

大模型驱动的智能客服在电子商务中的应用与挑战

吴道生

贵州大学大数据与信息工程学院, 贵州 贵阳

收稿日期: 2025年9月22日; 录用日期: 2025年10月11日; 发布日期: 2025年11月6日

摘要

随着电子商务不断发展, 客户服务需求变得规模化且多样化, 传统依靠规则和检索的智能客服在理解语义、服务深度上逐渐呈现出自身的局限性。近年来, 人工智能技术在自然语言处理方面取得进展, 给电子商务智能客服带来新的发展契机。由大模型驱动的智能客服能靠更强大的语义理解与生成能力, 达成高效解答问题、个性化推荐以及多语言交流, 既提升用户体验和服务效率, 又为企业节省人力成本、优化运营流程创造可能性。但大模型用于电商客服还存在知识幻觉、数据安全、隐私保护以及昂贵算力成本等问题。本文通过对大模型智能客服的应用场景与优势进行梳理, 剖析其在电子商务实践里的实际困境, 给出未来改进的方向与办法, 期望能为智能客服的研究与实践给予具有实际意义的参考。

关键词

大模型, 智能客服, 电子商务

Applications and Challenges of Large Language Model-Driven Intelligent Customer Service in E-Commerce

Daosheng Wu

College of Big Data and Information Engineering, Guizhou University, Guiyang Guizhou

Received: September 22, 2025; accepted: October 11, 2025; published: November 6, 2025

Abstract

With the continuous development of e-commerce, customer service demands have become increasingly large-scale and diverse. Traditional rule-based and retrieval-based intelligent customer service

systems are showing limitations in semantic understanding and service depth. In recent years, advances in artificial intelligence, particularly in natural language processing, have brought new opportunities for intelligent customer service in e-commerce. Large language model-driven customer service systems, with their powerful semantic understanding and generation capabilities, can provide efficient problem-solving, personalized recommendations, and multilingual interactions. These advantages not only enhance user experience and service efficiency but also enable enterprises to reduce labor costs and optimize operational processes. However, challenges remain in applying large models to e-commerce customer service, including hallucinated knowledge, data security, privacy protection, and the high cost of computational resources. This paper reviews the application scenarios and advantages of large-model-based intelligent customer service, analyzes the practical challenges in e-commerce contexts, and proposes directions and approaches for future improvement, with the aim of providing meaningful references for both research and practice in this field.

Keywords

Large Language Models, Intelligent Customer Service, E-Commerce

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

近些年,随着互联网技术以及移动支付不断普及开来,电子商务已然变成推动全球零售业发展的关键驱动力量。用户于电商平台所开展的购物活动变得越来越频繁,在此情形之下,与之相伴随的客户服务方面的需求同样呈现出快速的增长态势,并且还表现出多样化的走向。那种高效能的、操作便捷的并且具备个性化特点的客户服,其不但同用户体验以及交易时的满意程度有着极为直接的关联,而且在相当的程度上会对平台所拥有的竞争力还有用户的黏性产生影响。

传统的电子商务客服体系主要是依靠人工坐席以及依据规则所构建的自动化系统来运行的。虽说在一定程度上能够对一些高频出现的问题给予解决,然而当碰到那些复杂的语义表达情况,或者是涉及跨领域的知识咨询事宜,又或者面临用户需求呈现出高并发的状态之时,往往就会出现响应的效率比较低、服务所达到的深度不够充分、用户的使用体验也较为欠缺等一系列的局限性状况。近些年来新冒头的检索式客服模型以及小规模机器学习客服模型,在语义匹配以及自动回复这两个方面都取得了一定程度的改进成效,可是依旧很难在语义理解的深度以及灵活性这两方面的瓶颈得以突破。

随着人工智能尤其是大语言模型的迅猛发展,智能客服迎来了全新的变革机遇[1]。像 GPT 系列、ERNIE、LLaMA 这类大模型,有着海量语料的学习能力以及强大的自然语言理解和生成能力,在上下文维持、逻辑推理、多轮对话以及多语言交互等方面,能呈现出比传统模型更为出色的性能[2]。在电子商务场景里,这样的技术不仅能给予更为自然、顺畅的人机交互感受,还在售前咨询、售中跟进以及售后服务等诸多环节都能发挥出更大的效用。

但是,大模型驱动的智能客服在实际的应用场景中也呈现出一系列的问题[3]。首先,模型所生成的内容很可能会出现“知识幻觉”方面的状况,如此一来,答复的准确性以及可靠性便都遭到了怀疑;其次,电商平台牵涉数量众多的用户隐私以及交易数据,如何在确保服务能够智能化的同时,还能够同步达成数据的安全防护以及合规处置,这已然成了无法逃避的关键问题。除此之外,大模型在训练以及部

署环节的成本颇高，关于它的商业可持续性，还有与人工客服相互协同的机制，依旧需要展开更为深入的探究。

基于上述背景情况，本文拟以大模型驱动的智能客服为研究对象，全面地梳理其在电子商务领域里的典型应用场景，对其相比传统客服所具有的各项优势加以归纳总结，同时还要深入剖析其在技术方面、数据方面、商业方面以及伦理方面所面临的挑战。针对其未来的发展走向与应对策略展开相应的探讨。通过此项研究，旨在为智能客服相关的学术研究以及行业实际操作给予具有一定价值的参考内容和启发性的思考。

2. 大模型驱动的智能客服概述

2.1. 大模型技术简介

大语言模型(Large Language Model, LLM)属于近年来人工智能领域所取得的核心进展范畴，其根本在于针对大规模语料库展开训练操作，借助深度学习，特别是依据 Transformer 架构构建的神经网络来达到对自然语言的理解以及生成目的。像 GPT 系列、ERNIE、LLaMA 等这类大模型，拥有着数量达到数十亿甚至上千亿级别的参数[4]，在多轮对话、语义推理、上下文保持以及跨语言迁移等一系列任务当中，均能够呈现出颇为出色的性能表现。相较于传统的规则匹配或者检索式算法而言，大模型在语言理解的层次深度、生成的灵活程度以及知识迁移的能力等方面，都具备着十分明显的竞争优势，而这无疑为智能客服系统给予了全新的技术方面的有力支撑。

2.2. 智能客服的核心功能

在电子商务领域当中，智能客服所承担的主要任务在于提升用户体验，降低人工方面的成本，并且对服务流程加以优化。它的核心功能可从如下几个方面来概括：

- 1) 问答与问题解决：借助自然语言理解技术能够迅速回应用户所提出的各类问题，像是商品相关信息、订单当前的状态以及物流的进展情况等等。
- 2) 情感识别与交互：凭借情绪分析来察觉用户情绪方面的变化，进而达成安抚、鼓励或者个性化的回应效果，以此来提高用户的满意度。
- 3) 个性化推荐与辅助营销：通过将用户行为数据同兴趣偏好相结合的方式，主动去推送那些契合用户需求的商品还有促销信息，以此来让营销效果得以进一步地增强。
- 4) 多模态交互支持：支持文本、语音甚至图像输入与输出，实现更自然的人机沟通方式。

2.3. 大模型赋能的智能客服优势

相较于传统客服系统，大模型驱动的智能客服在以下几个方面表现出显著优势：

- 1) 语义理解能力增强：大模型拥有上下文理解以及语义推理的能力，可有效地减少“答非所问”的情况出现，进而提升回答的准确性以及相关性。
- 2) 对话生成的自然性：基于大模型的客服系统能够生成更为通顺且自然的言语表达，进而让交互所带给用户的体验无限接近于和真人展开沟通交流时的感受。
- 3) 多语言与跨文化适应性：大模型可支持多语言对话，能应用于跨境电商场景，降低语言方面的壁垒，提高国际用户的体验。
- 4) 知识扩展与持续学习：大模型能够通过和知识库加以结合或者经过微调的方式，达成领域知识的强化，进而满足不同电商平台所提出的业务方面的各种需求。
- 5) 可扩展性与灵活性：大模型智能客服可以和推荐系统、搜索引擎还有物流平台等诸多其他的电商

模块实现集成，进而形成一个完整的服务生态。

综上所述，大模型的引入不仅提升了智能客服在语言交互层面的能力，也为电子商务平台提供了更加智能化、个性化和国际化的客户服务方案，为后续的应用拓展奠定了坚实基础。

3. 大模型在电子商务智能客服中的应用场景

随着大语言模型在自然语言处理领域取得突破，它在电子商务智能客服中的应用也发生了变化，已从单一的问答服务逐步拓展至全流程的客户交互环节。大模型不但可提供更为精准的语义理解，而且在多模态交互以及复杂情境里，还表现出较强的适应能力，进而促使客服系统朝着智能化与人性化的方向发展。下面本文将从不同环节来分析其具体应用情况。

3.1. 售前服务

在销售前的阶段当中，用户往往得去了解有关产品的各类信息，要对不同的商品展开比较，同时还会开展个性化的咨询活动。由大模型来驱动的智能客服，能够凭借对上下文的精准理解以及对用户偏好数据的掌握，迅速给出商品规格、价格、库存等方面的信息，并且借助生成式的推荐方式达成“千人千面”般的个性化服务效果[5]。就好比说，该模型能够依据用户以往的浏览记录以及消费习惯情况，生成与用户需求相契合的商品清单，进而促使购买转化率得以提升。

3.2. 售中服务

在售中的环节当中，其核心的需求主要聚焦于订单处理以及物流跟踪这两个方面。大模型所具备的智能客服功能，能够凭借多轮的对话来深入理解用户所提出的有关支付、配送还有退换货等方面那些较为复杂的各类问题，并且还能够给出即刻的解决办法。相较于传统的那种检索式的客服而言，大模型在保持上下文这一点上能够呈现出更为优异的表现，进而能够让用户在一个会话的过程里面就能够顺利完成多项不同需求的处理事宜。比如说，当用户前来咨询物流相关情况的时候，该客服一方面能够将实时的位置信息告知给用户，另一方面还能够主动地去提醒用户预计的送达时间，并且还会依据物流的实际状态来为用户给出相应的售后选项。

3.3. 售后服务

在售后服务阶段，用户往往更为着重于投诉处理以及问题诊断这两方面的情况。大模型有着不错的语义分析能力，同时在情感识别方面也有着一定的优势，其能够一边识别出用户所存在的不满情绪，另一边还能生成那种带有安抚作用且颇具建设意义的回应内容。除此之外，大模型还能够针对常见的各类问题展开自动化的分类操作，进而追溯到问题的源头所在，并且还能给出多种多样的解决办法，如此一来便能让问题处理的周期得以缩短，促使用户的满意度获得提升。而对于那些较为复杂的难题来讲，便可以通过人机协同这样的一种方式将其转接到人工客服那边去处理，以此达成效率与服务质量之间的平衡状态。

3.4. 创新应用

除了传统的电商服务环节，大模型还催生了智能客服的新应用形式：

1) 电商直播中的实时问答：大模型可在直播场景中实现对观众问题的实时解答，辅助主播提升互动效率。

2) 虚拟数字人客服：电商平台结合大模型以及语音合成、图像生成技术，打造出“数字人客服”，可实现全天候且沉浸式的交互体验。

3) 多模态交互：大模型能够联合运用图像识别以及语音处理相关技术，从而给用户给予更为直观的商品咨询方面的服务，例如借助对用户所上传图片加以识别的方式，可迅速精准地定位到同类商品。

综上，大模型驱动的智能客服不仅在传统的售前、售中与售后环节发挥重要作用，还拓展出多样化的创新应用场景。这些应用不仅提升了客户服务的效率和质量，也推动了电子商务服务模式的升级与转型。

4. 大模型智能客服的挑战

大模型在电子商务智能客服领域，已然呈现出颇为强大的语义理解以及生成方面的实力。然而在实际的应用进程里，依旧存在着不少的挑战。而这些挑战一方面涉及技术自身所存在的局限性，另一方面还涵盖了数据安全、商业模式以及伦理合规等诸多方面的诸多因素。若无法妥善且有效地去应对这些挑战，很可能会对大模型智能客服的广泛运用以及可持续发展产生影响。

4.1. 技术层面挑战

首先，大模型普遍存在“知识幻觉”(hallucination)问题，即在缺乏真实知识支撑时生成看似合理但错误的回答[6]。这种情况在涉及商品规格、价格政策或售后规则时尤其严重，容易误导用户。其次，大模型在垂直领域的知识储备有限，难以满足电子商务中涉及专业术语和行业规范的需求。此外，大模型的可解释性不足，客服回答的逻辑路径难以追溯，限制了其在高风险业务场景中的应用[7]。

4.2. 数据与隐私问题

电子商务平台累积了数量众多且极为敏感的数据，其中包含了用户的诸多身份相关信息、各式各样的交易记录以及各类支付方面的信息。当大模型针对这些数据展开处理操作的时候，极有可能会引发出隐私出现泄露的情况以及数据遭到滥用的风险情况。除此之外，不同地区在有关数据保护方面的法律法规并不是统一的，存在着一定的差异，如《通用数据保护条例》《数据安全法》等，如此一来便给跨境电商平台带来了更高的合规方面的要求[8]。怎样在促使服务朝着智能化方向不断提升的过程中，达成对数据实行最小化使用这一目标并切实做好隐私保护相关工作，这依旧是当下迫切需要去破解的一个难题。

4.3. 商业与运营挑战

从商业角度来讲，大模型在训练以及部署方面所需的成本颇高，尤其是在需要海量算力予以支撑的情形下，这或许会给中小型电商企业设置一道门槛。大模型客服虽说能够大幅度削减人工客服所承担的工作量，然而在应对复杂情感以及突发状况的时候，依旧得依靠人工来介入。如何设计一套合理的人机协同机制，防止用户在自动化服务和人工服务之间产生脱节的感觉，这是平台需要仔细考量的一个关键问题。在用户对于 AI 给出回答的信任程度还没有彻底建立起来的情况下，一旦出现错误的回复或者不恰当的交互情况，可能致使用户流失，甚至还可能对企业声誉造成损害。

4.4. 伦理与社会影响

大模型的广泛运用引发了诸多伦理以及社会方面的争端。例如，长时间依靠 AI 客服，这或许会让人工客服岗位不断缩减，进而促使就业结构产生变动。而且，由模型生成的内容当中，有可能暗藏着偏见或者歧视，如此一来便会会影响用户群体所应享有的公平使用体验。在没有明确标识的情形下，用户往往很难将 AI 客服与人工客服区分开来，这就进一步催生出了信任以及透明性方面的问题。这些相关问题迫切需要借助行业标准以及政策监管来进行引导并且予以解决。

5. 发展趋势与对策建议

针对前文分析的大模型驱动智能客服在电子商务场景中面临的技术瓶颈、数据风险与伦理挑战，本章从技术创新、数据治理与社会责任等维度出发，提出未来的发展趋势与对策建议，以期智能客服系统的安全、合规与可持续发展提供思路与路径。

5.1. 技术改进方向

1) 知识增强与行业垂直化

当下大模型虽说通用性强，可在电商领域通常缺少针对性知识，未来的发展走向是借助知识增强技术，把大模型和电商知识库、企业 FAQ、产品数据库深度融合，形成“通用模型 + 行业微调”的混合方案，例如京东或者亚马逊可构建自有商品知识图谱，将其和大模型对接起来，让客服回答更为准确可靠。

2) 可控生成与回答质量优化

要降低“知识幻觉”方面的问题，可以引入依据规则所设定的结果约束以及可控生成技术。例如，客服在遇见支付、退货政策等这类关键问题的时候，能够借助预先设置好的规则模板来对结果加以验证，以此保证给出的回答不会偏离平台实际的业务逻辑。在未来，或许会出现所谓的“混合式客服系统”，也就是先由大模型来生成初稿，然后再交由验证模块去进行校正处理。

3) 多模态融合与智能交互升级

未来智能客服不仅限于文本交互，还将发展为多模态客服。例如，用户上传商品图片，大模型可通过视觉识别功能快速定位相似产品并生成推荐；用户在电商直播间提问时，AI 可实时语音回复并辅以商品图像链接，增强交互体验。这种融合语音、图像与文本的多模态客服，将大幅提升用户的沉浸感和便利性。

4) 低成本部署与轻量化模型

算力与成本问题是大模型应用的主要制约。未来趋势是通过模型蒸馏、参数压缩和边缘计算等技术，实现轻量化大模型的部署[9]。例如，企业可以在本地或云边协同环境下运行小规模模型，在保证性能的同时降低算力消耗和运营成本，使中小电商也能负担得起智能客服系统。

5.2. 数据隐私保护对策

数据隐私保护是大模型智能客服可持续发展的关键前提。面对电商场景中数据高敏感度与跨境流通的复杂性，需从技术防护、治理体系与行业协同三个层面构建系统化的隐私保护框架。

1) 技术防护：构建隐私增强型模型架构

在模型训练与推理环节，可引入差分隐私(Differential Privacy)、联邦学习(Federated Learning)、数据脱敏与加密计算等技术，以实现“数据可用但不可见”的安全共享机制。此外，通过安全多方计算(SMC)与隐私保护型微调(Privacy-preserving Fine-tuning)，可在多主体协作环境下确保数据不离源，从根本上降低隐私泄露风险。

2) 治理体系：建立数据全生命周期管理机制

企业应建立完善的数据治理制度，覆盖采集、传输、存储、使用及销毁等环节，确保符合《数据安全法》《个人信息保护法》与《通用数据保护条例》等相关法规。同时，应设立数据保护官与隐私审查机制，定期进行风险评估与合规审计，以实现数据安全的动态监管。

3) 行业协同：推动标准化与国际合作

行业应推动建立统一的隐私保护技术标准与安全认证体系，对智能客服系统进行等级评估与备案管理。对于跨境电商企业，可通过国际合作建立数据流通的合规认证与互信机制，以促进全球范围内的安

全数据交换。

4) 人机协同与最小化原则结合

在客服流程中可采用“AI 先行、人工兜底”的模式，通过分级响应体系减少用户数据在多环节中的重复处理，从而在保障服务效率的同时实现数据最小化使用原则。

5.3. 商业与生态发展方向

未来智能客服的发展将呈现出“开放化、生态化、服务化”的趋势。大型平台可与第三方 AI 企业共建开放生态，形成可插拔式智能客服插件体系，允许中小企业低门槛接入。同时，通过 SaaS 化部署模式与按需定制微调，实现成本共担与服务个性化。

此外，电商企业还应重视品牌信任建设，在交互界面明确区分 AI 与人工回复，增强用户透明度，并通过情感计算技术提升客服语气自然度与共情能力，从而增强用户对智能客服的接受度与品牌忠诚度。

5.4. 伦理与政策建议

大模型的广泛部署不仅是技术问题，更涉及伦理与社会责任。为规范行业发展、平衡智能化与人本化之间的关系，应从政策引导与社会治理两方面加以完善。

1) 强化伦理治理与透明责任机制

企业应建立 AI 伦理审查制度，确保智能客服在内容生成、用户交互与决策过程中遵循公平、透明与可追溯原则。应对模型偏见、歧视性表达等潜在风险进行预警与干预，保障不同用户群体的平等体验权。

2) 推动行业标准与监管政策完善

建议政府部门与行业协会制定智能客服系统的标准化指南，涵盖回答准确率、隐私安全性、模型透明度与应急处理机制等维度。同时，可建立黑箱测试与风险备案机制，定期抽检 AI 客服回答内容，防止错误传播与信息误导。

3) 履行社会责任与保障劳动权益

随着 AI 客服对人工岗位的部分替代，企业应承担相应的社会责任。可通过转岗培训与职业再教育计划，帮助客服人员向模型管理、数据标注、质量评估等新兴岗位转型，避免就业结构的单一化冲击。政府亦可出台行业用工指导政策，保障人机协同环境下的劳动者权益与职业安全。

6. 结论

本文重点针对“大模型驱动的智能客服在电子商务领域里的应用状况以及所面临的诸多挑战”来开展相关的研究工作。大模型依靠着自身颇为强大的语义理解和生成能力，在当下正逐步变成推动电子商务智能客服向前发展的关键力量。从实际应用的角度来讲，大模型客服可达成更为自然的那种人机交流状态，同时还能给出更为高效的针对用户需求的回应，并且能够实现对多语种以及多场景的服务范围覆盖，进而为平台去优化用户的使用体验、提高运营工作的效率开拓出全新的解决办法。不过经过研究同时也察觉到，现阶段的大模型在技术所具备的可靠性方面、数据的安全保障方面、商业应用的实际落地情况以及伦理责任等相关领域，依旧存在着不少较为棘手的挑战。

对于上述所提及的问题，本文给出了一些相应的对策以及发展方面的建议。其一，要积极推动大模型针对特定行业的训练工作，并且加强知识方面的增强举措，以此来提高其在电商领域所具有的专业适配程度。其二，需要进一步强化有关数据安全以及隐私保护的相关机制，从而保证智能客服能够在一个既合规又具备可信度的框架范围之内正常运行。其三，推动人机协同客服体系建设，充分发挥人工与智能客服的互补优势，兼顾服务效率与情感关怀。其四，完善伦理与社会责任框架，大力推动行业标准以及监管政策朝着更加完善的方面去发展，进而有效减少可能出现的诸如偏见、歧视以及就业风险等潜在

情况。其五，得引导企业积极开展对可持续商业模式的探索活动，通过这样的方式来降低中小企业在应用相关技术时所面临的门槛限制。

综上所述，大模型驱动的智能客服在电子商务中具有广阔前景，但其发展仍处于探索与优化阶段。未来，随着大模型技术的不断演进和行业应用的深入，智能客服有望在提升用户体验、促进产业升级和推动数字经济发展方面发挥更为重要的作用。同时，业界和学界需要共同努力，推动技术创新与规范治理的协同发展，以实现人工智能与电子商务的健康融合。

参考文献

- [1] 张小朝. AIGC 在商旅行业中的应用探索[J]. 广东通信技术, 2024, 44(1): 75-79.
- [2] 杨希军, 孔红芳, 赵东, 等. 自然语言方法提取油井修井施工信息提高智能化效率[J]. 石油钻采工艺, 2024, 46(4): 492-508.
- [3] 邓鸿志, 邓鸿丽, 任文. DeepSeek 赋能商业银行的逻辑机理、技术路线与应用场景研究[J]. 经济研究参考, 2025(5): 79-94.
- [4] 曹亚菲. AI 新征途——万物皆可模型化[J]. 软件和集成电路, 2023(6): 16-20.
- [5] 许蓓莹. 融合传承人社交关系的非遗内容推荐方法研究[D]: [硕士学位论文]. 西安: 西安建筑科技大学, 2024.
- [6] 王辉. 基于多模态理解与推理的视觉问答技术研究[D]: [博士学位论文]. 合肥: 合肥工业大学, 2023.
- [7] 徐睿璇, 冯逸超. 从探索到实践: 金融大模型的应用现状、挑战与政策建议[J]. 西部金融, 2025(3): 17-21.
- [8] 李泳佳. 数字经济背景下跨境电子商务发展的机遇与挑战研究[J]. 中国商论, 2025, 34(3): 39-42.
- [9] 王智, 夏树涛, 毛睿. 基于边缘智能的沉浸式元宇宙关键技术与展望[J]. 大数据, 2024, 10(1): 35-45.