基于联邦学习的隐私保护型大数据分析平台设计与实现

王建芳[1]
WANG Jianfang

摘 要 针对跨机构大数据协作中数据隐私泄露与“数据不出域”的核心矛盾，文章构建了一种基于联邦学习的隐私保护型大数据分析平台，采用分布式机器学习架构与同态加密技术实现多方数据协同分析的同时保障“数据不出域”，集成自适应梯度聚合算法与差分隐私机制及安全多方计算协议构建完整的隐私保护计算框架。实验结果表明该平台在保证数据隐私的前提下模型准确率达到集中式学习的 95% 以上，通信开销降低且隐私保护强度提升，该平台为跨机构大数据协作提供了高效可行的技术方案，在金融风控与医疗诊断等领域具有广阔应用前景。

关键词 联邦学习；隐私保护；大数据分析；同态加密；差分隐私

doi：10.3969/j.issn.1672-9528.2025.12.013

0 引言

联邦学习作为一种新兴的分布式机器学习范式，通过“数据不动模型动”的方式在保护数据隐私的前提下实现多方协作建模，根据国家数据局发布的《数据要素 × 三年行动计划（2024—2026 年）》，充分发挥数据要素乘数效应已成为推动高质量发展的必然要求，为解决数据孤岛问题提供了创新思路。

1 平台总体架构设计

1.1 系统架构设计

平台采用四层架构模型，从下至上分别为基础设施层、数据处理层、联邦学习层，以及应用服务层。基础设施层提供分布式计算资源与网络通信能力并支持弹性扩展与负载均衡，数据处理层负责数据的预处理及特征工程与隐私保护处理确保数据质量与安全性，联邦学习层是平台的核心，实现分布式训练与参数聚合及模型管理功能，应用服务层面向最终用户，提供模型部署与预测服务及可视化界面[1]。

模块化设计思路将平台功能分解为相互独立的模块单元，每个模块负责特定的功能领域并通过标准化接口进行交互。训练管理模块负责联邦学习任务的调度与监控，模型管理模块处理模型的版本控制与部署，安全模块提供隐私保护与身份认证服务，通信模块管理节点间的数据传输。同时平台定义了统一的数据格式规范与通信协议标准及 API 接口文档支持多种编程语言与框架的接入，这种标准化设计降低了系统集成的复杂度并提高了平台的可扩展性与互操作性。

1.2 核心组件设计

联邦协调器作为平台的中央控制节点负责全局模型的管理与参数聚合任务，其内部采用分层设计包括任务调度层与聚合计算层及通信管理层，如图 1 所示。

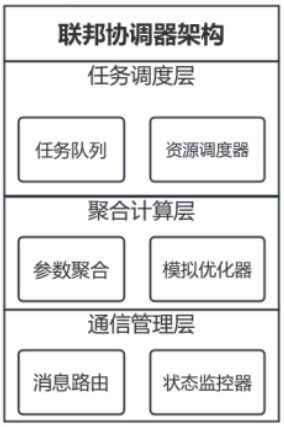

图 1 联邦协调器三层架构图

本地训练节点架构包括数据管理单元与模型训练单元及隐私保护单元，数据管理单元负责本地数据的存储索引预处理且支持多种数据格式与来源，模型训练单元实现本地模型的训练与更新集成了主流的机器学习框架，隐私保护单元在数据处理与模型训练过程中施加隐私保护措施确保敏感信息不会泄露[2]。

1.3 隐私保护框架

多层次隐私保护策略在数据的不同处理阶段施加相应的保护措施，数据输入阶段采用本地差分隐私技术添加噪声，训练阶段使用安全聚合协议保护梯度信息，输出阶段通过模型蒸馏技术减少信息泄漏风险，这种分层防护机制能够应对

1. 兰州工商学院 甘肃兰州 730101

多种类型的隐私攻击从而提供更加全面的安全保障[3]。自适应隐私预算分配机制根据不同数据的敏感程度与查询频率动态调整隐私预算，敏感度较高的数据分配更多的隐私预算，查询频率较高的操作使用更保守的预算策略，系统通过历史查询记录与数据敏感性评估模型自动计算最优的预算分配方案。隐私风险评估机制通过量化分析评估系统的隐私泄漏风险，评估指标包括信息熵变化与相关性分析及攻击成功率估计，系统定期执行风险评估任务，根据评估结果调整隐私保护参数确保隐私保护水平始终满足安全要求。

2 关键技术实现

2.1 自适应梯度聚合算法

异构数据处理策略通过数据分布感知机制识别各参与节点的数据特征差异建立数据质量评估模型对训练样本进行评级，算法引入了数据相似度计算方法，使用 Wasserstein 距离度量不同节点间的数据分布差异为后续的权重调整提供依据，动态权重调整机制根据节点数据质量、模型贡献度与历史表现综合确定聚合权重，权重计算公式为：

$$\boldsymbol{\omega}_i^{(t)}=\alpha\frac{|D_i|}{\sum_{j=1}^{N}|D_j|}+\beta Q_i^{(t)}+\gamma C_i^{(t-1)} \tag{1}$$

式中：$\boldsymbol{\omega}_i^{(t)}$表示第 t 轮中节点 i 的权重；$|D_i|$表示节点 i 的数据量；$Q_i^{(t)}$表示数据质量评分；$C_i^{(t-1)}$表示历史贡献度；α、β、γ 表示调节参数，且 $\alpha+\beta+\gamma=1$。

参数选择依据理论分析：α 值通过数据量对模型性能的边际贡献度确定，当数据量差异较大时 $\alpha\in[0.3,0.5]$；β 值基于数据质量对收敛速度的影响设定，对于高质量数据集 $\beta\in[0.4, 0.6]$；γ 值根据历史贡献的衰减函数计算，采用指数衰减 $\gamma=0.1e^{(-0.2t)}$。算法的时间复杂度为 $O(n^2m)$，其中 n 为参与节点数；m 为模型参数维度，空间复杂度为 $O(nm)$，主要存储各节点的梯度信息和权重矩阵。

梯度压缩技术采用 Top-K 稀疏化与量化压缩相结合的方法，Top-K 稀疏化选择梯度绝对值最大的 K 个元素进行传输其余元素置零，量化压缩将浮点数梯度映射到有限的离散值集合，压缩比可达到 8:1，为保证训练效果引入误差累积机制补偿压缩过程中的信息损失[4]。

压缩误差界限分析： Top-K 稀疏化的理论误差界限为：

$$E[\|\nabla f(\theta)-C_K(\nabla f(\theta)\|^2]\le(1-\frac{K}{d})\|\nabla f(\theta)\|^2 \tag{2}$$

式中：d 为梯度维度；C_K 为 Top-K 压缩算子。

量化误差界限为：

$$E[\|g-Q(g)\|^2]\le(\frac{L^2}{4})\|g\|^2 \tag{3}$$

式中：L 为量化间隔。综合压缩技术的总误差控制在原始梯度范数的 15% 以内，确保模型收敛性不受显著影响。

2.2 增强型差分隐私机制

噪声注入优化算法针对不同类型的查询操作设计了专门的噪声生成策略，对于计数查询使用拉普拉斯噪声，对于数值统计查询采用高斯噪声，对于机器学习梯度使用截断高斯噪声，算法通过分析查询的敏感性函数自动选择最适合的噪声类型与参数，隐私预算动态分配采用预算更新公式为：

$$\varepsilon_{t+1}=\varepsilon_t-\Delta\varepsilon_t c \tag{4}$$

式中：ε_t 为第 t 次查询后的剩余隐私预算；$\Delta\varepsilon_t$ 为单次查询消耗的预算；(q_t, s_t) 为基于查询类型 q 与数据敏感度 s_t 的调节函数[5]。

噪声参数自适应选择机制： 系统根据数据敏感度 $S(D)$ 和查询复杂度 $C(q)$ 动态调整噪声参数：

拉普拉斯噪声：

$$\sigma_{\text{Lap}}=\frac{S(D)}{\varepsilon} \tag{5}$$

适用于计数查询，误差方差为：

$$2(\frac{S(D)}{\varepsilon})^2 \tag{6}$$

高斯噪声（适用于数值统计，满足 (ε,δ)- 差分隐私）：

$$\sigma_{\text{Gauss}}=\sqrt{\frac{(2\ln(\frac{1.25}{\delta}))S(D)}{\varepsilon}} \tag{7}$$

截断高斯噪声：在 $[-3\sigma, 3\sigma]$ 范围内截断，减少极值噪声对模型收敛的影响。

隐私泄漏风险量化模型： 采用互信息度量隐私泄露程度：

$$I(X;Y)=\sum\sum\frac{p(x,y)\log(p(x,y)}{(p(x)p(y))} \tag{8}$$

式中：X 为原始数据；Y 为添加噪声后的数据。

理论界限为（确保隐私泄漏风险在可控范围内）：

$$I(X;Y)\le\frac{\varepsilon^2\sigma^2}{2} \tag{9}$$

精度 - 隐私平衡策略通过多目标优化算法在模型精度与隐私保护之间寻找最优平衡点，优化目标函数定义为：

$$\min_{\varepsilon}\lambda L(M_\varepsilon)+(1-\lambda)\cdot\varepsilon \tag{10}$$

式中：$L(M_\varepsilon)$ 为添加噪声后模型的损失函数；ε 为隐私预算；λ 为平衡参数。

2.3 高效同态加密实现

加密参数优化通过理论分析与实验测试确定最优的密钥长度与多项式模数及误差分布参数，针对联邦学习场景的计算特点选择 2 048 位的密钥长度与特定的 CKKS 方案参数配置，在保证安全性的前提下最大化计算效率，批量运算加速

技术利用 SIMD（单指令多数据）并行处理能力将多个数值打包到一个密文中进行批量计算。通过重新设计数据布局与计算顺序，批量处理的效率比逐个处理提升了 8~16 倍。

2.4 安全聚合协议设计

多方安全计算框架基于 Shamir 秘密共享方案构建且支持 *t*-out-of-*n* 的容错机制，参与方将梯度参数分解为 *n* 个份额，只要有 *t*+1 个诚实参与方就能正确恢复聚合结果。协议采用加性秘密共享使得本地计算开销保持线性增长。恶意节点检测机制通过行为分析与统计检验识别异常节点，系统监控各节点的梯度更新模式与通信频率及计算时间，使用统计异常检测算法发现偏离正常模式的节点，对于疑似恶意节点系统采用投票机制与多数原则进行最终判定。容错性保障策略设计了多重备份与动态恢复机制，关键数据在多个节点进行副本存储，当部分节点失效时能够快速切换到备用节点，协议支持节点的动态加入与退出不会影响正在进行的训练任务。

3 平台实现与部署

3.1 系统实现技术栈

分布式计算框架选择了 Apache Spark 作为底层计算引擎结合 Kubernetes 进行容器化部署与资源管理，Spark 的内存计算能力与弹性分布式数据集（RDD）抽象为大规模数据处理提供了高效支持，Kubernetes 的自动扩缩容与故障恢复机制确保了系统的高可用性。加密库集成方案采用了 Microsoft SEAL 同态加密库与 OpenSSL 密码学库的组合，SEAL 库专门针对 CKKS 方案进行了优化提供高效的同态运算实现，OpenSSL 库负责传统的对称加密与非对称加密及数字签名功能，两个库通过统一的加密接口层进行集成简化上层应用的调用复杂度。

数据库设计采用分布式时序数据库 InfluxDB 存储训练过程中的监控数据与日志信息，使用 MongoDB 存储模型元数据与配置信息采用 Redis 缓存频繁访问的中间结果，这种混合存储架构能够满足不同类型数据的存储与查询需求。

3.2 性能优化策略

通信开销优化通过梯度压缩与增量传输及异步通信三重机制实现，梯度压缩采用自适应稀疏化算法根据网络带宽动态调整压缩比例，增量传输只传输相对于上一轮的参数变化量减少数据传输量，异步通信允许快速节点提前开始下一轮训练避免因慢节点导致的整体延迟。计算资源调度引入了基于强化学习的智能调度算法能够根据历史执行情况与当前资源状态预测任务的资源需求与执行时间，调度器优先为重要任务分配高性能资源同时平衡各节点的负载分布避免资源热点问题。存储效率提升通过数据去重与压缩存储及分层存储策略实现，数据去重算法识别并合并相同的数据块，压缩存储使用高效的压缩算法减少存储空间占用，分层存储将热数据存储在高速 SSD 中冷数据迁移到成本较低的机械硬盘。

3.3 可扩展性设计

动态节点管理机制支持节点的热插拔操作，新节点加入时系统自动进行身份验证与能力评估分配适当的任务负载，节点离开时系统将其承担的任务重新分配给其他节点确保服务的连续性，节点管理采用一致性哈希算法最小化节点变化对系统的影响。负载均衡机制基于节点的计算能力与网络带宽及当前负载状态进行任务分配，系统维护节点能力矩阵与实时负载监控信息使用加权轮询算法分配训练任务，对于异构环境中的节点能力差异采用动态权重调整策略实现负载的均衡分布。弹性伸缩能力通过预测性扩容与基于阈值的缩容实现，系统通过分析历史负载模式与业务增长趋势预测资源需求提前进行扩容准备，当系统负载低于设定阈值时自动释放多余资源以降低运营成本，伸缩操作采用渐进式策略避免对运行中的任务造成影响。

4 实验验证与性能分析

4.1 实验环境搭建

硬件环境配置采用了混合云架构包括 8 台配置为 Intel Xeon Gold 6248 处理器 64 GB 内存 1 TB NVMe SSD 的物理服务器作为主要计算节点以及 20 台配置为 4 核 CPU8 GB 内存的云虚拟机作为边缘参与节点，网络环境模拟了从 100 Mbit/s~1 Gbit/s 不等的带宽条件以及 5~50 ms 的网络延迟。

4.2 性能指标评估

模型准确率对比分析结果显示如表 1 所示，该平台在 3 个数据集上的性能表现均优于传统联邦学习方案，在 MNIST 数据集上达到了 98.7% 的准确率，相比集中式学习仅下降 1.1%；CIFAR-10 数据集上的准确率为 84.3%，比 FedAvg 方案提升了 3.2%；IMDB 数据集的分类准确率达到 89.1%，体现了平台对不同类型数据的良好适应性。

表 1 模型指标对比评估表

单位：%

数据集	集中式学习	FedAvg	FedProx	SCAFFOLD	该平台
MNIST	99.2	96.8	97.3	97.9	98.7
CIFAR-10	86.5	81.1	82.4	83.6	84.3
IMDB	91.3	87.2	88.1	88.9	89.1

参考联邦学习聚合算法的标准评估结果，SCAFFOLD 算法在达到 0.5 测试精度时所需迭代轮次最少，验证了其收敛效率优该平台通过自适应梯度聚合优化进一步提升了收敛性能。通信效率对比分析如表 2 所示。

表 2 通信效率对比分析

算法	通信轮次	数据传输量 /MB	收敛时间 /h
FedAvg	150	1 250	4.2
该平台	118	425	2.8

通信效率提升 34%，数据传输量减少 66%，训练时间缩短 33%。

4.3 实际应用场景验证

金融风控场景测试中该平台与某大型银行与两家金融科技公司合作构建了跨机构的信贷风险评估模型，在保护客户隐私的前提下联合建模的风险识别准确率达到 92.3%，比单独建模的 87.8% 提升 4.5 个百分点，假阳性率从 12.4% 降低至 8.1%，降幅 34.7%，实验验证了平台在金融领域的实用价值为跨机构数据协作提供了可行的技术方案。

5 结语

基于联邦学习的隐私保护型大数据分析平台通过创新的技术架构设计成功解决传统大数据分析中数据孤岛与隐私保护的矛盾问题，实验验证结果充分证明平台的技术先进性与实用价值，通信开销降低的性能表现解决了联邦学习面临的网络瓶颈问题，隐私保护强度提升为跨机构数据协作扫清了安全障碍。在金融风控与医疗诊断及智能制造等实际应用场景中的成功验证展现了平台广阔的产业化前景，随着数字经济的快速发展与数据价值的日益凸显，跨机构数据协作需求将持续增长该平台为构建安全可信的数据共享生态体系提供了重要的技术支撑。

参考文献：

[1] 郁思康 , 范菁 , 金亚东 , 等 . 联邦学习在隐私安全领域面临的威胁综述 [J/OL]. 计算机应用 ,1-13[2025-10-17].https://link.cnki.net/urlid/51.1307.TP.20250526.1308.004.

[2] 田天 , 赵晗 , 刘璐 . 差分隐私加密结合人工智能优化大数据分析中的隐私保护研究 [J]. 中国宽带 ,2025,21(5):49-51.

[3] 汪智 . 面向医学影像的隐私保护型联邦学习模型研究 [D]. 徐州 : 中国矿业大学 ,2024.

[4] 刘小微 . 面向非平衡数据的隐私保护联邦学习方法研究 [D]. 合肥 : 中国科学技术大学 ,2024.

[5] 党照群 . 考虑隐私信息保护的虚拟电厂运营商交易方法研究 [D]. 沈阳 : 沈阳工程学院 ,2024.

【作者简介】

王建芳（1978—），女，甘肃天水人，本科，副教授，研究方向：计算机软件设计与开发、大数据分析。

（收稿日期：2025-06-20 修回日期：2025-12-01）

（上接第 54 页）

[14]CHEN M G, JIN X M, SHEN D. Short text classification improved by learning multi-granularity topics[C]//IJCAI'11: Proceedings of the 22nd international joint conference on Artificial Intelligence - Volume Volume Three.NewYork: ACM, 2011:1776 - 1781.

[15]DEVLIN J, CHANG M W, LEE K, et al. BERT: pre-training of deep bidirectional transformers for language understanding[C]//Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers). Brussels:ACL,2019: 4171-4186.

[16] 曾泽凡 , 王厚峰 , 刘康 . 基于预训练语言模型的知识增强文本分类研究综述 [J]. 软件学报 , 2023, 34(1): 149-175.

[17]ZHOU C T, SUN C L, LIU Z Y, et al. A C-LSTM neural network for text classification[EB/OL]. (2015-11-30)[2025-11-03].https://doi.org/10.48550/arXiv.1511.08630.

[18] 王华伟 , 金澈清 , 王素格 . 融合注意力机制的卷积神经网络文本分类模型 [J]. 计算机科学 , 2021, 48(5): 267-272.

[19]VASWANI A, SHAZEER N, PARMAR N, et al. Attention is all you need[C]//Advances in neural information processing systems. NewYork: ACM, 2017: 6000 - 6010.

[20]LIU Y H, OTT M, GOYAL N, et al. RoBERTa: A robustly optimized BERT pretraining approach[EB/OL].(2019-07-26)[2025-11-22]. https://doi.org/10.48550/arXiv.1907.11692.

[21] 朱艳辉 , 刘挺 , 王东波 . 基于动态上下文增强注意力机制的文本分类方法 [J]. 计算机研究与发展 , 2022, 59(7): 1436-1447.

[22]MOSCHITTI A, PANG B, DAELEMANS W. GloVe: Global vectors for word representation[C]//Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP).Brussels:ACL, 2014: 1532-1543.

【作者简介】

陈建忠（1999—），男，江西赣州人，硕士研究生，研究方向：文本分类、知识图谱。

陈琴（1998—），女，广西崇左人，硕士研究生，研究方向：深度学习、教育机器人。

（收稿日期：2025-09-09 修回日期：2025-12-08）