低空经济背景下 AI 大模型的数据安全与隐私增强机制研究

谢统薇[1] 张希坤[2*] 侯燕[3]

（1.郑州工程技术学院，河南 郑州 450044；2.天津大学，天津 300000；3.郑州工程技术学院，河南 郑州 450044）

摘 要：低空经济的国家战略推进与 AI 大模型的深度融合，凸显了数据安全与隐私保护的核心价值。针对现有研究技术与经济管理适配不足、中小企业差异化需求被忽视的问题，本文构建“技术-管理-经济”协同增强框架，提出“源头防控-过程管控-后端保障-动态优化”全链条机制，结合轻量化分级防护、跨主体治理与场景适配策略，实现安全、效率与成本的动态平衡。基于 12 家低空物流企业的实证验证表明，该机制可将隐私泄露风险降至 0.08%，合规成本降低 35%，训练数据覆盖率提升至 92%。研究为不同规模主体提供梯度化方案，完善了低空经济数据治理理论，为产业高质量发展提供实践支撑。

关键词：低空经济；AI 大模型；数据安全；隐私增强；协同机制；成本优化

一、引言

新一轮科技革命与产业变革纵深推进，低空经济作为战略性新兴产业的战略地位持续凸显。从深圳“空中出租车”商业化试点、湖南全域低空开放改革落地，到 2023 年中央经济工作会议明确其国家战略定位，低空经济已实现从概念探索到战略落地的跨越式发展。预计 2026 年产业规模将突破万亿元，成为驱动经济高质量发展的重要增长，其产业链涵盖飞行器制造、空域运营、数据服务等多元领域，形成多主体协同共生的产业生态格局[1]。

人工智能大模型凭借卓越的多源异构数据处理能力，在飞行器自主决策、空域资源优化调度等核心场景中发挥关键支撑作用，是激活低空经济数据要素价值的核心引擎[2]。但低空运营产生的飞行轨迹、地理信息、用户需求等敏感数据，兼具隐私属性与战略价值，在 AI 大模型采集、训练、应用全生命周期中，面临数据泄露、权属纠纷、算法滥用等多重安全挑战。此类风险不仅危及个人隐私与国家空域安全，更推高企业合规成本、加剧数据要素流通壁垒，制约产业链协同效率与价值释放。

现有研究存在显著的理论与实践脱节问题：一方面，文献多聚焦单一技术路径优化或宏观产业分析，缺乏对隐私增强技术在低空经济场景中经济可行性与成本收益比的系统性探讨[3]。另一方面，技术方案忽视低空经济多主体（监管机构、运营企业、技术服务商）协同特征与差异化需求，难以适配不同规模主体的运营实际。这一研究缺口使企业尤其是中小运营主体，在技术选型、合规实践与成本控制中陷入困境，不利于产业生态均衡发展。

本研究突破“技术孤岛”认知，构建融合技术可行性、经济合理性与管理有效性的协同增强框架，核心贡献在于提出并验证适配低空经济产业特征的系统化解决方案，通过整合隐私增强技术与经济管理机制，搭建安全防护与产业效率兼顾的落地路径。研究从理论层面完善“技术-经济-管理”跨学科治理体系，方法论层面建立多维度（安全、效率、经济）评估范式，实践层面为不同规模主体提供梯度化实施方案，助力实现数据价值最大化，赋能低空经济高质量可持续发展。

二、文献综述

基金项目：2026 年度河南省高等学校重点科研项目“双轮驱动下河南省校企研发中心协同创新机制与高质量发展路径研究”（项目编号：26B630028）；郑州工程技术学院重点学科建设项目资助。

作者简介：谢统薇（1989-），女，讲师，博士，研究方向为人工智能教育和机器学习。
侯 燕（1982-），女，副教授，硕士，研究方向为创新生态与科技治理。
通讯作者：张希坤（1981-），男，副教授，博士，研究方向为企业数字化。

2.1 低空经济与 AI 大模型融合的研究现状与挑战

低空经济向“物理—社会—信息”三元空间深度拓展，预计 2026 年产业规模突破万亿元，成为推动区域协调发展、带动产业链升级的核心引擎。这一发展态势对多源异构数据整合利用与复杂决策支持提出迫切需求，为 AI 大模型规模化应用提供了广阔场景。现有研究证实，AI 大模型在飞行器自主调度、空域资源优化配置、运营风险预警等关键环节的应用，可显著提升低空运营效率、降低边际成本，为产业赋能效果显著[4]。

但当前研究存在明显应用断层，多数文献聚焦单一技术路径优化或特定场景解决方案，缺乏对数据安全与隐私保护的系统性考量，尤其忽视技术应用的经济成本与管理适配性。这一研究局限直接制约 AI 大模型在低空经济中的规模化落地，在多主体协同、跨境数据流动、中小企业适配等复杂场景中，现有方案难以平衡安全防护、运营效率与成本控制的三重需求，成为阻碍产业协同发展的核心瓶颈。

2.2 低空 AI 大模型的数据安全与隐私风险研究

低空 AI 大模型面临的数据安全挑战具有多维特征与产业链传导效应。从数据属性看，低空数据涵盖地理信息、用户轨迹、商业机密等高敏感内容，其产生与处理贯穿多环节、涉及多主体，导致数据权属界定模糊、责任划分困难。现有研究虽已识别出全生命周期潜在漏洞，但多停留在风险识别层面，缺乏对风险沿产业链传导的经济影响机制分析，尤其缺乏对合规成本攀升、产业链协同效率下降等后果的量化研究，直接限制了针对性防护策略与风险管控机制的构建，难以形成适配产业特征的风险评估与应对体系[5]。

隐私保护领域核心存在双重矛盾，即数据流通利用与隐私安全防护的平衡矛盾、技术方案有效性与经济可行性的适配矛盾。低空经济的产业特殊性进一步加剧了这两组矛盾，既要通过数据共享激活产业链协同价值、满足合规要求，又受限于不同规模主体的成本承受能力，难以兼顾高强度防护与经济性。现有技术方案普遍存在供需错配，传统防护技术无法适配低空运营实时性需求，新型隐私计算技术则面临部署成本高、运维难度大的问题，且现有研究对中小企业等成本敏感型主体的差异化需求关注不足，缺乏兼顾安全与成本的梯度化方案，不利于产业生态均衡发展[6]。

2.3 隐私增强技术的应用研究现状与局限

隐私增强技术研究呈现分层特征，基础技术部署简便但防护强度有限，高阶技术安全性更优但经济成本较高[7]。现有研究对单一技术特性分析较为充分，却忽视技术协同效应与产业适配性，面对低空经济多样化场景与多主体需求，单一技术方案难以满足差异化诉求，而技术组合优化配置、成本分摊机制等关键问题的研究相对匮乏。此外，现有研究多聚焦技术本身优化，缺乏从产业治理、成本控制、合规管理视角的系统工程考量，导致技术方案落地推广难度大，与产业实际需求脱节。

系统梳理文献后发现，现有研究存在三大核心局限：一是研究视角单一，缺乏经济学视角的技术适配性与成本收益分析，导致技术方案与企业实际承受能力失衡；二是方案设计缺乏场景针对性与主体差异化考量，难以实现精准防护与成本优化；三是防护体系碎片化，未与产业治理、合规管理深度融合，无法应对复杂安全威胁与监管要求。这些局限严重制约技术应用效果，难以支撑低空经济规范化发展。基于此，本研究确立应用导向定位，核心贡献在于构建“技术—管理—场景”协同框架、建立多维度（安全、效率、经济）评估方法、设计差异化实施路径与成本分摊机制，填补系统性解决方案空白，通过技术与业务、管理的深度融合，为产业实践提供可行参考。

三、研究设计与方法

3.1 研究框架与方法论

本研究采用设计科学研究范式，遵循“问题识别-方案设计-评估验证”的逻辑脉络，系统性开展低空经济背景下 AI 大模型数据安全与隐私增强机制研究。研究先通过文献分析与产业调研，明确低空经济中 AI 大模型数据安全的核心挑战及不同主体的差异化需求；再构建融合技术防护、管理治理与成本优化的协同增强框架，重点搭建适配产业特征的成本分摊与合规管理机制；最终通过多案例实证研究，从安全、效率、经济三维度验证框架的有效性与实用性。

3.2 研究数据收集与处理

研究采用多源数据三角验证法，从三方面采集数据以兼顾权威性、实用性与代表性：一是宏观行业数据，涵盖 2018-2023 年低空经济产业规模、无人机保有量、合规成本等指标，源自中国民航局、工信部等官方年报及行业报告，为产业分析与经济可行性评估提供支撑；二是企业运营数据，通过分层抽样选取 12 家代表性低空物流企业（3 家大型、5 家中型、4 家小型），采集日均配送量、运营成本、合规投入等核心数据，精准捕捉不同规模主体需求；三是实验数据集，基于真实场景生成多模态敏感数据集，覆盖不同敏感级别与应用场景，为安全效果与运营效率评估奠定基础。

为保障数据质量与研究规范性，采用系统化处理流程：先开展数据清洗与异常值剔除，确保数据准确性；再由 5 名跨领域专家（2 名低空运营专家、2 名数据合规专家、1 名经管专家），依据《低空数据分类分级指南》完成数据敏感度标注与合规校验[8]。最后对隐私及商业机密信息脱敏处理，符合伦理与法规要求，并通过数据校验、交叉验证建立严格质量控制机制，保障数据可靠性。

3.3 协同增强框架构建方法

基于系统工程理论与产业需求，本研究构建多层次自适应协同增强框架，遵循四大原则：隐私保护优先筑牢合规底线，性能效率平衡降低运营影响，成本适配性保障方案落地，可扩展性支撑产业升级[9]。框架采用“技术防护-管理治理-成本优化”三位一体架构，包含数据采集防护、安全协同处理、全流程管理、动态优化四大模块，通过标准化接口联动，既实现全环节安全防护，又依托管理机制与成本分摊方案，破解技术落地的管理与成本瓶颈，适配多主体协同特征。

技术层面整合隐私增强技术，构建轻量化协同防护体系，聚焦实用性与经济性，避免过度追求技术复杂度。管理层面配套多主体协同治理、分级合规管理及成本分摊机制，明确权责边界与合作模式，依托智能合约与区块链实现责任追溯，并按业务规模、受益程度设计梯度化成本分摊方案，降低中小企业落地门槛[10]。

3.4 评估验证方案设计

实验环境部署于云平台，满足低空运营实时性与稳定性需求。评估体系围绕经管类期刊核心关切，构建三大维度 12 项指标的综合体系：安全防护类（权重 0.45）衡量合规与防护效果，数据利用类（权重 0.30）评估数据价值释放效率，经济成本类（权重 0.25）验证方案经济性。采用对照组实验设计，实验组应用本研究协同框架，对照组采用传统集中式及单一隐私保护方案，实验周期 6 个月，通过 A/B 测试、安全与效率测试、成本效益分析，结合用户调研与专家评审，确保评估结果全面可靠。

3.5 数据分析与验证方法

采用定量与定性结合的混合研究方法：定量分析依托 SPSS 26.0 与 Python 工具，通过描述性统计、假设检验、相关性及回归分析量化框架表现，显著性水平 $\alpha=0.05$；定性分析通过专家访谈、案例研究挖掘框架应用效果与局限。为保障结果可靠性，采用交叉验证、重采样等方法验证统计结论稳定性，确保研究结论科学可信。

四、AI 大模型数据安全与隐私增强协同机制构建

在低空经济快速发展与多主体协同的产业背景下，AI 大模型安全部署面临安全防护、运营效率、成本控制三重挑战。本文提出“源头防控-过程管控-后端保障-动态优化”全链条协同机制，通过技术协同、管理协同、成本协同与场景适配的深度融合，实现数据安全、产业效率与经济可行性的动态平衡，既满足多主体数据利用需求，又为个人隐私、企业利益和国家安全提供坚实保障，适配低空经济高质量发展核心诉求，具体机制如下图 1 所示：

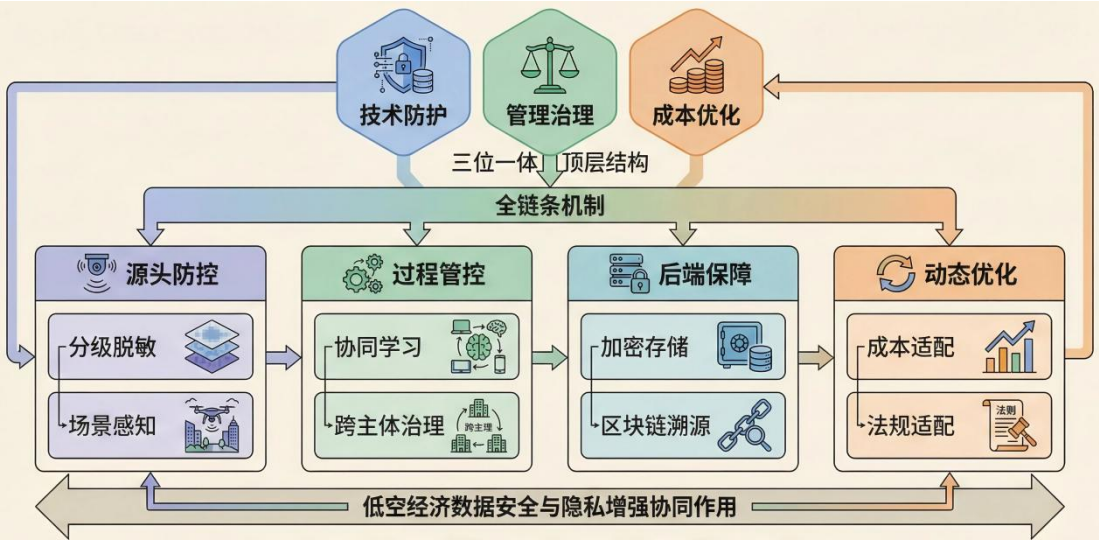

图 1 低空经济 AI 大模型数据安全与隐私增强协同框架

4.1 技术协同机制：轻量化分级防护体系

本文构建的轻量化分级防护体系，采用“分层防御、场景适配”架构，形成覆盖“数据采集-处理-传输-存储”全流程的防护链条，核心聚焦技术实用性与成本可控性，规避过度技术化设计，适配低空经济运营场景与企业实际能力。

数据采集端以分级防护与源头管控为核心，基于数据敏感度分级与场景风险评估实施差异化策略，平衡安全与采集效率。针对无人机、地面传感器等异构设备部署轻量化防护模块，对人脸、车牌、关键地理坐标等敏感信息实时脱敏，从源头降低泄露风险。引入场景感知机制，根据采集环境风险等级自动调整防护强度与数据精度：低风险场景采用基础防护保障效率，高风险场景启用强化防护，通过控制数据粒度、加强设备身份认证提升防护等级，结合硬件安全认证与空间范围控制，筑牢源头防线。

处理中端采用协同学习与隐私保护融合的技术路线，实现“数据不动价值动”，破解数据孤岛与隐私保护的矛盾[11]。构建分布式协同训练架构，各主体在本地完成模型训练，仅传输加密模型参数，避免原始数据跨主体流动。针对不同规模主体技术能力差异，配置梯度化技术方案：大型企业部署完整功能模块，中小企业采用简化版架构，降低技术门槛与运维成本；同时通过参数优化与流程简化，在保障隐私安全的前提下最小化对运营效率的影响，适配主体差异化能力。

后端保障层构建覆盖传输、存储、溯源的全链路安全体系，配套管理机制实现责任可追溯。传输环节按数据敏感等级采用差异化加密方案，平衡安全与效率；存储环节实施分布式加密存储与备份策略，防范数据丢失与篡改；引入区块链技术记录全量数据操作，实现生命周期可追溯[12]。该体系既为安全事件追责提供支撑，又简化合规审计流程、降低合规成本，形成技术与管理融合的后端保障闭环。

4.2 管理协同机制：跨主体治理与动态合规框架

为保障技术方案在复杂产业生态中落地，构建跨主体协同治理与动态合规框架，通过责任界定、流程规范、监管响应的有机整合，形成与技术体系配套的管理支撑，实现“技术-管理-治理”三位一体协同，破解多主体权责纠纷与合规难题。

多主体协同治理体系基于“数据权责对等”原则，明确监管机构、运营企业、技术服务商等各方权责边界：采集方对设备安全、数据质量与隐私保护负责，处理方承担算法合规与过程管控责任，使用方恪守数据授权范围，监管机构负责规则制定、监督执法与风险预警。搭建跨部门协同治理平台，实现威胁情报共享、异常行为协同处置与合规信息互通，依托智能合约将权责关系数字化映射与自动化执行，解决责任虚化问题；建立多方协商机制，就数据权属、共享边界等核心问题形成共识，平衡各方利益。

全生命周期合规管理规范以标准化流程为核心，确保各环节符合《网络安全法》《数据安全

法》等法规要求[13]。建立“公开-敏感-涉密”三维数据分类体系，实施差异化管理策略；模型开发阶段引入隐私影响评估机制，遵循“最小必要”原则控制数据访问权限，确保操作可追溯可审计；建立数据销毁认证制度，通过标准化流程与自动化工具降低合规成本，为中小企业提供清晰指引。

智能监管与自适应响应机制依托大数据构建智能监管平台，实时监测数据流异常行为，通过多维度指标动态识别威胁与合规风险。建立分级响应机制：轻微事件自动处置降低运维成本，重大事件启动跨部门应急机制快速控险。采用“平战结合”理念，日常通过演练优化策略，应急状态下依托预案库高效响应；建立闭环优化机制，沉淀应急经验并动态调整监管规则，适配技术演进与法规更新，提升管理体系韧性。

4.3 场景适配机制：分级动态防护与成本优化

针对低空经济多场景差异化需求与主体成本敏感度，构建基于风险评估的分级动态防护体系，结合成本分摊与梯度化方案，解决传统“一刀切”模式的防护失衡、成本过高问题，实现安全投入精准化。

低敏感场景（农业监测、普通物流等）采用“效率优先、成本可控”的轻量化方案，适配中小企业资源约束。采集层仅对核心敏感字段基础脱敏，处理层采用简化版协同学习架构，传输存储层选用标准化加密算法；案例显示，该方案在无人机物流场景中可提升系统吞吐量 40%，降低运维成本 25%以上，以低成本满足基础安全与合规需求。

中敏感场景（城市交通调度、商业测绘等）采用“安全与效率并重”的均衡方案，适配中等规模企业核心场景。预处理阶段实施特征级脱敏保留数据价值，训练阶段融合协同学习与隐私保护技术，数据交换环节兼顾加密传输与操作存证。在城市低空交通管理场景中，该方案实现多部门数据安全协同，既规避隐私泄露，又提升空域资源利用率，合规成本较高阶方案降低 30%，实现三维平衡。

高敏感场景（军事监测、跨境数据流动等）构建“安全优先”的强化防护体系，适配大型企业与涉密需求。全环节实施深度防御，配套严格的访问控制、身份认证与审计机制；虽较其他模式增加 15%运营成本，但数据泄露风险降至万分之一以下，符合高敏感场景要求。针对跨境场景，额外配套合规评估机制，结合目的地法规设计脱敏、本地化存储方案，规避跨境合规风险。

4.4 动态优化机制：自适应演进与成本管控

设计基于反馈循环的自适应优化框架，通过技术迭代、管理调整、成本优化与效果评估的三重闭环，实现机制体系动态演进，兼顾长期有效性与经济可行性。

技术与管理自适应演进依托威胁情报与法规监测双驱动：构建行业安全威胁知识库，结合机器学习预测威胁趋势，实现主动防御；搭建全球法规动态监测平台，跟踪立法动向并生成合规调整建议。技术层面动态优化配置，布局新型隐私保护技术；管理层面调整治理规则与合规流程，将新威胁、新法规响应时间缩短至 12 小时内，提升体系适应性。

成本策略动态优化构建“成本-效益”评估机制，结合运营数据调整分摊方案与技术配置。为中小企业提供基础版、进阶版梯度方案，降低初期投入 30-50%；基于业务规模、受益程度、风险承担比例动态调整分摊比例，避免成本失衡；建立成本节约共享机制，激励各方参与协同建设，形成良性循环[14]。

多维度持续评估以安全、效率、经济为核心指标，建立常态化评估机制：安全维度监测泄露发生率、攻击阻断率，效率维度跟踪吞吐量、响应延迟，经济维度核算总拥有成本、投资回报率。采用自动化监测与专家评审结合的方式，每季度开展深度评估，通过层次分析法确定指标权重，形成“评估-分析-优化-验证”闭环。某低空物流联盟实践显示，6 个月内隐私泄露风险降低 95%，运营效率提升 28%，合规成本下降 22%，验证了优化机制有效性。

五、机制应用效果验证

5.1 验证背景与基准设定

本研究选取某区域低空物流联盟作为实证对象，该联盟由 12 家物流企业构成，含 3 家大型企业、5 家中型企业及 4 家小型企业，业务覆盖 3 省 8 市经济区，日均完成无人机配送约 2 万单，月均产生多维度异构数据约 15TB。其业务场景多元、主体类型丰富，兼具强烈的数据共享需求与

隐私保护诉求，在成本承受能力、合规需求等方面贴合行业普遍特征，可全面检验机制对不同规模主体的适配性，具备充分的实证代表性。

验证过程严格遵循三大核心约束以贴合产业实际：一是安全约束，在保障业务数据共享的同时，将敏感数据泄露风险控制在≤0.15%的行业标准内，确保满足合规要求；二是效率约束，机制应用不得对现有运营效率产生显著负面影响，保障业务正常开展；三是成本约束，严格控制合规与技术投入成本，核心企业成本增幅不超过年度运营成本的 5%，中小企业成本增幅不超过年度运营成本的 3%，适配不同主体成本承受能力。

本研究构建包含安全防护、数据利用、经济成本三大类 12 项指标的综合评估体系，采用层次分析法确定各指标权重，突出经济管理维度的评估价值以契合期刊定位。其中安全防护类权重 0.45，涵盖隐私泄露发生率（权重 0.15，取值范围 0-100%，越优值越小）、数据篡改抵御率（权重 0.12，取值范围 0-100%，越优值越大）、合规审计通过率（权重 0.10，取值范围 0-100%，越优值越大）、访问控制准确率（权重 0.05，取值范围 0-100%，越优值越大）、溯源定位准确率（权重 0.03，取值范围 0-100%，越优值越大）；数据利用类权重 0.30，涵盖训练数据覆盖率（权重 0.10，取值范围 0-100%，越优值越大）、模型预测准确率（权重 0.10，取值范围 0-100%，越优值越大）、共享响应速度（权重 0.10，单位为秒，越优值越小）；经济成本类权重 0.25，涵盖合规投入成本（权重 0.08，单位为万元，越优值越小）、系统运维成本（权重 0.07，单位为万元，越优值越小）、配送成本降幅（权重 0.06，取值范围 0-100%，越优值越大）、客户满意度（权重 0.04，取值范围 0-100%，越优值越大）。

5.2 实施框架与技术方案

本研究构建“三层协同+三维保障”技术架构，覆盖数据采集、传输、训练及存储全流程，集成轻量化脱敏、协同学习与区块链溯源技术，实现数据“可用不可见”的核心目标。同时配套三大管理机制形成技术与管理的深度融合：一是多主体协同治理机制，明确各参与方权责边界以规避纠纷；二是梯度化成本分摊机制，平衡不同规模企业成本负担；三是动态合规管理机制，实时适配法规更新需求，保障机制长效合规。

技术参数配置聚焦实用性与成本可控性，核心目标明确：数据脱敏模块确保信息替换准确率不低于 98.5%，同时将处理延迟控制在 80 毫秒以内，满足业务实时运营需求；协同学习采用横向联邦架构适配分布式场景，迭代周期设定为 4 小时/次，在保障时效性的同时合理控制资源消耗；区块链模块部署 15 个共识节点强化安全性，上链时间控制在 5 秒以内实现数据实时溯源，避免过度技术配置导致成本攀升。

本次实证项目采用“分级分摊+收益共享”模式兼顾公平性与激励性。核心企业因业务规模大、受益程度高，承担 35%的总成本；中小企业按业务量比例分摊剩余 65%成本，平均每家中小企业成本较均摊模式降低约 40%，显著降低其落地门槛。同时建立收益分配机制，将机制应用带来的运营成本节约（含配送成本降幅、效率提升转化收益等），按成本分摊比例与实际贡献度在各企业间分配，激励中小企业积极参与，构建“成本共担、收益共享”的良性产业生态。

5.3 效果评估与分析

经过 6 个月实证验证，协同机制在安全防护维度表现优异，各项指标均优于传统方案且满足行业合规标准。其中隐私泄露发生率降至 0.08%，较传统方案的 1.25%降低 93.6%，有效管控核心安全风险；数据篡改抵御率达 98.5%，较传统方案的 75.5%提升 23.0 个百分点，充分保障数据完整性；合规审计通过率提升至 95.2%，较传统方案的 80.5%提升 14.7 个百分点，显著降低企业合规风险，筑牢运营安全防线，具体如下图 2 所示：

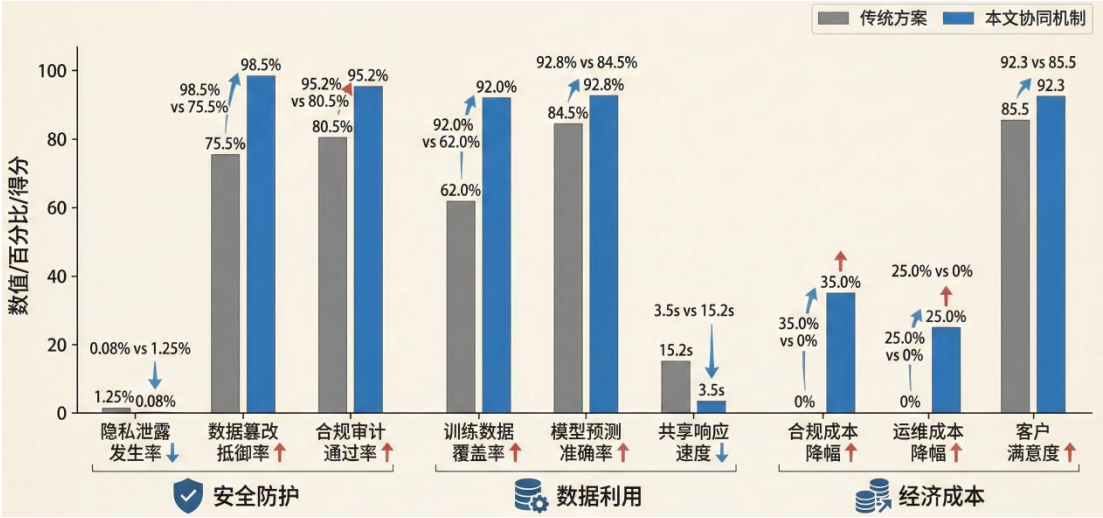

图 2 低空经济 AI 大模型协同机制与传统方案的效果对比

数据利用效率维度，协同机制有效打破数据孤岛，激活数据要素价值。训练数据覆盖率从传统方案的 62.0%提升至 92.0%，增幅 30.0 个百分点，为 AI 大模型优化提供更全面的数据支撑；模型预测准确率从 84.5%提升至 92.8%，增幅 8.3 个百分点，显著提升运营决策科学性；共享响应速度从 15.2 秒缩短至 3.5 秒，提升幅度达 77.0%，充分满足业务实时性需求，实现数据安全与利用效率的双重优化。

经济效益层面，协同机制通过技术优化与管理创新实现成本显著降低、收益稳步提升。合规投入成本从每年 82.5 万元降至 53.6 万元，降幅 35.0%，大幅减轻企业合规负担；系统运维成本从每年 45.2 万元降至 33.9 万元，降幅 25.0%，提升运营效率；客户满意度从 85.5%提升至 92.3%，增幅 6.8 个百分点，助力企业增强市场竞争力。从主体差异来看，大型企业通过数据共享与效率提升，年均新增收益约 50 万元；中小企业借助梯度化方案与成本分摊机制，合规与运维成本合计降低 40%以上，实现成本与风险的双重管控，验证了机制对不同规模主体的适配性与经济可行性。

基于前述评估指标体系及权重计算，协同机制综合得分 85.6 分，较传统方案的 58.2 分提升 27.4 分，在安全、效率、经济三大维度实现均衡且显著的改善。其中安全防护维度得分 88.2 分，数据利用维度得分 86.5 分，经济成本维度得分 81.3 分，整体表现稳健。实证结果充分表明，该协同机制既能有效提升低空 AI 大模型的数据安全与合规水平，又能通过数据共享与效率优化激活数据要素价值，同时依托成本分摊与管理创新降低企业运营成本，适配低空经济多主体、差异化的产业特征，为产业高质量发展提供有力支撑。

六、结论与展望

6.1 研究结论

本研究针对低空经济场景下 AI 大模型数据安全与隐私保护需求，构建融合技术防护、管理治理与成本优化的协同增强框架，经实证验证可实现数据安全、产业效率与经济可行性的动态平衡，适配低空经济多主体、多场景特征。安全层面，轻量化分级防护机制将隐私泄露风险控制在 0.08%行业标准内，数据篡改抵御率达 98.5%，筑牢合规底线；效率层面，在保障隐私前提下实现 92%训练数据覆盖率与 92.8%模型预测准确率，有效打破数据孤岛；经济层面，助力企业合规成本降低 35%、运维成本下降 25%，梯度化分摊方案降低中小企业落地门槛，推动主体均衡发展。

6.2 理论贡献与实践意义

理论上，本研究突破单一技术路径局限，构建“技术-管理-经济”跨学科协同框架，完善低空经济数据治理理论体系；建立安全、效率、经济多维度评估体系，丰富技术经济学在新兴产业的应用；设计动态优化机制，为新技术长期适配提供理论支撑。实践中，为不同规模主体提供差异化方案，促进产业生态均衡；为监管机构提供治理参考，助力构建适度监管、激励创新的环境；破解数据壁垒，提升产业链协同效率，推动产业规模化规范化发展。需说明的是，框架效果受实

施环境、技术基础等因素影响，实际应用需针对性调整，不可简单套用。

6.3 局限性与未来研究方向

本研究存在三方面局限：实证验证集中于低空物流场景，在应急救援、城市管理等场景的适用性待进一步验证；框架对主体技术与管理基础有要求，在基础薄弱中小企业落地易遇阻力；量子计算等新技术对现有隐私保护技术构成潜在挑战，框架需持续演进。未来将从三方面拓展：拓展应用场景，优化适配机制提升普适性；深化成本优化研究，设计简化低成本方案并配套指引，降低中小企业实施门槛；融合边缘计算、后量子密码等新技术，探索跨域数据共享与跨境合规机制，助力框架适配产业发展与技术变革需求。

参考文献：

[1]汤凯,孙植华.低空经济政策赋能城市新质生产力的机制研究——基于国家通用航空区与无人驾驶航空区的准自然实验[J/OL].新疆师范大学学报(哲学社会科学版),2026(1):1-20.
[2]兰旭东.低空经济的核心优势与趋势前瞻[J].人民论坛,2025(23):35-40.
[3]庄茁.人工智能赋能低空经济：应用场景与未来方向[J].人民论坛·学术前沿,2024(15):38-44.
[4]王珏,贺姝荣.人工智能时代的低空经济监管：基于新制度经济学视角[J/OL].商业经济与管理,2026(1):1-8.
[5]苏志远,赵利绪,郝志恒,等.低空经济背景下人工智能保障eVTOL飞行安全综述[J].计算机科学,2025,52(S1):177-189.
[6]杨骏,李长健.生成式人工智能助推低空经济的实践研判、风险识别及制度应对[J].当代经济管理,2025,47(03):77-86.
[7]褚鹏,王军,刘树光,等.基于人工智能技术的低空飞行器管控关键技术研究[J].航空兵器,2023,30(02):120-124.
[8]郑凌霄,唐欣,曹先彬,等.面向场景化AI的空地一体信息网能力架构与关键技术[J/OL].无线电通信技术,2026(1):1-10.
[9]喻鹏,谭灿,李文璟,等.数字孪生驱动的低空智联网自智管控架构及关键技术[J].中国科学：信息科学,2025,55(10):2449-2470.
[10]蔡芳,刘智珺.基于区块链和AI的农机导航数据处理技术研究[J].农机化研究,2022,44(11):211-215.
[11]张珺皓,郭栋.低空经济产业发展的法治保障研究[J].重庆社会科学,2025(11):138-152.
[12]杨琴.低空经济助力新质生产力培育的核心路径、现实约束与破局之策[J].管理现代化,2025,45(03):1-9.
[13]苏美文,杨文爽,李博文,等.推动人工智能与实体经济深度融合加快发展新质生产力[J].工业技术经济,2025,44(04):32-59.
[14]林旭,刘涛,张诗壮,等.通感低空覆盖关键技术与组网[J].中兴通讯技术,2025,31(01):53-57.

Research on Data Security and Privacy Enhancement Mechanisms of AI Large Models in the Context of Low-Altitude Economy

XIE Tongwei[1], ZHANG Xikun[2]*, HOU Yan[3]

(1. Zhengzhou University of Technology, Zhengzhou, Henan 450044, China; 2. Tianjin University, Tianjin 300000, China; 3, Zhengzhou University of Technology, Zhengzhou, Henan 450044, China)

Abstract: The advancement of low-altitude economy as a national strategy and its in-depth integration with AI large models have highlighted the core value of data security and privacy protection. Addressing the issues of inadequate adaptation between existing research technologies and economic management, as well as the neglect of differentiated needs of small and medium-sized enterprises, this paper constructs a "technology-management-economy" collaborative enhancement framework and proposes a full-chain mechanism of "source prevention-process control-backend guarantee-dynamic optimization". Integrating lightweight hierarchical protection, cross-subject governance and scenario-adaptive strategies, the framework achieves a dynamic balance among security, efficiency and cost. Empirical verification based on 12 low-altitude logistics enterprises shows that the mechanism can reduce the risk of privacy leakage to 0.08%, cut compliance costs by 35%, and increase training data coverage to 92%. This research provides gradient solutions for subjects of different scales, improves the theoretical system of low-altitude economy data governance, and offers practical support for the high-quality development of the industry.

Keywords: Low-altitude economy; AI large models; Data security; Privacy enhancement; Collaborative mechanism; Cost optimization