborative machine learning without centralized training data[EB/OL]. 2017. https://www.googblogs.com/federated-learning-collaborative-machine-learning-without-centralized-training-data/.

[20] 彭南博，王虎等. 联邦学习技术及实战[M]. 电子工业出版社，2021.

PENG N B, WANG H, et al. Federated learning technology and practice[M]. Publishing House of Electronics Industry, 2021. (in Chinese)

[21] BONAWITZ K, EICHNER H, GRIESKAMP W, et al. Towards federated learning at scale: system design[J]. CoRR, 2019, ArXiv: 1902.01046.

[22] 联邦学习全球研究与应用趋势报告 2022[R]. 2022. 清华大学深圳国际研究生院知识工程研究中心.

Global research and application trend report on federated learning 2022[R]. 2022. Knowledge Engineering Research Center, Shenzhen International Graduate School, Tsinghua University. (in Chinese)

[23] KAIROUZ P, MCMAHAN H B, AVENT B, et al. Advances and open problems in federated learning[J]. Found. Trends Mach. Learn. 2019, 14, 1-210.

[24] 邢云隆. 基于网络安全维护的计算机网络安全技术应用探讨[J]. 科技创新与应用, 2022, 12(25): 189-192.

XING Y L. Discussion on the application of computer network security technology based on network security maintenance[J]. Science and Technology Innovation and Application, 2022, 12(25): 189-192. (in Chinese)

[25] AHMED I, THAKKER U, WANG S Q, et al. A survey on federated learning for resource-constrained IoT devices[J]. IEEE Internet of Things Journal 9, 2021, 1-24.

[26] 梁天恺, 曾碧, 陈光. 联邦学习综述：概念、技术、应用与挑战[J]. 计算机应用, 2022, 42(12): 3651-3662.

LIANG T K, ZENG B, CHEN G. Review of federated learning: concept, technology, application and challenge[J]. Computer Applications, 2022,42(12): 3651-3662. (in Chinese)

[27] 王腾, 霍峥, 黄亚鑫等. 联邦学习中的隐私保护技术研究综述[J/OL]. 计算机应用：1-15[2022-12-21]. http://kns.cnki.net/kcms/detail/51.1307.TP.20220425.1937.008.html.

WANG T, HUO Z, HUANG Y X, et al. Overview of privacy protection technology in federated learning [J/OL]. Computer application: 1-15 [2022-12-21]. http://kns.cnki.net/kcms/detail/51.1307.TP.20220425.1937.008.html. (in Chinese)

[28] 吴建汉, 司世景, 王健宗等. 联邦学习攻击与防御综述[J].大数据, 2022, 8(05): 12-32.

WU J H, SI S J, WANG J Z, et al. Overview of federated learning attack and defense[J]. Big Data, 2022,8(05):

12-32. (in Chinese)

[29] QIAN C, YAO L, WANG L, et al. SecMDGM: federated learning security mechanism based on multi–dimensional auctions[J]. Sensors (Basel, Switzerland) 22, 2022.

[30] 王坤庆, 刘婧, 李晨等. 联邦学习安全威胁综述[J]. 信息安全研究, 2022, 8(03): 223-234.

WANG K Q, LIU J, LI C, et al. A review of security threats of federated learning[J]. Information Security Research, 2022, 8(03): 223-234. (in Chinese)

[31] 陈明鑫, 张钧波, 李天瑞.联邦学习攻防研究综述[J]. 计算机科学, 2022, 49(07): 310-323.

CHEN M X, ZHANG J B, LI T R. A review of the research on attack and defense of federated learning [J]. Computer Science, 2022, 49(07): 310-323. (in Chinese)

[32] VIRAAJI M, PARIXI R M, POURIYEH S, et al. A survey on security and privacy of federated learning[J]. Future Gener. Comput. Syst. 115, 2021, 619-640.

[33] TRUC D T N, THAI T. Preserving privacy and security in federated learning[J]. ArXiv: 2202.03402, 2022.

[34] 景慧昀, 周川, 贺欣. 针对人脸检测对抗攻击风险的安全测评方法[J]. 计算机科学, 2021, 48(07): 17-24.

JING H Y, ZHOU C, HE X. Security evaluation method for face detection against attack risk[J]. Computer Science, 2021,48 (07): 17-24. (in Chinese)

[35] CAO J R, ZHU L H. A highly efficient, confidential, and continuous federated learning backdoor attack strategy[C]//2022 14th International Conference on Machine Learning and Computing (ICMLC), 2022.

[36] LI M H, WAN W, LU J R, et al. Shielding federated learning: mitigating byzantine attacks with less constraints[J]. ArXiv: 2210.01437, 2022.

[37] 孙爽, 李晓会, 刘妍等. 不同场景的联邦学习安全与隐私保护研究综述[J]. 计算机应用研究, 2021, 38(12):3527-3534.

SUN S, LI X H, LIU Y, et al. A review of the research on federated learning security and privacy protection in different scenarios[J]. Computer Application Research, 2021, 38(12): 3527-3534. (in Chinese)

[38] JIANG Y F, ZHANG W W, CHEN Y X. Data quality detection mechanism against label flipping attacks in federated learning[J]. IEEE Transactions on Information Forensics and Security 18, 2023, 1625-1637.

[39] CHIU T C, LIN W R, PANG A C, et al. Dual-Masking framework against two-sided model attacks in federated learning[C]//2021 IEEE Global Communications Conference (GLOBECOM), 2021, 1-6.

[40] CHEN L, CHIU T C, PANG A C, et al. FedEqual: defending model poisoning attacks in heterogeneous federated learning[C]//2021 IEEE Global Communications Conference (GLOBECOM), 2021, 1-6.

[41] WANG Y K, ZHAI D H, HE Y P, et al. An adaptive robust defending algorithm against backdoor attacks in federated learning[J]. Future Gener. Comput. Syst. 143, 2023, 118-131.

[42] ZHAO C, WEN Y, LI S L, et al. FederatedReverse: a detection and defense method against backdoor attac ks in federated learning[C]//Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security, 2021.

[43] YANG X, FENG Y, FANG W J, et al. An accuracy-lossless perturbation method for defending privacy attacks in federated learning[C]//Proceedings of the ACM Web Conference 2022, 2020.

[44] 张鹏. 基于区块链的联邦学习隐私安全性研究[D]. 长春工业大学, 2022.

ZHANG P. Research on privacy security of federated learning based on blockchain[D]. Changchun University of Technology, 2022. (in Chinese)

[45] 钱文君, 沈晴霓, 吴鹏飞等. 大数据计算环境下的隐私保护技术研究进展[J]. 计算机学报, 2022, 45(04): 669-701.

QIAN W J, SHEN Q N, WU P F, et al. Research progress of privacy protection technology in big data computing environment[J]. Journal of Computer Science, 2022, 45(04): 669-701. (in Chinese)

[46] 中国信通院-隐私计算白皮书（2021 年）[R]，隐私计

算联盟，中国信息通信研究院云计算与大数据研究所. China academy of information and communications - white paper on privacy computing (2021)[R], Privacy Computing Alliance, Institute of Cloud Computing and Big Data, China Academy of Information and Communications. (in Chinese)

[47] YAO A C. How to generate and exchange secrets[C]//27th Annual Symposium on Foundations of Computer Science (sfcs 1986), 1986, 162-167.

[48] 冯琦. 基于安全多方计算的数据隐私保护技术研究[D]. 武汉大学, 2021.
FENG Q, Research on data privacy protection technology based on secure multi-party computing[D]. Wuhan University, 2021. (in Chinese)

[49] 孙茂华. 安全多方计算及其应用研究[D]. 北京邮电大学, 2013.
SUN M H, Research on secure multi-party computing and its application[D]. Beijing University of Posts and Telecommunications, 2013. (in Chinese)

[50] ZHANG C, EKANUT C, ZHEN L L, et al, Augmented multi-party computation against gradient leakage in federated learning[J]. in IEEE Transactions on Big Data, 2022.

[51] HOSSEINI S M, SIKAROUDI M, BABAIE M, et al. Cluster based secure multi-party computation in federated learning for histopathology images[C]//DeCaF/FAIR@MICCAI, 2022.

[52] KANAGAVELU R, WEI Q S, LI Z X, et al. CE-Fed: communication efficient multi-party computation enabled federated learning[J]. Array, 2022, 15.

[53] SUN L T, DU R M, HE D J, et al. Feature engineering framework based on secure multi-party computation in federated learning[C]//2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), 2021, 487-494.

[54] RIVEST, R L, MICHAWL L D. ON DATA BANKS AND PRIVACY HOMOMORPHISMS[J]. 1978.

[55] 周启贤. 基于同态加密的安全的机器学习研究[D]. 电子科技大学, 2021.
ZHOU Q X, Research on secure machine learning based on homomorphic encryption[D]. University of Electronic Science and Technology, 2021. (in Chinese)

[56] TIAN H B, WEN Y C, ZHANG F G, et al. A distributed threshold additive homomorphic encryption for federated learning with dropout resiliency based on lattice[C]//CSS, 2022.

[57] WIBAWA F, CATAK F O, SARP S, et al. Homomorphic encryption and federated learning based privacy-Preserving CNN training: COVID-19 detection use-case[C]//Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference, 2022.

[58] PARK J, YU N Y, LIM H, et al. Privacy-Preserving federated learning using homomorphic encryption with different encryption keys[C]//2022 13th International Conference on Information and Communication Technology Convergence (ICTC), 2022, 1869-1871.

[59] QIU F Y, YANG H, ZHOU H, et al. Privacy preserving federated learning using CKKS homomorphic encryption[J]. Wireless Algorithms, Systems, and Applications, 2022.

[60] ZHANG S L, LI Z R, CHEN Q, et al. Dubhe: towards data unbiasedness with homomorphic encryption in federated learning client selection[C]//50th International Conference on Parallel Processing, 2021.

[61] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating noise to sensitivity in private data analysis[C]//Theory of Cryptography Conference, 2006.

[62] 张鸿鸣, 鲍晓涵, 倪巍伟. 基于差分隐私的数据流频繁项集发布[J]. 计算机工程与设计, 2022, 43(11): 3051-3056.
ZHANG H M, BAO X H, NI W W. Data stream frequent itemset publishing based on differential privacy[J]. Computer Engineering and Design, 2022, 43(11):

3051-3056. (in Chinese)

[63] 张珊. 深度学习中差分隐私保护算法研究[D]. 内蒙古大学,2022.

ZHANG S, Research on differential privacy protection algorithm in deep learning[D]. Inner Mongolia University, 2022. (in Chinese)

[64] 李明霜. 基于分类数据的差分隐私保护研究[D]. 陕西师范大学, 2021.

LI M S. Research on differential privacy protection based on classified data[D]. Shanxi Normal University, 2021. (in Chinese)

[65] 杨庚, 王周生. 联邦学习中的隐私保护研究进展[J].南京邮电大学学报(自然科学版), 2020, 40(05): 204-214.

YANG G, WANG Z S. Research progress on privacy protection in federated learning[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2020,40 (05): 204-214. (in Chinese)

[66] AVENT B, KOROLOVA A, ZEBER D, et al. BLENDER: enabling local search with a hybrid differential privacy model[J]. J.Priv. Confidentiality, 9, 2017.

[67] WANG C, WU X K, LIU G Y, et al. Safeguarding cross-silo federated learning with local differential privacy[J]. Digital Communications and Networks, 2022, 8(4): 446-454.

[68] MAHAWAGA A, PATHUM C, LIU D X, et al. Local differential privacy for federated learning[J]. ESORICS, 2022.

[69] ZONG H X, WANG Q, LIU X F, et al. Communication reducing quantization for federated learning with local differential privacy mechanism[C]//2021 IEEE/CIC International Conference on Communications in China (ICCC), 2021: 75-80.

[70] BYRD D, MUGUNTHAN V, POLYCHRONIADOU A, et al. Collusion resistant federated learning with oblivious distributed differential privacy[C]//Proceedings of the Third ACM International Conference on AI in Finance, 2022.

[71] JIANG Z F, WANG W, CHEN R C, et al. Taming client dropout for distributed differential privacy in federated learning[J]. ArXiv: 2209.12528, 2022.

[72] LIU W Y, CHENG J H, WANG X L, et al. Hybrid differential privacy based federated learning for Internet of Things[J]. J.Syst. Archit.124, 2022, 102418.

[73] 姜建林. 基于可信执行环境的联邦学习模型安全聚合技术研究[D]. 武汉大学, 2021.

JIANG J L. Research on security aggregation technology of federated learning model based on trusted execution environment[D]. Wuhan University, 2021. (in Chinese)

[74] 宁振宇, 张锋巍, 施巍松. 基于边缘计算的可信执行环境研究[J]. 计算机研究与发展, 2019, 56(07):1441-1453.

NING Z Y, ZHANG F W, SHI W S. Research on trusted execution environment based on edge computing [J]. Computer Research and Development, 2019, 56 (07): 1441-1453. (in Chinese)

[75] ZHANG Y H, WANG Z W, CAO J F, et al. ShuffleFL: gradient-preserving federated learning using trusted execution environment[C]//Proceedings of the 18th ACM International Conference on Computing Frontiers, 2021.

[76] XU T X, ZHU K L, ANDRZEJAK A, et al. Distributed learning in trusted execution environment: a case study of federated learning in SGX[C]//2021 7th IEEE International Conference on Network Intelligence and Digital Content (IC-NIDC), 2021:450-454.

[77] MO F, HADDADI H, KATEVAS K, et al. PPFL: privacy-preserving federated learning with trusted execution environments[C]//Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services, 2021.

[78] CHEN Y, LUO F, LI T, et al. A training-integrity privacy-preserving federated learning scheme with trusted execution environment[J]. Inf. Sci.522, 2020: 69-79.

[79] JIA B, ZHANG X S, LIU J W, et al. Blockchain-Enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT[J]. IEEE Transactions on Industrial Informatics, 18,

2021: 4049-4058.

[80] KATO F, CAO Y, YOSHIKAWA M, et al. OLIVE: oblivious and differentially private federated learning on trusted execution environment[J]. ArXiv: 2202.07165, 2022.

[81] YAO J J, ANSARI N. Enhancing federated learning in fog-aided IoT by CPU frequency and wireless power control[J]. IEEE Internet of Things Journal, 8, 2021: 3438-3445.

[82] KONECNY J, MCMAHAN H B, YU F X, et al. Federated learning: strategies for improving communication efficiency[J]. ArXiv: 1610.05492,2016.

[83] LI X, HUANG K X, YANG W H, et al. On the convergence of FedAvg on Non-IID data[J]. ArXiv: 1907.02189, 2019.

[84] MOHRI M, SIVEK G, SURESH A, et al. Agnostic federated learning[J]. ArXiv: 1902.00146, 2019.

[85] ZHAO Y, et al. Federated learning with Non-IID Data[J]. ArXiv: 1806.00582, 2018.

[86] LI T, SAHU A K, TALWALKAR A, et al. Federated learning: challenges, methods, and future directions[J]. IEEE Signal Processing Magazine, 37, 2019: 50-60.

[87] 赵杨, 张海岩, 王硕. 联邦学习综述[J]. 电脑编程技巧与维护, 2022(01): 117-119.

ZHAO Y, ZHANG H Y, WANG S. Overview of federated learning[J]. Computer Programming Skills and Maintenance, 2022(01): 117-119. (in Chinese)

[88] 周传鑫, 孙奕, 汪德刚等. 联邦学习研究综述[J]. 网络与信息安全学报, 2021, 7(05): 77-92.

ZHOU C X, SUN Y, WANG D G, et al. Overview of federated learning research[J]. Journal of Network and Information Security, 2021, 7(05): 77-92. (in Chinese)