E-Commerce Letters 电子商务评论, 2026, 15(9), 695-704
Published Online September 2026 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2026.1591048

Hans汉斯

联邦学习在电子商务场景中的应用研究

孙　跃

贵州大学数学与统计学院，贵州　贵阳

收稿日期：2026年7月30日；录用日期：2026年8月13日；发布日期：2026年9月20日

摘　要

随着电子商务的迅速发展，平台、商家、支付机构及物流企业都积累了大量的用户行为数据、交易数据及运营数据，这些数据对推荐优化、精准营销、风险控制都有着重大的潜在价值。但电商数据大多分散于不同主体，又常涉及到用户的隐私和商业机密，因此传统的集中式数据整合方式有着明显的局限。联邦学习(Federated Learning, FL)作为一种数据不出本地、模型协同训练的新兴分布式机器学习模式，自然地成为电商场景中数据协同利用的新解题思路。本文首先系统地分析了电子商务业务的特点，厘清了电商数据规模大、更新快、来源多样、异构性强、隐私敏感等诸多特性，继而讨论了联邦学习在个性化推荐、精准营销、风险防控与反欺诈等核心场景中的主要应用，再进一步探讨其在广告投放、搜索排序、供应链协同中的拓展价值。同时，本文也客观地指出现有联邦学习在电商场景应用中所面临的问题：数据异构、隐私保护风险、通信成本高、多方协同落地难。最终得出结论：联邦学习在保障数据安全、尊重商业边界的前提下有利于实现电商多方数据价值协同，故其有极好的应用潜力和发展前景。

关键词

电子商务，联邦学习，个性化推荐，精准营销，风控与反欺诈

Research on the Application of Federated Learning in E-Commerce Scenarios

Yue Sun

School of Mathematics and Statistics, Guizhou University, Guiyang Guizhou

Received: July 30, 2026; accepted: August 13, 2026; published: September 20, 2026

Abstract

With the rapid development of e-commerce, platforms, merchants, payment institutions, and logistics enterprises have accumulated vast amounts of user behavior data, transaction records, and operational metrics. These datasets hold significant potential value for recommendation optimization,

文章引用: 孙跃. 联邦学习在电子商务场景中的应用研究[J]. 电子商务评论, 2026, 15(9): 695-704.
DOI: 10.12677/ecl.2026.1591048

precision marketing, and risk management. However, most e-commerce data is scattered across multiple entities and often involves user privacy and commercial secrets, rendering traditional centralized data integration approaches inherently limited. Federated Learning (FL), an emerging distributed machine learning paradigm that enables model training without local data migration, naturally emerges as a novel solution for collaborative data utilization in e-commerce contexts. This paper first systematically analyzes the characteristics of e-commerce operations, highlighting key features such as massive data volumes, rapid updates, diverse sources, strong heterogeneity, and privacy sensitivities. It then examines federated learning's primary applications in core scenarios—including personalized recommendations, targeted marketing, risk mitigation, and fraud prevention—and further explores its extended value in advertising delivery, search ranking, and supply chain collaboration. The study also objectively identifies challenges in current federated learning implementations: data heterogeneity, privacy protection risks, high communication costs, and difficulties in cross-party coordination. The conclusion emphasizes that federated learning effectively enables collaborative utilization of multi-party data while ensuring data security and respecting business boundaries, demonstrating exceptional application potential and growth prospects.

Keywords

E-Commerce, Federated Learning, Personalized Recommendation, Precision Marketing, Risk Control and Anti-Fraud

1. 引言

1.1. 研究背景

近年来，随着互联网技术和数字经济的迅猛发展，电子商务已经成为现代商业体系中举足轻重的一部分，而电商平台在商品交易、内容分发、广告投放、会员运营等环节积累了极为丰富、多维交织的数据资源，如用户浏览数据、点击数据、搜索数据、订单数据、支付数据及配送数据等。这些数据对提高平台智能化运营水平、改善用户服务体验、辅助商家经营决策等都具有重大的价值。

然而，在真实的电商生态中数据不是集中于某一主体，例如：商家掌握订单及库存数据，平台掌握流量及行为数据，支付机构掌握支付风险数据，物流企业掌握履约及签收数据。随着用户隐私保护的要求不断加强和各主体之间又存在商业竞争关系，因此不同主体之间难以直接共享原始数据，数据孤岛问题十分突出。从而导致传统的集中式建模方式在电商场景中的适用性受到极大限制。

联邦学习作为一种新型分布式机器学习技术，不仅具备在不直接共享原始数据的情况下做多方联合建模的天然优势，而且可以保护用户隐私。故而成为解决电商数据孤岛、隐私保护两者矛盾的新途径，因此研究联邦学习在电商场景中的应用有较强的现实意义[1]。

1.2. 研究意义

从理论层面看，联邦学习在医疗、金融等领域已有相当充分、成熟的研究，而目前就电商场景中联邦学习的应用仍有进一步拓展空间，因此对电商场景下联邦学习应用予以系统分析，有利于完善联邦学习的行业应用研究[2]。

从实践层面看，电商平台在个性化推荐、精准营销、风险控制诸方面都对数据协同有十分明确、迫切的需求，而联邦学习能在保证数据安全、尊重商业边界的基础上提高模型训练效果，故能妥帖地缓解数据孤岛问题，切实提高电商平台智能化决策的能力[3]-[5]。因此，对联邦学习在电商场景中的应用宜予以充分研究。

2. 研究综述

在《中华人民共和国个人信息保护法》[1]和《中华人民共和国消费者权益保护法》[2]等法律法规强化个人信息处理与自动化决策合规要求的背景下，国内电商平台越来越难以依赖传统“集中汇聚用户数据”的方式训练推荐、营销和风控模型。联邦学习通过“数据不出本地、模型协同训练”的方式，使平台、商家、物流、支付与金融机构能够在不直接交换用户原始数据的前提下建模，因而适合电商高频、强隐私、跨主体的数据协同利用场景[6] [7]。

个性化推荐与商品排序是联邦学习在电商场景中最直接的应用，电商推荐依赖点击、收藏、加购、购买、评价等行为因素，但这些数据分散在平台、店铺和终端侧，无法直接有效的利用。因此，薛大暄等提出了基于差分隐私通信高效联邦推荐方法，通过将差分隐私、矩阵分解和深度推荐结合，既能保证用户隐私的同时又能提高通信效率，并且强调了推荐系统在电商场景中的广泛使用[6]。郭剑岚等进一步将区块链技术与联邦学习结合，用去中心化方式提升推荐系统中的可信协同和隐私保护能力[8]。然而，在实时推荐和内容推荐中，个性化联邦多臂赌博机框架可缓解数据异质、通信成本高和用户偏好快速变化的问题[9]。

此外，联邦学习还可以用于跨平台、跨商家的协同建模，更能精准反映用户的需求和解决非独立同分布数据带来的建模困难。这是因为大型平台掌握总体流量，小商家掌握细粒度商品与交易反馈，在二者数据研究中，Park 等直接面向电商平台提出带数据价值评估的联邦推荐系统，讨论大型购物平台与小型线上商店协同训练的问题[4]；FedRAP 和公平个性化联邦推荐则从全局偏好、个体偏好与公平性角度，改善联邦推荐在非独立同分布数据下的表现[10] [11]。

联邦学习还可用于电商场景下的风控、反欺诈和安全运营，如平台、支付机构和物流企业在无需共享完整用户画像的前提下，可联合识别刷单、薅羊毛、异常退货、虚假交易和账号攻击。近年来，国内研究集中解决联邦学习中的隐私聚合、异构数据、安全鲁棒和恶意参与方问题：安全自适应联邦学习框架关注非独立同分布和投毒检测[12]；基于用户选择的鲁棒隐私保护方案处理推理攻击与拜占庭攻击[13]；动态群签名与区块链联邦学习方案则用于身份隐私、恶意用户追踪和贡献激励[14]。这些机制虽然不全是专门限定于电商场景中，但为电商风控协同提供了可迁移技术基础。

总体来看，近年来国内外联邦学习在电商场景中的应用研究已从“能否保护隐私”转向“能否在推荐效果、通信效率、抗攻击能力和合规审计之间取得平衡”。未来重点在于：将差分隐私、安全聚合、区块链审计、量化、压缩等技术与个性化联邦推荐结合；面向冷启动、长尾商品和直播电商场景优化非 IID 建模；并建立可解释、可审计、可退出的数据协作机制，使联邦学习真正嵌入电商推荐、营销和风控全链路。

本文系统分析了电商场景联邦学习应用体系，详细阐述了联邦学习在个性化推荐、精准营销、风控与反欺诈三大核心场景的应用逻辑与价值，并且说明联邦学习在广告投放、搜索排序、供应链协同等拓展场景的应用潜力，强调其对电商全链路智能化运营的推动作用，如通过多方数据联合优化广告匹配度和库存预测准确性，最后针对性提出电商场景落地挑战与对策。

[1]http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html
[2]https://www.samr.gov.cn/zfjcj/tzgg/art/2023/art_615af9ed6bcd4974bf853dd2e02bc663.html

3. 联邦学习在电商场景中的主要应用

随着电子商务平台业务规模持续扩张，平台、商家、支付机构、物流企业、内容平台等主体都积累了十分丰富、多维关联的数据资源，包括用户浏览、点击、搜索、收藏、加购、下单、支付、评价、退货、物流签收等行为数据，这些数据对提高电商平台智能化运营水平有重大的价值。然而，现实中各主体所持数据彼此分散，既有极强的互补性，又受隐私保护、商业竞争、数据安全等因素的严格制约，难以采用传统集中式方式进行整合。联邦学习以“数据不出本地、模型协同训练”的方式，为电商多方数据协同利用提供了新的技术路径。更重要的是，目前联邦学习在电商场景中的应用已有十分明确、成熟的落地方向：个性化推荐、精准营销、风控与反欺诈。

3.1. 个性化推荐中的应用

个性化推荐是电商平台改善用户体验、提高经营效率重要的手段[15]。由于海量商品使得用户在主动搜索时往往难以及时、准确地找到符合自己需求的商品，故而平台利用用户的历史行为、兴趣偏好、消费等特征数据来推断用户可能感兴趣的商品并予以推荐。更重要的是，推荐效果的好坏也直接影响用户的浏览体验，同时也关系到商品曝光效率、点击率、转化率及平台留存率，因此推荐系统已然成为电商平台的核心能力[4]。

传统电商推荐模型一般是从平台内部行为数据出发来建模，即利用浏览、点击、搜索关键词、收藏、加购等数据来识别用户兴趣，但是这类数据有十分明确的局限性：第一，平台侧数据主要反映用户的意向行为，而商家侧数据如购买频次、复购情况、退货记录、会员等级等指标都可以准确反映用户的实际消费行为。第二，随着直播电商、短视频电商等新形态崛起之后，用户兴趣的表达早已不局限于传统站内操作，如直播间停留时长、内容互动、评论反馈等都是新的兴趣信号。因此，若仅依靠单一平台数据，所得用户画像必然是残缺的，推荐结果自然也难以真正切中用户实际需求。

联邦学习可以有效缓解前面所论述的问题，其在推荐场景中的应用十分明确：电商平台、商家、内容平台作为参与方可以在不共享原始用户数据的前提下联合训练推荐模型，即各参与方先在本地用自身数据做模型训练，再把模型参数或加密后的中间结果上传给联邦协调端做参数聚合，由此可以得到泛化性能更好的全局模型。因此联邦学习既能很好地解决了原始数据跨主体流动的问题，又能充分利用多源异构数据中蕴含的信息。

联邦学习在电商业务个性化推荐场景中的价值主要体现在以下三方面：第一，由于不同主体的数据能从不同角度反映用户的兴趣偏好，从而多方数据联合利用有利于完善用户画像和补全单一数据源所缺乏的信息，从而能有效提高推荐准确率。第二，由于新用户、新商品、长尾商品都因单一平台数据量小而面临数据稀疏的困难，因此联邦学习能有效缓解推荐系统中长期存在的数据稀疏问题。而多方协同能切实缓解冷启动问题，因而更有利于长尾商品被发现、被推荐。第三，联邦学习有利于让推荐结果更契合用户真实的消费需求，避免单纯依靠短期点击行为做推荐时产生的偏差，因此能给出更符合用户长期价值及真实偏好的推荐[3] [5]。

因此，个性化推荐是联邦学习在电商场景中最典型的应用。它帮助平台提高点击率、转化率和用户留存的同时也帮助商家精准地触达目标用户，提高商品曝光效率和营销回报。

3.2. 精准营销中的应用

精准营销是电商平台精细化运营、提高商业收益十分有力的手段，与传统的广投放模式不同，精准营销是以用户特征、消费行为为基本依据来做差异化触达，因此能有效地识别高潜力用户、高价值用户及流失风险用户，进而制定高效营销策略。典型的电商营销任务包括用户分层、活动响应预测、复购预

测、流失预警、优惠券发放优化和会员召回等。营销是否精准直接关系促销转化率、优惠资源使用效率及商家整体营销的回报率。

在实际电商业务中精准营销所依赖的数据来源十分分散，这是因为平台有用户浏览、搜索、点击、加购、活动参与行为数据，商家有订单成交、会员体系、售后服务、复购记录数据，广告渠道有曝光、点击反馈数据，线下门店有到店消费、核销数据。这些数据彼此衔接、互为补充。由于受用户隐私保护规则及各方商业边界的限制，这些数据源难以直接集中使用，因此营销模型对用户需求的判断必然受到一定限制。

联邦学习为电商精准营销提供了有力的新思路：通过多方联合建模的方式让各参与方不共享原始数据，只共享模型训练中所用的参数信息，因而能有效的解决用户价值评估、营销响应预测的问题。具体而言，平台侧有用户浏览兴趣、搜索频次等数据，商家侧有购买金额、复购周期、客单价等数据，将二者用联邦学习联合建模之后，识别高意向用户和潜在复购用户的准确性大大提高，故而对优惠券投放、节日促销、会员运营等典型业务场景都有直接的营销增效作用。

从应用效果可以看到联邦学习在精准营销中的应用价值主要体现在三个方面：第一，联邦学习有利于提高用户分层的准确性，因为用站内行为及单笔交易记录来做用户分层肯定不够充分，而多方数据协同能更可靠、更充分地刻画用户消费能力、购买偏好和活跃程度，因此用户标签划分更精细。第二，联邦学习有利于改进活动响应预测效果，平台及商家由此能更准确地判断哪些用户更有可能参与活动、领取优惠券、产生二次购买，因而能更合理地分配营销资源。第三，联邦学习对用户生命周期管理有直接而重大的帮助，平台可借助多方数据及时、准确地识别潜在流失用户、沉默用户和高价值用户，再据此制定差异化的运营策略，提高用户留存率及复购率。

由于电商企业开展营销的根本目的不是单纯提高曝光量，而是要提高转化效率、获得经营收益，因此联邦学习在精准营销中的价值十分明确：在保护用户隐私、保证商业数据安全的前提下实现数据价值共享，由此让平台、商家双方都切实提高营销决策能力，这对目前用户获取成本不断上升的电商行业有直接而重大的现实意义。

3.3. 风险防控与反欺诈中的应用

近年来随着电商交易规模持续扩大，平台所面临风险的种类日趋复杂，刷单、虚假注册、薅羊毛、恶意退款、支付欺诈、虚假收货、团伙化异常交易等风险行为都可能给平台、商家带来直接经济损失和破坏正常交易秩序，损害用户信任，危及平台生态的稳定。因此，建设高效、精准、动态响应的风险控制体系，是电商平台稳健运营的根本保证。

由于电商风险行为通常具有跨环节、跨主体和隐蔽性强的特点，仅依靠单一主体的数据很难有效地识别风险。具体而言，平台有账号行为轨迹、设备指纹、登录频率、下单路径和页面停留等数据，商家有订单异常、退货退款、售后投诉和异常收货行为等数据，支付机构有支付方式、支付频率、支付失败率等数据，物流企业有发货地址、签收异常、拒收情况、配送轨迹异常等数据。各主体所掌握的风险特征分散于不同链路，通过联邦学习将各主体数据合理联用能有效提高风险识别的准确性[16]。

联邦学习在电商风控中的应用逻辑较为清晰，通过利用多方风险特征来提升模型的识别能力，因此各参与方先在本地用自身的风险样本及业务特征训练模型，然后用联邦机制对风险模型做联合优化。这样既能保护用户隐私又能很好地让各方风险信息彼此协同、互为补充。对于跨平台套利、恶意退款、欺诈支付、团伙刷单等复杂行为的识别，多方联合建模显然优于单点风控。

联邦学习在风控及反欺诈领域的应用价值为：第一是提高风险识别的准确率，因为联邦学习能有效地联合平台、商家、支付、物流等数据，能提取更充分的异常行为特征，从而切实降低单一维度判断中

漏判的风险。第二是有利于降低误判率，传统风控中常有用户因某一环节异常而被错误识别为高风险对象，而联邦学习借助多方交叉验证，所作判断更加审慎可靠。第三是有利于增强对新型欺诈行为的适应能力，由于黑灰产攻击手段日新月异，单一数据源上的风控模型极易失效，因此多方联动更有利于尽早发现新风险模式，同时能有效提高了平台动态防御的能力。

因此，风控与反欺诈是联邦学习在电商场景中最迫切的应用方向之一。它能够在不突破数据边界的前提下，形成覆盖账号、交易、支付和物流等环节的综合风控能力。

3.4. 拓展应用

联邦学习还可以用于广告投放，搜索排序和供应链协同与库存预测。广告投放和搜索排序是电商平台进行流量分配和商业变现的重要环节，用户的搜索行为、商品浏览行为、点击行为和转化行为，都会影响广告展示逻辑和搜索结果排序。而随着电商平台经营规模扩大，库存管理、补货决策、仓储调度、物流协同诸环节都日趋关键，销量预测的不准必然导致缺货、积压、配送延误等问题，进而直接损害用户体验，也降低商家经营效率[17]。

然而，在实际业务中广告投放、搜索排序所涉及的数据分散在不同的主体，平台侧有搜索词、点击路径、停留时长、浏览偏好等行为数据，商家侧有商品价格、库存、转化表现、复购率、促销信息，广告系统有广告曝光、点击反馈、投放预算数据。不同主体的数据从不同角度刻画商品吸引力及用户购买意图，但彼此间不能直接共享，因此预测模型难以直接利用全量信息。类似的，供应链上各类数据也分散于不同主体，平台掌握商品搜索热度、浏览趋势、大促活动信息及区域需求变化，商家掌握库存水平、历史销量、补货周期及生产能力，物流企业掌握仓储周转率、配送压力及区域履约时效等数据对需求预测、库存优化都极有价值。但也正因主体不同，系统相对独立，数据敏感，在现实中难于直接集中分析。

联邦学习技术可以在保护用户隐私和各方利益的前提下让各主体联合建模，共同训练一个模型，因此可以有效的解决广告投放，搜索排序和供应链协同与库存预测中存在的问题。通过这种方式，模型既能利用用户搜索和浏览行为，又能结合商品成交表现、库存状态和促销信息，从而提高广告匹配度和搜索排序的合理性。同时，让平台、商家、物流企业联合、有序地做销量预测及库存优化的模型训练。如平台用用户搜索热度、浏览趋势来预测短期需求波动，商家用历史销量、现有库存来制定补货计划，物流企业用配送能力、仓储压力来安排资源调度，从而提高需求预测的准确性，切实降低缺货率、滞销率，最终提升全供应链的运营效率。

从电商全链路运营角度看，联邦学习不仅可用于前端交易而且可以用于后端运营。它不仅关注“商品能否卖出去”，也关注“能否及时供给、稳定履约和降低运营损耗”。因此，联邦学习有助于推动电商平台形成更加完整的智能化运营体系。

4. 面临的挑战与对策建议

4.1. 关于数据异构挑战与对策建议

因为电商参与主体较多，所以不同主体所采集的数据结构、字段定义、标签体系有明显而实质性的差异：平台侧关心浏览、点击，商家侧关心成交、复购，支付侧关心支付状态、风险评分，物流侧关心履约时效、签收异常。因此数据异构性给联邦建模带来极大困难，也直接不利地影响模型训练效率及效果。例如：从产业规模看，电商数据具有规模极大的特征。根据国家统计局数据显示，2024 年，全国网上零售额 155,225 亿元，比上年增长 7.2%。其中，实物商品网上零售额 130,816 亿元，增长 6.5%，占社会消费品零售总额的比重为 26.8% [18]。这些数据说明电商交易行为数据规模巨大，若缺乏统一的数据标准，数据异构问题会在联邦学习建模过程中会被进一步放大。此外，相关研究表明，非独立同分布数据是联

邦学习中的重要挑战，不仅会导致模型性能下降，而且影响训练收敛速度，并增加通信成本和优化难度[19]。因此，联邦学习在电商场景的应用中，数据异构并不是简单的数据格式问题，而是会影响模型效果、训练效率和业务可用性等核心问题。

可以采取以下对策建议：

(1) 建立统一的数据标准及字段规范，即平台、商家、支付机构、物流企业都以用户、商品、订单、支付、物流、售后诸种对象为核心，先建立统一的数据字典，再就各字段的名称、含义、数据类型、统计口径、更新时间予以明确。如统一“订单完成”的定义，厘清“已下单”“已支付”“已发货”“已签收”“已完成售后周期”等状态，从而避免不同主体对同一业务概念的不同理解。

(2) 建立跨主体的特征映射机制，对不能严格统一的数据字段用特征映射表、标签转换规则、元数据管理平台等手段进行对齐，如把平台侧的“点击率”“加购率”，商家侧的“成交率”“复购率”，物流侧的“签收及时率”映射到用户行为、交易意愿、履约质量等统一特征维度中，从而切实提高联邦建模中数据的可用性。

(3) 在模型层面引入处理异构数据的联邦学习方法，对于不同主体数据分布不一致的问题采用个性化联邦学习、分层聚合、知识蒸馏、迁移学习等方法，切实提高模型对异构数据的适应能力。同时对数据质量差或样本分布严重偏离的参与方，应设计数据质量评估及权重调整机制，防止低质量数据破坏全局模型。

(4) 要建立健全的数据质量评估制度，即参与方在加入联邦学习以前先对数据的完整性、准确性、及时性、一致性做系统检测，得出数据质量评分，然后对缺失率高、噪声大、字段口径不清的数据进行清洗、补全、标准化处理之后再正式参与模型训练。

4.2. 关于隐私保护与安全风险挑战与对策建议

虽然联邦学习没有直接共享原始数据，但是模型参数、梯度信息在传输过程中仍有泄露的风险，所以联邦学习也面临模型反演、梯度推断、恶意节点攻击、数据投毒等安全问题。例如：根据 IBM《2024 年数据泄露成本报告》显示，全球数据泄露事件在 2024 年的平均成本达到 488 万美元，较 2023 年增长 10%；此外，报告还指出，数据泄露事件涉及客户个人身份信息占 46%，35%的数据泄露事件涉及“影子数据”，这说明在数据来源复杂、系统边界模糊的业务场景中，仅依靠“不共享原始数据”并不足以完全消除隐私泄露的风险[20]。此外，Verizon《2024 年数据泄露调查报告》分析了不少于 3 万起安全事件和 1 万多起确认数据泄露事件，指出凭证滥用、基础 Web 应用攻击、系统入侵等仍是重要的风险来源[21]。

可以采取以下对策建议：

(1) 应当把联邦学习与隐私增强技术有效地结合起来，即对敏感数据及模型参数都引入差分隐私、安全多方计算、同态加密、可信执行环境等技术，从而切实降低模型训练中信息泄露的风险。对于用户画像、支付风控、精准营销诸种场景，应按照数据敏感等级选用不同强度的加密脱敏方案。

(2) 联邦学习系统应建立模型安全防护机制，对所上传的模型参数、梯度信息及训练结果做异常检测，及时发现恶意节点、异常梯度、数据投毒行为，对明显偏离整体分布的模型更新采用鲁棒聚合算法、节点信誉评分、异常剔除机制等方法进行处理，进而降低攻击影响。

(3) 对身份认证及访问控制加以完善，即对所有接入联邦学习平台的各方都必须先完成主体身份认证、权限审核、安全评估，然后系统根据“最小权限原则”合理分配数据访问、模型训练、参数上传、结果调用等权限，从而有效防范敏感信息泄露。

(4) 建立隐私风险评估和审计机制，参考 NIST 隐私框架，把隐私风险管理正式纳入企业整体风险治理体系之中，对数据采集、使用、传输、建模、结果输出等环节都予以持续评估。NIST 隐私框架的根本

目的正是帮助组织识别、管理隐私风险，既保护个人隐私，又促进创新产品和服务的发展[22]。同时，相关研究也提出了识别和缓解去标识化数据再识别风险的框架，可为电商企业开展数据脱敏和隐私保护提供参考[23]。

4.3. 关于通信与计算成本较高挑战与对策建议

因为电商数据规模大、更新极快，而联邦学习又要求各参与方做多轮本地训练、多次参数交互，故当参与主体数目较多时通信开销、训练时间都会大大增加。更严重的是，各参与方的计算能力、网络条件不同，因此协同训练的效率会降低，也直接不利于实际应用。随着我国电商业务的发展，每天会产生大量用户行为、交易和履约数据。在此基础上，如果平台、商家、支付和物流等多方频繁进行模型交互，通信链路、服务器资源和本地计算资源都会承受较大压力。

此外，数据异构和非独立同分布还会进一步增加联邦学习中的训练成本。相关研究表明，非独立同分布数据不仅会影响联邦学习的准确率和收敛效果，还会导致通信效率下降和本地模型更新不均衡[24]。因此在电商场景中，不同商家、不同地区、不同消费群体的数据差异越大，模型要达到稳定状态所需的训练轮次越多，通信、计算开销也就越大。

可以采取以下对策建议：

(1) 技术层面，可以采用通信压缩技术，即采用梯度压缩、参数量化、稀疏更新、模型剪枝等方法来减少每轮传输的数据量，即在每轮训练时不需要上传全部模型参数，只需上传变化较大的重要参数或其压缩后的梯度信息，从而减轻网络传输负担。

(2) 由于不同场景对实时性的要求不同，因此优化训练频率及聚合层面应作合理的划分：对实时性要求不高的营销推荐、用户分层、商品偏好分析等任务，可采用周期性训练或异步训练机制，从而避免所有参与方都频繁上传模型参数。而对重要活动期间的实时风控、异常交易识别等任务，应适当提高训练频率。

(3) 联邦学习层面，采用分层联邦学习的架构，先从平台、区域、行业、商家类型等维度做局部聚合，再做全局聚合，即先在同区域或同品类商家的数据上分别训练局部模型，再把局部模型上传给全局服务器做聚合，由此可以减轻通信负担，也有利于模型学习局部市场特征。

(4) 由于不同商家所拥有的服务器配置、网络条件、技术能力各不相同，因此各参与方应建立参与方算力评价及资源调度的机制，即联邦学习平台从参与方的算力、带宽、数据量、在线稳定性诸种因素出发动态分配训练任务，对算力薄弱的中小商家应适当降低接入门槛，可采用轻量级模型、边缘计算节点或云端代理训练等方法。

4.4. 关于多方协同与工程落地难度大的挑战与对策建议

联邦学习在电商中的落地既是技术问题，也属于组织协同问题。这是因为平台、商家、支付机构、物流企业等主体在合作意愿、技术能力、利益目标方面都存在差异，因此要让联邦学习真正落地，就必然要解决统一协作机制、数据接口标准、收益分配方式等问题[25]。如果缺乏统一的协作机制，即使算法本身可行，也难以在真实业务中稳定运行，这是因为在联邦学习落地时会面临数据接口、模型接口、训练流程、权限管理、日志审计、效果评估等一系列工程问题。因此，数据治理是组织在利用数据价值并管理隐私风险时的重要起点，说明技术应用必须与治理机制、管理流程和风险控制相结合。

由于现实中大型平台与中小商家在技术上存在明显差距，因此联邦学习的推广也会受到影响，大型平台有较为完善的数据治理、模型训练、安全合规等能力，而中小商家一般没有专业算法团队及安全基础设施，因此若没有低门槛的工程工具及合理可行的合作机制，联邦学习就很容易停留在试点阶段，难

以形成规模化应用。

可以采取以下对策建议：

(1) 从机制角度考虑，各参与方应共同建立多方协同治理机制，即在合作前要明确数据使用边界、模型训练目标、责任分工、收益分配和风险承担方式，继而签订数据合作协议、模型使用协议和安全责任协议，切实降低合作的不确定性。

(2) 从标准层面考虑，各参与方应先建设统一的联邦学习平台及标准化接口，因此平台可以提供统一的 API 接口、数据接入规范、模型训练流程、权限控制模块和日志审计功能，从而降低商家、支付机构、物流企业接入联邦学习系统的成本。对中小商家而言，联邦学习平台应提供完整低配版联邦学习技术或可视化配置工具，切实降低平台部署难度。

(3) 模型效果评估和利益分配层面，联邦学习平台应设置统一明确的评估指标，如点击率提升、转化率提升、复购率提升、欺诈识别准确率提升、物流异常预测准确率提升等，并且根据这些指标评估各参与方的数据贡献、模型贡献和业务收益，从而建立公平的收益分配机制，同时增强各方参与意愿。

(4) 从落地策略考虑，可以通过“小范围试点－效果评估－制度完善－规模推广”的路径来降低工程落地风险，因此电商企业可以先在风险较小、收益明确的场景做试点，如联合用户分层、商品推荐优化、物流异常预测等，待技术稳定、规则成熟之后，再将该策略扩展到支付风控、跨平台用户画像、供应链金融等场景。

5. 结论与展望

5.1. 结论

本文对联邦学习在电商场景下的应用做了较为详细的研究，研究表明联邦学习为电商场景中的数据协同利用提供了可行路径。具体说明其在个性化推荐、精准营销、风控与反欺诈等核心业务中的实际应用价值，不仅缓解数据孤岛问题，而且切实提高模型效果[1] [3]。还拓展了联邦学习在电商场景中广告投放，搜索排序和供应链协同与库存预测的应用。最后给出了联邦学习在电商场景下应用所面临技术和工程落地的挑战的对策建议。

5.2. 展望

联邦学习在电商领域有十分广阔的发展前景，第一是在电商场景中采用更加高效的联邦学习算法，切实提高数据安全保障能力的同时提高通信效率，第二是加快联邦学习在真实电商环境中的工程化落地，建立健全的标准体系及多方协作机制，第三是结合大模型和人工智能技术，面向大规模电商场景。随着技术不断成熟，联邦学习有望在电商全链路智能化运营中发挥更大作用[5] [15]。

参考文献

[1] McMahan, B., Moore, E., Ramage, D., *et al*. (2017) Communication-Efficient Learning of Deep Networks from Decentralized Data. arXiv: 1602.05629.

[2] Kairouz, P. and McMahan, H.B. (2021) Advances and Open Problems in Federated Learning. *Foundations and Trends® in Machine Learning*, **14**, 1-210. https://doi.org/10.1561/2200000083

[3] Sun, Z., Xu, Y., Liu, Y., He, W., Kong, L., Wu, F., *et al*. (2025) A Survey on Federated Recommendation Systems. *IEEE Transactions on Neural Networks and Learning Systems*, **36**, 6-20. https://doi.org/10.1109/tnnls.2024.3354924

[4] Park, J., Kang, M., Sim, W., Lee, S. and Park, H. (2026) Federated Recommender System with Data Valuation for E-Commerce Platform. *Expert Systems with Applications*, **298**, Article ID: 129695. https://doi.org/10.1016/j.eswa.2025.129695

[5] Liu, F., Zheng, Z., Shi, Y., Tong, Y. and Zhang, Y. (2023) A Survey on Federated Learning: A Perspective from Multi-

Party Computation. *Frontiers of Computer Science*, **18**, Article No. 181336. https://doi.org/10.1007/s11704-023-3282-7

[6] 薛大暄, 杜宜霏, 陈红, 等. 基于差分隐私的通信高效联邦推荐方法[J]. 软件学报, 2026, 37(6): 2584-2606.

[7] 仇健, 马海英, 王占君, 等. 联邦学习中隐私保护聚合机制综述[J]. 计算机应用研究, 2025, 42(6): 1601-1610.

[8] 郭剑岚, 陈俞强, 卢荣, 等. 基于区块链和联邦学习的隐私保护去中心化推荐系统[J]. 计算机应用研究, 2026, 43(4): 1005-1012.

[9] 陈家晟, 秦航. 通信高效的个性化联邦多臂赌博机推荐框架[J]. 计算机应用研究, 2025, 42(11): 3257-3264.

[10] Li, Z.W., Long, G.D. and Zhou, T.Y. (2024) Federated Recommendation with Additive Personalization. arXiv: 2301.09109.

[11] Wang, S., Tao, H., Li, J., Ji, X., Gao, Y. and Gong, M. (2024) Towards Fair and Personalized Federated Recommendation. *Pattern Recognition*, **149**, Article ID: 110234. https://doi.org/10.1016/j.patcog.2023.110234

[12] 李功丽, 刘芳芳, 雷宏志, 等. 面向异构数据的安全自适应联邦学习框架[J]. 计算机应用研究, 2025, 42(5): 1523-1531.

[13] 王晓明, 黄斌枘. 基于用户选择的鲁棒与隐私保护联邦学习方案[J]. 计算机应用研究, 2025, 42(6): 1859-1867.

[14] 张蒙, 古春生, 张言, 等. 基于动态群签名的区块链联邦学习隐私保护方案[J]. 计算机应用研究, 2025, 42(11): 3468-3475.

[15] 曹俊伟, 李军祥, 李玉璐. 电子商务推荐系统研究综述[J]. 电子商务评论, 2025, 14(12): 3087-3097.

[16] Chen, F., Luo, M., Dong, Z., *et al*. (2018) Federated Meta-Learning with Fast Convergence and Efficient Communication. arXiv: 1802.07876.

[17] 马祁. 基于联邦学习的供应链节点信誉评估与资源配置方法[D]: [硕士学位论文]. 北京: 北京邮电大学, 2023.

[18] 2024 年 12 月份社会消费品零售总额增长 3.7% [EB/OL]. https://www.stats.gov.cn/sj/zxfb/202501/t20250117_1958327.html, 2025-01-17.

[19] Solans, D., Heikkila, M., *et al*. (2024) Non-IID Data in Federated Learning: A Survey with Taxonomy, Metrics, Methods, Frameworks and Future Directions. arXiv: 2411.12377v1.

[20] IBM. Cost of a Data Breach Report 2024. https://www.ibm.com/downloads/documents/cn-zh/107a02e94948f4ec

[21] Verizon. 2024 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

[22] NIST. National Institute of Standards and Technology U.S. Department of Commerce. NIST Privacy Framework. https://csrc.nist.rip/CSRC/media/Presentations/Privacy-Framework/images-media/1040%20Privacy%20Framework%20-%20Lefkovitz.pdf

[23] ISO/IEC 27559:2022 (2022) Information Security, Cybersecurity and Privacy Protection-Privacy Enhancing Data Deidentification Framework.

[24] Zhao, Y., Li, M., Lai, L.Z., *et al*. (2018) Federated Learning with Non-IID Data. arXiv: 1806.00582.

[25] Yang, Q., Liu, Y., Chen, T. and Tong, Y. (2019) Federated Machine Learning: Concept and Applications. *ACM Transactions on Intelligent Systems and Technology*, **10**, 1-19. https://doi.org/10.1145/3298981