中国科学: 信息科学 2021 年 第 51 卷 第 10 期: 1755–1774
SCIENTIA SINICA Informationis
论文

一种基于区块链的隐私保护异步联邦学习

高胜[1*], 袁丽萍[1], 朱建明[1], 马鑫迪[2], 章睿[3], 马建峰[2]

1. 中央财经大学信息学院, 北京 100081
2. 西安电子科技大学网络与信息安全学院, 西安 710071
3. 中国科学院信息工程研究所, 北京 100093
* 通信作者. E-mail: sgao@cufe.edu.cn

收稿日期: 2021–03–10; 修回日期: 2021–05–21; 接受日期: 2021–07–08; 网络出版日期: 2021–10–12

国家自然科学基金 (批准号: 62072487, 61902290)、北京市自然科学基金 (批准号: M21036)、全国统计科学研究 (批准号: 2020LD01) 和陕西省重点研发计划 (批准号: 2020ZDLGY09-06, 2019ZDLGY12-04) 资助项目

摘要 联邦学习能够在保障本地数据隐私前提下利用分布式数据和计算资源实现机器学习模型联合训练. 现有异步联邦学习有效解决了同步联邦学习所存在的计算资源浪费、训练效率低等问题. 然而, 现有异步联邦学习通过聚合不同节点训练得到局部模型, 并通过中心服务器完成全局模型更新, 内生性地受制于中心化信用模式, 存在单点失效、隐私泄露等问题. 为此, 提出了一种基于区块链的隐私保护异步联邦学习, 通过上链局部模型并通过共识算法生成全局模型, 保证异步联邦学习的可信性. 为了保证联邦学习的隐私性, 同时提高模型效用, 提出利用差分隐私中的指数机制以高概率选择贡献度高的模型梯度, 并分配较低的隐私预算以保证局部模型的隐私性. 另一方面, 针对异步联邦学习时钟不同步问题, 提出了双因子调整机制进一步提高全局模型效用. 最后, 理论分析与实验结果表明所提出的方案能有效保证异步联邦学习的可信性和隐私性, 同时提高了模型效用.

关键词 联邦学习, 区块链, 差分隐私, 模型效用, 异步训练

1 引言

随着物联网和边缘计算的兴起, 数据通常不由单一主体管理而是分布在多个参与方. 然而, 由于经济效用、法律政策、标准体系等因素, 各参与方之间数据共享面临 “不愿、不敢、不能” 等困境, 进而形成了各自为政的 “数据孤岛”, 严重阻碍数据驱动型技术的广泛应用. 联邦学习本质上是一种分布式机器学习, 能在保障各参与方数据不出本地情况下协同训练共享的全局模型, 成为整合数据碎片化、破除数据孤岛化、推动人工智能发展的新范式 [1,2]. 一般地, 联邦学习主要实体包括任务参与方和参数服务器. 参数服务器首先以外包形式 [3] 将初始全局模型发送给任务参与方. 然后在每轮协作训练过程中, 每个参与方基于本地训练数据集迭代执行局部模型训练, 并将模型参数发送给参数服务器, 之

引用格式: 高胜, 袁丽萍, 朱建明, 等. 一种基于区块链的隐私保护异步联邦学习. 中国科学: 信息科学, 2021, 51: 1755–1774, doi: 10.1360/SSI-2021-0087
Gao S, Yuan L P, Zhu J M, et al. A blockchain-based privacy-preserving asynchronous federated learning (in Chinese). Sci Sin Inform, 2021, 51: 1755–1774, doi: 10.1360/SSI-2021-0087

后由参数服务器聚合每个参与者发送的参数更新全局模型参数, 并返回给任务参与者 [4,5]. 相比将不同来源的数据统一聚合到参数服务器建立机器学习模型, 联邦学习能够确保参与方拥有的本地数据不脱离参与方控制而进行联合模型训练, 较好地解决了数据孤岛、数据隐私等问题. 目前联邦学习已广泛应用于各个领域 [6], 如智慧金融 [7]、智慧医疗 [8]、自动驾驶 [9]、无线通信 [10]、目标检测 [11] 等.

然而, 现有联邦学习大多依赖于参数服务器生成或更新全局模型参数, 是一种典型的中心化架构, 存在单点失效、隐私泄露、性能瓶颈等问题 [12,13]. 全局模型的可信性依赖于参数服务器, 本质上内生性地受制于中心化信用模式. 区块链作为一种由多方共同维护的分布式共享总账, 通过分布式账本技术、密码算法、点对点通信、共识机制、智能合约等多种技术组合创新, 实现在不依赖于可信第三方信用背书条件下建立参与方之间的信任关系 [14,15]. 为此, 现有研究利用区块链构建分布式可信联邦学习, 通过链上存储模型更新并执行设计的共识机制以完成联邦学习任务, 有效缓解因参数服务器中心化所带来的问题 [16~21]. 然而, 这些方案都没有考虑更新参数所带来的隐私泄露问题. 参与者或攻击者可以利用局部模型更新参数逆向推断出其他参与者本地训练数据的隐私信息 [22~24].

为解决联邦学习过程中模型参数带来数据隐私泄露问题, 现有一部分研究利用密码技术, 如同态加密 [25]、安全多方计算 [26~28] 等, 加密各参与者发送的模型参数以抵御模型推断攻击. 尽管密码技术可以实现较好隐私保护, 但带来较高的计算复杂度和通信开销, 难以满足大规模数据训练需求. 另一部分研究差分隐私 [29,30], 通过给模型参数添加扰动噪声使得攻击者难以推断出原始模型参数 [31~33]. 尽管差分隐私具有较好的隐私保护性能, 但需要权衡数据隐私和模型效用. 总体而言, 这些方案大都依赖于参数服务器聚合参与者发送的模型参数, 难以保证全局模型的可信性.

此外, 上述方案大都是同步联邦学习, 即需要等待所有参与者完成局部模型训练后才能进行全局模型的更新. 显然, 每轮全局模型迭代训练都要求参与者花费大量时间等待局部模型训练最慢的一方. 当参与者数量较多时, 局部模型的并行通信会导致信道资源的紧张, 降低联邦学习的训练效率. 虽然已有研究提出异步联邦学习以缓解上述问题, 但这些方案依旧受到中心化架构带来的安全威胁, 同时忽略了不可靠的局部更新模型对全局模型质量的影响 [34~36]. 因此, 如何在保护数据隐私的同时提高全局模型的质量、保障模型的可信性是实现异步联邦学习可持续发展的关键性问题.

为解决上述问题, 本文提出了一种基于区块链的隐私保护异步联邦学习. 为均衡数据隐私与模型效用, 采用差分隐私中的指数机制完成对局部模型训练目标贡献度高的模型梯度值的采样, 并通过拉普拉斯机制进一步实现不同隐私预算分配下模型的扰动. 在此基础上, 提出双因子调整机制以降低不可靠局部模型对全局模型质量的影响. 本文的主要贡献如下:

- 提出了一种基于区块链的隐私保护异步联邦学习, 解决同步联邦学习中模型训练效率低、计算资源闲置浪费等问题. 为解决异步联邦学习中数据隐私与模型效用不均衡问题, 利用指数机制实现对较高贡献度梯度值的隐私采样, 并在此基础上利用拉普拉斯机制差异化扰动模型梯度值.
- 为降低异步联邦学习中由时钟不同步问题对全局模型可用性的影响, 本文提出了一种双因子调整机制, 通过定义模型时间权重与质量权重以完成全局模型更新, 进一步提高全局模型效用.
- 从隐私性、可信性、可用性等方面理论分析了本文所提出方案的安全性并在真实数据集上进行仿真实验, 实验结果表明本文所提出的方案在保障数据隐私, 同时提高了联邦学习的模型效用.

本文第 2 节介绍了联邦学习的相关研究工作. 第 3 节介绍了区块链、联邦学习和差分隐私的基本理论知识. 第 4 节介绍了本文的系统架构与设计目标. 第 5 节介绍了基于区块链的隐私保护异步联邦学习的设计细节. 第 6 节主要从隐私性、可信性和可用性 3 个方面对所提出的方案进行了分析. 第 7 节在真实数据集上通过对比仿真实验验证方案的有效性. 第 8 节对本文的工作进行了总结.

2 相关工作

联邦学习是一种具有本地数据隐私保护的分布式机器学习, 它允许训练数据在不出本地的情况下通过参数交换的方式构建全局模型. 然而, 现有研究大部分依赖于参数服务器协同完成全局模型更新, 存在单点失效、性能瓶颈、隐私泄露、模型不可信等问题 [12,13]. 部分工作研究具有隐私保护的联邦学习, 即利用同态加密、安全多方隐私、差分隐私等技术保证训练数据或模型参数等隐私信息 [25~28,31~33]. 然而, 这些研究中模型可信性本质上依赖于参数服务器. 为保证模型可信性, 部分研究利用区块链的技术特性构建了不依赖于参数服务器的可信联邦学习. 例如, Kim 等 [16] 提出构建基于区块链的联邦学习架构, 通过分布式场景下对局部模型更新参数进行交叉验证来增强全局模型可信性. Ramanan 和 Nakayama [17] 利用区块链存储全局模型, 并通过智能合约聚合模型更新参数. Li 等 [18] 设计不同区块结构存储局部模型和全局模型以降低参与节点存储开销, 并提出了采用群组共识提高联邦学习效率. Kang 等 [19] 提出利用区块链存储主观逻辑模型计算的信用值来选择可信参与者, 从而增强移动网络中联邦学习可靠性. Peng 等 [20] 利用区块链构建了可验证和可审计的安全联邦学习, 并且设计了可验证的数据结构提高区块审计效率. 然而, 这些研究大都没有考虑模型更新参数所带来的数据隐私泄露问题.

为此, Chen 等 [37] 提出了一种基于区块链的安全隐私分布式机器学习系统 LearningChain, 利用差分隐私扰动局部模型梯度保护数据隐私, 通过聚合与区块链存储的局部模型梯度值之和最接近的若干梯度更新全局模型梯度来抵御拜占庭攻击. 然而, 他们采用工作量证明 (proof of work, PoW) 共识, 存在计算开销大、效率低等, 并且难以抵御串谋攻击. Kim 等 [38] 采用联盟链 Hyperledger Fabric 构建分布式机器学习系统以提高 LearningChain 训练效率, 同时在差分隐私的随机梯度下降算法中使用基于错误的参数聚合规则以抵御串谋攻击. Lu 等 [39] 将互不可信多方数据共享问题转化为可信联邦学习问题, 利用差分隐私扰动本地训练数据, 并通过与数据查询相关的参与者构成群组执行训练质量证明共识来保证区块链存储局部模型和全局模型的可信性. Zhao 等 [40] 利用区块链构建了一种面向智能家居设备的隐私保护联邦学习, 用以预测用户需求及习惯. 通过差分隐私扰动卷积神经网络提取的设备特征保护数据隐私, 同时提出了新的批归一化方法和信誉激励机制提高模型训练准确性和可靠性. Weng 等 [41] 提出了基于区块链的分布式深度学习 DeepChain, 其中采用区块链激励机制保障模型训练的公平性, 利用非交互零知识证明实现模型训练的可审计性, 利用门限 Paillier 加法同态保证模型参数的隐私性. Lyu 等 [42] 基于区块链构建了具有公平性和隐私性的联邦学习, 通过参与者之间信用相互评估机制保证模型训练的公平性, 同时结合差分隐私生成对抗网络和三重加密来保证模型训练的准确性和隐私性. 总体而言, 这些联邦学习方案大都采用同步化网络设置, 即要求参与方将局部模型参数发送给其他参与方, 同时等待更新后才进行下一轮模型迭代训练. 然而, 参与方局部模型训练的不确定性、传输数据量及通信质量等使得同步联邦学习可能面临通信时延大、等待时间长、计算资源闲置浪费等问题.

异步联邦学习通过避免各参与方的空闲等待时间减少通信开销, 同时在部分计算节点失效的情况下仍能保障协作训练的有效性. Xie 等 [34] 提出了一种基于非独立同分布训练数据的异步联邦学习优化算法以提高协作训练的灵活性和可扩展性. Lu 等 [43] 提出了一种隐私保护异步联邦学习机制, 通过设计自适应梯度压缩算法以减少由于频繁梯度通信所导致的隐私泄露风险, 并提出双权重矫正机制以解决异步联邦学习中各参与方训练状态不平衡问题. 然而上述方案仍然受到传统中心化架构所带来的安全威胁, 同时在传输局部模型参数时容易产生数据隐私间接泄露的风险 [22~24]. Lu 等 [44] 提出了一种基于差分隐私的异步联邦学习方案, 通过设计随机分布式更新机制以完成全局模型的更新. Chen

表 1 符号与描述

Table 1 Notations and descriptions

Notations	Descriptions
N	The number of federated learning participants
$P=\{p_1,p_2,\ldots,p_N\}$	The set of federated learning participants
D_i	The private local training dataset of participant p_i
w_i^k, w_G^k	The local model and the global model at the k-th epoch
$B=\bigcup_{i=1}^{N} B_i$	The mini-batch of the training dataset
η_i	The learning rate of participant p_i
$\nabla g(\cdot)$	The gradients of the local model
$f(\cdot)$	The prediction function
$L(w_i^k)$	The local loss function of participant p_i at the k-th epoch
$L(w_G^k)$	The global loss function at the k-th epoch
M	The stochastic algorithm
ε	The privacy budget
q	The query function
Δq	The global sensitivity
u	The utility function

等 [45] 基于区块链构建了一种用于协同训练疾病分类模型的异步联邦学习, 通过差分隐私扰动随机梯度下降算法参数保护数据隐私, 同时利用梯度延迟补偿算法 [46] 解决同步联邦学习存在问题. Lu 等 [47] 基于混合区块链提出了一种用于车联网数据安全共享的异步联邦学习. 首先使用深度强化学习选择合适的车辆以异步联邦学习效率, 然后利用所选择的车辆将每轮迭代局部模型参数以交易形式写入有向无环图, 最后由选择的路侧单元进行全局模型更新. 然而, 其全局模型更新仍然采用同步化方式. 总体而言, 目前对异步联邦学习的研究仍然不充分, 特别是对模型可信性、模型质量和数据隐私等方面的研究仍然比较匮乏.

3 预备知识

本节简单介绍相关的基础知识, 包括区块链、联邦学习和差分隐私. 在介绍之前, 为了描述方便, 表 1 列出了本文常用的符号和相应的描述.

3.1 区块链

比特币[1)] (Bitcoin) 的成功使得其底层支撑技术区块链受到广泛关注 [48, 49]. 区块链本质上是一种分布式共享总账, 通过密码学、点对点通信、分布式存储、共识机制、智能合约等多种技术组合创新, 保障互不信任双方交易过程的可信性, 解决了传统交易过程内生性地受制于可信第三方信用背书的问题 [14]. 根据应用需求不同, 区块链部署类型可分为公有链, 如 Bitcoin[2)], Ethereum[3)] 等; 联盟链,

1) https://bitcoin.org/en/bitcoin-paper.
2) https://bitcoin.org/en/.
3) https://ethereum.org/en/.

如 Hyperledger Fabric[4]; 私有链, 如 Multichain[5]. 公有链允许任何节点自由参与或退出, 而联盟链需要由联盟、私有链需要由机构对参与节点进行身份认证. 相比于公有链的去中心化、低吞吐量、难监管等以及私有链的中心化、高吞吐量等, 联盟链因其多中心化、较高吞吐量、容易监管等特点成为实用性强的部署形式. 区块链中每个区块由包含元数据的区块头和包含交易数据的区块体组成. 区块头通过包含上一个区块哈希形成链式结构, 以及通过 Merkle 根哈希保证区块体中交易数据的存在性和完整性. 区块体记录了面向不同应用场景的交易数据, 其中每笔交易数据本质上是一个交易地址发往另一位交易地址的签名数据包.

共识机制作为驱动区块链运转的核心, 定义了在预设规则下分布式节点对打包交易形成的区块达成一致性意见的过程. 根据区块链部署类型分为公有链共识算法和联盟链共识算法. 公有链共识算法的特点是任何节点均可参与或退出共识过程, 典型的如工作量证明 (proof of work, PoW)、权益证明 (proof of stake, PoS)、委托权益证明 (delegated proof of stake, DPoS) 及其衍生算法等. PoW 依据节点算力值决定记账节点, 存在资源浪费、效率低等问题. PoS 则用代表节点资产的权益值选择记账节点以缓解 PoW 的不足, 然而权益值高的节点未必愿意参与记账过程, 同时其还面临诸如无利害关系攻击 (nothing-at-stake)、长程攻击 (long-range attack)、后腐败攻击 (posterior corruption) 等问题 [50]. DPoS 将节点所持有的权益值作为选票选举出得票数多且愿意参与共识的前若干代理节点组成共识委员会, 由代理节点按照时间片轮转方式生成区块. 联盟链共识算法的特点是通过了准入控制的节点方可加入共识委员会, 可以分为故障容错 (crash fault tolerant, CFT)、拜占庭容错 (Byzantine fault tolerant, BFT) 及其衍生算法等. 除了 CFT 类共识中节点宕机、网络故障等因素外, BFT 类共识还能在容忍一定节点作恶情况时达成意见一致性, 典型的如 PBFT 算法. PBFT 算法 [51] 在弱同步网络下可容忍不超过全网节点数 1/3 的拜占庭节点, 同时将原始 BFT 算法复杂度由指数级降低到多项式级, 增强了实际应用可行性.

3.2 联邦学习

联邦学习中参数服务器可将训练任务外包给参与方, 各参与方通过参数交换的方式协作完成全局模型的构建. 一般地, 假设有 N 个参与者 $P=\{p_1,p_2,\ldots,p_N\}$ 构成的集合协同进行联邦学习, 其中参与者 p_i 拥有本地训练数据集 $D_i=\{(x_1,y_1),(x_2,y_2),\ldots,(x_m,y_m)\}$, 其中 $x_i\in \mathrm{X}^u$ 表示维度为 u 的输入样本, y_i 表示样本的标签值. 整个训练数据集为 $D=\bigcup_{i=1}^{N} D_i$. 联邦学习过程可形式化描述如下 [1,12].

(1) 系统初始化. 首先定义联邦学习任务, 并初始化模型训练的超参数, 如迭代次数、学习速率等; 然后将初始化全局模型 w_G^0 广播给联邦学习参与者集合 P.

(2) 局部模型训练. 在第 k 轮迭代过程中, 参与者 p_i 在上一轮局部模型 w_i^{k-1} 基础上利用本地数据集 D_i 训练局部模型 w_i^k, 其目标是使得局部模型损失函数最小化, 即

$$w_i^k \leftarrow \min_{w_i^{k-1}} \left\{ \frac{1}{m}\sum_{j=1}^{m} L(f(w_i^{k-1},x_j),y_j) \right\}, \tag{1}$$

其中 $f(w_i^{k-1},x_j)$ 表示第 k 轮迭代的局部模型预测值, y_i 表示样本 x_i 的实际标签值. 损失函数 $L(w_i^{k-1})$ 表示模型的预测值与真实值之间的误差值, 即 $L(w_i^{k-1})=\frac{1}{m}\sum_{j=1}^{m} L(f(w_i^{k-1},x_j),y_j)$. 常见的损失函数计算方法可参见文献 [12].

4) https://www.hyperledger.org/use/fabric.
5) https://www.multichain.com/.

一般地, 通过随机梯度下降 (stochastic gradient descent, SGD) 算法 [52] 完成局部模型更新. 为了提高联邦学习中模型训练效率, 通常采用小批量数据样本 $B_i \in D_i$ 计算模型梯度值, 即

$$w_i^k = w_i^{k-1} - \eta_i \nabla g(w_i^{k-1}; B_i), \tag{2}$$

其中 $\nabla g(w_i^{k-1}; B_i) = \frac{1}{|B_i|}\sum_{j=1}^{|B_i|}\frac{\partial L(f(w_i^{k-1}, x_j), y_j)}{\partial w_i^{k-1}}$, η_i 为 p_i 的学习速率.

经过 t 轮迭代后, p_i 将迭代更新的局部模型 w_i^t 发送给参数服务器.

(3) 全局模型聚合. 参数服务器收集所有参与者返回的局部模型之后, 进行安全聚合生成新的全局模型 w_G^t, 并返回给参与者集合 P 进行新一轮迭代. 当前研究者提出了多种安全聚合算法 [53], 其中最常见是 Google 提出的联邦平均算法 FedAvg [1], 其是一种基于局部 SGD 算法平均更新的方法, 即 $w_G^t = \frac{1}{\sum_{i=1}^N |B_i|}\sum_{i=1}^N |B_i| w_i^t$. 参数服务器可计算经过 t 轮迭代后全局模型损失函数:

$$L(w_G^t) = \frac{1}{N}\sum_{i=1}^{N} L(w_i^t) = \frac{1}{Nm}\sum_{i=1}^{N}\sum_{j=1}^{m} L(f(w_i^t, x_j), y_j). \tag{3}$$

重复过程 (2) 和 (3) 直到联邦学习全局模型损失函数收敛或者达到满意准确度.

3.3 差分隐私

差分隐私最早由 Dwork 在 2006 年提出, 主要解决数据库隐私泄露问题, 其核心思想是通过给数据库中数据记录添加扰动噪声, 保证数据库中添加或删除一条数据记录不会影响输出计算结果, 从而使得攻击者难以通过观察计算结果推断出原始数据记录信息 [30]. 相比于匿名化技术, 差分隐私不需要考虑攻击者背景知识并且建立在严格数学理论基础之上, 能有效量化隐私保护程度. 此外, 对比密码技术, 差分隐私计算复杂度较低, 但其需要平衡隐私保护和数据效用关系. 这里给出差分隐私的形式化定义及其实现方式.

定义1 (差分隐私 [29, 30]) 给定任意一对仅相差一条数据记录的相邻数据集 D_1, D_2. 若随机算法 M 对其输出的所有集合中任意子集 O 满足:

$$\Pr[M(D_1) \in O] \leqslant \exp(\varepsilon) \cdot \Pr[M(D_2) \in O], \tag{4}$$

则称算法 M 满足 ε- 差分隐私, 其中 ε 为隐私预算, 其控制了 M 分别在 D_1, D_2 上输出相同计算结果的概率比值. 显然, ε 越小, 则表示隐私保护程度越高. 若 $\varepsilon = 0$, 隐私保护程度达到最高, 即表示 M 在 D_1, D_2 输出相同计算结果的概率相同, 也就是说计算结果不反映任何原始数据集信息.

给查询函数 q 的返回值添加噪声是实现差分隐私的主要手段. 常用的添加噪声方法有拉普拉斯机制 [54] 和指数机制 [55], 其中拉普拉斯机制适用于输出结果为数值型的数据扰动, 而指数机制常被应用于输出结果为非数值型的数据扰动. 不同机制满足差分隐私需要添加的噪声量大小受全局敏感度影响, 全局敏感度是指删除一条数据记录对查询结果产生的最大影响.

定义2 (全局敏感度 [29, 30]) 给定查询函数 $q: D \to R^d$, 其中 D 为输入数据集, R^d 为查询返回的 d 维实数向量. 对于任意一对仅相差一条数据记录的相邻数据集 D_1, D_2, 查询函数 q 的全局敏感度定义为

$$\Delta q = \max_{D_1, D_2} ||q(D_1) - q(D_2)||_l, \tag{5}$$

其中 l 表示度量距离的向量范数, 通常采用 1- 阶范数距离.

定义3 (拉普拉斯机制[54]) 给定查询函数 $q: D \to R^d$, q 的全局敏感度为 Δq. 若随机算法 M 的输出结果满足

$$M(D) = q(D) + \left\langle \mathrm{Lap}\left(\frac{\Delta q}{\varepsilon}\right)\right\rangle^d, \tag{6}$$

则随机算法 M 满足 ε- 差分隐私. 其中 $\langle \mathrm{Lap}(\frac{\Delta q}{\varepsilon})\rangle^d$ 为 d 维随机变量, 其服从参数为 $\frac{\Delta q}{\varepsilon}$ 的拉普拉斯分布.

定义4 (指数机制[55]) 给定可用性函数 $u: (D, Q) \to R$, 其中 D 为输入数据集, Q 为查询函数 q 的非数值型输出结果集. 对于 Q 中任一实体对象 s ($s \in Q$), 其可用性函数 $u: (D, s)$ 的全局敏感度为 Δu. 若随机算法 M 以正比例于 $\exp(\frac{\varepsilon q(D,s)}{2\Delta u})$ 的概率输出 s, 即 $M(D, q) = \{s: \Pr[s \in Q] \propto \exp(\frac{\varepsilon q(D,s)}{2\Delta u})\}$, 则随机算法 M 满足 ε- 差分隐私.

4 系统设计

本节介绍了基于区块链的隐私保护异步联邦学习系统架构并给出总体设计目标.

4.1 系统架构

不同于传统集中式机器学习将各参与方数据聚合到中心服务器进行全局模型训练, 联邦学习在保证各参与方训练数据不出本地的情况下协同训练全局模型, 从而有效保护数据隐私. 在分析现有联邦学习不足基础上, 本文提出了一种基于区块链的隐私保护异步联邦学习, 在保证联邦学习可信性和隐私性基础上, 提高联邦学习效率. 如图 1 所示, 本文提出的系统架构包括任务发布者、参与者、共识委员会和区块链等. 为了参与联邦学习, 任务发布者、参与者等实体都需要事先在区块链上注册获得各自公私钥对. 公钥用来生成标识实体的交易地址, 私钥用来签名交易数据确保交易的完整性和不可否认性.

(1) 任务发布者. 数据孤岛化和碎片化使得任务发布者难以通过本地有限的数字资源训练获得准确性高的机器学习模型. 为了保证机器学习模型的准确性和可信性, 任务发布者一般以任务外包形式将面向不同场景需求的联邦学习任务发布到区块链上. 对于每个具体的联邦学习, 外包学习任务中规定了本次协作训练目标、所需训练数据类型与格式、联邦学习初始化模型及其超参数等内容. 为了防止任务发布者作恶, 其需要在区块链上预付一定的押金, 用来激励参与者参与联邦学习任务. 经过若干轮迭代之后, 当任务发布者获得最终全局模型后, 其预付押金将按照事先制定的奖励规则分别支付给提供有效局部模型的诚实参与者以及参与共识过程的节点.

(2) 参与者. 为了获得发布到区块链上联邦学习任务的报酬奖励, 参与者从区块链上下载初始化联邦学习全局模型, 并基于所拥有的本地数据集独立进行局部模型更新训练. 每个参与者在符合要求情况下可根据能力和兴趣参与多个联邦学习任务. 为了抵御攻击者通过局部模型更新参数逆向推断参与者数据隐私, 本文提出发送差分隐私扰动的局部模型到区块链, 具体过程将在 5.1 小节中介绍. 由于每个参与者拥有训练数据量大小和计算能力不同, 训练局部模型所需时间存在差异性. 现有同步联邦学习需要收集所有训练得到的局部模型才进行全局模型更新, 使得每轮迭代时间依赖于局部模型训练最慢的参与者, 从而导致训练时间开销大、计算资源浪费等问题. 本文提出的异步联邦学习能较好解决该问题, 在每轮迭代过程中, 当某个参与者将完成的隐私保护局部模型发送到区块链后, 共识委员会对局部模型的完整性和有效性进行共识验证. 一旦验证通过随即进行异步全局模型更新而不用等待收集来自其他参与者的局部模型更新.

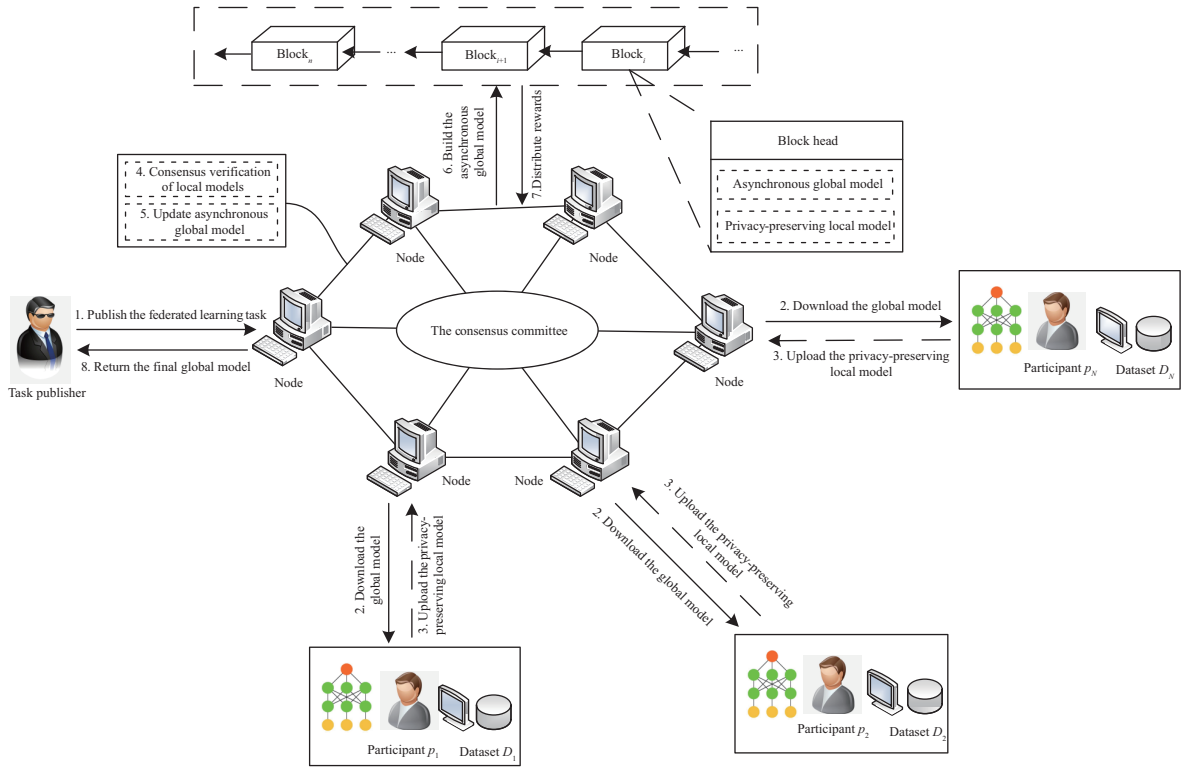

图 1　(网络版彩图) 基于区块链的隐私保护异步联邦学习系统架构

Figure 1　(Color online) Privacy-preserving asynchronous federated learning system architecture based on blockchain

(3) 共识委员会. 节点按照一定规则组建的共识委员会, 替代所有节点参与共识过程, 从而提高联邦学习迭代训练效率. 每个符合规则的合法参与者均可加入共识委员会. 本文所采用具体规则是利用 DPoS 共识算法 [56] 的节点选举策略, 即每个节点通过各自所持有的权益值投票选择票数多且愿意参与共识的前若干个代理节点组成共识委员会. 为了抵御部分代理节点作恶, 共识委员会采用 PBFT 共识算法 [51] 验证参与者异步提交的局部模型的完整性和有效性. 更多关于共识过程细节将在第 5.3 小节中介绍.

(4) 区块链. 在每轮迭代过程中, 区块体用以存储执行联邦学习任务产生的交易数据, 主要包括异步全局模型和隐私保护局部模型. 区块头用以存储上一个区块哈希值形成链式结构, 以及 Merkle 根哈希以确保交易数据存在性和完整性. 任务发布者可访问并审计区块链上存储的联邦学习异步全局模型, 若全局模型损失函数收敛或者达到满意准确度, 则可以停止迭代并将最终全局模型返回给任务发布者; 否则, 继续进行下一轮迭代过程.

4.2　设计目标

围绕联邦学习的系统架构, 本文的设计目标如下:

(1) 保证联邦学习的可信性. 现有联邦学习依赖于参数服务器, 全局模型可信性本质上内生性地受制于对参数服务器的可信性. 利用区块链构建不依赖于可信第三方的联邦学习系统架构, 保证全局模型的可信性, 确保更新过程可追溯、结果可审计和不可篡改等.

(2) 平衡数据隐私和模型效用. 联邦学习本身可保证参与者数据不出本地即可完成协同模型训

练. 参与者之间是相互独立且互相不信任的, 但他们可通过联邦学习过程中交互的参数发起成员推理攻击, 获得参与者数据隐私信息 [22~24]. 现有研究通过差分隐私扰动训练参数保护数据隐私, 但容易降低模型效用. 本文所考虑的联邦学习应在保证训练模型隐私性, 同时提高模型效用.

(3) 保证训练模型的可靠性. 本文考虑联邦学习的可靠性, 主要包括: (i) 参与者训练局部模型的可靠性. 参与者因本地训练数据质量和数量的不同导致训练局部模型质量参差不齐, 进而影响全局模型的可靠性. 在异步联邦学习中, 应通过优化调整不同质量的局部模型权重以提高全局模型的可靠性. (ii) 共识委员会共识过程的可靠性. 共识委员会中节点存在不响应或丢弃消息、发送错误消息甚至共谋等恶意行为, 应保证训练得到的局部模型在容忍一定数量节点作恶情况下能被准确地配置到全局模型.

(4) 提高训练过程的高效性. 同步联邦学习需要收到所有参与者发送的局部模型才进行全局模型更新, 存在训练时间开销大、计算资源浪费等问题. 应设计异步联邦学习在保证训练模型质量和可信性基础上, 提高训练过程的效率.

5 基于区块链的隐私保护异步联邦学习

本节详细介绍了基于区块链的隐私保护异步联邦学习方案的具体步骤, 主要包括差分隐私局部模型更新和双因子异步全局模型更新两部分.

5.1 差分隐私局部模型更新

在联邦学习中, 各参与方通过共享局部模型更新而非原始数据生成全局模型. 然而由于局部模型参数会反映训练数据的特征信息, 直接共享局部模型会导致数据隐私的间接泄露 [22~24]. 为此, 本文采用差分隐私机制扰动局部模型参数, 保障参与者数据隐私. 考虑到模型效用与数据隐私之间的平衡问题, 本文根据不同维度梯度值对训练的局部模型贡献程度不同, 为其提供不同的隐私保护水平. 算法 1 描述了基于差分隐私的局部模型训练过程. 总体而言, 各参与方执行本地训练任务可分为两个阶段: 局部模型更新和局部模型扰动.

(1) 局部模型更新. 在本文所提出的异步联邦学习中, 参与者集合 $P=\bigcup_{i=1}^{N} p_i$ 不再等待收集所有参与者发送的局部模型才进行全局模型更新, 而是收到经过共识的有效局部模型即进行全局模型更新. 在每轮全局模型迭代过程中, 联邦学习的参与者首先下载上一轮生成的异步全局模型并用其初始化本轮迭代的局部模型, 其中首轮迭代下载的是任务发布者发布到链上的初始化全局模型 w_G^0. 然后每个参与者执行 SGD 算法进行局部模型更新. 具体地, 在第 k 轮局部模型迭代过程中, p_i 计算在样本数据 (x_j, y_j) 上的损失函数 $L(f(w_i^{k-1}, x_j), y_j)$, 并计算局部模型梯度值 $\nabla g(w_i^{k-1}; D_i)$. 为了提高局部模型训练效率, 这里同样采用小批量数据样本集合计算局部模型梯度 [1], 即

$$\nabla g(w_i^{k-1}; B_i) = \frac{1}{|B_i|} \sum_{j=1}^{|B_i|} \frac{\partial L(f(w_i^{k-1}, x_j), y_j)}{\partial w_i^{k-1}}. \tag{7}$$

之后, p_i 利用局部模型梯度更新局部模型, 即

$$w_i^k = w_i^{k-1} - \eta_i \nabla g(w_i^{k-1}; B_i), \tag{8}$$

其中 η_i 为 p_i 的学习速率. 为了简化模型, 大多数情况下不区分所有参与者的学习速率, 认为它们都是一样的.

Algorithm 1 Differential private local model updating

Input: $P=\bigcup_{i=1}^{N} p_i$, $D=\bigcup_{i=1}^{N} D_i$, $B=\bigcup_{i=1}^{N} B_i, B_i \in D_i$, t, $\eta=\bigcup_{i=1}^{N} \eta_i$, $\varepsilon=\varepsilon_1+\varepsilon_2+\varepsilon_3$ $(\varepsilon_2<\varepsilon_3)$;
Output: $\hat{w}_i^t$;

Download initial global model w_G^0 from blockchain;
for $p_i \in P$ **do**
  Initialize the local model $w_i^0 \leftarrow w_G^0$;
  //Update local model;
  for $k=1$ to $t-1$ **do**
    Compute $L(f(w_i^{k-1}, x_j), y_j)$ with (x_j, y_j);
    Compute local model gradient $\nabla g(w_i^{k-1}; B_i)=\frac{1}{|B_i|}\sum_{j=1}^{|B_i|}\frac{\partial L(f(w_i^{k-1}, x_j), y_j)}{\partial w_i^{k-1}}$;
    Update local model $w_i^k=w_i^{k-1}-\eta_i \nabla g(w_i^{k-1}; B_i)$;
  end for
  //Perturb local model;
  Compute the t-th local model gradient $\nabla g(w_i^{t-1}; B_i)$ with B_i as $\nabla g(w_i^{t-1}; B_i)=\frac{1}{|B_i|}\sum_{j=1}^{|B_i|}\frac{\partial L(f(w_i^{t-1}, x_j), y_j)}{\partial w_i^{t-1}}$;
  Sample r model gradients using exponential mechanism with $\Pr[\nabla g_l \in \nabla g(w_i^{t-1}; B_i)] \propto \exp(\frac{\varepsilon_1 u(\nabla g_l, B_i)}{2r\Delta u})$;
  //Add noises to the sampled r model gradients using Laplace mechanism with privacy budget ε_2;
  for $l=1$ to r **do**
    $\nabla \hat{g}_l(w_i^{t-1}; B_i) \leftarrow \nabla g_l(w_i^{t-1}; B_i)+\mathrm{Lap}_l(\frac{\Delta q}{\varepsilon_2})$;
  end for
  //Add noises to the remaining $n-r$ model gradients using Laplace mechanism with privacy budget ε_3;
  for $l=r+1$ to n **do**
    $\nabla \hat{g}_l(w_i^{t-1}; B_i) \leftarrow \nabla g_l(w_i^{t-1}; B_i)+\mathrm{Lap}_l(\frac{\Delta q}{\varepsilon_3})$;
  end for
  $\nabla \hat{g}(w_i^{t-1}; B_i) \leftarrow \langle \nabla \hat{g}_l(w_i^{t-1}; B_i)\rangle_{l=1}^{n}$;
  $\hat{w}_i^t=w_i^{t-1}-\eta_i \nabla \hat{g}(w_i^{t-1}; B_i)$;
end for
return $\hat{w}_i^t$;

(2) 局部模型扰动. 为了抵御局部模型梯度值逆向推理带来的数据隐私问题, 本文利用差分隐私扰动上链的局部模型梯度值. 考虑到不同维度梯度值对局部模型贡献程度的差异性, 本文提出基于差分隐私机制的差异化局部模型扰动方法, 实现数据隐私和模型效用有效平衡. 通过给较高贡献度的梯度值分配较小隐私预算以添加较大噪声保证数据隐私, 给贡献度较低的梯度值分配较大隐私预算以添加较小的噪声, 从而提高模型效用. 然而现有研究指出梯度值选择过程和选择的梯度值均会带来隐私泄露 [31,57]. 为此, 本文通过隐私梯度采样和模型梯度扰动实现局部模型隐私保护, 同时最大化模型效用.

(i) 隐私梯度采样. 为了解决梯度值选择过程带来的隐私泄露问题, 本文采用指数机制实现对较高贡献度的梯度值的隐私采样. 在第 t 轮迭代过程中, p_i 利用小批量数据样本 B_i 计算局部模型梯度 $\nabla g(w_i^{t-1}; B_i)$. 为了度量不同梯度值的贡献度, 本文定义可用性函数 u 为 p_i 不同维度梯度的绝对值大小 [57], 即对于维度为 n 中的任意梯度值 $\nabla g_j(w_i^{t-1}; B_i)$, 其可用性函数为

$$u(\nabla g_j(w_i^{t-1}; B_i), B_i)=|\nabla g_j(w_i^{t-1}; B_i)|, \quad j=1,2,\ldots,n, \tag{9}$$

然后利用指数机制对 $\nabla g(w_i^{t-1}; B_i)$ 以分配的总隐私预算 ε_1 共采样 r 个模型梯度值, 即

$$\Pr[\nabla g_l \in \nabla g(w_i^{t-1}; B_i)] \propto \exp\left(\frac{\varepsilon_1 u(\nabla g_l, B_i)}{2r\Delta u}\right), \quad l=1,2,\ldots,r. \tag{10}$$

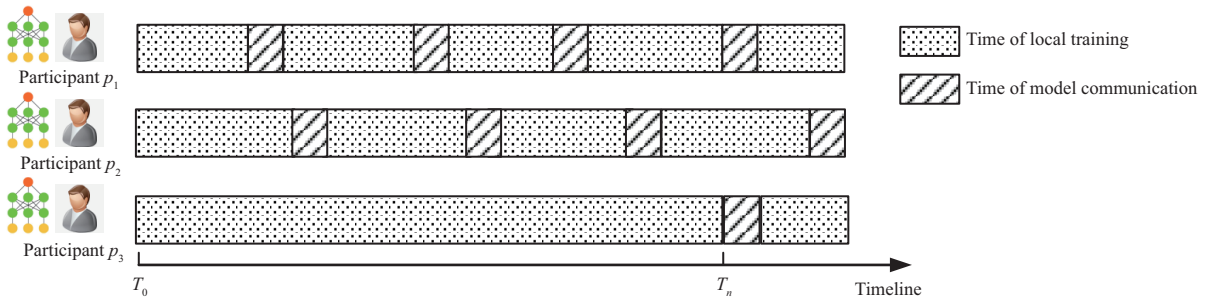

图 2 (网络版彩图) 异步联邦学习训练过程

Figure 2 (Color online) The training process of asynchronous federated learning

可见, 若局部模型某个梯度的可用性函数值越大, 即说明其对全局模型的贡献度越大, 则该梯度被选择的概率就越大; 反之被选择的概率就越小.

(ii) 模型梯度扰动. 为了保护所选择梯度值并且最大化模型效用, 在隐私梯度采样基础上利用拉普拉斯机制差异化扰动模型梯度值. 对于隐私采样得到贡献度较大的 r 个梯度值加隐私预算为 ε_2 的噪声数据, 对于剩余的 $n-r$ 个模型梯度值加隐私预算为 ε_3 的噪声数据, 即

$$\nabla \hat{g}_l(w_i^{t-1}; B_i) = \nabla g_l(w_i^{t-1}; B_i) + \mathrm{Lap}_l\left(\frac{\Delta q}{\varepsilon_m}\right), \tag{11}$$

其中, 当 $l = 1, 2, \ldots, r$ 时, $m = 2$; 当 $l = r+1, r+2, \ldots, n$ 时, $m = 3$. $\mathrm{Lap}_l(\frac{\Delta q}{\varepsilon_m})$ 是服从参数为 $\frac{\Delta q}{\varepsilon_m}$ 的拉普拉斯分布的噪声. 显然 $\varepsilon_2 < \varepsilon_3$, 最后生成扰动后的梯度 $\nabla \hat{g}(w_i^{t-1}; B_i)$. 然后, p_i 计算 t 轮迭代之后生成差分隐私扰动的局部模型 $\hat{w}_i^t = w_i^{t-1} - \eta_i \nabla \hat{g}(w_i^{t-1}; B_i)$.

5.2 双因子异步全局模型更新

在本文提出的基于区块链的异步联邦学习中, 各参与方并行执行局部模型更新训练和全局模型的更新操作以缓解同步联邦学习通信效率低、计算资源浪费等问题. 然而, 由于各参与方所拥有训练数据量大小与计算资源的不同, 因此同一时刻各参与方局部模型训练状态和局部模型质量都有所差异. 如图 2 所示, 在 T_n 时刻, 全局模型已基于参与者 p_1 和 p_2 的多轮迭代训练的局部模型完成了多轮更新, 而参与者 p_3 提供的基于 T_0 时刻的局部模型更新则会在一定程度上损害全局模型的质量.

为解决异步联邦学习中时钟不同步问题和低质量局部模型对全局模型可用性的影响, 本文在异步更新全局模型的过程中引入双因子调整机制, 通过定义时间权重和质量权重以降低不可靠局部模型的权重值. 算法 2 描述了基于区块链的双因子异步全局模型更新过程, 其中具体的共识过程将在 5.3 小节中进行介绍.

(1) 时间权重. 在异步联邦学习中, 参与者拥有本地数据集大小、计算资源以及通信带宽等不同, 从而使得全局模型更新并不同步. 显然, 异步联邦学习中局部模型新鲜性对全局模型效用的影响会随时间增加而降低. 因此, 为了降低较长训练时间的局部模型更新对全局模型效用的影响, 本文定义时间权重函数为

$$S_t(w_i^t, T_i) = \exp(-\alpha \cdot T_i), \tag{12}$$

其中 T_i 表示 p_i 训练生成 $\hat{w}_i^t$ 所花费时间, α ($\alpha > 0$) 为时间参数.

与现有工作类似 [16, 19], 为了抵御恶意参与者伪造 $\hat{w}_i^t$ 的训练时间 T_i, 即未完成甚至没有在本地数据集上进行训练便提交 $\hat{w}_i^t$ 以影响全局模型效用, 本文采用 Intel 的 SGX (software guard extensions)

技术 [58] 保证局部模型 $\hat{w}_i^t$ 训练时间的真实性和可信性, 其中本地训练时间与训练数据集的大小成正比.

(2) 质量权重. 参与者 p_i 将训练生成 $\hat{w}_i^t$ 以交易形式发送到区块链, 所有参与者利用各自本地数据集评估 $\hat{w}_i^t$ 质量权重. 例如, p_j 利用本地数据集 D_j 训练 $\hat{w}_i^t$ 得到预测模型值 $f(\hat{w}_i^t, x_k)$, 并计算与实际标签值 y_k 之间的偏差值以评估 $\hat{w}_i^t$ 质量. Zhao 等 [59] 研究发现预测模型值理论上可无限偏离实际标签值, 但实际上不会超过实际标签值的 3 倍, 通常 $0 \leqslant |\frac{f(\hat{w}_i^t, x_k) - y_k}{y_k}| \leqslant 1$. 基于此, 本文定义 p_j 评估 $\hat{w}_i^t$ 的质量分数为

$$\mathrm{Score}_j(\hat{w}_i^t) = \frac{1}{m} \sum_{(x_k, y_k) \in D_j} \left(1 - \left|\frac{f(\hat{w}_i^t, x_k) - y_k}{y_k}\right|\right), \quad j = 1, 2, \ldots, N. \tag{13}$$

可见, 若预测模型值与实际标签值偏差较大, 则说明经过差分隐私扰动后的模型效用较差, 从而得到质量分数较低. 反之则说明差分隐私扰动后的模型效用较好, 从而得到质量分数也将较高. 为了降低低质量 $\hat{w}_i^t$ 对全局模型影响, 甚至抵御恶意参与者发送篡改或伪造局部模型发起的局部模型投毒攻击 [60], 由部分区块链节点组建的共识委员会需要对 $\hat{w}_i^t$ 进行共识验证, 以确保 $\hat{w}_i^t$ 的真实性和可信性. 具体共识验证过程将在 5.3 小节中进行介绍.

然后, 将通过共识验证 $\hat{w}_i^t$ 的质量分数 $\mathrm{Score}_j(\hat{w}_i^t)$ 以交易形式发送到区块链, 从而所有参与者可计算得到 $\hat{w}_i^t$ 的质量权重为

$$S_q(\hat{w}_i^t) = \frac{1}{N} \sum_{j=1}^{N} \mathrm{Score}_j(\hat{w}_i^t). \tag{14}$$

综合考虑本文定义的时间权重和质量权重, 计算在全局模型更新中的权重值为

$$S(\hat{w}_i^t) = \beta S_t(\hat{w}_i^t, T_i) + (1 - \beta) S_q(\hat{w}_i^t), \tag{15}$$

其中, β $(0 < \beta < 1)$ 为调节因子, 用以平衡 $\hat{w}_i^t$ 的时间权重和质量权重之间的关系.

因此, 该轮异步联邦学习在定义时间段内收到 K $(1 \leqslant K \leqslant N)$ 个经过 t 轮迭代更新并且通过共识验证的 $\hat{w}_i^t$ 之后即可进行全局模型更新:

$$w_G^t = \frac{1}{K} \sum_{i=1}^{K} S_i(\hat{w}_i^t) \cdot \hat{w}_i^t, \quad 1 \leqslant K \leqslant N. \tag{16}$$

5.3 共识过程

为了提高联邦学习迭代训练效率, 从所有参与者中按照一定规则挑选若干个参与者组建共识委员会, 由其负责对差分隐私局部模型和全局模型进行有效性验证. 本文结合 DPoS [56] 和 PBFT [51] 实现异步联邦学习共识算法, 其中 DPoS 主要用来遴选参与者组建高可靠的共识委员会, PBFT 用来验证局部模型有效性以及区块生成过程. 具体而言, 本文的共识过程包括如下模块.

(1) 共识委员会组建. 本文利用 DPoS 共识算法 [56] 的节点选举策略构建高可靠的共识委员会. 每个节点通过各自所持有的权益值投票选择票数多且愿意参与共识的前若干个代理节点组成共识委员会. 共识委员会将履行职责, 负责在分布式的互不信任的联邦学习环境下完成全局模型的构建, 确保全局模型的可信性和可审计性.

(2) 主节点选择. 主节点负责打包候选区块并存储到区块链中以实现可信的协作训练过程. 成功完成区块上链操作的诚实主节点会从任务发布者那里获得相应的报酬奖励. 因此, 为促进联邦学习

Algorithm 2 Blockchain-based two-factor asynchronous global model updating

Input: $P=\bigcup_{i=1}^{N} p_i$, $D=\bigcup_{i=1}^{N} D_i$, $\hat{w}_i^t$, α, β;
Output: $\hat{w}_G^t$;
Verify $\hat{w}_i^t$ by invoking consensus process;
if Verify($\hat{w}_i^t$) is true **then**
  for each $p_i \in P$ **do**
    Compute and broadcast $\text{Score}_i(\hat{w}_i^t)$;
    Compute $S_t(w_i^t, T_i)=\exp(-\alpha \cdot T_i)$;
    Compute $S_q(\hat{w}_i^t)=\frac{1}{N}\sum_{i=1}^{N}\text{Score}_i(\hat{w}_i^t)$;
    Compute $S(\hat{w}_i^t)=\beta S_t(\hat{w}_i^t, T_i)+(1-\beta)S_q(\hat{w}_i^t)$;
    Update asynchronous global model $w_G^t=\frac{1}{K}\sum_{i=1}^{K} S_i(\hat{w}_i^t)\cdot\hat{w}_i^t, 1\leqslant K\leqslant N$;
  end for
end if
Verify w_G^t by invoking consensus process;
if Verify(w_G^t) is true **then**
  return $\hat{w}_G^t$;
end if

的持续发展, 激励更多持有高质量数据样本的参与者加入, 本文将最近一轮全局模型更新中节点持有的 $S(\hat{w}_i^t)$ 作为遴选主节点的依据. 其中, 共识委员会组中持有 $S(\hat{w}_i^t)$ 最高的节点被选作主节点以完成区块的打包工作.

(3) 打包区块. 主节点将收集本轮异步全局模型训练过程中产生的合法但未被确认的交易到候选区块 $\text{Block}=(\text{header}, \langle Tx_{\hat{w}_i}^{(e)}\rangle, Tx_{wG}^{(e)}), i\in[1,2,\ldots,N]$ 中, 其中, header 表示区块头, 包含时间戳、前一个区块哈希值等字段. $\langle Tx_{\hat{w}_i}^{(e)}\rangle$ 表示第 e 轮异步全局模型更新中产生的经共识的局部模型交易, 该交易中包含 p_i 训练的差分隐私局部模型 $\hat{w}_i$, 本地训练时间 T_i, 模型质量分数 $\langle\text{Score}_j(\hat{w}_i)\rangle, j\in[1,2,\ldots,N]$ 与权重值 $S(\hat{w}_i)$. $Tx_{wG}^{(e)}$ 表示第 e 轮更新的异步全局模型. 主节点对打包好的 Block 进行数字签名并广播, 进入区块验证阶段.

(4) 区块验证. 共识委员会组通过执行 PBFT 算法 [51] 验证模型有效性及区块生成过程. 具体地, 主节点对交易进行排序并将打包好的区块 Block 广播给共识委员会成员进行区块验证. 基于接收到的 Block, 共识委员会将验证区块签名的正确性、交易格式的合法性、局部模型的有效性、全局模型更新的正确性等. 特别地, 若差分隐私局部模型 $\hat{w}_i$ 的质量分数 $S(\hat{w}_i)$ 在预先规定的有效取值范围内, 则 $\hat{w}_i$ 通过验证并用于全局模型的更新操作中.

(5) 区块上链. 主节点将通过验证的合法 Block 链接到区块链的尾部, 完成本轮异步全局模型更新训练过程. 相应地, 参与共识的节点可从任务发布者那里获得与自身贡献成正比的奖励, 这将推动联邦学习的可持续发展.

6 安全性分析

本节将从隐私性、可信性和可用性这 3 个方面对所提方案进行安全性分析.

(1) 隐私性. 异步联邦学习允许各参与方在不交换本地训练数据的前提下, 通过共享模型参数信息协作共建全局模型, 因此各参与方的原始数据信息得到保护. 然而在联邦学习过程中敌手可以通过发起模型反演攻击或成员推理攻击等攻击手段造成数据隐私的间接泄露. 本文引入差分隐私技术实现安全异步联邦学习, 通过采用指数机制与拉普拉斯机制实现在保障梯度值选择过程和所选梯度值隐私

安全的情况下均衡数据隐私与模型效用, 构建安全异步协作训练过程. 由差分隐私的定义和序列组合性可知, 由于每个模型梯度值采样过程满足 ε_1/r- 差分隐私, 则采样 r 个模型梯度值满足 ε_1- 差分隐私. 此外, 拉普拉斯机制对采样的 r 个模型梯度值和剩余 $n-r$ 个模型梯度值的扰动分别满足 ε_2- 差分隐私和 ε_3- 差分隐私. 由于算法作用于同一小批量训练数据样本 B_i 上, 则由差分隐私的序列组合性可知, 参与者 p_i 在每轮局部模型训练过程中满足 ε_i- 差分隐私, 其中 $\varepsilon_i=\varepsilon_1+\varepsilon_2+\varepsilon_3$. 此外, 各参与方基于算法 1 完成经隐私保护的局部模型训练, 并基于此更新异步全局模型. 显然各参与方用于训练局部模型的小批量数据样本 B_i 互不相交, 即没有相同的数据样本. 根据差分隐私的并行组合性可知, 每轮全局模型的更新训练满足 $\max\{\varepsilon_i\}$- 差分隐私, 其中 $i=1,2,\ldots,N$, 因此本文所提方案能为各参与方提供数据隐私保护.

(2) 可信性. 在传统异步联邦学习中, 参数服务器占据协作训练的主导地位, 负责接收各参与方的局部模型更新参数并异步执行全局模型更新操作. 然而传统异步联邦学习所采用的这种中心化协作训练架构容易使协作训练过程遭受单点失效、数据隐私泄露、模型不可信等关键性问题. 本文提出的基于区块链的隐私保护异步联邦学习能够有效解决传统中心化架构所带来的安全威胁, 实现可信分布式联邦学习. 通过引入区块链技术, 消除传统异步联邦学习对参数服务器的依赖, 允许各参与方存储经隐私保护的局部模型到区块链中而不是上传至参数服务器以完成全局模型更新. 各参与方通过执行共识算法协同完成双因子异步全局模型更新操作并对结果的有效性和完整性进行共识验证. 经过共识的全局模型会以交易的形式上传到区块链中, 参与者可以对结果进行审计, 保障异步联邦学习的可信性.

(3) 可用性. 在基于隐私保护的异步联邦学习中, 影响模型可用性的主要因素有以下两个方面. 一方面, 差分隐私技术牺牲部分模型可用性, 通过在模型参数中添加噪声以防止数据隐私的间接泄露. 另一方面, 由于各参与方持有的数据质量和计算资源存在差异性, 由此产生的时钟不同步等问题会导致低质量局部模型影响全局模型的可用性. 针对上述问题, 本文首先介绍了基于差分隐私的局部模型更新过程. 通过引入指数机制完成对局部模型训练目标具有较高贡献度的梯度值的采样, 并在此基础上利用拉普拉斯机制对模型梯度值进行差异化扰动. 其中, 贡献度高的局部模型梯度值被分配较小的隐私预算值, 即添加较大噪声值以保障数据隐私. 相反, 贡献度低的局部模型梯度值被分配较大的隐私预算值, 即添加较小的噪声值以保障模型可用性. 在此基础上, 为解决异步联邦学习中不可靠局部模型对全局模型可用性的影响, 本文提出一种双因子调整机制以完成异步全局模型的协作更新操作, 通过降低不可靠局部模型的权重值进一步提高全局模型的可用性.

7 实验评估

本节主要在真实数据集上对所提方案进行实验, 通过与相关方案进行比较进一步验证所提方案的有效性.

7.1 实验数据集与实验环境

本文在 MNIST[6)] 数据集上进行测试, 由 60000 个训练数据样本和 10000 个测试数据样本组成. 该数据集中每个数据样本都是一张 28×28 的灰度图像, 显示 0~9 之间的某一手写数字. 为仿真异步联邦学习场景, 本文为每个联邦学习任务参与者添加停顿时间, 即在完成每轮局部模型训练后停顿一段时间间隔 [43]. MNIST 训练数据样本被随机平分为 10 个互不相交的子集, 其中每个参与者持有 6000 个样本作为本地训练数据集. 本文实验结果均为测试 10 次的平均值, 实验所使用的开发工具是 Pycharm

6) Lecun Y, Cortes C. The MNIST database of handwritten digits. http://yann.lecun.com/exdb/mnist/.

表 2 协作训练参数配置

Table 2 Configuration of parameters for collaborative training

η	bs	α	β	epoch
0.01	64	1	0.1	100

2019.3.4, 编程语言为 Python3.6.10, 配备 2.20 GHz Intel(R)Core(TM)i3-8130U 处理器, 8 GB 内存, 操作系统为 Windows 10.

7.2 实验设置

本文采用多层感知机 (multi-layer perception, MLP) 作为训练模型, 通过执行 SGD 算法以完成局部模型训练. MLP 分为输入层、隐藏层和输出层, 每层神经元个数分别设为 784, 100 和 10. 该模型采用线性整流函数 $\mathrm{ReLU}(x)=\max\{0,x\}$ 作为激活函数, 交叉熵损失函数 $L(\mathrm{pr}(x_i),y_i)=-\sum_{c=1}^{C}y_{i,c}\log(\mathrm{pr}_c(x_i))$ 作为损失函数, 其中 C 为分类个数, $\mathrm{pr}_c(x_i)$ 为样本 x_i 属于第 c 类的概率, $y_{i,c}$ 是样本标签的 one-hot 编码值, 即若样本 x_i 属于类别 c, 则 $y_{i,c}=1$, 否则 $y_{i,c}=0$. 在没有特别说明的情况下, 参与者本地训练的学习率 $\eta=0.01$, 小批量训练数据样本大小 $\mathrm{bs}=64$, 超参数 $\alpha=1$, $\beta=0.1$. 此外, 本方案与标准异步随机梯度下降算法 (asynchronous stochastic gradient descent, ASGD) [46] 进行对比实验. ASGD 中参与者基于接收到的全局模型完成局部模型的训练, 并将训练好的模型梯度值用于更新最新的全局模型. 为了描述方便, 表 2 列出了协作训练的参数配置.

7.3 实验结果

图 3 展示了在隐私预算值分别取 2, 4, 8 时全局模型的准确性与损失情况, 并与 ASGD 进行了对比实验. 从实验结果可知, 随着训练次数与隐私预算值的增加, 本方案的准确性不断提升且接近 ASGD. 主要原因一方面是 ASGD 没有考虑任务参与者的数据隐私, 在异步协作训练过程中通过发送原始模型参数完成全局模型的更新, 这会产生数据隐私泄露的风险, 但具有较高的模型质量. 另一方面, 本文在为异步联邦学习提供隐私保护的前提下, 通过执行双因子调整机制进一步提升全局模型的可用性. 此外, 任务参与方执行设计的差分隐私局部模型更新以实现数据隐私与模型效用间的均衡, 这保障了异步联邦学习的隐私性和效用性. 此外, 由于隐私预算值的大小与隐私保护水平成反比, 因此较大的隐私预算值产生的噪声值较小, 但模型的可用性较高. 通过观察模型的收敛情况可以发现, 全局模型在经过 80 轮次迭代训练后达到收敛, 损失值稳定在 0.5 左右, 这表明本文所提出的方案相比较标准异步联邦学习方案具有一定的可比性.

图 4 展示的是当任务参与者人数分别为 3, 6, 9 时, 不同的小批量数据大小和隐私预算值下异步全局模型的效用情况. 其中, 小批量数据大小的取值范围为 $\mathrm{bs}\in\{32,96\}$, 隐私预算的设置分别为 $\varepsilon_1=1$, $\varepsilon_3=2$. 特别地, 对 ε_2 三种不同取值情况分别进行测试评估, 即 $\varepsilon_2=\nu\cdot\varepsilon_3,\nu\in\{0.1,0.25,0.5\}$. 观察图 4 可知, 首先, 全局模型的准确性随着训练次数和任务参与者人数的增加而提升. 例如, 在第 100 轮迭代训练中, 当小批量数据大小 $\mathrm{bs}=32$, $v=0.5$ 时, 3, 6 和 9 个任务参与者异步协作训练的全局模型的平均准确性分别为 91.79%, 91.93% 和 91.98%. 这表明随着任务参与者人数的增加, 用于异步更新全局模型的数据样本变得多样化, 能够有效避免由于模型过拟合所导致无法对新任务提供有效预测结果的情况.

其次, 图 4 实验结果表明, 小批量数据大小取 32 时的模型的准确性明显高于取值为 96 时的模型准确性. 主要原因是由于较小的小批量数据大小会增加任务参与者局部模型迭代训练的次数, 即通过

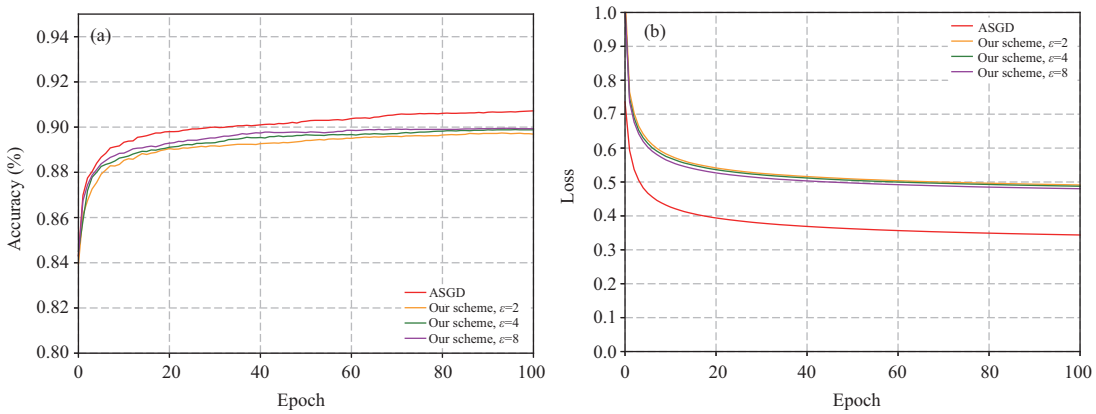

图 3　不同隐私预算对全局模型准确性和损失的影响对比

Figure 3　Comparisons of the impacts under different privacy budgets on (a) model accuracy and (b) model loss

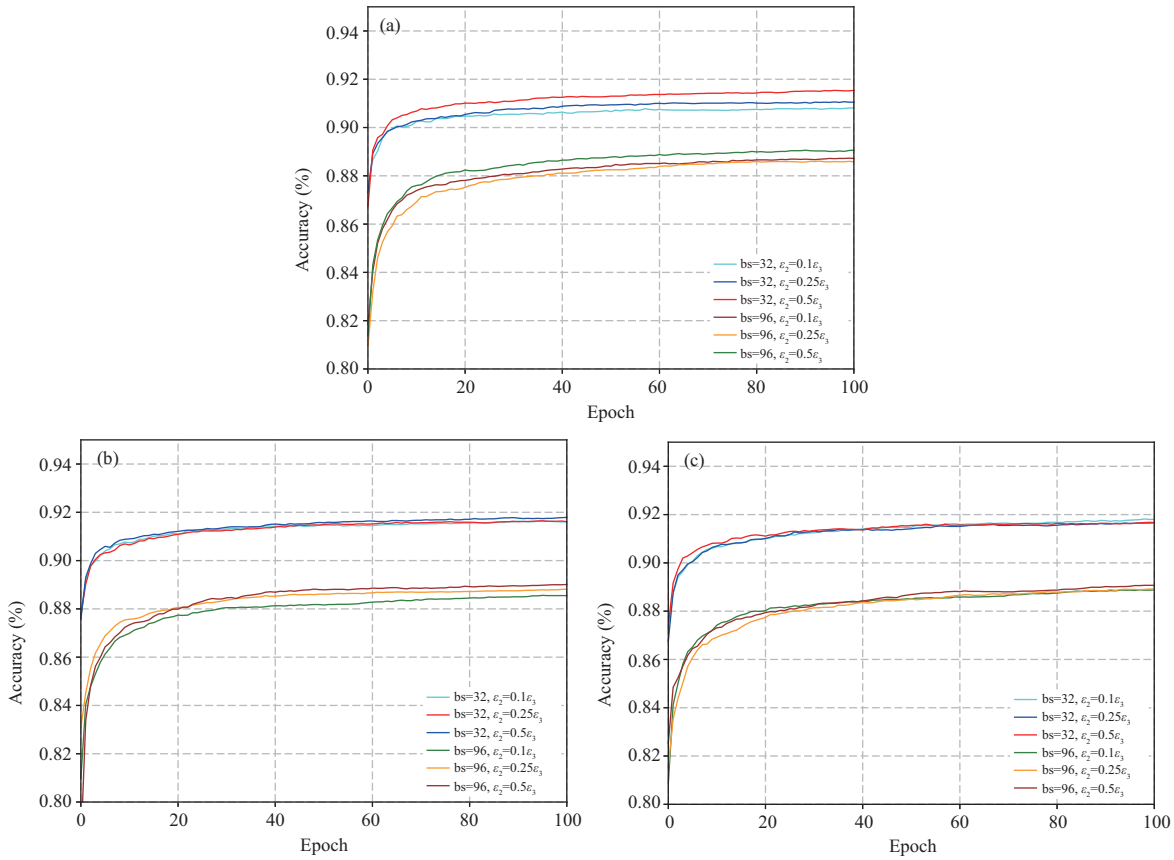

图 4　不同小批量数据大小和隐私预算值依次在 3, 6, 9 个任务参与方场景下对全局模型准确性的影响

Figure 4　The impacts of different mini-batch sizes and privacy budgets on the accuracy of the global model in the scenarios of (a) 3, (b) 6 and (c) 9 participants

增加任务参与者的本地训练的计算量而降低达到全局模型目标准确性的训练次数, 能够有效加快模型的收敛. 最后, 通过对比观察隐私预算值的不同取值情况, 在 ε_1 和 ε_3 取值固定的情况下, 当 ε_2 占 ε_3

表 3 异步联邦学习不同参数下模型损失结果对比

Table 3 Comparisons of the model loss results of asynchronous federated learning under different parameters

$P=3$			$P=6$			$P=9$		
bs	ε_2	Loss	bs	ε_2	Loss	bs	ε_2	Loss
32	$0.1\varepsilon_3$	0.511275	32	$0.1\varepsilon_3$	0.341515	32	$0.1\varepsilon_3$	0.334765
	$0.25\varepsilon_3$	0.510888		$0.25\varepsilon_3$	0.341015		$0.25\varepsilon_3$	0.337472
	$0.5\varepsilon_3$	0.347581		$0.5\varepsilon_3$	0.340100		$0.5\varepsilon_3$	0.335947
96	$0.1\varepsilon_3$	0.550817	96	$0.1\varepsilon_3$	0.55017	96	$0.1\varepsilon_3$	0.542361
	$0.25\varepsilon_3$	0.559172		$0.25\varepsilon_3$	0.54964		$0.25\varepsilon_3$	0.546989
	$0.5\varepsilon_3$	0.546275		$0.5\varepsilon_3$	0.53139		$0.5\varepsilon_3$	0.533502

的比例较大时全局模型的准确性有所提升. 例如在 6 个参与者的训练场景中, 当 ε_2 分别取值为 $0.1\varepsilon_3$ 和 $0.5\varepsilon_3$ 的情况下, bs = 32 时的模型准确性分别为 91.80%, 91.93%. 主要原因是较大的隐私预算值会产生较小的噪声值扰动局部模型, 即为训练数据提供较低的隐私保护水平以保障模型的质量. 相反, 较小的隐私预算提供的隐私保护水平较高, 产生用于扰动局部模型的噪声值较大, 因此模型的质量会有所降低. 然而值得注意的是, 当 ε_2 取不同值时全局模型的准确性不会产生明显的变化, 这表明本方案能够实现良好的模型效用与数据隐私均衡. 此外, 表 3 给出了经过异步迭代更新全局模型 100 次后, 在不同协作训练参数下模型损失结果对比的情况. 表中 P 表示参与者人数, Loss 表示模型损失. 该结果表明本文所提的方案能够在多轮迭代训练后使得损失函数值收敛到一个较小的值, 这表明了本方案具有良好的收敛性.

8 总结

在异步联邦学习中, 如何在有效保障数据隐私安全的前提下实现可信且高质量的全局模型构建是一个关键性问题. 基于此, 本文提出了一种基于区块链的隐私保护异步联邦学习方案, 通过存储更新模型到区块链中以保障可信性. 为权衡数据隐私与模型效用, 利用差分隐私中的指数机制以较高概率选择贡献度高的模型梯度, 并分配较低的隐私预算值以保证局部模型的隐私性. 此外, 在构建全局模型的过程中本文引入了双因子调整机制, 这有利于减少不可靠的局部模型对全局模型质量的影响. 最后, 通过理论分析和系列对比实验证明了本文所提出方案的有效性.

参考文献

1 Mcmahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data. In: Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 2017. 1273–1282

2 Konečný J, Mcmahan H B, Ramage D. Federated optimization: distributed optimization beyond the datacenter. 2015. ArXiv:1511.03575

3 Lin C, He D B, Zeadally S, et al. SecBCS: a secure and privacy-preserving blockchain-based crowdsourcing system. Sci China Inf Sci, 2020, 63: 130102

4 Yang Q, Liu Y, Chen T, et al. Federated machine learning: concept and applications. ACM Trans Intell Syst Technol, 2019, 10: 1–19

5 Konečný J, Mcmahan H B, Yu F X, et al. Federated learning: strategies for improving communication efficiency. 2016. ArXiv:1610.05492

6 Li L, Fan Y X, Tse M, et al. A review of applications in federated learning. Comput Industrial Eng, 2020, 149: 106854

7 Zheng W, Yan L, Gou C, et al. Federated meta-learning for fraudulent credit card detection. In: Proceedings of the 29th International Joint Conference on Artificial Intelligence, 2020. 4654–4660
8 Brisimi T S, Chen R, Mela T, et al. Federated learning of predictive models from federated electronic health records. Int J Med Inf, 2018, 112: 59–67
9 Pokhrel S R, Choi J. Federated learning with blockchain for autonomous vehicles: analysis and design challenges. IEEE Trans Commun, 2020, 68: 4734–4746
10 Niknam S, Dhillon H S, Reed J H. Federated learning for wireless communications: motivation, opportunities, and challenges. IEEE Commun Mag, 2020, 58: 46–51
11 Liu Y, Huang A, Luo Y, et al. FedVision: an online visual object detection platform powered by federated learning. In: Proceedings of the 34th AAAI Conference on Artificial Intelligence, 2020. 13172–13179
12 Lim W Y B, Luong N C, Hoang D T, et al. Federated learning in mobile edge networks: a comprehensive survey. IEEE Commun Surv Tut, 2020, 22: 2031–2063
13 Li T, Sahu A K, Talwalkar A, et al. Federated learning: challenges, methods, and future directions. IEEE Signal Process Mag, 2020, 37: 50–60
14 Yuan Y, Wang F Y. Blockchain and cryptocurrencies: model, techniques, and applications. IEEE Trans Syst Man Cybern Syst, 2018, 48: 1421–1428
15 Dinh T T A, Liu R, Zhang M, et al. Untangling blockchain: a data processing view of blockchain systems. IEEE Trans Knowl Data Eng, 2018, 30: 1366–1385
16 Kim H, Park J, Bennis M, et al. Blockchained on-device federated learning. IEEE Commun Lett, 2020, 24: 1279–1283
17 Ramanan P, Nakayama K. BAFFLE: blockchain based aggregator free federated learning. In: Proceedings of IEEE International Conference on Blockchain, 2020. 72–81
18 Li Y Z, Chen C, Liu N, et al. A blockchain-based decentralized federated learning framework with committee consensus. 2020. ArXiv:2004.00773
19 Kang J, Xiong Z, Niyato D, et al. Reliable federated learning for mobile networks. IEEE Wireless Commun, 2020, 27: 72–80
20 Peng Z, Xu J, Chu X, et al. VFChain: enabling verifiable and auditable federated learning via blockchain systems. IEEE Trans Netw Sci Eng, 2021. doi: 10.1109/TNSE.2021.3050781
21 Qu Y Y, Gao L X, Luan T H, et al. Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet Things J, 2020, 7: 5171–5183
22 Melis L, Song C Z, Cristofaro E D, et al. Exploiting unintended feature leakage in collaborative learning. In: Proceedings of IEEE Symposium on Security and Privacy, 2019. 691–706
23 Orekondy T, Oh S J, Zhang Y, et al. Gradient-leaks: understanding and controlling deanonymization in federated learning. 2018. ArXiv:1805.05838
24 Zhu L G, Liu Z J, Han S. Deep leakage from gradients. In: Proceedings of the 33rd Annual Conference on Neural Information Processing Systems, 2019. 14747–14756
25 Phong L T, Aono Y, Hayashi T, et al. Privacy-preserving deep learning via additively homomorphic encryption. IEEE Trans Inform Forensic Secur, 2018, 13: 1333–1345
26 Ma X, Zhang F G, Chen X F, et al. Privacy preserving multi-party computation delegation for deep learning in cloud computing. Inf Sci, 2018, 459: 103–116
27 Duan J, Zhou J T, Li Y M. Privacy-preserving distributed deep learning based on secret sharing. Inf Sci, 2020, 527: 108–127
28 Feng Q, He D B, Liu Z, et al. SecureNLP: a system for multi-party privacy-preserving natural language processing. IEEE Trans Inform Forensic Secur, 2020, 15: 3709–3721
29 Dwork C, Roth A. The algorithmic foundations of differential privacy. FNT Theor Comput Sci, 2014, 9: 211–407
30 Dwork C. Differential privacy. In: Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, 2006. 1–12
31 Shokri R, Shmatikov V. Privacy-preserving deep learning. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015. 1310–1321
32 Huang X X, Ding Y, Jiang Z L, et al. DP-FL: a novel differentially private federated learning framework for the unbalanced data. World Wide Web, 2020, 23: 2529–2545
33 Wei K, Li J, Ding M, et al. Federated learning with differential privacy: algorithms and performance analysis. IEEE Trans Inform Forensic Secur, 2020, 15: 3454–3469

34 Xie C, Koyejo S, Gupta I. Asynchronous federated optimization. 2019. ArXiv:1903.03934
35 Dijk M V, Nguyen N V, Nguyen T N, et al. Asynchronous federated learning with reduced number of rounds and with differential privacy from less aggregated gaussian noise. 2020. ArXiv:2007.09208
36 Chen Y, Sun X Y, Jin Y C. Communication-efficient federated deep learning with layerwise asynchronous model update and temporally weighted aggregation. IEEE Trans Neural Netw Learn Syst, 2020, 31: 4229–4238
37 Chen X H, Ji J L, Luo C Q, et al. When machine learning meets blockchain: a decentralized, privacy-preserving and secure design. In: Proceedings of IEEE International Conference on Big Data, 2018. 1178–1187
38 Kim H, Kim S H, Hwang J Y, et al. Efficient privacy-preserving machine learning for blockchain network. IEEE Access, 2019, 7: 136481
39 Lu Y L, Huang X H, Dai Y Y, et al. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Trans Ind Inf, 2020, 16: 4177–4186
40 Zhao Y, Zhao J, Jiang L, et al. Privacy-preserving blockchain-based federated learning for IoT devices. IEEE Internet Things J, 2021, 8: 1817–1829
41 Weng J S, Weng J, Zhang J L, et al. DeepChain: auditable and privacy-preserving deep learning with blockchain-based incentive. IEEE Trans Dependable Secure Comput, 2021, 18: 2438–2455
42 Lyu L J, Yu J S, Nandakumar K, et al. Towards fair and privacy-preserving federated deep models. IEEE Trans Parallel Distrib Syst, 2020, 31: 2524–2541
43 Lu X F, Liao Y Y, Lio P, et al. Privacy-preserving asynchronous federated learning mechanism for edge network computing. IEEE Access, 2020, 8: 48970–48981
44 Lu Y L, Huang X H, Dai Y Y, et al. Differentially private asynchronous federated learning for mobile edge computing in urban informatics. IEEE Trans Ind Inf, 2020, 16: 2134–2143
45 Chen X H, Wang X F, Yang K. Asynchronous blockchain-based privacy-preserving training framework for disease diagnosis. In: Proceedings of IEEE International Conference on Big Data, 2019. 5469–5473
46 Zheng S X, Meng Q, Wang T F, et al. Asynchronous stochastic gradient descent with delay compensation. In: Proceedings of the 34th International Conference on Machine Learning, 2017. 4120–4129
47 Lu Y L, Huang X H, Zhang K, et al. Blockchain empowered asynchronous federated learning for secure data sharing in Internet of vehicles. IEEE Trans Veh Technol, 2020, 69: 4298–4311
48 Underwood S. Blockchain beyond bitcoin. Commun ACM, 2016, 59: 15–17
49 Tschorsch F, Scheuermann B. Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun Surv Tut, 2016, 18: 2084–2123
50 Xiao Y, Zhang N, Lou W J, et al. A survey of distributed consensus protocols for blockchain networks. IEEE Commun Surv Tut, 2020, 22: 1432–1465
51 Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proceedings of the 3rd USENIX Symposium on Operating Systems Design and Implementation, 1999. 173–186
52 Zhang T. Solving large scale linear prediction problems using stochastic gradient descent algorithms. In: Proceedings of the 21st International Conference on Machine Learning, 2004
53 Mothukuri V, Parizi R M, Pouriyeh S, et al. A survey on security and privacy of federated learning. Future Generation Comput Syst, 2021, 115: 619–640
54 Dwork C, Mcsherry F, Nissim K, et al. Calibrating noise to sensitivity in private data analysis. J Priv Confidentiality, 2006, 7: 17–51
55 Mcsherry F, Talwar K. Mechanism design via differential privacy. In: Proceeding of the 48th Annual IEEE Symposium on Foundations of Computer Science, 2007. 94–103
56 Larimer D. Delegated Proof-of-Stake (DPOS). Bitshare Whitepaper. 2014
57 Liu R X, Cao Y, Yoshikawa M, et al. FedSel: federated SGD under local differential privacy with top-k dimension selection. In: Proceedings of the 25th International Conference on Database Systems for Advanced Applications, 2020. 485–501
58 Chen L, Xu L, Shah N, et al. On security analysis of proof-of-elapsed-time (PoET). In: Proceedings of the 19th International Symposium on Stabilization, Safety, and Security of Distributed Systems, 2017. 282–297
59 Zhao L C, Wang Q, Zou Q, et al. Privacy-preserving collaborative deep learning with unreliable participants. IEEE Trans Inform Forensic Secur, 2020, 15: 1486–1500
60 Fang M H, Cao X Y, Jia J Y, et al. Local model poisoning attacks to Byzantine-robust federated learning. In: Proceedings of the 29th USENIX Security Symposium, 2020. 1605–1622

A blockchain-based privacy-preserving asynchronous federated learning

Sheng GAO[1*], Liping YUAN[1], Jianming ZHU[1], Xindi MA[2], Rui ZHANG[3] & Jianfeng MA[2]

1. *School of Information, Central University of Finance and Economics, Beijing* 100081, *China*;
2. *School of Cyber Engineering, Xidian University, Xi'an* 710071, *China*;
3. *Institute of Information Engineering, Chinese Academy of Science, Beijing* 100093, *China*
* Corresponding author. E-mail: sgao@cufe.edu.cn

Abstract Federated learning enables the joint training of machine learning models by utilizing distributed data and computing resources while protecting local data privacy. The existing asynchronous federated learning can effectively solve the problems such as waste of computing resources and low training efficiency caused by synchronous learning. However, it aggregates local models from different nodes and updates the global model through the central server, which makes it endogenously subject to the centralized trust mode and suffers from some issues such as single point of failure and privacy leakage. In this paper, we propose a blockchain-based privacy-preserving asynchronous federated learning, which ensures the trustability by storing local models into the blockchain and generating the global model through the consensus algorithm. In order to guarantee the privacy of federated learning and improve the model utility, the exponential mechanism of differential privacy is used to select model gradients with high contribution at high probability, and a lower privacy budget is allocated to ensure the model privacy. In addition, in order to solve the problem of clock desynchronization in asynchronous federated learning, we propose a two-factor adjustment mechanism to further improve the global model utility. Finally, theoretical analysis and experimental results demonstrate that our proposed scheme can effectively guarantee the trustability and privacy of the asynchronous federated learning while improving the model utility.

Keywords federated learning, blockchain, differential privacy, model utility, asynchronous training

Sheng GAO was born in 1987. He received his B.S. degree in information and computation science from Xi'an University of Posts and Telecommunications in 2009, and his Ph.D. degree in computer science and technology from Xidian University in 2014. He is now an associate professor at the School of Information in Central University of Finance and Economics. His current research interests include blockchain, data security, and privacy computing.

Liping YUAN was born in 1996. She received her B.S. degree in computer science and technology from Henan University in 2019. She is now working toward her M.S. degree at Central University of Finance and Economics. Her current research interests focus on the security and privacy issues in machine learning.

Jianming ZHU was born in 1965. He received his M.S. degree in computer application from Taiyuan University of Technology in 1998, and his Ph.D. degree in computer application technology from Xidian University in 2004. He is now a professor at the School of Information in Central University of Finance and Economics. His research interests include wireless network security, data privacy and blockchain.

Xindi MA was born in 1989. He received his B.S. degree in School of Computer Science and Technology from Xidian University, in 2013, and his Ph.D. degree in computer science from Xidian University, in 2018. From September 2019 to September 2020, he worked as a research assistant at the Department of Computer Science in Virginia Polytechnic Institute and State University. He is now a postdoctor at the School of Cyber Engineering in Xidian University. His current research interests include cloud computing security and data privacy in the context of recommender system and machine learning.