基于横向联邦学习的隐私保护研究

王 斌[1,2],尹晓雅[1],张 磊[1*]
(1. 佳木斯大学 信息电子技术学院 黑龙江省自主智能与信息处理重点实验室,
黑龙江 佳木斯 154007;
2. 佳木斯大学 佳木斯大学科技处,黑龙江 佳木斯 154007)

摘 要:近年来,随着人工智能的快速发展,机器学习成为处理数据的重要手段。传统的机器学习在处理数据时需要上传到中心服务器,无法保证用户数据隐私。但联邦学习的分布式特性保证了数据安全和隐私,同时也解决了数据孤岛问题,提高了不同应用环境下数据的可用性。然而,越来越多的研究表明,基于联邦学习的方法仍然遭受不同的隐私威胁,因此如何保护联邦学习场景下的用户数据隐私成为一个挑战。为应对联邦学习的隐私问题,对现有的隐私保护手段进行了调查分析。首先,介绍了联邦学习的定义、发展和分类;其次,介绍联邦学习的系统架构并分析了所遭受的隐私威胁手段;再次,根据联邦学习训练过程的生命周期对隐私保护技术进行分类和整理,同时比较了各技术的优缺点;最后,指出了目前联邦学习所面临的挑战,以及未来的发展趋势。

关键词:隐私保护技术;隐私安全;联邦学习;同态加密;差分隐私
中图分类号:TP391.1 **文献标识码**:A **文章编号**:1673-629X(2024)10-0001-07
doi:10.20165/j.cnki.ISSN1673-629X.2024.0194

Survey and Analysis of Privacy-preserving Based on Horizontal Federated Learning

WANG Bin[1,2], YIN Xiao-ya[1], ZHANG Lei[1*]
(1. Key Laboratory of Autonomous Intelligence and Information Processing of Heilongjiang Province,
School of Information & Electronic Technology, Jiamusi University, Jiamusi 154007, China;
2. Science and Technology Department of Jiamusi University, Jiamusi University, Jiamusi 154007, China)

Abstract: In recent years, with the rapid development of artificial intelligence, machine learning has become an important approach for data processing. Traditional machine learning methods require data to be uploaded to central servers, which raises concerns about data privacy. However, the distributed nature of federated learning ensures data security and privacy, while also addressing the issue of data silos and improving data availability in different application environments. Nevertheless, increasing research indicates that federated learning methods still face various privacy threats, making it a challenge to protect user data privacy in federated learning scenarios. To address the privacy issues in federated learning, we investigated and analyzed existing privacy protection mechanisms. Firstly, we introduced the definition, development, and classification of federated learning. Secondly, presented the system architecture of federated learning and analyzed the privacy threats it faces. Furthermore, classified and organized privacy protection techniques based on the lifecycle of the federated learning training process, while comparing the advantages and disadvantages of each technique. Finally, highlighted the current challenges faced by federated learning and discussed future development trends.

Key words: privacy preserving technology; privacy and security; federated learning; homomorphic encryption; differential privacy

0 引 言

随着人工智能的快速发展,机器学习作为处理海量数据的核心技术,其隐私性得到广泛的关注。传统的机器学习需要将用户数据存储到中央服务器进行训练,如果这些信息收集到中央服务器后遭到隐私攻击,人身和财产安全将受到威胁,这导致用户不愿意透漏

收稿日期:2023-12-13 **修回日期**:2024-04-17
基金项目:黑龙江省省属高等学校基本科研业务费优秀创新团队建设项目(2023-KYYWF-0639);佳木斯大学国家基金培育项目(JMSUGPZR2022-014);佳木斯大学博士启动基金项目(JMSUBZ2022-12)
作者简介:王 斌(1979-),男,教授,博士,研究方向为信息安全、隐私保护;通讯作者:张 磊(1982-),男,教授,博士,研究方向为信息安全、隐私保护。

个人信息,而人工智能的发展必须依靠大量的数据,这也直接限制了机器学习的研究与发展。

同时,在企业内部数据孤立地存储在服务器中,而企业之间不会共享数据,导致数据质量较差,阻碍机器学习训练有价值的模型,造成数据孤岛现象。于是,谷歌公司在2016年提出联邦学习[1](Federated Learning,FL)。它由多个持有私有数据的联合客户端组成,并以协作的方式为机器学习模型的训练做出贡献,允许数千个客户端在自己的设备上保留原始数据,但在执行联邦平均之前,拦截客户端对服务器共享的本地梯度,并根据梯度重构出本地数据,使得个人信息泄露,因此有许多研究进一步通过不同的技术提高联邦学习的隐私性。

目前联邦学习的隐私保护技术成为联邦学习领域的热点,许多学者发表了不少相关的研究综述。刘艺璇等人[2]根据隐私保护机制归纳隐私保护技术,从中心、本地、中心和本地结合三个层面对现有的联邦学习隐私保护进行总结。汤凌韬等人[3]根据敌手攻击目标将隐私攻击方法进行分类,同时总结分析目前主流的隐私保护技术。Rodríguez等人[4]总结了一个对抗攻击的分类和防御方法的分类,分析联邦学习的脆弱性和如何克服这种脆弱性的一般情况。

现在已有的综述分别从技术、攻击手段以及安全威胁等角度分析联邦学习隐私保护方案,并通过研究人员的深入研究取得了一定的进展。与已有的研究综述侧重点不同,该文从横向联邦学习训练过程生命周期的角度进行分析,因而研究分析该角度的每个阶段所遭受的隐私威胁,并归纳分类每个阶段的隐私保护技术,进而分析采用不同保护技术的共性以及优缺点,并在此基础上对联邦学习隐私保护的未来发展提出建议。

1 相关知识

1.1 系统架构

联邦学习系统架构主要由以下五部分组成:

(1)模型初始化:聚合器选择合适的模型和超参数,生成初始的全局模型;

(2)模型下载:客户端从聚合服务器下载目标模型与超参数;

(3)模型本地训练:参与方使用本地数据对初始全局模型进行训练,生成局部模型;

(4)模型聚合:收集参与方发送的模型参数,并使用聚合算法将局部模型参数聚合;

(5)模型更新:聚合后得到新的全局模型。

该过程反复执行多次,直至服务器得到的模型达到收敛状态。

1.2 隐私威胁

攻击者在不同阶段存在不同的安全威胁,同时也需要不同的背景知识和能力。以下将介绍在本地训练阶段、模型上传阶段和模型聚合阶段的隐私威胁:

(1)本地训练阶段的隐私威胁。

被动成员推理攻击[5]:攻击者作为内部成员通过多样的攻击手段获取某些信息,然后利用这些信息推理获得想要的信息;

中毒攻击[6]:攻击者修改原始训练数据集的单个特征或小区域,然后将其作为后门嵌入模型中;

属性推理攻击[7]:攻击者试图提取未明确编码为特征或与学习任务无关的数据集属性,可以获得训练数据的相关信息。

(2)模型上传阶段的隐私威胁。

重构攻击[8]:外部攻击者利用联邦学习建模过程中传递的模型信息重构出原始数据;

共谋攻击:客户端之间或者客户端与服务器之间相互勾结,得到想要的数据。

(3)模型聚合阶段的隐私威胁。

主动成员推理攻击[9]:不诚实的服务器恶意地调整模型参数,以确定目标数据样本是否在客户端的本地训练数据集中,从而得到数据信息;

模型反演攻击[10]:服务器使用辅助数据构造恶意模型参数,然后通过发送恶意平均梯度来篡改用户的模型参数。

2 本地训练阶段的隐私保护

2.1 基于数据扰动技术

本地训练阶段的噪声添加方式如图1所示。

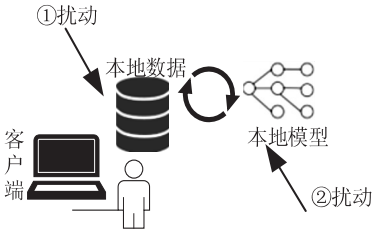

图1 本地训练阶段数据扰动技术

为了避免本地模型参数的隐私遭受外部攻击,例如第三方窃取信息,应作斌等人[11]在本地模型训练阶段引入差分隐私机制。添加一样的噪声可能对客户端造成隐私不足或者造成隐私过足,因此Wu等人[12]根据数据特征和全局灵敏度对模型参数添加噪声;而Hu等人[13]为每个用户实现个性化的差分隐私,保证参与者的个人敏感信息。

此外,本地训练过程中的内部攻击也是数据泄露的重要原因,Zhang等人[14]设计一个具有差分隐私的博弈论联邦学习方案;而为了应对攻击者扮作参与者

执行重构攻击,Yin 等人[15]对模型参数添加噪声并上传到边缘聚合器进行聚合。

2.2　基于硬件的技术

可信执行环境的数据计算仅在该安全环境内进行,通过依赖可信硬件来保障其安全。恶意参与者生成不正确的梯度导致模型被注入恶意属性,因此 Chen 等人[16]提出一个基于可信执行环境的联邦学习隐私保护方案,要求每个参与者必须正确执行方案的隐私保护学习算法,不可篡改算法中的任何参数。此外,存在异常客户端阻碍模型训练泄露数据隐私,Dong 等人[17]由可信执行环境赋能的边缘服务器可靠地帮助性能较差的联邦学习客户端。Mondal 等人[18]为单独执行代码和处理数据提供了一个可信平台,避免本地数据训练过程的隐私泄露,由于该文提出的方法是在理想的可信执行环境中训练,在实际工作中可能由于空间受限等原因导致性能受损等。

由于密钥分发中心等第三方是诚实但好奇的,因此 Huang 等人[19]通过将密钥分发中心与可信执行环境结合,可以为本地模型和本地数据提供更多的安全保障,但由于可信执行环境的空间受限,基于硬件的联邦学习隐私保护方法缺少一定的灵活性。为了保证在空间受限环境下隐私保护效果不会受损,Mo 等人[20]在客户端上使用可信执行环境对数据进行本地训练,具体来说,该方法在客户端的可信执行环境中采用贪婪的分层联邦学习训练,防止了白盒成员的推理攻击,同时降低了通信和系统开销。

表 1　本地训练阶段隐私保护方法比较

方法	隐私威胁	技术核心	优点	缺点
个性化差分隐私[12-13]	第三方窃取信息	根据全局灵敏度和数据特征添加噪声	隐私性好,部署方便	模型训练的收敛效率和对大规模数据场景的可用性存在局限性
本地化差分隐私[14-15]	恶意客户端	自适应的向本地模型训练过程中添加噪声	保证单个客户端的隐私性,通信开销小	模型收敛效率降低
可信执行环境[16-17]	中毒攻击	在每个参与者的 TEE 中执行梯度的计算	保证训练过程完整性、攻击成功率下降、客户端效率提高	缺少验证机制,空间有限、缺少灵活性

3　模型上传阶段的隐私保护

3.1　基于密码学技术

模型上传阶段密码学技术有三种技术,如图 2 所示。为了防止在传输过程中遭受外部敌人的攻击,Zhang 等人[21]采用同态加密技术对需要上传的模型参数加密。Ma 等人[22]采用多密钥同态加密方法,抵抗了 $N-1$ 个用户和服务器之间的勾结,但服务器和客户端通信开销巨大,所以余晟兴等人[23]通过对梯度进行筛选、量化裁剪并对梯度进行同态加密,保证数据安全和性能高效。

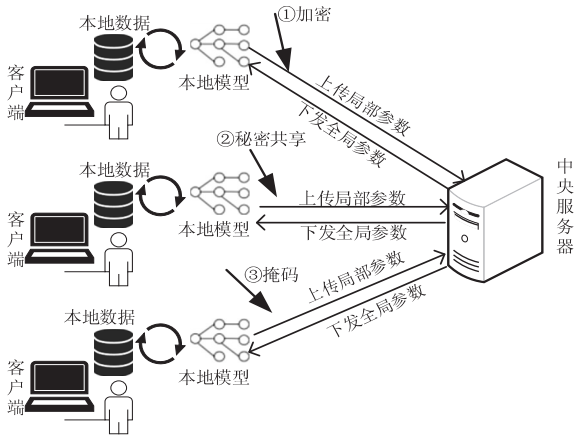

图 2　模型上传阶段密码学技术

雾计算[24]是云计算的扩展,充当云和用户设备之间的桥梁。由于用户设备计算能力不足,Ku 等人[25]提出一种基于雾节点的同态重加密的联邦学习隐私保护方法。由于同态加密技术通信开销较大,Wang 等人[26]采用雾节点从设备中收集数据并将随机掩码添加到梯度中避免梯度的泄露。

由于雾节点可能会泄露敏感信息,所以 Li 等人[27]通过将参数进行秘密共享给多个雾节点来保证参数安全。

3.2　基于数据扰动技术

如图 3 所示,在模型训练完成后的模型参数中添加噪声,避免上传过程中遭受敌人的攻击。

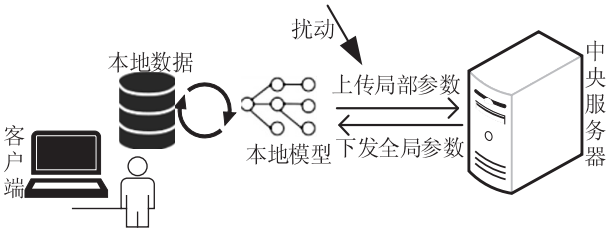

图 3 模型上传阶段数据扰动技术

对于工业数据在模型上传时容易受到外部攻击，Islam 等人[28]将在本地训练过程中添加拉普拉斯噪声；而 Jiang 等人[29]提出对梯度进行自适应裁剪保证了梯度质量再添加噪声。而 Truex 等人[30]在多个个体参与者数据集上根据隐私级别对参数执行基于本地差分隐私的扰动；而 Li 等人[31]采用的自适应差分隐私向更新后的模型参数添加高斯噪声，防止上传过程恶意攻击者通过本地更新从梯度数据中提取相关信息。

由于上述方法在添加噪声后造成模型性能受损，Liu 等人[32]提出一种混合隐私保护机制，使用分层相关性传播算法计算每个属性类对输出的贡献。而 Yuan 等人[33]提出一种具有时变噪声幅度的 DP 微扰机制，该机制对扰动噪声进行了精心设计的时变根均方振幅。此外，边缘计算比用户设备的计算能力强，Zhou 等人[34]提出基于边缘计算的联邦学习方案，可以根据训练的次数灵活地分配给用户噪声，保证一定的通信开销与数据隐私。

表 2 模型上传阶段隐私保护方法比较

方法	隐私威胁	技术核心	优点	缺点
同态加密[21-22]	敌手窃取上传过程的梯度	采用多密钥同态加密对上传梯度数据进行加密	稳健性和隐私性强	通信开销大，依赖多个云服务器
秘密共享[26-27]	共谋攻击	通过随机掩码对梯度数据进行加密，并秘密共享给服务器	高可扩展性，支持雾节点掉线状态，防止多个雾节点相互勾结	计算复杂度高，实用性较差
本地化差分隐私[28-30]	外部攻击	引入本地化差分隐私机制对模型参数进行扰动	隐私性能高，通信开销小，对模型精度影响小	模型收敛性差

4 模型聚合阶段的隐私保护

4.1 基于密码学技术

模型聚合阶段所需要的密码学技术如图 4 所示。

在模型聚合过程中同态加密是保证数据安全的一种技术，但聚合过程中仍然存在一定的隐私泄露，因此 Truex 等人[35]采取同态加密技术在同态操作下对参数进行聚合，并且必须由多个参与方加入才能共同解密聚合值。然而仍然存在恶意服务器伪造聚合梯度造成隐私泄露，因此需要验证聚合值的正确性。Fu 等人[36]在加密的聚合参数返回给用户后，通过拉格朗日插值验证聚合值的正确性，再决定是否更新参数。

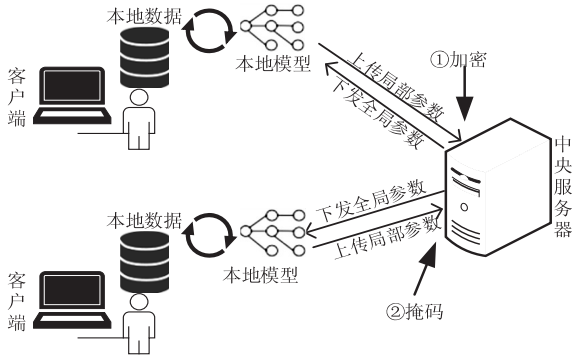

图 4 模型聚合阶段密码学技术

Li 等人[37]采用门限 Paillier 密码系统，对模型参数进行加密，并将加密后的梯度上传到服务器，然后聚合加密梯度并将其发送给用户。为了保护客户端的输入不被其他对手窃听以及为了处理服务器和客户端之间的勾结，Liu 等人[38]提出一个双掩码策略对客户端的模型参数添加两个掩码。为了保证服务器只知道梯度的综合结果而无法得知每个用户的梯度信息，Lu 等人[39]对本地数据集添加噪声并根据公共数据集生成

成对掩码。但是上述方法忽略了恶意参与方的存在会严重影响聚合过程,蔡红云等人[40]利用聚类划分良性客户端和异常客户端,并将两方客户端盲化后聚合参数。

4.2　基于数据扰动技术

模型聚合阶段的数据扰动技术如图 5 所示。

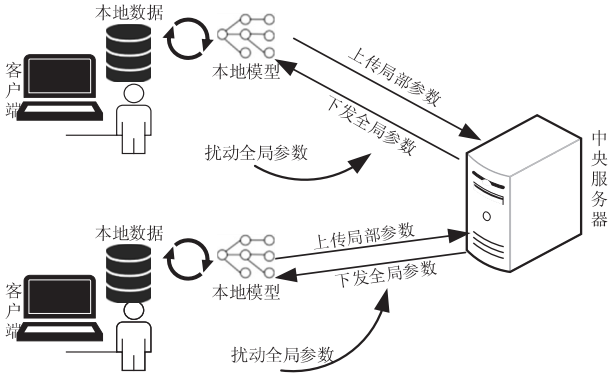

图 5　模型聚合阶段数据扰动技术

在模型聚合过程中,为保护聚合结果的隐私安全,Zhou 等人[41]根据全局灵敏度对每个客户端的模型参数添加不同的高斯噪声。为了确保聚合过程中服务器在任何辅助信息和攻击都不能从用户样本中学到太多信息,Hu 等人[42]在差分隐私框架下设计了差分隐私算法。为提高通信效率,Hu 等人[43]提出一种稀疏编码差分隐私机制,通过对梯度稀疏化并添加噪声,使服务器无法从梯度中得到私人信息。该方法导致模型准确率降低,因此 Shen 等人[44]通过采用个性化差分隐私扰动算法对中间参数进行处理,提高模型精确度。为了防止重构攻击和成员推理攻击,Sun 等人[45]提出一种局部差分隐私机制,对更新后的模型参数添加噪声。

表 3　模型聚合阶段隐私保护方法比较

方法	隐私威胁	技术核心	优点	缺点
可验证的同态加密[36]	恶意聚合服务器返回伪造聚合梯度	对梯度进行加密在同态下聚合,验证聚合值的正确性	聚合过程无法得知用户信息,隐私性强,精度高、效率高	验证开销大,计算复杂度高
成对掩码[38-39]	服务器与客户端共谋	采用双掩码策略对梯度添加两次不同的掩码	精度高,通信开销低,支持客户端离线,隐私性强	计算复杂度高
对中间参数个性化添加噪声[41]	隐私攻击侵犯中央服务器	采用差分隐私对模型参数添加噪声	高效、隐私性高,用户传输数据到服务器的延迟降低	数据质量降低,未考虑针对各种隐私攻击的性能

5　发展趋势

不同于传统的机器学习,联邦学习由于本身分布式的特性,使数据获得部分隐私保护,但由于联邦学习面临许多精心设计的隐私攻击而更迫切地需要隐私保护。现有的联邦学习隐私保护技术在异质数据、抵抗隐私攻击和隐私保护成本中仍然存在许多不足之处。对已有研究进行比较分析,提出了对现有联邦学习隐私保护研究的看法和对未来的展望。

(1)横向联邦学习攻击方法研究。

现已有针对横向联邦学习的推理攻击,攻击者通过梯度信息推理用户信息,但攻击效果随着模型泛化程度的提高而下降;为了抵抗模型投毒攻击需要牺牲鲁棒性,如何解决在抵抗模型投毒攻击时提高鲁棒性是联邦学习未来的一个挑战;对于目前的攻击方法大多有固定的应用场景,且针对不同目标模型和威胁模型提出的,因此攻击方法的有效性取决于实际应用场景,如何解决不同场景下攻击手段的有效性是未来研究的挑战。

(2)去中心化的联邦学习隐私保护研究。

现有的研究中大部分是针对有中央服务器对数据进行联邦学习,但存在中央服务器容易出现单点故障或第三方服务器不诚实等问题,尽管已经存在去中心化的联邦学习解决了在第三方,但由于去中心化的联邦学习不能应用于存在大规模参与者的情况,因此如何解决去中心化联邦学习的可扩展性,同时防止扩展大规模参与者导致效率降低是一个可行的研究方向。

(3)在非独立同分布数据上的联邦学习研究。

现有研究大多是对横向联邦学习数据进行训练,可以对特征相同的数据进行模型优化,但在现实的复

杂应用场景中,不同用户间的数据类型可能不相同,很难满足数据独立同分布这个前提。同时,非独立同分布数据很难与差分隐私等技术相结合保证数据的隐私,因此如何在数据非独立同分布情况下对模型进行优化,并保证数据隐私性是联邦学习未来的一个挑战。

6 结束语

联邦学习的出现打破了数据孤岛现象,同时解决了部分数据隐私问题,充分挖掘了终端设备中存储数据的价值。但是随着参与者的类型增多,攻击者的攻击手段越来越精细,联邦学习也面临着越来越多的隐私泄露问题,严重威胁正常的训练过程,危害用户的数据隐私,成为联邦学习发展的重要挑战。该文对联邦学习的隐私威胁和保护技术做了充分的调查和分析,介绍了横向联邦学习的系统架构;按照联邦学习在训练过程中生命周期所遭受的隐私威胁对隐私保护技术进行分类整理,总结各个保护技术的不足之处。最后,根据已有的研究分析未来的研究发展。虽然目前对联邦学习的隐私保护研究已有不少,但由于抵抗攻击能力有限、应用场景单一、通信开销巨大,仍然存在许多问题未被解决。未来联邦学习隐私保护仍然是一个更长久的挑战。

参考文献:

[1] MCMAHAN B,MOORE E,RAMAGE D,et al. Communication-efficient learning of deep networks from decentralized data[C]//Proceedings of the 20th international conference on artificial intelligence and statistics. Florida:PMLR,2017:1273-1282.

[2] 刘艺璇,陈 红,刘宇涵,等. 联邦学习中的隐私保护技术[J]. 软件学报,2021,33(3):1057-1092.

[3] 汤凌韬,陈左宁,张鲁飞,等. 联邦学习中的隐私问题研究进展[J]. 软件学报,2021,34(1):197-229.

[4] RODRÍGUEZ-BARROSO N,JIMÉNEZ-LÓPEZ D,LUZÓN M V,et al. Survey on federated learning threats:concepts,taxonomy on attacks and defences,experimental study and challenges[J]. Information Fusion,2023,90(1):148-173.

[5] HITAJ B,ATENIESE G,PEREZ-CRUZ F. Deep models under the GAN:information leakage from collaborative deep learning[C]//Proceedings of the 2017 ACM SIGSAC conference on computer and communications security. Texas:ACM,2017:603-618.

[6] SHOKRI R,STRONATI M,SONG C,et al. Membership inference attacks against machine learning models[C]//Proceedings of the 2017 IEEE symposium on security and privacy. California:IEEE,2017:3-18.

[7] CAO X,GONG N Z. Mpaf:model poisoning attacks to federated learning based on fake clients[C]//Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. Louisiana:IEEE,2022:3396-3404.

[8] MALEKZADEH M,BOROVYKH A,GÜNDÜZ D. Honest-but-curious nets:sensitive attributes of private inputs can be secretly coded into the classifiers' outputs[C]//Proceedings of the 2021 ACM SIGSAC conference on computer and communications security. New York:ACM,2021:825-844.

[9] NGUYEN T,LAI P,TRAN K,et al. Active membership inference attack under local differential privacy in federated learning[J]. arXiv:2302.12685,2023.

[10] ZHANG S,HUANG J,ZHANG Z,et al. Compromise privacy in large-batch federated learning via model poisoning[J]. Information Sciences,2023,647:119421.

[11] 应作斌,方一晨,张怡文. 动态聚合权重的隐私保护联邦学习框架[J]. 网络与信息安全学报,2022,8(5):56-65.

[12] WU X,ZHANG Y,SHI M,et al. An adaptive federated learning scheme with differential privacy preserving[J]. Future Generation Computer Systems,2022,127(1):362-372.

[13] HU R,GUO Y,LI H,et al. Personalized federated learning with differential privacy[J]. IEEE Internet of Things Journal,2020,7(10):9530-9539.

[14] ZHANG L,ZHU T,XIONG P,et al. A robust game-theoretical federated learning framework with joint differential privacy[J]. IEEE Transactions on Knowledge and Data Engineering,2023,35(4):3333-3346.

[15] YIN K,WU B,ZHU R,et al. DLDP-FL:dynamic local differential privacy federated learning method based on mesh network edge devices[J]. Journal of Computational Science,2022,63(1):1-20.

[16] CHEN Y,LUO F,LI T,et al. A training-integrity privacy-preserving federated learning scheme with trusted execution environment[J]. Information Sciences,2020,522(1):69-79.

[17] DONG S,ZENG D,GU L,et al. Offloading federated learning task to edge computing with trust execution environment[C]//2020 IEEE 17th international conference on mobile ad hoc and sensor systems. Delhi:IEEE,2020:491-496.

[18] MONDAL A,MORE Y,ROOPARAGHUNATH R H,et al. Poster:FLATEE:federated learning across trusted execution environments[C]//Proceedings of the 2021 IEEE European symposium on security and privacy. Vienna:IEEE,2021:707-709.

[19] HUANG A,LIU Y,CHEN T,et al. StarFL:hybrid federated learning architecture for smart urban computing[J]. ACM Transactions on Intelligent Systems and Technology,2021,12(4):1-23.

[20] 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.

Wisconsin:ACM,2021:94-108.

[21] ZHANG Z,HE N,LI Q,et al. DetectPMFL:privacy-preserving momentum federated learning considering unreliable industrial agents[J]. IEEE Transactions on Industrial Informatics,2022,18(11):7696-7706.

[22] MA J,NAAS S A,SIGG S,et al. Privacy-preserving federated learning based on multi - key homomorphic encryption [J]. International Journal of Intelligent Systems,2022,37(9):5880-5901.

[23] 余晟兴,陈　钟. 基于同态加密的高效安全联邦学习聚合框架[J]. 通信学报,2023,44(1):14-28.

[24] YI S,LI C,LI Q. A survey of fog computing:concepts,applications and issues[C]//Proceedings of the 2015 workshop on mobile big data. New York:ACM,2015:37-42.

[25] KU H,SUSILO W,ZHANG Y,et al. Privacy-preserving federated learning in medical diagnosis with homomorphic re-encryption[J]. Computer Standards & Interfaces,2022,80:103583.

[26] WANG R,LAI J,ZHANG Z,et al. Privacy-preserving federated learning for internet of medical things under edge computing[J]. IEEE J Biomed Health Inform,2023,27(2):854-865.

[27] LI Y,LI H,XU G,et al. Practical privacy-preserving federated learning in vehicular fog computing[J]. IEEE Transactions on Vehicular Technology,2022,71(5):4692-4705.

[28] ISLAM T U,GHASEMI R,MOHAMMED N. Privacy-preserving federated learning model for healthcare data[C]// Proceedings of the 2022 IEEE 12th annual computing and communication workshop and conference. Nevada:IEEE,2022:281-287.

[29] JIANG B,LI J,WANG H,et al. Privacy-preserving federated learning for industrial edge computing via hybrid differential privacy and adaptive compression[J]. IEEE Transactions on Industrial Informatics,2023,19(2):1136-1144.

[30] TRUEX S,LIU L,CHOW K H,et al. LDP-fed:federated learning with local differential privacy[C]//Proceedings of the third ACM international workshop on edge systems, analytics and networking. Heraklion:ACM,2020:61-66.

[31] LI Z,TIAN Y,ZHANG W,et al. RR-LADP:a privacy-enhanced federated learning scheme for internet of everything [J]. IEEE Consumer Electronics Magazine,2021,10(5):93-101.

[32] LIU X,LI H,XU G,et al. Adaptive privacy-preserving federated learning[J]. Peer-to-Peer Networking and Applications,2020,13(6):2356-2366.

[33] YUAN X,NI W,DING M,et al. Amplitude-varying perturbation for balancing privacy and utility in federated learning [J]. IEEE Transactions on Information Forensics and Security,2023,18(1):1884-1897.

[34] ZHOU H,YANG G,DAI H,et al. PFLF:privacy-preserving federated learning framework for edge computing[J]. IEEE Transactions on Information Forensics and Security,2022,17(1):1905-1918.

[35] TRUEX S,BARACALDO N,ANWAR A,et al. A hybrid approach to privacy-preserving federated learning[C]//Proceedings of the 12th ACM workshop on artificial intelligence and security. New York:ACM,2019:1-11.

[36] FU A,ZHANG X,XIONG N,et al. VFL:a verifiable federated learning with privacy-preserving for big data in industrial IoT[J]. IEEE Transactions on Industrial Informatics,2022,18(5):3316-3326.

[37] LI Y,LI H,XU G,et al. Efficient privacy-preserving federated learning with unreliable users [J]. IEEE Internet of Things Journal,2022,9(13):11590-11603.

[38] LIU Y,QIAN X,LI H,et al. Fast secure aggregation for privacy-preserving federated learning[C]//GLOBECOM 2022 - 2022 IEEE Global communications conference. Rio de Janeiro:IEEE,2022:3017-3022.

[39] LU S,LI R,LIU W,et al. Top-k sparsification with secure aggregation for privacy-preserving federated learning[J]. Computers & Security,2023,124(1):34-48.

[40] 蔡红云,张　宇,王诗云,等. 基于相似度聚类的可信联邦安全聚合算法[J]. 电子与信息学报,2023,45(3):894-904.

[41] ZHOU H,YANG G,HUANG Y,et al. Privacy-preserving and verifiable federated learning framework for edge computing[J]. IEEE Transactions on Information Forensics and Security,2023,18(1):565-580.

[42] HU R,GUO Y,LI H,et al. Privacy-preserving personalized federated learning [C]//Proceedings of the ICC 2020 - 2020 IEEE international conference on communications. Rio de Janeiro:IEEE,2020:1-6.

[43] HU R,GONG Y,GUO Y. Federated learning with sparsification-amplified privacy and adaptive optimization[J]. arXiv:2008.01558,2021.

[44] SHEN X,JIANG H,CHEN Y,et al. PLDP-FL:federated learning with personalized local differential privacy[J]. Entropy (Basel),2023,25(3):52-63.

[45] SUN L,QIAN J,CHEN X,et al. Ldp-fl:practical private aggregation in federated learning with local differential privacy [J]. arXiv:2007.15789,2020.