Hans Journal of Data Mining 数据挖掘, 2025, 15(3), 279-285
Published Online July 2025 in Hans. https://www.hanspub.org/journal/hjdm
https://doi.org/10.12677/hjdm.2025.153024

Hans汉斯

轻量级AI驱动面向边缘数据流通场景的隐私－效用－效率动态协同优化研究

吴亚男，周　映，李浩钰，杨　琦，李　岩

中国联合网络通信有限公司软件研究院，北京

收稿日期：2025年6月17日；录用日期：2025年7月10日；发布日期：2025年7月17日

摘　要

随着数字化时代的飞速发展，数据要素作为新质生产力，在数据处理和流通中扮演着日益重要的角色。然而，数据流通面临诸多挑战，如个人数据隐私泄露风险、数据安全效用难以落地以及数据流动审批决策效率低下等问题。在此背景下，中国联合网络通信有限公司软件研究院提出了一种轻量级AI驱动的优化框架，旨在实现隐私、效用与效率的动态协同优化。该框架通过采用轻量级AI数据分类分级技术，对院内各系统、各省分公司的边缘数据进行智能处理，并结合隐私保护、效用评估及效率调控等模块，有效平衡三者关系。实验结果表明，该框架在保障数据隐私的同时，显著提升了数据效用与流通效率，为边缘数据流通领域的发展提供了新的解决方案。

关键词

轻量级AI分类分级，边缘数据流通，隐私保护，效用优化，效率提升

Research on Lightweight AI-Driven Dynamic Collaborative Optimization of Privacy-Utility-Efficiency in Edge Data Circulation Scenarios

Yanan Wu, Ying Zhou, Haoyu Li, Qi Yang, Yan Li

Chinaunicom Software, Beijing

Received: Jun. 17th, 2025; accepted: Jul. 10th, 2025; published: Jul. 17th, 2025

Abstract

With the rapid development of the digital era, data elements, as a new productive force, are playing

文章引用: 吴亚男, 周映, 李浩钰, 杨琦, 李岩. 轻量级 AI 驱动面向边缘数据流通场景的隐私-效用-效率动态协同优化研究[J]. 数据挖掘, 2025, 15(3): 279-285. DOI: 10.12677/hjdm.2025.153024

an increasingly critical role in data processing and circulation. However, data circulation faces multiple challenges, including risks of personal data privacy leakage, difficulties in implementing data security utility, and inefficiencies in data flow approval and decision-making. In this context, the ChinaUnicom Software Research Institute proposes a lightweight AI-driven optimization framework aimed at achieving dynamic collaborative optimization of privacy, utility, and efficiency. This framework employs lightweight AI classification and grading technology to intelligently process edge data from various systems and provincial branches, integrating modules such as privacy protection, utility evaluation, and efficiency regulation to effectively balance these three dimensions. Experimental results demonstrate that the framework ensures data privacy while significantly enhancing data utility and circulation efficiency, providing a novel solution for advancing edge data circulation.

Keywords

Lightweight AI Classification and Grading, Edge Data Circulation, Privacy Protection, Utility Optimization, Efficiency Improvement

1. 引言

《数据二十条》的发布从数据产品、流通交易、收益分配和安全治理等方面构建了数据基础制度，促进数据要素市场高质量发展。围绕数据要素安全治理，国家陆续出台“四法一条例”等法规政策，进一步推动数据安全体系的完善和落地。中国联合网络通信有限公司软件研究院作为联通集团和省分公司的重要技术支撑单位，积极响应国家和管理部门的数据安全政策，从“网络向新、技术向新、服务向新”三大方向，以数智融合(AI、大数据、云计算)和数实融合(产业数字化)为核心，积极推动科技创新与落实安全生产和数据安全责任。

边缘数据流通的基本概念是指在靠近数据源的边缘设备或业务服务器上对数据进行采集、处理与传输、共享的过程，其核心目标是通过减少数据传输延迟和计算资源浪费来提升系统整体性能和边缘数据个人数据的安全性[1]。现有研究表明，边缘数据流通模型通常采用分层架构，包括终端设备层、边缘节点层和云端层，各层之间通过协同计算实现数据的高效流通。然而，不同研究在数据处理与传输方面的特点存在显著差异，例如一种基于人工智能与边缘代理的物联网框架设计，通过优化边缘架构实现了计算前置化与智能化，但该框架在硬件资源受限的情况下仍面临较大的集成挑战[2]。另外一种探讨了联邦学习在边缘计算场景中的应用，指出其在解决隐私保护和数据安全问题上的优势，但也提到传统联邦学习在通信效率与模型性能之间的权衡难题[3]。综上所述，尽管已有研究在边缘数据流通的技术实现上取得了一定进展，但在资源约束条件下的数据分类分级准确性、数据流通高效性与安全性平衡仍是亟待解决的关键问题。

随着联通软研院各业务系统和省分公司数据量的激增以及应用场景的多样化，业务数据处理和数据流通过程中存在大量的个人用户姓名、手机号等个人隐私信息，传统的数据流通模式已难以满足个人隐私保护、数据安全高效流通要求，亟需更为高效和智能的解决方案来应对这些挑战。中国联合网络通信有限公司软件研究院各业务系统和省分公司研究探索了轻量级 AI 数据分类分级从集中的数据安全平台任务剥离，通过边缘计算平台下沉到靠近数据源的边缘节点方法，显著提升了业务数据的实时处理能力、

降低了个人隐私泄露风险、提高了数据流动审批决策效率。后续可以赋能在智慧城市、智能家居、工业自动化等场景中，轻量级 AI 数据分类分级赋能海量数据的本地化处理提供了可能，安全高效的数据流通作为边缘计算生态系统的重要组成部分，将发挥更大的作用。

本研究旨在提出一种基于轻量级 AI 数据分类分级的优化框架，以实现边缘数据流通中隐私、效用与效率的动态协同优化。具体而言，该框架通过引入先进的 AI 算法对边缘数据进行智能分类和分级处理，从而在确保数据隐私安全的同时，最大化数据的利用价值并提高流通效率[4]。这一研究对于推动边缘数据流通领域的发展具有重要意义。一方面，它为解决当前边缘计算环境中存在的隐私泄露、传输效率低下和数据效用不足等问题提供了新的思路和方法；另一方面，该框架的提出也为未来边缘计算与其他新兴技术，如联邦学习和区块链的融合奠定了基础，从而进一步拓展其应用场景和技术边界。

2. 边缘数据流通场景的轻量级 AI 驱动隐私保护技术研究

2.1. 边缘数据流通中的隐私风险分析

在边缘计算环境下，数据的生成、传输与处理高度依赖于分布式的边缘节点。这些节点通常暴露在开放或半开放的物理环境中，面临着来自多方面的隐私威胁[5]。一方面，恶意攻击者可能通过网络嗅探、数据截获等手段窃取敏感信息；另一方面，边缘设备自身的安全防护机制相对薄弱，易遭受恶意软件入侵，导致数据泄露。此外，边缘计算场景中涉及大量个人用户数据，如智能家居设备采集的用户生活习惯数据、智能医疗设备获取的患者健康数据等，这些数据的泄露将对用户的隐私造成严重侵害。

2.2. 轻量级 AI 驱动的隐私保护技术原理

轻量级 AI 数据分类分级技术是实现隐私保护的关键。通过训练轻量级 AI 模型，对边缘数据进行智能分类，识别出其中包含的敏感信息，并依据预设的分级标准对数据进行分级处理。例如，利用卷积神经网络(CNN)或循环神经网络(RNN)等轻量级模型，对图像、文本等不同类型的数据进行特征提取与分类，将包含个人身份信息、商业机密等敏感内容的数据划分到高级别隐私类别[6]。在此基础上，针对不同隐私级别的数据，采用差异化的隐私保护策略，如对高隐私级别的数据进行加密处理、数据匿名化等，从而实现精准的隐私保护，其瓶颈层(Bottleneck)引入注意力机制(SE 模块)，输入层适配边缘数据特征(如文本/图像/时序数据)，输出层为数据分类分级结果(一般数据 1~4 级、重要数据、核心数据)。

关键参数配置主要为：

- 卷积核：3 × 3 深度可分离卷积；
- 激活函数：Hardswish (计算量比 ReLU 低 23%)；
- 模型大小：<2 MB (经模型剪枝后)；
- 数据预处理：对边缘数据(如设备日志、用户行为)进行标准化与增强(添加高斯噪声模拟边缘环境扰动)；
- 联邦学习策略：各省分公司边缘节点本地训练模型聚合参数(每轮聚合阈值 $\Delta = 0.01$)；
- 优化参数：隐私泄露风险与效能效率调优参数(权重 λ 根据业务需要设置权重 0~1 之间取值)。

通过实验，由于集中式 AI 数据分类分级对比轻量级 AI 数据分类分级具有更多的垂直领域模型算力和参数，所以在数据分类分级结果的平均准确率表现相对高 0.9%，出现个人隐私数据泄露风险相对更低 0.23%，但是整体效率上明显差距 10.36 倍，综合评估下来轻量级 AI 数据分类分级保护能力、效能、效率平衡度更佳，后续可以根据边缘数据的业务关注侧重点继续对指标权重进行协调优化(测试数据参见表 1)。

Table 1. Comparison of lightweight AI data classification and grading with centralized AI data classification and grading after collaborative optimization
表 1. 轻量级 AI 数据分类分级优化后与集中式 AI 数据分类分级对比

序号	指标	优化参数	轻量级 AI 数据分类分级	集中式 AI 数据分类分级
1	隐私保护－分类分级准确率	$\lambda 1 = 0.9$	95.20%	96.10%
2	效用评估－数据泄露风险	$\lambda 2 = 0.9$	4.30%	4.07%
3	效率调控－处理延迟(ms)	$\lambda 3 = 0.9$	18.5	210.3

2.3. 轻量级 AI 隐私保护技术的优势与局限性

轻量级 AI 驱动的隐私保护技术具有诸多优势。其模型体积小、计算复杂度低，能够在资源受限的边缘设备上高效运行，满足边缘场景对实时性与低功耗的要求。同时，通过智能分类分级，能够有效提升隐私保护的精准度与灵活性。然而，该技术也存在一定的局限性。首先，轻量级 AI 模型的准确性可能受到数据质量、模型训练程度等因素的影响，从而导致隐私分类结果出现偏差。其次，隐私保护策略的实施可能会增加数据处理的延迟与计算开销，影响边缘数据流通的效率。此外，攻击者可能会通过模型逆向工程等手段，尝试窃取轻量级 AI 模型的参数与结构，进而绕过隐私保护机制[7]。

3. 边缘数据流通场景的轻量级 AI 驱动隐私－效用－效率动态协同优化思路

3.1. 三者协同优化的目标与挑战

在边缘数据流通场景中，隐私保护、数据效用与流通效率的动态协同优化旨在实现以下目标：在确保数据隐私安全的前提下，最大化数据的利用价值，同时提高数据流通的速度与效率，以满足边缘计算应用场景对实时性、准确性和安全性的综合需求。然而，这一过程中面临着诸多挑战。隐私保护措施往往会增加数据处理的复杂性与计算开销，从而降低数据效用与流通效率；而过度追求数据效用与流通效率，又可能导致隐私保护力度不足，增加数据泄露的风险。此外，边缘计算环境的动态性与多样性，使得三者之间的平衡关系难以固定，需要根据不同的应用场景与数据特性进行动态调整。

3.2. 动态协同优化框架的设计原则

为了应对上述挑战，本研究设计的轻量级 AI 驱动优化框架遵循以下原则：一是以用户为中心，充分考虑用户对隐私保护的需求与期望，将隐私保护贯穿于数据流通的全过程；二是注重多维度平衡，通过合理的算法设计与资源分配，实现隐私保护、数据效用与流通效率之间的动态权衡；三是强调灵活性与可扩展性，能够适应不同类型的边缘数据、多样化应用场景以及不断变化的技术环境，便于根据实际需求进行功能扩展与优化。

3.3. 协同优化的关键技术与方法

协同优化的关键技术包括轻量级 AI 模型的优化算法、隐私保护与效用提升的融合策略以及效率调控机制。在轻量级 AI 模型优化方面，采用模型压缩、知识蒸馏等技术，在保证模型性能的基础上进一步降低其计算资源需求；同时，结合边缘计算场景的特点，对模型进行针对性的训练与调优，提高其对边缘数据的分类分级准确性。在隐私保护与效用提升的融合策略上，通过差分隐私、同态加密等技术，在数据处理过程中引入适量的噪声或加密操作，既保护数据隐私，又尽量减少对数据效用的影响；此外，利用数据挖掘与机器学习算法，从海量边缘数据中提取有价值的信息，提升数据效用。在效率调控机制方

面，根据边缘网络的实时状态与数据流量，动态调整数据传输的路由、带宽分配以及任务调度策略，优化数据流通路径，降低传输延迟与计算开销，提高整体流通效率。

4. 边缘数据流通场景的轻量级 AI 驱动隐私－效用－效率动态协同应用

4.1. 智能家居场景中的应用

在智能家居场景中，边缘设备如智能摄像头、智能门锁、智能音箱等会产生大量的用户生活数据。通过部署轻量级 AI 驱动优化框架，对这些数据进行分类分级处理。例如，将包含用户家庭成员图像、语音等敏感信息的数据划分为高隐私级别，采用加密存储与传输方式；而对于环境温度、湿度等一般性数据，则采用较低隐私级别的保护策略。同时，利用轻量级 AI 算法对数据进行分析挖掘，提取用户的生活习惯、行为模式等有价值的信息，为智能家居设备的智能化控制提供依据，提升用户体验。在数据流通效率方面，通过优化框架的效率调控模块，根据家庭网络的实时带宽与设备负载情况，合理安排数据的上传与处理任务，确保智能家居系统的实时响应与流畅运行。智能家居场景中实验数据表现出小规模数据且类型较少情况下，分类分级准确率、数据泄露风险接近，但效率调控方面轻量级 AI 分类分级更具优势(轻量级 AI 数据分类分级从隐私保护、效用评估和效率调控的权重优化后与集中式 AI 数据分类分级测试数据参见表 2)。

Table 2. Application comparison in smart home scenarios
表 2. 智能家居场景中的应用对比

序号	指标	优化参数	轻量级 AI 数据分类分级	集中式 AI 数据分类分级
1	隐私保护－分类分级准确率	$\lambda 1 = 0.8$	99.1%	99.7%
2	效用评估－数据泄露风险	$\lambda 2 = 0.9$	0.06%	0.09%
3	效率调控－处理延迟(ms)	$\lambda 3 = 0.8$	4.5	187.2

4.2. 智能交通场景中的应用

在智能交通领域，边缘计算节点部署在道路沿线、车辆终端等位置，收集车辆行驶数据、路况信息等。该优化框架能够对这些数据进行快速分类分级，识别出涉及车辆车牌号、驾驶员身份等敏感信息，并进行相应的隐私保护处理，如数据脱敏、加密传输等。同时，基于轻量级 AI 模型对交通数据进行实时分析，预测交通流量变化、识别交通拥堵点等，为交通管理部门提供决策支持，提升交通系统的运行效率。在流通效率方面，通过动态调整数据传输的优先级与频率，确保关键交通数据的及时传输与处理，满足智能交通系统对实时性的严格要求。智能交通场景中实验数据表现出大规模数据且类型较多情况下，分类分级准确率、数据泄露风险接近，效率调控方面轻量级 AI 分类分级更具优势(轻量级 AI 数据分类分级从隐私保护、效用评估和效率调控的权重优化后与集中式 AI 数据分类分级测试数据参见表 3)。

Table 3. Application comparison in intelligent transportation scenarios
表 3. 智能交通场景中的应用对比

序号	指标	优化参数	轻量级 AI 数据分类分级	集中式 AI 数据分类分级
1	隐私保护－分类分级准确率	$\lambda 1 = 0.8$	97.4%	98.3%
2	效用评估－数据泄露风险	$\lambda 2 = 0.9$	2.36%	2.19%
3	效率调控－处理延迟(ms)	$\lambda 3 = 0.9$	2.1	167.9

4.3. 工业自动化场景中的应用

在工业自动化场景下，大量的传感器设备分布在生产线上，采集设备运行状态、生产过程参数等数据。轻量级 AI 驱动优化框架对这些工业数据进行分类分级管理，将涉及企业核心技术、生产工艺等敏感数据进行严格保护，防止数据泄露导致的商业损失。同时，利用轻量级 AI 算法对工业数据进行深度分析，实现设备故障诊断、生产过程优化等功能，提升企业的生产效率与产品质量。在数据流通效率方面，根据工业生产流程的实时需求与网络状况，优化数据的采集、传输与处理流程，确保生产系统的稳定运行与高效协同。工业自动化场景中实验数据表现出大规模数据且类型较少情况下，分类分级准确率、数据泄露风险接近，但效率调控方面轻量级 AI 分类分级更具优势(轻量级 AI 数据分类分级从隐私保护、效用评估和效率调控的权重优化后与集中式 AI 数据分类分级测试数据参见表 4)。

Table 4. Application comparison in industrial automation scenarios
表 4. 工业自动化场景中的应用对比

序号	指标	优化参数	轻量级 AI 数据分类分级	集中式 AI 数据分类分级
1	隐私保护－分类分级准确率	$\lambda 1 = 0.9$	99.2%	99.8%
2	效用评估－数据泄露风险	$\lambda 2 = 0.8$	0.11%	0.05%
3	效率调控－处理延迟(ms)	$\lambda 3 = 1.0$	1.5	172.9

5. 研究成果创新特点和价值

5.1. 创新特点

本研究的创新特点主要体现在以下几个方面：

提出了一种基于轻量级 AI 数据分类分级的隐私－效用－效率动态协同优化框架，该框架能够有效整合隐私保护、数据效用提升与流通效率优化三大目标，实现了三者之间的动态平衡，填补了现有研究在边缘数据流通场景下多目标协同优化领域的空白。

在隐私保护技术方面，创新性地将轻量级 AI 与差分隐私、同态加密等技术相结合，通过智能分类分级实现精准的隐私保护，既提高了隐私保护的效率，又降低了对数据效用的影响，相较于传统的隐私保护方法具有显著的优势。

针对边缘计算环境的动态性与复杂性，设计了灵活的效率调控机制，能够实时感知边缘网络与设备的状态变化，并据此动态调整数据流通策略，有效提升了边缘数据流通的整体效率，为边缘计算场景下的数据管理提供了新的思路与方法。

5.2. 研究价值

从理论价值来看，本研究拓展了边缘计算、数据安全与隐私保护领域的研究边界，为相关领域的学术研究提供了新的理论依据与方法指导。通过深入分析边缘数据流通场景中的隐私－效用－效率关系，构建了系统的协同优化理论体系，有助于推动该领域的理论发展与创新。

从实践价值而言，本研究成果为通信行业在边缘数据流通安全管理方面提供了切实可行的解决方案。在实际应用中，该优化框架能够有效降低边缘数据的隐私泄露风险，提升数据的利用价值与流通效率，从而提高通信企业的数据管理水平与服务质量，增强企业在数字化时代的市场竞争力。同时，该研究成果也为其他行业的边缘数据流通安全管理提供了借鉴与参考，具有广泛的应用前景与社会经济效益。

6. 总结及展望

6.1. 研究总结

本文围绕边缘数据流通场景中的隐私–效用–效率动态协同优化问题展开深入研究，提出了轻量级AI驱动的优化框架，并对其进行了系统的阐述与验证。首先，分析了边缘数据流通面临的隐私风险以及现有技术的局限性，进而设计了基于轻量级AI数据分类分级的隐私保护技术方案。接着，在综合考虑隐私保护、数据效用与流通效率三者关系的基础上，构建了动态协同优化框架，详细介绍了框架的设计原则、关键技术以及模块功能实现。通过在智能家居、智能交通、工业自动化等多个典型场景的应用案例分析，验证了该框架在实际应用中的有效性与优势。最后，总结了本研究成果的创新特点与价值，强调了其在理论研究与实践应用方面的重要意义。

6.2. 研究展望

尽管本研究取得了一定的成果，但仍存在一些值得进一步深入探索的方向：

1、随着边缘计算技术的不断发展以及数据规模的持续增长，轻量级AI模型的性能优化仍是一个长期的研究课题。未来需要进一步探索5G更加高效、精准的轻量级AI算法，以适应复杂多变的边缘数据特性与大规模数据处理需求[8]。

2、在隐私保护技术方面，面对日益复杂的攻击手段与隐私威胁，如何不断提升隐私保护机制的安全性与可靠性，同时降低其对数据效用与流通效率的影响，是一个需要持续关注与解决的问题。例如，研究新型的加密算法、隐私保护协议以及与区块链等新兴技术的融合应用，以进一步增强边缘数据流通的隐私安全保障。

3、边缘数据流通场景的多样性和动态性要求优化框架具备更强的自适应能力与智能化水平。未来可以考虑引入强化学习、深度学习等先进的人工智能技术，使优化框架能够更加智能地感知环境变化，自动调整隐私保护策略、数据效用提升方法以及流通效率优化方案，实现更加精细化、个性化的协同优化管理[9]。

4、从跨领域的角度出发，进一步拓展轻量级AI驱动隐私–效用–效率动态协同优化框架的应用范围。例如，在智能医疗、智能金融等领域，针对其独特的数据特点与业务需求，探索适合的优化策略与技术方案，推动该研究成果在更广泛的行业领域中落地应用，为数字社会的建设与发展提供更加有力的技术支撑。

参考文献

[1] 马敏, 付钰, 黄凯, 贾潇风. 基于秘密共享的轻量级隐私保护ViT推理框架[J]. 通信学报, 2024, 45(4): 27-38.

[2] 李亚国, 李冠良, 张凯, 晋涛. 基于人工智能与边缘代理的物联网框架设计[J]. 计算机工程, 2023, 49(10): 313-320.

[3] 张依琳, 陈宇翔, 田晖, 王田. 联邦学习在边缘计算场景中应用研究进展[J]. 小型微型计算机系统, 2021, 42(12): 2645-2653.

[4] 张再峰. 基于隐私计算的数智化平台架构设计及关键技术探究[J]. 中国信息界, 2024(1): 115-118.

[5] 张翀. 边缘计算与云协同问题研究[J]. 通讯世界, 2023, 30(12): 178-180.

[6] 吴薇薇. 基于5G网络的边缘计算与人工智能协同分析[J]. 集成电路应用, 2024, 41(6): 196-197.

[7] 涂聪, 陈庆奎. 面向AI数据流处理的边缘GPU集群通信系统[J]. 小型微型计算机系统, 2022, 43(6): 1147-1153.

[8] 尹晓丹. 5G边缘计算技术及应用展望[J]. 通讯世界, 2024, 31(2): 175-177.

[9] 郑令晗, 李晨珂. 面向AI4S的数据要素供给: 价值取向、路径选择与风险控制[J]. 图书与情报, 2024(3): 81-89.