·热点与综述·　　文章编号：1000-3428(2023)01-0022-09　　文献标志码：A　　中图分类号：TP391

基于超级账本的集群联邦优化模型

李尤慧子[1]，俞海涛[1]，殷昱煜[1]，高洪皓[2,3]

（1.杭州电子科技大学 计算机学院，杭州 310018；2.上海大学 计算机工程与科学学院，上海 200444；
3.韩国嘉泉大学 计算机工程系，城南 461701）

摘　要：联邦学习作为分布式机器学习框架，在数据不离开本地的情况下，通过共享模型参数达到协作训练的目标，一定程度上解决了隐私保护问题，但其存在中心参数服务器无法应对单点故障、潜在恶意客户端梯度攻击、客户端数据偏态分布导致训练性能低下等问题。将去中心化的区块链技术与联邦学习相结合，提出基于超级账本的集群联邦优化模型。以超级账本作为分布式训练的架构基础，客户端初始化后在本地训练向超级账本传输模型参数及分布信息，通过聚类优化联邦学习模型在客户端数据非独立同分布下的训练表现。在此基础上，随机选举客户端成为领导者，由领导者代替中央服务器的功能，领导者根据分布相似度和余弦相似度聚类并下载模型参数聚合，最后客户端获取聚合模型继续迭代训练。以EMNIST数据集为例，数据非独立同分布情况下该模型平均准确率为79.26%，较FedAvg提高17.26%，在保证准确率的前提下，较集群联邦学习训练至收敛的通信轮次减少36.3%。

关键词：区块链；超级账本；联邦学习；隐私保护；智能合约

开放科学（资源服务）标志码（OSID）：

中文引用格式：李尤慧子，俞海涛，殷昱煜，等. 基于超级账本的集群联邦优化模型[J]. 计算机工程，2023，49(1)：22-30.

英文引用格式：LI Y H Z，YU H T，YIN Y Y，et al. Cluster federated optimization model based on Hyperledger Fabric[J]. Computer Engineering，2023，49(1)：22-30.

Cluster Federated Optimization Model Based on Hyperledger Fabric

LI Youhuizi[1]，YU Haitao[1]，YIN Yuyu[1]，GAO Honghao[2,3]

（1.School of Computer Science，Hangzhou Dianzi University，Hangzhou 310018，China；
2.School of Computer Engineering and Science，Shanghai University，Shanghai 200444，China；
3.Department of Computer Engineering，Gachon University，Seongnam 461701，Republic of Korea）

【Abstract】As a distributed machine learning framework，Federated Learning（FL）achieves collaborative training by sharing model parameters without leaving the data locally and ensures privacy protection to a certain extent. However，several challenges are encountered in FL，such as potential malicious client gradient attacks，inability of the central parameter server to cope with a single point of failure，and poor training performance due to skewed client data distribution. In response to the above-mentioned problems，the decentralized blockchain technology is combined with FL and a cluster federated optimization model is proposed based on Hyperledger Fabric. The model uses Hyperledger Fabric as the architectural basis for distributed training. After the client is initialized，the local training transmits model parameters and distribution information to the Hyperledger Fabric. The training performance of FL under the Non-IID distribution of client data is optimized through clustering；then，a client is randomly elected to become the leader；the leader replaces the central server. The leader clusters and downloads the model parameter aggregation according to the distribution similarity and cosine similarity. The client obtains the aggregation model and iterative training continues. On the EMNIST dataset，the average accuracy of the proposed model is 79.26% under Non-IID distribution of data，which is 17.26% higher than that of FedAvg. For a high rate，it requires 36.3% less time than the communication round of Cluster Federated Learning（CFL）training to convergence.

【Key words】blockchain；Hyperledger Fabric；Federated Learning（FL）；privacy protection；smart contract

DOI：10. 19678/j. issn. 1000-3428. 0064301

基金项目：浙江省“尖兵”“领雁”研发攻关计划“基于异质多模态数据融合的卒中后认知功能障碍智能诊疗技术研究与应用示范”（2022C03043）；浙江省自然科学基金“车联网中全路径轨迹隐私保护关键技术研究”（LY22F020018）。

作者简介：李尤慧子（1989—），女，副教授、博士，主研方向为边缘计算、隐私保护；俞海涛，硕士研究生；殷昱煜、高洪皓，教授、博士。

收稿日期：2022-03-25　　**修回日期：**2022-10-14　　**E-mail：**yinyuyu@hdu.edu.cn

0　概述

随着人工智能的发展，机器学习模型[1-3]变得越发庞大复杂，需要的训练数据量也持续增加。例如，词向量预训练模型GPT-2训练语料规模达40 GB，参数量更是高达15亿。然而，随着人们对数据隐私保护的愈加关注，海量数据难以直接共享。在法律层面，欧盟颁布了目前全球最严格也最健全的网络数据隐私保护框架——《通用数据保护条例》，规范了企业收集、管理、删除客户和个人数据。全国人大常委会于2021年8月20日表决通过了《中华人民共和国个人信息保护法》并于2021年11月施行。在医疗[4]、智慧城市[5]、移动边缘计算[6]等很多领域，由于数据属于不同的组织和部门，隐私敏感度高，极易导致机器学习算法因有效训练数据不足而准确率低下的问题。

为打破数据孤岛困局，同时满足数据隐私保护相关重要标准，联邦学习（Federated Learning，FL）[7]应运而生。作为一种特殊的分布式机器学习框架，联邦学习训练不传输源数据而仅需传输模型参数，因此具有一定的隐私保护能力，是目前最具吸引力的分布式机器学习框架。然而，多项研究[8-10]证明，联邦学习仍存在隐私漏洞，攻击者通过窃取参数服务器数据，容易从梯度、模型参数中推断源数据[11-12]。梯度攻击的过程是随机生成虚拟数据并计算虚拟梯度，然后将缩小虚拟梯度与真实梯度差距作为优化目标，通过梯度下降反复迭代还原用户隐私数据。其次，联邦学习更适用于数据独立同分布（IID）的场景，模型训练的准确率和收敛速度表现良好，但是无法有效处理非独立同分布（Non-IID）的数据[13-14]。LI等[15]从理论上对FedAvg[16]的收敛性进行分析，证明了异构数据会降低收敛速度。同时，ZHAO等[17]指出在严重偏态分布的CIFAR-10上进行训练，模型准确率会降低55%。此外，中心化的联邦参数服务器难以应对单点故障，一旦出现网络故障或宕机问题，短时间内难以快速解决，导致模型训练中断。区块链技术因其去中心化特性可以解决单点故障问题，也可以溯源监测恶意攻击者的破坏行为[18]。

本文构建一种基于超级账本（Hyperledger Fabric）的集群联邦优化模型，在保障跨部门跨设备协作训练不泄露数据隐私的同时，优化模型在非独立同分布下的训练效果。本文对协作训练成员进行身份控制，防止其获取多轮参数进行推理攻击。针对中心参数服务器的单点故障问题，设计基于超级账本的参数传输模块，选举动态领导者避免单点失效。针对数据异构导致性能下降的问题，提出客户端重排算法，在训练前根据客户端数据分布计算分布相似度进行聚类，在联邦训练过程中根据模型参数计算余弦相似度进行聚类。

1　相关研究

1.1　超级账本

2008年，中本聪提出了比特币的概念[19]，而区块链技术正是起源于比特币。区块链作为一个去中心化、不可变、共享的分布式账本和数据库，网络中所有节点共同维护着分布式系统的一致性，规避了中心化系统数据可能泄露的弊端，加强了隐私保护和数据安全。

然而，比特币使用的脚本语言只能实现简单的业务操作。超级账本相对比特币实现了更多创新的设计，例如身份权限管理、细粒度隐私保护、可插拔模块等。超级账本是由IBM牵头发起的一个联盟链项目，于2015年底移交给Linux基金会。类似于比特币网络，其本质上是一个分布式账本，并且账本交互逻辑可以由使用者根据自身业务需求定制。但与比特币、以太坊等公共非许可区块链不同，超级账本属于联盟链，存在准入限制，较公链安全度更高。同时，超级账本具有去中心化、细粒度隐私保护、模块可插拔等创新设计理念。超级账本与联邦学习相结合，既能保证数据的隐私，又能为分布式学习提供可靠的架构基础。

如图1所示，超级账本是一个认证性的网络[20]，区块链参与者需要向网络中的其他参与者证实身份才能在网络中交易。CA是网络的证书授权中心，节点通过颁发的数字身份参与区块链网络。成员服务提供者（MSP）通过生成用于证实身份的公私钥键值对来发放认证信息。超级账本网络主要由Peer节点组成，Peer节点是网络的基本元素，它们存储了账本和智能合约。Peer节点主要分为记账节点和背书节点：记账节点负责保存整个区块链的账本信息，包括世界状态、历史状态等；背书节点对交易进行检查，如果交易合法，则为之背书，并且计算交易执行结果，之后将结果发送给排序服务节点。

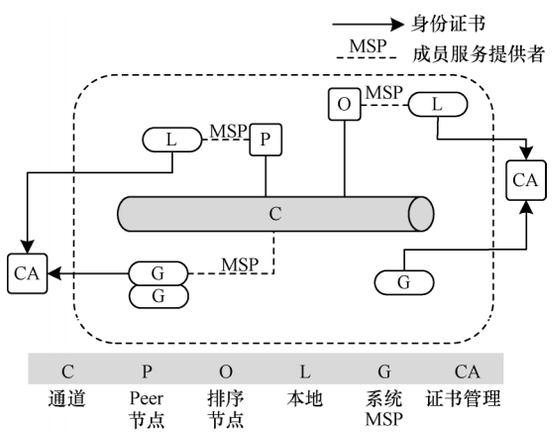

图1　超级账本认证网络

Fig.1　Hyperledger Fabric authentication network

在超级账本网络中，MSP分为本地MSP和通道MSP两种：本地MSP是为客户端和节点（Peer节点

和排序节点)定义的;通道MSP(系统通道的MSP)在通道层面上定义了管理权和参与权。

1.2 集群联邦学习

在本节中,介绍联邦学习和改进的集群联邦学习(Clustered Federated Learning,CFL)技术。联邦学习技术最早由谷歌于2017年4月提出,目的是解决用户终端设备上的输入法预测问题。以手机上人们每天使用的输入法为例,每个人有不同的打字拼音习惯,手机根据输入法中的数据进行训练与用户的打字习惯进行匹配,那么用户就会觉得输入法越来越智能。集中式学习的做法是将用户每天产生的行为数据上传至云端服务器,服务器进行数据处理和模型训练,然后更新模型参数,最终在实际应用时,本地需要从云端获取最新模型。由于云服务器获取了全部用户的源数据,这种训练方式存在严重的隐私安全问题,尤其是在隐私保护监管越来越规范的情况下,难以得到推广使用。

如图2所示,在联邦学习框架[21]中,客户端训练集数据不出域,模型训练都是在本地设备进行的,仅上传模型参数。具体训练过程如下:中心服务器初始化全局模型后发放至本地,本地模型训练完毕后将模型参数上传至参数服务器,服务器接收到本地上传的参数后进行统一的聚合(通过加权平均得到新的模型参数),然后将聚合结果重新发放到本地,本地更新得到一个全新的模型,如此循环迭代。

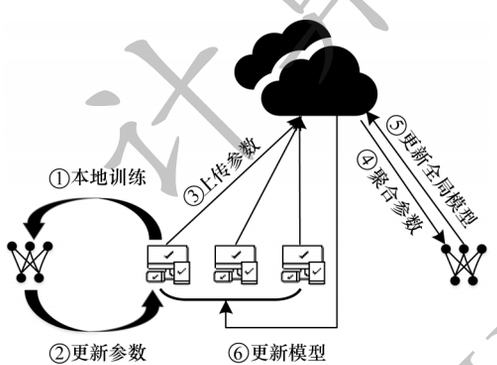

图2 联邦学习过程

Fig.2 Federated learning process

目前联邦学习的主要挑战之一是Non-IID。数据Non-IID分布十分多样,例如,不同客户端的训练数据量相差悬殊。从数据偏移的角度分析,Non-IID包括:

1)协变量偏移(Covariate Shift):$P_i(x)$分布不相同而$P(x|y)$分布相同,例如IFCA[22]。

2)先验概率偏移(Prior Probability Shift):$P_i(y)$分布不相同而$P(x|y)$分布相同,例如FedRS[23]。

3)概念偏移(Concept Shift):$P(x|y)$分布不相同而$P_i(y)$分布相同,反之亦然。

传统的联邦学习可以在Non-IID数据集上训练并获取全局模型,但性能较差。因此,GHOSH等[22]提出了IFCA模型,随机生成多个集群中心并将客户端划分为可最小化其损失值的集群。SATTLER等[24]提出了集群联邦学习框架,将优化目标划分为多个子目标分别做个性化优化。该框架包含一种基于梯度余弦距离聚类的递归优化算法,将集群内客户端递归地划分成两组。这种递归聚类是一种后处理方式,只有在联邦训练时才可以计算梯度进行聚类。为了提高集群联邦学习的效率,DUAN等[25]又提出了基于余弦欧氏距离的集群联邦学习方法。然而,IFCA虽然提升了效率,但同时训练K个模型会消耗更多的计算资源。本文根据客户端分布信息,以JS散度为度量进行预处理聚类,加快收敛速度。

2 系统架构

本文将成员准入、去中心化、数据可溯源的超级账本作为分布式训练的参数传输链,提出集群联邦客户端层级的重排算法,利用智能合约随机选举客户端聚合模型参数。为了更好地应对大模型参数传输问题,选用星际文件系统(IPFS)存储模型参数,Hyperledger Fabric仅记录存储在IPFS中文件对应的Hash,从而减小超级账本网络的通信负载。IPFS是基于文件内容的Hash,不同文件对应的Hash值不相同,Hash值与文件内容构成键值对。客户端上传参数至IPFS后返回该文件的存储Hash地址,其他客户端可通过Hash地址下载IPFS中的参数。由于账本记录Hash地址所需的空间远小于模型参数,因此IPFS减小了超级账本网络的通信压力。此外,传统联邦学习中参数服务器同客户端通信来完成聚合,而CFL训练过程中客户端不断聚类,仅聚合簇内的客户端。IPFS支持冗余备份技术Erasurecoding,客户端可以自定义备份客户端文件数量。本文设定客户端是具有计算资源和通信能力的组织或者企业,拥有大量可训练的用户数据。

2.1 基于超级账本的参数传输模块

超级账本是点对点通信的去中心化分布式账本,因此,参与者需要向网络中的其他参与者证实自己的身份来获得交易的许可。在集群联邦优化模型中,客户端只有经过认证才可以参与训练,基于证书授权中心(CA)和成员服务提供者(MSP)进行成员身份认证,认证完成后方可参与训练,并且多通道可保证隐私安全和业务隔离,假设存在恶意攻击者想要破坏训练,必须进行身份验证后获得对账本操作的权限才能将错误数据同步到其他账本中。因此,Hyperledger Fabric保证了组织成员之间的相互信任,为训练提供了隐私保护的架构基础。

在横向联邦学习中,全局模型和本地模型具有相同的结构。假设模型有l层参数,每一层参数有参数向量$\boldsymbol{V}^l$,将模型参数分为$b(0<b\leqslant l)$个参数向量。客户端同一层参数维度相同,所有簇内客户端上传的参数块中必然存在两个或多个结构相同的参数块。对于每个参数块,由参数分割传输模块上传至星际文件系统(IPFS),如图3所示,参数块存入IPFS返回的Hash值,封装后存入超级账本中。

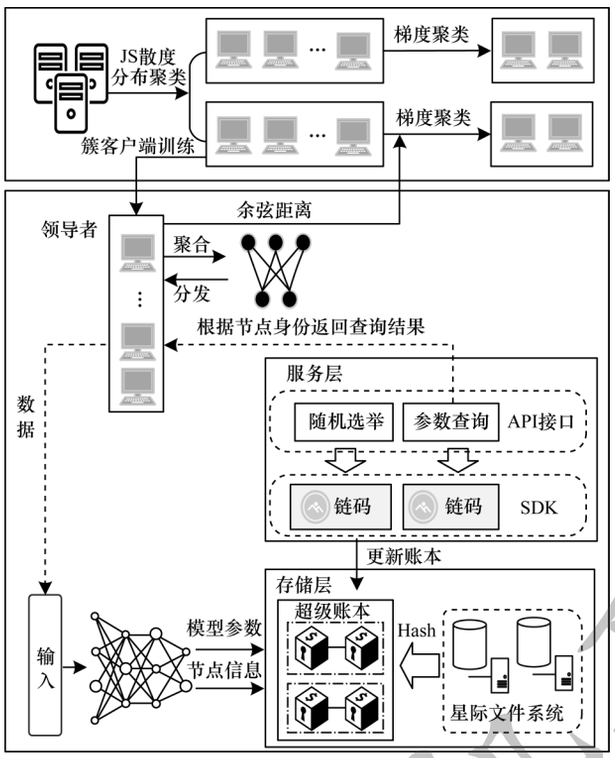

图3　基于超级账本的集群联邦优化模型

Fig.3　Cluster federated optimization model based on Hyperledger Fabric

如图4所示,客户端A和B分别有3层网络,将3层网络分割上传。超级账本虚线所指为训练成员A的存储示例,ParamHash存储的是客户端A的正确参数顺序(Layer代表上传的3层网络参数),Hash(Layer)代表对应层参数在星际文件系统中的哈希地址。服务层使用链码富查询方式查询状态数据库,根据联邦训练成员是否为领导者进行乱序操作:若为普通成员则由服务层将参数合并打乱顺序;若为领导者则正常返回。在图4中,客户端A被选举为领导者。若查询者为领导者A,则返回各客户端的参数Hash;若查询者为普通成员B,则返回参数乱序集合。其中服务层的乱序操作过程是把各客户端ParamHash合并,然后用随机函数将合并集合内的顺序打乱。普通成员返回乱序集合的目的是客户端可根据返回集合验证参数上传成功与否。客户端B的查询结果为一个乱序集合,对比上传文件返回的Hash查找验证集合中是否包含(包含什么)。

假设超级账本内部存在成员恶意攻击,混乱的参数顺序可以模糊真实的模型参数。假设分布式训练中有n个客户端,客户端对训练所得模型参数划分b个参数块。若客户端最大化分割参数使$b=l$,那么相同结构的参数块会有n个。恶意攻击者查询获得了乱序的集合,其在一个通信轮次中获取正确模型的概率为:

$$P(c_i)=\frac{1}{b^n},c_i\in C(0\leqslant i\leqslant n) \tag{1}$$

由式(1)可知,客户端数量越多,分割的参数层数越多,系统的安全性越高。因此,恶意攻击者难以进行梯度攻击。C是集群内客户端参数集$C=\{c_1,c_2,\cdots,c_n\}$。当集群联邦的通信轮次为R时,攻击者计算正确模型参数的难度指数级上升,攻击成功概率为$\left(\frac{1}{b^n}\right)^R$。同时,每一通信轮次中领导者随机选举产生,同一客户端获得连续聚合参数机会的概率很小。

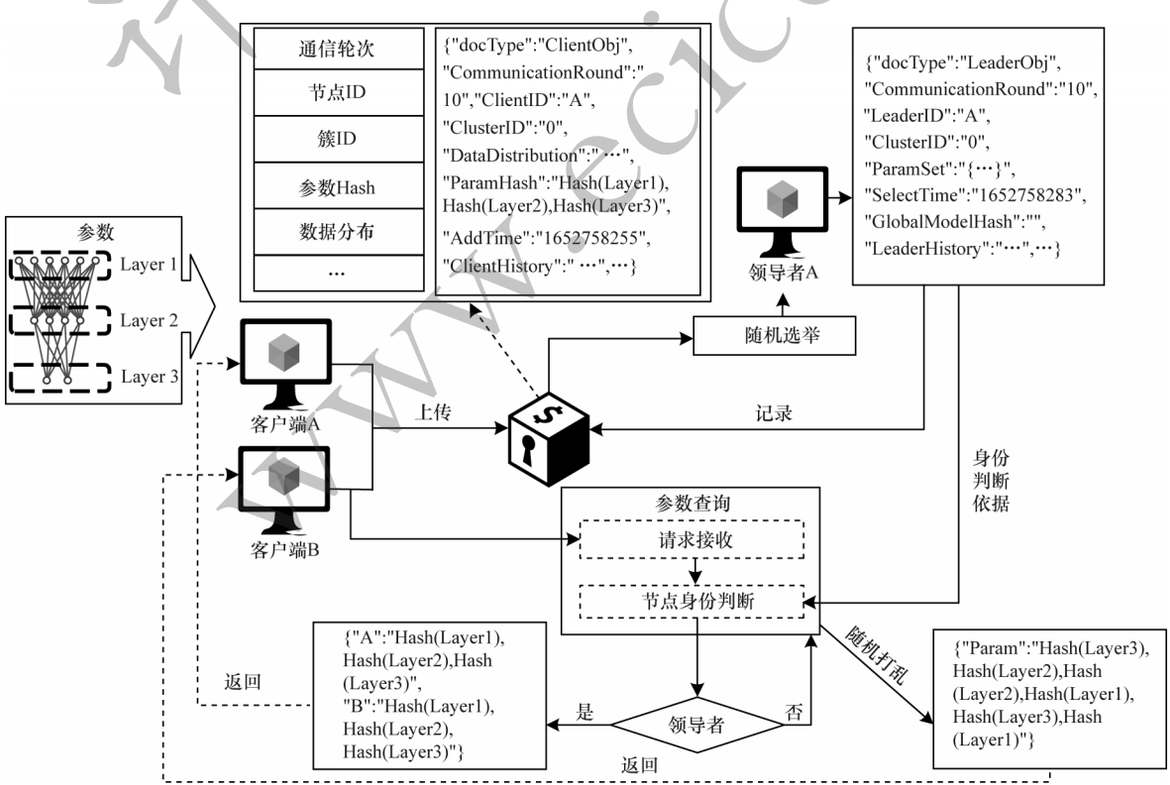

图4　客户端参数传输和查询过程

Fig.4　Client parameter transmission and query process

2.2 基于集群联邦学习的客户端重排算法

2.2.1 分布相似度

在实际应用场景中，客户端分布Non-IID和IID情况是可以同时存在的。将分布均匀的客户端单独分为一组，可以降低联邦训练的通信轮次，更快达到收敛状态。对客户端进行分类成为一个问题，因为联邦学习本身不会分析客户端的生成分布或其他任何元信息。由于Hyperledger Fabric是许可链，因此本文仅统计客户端的分布信息，并不会泄露任何数据隐私。为度量客户端之间的分布差异，实现良好的聚类效果，在机器学习中，经常使用KL散度衡量不同分布的差异，但KL散度本身是不对称的。基于KL散度的变体，JS散度解决了KL散度不对称的问题。一般地，JS散度是对称的，其取值在0到1之间。由以下公式可计算JS散度，其中P、Q分别代表两个分布，$P(x_i)$表示数据集中x_i标签的数量。

$$\mathrm{KL}(P\|Q)=\sum_{i=1}^{n}P(x_i)\mathrm{lb}\left(\frac{P(x_i)}{Q(x_i)}\right) \tag{2}$$

$$\mathrm{JS}(P\|Q)=\frac{1}{2}\mathrm{KL}\left(P\|\frac{P+Q}{2}\right)+\frac{1}{2}\mathrm{KL}\left(Q\|\frac{P+Q}{2}\right) \tag{3}$$

当客户端数量为n时，计算JS散度可得到$n\times n$的矩阵，使用K-means++进行聚类。由于客户端数据分布在训练过程中不发生变化，因此根据分布相似度所得的JS散度矩阵只在联邦训练初始化阶段用于聚类。

2.2.2 梯度相似度

本节将讨论服务器没有数据分布以及其他任何信息的情况下如何对客户端进行聚类。在上文叙述的Non-IID场景中，由于不同集群的客户端知识转移受到限制，因此性能产生了下降，而传统的联邦学习无法解决这个问题。与上文根据散度度量客户端分布类似，将模型优化方向一致的客户端分为同一组，能够提高组内模型的训练性能，梯度信息能更好地表达当前模型的优化方向。因此，本文用余弦距离度量两个客户端优化方向之间的距离。经验风险函数表示如下：

$$e_i(\theta)=\sum_{x\in D_i}l_\theta(f(x_i),y_i) \tag{4}$$

其中：l_θ是损失函数；y_i是真实标签；$f(x_i)$是预测结果；D_i是客户端数据分布。

由于模型参数不是一维的，因此本文使用Flatten方法，将多维的输入一维化，余弦距离计算公式如下：

$$\cos(\Delta e_i(\theta^*),\Delta e_j(\theta^*))=\frac{\left\langle\Delta e_i(\theta^*),\Delta e_j(\theta^*)\right\rangle}{\left\|\Delta e_i(\theta^*)\right\|\left\|\Delta e_j(\theta^*)\right\|} \tag{5}$$

当客户端数量为n时，计算客户端的余弦距离可得到$n\times n$的矩阵。客户端之间的梯度优化方向在联邦训练中才可以计算，联邦训练至收敛后且簇内模型参数满足聚类规则，则根据余弦相似度矩阵进行层次聚类。聚类得到的簇继续联邦训练，簇内聚合其内部客户端的模型参数。模型训练收敛后若满足聚类规则，则根据余弦相似度矩阵聚类；若不满足，则无须对该簇内客户端聚类划分。余弦相似度矩阵是该递归聚类划分过程中的数据特征。

2.2.3 客户端重排算法

集群联邦优化(CFO)算法以自上而下的方式递归地对客户端集群进行二分区划分。客户端重排则是优化的关键，算法执行集群联邦优化的聚类过程如图5所示[24]。

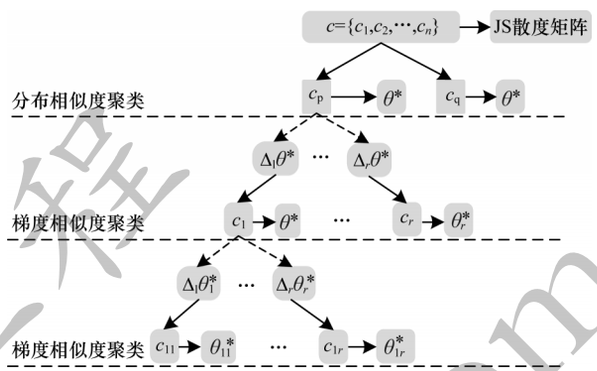

图5 集群联邦学习训练过程

Fig.5 Cluster federated learning training process

客户端余弦距离聚类规则如下：1)集群内模型训练已经收敛到一个驻点；2)客户端的经验风险函数接近真实风险；3)根据经验风险函数计算余弦相似度。上述3个规则可由下式表达：

$$\max_{i\in c^*}\left\|\Delta e_i(\theta^*)\right\| \tag{6}$$

$$\mathrm{mean}\left\|\Delta e_i(\theta^*)\right\| \tag{7}$$

式(6)表示集群联邦训练簇内模型参数变化最大的客户端的值，该值大于ε则表示簇内存在客户端未收敛。式(7)表示簇内所有客户端参数的平均值，该值小于τ则表示簇内客户端整体已趋近于收敛。

上述两种分布相似度，分别在训练前和训练中聚类使用。训练开始前根据分布相似度公式(见式(3))生成客户端JS散度矩阵对客户端进行聚类，训练过程中根据梯度相似度公式(见式(5))计算余弦距离矩阵，对余弦距离矩阵进行层次聚类，得到簇间余弦距离最大的两组。

集群联邦优化算法训练过程如算法1所示。首先，初始化客户端集群$c=\{c_1,c_2,\cdots,c_n\}$和模型参数θ_0；然后，依据式(3)计算JS散度矩阵，使用K-means++算法进行聚类，将客户端划分为C_p、C_q。客户端预处理完成后，聚类完成的各个簇(集群)开始联邦训练直到达到后处理聚类要求。算法使用客户端模型最大参数$\max_{i\in c^*}\left\|\Delta e_i(\theta^*)\right\|$和平均参数$\mathrm{mean}\left\|\Delta e_i(\theta^*)\right\|$表达余弦聚类规则，满足规则后进行层次聚类划分客户端集群，递归地二分区；最后，训练结束，输出目标模型的平稳解θ^*。若新客户端想要加入训练，则如算法2所示加入训练。算法从联邦优化的参数划分树的根节点开始遍历，新客户端

将本地数据集训练的模型参数与参数树节点的客户端进行对比,匹配梯度优化方向一致的簇。

算法1　集群联邦优化(CFO)

输入　初始化模型参数θ_0,客户端c,超参数$\varepsilon>0$,客户端数据D_i,阈值τ

输出　全局模型参数θ^*

Before//进入优化前执行

JS(c)→matrix//根据客户端分布计算JS散度矩阵

K-means++(matrix)→c^*//客户端根据矩阵聚类

1.Federated Learning(θ,c^*)//联邦训练

2.$\dfrac{\left\langle \Delta e_i(\theta^*),\ \Delta e_j(\theta^*)\right\rangle}{\left\|\Delta e_i(\theta^*)\right\|\left\|\Delta e_j(\theta^*)\right\|}\rightarrow \beta_{i,j}$//计算余弦距离矩阵

3.$\max\limits_{i\in c^*,j\in c^*}(\beta_{i,j})\rightarrow c_1,c_2$//最大余弦距离划分

4.if ($\max\limits_{i\in c^*}\left\|\Delta e_i(\theta^*)\right\|\geqslant\varepsilon$ and mean$\left\|\Delta e_i(\theta^*)\right\|\leqslant\tau$)

//簇内客户端最大梯度大于等于ε且平均梯度小于等于τ

5.CFO(θ,c_1)→θ_i^*, $i\in c_1$

6.CFO(θ,c_2)→θ_i^*, $i\in c_2$

7.else

8.$\theta^*\rightarrow\theta_i^*$

9.return θ_i^*, $i\in c$

算法2　新客户端加入集群

输入　新客户端数据D_{new},参数树$T=(V,E)$

输出　新加入客户端匹配组c_v

1.$v_{root}\rightarrow v$

2.While child(v) is not null//v存在孩子

3.child(v)→v_{left}, v_{right}

4.SGD(θ^*, D_{new})−$\theta_v^*\rightarrow\Delta\theta_{new}$//随机梯度下降

5.$\max\limits_{v\rightarrow v_{left}}(\Delta\theta_{new},\Delta\theta)\rightarrow\alpha_{left}$

6.$\max\limits_{v\rightarrow v_{right}}(\Delta\theta_{new},\Delta\theta)\rightarrow\alpha_{right}$

7.if $\alpha_{left}<\alpha_{right}$

8.$v\rightarrow v_{left}$

9.else

10.$v\rightarrow v_{right}$

11.return c_v

2.3　可信智能合约模块

智能合约是运行在区块链上的一段代码,代码的逻辑定义了合约的内容。超级账本中智能合约被称为链码,开发人员实现接口则可通过API实现对账本的操作。超级账本中的链码分为系统链码和用户链码,一般系统链码无须安装,用户链码则可由用户自定义业务逻辑。用户链码安装实例化后有2种调用方式:1)直接使用命令调用;2)通过SDK后端调用。命令行一般由开发人员调用,SDK更灵活且适合用户。因此,本文选用第2种方式。参与联邦训练的客户端共有2种角色:领导者和普通成员。领导者和普通成员都可通过后端服务访问账本,但不同的身份查询参数会返回不同的结果。服务层通过链码可以查询获得各个客户端上传的参数,根据查询者是否为领导者进行参数乱序操作。

2.3.1　选举

超级账本为模型提供了去中心化的平台和隐私保护的支持,可在安全的环境下对分散的模型进行训练。集群联邦优化模型与联邦学习相比省略了一个中心参数服务器,但客户端集群仍需要一个全局模型。客户端本地训练完成后,通过服务层将客户端分割参数上传至超级账本。集群内客户端上传参数后,服务层调用链码选举出领导者。本文采用随机选举的方式产生领导者,选举的范围是当前通信轮次中传输参数的客户端,选举产生的结果记录在超级账本中。如图4所示,客户端A被选举为领导者,其客户端与簇的信息也会被同时记录。客户端被选举为领导者后查询客户端参数Hash并下载聚合,完成聚合后则上传全局模型参数并更新账本中领导者信息全局模型哈希地址(Global ModelHash),普通成员更新全局模型。领导者的功能是代替原有的中央服务器,动态的领导者可以避免中心化训练的单点故障问题[26],保证正常训练。当模型训练趋于收敛时,领导者可以执行2.2.3节中的客户端重排算法。

领导者聚合时间为选举结束至获取参数聚合,若超时则重新选举。因此,重新选举后只需要更新账本中的领导者信息,无须回滚。

2.3.2　聚合

目前,联邦学习中广泛应用的聚合算法是FedAvg[16]。FedAvg对客户端的梯度更新进行平均以形成全局更新,同时用当前全局模型替换未采样的客户端。领导者聚合获得全局模型并评估,将全局模型上传至超级账本,客户端下载获得最新全局模型。在下一通信轮次前,客户端更新模型和超参数。集群联邦学习在集群内的聚合方式与FedAvg相同,智能合约聚合方式如算法3所示。

算法3　聚合

输入　初始化全局模型参数w_0

1.$w_0\rightarrow w_1$

2.for 通信轮次 t=1,2,…,T

3.for 客户端$c_i\in c_k$

4.本地训练(c_i, w_t)→Δw_{t+1}^i

5.$w_t+\sum\limits_{i\in c_k}\dfrac{n_i}{n}(c_i,w_t)\rightarrow\Delta w_{t+1}^i$//领导者下载参数聚合

6.本地训练(c_i, w_t):本地训练

7.$w\rightarrow w^*$

8.for 本地训练批次 e=1,2,…,E

9.$w-\eta\Delta L(b;w)\rightarrow w^*$//学习率η,损失函数L,批数据b

10.return $w-w^*\rightarrow\Delta w$

3　实验与评估

基于超级账本的集群联邦优化模型使用超级账本作为底层平台,使用星际文件系统传输和存储数据。本文实验在Ubuntu 20.04.4 LTS,4 GB内存,6核处理器中部署超级账本网络,服务层部署在装有超级账本容器的虚拟机上,联邦客户端训练环境为PyTorch 1.9.0,显卡GTX-1660Ti。实验环境中后端服务仅单机部署,若需要应对服务层故障,在实际场景下建议多机部署

并使用Nginx代理,保证服务的可用性。

3.1 数据集和模型

在MNIST、EMNIST两个公开图像数据集上评估本文方法的有效性。MNIST[27]中包含10类手写数字图像分类任务,分别为0~9的数字;因为神经网络模型在MNIST上都有很高的精度,为了增加难度,所以选用Extended MNIST,分别加入26类小写字母和大写字母。训练模型具体如表1所示。

表1 训练模型

Table 1 Training model

卷积神经网络	MNIST	EMNIST
Layer 1	Conv2d(5,5)	Conv2d(5,5)
Layer 2	MaxPool(2,2)	MaxPool(2,2)
Layer 3	Conv2d(5,5)	Conv2d(5,5)
Layer 4	MLP(256)	MLP(256)
Layer 5	MLP(84)	MLP(62)
Layer 6	MLP(10)	—

3.2 实验结果分析

实验使用的超级账本网络含2个组织,客户端中包含IID和Non-IID数据。为了模拟数据在Non-IID下的情况,实验取部分数据将其标签按狄利克雷分布划分至客户端,因为采用样本标签分布来划分Non-IID是简便有效的方法。MNIST和EMNIST数据集均使用SGD随机梯度下降算法作为优化器,客户端c=10,学习率η=0.1,动量参数momentum=0.9,批数据大小batch size=128。

MNIST、EMNIST数据集所用模型前3层基本相同:第1层是单通道卷积层,卷积核大小为5×5,步长为1;第2层是池化层,最大池化窗口为2×2;第3层是通道数为6的卷积层,卷积核大小为5×5。由于2个数据集标签类别数不同,因此输出使用的全连接层略有区别,激活函数均为ReLU。如算法1集群联邦优化所描述,集群内客户端联邦训练收敛至驻点且经验风险函数接近真实风险,算法才会执行聚类。

图6所示为MNIST客户端在IID与Non-IID不同比例下集群联邦优化后的测试集准确率结果。图6(d)异构数据和非异构数据比例相等,训练开始前依据JS散度相似度进行客户端聚类,测试集平均准确率在第10轮通信前已经收敛到模型最优解。实验证明,聚类分布一致的客户端在更小通信代价和更少的计算资源下得到了联邦训练最优解。由图6(a)~图6(c)可以看出,客户端聚类后测试准确率明显上升(图中垂直竖线代表按余弦距离划分客户端)。在图6(d)中,按梯度相似度聚类后准确率没有明显提高,原因是训练前根据分布相似度聚类有效提高了模型训练效果。

图7所示为EMNIST客户端在IID与Non-IID不同比例下集群联邦优化后测试集的准确率结果,由于EMNIST数据集相对MNIST略微复杂,因此实验效果相对MNIST更明显。由图7(a)~图7(c)可以看出,依据梯度相似度聚类(垂线)后,准确率明显提高,同时图7(d)充分说明了分布相似度聚类对模型收敛和性能提升有显著效果。

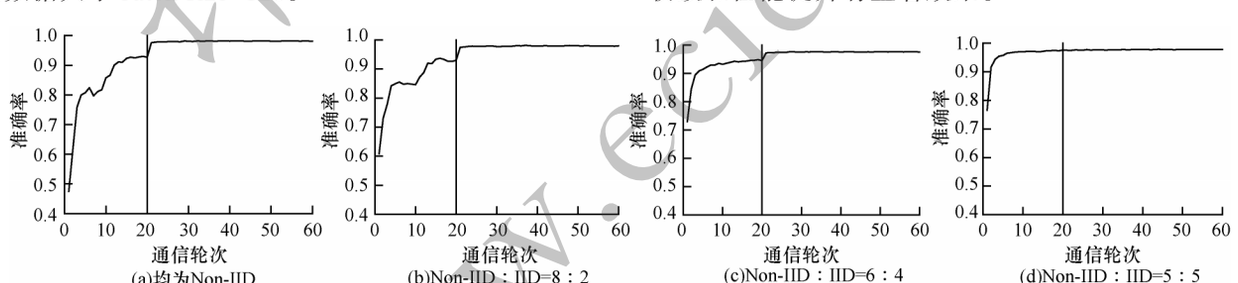

图6 MNIST客户端在IID与Non-IID不同比例下集群联邦优化后的测试集准确率

Fig.6 Test accuracy of the MNIST client after CFO under different ratios of IID and Non-IID

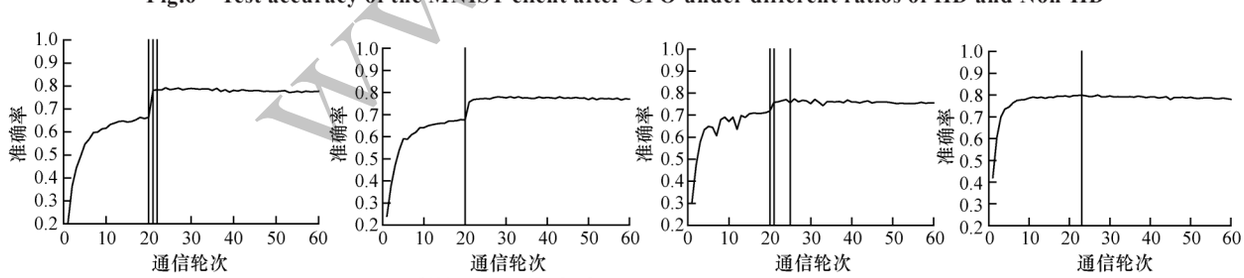

图7 EMNIST客户端在IID与Non-IID不同比例下集群联邦优化后的测试集准确率

Fig.7 Test accuracy of the EMNIST client after CFO under different ratios of IID and Non-IID

图8(a)和图8(b)分别为MNIST和EMNIST客户端经CFO优化后训练集准确率对比,可见较FedAvg分别提升了6.398%和17.260%,证明了集群联邦优化的有效性。

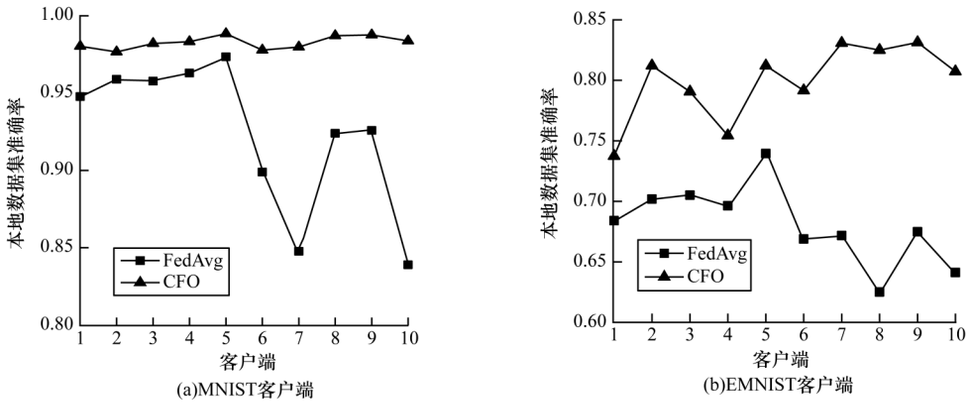

图8　客户端测试准确率

Fig.8　Client test accuracy

为了对比不同训练方式在数据Non-IID下的表现，本文分别在2个数据集上实验了4种不同的训练模式：集中训练，联邦平均（FedAvg），集群联邦（CFL），以及本文的优化方法。客户端含有IID和Non-IID数据（比例相等），如图9所示，可以看出：集中学习因数据集中统一训练，收敛速度和准确率表现最优；FedAvg表现最差；本文的优化方法相较CFL收敛更快，由图9(b)可以看出，本文相较CFL速度提升了36.3%。

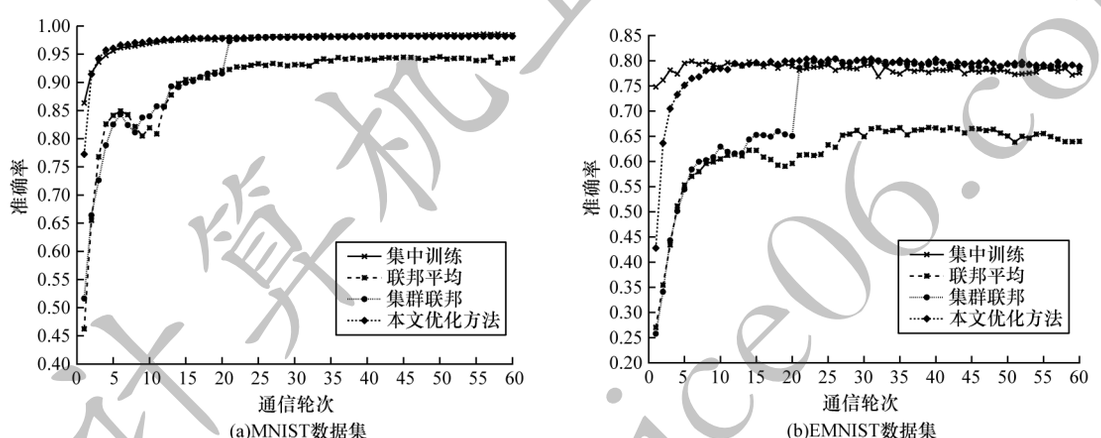

图9　Non-IID对比实验结果

Fig.9　Results of Non-IID comparison experiment

4　结束语

联邦学习是一种主流的分布式机器学习框架，但其存在单点故障、参数服务器泄露用户隐私数据风险以及数据偏态分布下训练性能较差的问题。本文设计一种基于超级账本的集群联邦优化模型，以超级账本作为分布式训练隐私保护的架构基础，使用星际文件系统存取参数，结合集群联邦学习对异构数据进行优化，利用智能合约可信聚合参数。实验结果表明，该模型在保护数据隐私的同时，较传统联邦学习模型具有更好的性能。下一步将研究如何度量参与训练客户端的贡献度，设计正向积极的激励机制提升训练效率，扩大模型的适用范围。

参考文献

[1] RADFORD A，NARASIMHAN K，SALIMANS T，et al. Improving language understanding by generative pre-training[EB/OL]. [2022-04-27]. https://cdn. openai. com/research-covers/language-unsupervised/language_understanding_paper. pdf.

[2] RADFORD A，WU J，CHILD R，et al. Language models are unsupervised multitask learners[EB/OL]. [2022-04-27]. https://cdn. openai. com/better-language-models/language_models_are_unsupervised_multitask_learners. pdf.

[3] BROWN T B，MANN B，RYDER N，et al. Language models are few-shot learners[EB/OL]. [2022-04-27]. https://arxiv. org/pdf/2005. 14165. pdf.

[4] WARNAT-HERRESTHAL S，SCHULTZE H，SHASTRY K L，et al. Swarm learning for decentralized and confidential clinical machine learning[J]. Nature，2021，594(7862)：265-270.

[5] JIANG J C，KANTARCI B，OKTUG S，et al. Federated learning in smart city sensing：challenges and opportunities[J]. Sensors(Basel，Switzerland)，2020，20(21)：6230.

[6] LIM W Y B，LUONG N C，HOANG D T，et al. Federated learning in mobile edge networks：a comprehensive survey[J]. IEEE Communications Surveys & Tutorials，2020，22(3)：2031-2063.

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

[8] ZHU L, LIU Z, HAN S. Deep leakage from gradients[C]// Proceedings of the 33rd International Conference on Neural Information Processing Systems. New York, USA: ACM Press, 2019: 14774-14784.
[9] MELIS L, SONG C Z, DE CRISTOFARO E, et al. Exploiting unintended feature leakage in collaborative learning[C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2019: 691-706.
[10] YAN X D, CUI B J, XU Y, et al. A method of information protection for collaborative deep learning under GAN model attack[J]. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2021, 18(3): 871-881.
[11] HITAJ B, ATENIESE G, PEREZ-CRUZ F. Deep models under the GAN: information leakage from collaborative deep learning[C]//Proceedings of 2017 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM Press, 2017: 603-618.
[12] PYRGELIS A, TRONCOSO C, DE CRISTOFARO E. Knock knock who's there? Membership inference on aggregate location data[EB/OL]. [2022-04-27]. https://arxiv.org/pdf/1708.06145.pdf.
[13] SATTLER F, WIEDEMANN S, MÜLLER K R, et al. Robust and communication-efficient federated learning from non-i.i.d. data[J]. IEEE Transactions on Neural Networks and Learning Systems, 2020, 31(9): 3400-3413.
[14] SAHU A K, LI T, SANJABI M, et al. On the convergence of federated optimization in heterogeneous networks[EB/OL]. [2022-04-27]. https://arxiv.org/pdf/1812.06127.pdf.
[15] LI X, HUANG K, YANG W, et al. On the convergence of FedAvg on non-iid data[EB/OL]. [2022-04-27]. https://arxiv.org/pdf/1907.02189.pdf.
[16] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[EB/OL]. [2022-04-27]. https://arxiv.org/abs/1602.05629.
[17] ZHAO Y, LI M, LAI L, et al. Federated learning with non-IID data[EB/OL]. [2022-04-27]. https://arxiv.org/pdf/1806.00582.pdf.
[18] 朱建明,张沁楠,高胜,等. 基于区块链的隐私保护可信联邦学习模型[J]. 计算机学报,2021,44(12):2464-2484.
ZHU J M, ZHANG Q N, GAO S, et al. Privacy preserving and trustworthy federated learning model based on blockchain[J]. Chinese Journal of Computers, 2021, 44(12): 2464-2484. (in Chinese)
[19] SATOSHI N. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2022-04-27]. https://bitcoin.org/en/bitcoin-paper.
[20] The Technical Working Group China. Fabric-documentation[EB/OL]. [2022-04-27]. https://hyperledger-fabric.readthedocs.io/zh_CN/release-2.2/index.html.
[21] KONEČNÝ J, MCMAHAN B, RAMAGE D, et al. Federated optimization: distributed optimization beyond the datacenter[EB/OL]. [2022-04-27]. https://arxiv.org/pdf/1511.03575.pdf.
[22] GHOSH A, CHUNG J, YIN D, et al. An efficient framework for clustered federated learning[J]. Advances in Neural Information Processing Systems, 2020, 33: 19586-19597.
[23] LI X C, ZHAN D C. FedRS: federated learning with Restricted Softmax for label distribution non-IID data[C]// Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. New York, USA: ACM Press, 2021: 995-1005.
[24] SATTLER F, MÜLLER K R, SAMEK W. Clustered federated learning: model-agnostic distributed multitask optimization under privacy constraints[J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 32(8): 3710-3722.
[25] DUAN M M, LIU D, JI X Y, et al. Flexible clustered federated learning for client-level data distribution shift[J]. IEEE Transactions on Parallel and Distributed Systems, 2022, 33(11): 2661-2674.
[26] BAO X, SU C, XIONG Y, et al. FLChain: a blockchain for auditable federated learning with trust and incentive[C]// Proceedings of the 5th International Conference on Big Data Computing and Communications. Washington D. C., USA: IEEE Press, 2019: 151-159.
[27] LECUN Y, BOTTOU L, BENGIO Y, et al. Gradient-based learning applied to document recognition[J]. Proceedings of the IEEE, 1998, 86(11): 2278-2324.

编辑 金胡考