基于联邦学习的区域能源电力隐私保护数据共享方法

史渊源[1] 万 鹏[1] 王 亮[1]
SHI Yuanyuan WAN Peng WANG Liang

摘 要 能源数据包含用户用电行为、企业生产能耗、电网拓扑结构等敏感信息，在不同通信协议上存在明显差异，跨网数据交互需通过中间件转换，增加了共享成本与风险。为了缓解这一问题，文章提出了一种基于联邦学习的区域能源电力隐私保护数据共享方法。在区域化的数据存储结构基础上，通过生成区域独立的公钥和数据专属私钥，构建区域能源电力隐私保护数据的局部联邦学习模型。训练与更新局部联邦学习模型后，将模型聚合至中央服务器，以此替代海量数据作为数据共享对象。通过密钥身份验证，将局部联邦学习模型分发至目标参与节点，实现区域能源电力隐私保护数据的共享。实验结果表明，该方法数据共享过程的通信代价平均仅为 48 156 bit/s，共享效率较高，具有良好的实践应用前景。

关键词 数据共享；电力隐私保护数据；隐私保护数据共享；区域能源电力数据；联邦学习；电力数据共享

doi：10.3969/j.issn.1672-9528.2026.04.022

0 引言

由于当前的能源系统较为复杂，为更好地提供电力服务，现有的电力企业选择将不同区域的电力能源进行高度整合，采用智能化的手段实现电力能源的高质量调度。然而，在这一过程中，涉及大量电力数据的传输共享。如果数据的隐私保护问题处理不当，很可能会导致区域能源的电力数据产生泄露，为电力企业带来较大的经济损失。在这一情况下，为确保区域能源电力数据共享的安全性，需要采用有效的手段，对电力数据进行隐私保护下的数据传输。基于这一应用需求，领域内很多研究人员提出了隐私保护数据共享方法。

项胤兴等[1]提出了基于差分隐私保护的数据共享方法，该方法整合了区块链上的多方数据，利用区块链的可溯源特性，构建了不同安全等级下的差分隐私保护方案，实现了数据的多层级安全共享。该方法能够有效避免数据共享过程中的数据篡改问题。然而，在实际应用中，数据差分隐私保护所需的隐私预算可能较大，这可能会降低隐私保护数据共享的实时性，进而降低共享效率。张海俊等[2]提出了基于 CKKS 与 CP-ABE 的隐私保护数据共享方法，该方法采用 CKKS 方法对数据进行加密处理，以实现数据的隐私保护。在第三方服务基站的支持下，该方法计算数据共享的安全认证参数，并结合 CP-ABE 算法实现一对多的数据共享。该方法的计算误差较小，但其计算复杂度较高，所需的计算时间较长，导致实际的数据共享效率不高。王杨鹏等[3]提出了基于区块链的隐私保护数据共享方法，该方法在车联网环境下构建了数据加密处理的掩码模型。该方法通过轻量化处理，设计了分层联邦学习下的数据共享传输架构，将加密后的数据安全上传至区块链，并利用审计机制实现了隐私保护数据的共享过程。该方法能够应用于恶意环境下，有效提高了数据加密方案的精度。但数据加密的过程需要复杂的密钥管理，导致审计机制需要较多环节，导致该方法在实际应用中难以实现高效率的数据共享。曹来成等[4]提出了基于动态博弈策略的隐私保护数据共享方法。采用动态博弈策略对数据进行匿名化评估，设计相应的数据隐私保护方案。在数据匿名的情况下，采用生成对抗网络生成大量样本，实现小样本下的隐私保护数据共享。该方法通过数据增广能够降低小样本应用场景的限制。但为了适应数据属性的变化，该方法需要在匿名的情况下进行加密参数的更新，增加了数据共享系统的延迟，共享效率较低。

考虑到上述研究人员所提出的隐私保护数据共享方法难以满足预期的数据共享效率需求。为了缓解这一问题，本文提出了一种基于联邦学习的区域能源电力隐私保护数据共享方法。该方法通过构建联邦学习模型，代替数据传输个体，实现了高效率的区域能源电力隐私保护数据共享。

1 区域能源电力隐私保护数据共享方法设计

1.1 构建区域能源电力数据联邦学习模型

在电力企业的数据管理系统中，根据其中心化数据处理模式，采用联邦学习的方法在区域能源数据本地存储单元构建联邦学习模型，以此进行独立的数据隐私保护处理并更新，

1. 宁夏电力有限公司 宁夏银川 750001

实现电力隐私保护数据的安全共享。

以能源电力数据的区块链上链节点为联邦学习模型的参与节点，在数据存储的客户端，为区域能源电力数据生成分布式密钥，构建电力隐私保护数据的本地联邦学习模型[5]。定义电力数据隐私保护的多维度初始参数，用公式表示为：

$$R(X)=\left(\lambda,q(x),\sigma,a\right) \tag{1}$$

式中：$R(X)$ 表示区域 X 的本地联邦模型的电力数据隐私保护初始参数；λ 表示本地系统的安全系数；$q(x)$ 表示区域能源电力数据 x 的模数链；σ 表示随机整数；a 表示公共参数。

基于数据的初始参数，为该区域生成独立的公钥以及数据专属私钥[6]，用公式分别表示为：

$$b(x)=-\mathrm{as}(x)+e(\mathrm{mod}\,q(x)) \tag{2}$$

$$B(x)=-\mathrm{as}(x)+e(\mathrm{mod}\,P\cdot q(x)) \tag{3}$$

式中：$b(x)$ 表示电力能源数据存储区域节点的独立公钥；$B(x)$ 表示区域能源电力数据的专属私钥；e 表示生成噪声；mod 表示模运算；P 表示联邦学习模型的参与节点。

在数据共享的另一个参与方，共同生成一个隐私保护数据共享的公开密钥，用公式表示为：

$$A=e^{b(x)}\bmod P(x) \tag{4}$$

式中：A 表示数据公开密钥。

利用生成的密钥，建立数据隐私保护的合约，将加密后的区域能源电力数据上传到相应的区块链节点上，实现联邦学习模型中的隐私保护数据同步，完成区域本地联邦学习模型的构建。

1.2 基于联邦学习的电力数据全局聚合

根据所构建的区域本地联邦学习模型，通过本地训练与全局更新，实现区域能源电力隐私保护数据在服务器上的聚合。在区域节点上，对构建的联邦学习模型进行初始化处理，并在参与方本地，采用预定义的算法对数据加密的隐私保护过程进行局部模型训练，得到每个区域参与节点的能源电力隐私保护数据集 $D(x)$。在本地联邦学习模型训练的过程中，计算相应的梯度参数，用公式表示为：

$$g(D)=\nabla_{\theta}\sum_{i=1}^{n}F(\theta,x) \tag{5}$$

式中：$g(D)$ 表示联邦学习模型的本地梯度参数；θ 表示训练轮次；∇ 表示梯度运算；F 表示损失函数；i 表示联邦学习模型的本地参与节点；n 表示参与区域的数量[7]。其中，每个参与节点的损失函数用公式表示为：

$$F(i)=\frac{1}{n}\sum f(x) \tag{6}$$

式中：$f(x)$ 表示单点区域能源电力隐私保护数据的本地模型训练损失。

完成本地的联邦学习模型训练后，根据每个参与节点的梯度参数，通过加权平均操作，更新得到新的联邦学习全局模型[8]。用公式表示为：

$$g_{\theta+1}=\eta(g_{\theta}-\frac{1}{n}\sum_{i=1}^{n}g_{\theta+1}^{i}) \tag{7}$$

式中：$g_{\theta+1}$ 表示更新的联邦学习模型全局参数；g_{θ} 表示上一轮次的模型参数；η 表示学习率。

通过迭代训练，实现联邦学习模型的全局更新。将更新后的模型参数发送到数据共享的中央服务器上，执行多参与节点的模型聚合操作。定义这一过程的聚合参数权重，用公式表示为：

$$\beta=\sum_{i=1}^{n}w_{\theta+1}^{i}\cdot g_{\theta+1} \tag{8}$$

式中：β 表示聚合参数权重；$w_{\theta+1}^{i}$表示联邦学习模型全局更新的时间跨度参数。

通过聚合，在保留原始区域能源电力隐私保护数据的情况下，将局部模型聚合到中央服务器上，代替海量的原始数据作为数据共享的对象，以此消除数据集中共享的效率限制。

1.3 全局分发下的区域能源电力隐私保护数据共享

在区域能源电力隐私保护数据共享的多个参与方中，通过验证所生成的公开密钥，确定其安全身份，并将中央服务器上的局部联邦学习模型分发到通过身份认证的参与节点上，实现区域能源电力隐私保护数据的共享操作。使用数据共享参与双方的数据专属密钥及公开密钥计算参与节点的密钥身份[9]，用公式表示为：

$$K=Z^{B(x)}\bmod A \tag{9}$$

式中：K 表示数据共享参与节点的密钥身份；Z 表示数据共享的参与方。

根据上述计算结果，验证其是否满足区域独立公钥的哈希值，若满足，则判定为安全身份，建立全局联邦学习模型下的数据共享通道。为通过认证的参与节点分发解密密钥，为共享节点提供可读数据。用公式表示为：

$$Z(x)=L\sum_{i=1}^{m}(q(x)\bmod m^{2})\times(\theta\cdot b(x))^{-1} \tag{10}$$

式中：$Z(x)$ 表示通过认证的参与节点解密得到的数据明文；L 表示解密密钥；m 表示通过认证的数据共享参与节点数量。

通过中央服务器将局部联邦学习模型分发到目标参与节点上，经过解密处理，实现区域能源电力隐私保护数据的安全共享。

2 应用实践

2.1 区域能源电力数据

本次实验在区域电力能源交易系统中获取大量的隐私数据作为实验数据，其主要数据类型及数据获取情况如表 1 所示。

表 1 实验数据

交易维度	数据类型	数据量
区域电力能源生产者维度	火力发电数据	9 522
	风力发电数据	2 625
	水力发电数据	9 611
	光伏发电数据	6 151
区域电力能源消费者维度	工业用户	12 620
	商业用户	61 296
	微网用户	16 925
交易环节维度	交易记录	3 841
	交易方账户	2 951
	交易数据	1 627

构建一个区块链架构，将上述数据随机分配到各个区块链节点上，完成实验数据的区域划分。以每个区域所分配的能源电力数据作为数据共享的对象，开展区域能源电力隐私保护数据共享的实践应用测试。

2.2 数据共享测试与结果分析

基于实验数据的区块链场景下，模拟生成一组区域能源电力隐私保护数据的共享任务，以此对本文方法的实践应用性能进行检验。

本文方法通过构建联邦学习模型实现数据共享，为了确保模型性能，对模型的学习率参数进行测试选择。以准确率为指标，计算联邦学习模型在不同学习率下的指标值，结果如图 1 所示。

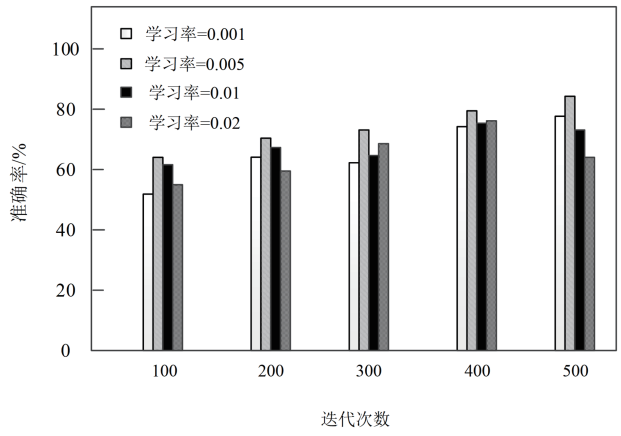

图 1 联邦学习模型的学习率选择

从图 1 可以看出，在不同轮次的联邦学习模型训练中，当学习率为 0.005 时，模型的准确率均能够保持在较高的水平上，相比于其他的学习率参数有着较大的优势。基于此，本次应用实践选用 0.005 作为学习率参数，对构建的区域联邦学习模型进行训练与全局更新。在此基础上，对目标的数据共享任务进行实现。经验证，本文方法成功将隐私保护下的区域能源电力数据共享到目标参与节点上，并完成了相应的解密处理，有效完成了数据共享操作。

在本次实践测试中，为检验本文方法的数据共享性能，统计测试过程中的通信代价，以此评估数据共享过程的整体效率。同时，采用基于差分隐私保护以及 CKKS 与 CP-ABE 两种隐私保护数据共享方法作为对比方法，对本文方法的实践应用性能水平进行对比评价。经测试，得到如图 2 所示的对比结果。

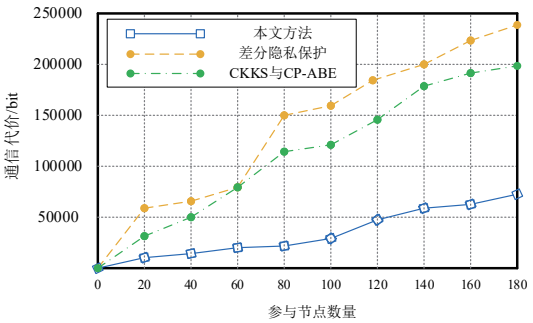

图 2 各方法的数据共享效率对比

从图 2 可以看出，相比于其他两种隐私保护数据共享方法，本文方法的数据共享过程明显能够减少系统所需消耗的通信代价，平均仅为 48 156 bit/s，这一结果表明本文方法所需的时延成本更低，数据共享过程的整体效率较高。这一优势主要得益于本文方法采用局部联邦学习模型代替海量的区域能源电力隐私保护数据，减少数据个体在共享过程中的资源消耗，在更短的时间内完成数据共享，有效提高了数据共享效率。

3 结语

本文所设计的基于联邦学习的区域能源电力隐私保护数据共享方法，通过在数据存储的本地区域上构建局部联邦学习模型，通过更新与全局聚合，实现了将海量区域能源电力隐私保护数据转换为局部联邦学习模型的表达形式，减少了数据共享所需分发的数据个体，从而成功提高了数据共享过程的整体效率。在本文方法的应用下，不仅能够保障区域能源电力数据共享过程的安全性，实现有效的数据隐私保护，同时，还能够通过提高数据共享效率，为区域能源电力交易等环节提供高效率的数据共享传输支持。

参考文献：

[1] 项胤兴，杨里，陈伯建，等．基于差分隐私保护的电力线损数据共享研究 [J]. 计算机应用与软件，2023, 40 (7): 333-336.

[2] 张海俊，丁平刚，彭一轩，等．基于 CKKS 与 CP-ABE 的国网电力数据共享方案 [J]. 信息安全研究，2023, 9 (3): 262-270.

[3] 王杨鹏，牛宪华，熊玲，等．基于联邦学习和区块链的车联网隐私保护数据共享方案 [J]. 计算机应用，2024, 44 (S1): 107-111.

基于可视图算法的数据序列网络特征分析

严 慧 [1]
YAN Hui

摘 要 复杂网络原理为数据分析开辟了全新的研究途径。可视图算法因其简单、高效、易实现等特点广泛用于为不同数据构建复杂网络。文章以癫痫脑电信号以及学习投入数据为实验对象，采用五种可视图算法为这些数据构建复杂网络，提取网络的八种统计特征，分析不同可视图算法下正常脑电与癫痫脑电网络特征的分布差异以及两类学习投入数据网络特征的分布差异，最后挑选出具有高辨别力的网络特征用于癫痫脑电识别以及学习投入数据分类。研究结果表明，五种可视图算法下，共有 13 个网络特征识别癫痫脑电的准确率达到 80% 以上，最高可达 88.0%；共有 7 个网络特征分类学习投入数据的准确率达到 80% 以上，最高可达 88.1%。实验证明了基于可视图算法为不同数据构建复杂网络进而提取高辨别力网络特征的可行性，为基于网络特征进行信号识别与数据分类提供研究思路与实践参考。

关键词 复杂网络；可视图；网络特征；信号识别；数据分类

doi：10.3969/j.issn.1672-9528.2026.04.023

0 引言

复杂网络是一种描述复杂系统中各个元素之间的相互关系的数学模型。将系统中的元素抽象为节点（如：人、城市、通信设备），将元素之间的关系抽象为边（如：人际关系、交通线路、通信链路），构建出一个网络结构，用以研究整个系统的拓扑结构、动态行为以及元素之间的相互作用。

可视图算法是一种将数据序列转变为复杂网络的方法。这类方法在数据序列与复杂网络之间架起了一座桥梁，为数据分析开辟了新途径。Lacase 等 [1] 在 2008 年首次提出可视图（visibility graph, VG），该算法可以将周期序列转变成规则网络，将随机序列转变成随机网络，将分形序列转变成

1. 金陵科技学院电子信息工程学院 江苏南京 211169

[基金项目] 2023 年度高校哲学社会科学研究一般项目“基于复杂网络的应用型本科院校大学生学习投入度研究”（2023SJYB0584）；2024 年江苏省产学研合作项目“基于复杂网络的病理性脑电信号的特征提取与检测识别”（BY20240093）

[4] 曹来成 , 后杨宁 , 冯涛 , 等 . 面向动态博弈的 k- 匿名隐私保护数据共享方案 [J]. 西安电子科技大学学报 , 2024, 51 (4): 170-179.

[5] 杨邵成 , 蔡英 , 范艳芳 . 车载社交网中基于密文属性加密的车队车辆数据共享方案 [J]. 汽车技术 , 2024 (8): 14-21.

[6] 葛胤池 , 张辉 , 孙浩航 . 基于隐空间扩散模型的差分隐私数据合成方法研究 [J]. 计算机科学 , 2024, 51 (3): 30-38.

[7] 高改梅 , 张瑾 , 刘春霞 , 等 . 基于区块链与 CP-ABE 策略隐藏的众包测试任务隐私保护方案 [J]. 计算机应用 , 2024, 44 (3): 811-818.

[8] 唐明坤 , 吴思竹 , 周佳茵 , 等 . 医学数据共享隐私保护中基于聚类的匿名化算法关键技术研究 [J]. 医学信息学杂志 , 2023, 44 (6): 65-71.

[9] 黄仁彦 , 杨立 . 数字化档案敏感信息混沌密钥加密算法仿真 [J]. 计算机仿真 ,2025,42(1):249-252.

【作者简介】

史渊源（1982—），男，宁夏固原人，本科，高级工程师，研究方向：大数据分析应用，email:yuany5819@163.com。

万鹏（1988—），男，宁夏石嘴山人，本科，高级工程师，研究方向：数据管理与运营。

王亮（1981—），男，吉林松原人，本科，高级工程师，研究方向：大数据分析应用。

（收稿日期：2025-08-14 修回日期：2026-03-25）