Sustainable Development 可持续发展, 2024, 14(3), 710-718
Published Online March 2024 in Hans. https://www.hanspub.org/journal/sd
https://doi.org/10.12677/sd.2024.143081

Hans汉斯

大模型驱动下的产业应用生态：内涵、演进与挑战

常永波，姚亦非，陈俊琰*

中国信息通信研究院华东分院，上海

收稿日期：2024年1月15日；录用日期：2024年2月27日；发布日期：2024年3月29日

摘　要

随着深度学习技术的快速发展，大模型已成为人工智能领域的研究热点和产业应用的核心驱动力。本文旨在全面解析大模型在产业应用中的生态体系，从其定义、发展历程、技术原理、产业环节、政策环境、企业动态、创新生态、风险挑战到未来趋势进行深入的学术探讨。通过本文的研究，我们希望能够为相关决策者、研究者和企业提供全面、深入地了解和参考，推动大模型技术和产业的健康、可持续发展。

关键词

大模型，产业应用，生态体系，创新生态，安全可信

Industrial Application Ecology Driven by Large Models: Connotation, Evolution and Challenges

Yongbo Chang, Yifei Yao, Junyan Chen*

East China Branch of China Academy of Information and Communications Technology, Shanghai

Received: Jan. 15th, 2024; accepted: Feb. 27th, 2024; published: Mar. 29th, 2024

Abstract

With the rapid development of deep learning technology, large-scale models have become a research hotspot in the field of artificial intelligence and a core driving force for industrial applications. The purpose of this paper is to comprehensively analyze the ecosystem of large-scale mod-

*通讯作者。

文章引用: 常永波, 姚亦非, 陈俊琰. 大模型驱动下的产业应用生态: 内涵、演进与挑战[J]. 可持续发展, 2024, 14(3): 710-718. DOI: 10.12677/sd.2024.143081

els in industrial applications, and conduct in-depth academic discussions from its definition, development history, technical principles, industry chain structure, policy environment, enterprise dynamics, innovation ecology, risk challenges to future trends. Through the research in this paper, we hope to provide a comprehensive and in-depth understanding and reference for relevant policymakers, researchers and enterprises, and to promote the healthy and sustainable development of big model technology and industry.

Keywords

Large-Scale Model, Industrial Applications, Ecosystem, Innovation Ecology, Safe and Trustworthy

Copyright © 2024 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

随着人工智能技术的飞速发展，深度学习作为其核心技术之一，正在引领着新时代的科技变革。大模型，作为深度学习技术的重要组成部分，以其强大的表征学习能力和泛化性能，在图像分类、自然语言处理、语音识别等领域取得了显著的成果。然而，大模型的研究和应用仍然面临着诸多挑战和问题，如模型的可解释性、计算资源的消耗、数据的隐私和安全等。因此，本文将从学术的角度出发，对大模型在产业应用中的生态体系进行全面的研究和探讨。

2. 大模型定义与发展历程

1、定义与内涵

2023 年，ChatGPT 的崛起使大模型成为科研、产业及社会各界的热点，推动众多创新产品形态与商业模式的出现。尽管大模型的精确定义尚未统一，但普遍被视为“大规模预训练模型”的简称。大模型指深度学习模型，具有大量参数和复杂结构，通过摄取海量数据进行训练，捕获数据背后的深层结构和潜在关联，为多种复杂任务提供解决方案，具有强大的表征学习能力和泛化性能。大模型可按应用场景分为通用和行业大模型，前者具备强大泛化能力，后者针对特定领域微调；按技术路线主要分为基于 GPT 和 BERT 两类，GPT 在 GPT-3 发布后逐渐成为主流；按模态划分包括自然语言处理(NLP)、计算机视觉(CV)、多模态及科学计算等大模型。

2、发展历程

从历史发展的视角审视，人工智能模型的参数规模经历了显著的演变过程，即从无参数状态逐渐增长到当前的“通用大模型结合专用小模型”的复合结构。早期的专家系统主要依赖人类专家的推理模式来构建计算机模型，以解决现实世界中需要专业解读的复杂问题，这些系统并不需要使用参数。然而，随着机器学习的兴起，模型的学习过程开始涉及参数，通常仅需几百到上千个参数即可完成学习任务。深度学习技术的出现进一步推动了参数规模的扩大，达到了万级水平。

近年来，随着超级智能计算、千亿级参数模型和 TB 级多模态数据的广泛应用，这一领域已经形成了主流的技术发展路线。行业领军企业正加速布局，推动技术的普及和应用；同时，计算速度快、专用性强的专用小模型也在不断发展，与通用大模型相互协同，形成了“通用大模型 + 专用小模型”的技术格局。展望未来，量子计算、类脑技术等新兴技术有望带来全新的理论体系变革，可能在自监督或无监

督学习方式下降低对参数规模的需求。

从技术发展的路径来看，自然语言处理领域是大模型技术最早取得突破性进展的领域[1]。自 2017 年至今，该领域已经历了三代的技术演进。具体而言，2017 年 Google 提出了基于自注意力机制的 Transformer 架构，这一创新为大模型预训练算法架构的发展奠定了基础。2018 年，以 OpenAI 的 GPT-1 和谷歌的 BERT 为代表的第一代大模型应运而生，尽管其模型规模相对较小，处于十亿级以下。到了 2020 年，OpenAI 公司推出了参数规模超过千亿的 GPT-3 模型，标志着第二代大模型的诞生。GPT-3 在零样本学习任务上实现了显著的性能提升，此后，基于人类反馈的强化学习、代码预训练、指令微调等策略相继出现，进一步提升了模型的推理能力和任务泛化性能；而第三代大模型则以搭载了 GPT3.5 的 ChatGPT 为代表，其具备高度逼真的自然语言交互能力和多场景内容生成能力，迅速在互联网领域引起了广泛关注和应用。

3. 大模型产业环节及发展意义

1、产业环节

大模型产业是一个多层次、专业化的生态体系，包括基础层、模型层、工具层、生态层和应用层(如图 1)。在基础层，智能算力、大规模数据集和高级算法等关键技术为大模型提供了坚实基础；智能算力依赖 AI 芯片、算力调度等技术确保高效训练和推理；大规模数据集经过处理提供丰富训练样本；高级算法实现高效学习和精准预测。在模型层，基础大模型的构建和训练是核心，具备强大表征学习和迁移学习能力；模型开发训练平台支持快速开发和部署。工具层包括 MaaS 服务商、模型开发平台等，提供全面支持。生态层涉及政策、开源社区等方面，提供良好生态环境和支持。应用层中大模型已渗透到多个领域，如自然语言处理等，提高工作效率和用户体验，推动相关行业创新和发展。

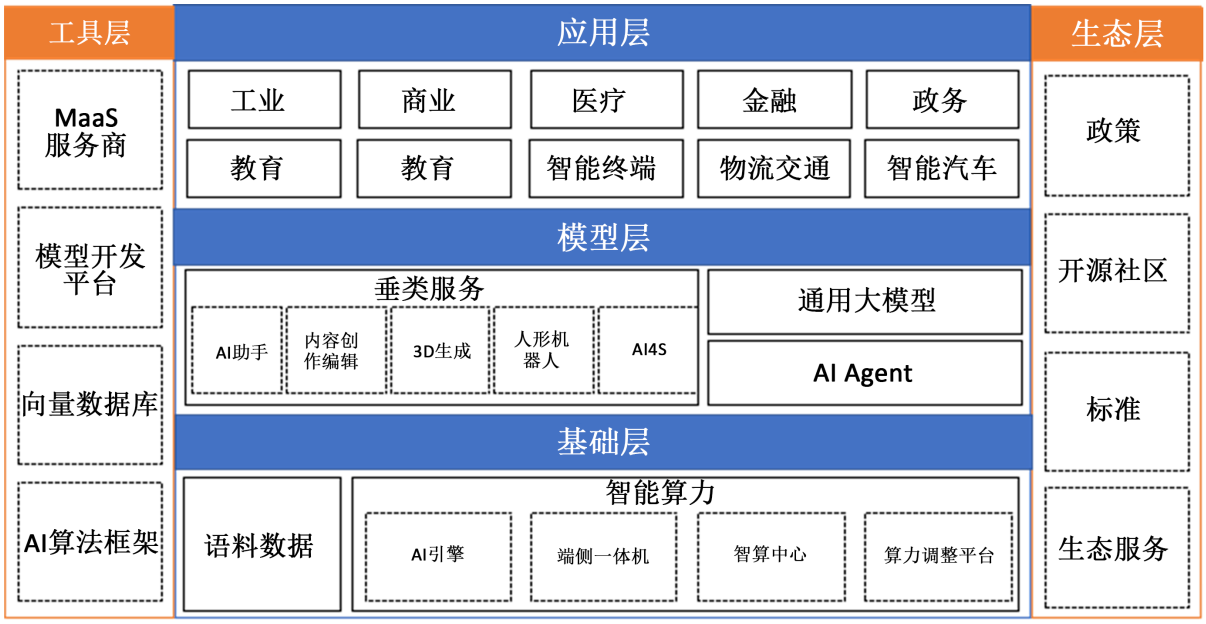


Figure 1. Large model industry link
图 1. 大模型产业环节

2、发展意义

大模型在人工智能领域的发展具有重大战略意义，体现在国家策略、产业升级和社会应用多个层面。在国家层面，发展大模型对于掌握 AI 战略制高点至关重要，独立研发和创新以构建自主知识产权的大模型

技术体系，对确保国家长期发展和安全具有不可估量的价值。在产业层面，大模型的进步推动 AI 产业向更高质量发展，促进相关领域的协同发展，包括模型训练、软硬件技术、开源算法、标准化和测试验证等，并驱动 AI 芯片、计算基础设施和软件平台等产业的创新与壮大。在社会应用层面，大模型促进 AI 与实体经济的深度融合，推动社会数字化转型，支持各行业的产品和应用创新，提升生产效率和服务质量，降低 AI 应用开发难度和成本，助力传统产业实现数字化转型和智能化升级，创造新的商业价值和竞争优势。随着技术进步和应用场景拓展，大模型将持续推动 AI 领域的创新和发展，为社会的进步和发展做出更大贡献。

4. 大模型政策规划与企业动态

1、政策规划

随着人工智能技术的飞速发展，大模型作为其核心组成部分，在全球范围内引发了广泛的关注。各国政府、科研机构和企业纷纷加快了对大模型技术的研发和应用，并制定了一系列针对性的政策规划，以期在人工智能领域取得领先地位。各国在大模型政策规划上呈现出以下特点(表 1)：一是注重技术的安全性和可控性；二是关注技术的伦理和治理问题；三是推动大模型技术在重点领域的创新应用；四是加强人才培养和引进工作。随着大模型技术的不断发展和广泛应用，各国政府和企业需要进一步加强合作与交流，共同应对挑战并推动人工智能技术的可持续发展。

Table 1. Characteristics of large model policy planning in major countries/regions
表 1. 主要国家/地区大模型政策规划特点

国家/地区	政策规划	特点
美国	科技巨头推动技术进步，政府加强监管与治理，注重技术安全性与版权问题。成立新数据工作组，增加透明度，发展审计机制。版权局发布指南应对生成式 AI 版权问题。	科技驱动，安全版权并重；政府与企业合作推动发展。
欧洲	强调伦理和治理，关注数据安全、偏见歧视和知识产权保护。欧盟拟在《人工智能法案》中新增大模型监管条款，成立 ChatGPT 特别工作组加强合作[2]。英国等发布草案和指南缓解风险。	伦理导向，注重治理；多国合作共同应对挑战。
其他国家	加速大模型研发应用，沙特和阿联酋购买先进芯片开发开源大型语言模型，韩国推动 AI 与数字技术在内容创作和传播领域融合。	创新驱动，聚焦特定领域与技术融合；借助外力加速发展。
中国	政府加大对大模型领域投资和研究，鼓励企业、研究机构和高校合作。发布法规规范大模型技术应用和发展，中共中央政治局会议强调重视通用 AI 发展、创新生态与风险防范。	投资引导，法规与技术共进；政府主导下多方参与推动发展。

资料来源：根据公开资料整理。

省市级层面，北京、深圳、上海、成都等率先推出大模型整体发展政策，强调场景落地的重要性。各省市在大模型政策规划上呈现出以下特点(表 2)：一是强调场景落地和应用创新；二是推动核心技术突破，加强产学研合作；三是营造一流创新环境，凸显地域优势及特色。随着政策的不断落地和实施，我国大模型技术的发展和应用将迎来更加广阔的前景和机遇。

2、企业动态

大模型的崛起标志着人工智能进入通用人工智能(AGI)时代，其卓越泛化性、通用性和迁移性正推动多领域变革，并有望成为推动全球经济、重塑产业格局、巩固国家竞争优势的关键技术。此趋势预示人类社会将迈向通用 AI 时代，催生新技术、新产业和业态。在技术和模型推动下，AI 大模型正逐步标准化和规模化，增强产业化应用基础，为实现 Maas 生态奠定基础。当前，国际大模型竞争激烈，中美两国发

Table 2. Characteristics of large-scale model policy planning of major provinces/cities
表 2. 主要省/市大模型政策规划特点

省/市	政策举措	特点描述
北京	政策推动场景创新，明确政务金融和商业化应用领域。设立创新标杆试点工程，提出量化目标以加速商业化落地。	场景驱动，量化目标推动技术应用。
深圳	搭建供需对接平台，推进 AI 融合应用模式。聚焦制造业数据问题，建立闭环机制以推动大模型技术应用。	供需对接，制造业数据闭环推进。
上海	全面支持大模型创新，鼓励研发先进大模型，并给予奖励。提升智能算力，构建智能芯片生态，共享语料数据资源。打造国际竞争力。	创新支持，智能算力与生态共享。
成都	加强算力基础设施建设，引导超算和智算中心扩容。布局通用智能算力和全栈运行环境，支持关键算法研发，推动大模型技术创新和迭代。	算力强化，核心技术突破与迭代。

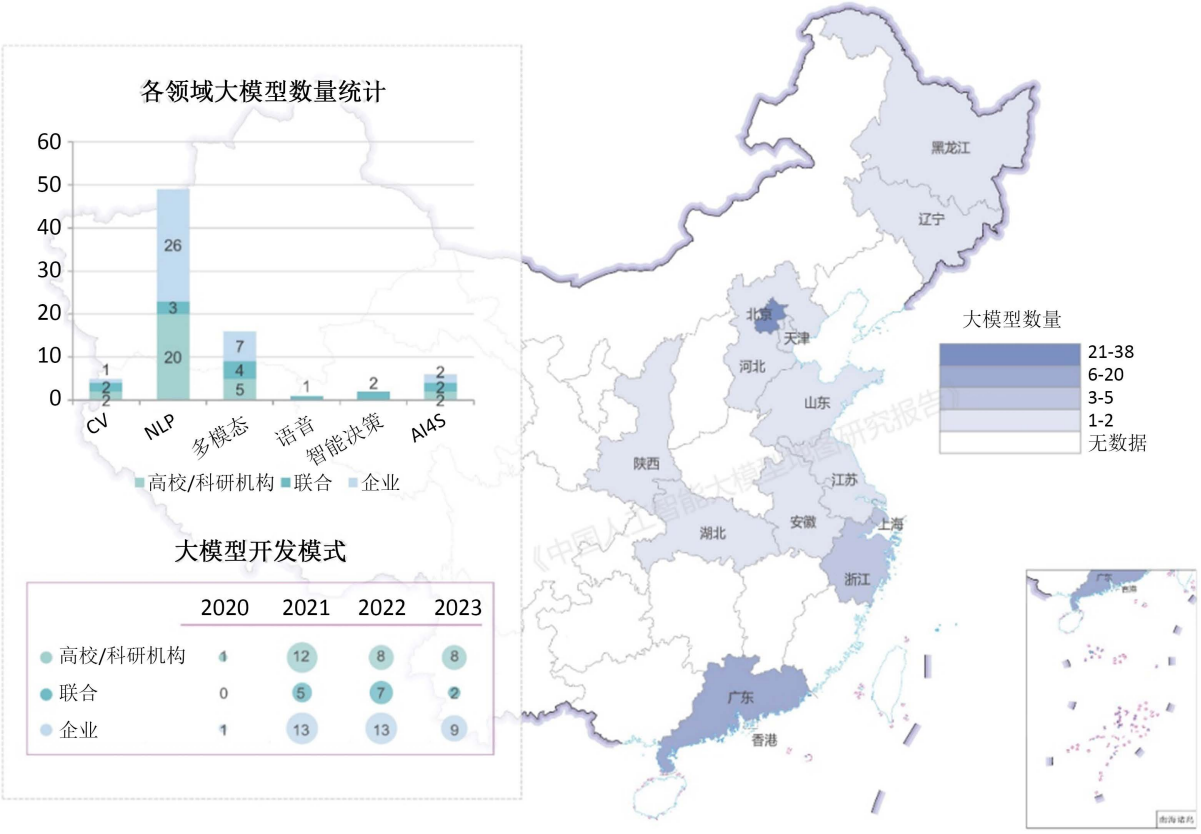
资料来源：根据公开资料整理。

布的大模型占全球超 80%，美国居首位，显示其在算法模型研发上的领先地位(表 3)。国内大模型发展呈“通用”与“垂直”并行趋势，但处于应用早期；通用大模型如百度文心、阿里通义等具备较强通用性和泛化能力；垂类大模型则通过通用和专用预训练实现业务场景应用，解决垂直领域或特定任务问题。

Table 3. Typical large models at home and abroad (incomplete statistics)
表 3. 国内外典型大模型(不完全统计)

类别	模型	主体	参数规模	数据规模	是否开源
NLP-文本生成	GPT-3	OpenAI	175B	45TB	否
	PaLM	Google	540B	3.6TB	否
	LLaMA	Meta	7B-65B	1.4TB	否
	Claude	Anthropic	520 亿	/	是
	MOSS	复旦大学	百亿	/	是
	ChatGLM-6B	清华大学	62 亿	/	是
	讯飞星火	科大讯飞	1000 亿	/	是
CV-图像生成	DALL-E 2	OpenAI	/	2.5 亿个图像文本对	否
	Midjourney V5	Midjourney	/	亿级	是
	Stable Diffusion	Stability.AI	/	/	是
	NovelAl	Novell	/	21 亿张图片	是
	文心一格	百度	/	/	是
多模态－跨模态	Gemini	Google	/	26TB	否
	GPT-4	OpenAI	1.8 万亿	13TB	否
	PALM-E	Google	5620 亿	0.78TB	否
	文心一言	百度	2600 亿	4TB	是
	通义千问	阿里	100 万亿	3TB	是
	日日新	商汤	千亿级	/	否
	盘古	华为	1000 亿	40TB	否
	混元	腾讯	1000 亿	2TB	否
科学计算	AlphaFold2	DeepMind	9300 万	17 万个蛋白质结构	是
	HelixFold 大模型	百度	/	/	是
	华为·气象大模型	华为	/	/	否

《中国人工智能大模型地图研究报告》数据显示(图 2)，北京、上海、广东和浙江在大模型发展上领先。科技大厂如百度、阿里和华为在算力层、平台层、模型层和应用层全面布局，垂直行业科技企业和科研院校则专注于大模型算法及细分领域应用的研发。应用前景显示，企业在前期以内部应用为主，后续将主要向 B 端企业拓展服务，少数企业预计在 C 端市场形成规模。目前，百度文心一言大模型已全面开放，阿里通义千问和腾讯混元助手等也在拓展 C 端市场应用。总体而言，国内大模型的研发与应用处于初级阶段，实际落地应用仍在探索中，与美国领先企业存在差距。因此，需加强自主研发和创新能力，推动国内大模型技术的快速发展和应用落地，并关注数据隐私和安全等问题，确保符合伦理规范和法律法规的要求。



资料来源：《中国人工智能大模型地图研究报告》。

Figure 2. Distribution of large models in key provinces and cities in my country
图 2. 我国重点省市大模型分布情况

3、创新生态

随着大模型技术的显著进步，从算法架构到计算并行加速，全球范围内的研发活跃度都在不断攀升。但在这一技术繁荣的背后，大模型的商业化落地却仍处于初级阶段，面临着众多亟待解决的问题。

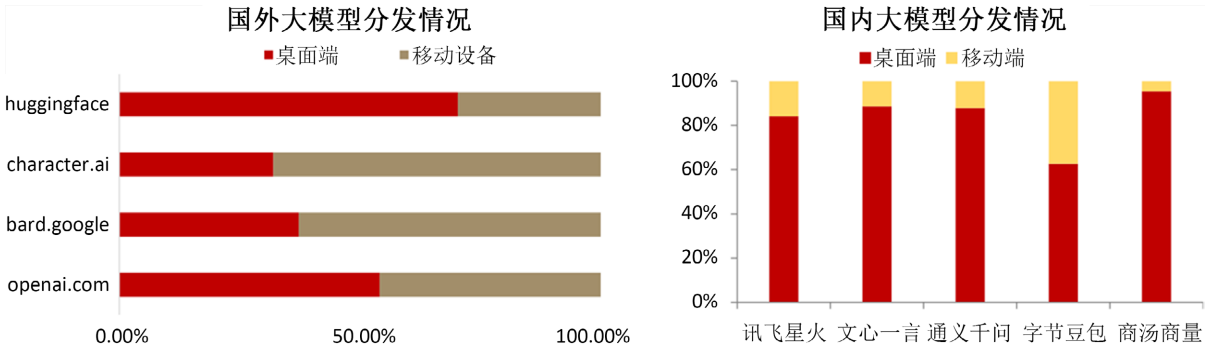
一方面，尽管技术进步显著，但如何将大模型技术有效地产品化并推向市场，仍是众多研发机构的首要难题。这不仅仅是技术转移的问题，更多地涉及对市场需求的深入理解、商业模式的创新以及与下游企业的紧密合作。目前，许多研发机构对于大模型的实际应用和市场接受度还缺乏充分的认知，这导致了技术与商业之间的鸿沟。在大模型落地过程中，降低企业学习开发成本和计算成本，满足模型开发定制需求至关重要，可通过 PaaS (平台即服务)、产品封装、SaaS (软件即服务)、解决方案以及 API(应用程序接口)等形态实现[3] (表 4)。

Table 4. Introduction and advantages of large model product model
表 4. 大模型产品模式介绍及优势

产品模式	模式介绍	模式优势
PaaS 模式	此模式将大模型技术集成到 AI 平台上，为用户提供一套完整的工具和服务。用户可灵活选择并集成大模型到自有系统中。	降低了用户开发和部署模型的成本，同时提供了便利的支持，使得用户能够更专注于业务创新。
产品封装模式	该模式通过封装大模型到 AI 应用中，实现了模型与应用的紧密融合，提升产品整体性能。	提升了产品的性能和用户满意度，实现了模型与应用的无缝衔接。
SaaS 模式	此模式通过互联网提供软件服务，用户无需购买和维护软件，而是通过租用基于 web 的软件来管理企业经营活动。	降低了用户的使用门槛，使得更多的企业和个人能够享受到大模型带来的便利。
解决方案模式	此模式根据用户的特定需求进行定制化开发和应用，将大模型集成到解决方案中，满足特定场景需求。	根据用户的特定需求进行定制化开发和应用，易用性较高。
API 模式	该模式将大模型的推理能力封装成标准 API 接口，供下游企业快速集成和使用。	降低了企业应用大模型的成本和技术门槛，使得更多的企业能够利用大模型的能力提升自身业务的智能化水平；但模型的性能和质量可能会影响 API 的使用效果[4]。

另一方面，随着大模型技术的逐渐普及，智能流量经济开始崭露头角。这种新经济形态主要以大数据和 AI 技术为基础，通过精准地分析和预测用户行为，为企业带来更高的流量和收益。在这种背景下，如何将大模型技术融入现有的产品或服务中，以提升其智能化水平和用户吸引力，成为众多企业的新挑战。如图 3，全球大模型的访问数据为我们揭示了这一趋势的微观层面：海外大模型，尤其是 OpenAI，已经在这一领域取得了显著的领先；而在国内，虽然百度和讯飞等表现突出，但在移动端的应用仍显示出巨大的增长空间。

综上所述，全球大模型的商业化落地不仅面临技术和市场的双重挑战，同时也孕育着智能流量经济这一巨大的商业机会。对于研发机构和下游企业而言，如何紧密合作、共同创新，将是大模型技术从实验室走向市场的关键。



资料来源：方正证券。

Figure 3. Distribution of representative large models at home and abroad
图 3. 国内外代表性大模型分发情况

6. 大模型发展风险与挑战

随着人工智能大模型的广泛应用，与之相关的安全事件不断浮现，揭示了其在内容生成、自身安全

以及其他方面的多重风险；本文旨在深入剖析这些风险，并探讨当前及未来的前瞻性议题。如图 4，一是大模型在内容生成方面存在显著的安全隐患，其生成式攻击与防御问题日益突出，具体表现为虚假信息传播与网络攻击赋能。二是大模型的自身安全风险，如数据泄漏风险[5]，包括提示语泄漏、学习敏感数据导致的隐私泄漏和软件漏洞导致的数据泄漏等，已成为影响范围最广、危害程度最大的安全风险；伦理道德问题，大模型可能学习并输出有害内容，如仇恨言论，同时其具身化应用也引发了关于机器人责任和伦理的新问题；攻击对抗问题，大模型面临多种新型攻击手段，如提示语攻击、数据投毒攻击等，其安全防护亟待加强。除上述风险外，大模型的可解释性和公平性也是当前讨论的重点，

一是可解释性之谜[6]，大模型的黑盒本质使其推理逻辑难以解释，特别是当其出现“幻觉性”问题时，可解释性面临更大挑战；二是公平性考量[7]，大模型在参与现实决策时，必须考虑其公平性，当前的研究主要从提高训练数据质量和优化模型数据敏感性两方面着手。

	安全问题	形成原因	问题表现
生成内容风险	生成虚假信息	可低成本生成个性化高质量的虚假内容	在新闻信息等领域应用可能带来虚假信息泛滥风险
	侵犯知识产权	模型产生结果无法被监督，AI内容无法被鉴别	模型模仿创作风格、生产结果造成侵权行为
	深度伪造的金融支付	大模型AI换脸更加真实且难以辨别	深度合成技术攻破金融支付APP，造成严重的财产威胁
	滥用为网络攻击工具	大模型能够快速生成钓鱼邮件等网络攻击工具	大模型的滥用成为网络攻击者手中新的攻击利器
自身安全风险	隐私泄漏问题	训练数据涉及隐私，底层软件存在漏洞	用户、企业隐私信息被大模型输出
	伦理道德问题	大模型的有爱信息检测能力不健全	输出有害社会、思想、健康的不良信息
	数据投毒/模型后门	训练数据集规模庞大，无法人工标注检查	攻击者在训练数据集中添加恶意样本，模型产生错误输出
	数据重构/成员推断	大规模参数记住了训连数据细节	攻击者通过构建特殊查询，从模型参数中还原训练数据
	模型窃取	完成相同任务的模型具有类似网络结构和参数	攻击者通过大规模查询，生成替代模型
	海绵样本攻击	通过API、PaaS集中模式对外提供商业服务	构建高资源消耗调用阻碍其他用户正常使用
其他风险	大模型不可解释	参数规模庞大，使用多种并行加速技术	处理过程难以追踪，推理结果难以邮箱解释
	大模型公平性问题	大模型技术的不公平负面后果分配给被边缘化的社会成员，加剧社会不平等	大模型生产内容的意识形态、主观性别存在偏见

资料来源：《可信 AI 技术和应用进展白皮书(2023)》。

Figure 4. Security and trustworthiness challenges faced in the era of large models
图 4. 大模型时代下面临的安全可信挑战

7. 结论与展望

随着人工智能技术的深入研究与广泛应用，大模型已逐渐成为 AI 发展的核心驱动力，其在数字经济、科学研究、生活服务、数字治理等多个领域展现出了巨大的潜力和价值。本文全面解析大模型在产业应用中的生态体系，从其定义、发展历程、技术原理、产业环节、政策环境、企业动态、创新生态、风险挑战到未来趋势进行深入的学术探讨。在发展趋势方面，垂直落地已成为大模型发展的重要趋势之一，特定领域的需求正在推动大模型向专业化发展，通过针对性的训练和优化策略，大模型在各行业的应用效果和创新能力将得到显著提升；同时，多模态与具身智能的融合发展也将为大模型带来新的机遇，大模型正在引领非结构化、多模态数据处理的新范式[8]，结合具身智能的发展，将催生出更多面向个体的新型生产力应用[9]；此外，开源开放策略对于大模型的发展也至关重要，打破技术壁垒、实现商业落地

需要开源开放的策略，这将促进底层技术的创新合作和共同进步；然而，随着大模型的广泛应用，伦理、监管与可信技术的问题也日益凸显，对大模型的监管评测工作以及对可信技术的探索和实践将更加重要。

展望未来，大模型的发展将进入一个更加成熟和多元化的阶段。跨模态理解与生成、可解释性与透明度增强、自适应学习与持续学习以及安全与隐私保护等方向值得进一步深入研究。随着技术的不断进步和应用需求的持续增长，大模型必将在未来的人工智能领域中扮演更加重要的角色；通过不断地研究和创新，我们有望见证大模型在推动人工智能发展、赋能各行各业以及提升人类生活品质方面的巨大贡献。

基金项目

本项研究受到上海市 2023 年度“科技创新行动计划”软科学研究项目(项目编号 23692102200)资助。

参考文献

[1] 郭华源, 刘盼, 卢若谷, 杨菲菲, 徐洪丽, 庄严, 黄高, 宋士吉, 何昆仑. 人工智能大模型医学应用研究[J]. 中国科学: 生命科学, 2024, 54(3): 482-506.

[2] 王卫. 欧盟《人工智能法案》实行风险分级监管[N]. 法治日报, 2023-12-18(005).

[3] 罗军舟, 金嘉晖, 宋爱波, 等. 云计算: 体系架构与关键技术[J]. 通信学报, 2011, 32(7): 3-21.

[4] 马祥跃, 杜晓婷, 采青, 郑阳, 胡峭, 郑征. 深度学习框架测试研究综述[J]. 软件学报, 2024: 1-33. https://doi.org/10.13328/j.cnki.jos.007059

[5] 郑志峰. 人工智能时代的隐私保护[J]. 法律科学(西北政法大学学报), 2019, 37(2): 51-60. https://doi.org/10.16290/j.cnki.1674-5205.2019.02.005

[6] 刘艳红. 人工智能的可解释性与 AI 的法律责任问题研究[J]. 法制与社会发展, 2022, 28(1): 78-91.

[7] 刘文炎, 沈楚云, 王祥丰, 等. 可信机器学习的公平性综述[J]. 软件学报, 2021, 32(5): 1404-1426. https://doi.org/10.16290/j.cnki.1674-5205.2019.02.005

[8] 刘学博, 户保田, 陈科海, 等. 大模型关键技术与未来发展方向——从 ChatGPT 谈起[J]. 中国科学基金, 2023, 37(5): 758-766. https://doi.org/10.16262/j.cnki.1000-8217.20231026.004

[9] 钟新龙, 渠延增, 王聪聪, 等. 具身智能产业发展动向及创新能力研究[J]. 软件和集成电路, 2023(11): 62-73. https://doi.org/10.19609/j.cnki.cn10-1339/tn.2023.11.010