改进联邦增量学习下多源能源跨域数据安全密钥共享技术

李文科[1] 王益彰[1] 田 钺[1] 董若烟[1] 姚 舜[1]
LI Wenke WANG Yizhang TIAN Yue DONG Ruoyan YAO Shun

摘 要 新能源节点加入多源能源系统中，使得能源数据呈现时空异质性，导致客户端权重散度不可控增大，难以根据权重散度分发子密钥份额，由此降低了数据跨域共享安全性。为此，文章引入改进联邦增量学习，设计多源能源跨域数据安全密钥共享技术。通过引入可修复门限方案，通过 Shamir 与 Ramp 门限区组化构造能源跨域数据安全密钥共享可修复门限，保障密钥安全。针对传统静态门限方案无法自适应调整客户端权重散度，导致子密钥份额分配偏离问题，引入联邦增量学习驱动的门限主密钥更新机制。根据数据之间的权重散度，判断安全密钥的共享方向，并在联邦增量学习的基础上引入正则项，在共享安全密钥更新任务蒸馏损失最小的条件下，更新数据共享门限主密钥，分发多源跨域数据安全共享主密钥子密钥份额，实现多源能源跨域数据密钥的安全共享。实验结果显示，所研究技术的密钥共享安全性较高，对于提升能源数据质量具有重要作用。

关键词 改进联邦增量学习；多源能源跨域数据；安全密钥；共享技术；子秘密份额

doi：10.3969/j.issn.1672-9528.2026.07.037

0 引言

多源能源系统整合了多种能源形式，如太阳能、风能、水能等，旨在实现能源的高效利用和优化配置[1]。然而，随着新能源节点的不断加入，多源能源系统跨域数据安全密钥共享问题尤为突出。不同新能源节点的能源产出会随着时间的变化而波动，如太阳能的发电量在白天和夜晚有巨大差异，风力发电也会受到季节和天气变化的影响。此外，能源需求同样具有时间异质性，不同时间段的能源需求量不同，进一步加剧了能源数据的复杂性。在多源能源跨域数据共享场景中，新能源节点的不断加入使得能源数据的时空异质性进一步加剧，这直接导致客户端权重散度不可控增大。传统的分发方式难以准确衡量和分配子密钥份额，导致跨域数据共享问题出现安全问题。

针对此类问题，相关领域专家研发了多种安全共享技术。王坚等[2]提出了基于无线信道密钥生成的多源能源跨域数据密钥共享技术，将会话密钥分发到无线信道中，通过预制共享密钥，实现数据安全密钥共享。但该技术的密钥生成速率有限，数据加密延迟，难以准确分发子密钥份额，导致密钥共享安全性较差。姜震等[3]提出了基于经验模态分解的多源能源跨域数据密钥共享技术，利用经验模态分解，将共享密钥分解成多个 IMF 分量，通过同态加密与密钥共享的方式，确保数据共享的有效性。该技术在密钥生成的过程中，窃取密钥与正确密钥之间的相关系数增加，导致子密钥份额丢失率增加。陈金木等[4]提出了基于云服务器应用的多源能源跨域数据密钥共享技术，将密钥拆分成用户共享份额与云服务器共享份额，选定用户共享份额为密码短语，通过迭代哈希操作，完成数据密钥共享任务。然而，一旦云端密钥被窃取，将会出现子密钥份额丢失率增加的情况，影响密钥共享的安全性。何志成[5]提出了基于 Shamir 算法的多源能源跨域数据密钥共享技术，利用 Shamir 算法的拉格朗日插值，分发多源能源跨域数据的量子密钥，直接共享量子密钥。该技术参与方的可信度参差不齐，密钥恢复过程中出现错误，导致难以分配子密钥份额，数据共享安全性较差。

在以上研究方法的基础上，将改进联邦增量学习应用到多源能源跨域数据安全密钥共享技术中，利用多源能源数据的多样性与互补性，更新密钥信息，完成子密钥份额的分发，从而确保跨域数据共享的安全性。

1 基于改进联邦增量学习的数据安全密钥共享技术设计

1.1 能源跨域数据共享可修复门限构造

当分布式光伏、储能等节点频繁加入系统时，其数据生成速率和地理分布差异会加剧客户端权重散度的不可控增长，传统静态门限方案无法自适应调整子密钥份额分配比例，

1. 贵州电网有限责任公司数智运营中心 贵州贵阳 550081

[基金项目] 中国南方电网有限责任公司科技项目“能源大数据中心海量实时架构与多源异构数据集成融合技术研究”（GZKJXM20232513）

造成高权重节点聚集过多份额而成为攻击突破口。为此，引入可修复门限方案，通过 Shamir 与 Ramp 门限的区组化设计实现密钥容错构造，维持跨域数据共享的安全性，解决新能源节点动态接入导致的权重散度问题，实现抗丢失、抗合谋的弹性密钥管理。

可修复门限是保障密钥安全的关键机制[6-7]。将 Shamir 门限与 Ramp 门限看作可修复门限的区组 $S(2\gamma+1, 4\gamma+3)$，构造能源跨域数据 (k, n) 门限方案。$S(2\gamma+1, \gamma, 4\gamma+3)$ 中的任意两个区组，均包含 γ 个密钥公共元素。将 D 设定为 $S(2\gamma+1, \gamma, 4\gamma+3)$ 的公共元素集合，D 具有可修复性，三个区组的元素为：

$$2k-\gamma=2\left(2\gamma+1\right)-\gamma=3\gamma+2 \tag{1}$$

$$4\gamma+3=p^k \tag{2}$$

式中：k 为正整数，p 为素数，γ 为公共元素。

每个公共元素出现在 $2\gamma+1>2$ 个区组上。将安全密钥共享可修复门限设定为四个阶段，分别为初始化阶段、分配阶段、构造阶段以及恢复阶段。在初始化阶段，q 为素数幂，且 $q>4\gamma+3$。密钥管理中心在多源能源跨域数据集 A 中，任意选取 $4\gamma+3$ 个不相等的非零元素 γ_i，并将 γ_i 发送给参与者。在密钥管理中心选取主密钥 $s\in A$ 与 $2\gamma+1$ 各非零元素，生成主密钥空间 S：

$$f(\gamma_i)=\left(2k-\gamma\right)p^k a_j\gamma_i \tag{3}$$

$$S=a_j\cdot f(\gamma_i) \tag{4}$$

式中：$f(\gamma_i)$ 为非零元素多项式，a_j 为参与者。

在分配阶段，γ_i 作为密钥共享门限的值，将 γ_i 公开，并发送给参与者，令每个参与者均拥有一个属于主密钥空间的秘密份额。在构造阶段，各个参与者均掌握自身的密钥份额共享，多源能源跨域数据安全密钥共享可修复门限 $h(S)$ 公式为：

$$h\left(S\right)=f(\gamma_i)\cdot S\cdot\frac{\gamma'-\gamma_j}{\gamma_i-\gamma_j} \tag{5}$$

式中：γ' 为参与者掌握的密钥份额，γ_j 为第 j 个参与者掌握的密钥份额。

假设参与者 j 丢失了 γ_j，想要修复 j 的 γ_j，将 γ_j 对应的区组 $2\gamma+1$ 进行修复。对于 $2\gamma+1$ 中的每个元素而言，均能够找到包含 γ_j 的元素，将 $2\gamma+1$ 中的 γ_j 发送给参与者 j，修复 j 的份额，确保密钥共享的可修复性，避免多源能源数据跨域数据丢失。

1.2 改进联邦增量学习门限主密钥更新下子份额分发

尽管可修复门限构造解决了部分密钥丢失问题，但新能源节点动态接入导致的时空异质性仍会引发更深层挑战。当光伏、储能等节点频繁加入时，传统静态门限方案无法自适应调整客户端权重散度，使得子密钥份额分配偏离安全阈值；而联邦增量学习驱动的门限主密钥更新机制，可抵御因权重漂移导致的合谋攻击[8-9]。联邦增量学习驱动下计算数据之间的权重散度，公式为：

$$w_d=\frac{\left\|w^F-w^S\right\|}{h\left(S\right)\left\|w^S\right\|} \tag{6}$$

式中：w_d 为跨域数据之间的权重散度，w^F 为非独立分布数据的权重，w^S 为使用所有数据进行中心化训练的联邦学习权重参数。当 w_d 增大时，$h(S)$ 中的安全密钥偏离正确的共享方向，影响数据安全密钥共享效果。增量学习能够从动态数据流中不断学习新知识，通过不断学习 $h(S)$ 中的 γ'，了解不同参与者掌握的密钥份额。将每个时刻学习的 γ' 作为增量任务，根据增量任务的特性，分配任务 ID 唯一标识。利用正则化项约束跨域数据密钥的更新，将 γ' 中的多源能源跨域数据蒸馏到 $h(S)$ 中，在 $h(S)$ 中共享安全密钥更新任务，计算任务蒸馏损失，公式为：

$$\ell\left(\gamma',h\left(S\right)\right)=-w_d\lg\gamma' \tag{7}$$

式中：$\ell\left(\gamma',h\left(S\right)\right)$为任务蒸馏损失。

在联邦增量学习下，引入正则项，使$\ell\left(\gamma',h\left(S\right)\right)$达到最低。在$\ell\left(\gamma',h\left(S\right)\right)$趋近于 0 时，将 γ_j 作为参与者的子密钥，通过安全信道秘密分配给参与者 j，验证参与者手中密钥的真伪，公式为：

$$\gamma_j=G\cdot\mathrm{ID}_j\left(\mathrm{mod}\,n\right)\ell\left(\gamma',h\left(S\right)\right) \tag{8}$$

式中：G 为公开参数，ID_j 为任务 ID 唯一标识，n 为常数。当式成立时，参与者得到的子密钥为真实的。所有参与者的子密钥真伪均验证完成之后，集合到 S 中保存，并在 S 中更新数据共享门限主密钥，公式为：

$$S'=\begin{cases}\gamma_1=S+a_1+\ldots+a_{n-1}\\ \gamma_2=S+2a_1+\ldots+2^{n-1}a_{n-1}\\ \vdots\\ \gamma_n=S+na_1+\ldots+n^{n-1}a_{n-1}\end{cases} \tag{9}$$

式中：S' 为多源能源跨域数据安全共享的唯一主密钥，γ_1、γ_2、…、γ_n 为不同参与者掌握的密钥份额，a_1、a_2、…、a_{n-1} 为 Lagrange 多项式插值。更新后的 S' 具有唯一性，数据共享的安全性更高。

在多源能源跨域数据安全共享的唯一主密钥中，存在多个参与者与一个可信的秘密子份额分发者。分发者选择一个质数 r，从 S' 中选择多个系数 a_1、a_2、…、a_{n-1}。分发者给每一个参与者分配相应的秘密子份额，公式为：

$$g=f\left(r\right)\gamma_i S' \tag{10}$$

式中：g 为每一个参与者分配到的多源能源跨域数据安全主密钥子秘密份额，$f(r)$ 为秘密值的域。

将每一个 g 带入式（8）中，替换 G，验证每一个 g 的真伪。每一个子份额均能够看作两个秘密子份额相加，证明 g 是可以唯一的确定秘密值。将 g 秘密地发送给参与者，从而实现

多源能源跨域数据密钥的安全共享。

2 多源能源跨域数据共享实验验证

2.1 实验过程

以 FISCO BCOS 平台为基础，在 Windows 服务器上，通过 Ubuntu16.04 系统搭建多源能源跨域数据安全密钥共享实验平台，验证改进联邦增量学习下多源能源跨域数据安全密钥共享技术的有效性。多源能源跨域数据共享架构如图 1 所示。

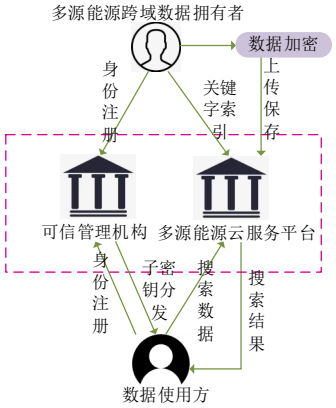

图 1 多源能源跨域数据共享架构

将 Docker 和 Docker Compose 作为实验环境，调用智能合约模拟 4 个月多源能源跨域数据，如表 1 所示。

表 1 多源能源跨域数据表

指标名称	4 个月累计	同比增长 /%
发电装机总容量	300 963×10^4 kW	14.1
水电	42 515×10^4 kW	2.1
火电	139 802×10^4 kW	4.0
核电	5 691×10^4 kW	0.3
风电	45 803×10^4 kW	20.6
太阳能发电	67 147×10^4 kW	52.4
供电煤耗率	296.3 g/kW·h	1.6
供热量	276 905×10^4×10^9 kJ	10.3
供热耗用原煤	17 196×10^4 t	9.5
供电量	25 994×10^8 kW·h	9.6

如表 1 所示，不同类型的能源数据在安全需求上存在差异，核电数据相对更为敏感，对安全性的要求较高。在制定密钥共享策略时，根据数据的敏感度为不同类型的数据分配不同级别的密钥保护，确保重要数据得到更严格的安全保障。同时，根据数据来源和传输路径，建立数据安全密钥共享交易，并在 FISCO BCOS 上配置智能合约，执行跨域数据安全密钥共享操作，并在不同数据规模下，设置联邦增量学习的超参数，如表 2 所示。

表 2 不同规模下的超参数设置表

规模组	学习率	本地训练轮次	降学习率轮次
cifar_N_10_2	0.01	70	20,30
cifar_N_10_5	0.01	70	10,20
cifar_N_10_7	0.01	70	10,20
cifar_N_10_10	0.01	70	10,20,30
ilsvrc_N_10_2	0.01	40	10,20
ilsvrc_N_10_5（N=5, 10, 20）	0.01	40	10,20
ilsvrc_N_10_5（N=15, 25）	0.001	40	—
ilsvrc_N_10_7	0.01	40	10,20
ilsvrc_N_10_10	0.01	40	10,20

如表 2 所示，将联邦增量学习轮数固定为 10，在每个能源跨域数据集中，均受到 10 个安全密钥共享的增量任务。固定每个增量任务的类别样本数，数据之间没有重叠部分，能够满足本次实验需求。

2.2 实验结果

使用生成的密钥对多源能源跨域数据进行共享操作，在可视化界面中，模拟数据安全密钥共享过程，查看密钥生成的相关提示与状态信息，确保数据能够按照设定的安全共享规则，正确共享密钥。密钥共享可视化界面如图 2 所示。

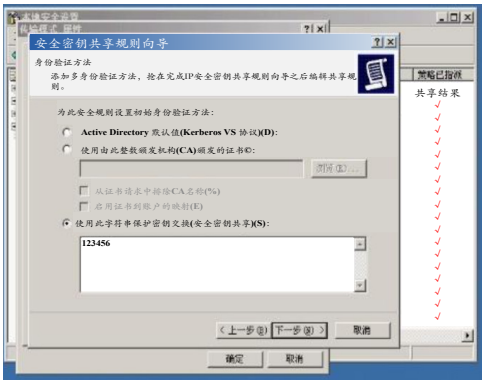

图 2 安全密钥共享可视化界面图

如图 2 所示，将 123456 作为待共享的安全密钥，模拟不同共享用户，尝试访问共享数据，共享结果中显示为“√”，能够有效将安全密钥共享到接收方，共享效果良好。

3 结语

本文设计的改进联邦增量学习下多源能源跨域数据安全密钥共享技术，根据多源能源跨域数据的特点与安全需求，对密钥进行安全备份，构造安全密钥共享可修复门限。引入联邦增量学习机制，持续学习跨域数据密钥，更新共享门限主密钥。将主密钥分解成多个子秘密份额，通过安全分发机制，实现了跨域数据密钥的安全共享，为能源数据安全提供保障。

（下转第 163 页）

machine learning methods for formation lithology identification: a comparison of tuning processes and model performances[J]. Journal of Petroleum Science and Engineering, 2018, 160: 182-193.

[6]Hall B. Facies classification using machine learning[J]. The Leading Edge, 2016, 35(10): 906-909.

[7]Liu Jingjing, Liu Jianchao. Integrating deep learning and logging data analytics for lithofacies classification and 3D modeling of tight sandstone reservoirs[J]. Geoscience Frontiers, 2022, 13(1): 101311.

[8]Breiman L. Random forests[J]. Machine Learning, 2001, 45: 5-32.

[9]Chen Tianqi, Guestrin C. XGBoost: a scalable tree boosting system[PP/OL].(2016-06-10)[2026-07-13].https://doi.org/10.48550/arXiv.1603.02754.

[10]Ke Guolin, Meng Qi, Finley T, et al. LightGBM: a highly efficient gradient boosting decision tree[C]//Advances in Neural Information Processing Systems. NewYork: ACM, 2017: 3146-3154.

[11]LeCun Y, Bengio Y, Hinton G. Deep learning[J]. Nature, 2015, 521: 436-444.

[12]Cho K, Van Merrienboer B, Gulcehre C, et al. Learning phrase representations using RNN encoder-decoder for statistical machine translation[PP/OL].(2014-09-03)[2026-07-13]. https://doi.org/10.48550/arXiv.1406.1078.

[13]He Haibo, Garcia E A. Learning from imbalanced data[J]. IEEE Transactions on Knowledge and Data Engineering, 2009, 21(9): 1263-1284.

[14]Lin T Y, Goyal P, Girshick R, et al. Focal loss for dense object detection[C]//2017 IEEE International Conference on Computer Vision (ICCV). Piscataway: IEEE, 2017: 2980-2988.

[15]Cui Yin, Jia Menglin, Lin T Y, et al. Class-balanced loss based on effective number of samples[PP/OL].(2019-01-16)[2026-07-13].https://doi.org/10.48550/arXiv.1901.05555.

[16]Chawla N V, Bowyer K W, Hall L O, et al. SMOTE: synthetic minority over-sampling technique[PP/OL].(2011-06-09)[2026-07-13].https://doi.org/10.48550/arXiv.1106.1813.

[17]Han Hui, Wang Wenyuan, Mao Binghuan. Borderline-SMOTE: a new over-sampling method in imbalanced data sets learning[C]//Advances in Intelligent Computing. Berlin: Springer, 2005: 878-887.

【作者简介】

王焜龙（1999—），男，河南平顶山人，硕士研究生，研究方向：机器学习、图像识别、灾害信息处理。

（收稿日期：2026-06-18 修回日期：2026-07-17）

（上接第 157 页）

参考文献：

[1] 贺英，王天一，李莹莹 . 线性光学克隆机改进的离散极化调制连续变量量子密钥分发可组合安全性分析 [J]. 物理学报 , 2024, 73(23): 49-58.

[2] 王坚，黄普善，金东方，等 . 基于无线信道密钥生成的群组通信密钥共享方法 [J]. 通信技术 , 2024, 57(12):1291-1296.

[3] 姜震，张勇，王莉 . 基于经验模态分解的企业等值连接共享数据加密方法 [J]. 信息技术 ,2023(11):120-125.

[4] 陈金木，陈少英，黄朝阳 . 基于云服务器应用的密码管理方案设计 [J]. 河南工程学院学报 (自然科学版), 2023, 35(2): 54-57.

[5] 何志成 . 基于 Shamir 算法的多 QKD 网络密钥共享策略 [J]. 信息与电脑 (理论版), 2023, 35(2): 231-234.

[6] 解建国，刘晶，吴涵，等 . 基于超晶格 PUF 的轻量级信息论安全密钥达成协议 [J]. 密码学报 (中英文), 2024, 11(2): 387-402.

[7] 唐长虹，赵艳琦，杨晓艺，等 . 加权门限 SM2 签名方案 [J]. 软件学报 , 2025, 36(8): 3883-3895.

[8] 臧洪睿，王天琰，姜姝宇，等 . 物联网环境下去中心化的联邦学习加密仿真 [J]. 计算机仿真 , 2025, 42(1): 400-404.

[9] 张泽辉，李庆丹，富瑶，等 . 面向非独立同分布数据的自适应联邦深度学习算法 [J]. 自动化学报 , 2023, 49(12): 2493-2506.

【作者简介】

李文科（1985—），男，贵州榕江人，本科，高级工程师，研究方向：人工智能、数据应用及治理。

王益彰（1998—），男，贵州安顺人，本科，助理工程师，研究方向：大数据。

田钺（1996—），男，贵州施秉人，本科，工程师，研究方向：电力行业数字化技术、数据运营。

董若烟（1995—），女，贵州贵阳人，硕士，工程师，研究方向：大数据、人工智能。

姚舜（1994—），男，贵州安顺人，硕士，研究方向：大数据、人工智能。

（收稿日期：2025-11-19 修回日期：2026-07-08）