

基于信息化视野的高职院校教学管理优化探讨

文 ◆ 山东商业职业技术学院 李 健

引言

随着信息技术的快速发展，在教育领域的应用越来越广泛，并逐渐在学校教学管理工作中展现出一定优势，让传统教学管理方式发生了较大的转变，实现了教学管理模式的革新突破。对于高职院校管理人员而言，应意识到信息技术在教学管理中的应用价值，并且合理应用信息技术，做到将信息技术在教学管理工作中灵活应用，进而提升工作质量与效率，推动学校整体管理实力的有效增强。目前，高职院校教学管理中存在一些需要改进之处，基于此，本文重点探讨了信息化视野下的教学管理优化策略。

1 教学管理信息化概述

1.1 教学管理信息化的概念和内涵

教学管理信息化是指在教育领域引入现代信息技术与有关设备和理念，改进和优化教学管理的各项工作。核心目的是通过技术手段提升教学管理的效率和质量，使教育管理不仅仅依赖传统的人工操作和纸质文件，更加依赖于信息系统的自动化、数字化管理。信息化手段能够实现数据的实时共享、教学资源的高效利用和管理决策的科学化，从而更好地服务于教学工作，最终提升教育质量和学校的办学水平^[1]。

1.2 教学管理信息化的作用

高职院校的教学管理工作通常有着较高的动态性和复杂性，涉及大量学生、教师、课程、设施等要素，管理任务繁重且多变。管理人员需要在众多细节中进行决策与协调，不仅要应对来自教育政策和社会需求的压力，还要关注学校内部的教学质量、师资力量和学生培养等问题。通过信息化系统，学校可以减少人工干预，自动化完成大部分日常工作，让管理人员将更多时间用于决策和问题解决。此外，信息化系统还能实现数据的实时更新和查询，保证教学管理的时效性和准确性。通过信息化，学校能够实现资源的最优配置和动态调整，提高学校整体的管理水平，还能帮助管理人员摆脱传统模式的束缚，从而更好地应对现代教育中日益复杂的管理任务。信息化的推广也使学校能够快速响应外部环境的变化，提高教育管理的社会适应性。

2 现阶段高职院校课程管理信息化管理现状

2.1 教师对数字化价值的认识不够清晰

在当前信息化时代，数字化课程管理已成为提高教育质量、优化管理效率和推动教育现代化的重要手段。然而，许多高职院校的教师对于信息化建设的认识仍然较为模糊，缺乏对数字化管理带来变革的深刻理解。许多教师仍旧习惯于采取传统的课程管理方式，如手工记录成绩、人工排课和传统的学生考核方式等。这些传统方式虽然在过去曾有效，但在现代教育环境下，无法应对复杂的课程管理需求和日益增多的教学资源。因此，教师在教学过程中耗费了大量的时间和精力，导致管理难度增加，效率

【作者简介】李健（1988—），男，山东济南人，研究生，讲师，研究方向：建筑环境设计及其理论研究。

低下，且人力物力的浪费也无法避免^[2]。

2.2 课程管理方法过于简单

尽管近年来一些高职院校已经在课程管理上进行了改革与创新，尝试采用信息化手段来优化管理流程，但总体来看，许多学校在课程管理方面依然停留在简单、传统的模式上，如排课、成绩统计等，仍然大多采取传统的管理方式，未能充分利用信息化手段进行有效跟踪与反馈。

3 信息化视野下高职院校教学管理优化路径分析

3.1 健全与完善高职院校信息化教学管理制度

首先，制定一套系统、科学的信息化管理机制，确保信息流的高效传递与管理，避免信息滞后和丢失。在此基础上，应加强信息化资源的管理与分配，建立健全的数字化管理平台，确保各项资源能够高效共享，提升管理效率。其次，学校可以利用大数据分析技术，对教学过程、学生表现、课程内容等多维度信息进行分析，以支持科学的教学评价体系建设。大数据不仅能帮助教师和管理者实时掌握教学进展和学生的学习情况，还能为个性化教学提供数据支持，提升教学质量。最后，高职院校还需要规范技术手段的使用，推进数字化教学体系的建设，做到教学与管理的有机融合，为信息化建设提供长期而稳定的制度保障。

3.2 强化信息化软硬件支撑

为顺利开展高职院校的信息化建设工作，学校不仅要在制度层面进行创新，还必须在软硬件方面做好充分的准备和支持。首先，高职院校需强化信息化建设

的顶层设计，制定科学合理的建设规划。这一规划应考虑学校的实际情况，如教学需求、管理需求以及未来的发展方向，清晰确定建设目标、任务与实施时间表，确保信息化建设的每一步都有明确的方向和目标。同时，学校需要注重技术的选择和研究，确保所选用的硬件和软件技术能够满足当前和未来的需求，具有较好的可扩展性和兼容性。除了硬 / 软件的选择外，高职院校还需加强和有关企业、研究机构与其他高校的合作沟通。通过与外部资源的共享与协作，学校引入先进的技术与管理经验，加快信息化建设速度^[3]。此外，高职院校还需增加信息化建设的资金投入，不仅要购买和升级硬件设施，还应进行教学平台、管理系统和教学软件的开发与购买。以某高职院校为例，该学校已制定数字化校园建设计划，升级了校园网络基础设施，扩展了无线网络覆盖面积，做到了整个校区的全时段、全区域的无线网络覆盖，满足了师生对网络资源的需求。并且，学校提高了网速与带宽容量，确保教学过程中能够支持高清视频、在线实验等大流量、高带宽需求的应用。为了配合信息化教学的发展，每个教学场所还装配了现代化的网络终端设施与交互式多媒体设备，解决了教师在课堂上灵活使用线上与线下教学资源的要求。

3.3 完善数字化资源建设

(1) 制定长期发展规划。学校应确定数字化资源的具体目标、战略定位、发展方向和技术路线，保证规划和学校总体战略保持相同步调。在规划过程中，要考虑未来技术的快速变化，预见数字化教育领域的新趋势，并根据学校的特色与需求合理规划资源的布局。(2) 整合和共享资源。学校应对现有的数字化资源进行全面盘点，识别冗余资源和不足之处，并创建数字化资源库或平台，集中管理各类资源，方便师生统一使用和共享。在整合过程中，学校可以与其他高校、企业或科研机构进行合作，借助外部资源扩展数字化资源的范围。此外，还应加强资源的维护与更新，确保资源的时效性和适用性，避免出现过时或重复建设的情况。(3) 更新与升级资源。学校应定期评估数字化教学资源的使用情况，并结合课程和技术发展的需求对资源加以改进。特别是对计算机、人工智能等技术类课程，资源的更新显得尤为重要。同时，学校应注重实践性课程的数字化建设，推出更多互动性、实验性强的数字化教学内容，增强学生的动手能力和实践经验^[4]。

3.4 提升师生的信息化应用能力

教师是数字化教育实施的关键力量，因此提高教师的信息技术应用能力是推动数字化转型的核心内容。学校应定期开展专业培训，帮助教师了解数字教学资源的制作方法、课件设计技巧、线上平台的使用方式等。培训内容不仅应涵盖信息技术的基本知识，还应结合教学实际，帮助教师灵活运用信息技术提升课堂教学效果。此外，学校应设立教师交流平台，定期邀请教师分享教学期间使用信息技术的经验和遇到的挑战，增强教师之间的相互学习与支持。学生的信息素养是数字化教育成功的另一关键因素，因此学校需要通过多种途径提升学生的信息技术应用能力。学校应开设信息技术基础课程，保障学生能够掌握常用的计算机操作技能和软件工具使用能力，为其后续学习和工作打下基础。

3.5 健全信息化教学评价与反馈机制

信息化教学评价机制应采纳多种评价方式，既包括定量的评价，又包括定性的评价。定量评价通过具体的数字和标准，使学生的成绩更为直观和客观，但仅依赖定量评价容易忽视学生的过程性表现和非认知能力的培养。因此，定性评价能够弥补这一不足，全面反映学生的综合能力与成长。通过这两者的结合，可以确保学生在知识、技能和情感态度等方面都得到全面评价与发展。凭借信息技术工具，教学评价可以实现对学生学习过程的全程监控与数据化管理。例如，通过学习管理系统收集学生的课堂出勤、作业提交、在线讨论参与情况、学习进度等数据，教师可以实时掌握学生的学习动态，及时发现学习中的薄弱环节。通过大数据分析，识别出学生在学习中的个性化需求、潜在问题和学习障碍，针对性地调整教学策略，提供个性化的辅导和支持。此外，利用收集的数据还可以帮助学校进行教学质量的评估与改进，从宏观层面发现教学中普遍存在的问题，优化课程设计和教学方法。信息化教学评价体系的核心之一是快速、高效的反馈机制。教师通过信息技术手段，可以在第一时间向学生反馈他们的学习成绩和表现。及时的反馈不仅能帮助学生了解自己在知识掌握和技能提升上的差距，还能鼓励学生发现问题并主动采取改进措施。学生通过学习管理平台查看自己的学习进度、成绩分析报告和教师评语，从而清晰地了解自己的优势和不足。有效的反馈机制还能增强学生的学习动机，激发他们的学习兴趣，并帮助学生调整学习策略，增强学习效果^[5]。

3.6 增强教学信息管理的开放性和互动性

教学管理平台的建设不仅是教学管理的工具，还是促进学生与企业、社会之间联系的重要纽带。高职院校应通过信息化手段建设更为开放的实践环节管理系统，使学生能够在平台上查看与企业合作的项目，获取企业的实践机会。平台的建立能够有效打破学校与社会、企业之间的壁垒，帮助学生在校期间就能接触到真实的行业需求，提升他们的实践能力和就业竞争力。教学管理平台不仅是教师管理学生的工具，还能教师与学生之间的双向互动提供便利。教师通过平台实时查看学生的学习进展，分析学生的学习数据，及时调整教学策略，并根据学生的反馈提供个性化的教学辅导。同时，学生通过平台随时与教师进行沟通，提出学习过程中遇到的问题和困惑，教师可以为学生提供针对性的解答与指导。这种互动不仅能提高学生的学习兴趣，还能加强师生之间的联系，使教师更深入地了解每个学生的学习需求和心理状态，进而提升教学质量。高职院校的教学管理应当具有高度的开放性，鼓励社会、企业、校友等外部资源的参与，丰富学生的学习体验和实践机会。同时，学校还鼓励毕业生与在校学生分享自己的工作经验，解决学生在职业发展过程中可能遇到的问题。通过这种开放性管理，学生不仅能够获得更为广泛的学习资源，还能在实践中获得更多的锻炼机会，增强其就业能力与社会适应能力。

结语

互联网以及信息技术的不断创新发展，带动了高职院校教学管理模式的转变，使之管理水平大幅提高，同时也促使教学质量获得了明显的提升。高职院校应高度重视对学生以及教职员工信息技术应用能力的培养，特别是在信息化时代背景下，需要合理引入信息技术，科学开展教学工作的信息化管理，并结合信息技术改进传统的教学模式，全面提升教学管理质量，为社会培养出更多优秀人才。■

引用

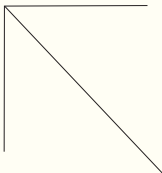
[1] 孙强,周玲.新时期下高职院校教学管理信息化建设策略研究[J].湖北开放职业学院学报,2024,37(1):166-168.

[2] 余丽.大数据背景下高职院校教学管理研究[J].西部学刊,2023(14):104-107.

[3] 徐来.“互联网+”背景下高职院校教学管理改革探析[J].中国新通信,2023,25(6):170-172.

[4] 黎诗琳.信息化视角下高职院校教务管理的优化对策[J].文化产业,2021(21):163-164.

[5] 刘明波,王从兵.大数据时代下的高职院校教育教学管理信息化策略[J].中阿科技论坛(中英文),2021(6):93-95.



新时代网信工作观的 生成逻辑、科学内涵和实践价值*

文◆山西工商学院 计算机信息工程学院 王 斌

引言

近年来，党中央瞩目新时代不断推进理论创新和实践创新，提出了一系列新思想、新观点、新论断，其中包括了关于网络和信息化建设的相关思想观念，可以将其统称之为“新时代网信工作观”。新时代网信工作观作为新时代网信建设管理相关工作的重要思想和系统观念，为各单位网信事业发展提供了根本遵循和行动指南。目前，学界对于新时代网信工作观中的某一具体内容进行研究较多，而整体性研究相对较少，尤其系统阐述研究新时代网信工作观的更少。本文深入应用“习近平新时代中国特色社会主义思想的世界观和方法论”这个研究问题、解决问题的“总钥匙”，来理解新时代网信工作观的生成逻辑、科学内涵和实践价值，以确保网络和信息化建设人员在工作中做到方向明确、头脑清醒、应对有方、行动有力。

1 新时代网信工作观的生成逻辑

新时代网信工作观的形成是

党中央从信息化发展大势和国内国际大局出发提出，其生成逻辑表现既包含了“实践—认识—再实践”的实践逻辑，又包含了“观察时代、解读时代、引领时代”的发展逻辑^[1]。

1.1 时代考验：用网治网能力是执政能力的重要方面和体现

互联网是重要的执政条件，网络空间是重要的执政环境，用网治网能力是重要的执政能力体现。第一，互联网带来了新的发展机遇，也带来了风险挑战，党中央面临着代表互联网先进生产力的时代考验。第二，网络意识形态工作已成为重中之重，党中央面临着代表网络先进文化的时代考验。第三，网络信息安全是当前人民群众亟须得到的保障，党中央面临着守护人民网络利益的时代考验。网络安全已成为非传统安全领域最严峻、最复杂、最现实的问题之一，网信领域已成为大国、强国竞争博弈的重点。在网络和信息技术仍在加速迭代升级和融合应用的年代，党中央提出了“过不了互联网这一关，就过不了长期执政这一关”“得网络者得天下”等纲领性观点，促使互联网这个能实现弯道超车的最大变量变成社会主义事业高质量发展的最大增量。

1.2 根本遵循：网络和信息化工作的五大要义

虽然内容分步提出，但新时代网信工作观是辩证统一的整体，具体可以把握为五大部分，其各有侧重却又紧密联系^[2]。第一，“没有网络安全就没有国家安全”等论述，深刻阐明了“党管互联网”的认识背景和网信工作的重要地位。第二，“技术先进、产业发达、攻防兼备、制网权尽在掌握”等论述，深刻阐明了网信建设乃至网络强国建设的基本要求和战略目标。第三，“坚持创新发展”“依法治理”“让亿万人民在共享互联网发展成果上有更多获得感”等论述，深刻阐明了发展和运用管理互联网的原则方向。第四，“四项原则”“五点主张”等论述，阐明了中国方案智慧，体现了谋和平发展、谋文明进步的使命担当。第五，“网信工作涉及众多领域，要加强统筹协调、实施综合治理”“要把握好安全和发展、自由和秩序、开放和自主、管理和服务的辩证关系”等论

*【基金项目】本文系山西省高等学校哲学社会科学项目（2022W170）、山西省高等学校科技创新项目（2024L499）阶段性成果

【作者简介】王斌（1986—），男，山西忻州人，硕士研究生，讲师，研究方向：网络信息安全。

述，深刻阐明了网信建设是系统工程，既是基础建设工作，又是应用管理工作。

1.3 战略升华：网络与信息化工作重点的交织迭代

几十年网络和信息化发展的实践沃土孕育了新时代网信工作观的诞生。在网络和信息化建设初期，信息化规模较小、应用量较小、网络数据量较小的时候，网络安全问题不太明显。当各类信息化应用达到一定服务规模和集成规模时，关键信息基础设施建设以及制度的网络安全问题随之而来。当网络信息安全事件影响，不断增大到一定程度时，网络安全上升到国家安全的高度。网络与信息化工作的重点，一直在发展中迭代。随着未来网络、数据和人工智能安全风险相互叠加交织的情况出现^[3]，网络和信息化建设工作的开展重点和关注重点也要相应地发生策略变化和战略升华。

2 新时代网信工作观的科学内涵

实践永无止境，理论创新同样如此，新时代网信工作观的内容仍在不断发展丰富。如何准确理解新时代网信工作观不断发展的科学内涵，需要把握“坚持把马克思主义基本原理同中国具体实际相结合、同中华优秀传统文化相结合”“坚持人民至上、自信自立、守正创新、问题导向、系统观念、胸怀天下理念”这两个基本的立场、观点、方法^[4]。

2.1 与中国具体实际相结合的内涵

面对不同时代的重大课题，党和国家均给予了理论与实践的系统回应，这些回应既一脉相承又与时俱进，其“回应”的本质是马克思主义中国化的发展过程，是中国特色社会主义理论不断实践丰富的具体体现。新时代网信工作观是党中央深刻洞察网络和信息化技术的先导作用后，结合中国具体实际提出的一系列网信建设工作的新思想；其以“网络强国”思想的提出为成熟化、系统化的标志，综合体现了网信建设工作与全面建成社会主义现代化强国、实现中华民族伟大复兴相结合的战略思想。网络和信息化建设工作的底层工作逻辑与最高价值追求，均与中国发展的具体实际相结合紧密。

2.2 与中华优秀传统文化相结合的内涵

传统文化中很多思想，既符合马克思主义基本原理的价值观念，又符合当前信息时代的价值追求，如“以民为本”“知行合一”“与时俱进”“大同世界”“求同存异”“和谐相处”“群策群力”等智慧思想。这些思想在“新时代网信工作观”中均有体现，并且又进一步地加深拓展。例如，有充分展现人民至上的“造福人民”等思想，有展现自信自立的“核心技术自主创新”等思想，有展现守正创新的“党管互联网”等思想，有展现问题导向的“老百姓上了网，民意也就上了网”等思想，有展现系统观念的“网络空间命运共同体”等思想，有充分展现胸怀天下的“全球治理体系”等思想。

2.3 中国特色治网之道是以新的理论创造继承发展了马克思主义

随着网络和信息化革命的发展，网信建设工作出现了很多“经典没有讲过、前人没有遇到过、外国经验也无法解决”的问题，这就需要党和国家创造和拓展新理论，以指引做好网信建设工作。新理论的创造和

拓展需要一组稳定、科学的价值观念、方法论，且需要一个不断实践完善的过程。新时代网信工作观是典型的新理论，其基于“习近平新时代中国特色社会主义思想的世界观和方法论”以及党管网治网的实践经验和总结而产生。其实现了一系列网信建设理论和实践上的重大突破、创新发展，以新理论创造、继承和发展了马克思主义，以新实践成果丰富和完善了中国特色社会主义，以新认识开创和拓展了中国特色治网之道。

3 新时代网信工作观的实践价值

新时代网信工作观植根于实践沃土，紧密联系发展实际，源于实践、指导实践、又被实践所验证，引领网信建设事业取得历史性成就、发生历史性变革，展现出坚实的实践基础、鲜明的实践导向和强大的实践伟力，具体来说表现为以下4个方面。

3.1 实践增进治理体系和治理能力现代化

网信建设实践增进了人民福祉，实现了中国式现代化。作为国家治理体系和治理能力的一部分，网络综合治理体系是新时代网信工作观中一项带有全局性、根本性的重要思想，其在实践中顶层设计日益完善，工作体系建设不断深化，综合治理能力和水平显著提升，形成了多主体参与，多手段结合的综合格局。新时代网信工作观实践，使网络和信息化建设过程具有社会成员整体共享性的公共利益最大化过程^[5]；使多元治理主体发挥并形成了治理合力；使政府的治理方式，不是传统地自上而下，而是做到与人民群众双向互动；使上

级顶层设计与下级治理创新有机结合起来；使人民群众有效参与国家治理过程。

3.2 实践促进信息领域核心技术自强自立

网信建设需要提升自主创新能力，突破关键核心技术，抢占发展制高点。社会主义制度优越不是说出来的，是做出来的，网信建设打赢的是中国特色举国体制的意识战。网信关键核心技术必须靠我国自己研发，做到立足技术自主创新。要正确认识自主创新和开放合作的关系，坚持在开放中吸收，在开放中检验。要坚持问题导向原则，奔着最紧急技术、最基础通用技术、前沿颠覆性技术等方面突破，有决心投入核心研发，有恒心遵循技术规律，有重心立足国情突破当下、面向世界引领未来。同时，要加强网信建设基础研究体系布局，发挥超大规模市场优势，以民用、商用推进科学研究，培育民族企业，使其形成有竞争力的信创产业体系。

3.3 实践推进网络生态建设和网络文明建设

互联网发展在世界范围内已经跃升到全面渗透、跨界融合的新阶段，使各个国家之间发展不平衡、合作规则不健全、贸易秩序不合理等问题日益突出。新的互联网世界，需要有新的网络生态文明指导实践。尽管世界各国各有其价值观念，但共赢是普适的价值追求。“四项原则”“五点主张”的提出，是中国在互联网治理实践基础上，针对全球网络治理提出的中国方案，体现了中国为网络生态文明贡献的智慧方

法，其化繁为简使全世界能够清晰理解并产生共鸣，得到了国际社会的广泛认同^[6]，在造福世界人民的文明格局上实现了超越。

3.4 实践改进党管体制建设和网信队伍建设

党的伟大事业一定要引领信息革命这一伟大工程。要想保证党的引领，必须坚持党管网络，这是党面临的形势和任务决定的。网信工作领导体制改革具体来说就是自上而下各个层级都设立集中统一领导的网络和信息化委员会，落实主要负责同志双重管理体制，将网信工作纳入党委重点工作计划和重要议事日程，做好统筹协调、整体推进。加快健全网信建设三级工作体系，构建上下贯通、运行顺畅、充满活力的制度，汇聚单位内、外各界力量推动网信工作快速高质量发展。不断深耕队伍建设，将讲政治、懂网络、敢担当、善创新的好干部选出来，从业内外培养、引进各类优秀网信人才到关键重要岗位。

结语

本文从生成逻辑、科学内涵和实践价值 3 个方面，对新时代网信工作观进行了深入分析，基本达到了学思、知信的层次。那么，如何在后续的网络和信息化建设工作中达到学思用贯通、知信行统一的境界，还需要网络和信息化建设的工作者们在不断的实践中得到答案。一方面，面对新时代、新征程，不仅要学习新时代网信工作观来开展具体、专项的网信工作，还要在工作中理解应用新时代网信工作观来谋划、部署和推进，审时度势、与时俱进，让具体的网信工作走在行业前列。另一方面，新时代网信工作观仍在伟大实践中不断丰富发展，必须时刻立足时代背景，理解时代理论，以实践过程来检验时代理论，以创新精神来发展创新理论，真正将新时代网信工作观融入日常网信建设工作中，只有这样才能更好地凝聚起共同奋斗的力量，在网信建设中蹚出一条高质量发展之路。^[8]

引用

[1] 赵周贤,吕宏.坚持用马克思主义观察时代解读时代引领时代[N].解放军报,2018-06-13(007).

[2] 庄荣文.推进网络强国建设的强大思想武器和科学行动指南[N].学习时报,2021-04-28(001).

[3] 郎平.数字时代国家安全困境与网络空间命运共同体构建[J].当代世界,2023(10):34-39.

[4] 中共中央关于认真学习宣传贯彻党的二十大精神的决定[N].人民日报,2022-10-31(001).

[5] 高卫星.把握治理体系和治理能力现代化的五个维度[OL].(2024-07-17)[2024-10-09].<https://theory.dahe.cn/2024/07-17/1787713.html>.

[6] 中央网络安全和信息化委员会办公室.向着网络强国阔步迈进——党的十八大以来我国网信事业发展综述[OL].(2023-07-15)[2024-11-01].https://www.cac.gov.cn/2023-07/15/c_1691068423442527.htm.

个人信息合理使用判定的困境与出路*

文◆南京理工大学知识产权学院 许嘉璐 陈希媛 唐静怡

引言

信息合理使用是指在未经主体同意的情况下，为维护正当利益使用其信息，是当前个人信息处理的主流方式之一。聚焦现代法治与本土资源，2020年，《中华人民共和国民法典》（以下简称《民法典》）出台，第九百九十九条和第一千零三十六条从民事基本法角度对信息合理使用进行了回应；2021年，《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）出台，其第十三条第1款第2至7项（以下简称“信息合理使用条款”）列举了具体的合理使用情形，搭建了信息合理使用的基本框架，为合理使用个人信息提供了法律引导^[1]。

隐私悖论在个人信息领域并不常见，主体多倾向于保持信息秘而不宣。但个人信息同时具备卓越的社会关联性和多元价值性，若一味将其封闭在主体“自留地”，必将引发“反公地悲剧”^[2]。信息合理使用利用法益限制理论，依据价值分量，确定利益序列，当个人信息上的不同利益发生冲突时，优先保障高阶利益，以确保各方得到适当的保护。然而，由于无需获取同意，信息合理使用会对主体的自主决定权产生遮蔽效应，致使部分处理者利用规则过度侵占主体权益^[3]。如何在既有框架下规范信息合理使用行为是亟待解决的痛点问题。

1 个人信息合理使用判定的实证考察与困境检视

合理使用制度是颇具实践价值的法律规则，与司法认定紧密相连。然而，实务对于个人信息合理使用的判定问题并未完成理论证成和法律政策破冰，同案不同判现象屡见不鲜。不仅影响了规则的运行实效，还削减了立法对个人信息的荫庇作用。本研究旨在通过实证分析，探索个人信息合理使用的程式化判定方法，以解决司法困境，保障司法公允，并产生管理效应，对理性约束信息合理使用提供启示。

1.1 个人信息合理使用的实证考察

合理使用个人信息是数字经济发展转型的务实选择，但其潜在的安全风险不容忽视。就个人信息合理使用判定，需从解释论出发，结合信息特质，进行细致入微的分析，以实现判定的圆满^[4]。通过查阅中国裁判文书网，以“个人信息”“合理使用”为关键词，以2021年1月1日

（即《民法典》生效后）至2023年12月31日为时间轴，共筛选出信息合理使用纠纷47件（见表1）。其中，涉及个人敏感信息的案件如“崔某某诉香厂路居委会”案以及涉及已公开个人的信息案件如“张某某诉拓福体育”案等。由于法律条文的模糊性和成熟案例群的缺乏，法院在认定信息合理使用时往往存在不一致的判决，导致同案不同判的情况时有发生，严重影响了法律的可预见性和裁判的权威性。

1.2 个人信息合理使用的困境检视

通过整合上述47件信息合理使用纠纷，梳理出当前合理使用判定中存在的诸多问题。

第一，对不同个人信息的处

*【基金项目】2024年大学生创新创业训练计划国家级创新训练项目“个人信息合理使用判定问题研究”（202410288103Z）

【作者简介】许嘉璐（2004—），女，江苏宜兴人，本科，研究方向：法学。

理过于粗犷，难以为个人信息的合理使用提供周延的保护。判决中，对于个人信息合理使用有涉案情形的梳理，但缺乏细粒化的处理和类型化的概括。例如，个人信息被简单地依附于名誉权、隐私权等民事权利进行考量，且仅以“公开”和“敏感”与否作为分类标准予以规制和救济。

第二，司法裁判场景抽离。上述裁判文书缺乏个性化调整，背离具体的利用场景，导致利用方式范围逐渐扩张^[5]。尽管在“钟某某诉《上海电视》杂志社”案中，法院从双方职业、信息类型、行为目的和方式等方面进行审查，有基于场域微调仲裁基准的尝试，但在“王某某诉腾讯”案中，法院以“合法、正当、必要和诚信原则”为审查依据，仍笼统迂阔，说理过程概括、笼统、抽象，缺乏层次性，这主要归因于法官审判活动缺乏场景的融入。

第三，论证方式缺乏标准范式。为确保审判的稳定性，合理性判定应建立一套标准化的论证方法。然而，以“行为正当”模式为例，其从行为本身正当性出发，重点考察权利行使是否适当，但实践中各法院的评估要素迥然有别。这种不统一的论证方法不仅影响了具体法律条文的选择和适用，还降低了事实认定的稳定性，并引发滥诉风险。例如，实践中不乏带有贬损、侮辱性的行为以“合理使用”“已公开”“非敏感”等为由进行抗辩，混淆视听。

综上所述，当前司法针对信息合理使用的裁定存在基础类型分类不明确、判定逻辑场景抽离、论证方式不统一等问题。通过现

表 1 中国裁判文书网相关信息合理使用纠纷的总体情况

类别	情形	案件数量
年份	2021 年	24
	2022 年	14
	2023 年	9
案由	网络侵权责任纠纷	27
	名誉权侵权纠纷	5
	个人信息保护侵权	4
	肖像权侵权纠纷	3
	隐私权侵权纠纷	2
	其他（劳动合同纠纷等）	2
	仅列明为民事纠纷	4
涉案情形	合理范围内处理公开个人信息	24
	合理范围内为公共利益实施舆论监督	11
	为履行合同所必需	6
	履行法定职责或法定义务所必需	3
	实施人力资源管理所必需	2
	应对突发公共卫生事件	1
审判结果	构成合理使用	17

象看本质，司法中的种种问题均是由于对制度本质的认知不足所致。合理使用制度是在权利限制理念指引下构建的利益平衡机制，其在著作权领域得到了充分发展。信息合理使用借鉴著作权经验，结合个人信息保护规定和实践总结而来，其不可避免地带有后者烙印。在立法目的上，两者均以实现利益平衡为制度追求；在运行机制上，两者均通过非自愿的方式开发客体价值；在作用对象上，两者的客体均具有非竞争性和非排他性，且均需在流通和传播中实现价值。

2 个人信息的类型处理

明确个人信息类型是借助法律手段保护个人信息的基石。为了更好地应对个人信息合理使用判定过程中的复杂场景，可以从类型化的视角出发，对个人信息进行更为细致的区分。通过打破“已公开标准”与“敏感/非敏感个人信息”的静态框架，采用更为动态的划分方式，更加精准地把握个人信息合理使用边界，从而更有效地保障个人信息的安全和合法权益，同时也符合物尽其用的原则，促进经济社会的健康发展。

2.1 “分离性标准”下对已公开个人信息的处理

“分离性标准”这一概念最早出现在 1976 年美国《版权法》，适用于著作权。基于个人信息权利与著作权的客体相似性，分离性标准存在移植的可能。将分离性标准应用于个人信息方面时，应以信息权益影响的法律事实为基础，将信息处理分为可分离使用与不可分离使用两类，

同时可通过以下两步骤判定已公开个人信息适用的合理性。

第一，判定已公开的个人信息是否有主体关联性。将个人信息的主体关联性置于核心位置时，个人信息处理活动对于信息的人格性就能得到更多考量。虽然“个人信息”范畴中的信息都具有主体关联性，但个人信息在不同用途下主体关联性强弱不同，意味着信息与其主体的联系不同。信息中与人联系密切的部分往往具有私密性且能精准体现主体个性，而彰显出人格性特征，并反映出较强的主体关联性。对于这部分信息，主体应享有完全的控制权；反之，与主体无关联的信息则可以保留其可转让性。

第二，判断已公开个人信息的处理行为能否产生特定法律效果。具体来说，若对已公开个人信息的处理行为能通过影响主体权益的形式产生特定效果，这种处理行为就应当被认定为“不可分离”的处理，其使用的合理范围应受到更多约束；反之，“可分离”处理使用的合理范围不应加以过多限制。以“刘某甲诉上海某实业公司、刘某乙个人信息保护纠纷”案为例，案中是被告对原告刘某甲个人信息的处理行为，而非原告个人信息的“已公开”状态本身对原告工作生活造成了严重的不利影响这一客观法律后果。这正契合了对“不可分离”处理的合理范围限制的要求。

2.2 “三步检验法”下对未公开敏感信息的处理

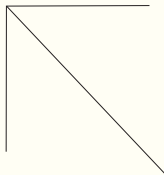
《伯尔尼公约》中的“三步检验法”是著作权进行合理使用判定的惯用工具，但由于著作权合理使用仅适用于已公开发表的作品，而我国《民法典》和《个人信息保护法》均未明确将未公开敏感个人信息排除在规则适用范围外。因此，“三步检验法”在个人信息上的适用应格外谨慎，不可将著作权的相关做法直接嵌套至个人信息的未公开敏感信息领域，其具体适用应结合《个人信息保护法》进行调整，体现个人信息特色。

《个人信息保护法》第十三条是信息合理使用的核心条款，可以其作为切入点，尝试对未公开敏感信息构建“双清单”模型，确定情形清单和评估清单，为“三步检验法”的适用提供落脚点。第一，情形清单。情形清单的作用在于明确何种情形属于合理使用。《个人信息保护法》第十三条的“信息合理使用条款”的“赋权”要件承袭《民法典》第九百九十九条规定，就个人信息做延伸处理，即为信息合理使用的情形清单。第二，评估清单。评估清单的意义在于评价个案中使用行为是否正当。《个人信息保护法》的“信息合理使用条款”的“限权”要件通过“必须”或“合理范围”发挥阀门作用，是对《民法典》第九百九十九条“不得不合理侵害”的落实，即为实质意义上的评估清单。“限权”要件虽穷尽式列举了“必须”和“合理范围”两项标准，但两项标准在内涵上具有不确定性和扩张性。第三，为增加评估清单的可操作性，需具化“必须”或“合理范围”的判断依据。若处理目的含糊不清、处理行为超出必要限度、保护措施应用不当，必然会给主体造成不合理损害。因此，可将第二十八条作为承接个人信息合理使用评估清单的具体条款^[6]。

2.3 “去标识化”下对未公开非敏感信息的安置

个人信息去标识化通过加密、假名化、哈希函数等高级技术手段，使得即使在面对复杂的数据分析时，也无法轻易重建个人信息与特定个体之间的桥梁。国际上，欧盟的“假名化”强调了即使有额外信息保存，也需要通过技术和组织管理措施确保数据无法用于识别特定数据主体，而美国的定义则侧重于数据在与附加信息分离后无法识别特定主体。我国的《中华人民共和国网络安全法》和《个人信息安全规范》也对去标识化进行了规定，强调在去标识化后，数据发布和使用需遵循隐私保护和数据最小化原则，以应对个人敏感信息与非敏感信息在不同场景下面临的不同规制挑战。

对于重点识别风险相对较低的非敏感信息，应首先评估、进行分级管理，确定合理的风险阈值。根据个人信息去标识化后具有的可识别性大小对去标识化个人信息进行效果分级，针对去标识化处理不同层级的数据集，对应不同的法律效果，从而设定各自的保护要求和利用限制。其中，对于高风险的数据基于风险进行规制，处理者需承担更重的



责任，包括但不限于个人信息保护影响评估、分类存储、限制共享等^[7]。同时，特定场景的高风险数据处理往往需制定具体的规则，而《个人信息安全规范》等标准已有的管理措施，则可有选择地使其上升为法律。此外，应更侧重于合理利用，允许更大的数据流通空间，使其豁免于知情同意规则，有效保护个人隐私、防止信息滥用。

3 个人信息合理使用判定场景的融入

对个人信息合理使用判定进行法理检视时，由于个人信息具有个体关联性，为保持“期待”认定的稳定性，法官需从社会视角出发，以普通情感认知为标准，融入场景以判定主体和社会的期待是否溢出常理。为此，可借助罗尔斯关于“无知之幕”和自利理性人的假设，使其合理限度内的信息处理成为所有理性人都会认同的普遍规则，并以社会资源的最优分配为目的，从帕累托最优原理的角度，为司法裁判说明个人信息合理使用的正当性提供思路。再从方法论的角度出发，以比例原则的目的适当、最小损害和狭义比例三项子原则，为司法工作人员提供具体的操作指南。

3.1 “无知之幕”下的自利理性人假设

在罗尔斯“无知之幕”的思想实验中，所有社会成员都被剥夺了社会知识，人们无从得知其价值观念和社会地位，甚至是自身所处的具体时代。基于这种假设，人们因无法预知“无知之幕”落下后自己是否处于弱势一方，在理性驱使下不会追逐某一方的最大利益。为了追求自身利

益最大化，自利理性人普遍追求所有群体利益最大化的平衡。

具体到个人信息方面，“无知之幕”下的自利理性人会普遍同意个人信息的合理使用。依据《个人信息保护法》第二条与第六条，任何组织、个人不得侵害自然人的个人信息权益，处理个人信息应采取对个人权益影响最小的方式^[8]。简而言之，为了使个人利益最大化，对权利主体个人信息的使用必须控制在一定的限度内，确保每个人的重大利益不被他人侵犯。在信息权利主体的角度，人们的诉求是最大限度地保护个人信息；而在信息处理者的角度，人们则期望最大限度地使用他人的个人信息获取利润。因此，为了使个人利益最大化，在合理限度内使用公开的个人信息就会成为所有自利理性人均会同意设立的行为规则^[9]。

3.2 “帕累托最优”原理下的社会资源分配

“帕累托最优”这一概念最先出现于经济学领域，是资源分配的一种理想状态。而法经济学的“卡—梅框架”将法律规范分为财产规则和责任规则，信息合理使用即为典型的责任规则，运用的核心在于依靠法律制度安排的资源配置应实现有效性，经济效率是其主要的评价依据。在“卡—梅框架”下，可将“帕累托最优”原理引入资源配置，以衡量信息主体与信息处理者两类群体之间的利益分配是否合适^[10]。

如果个人信息这类资源的使用程度未能达到“帕累托最优”状态，那么意味着在有一方的境况能够得到改善同时另一方不受损害。一方面，信息处理者在不严重侵犯主体权益的情况下对他人个人信息利用过少，意味着在信息主体权益得到保障的情况下，信息处理者本可以通过处理这些信息获得更多的财富。另一方面，若信息处理者在获得相同利润的前提下选择对主体信息披露较多的方案，则信息主体本可以因更少的信息使用而受到更强有力的保护。因此，为达到“帕累托最优”状态，需将个人信息的使用框定在一个“合理”的范畴内，在不损害对方的前提下达成保护信息主体权益与增加信息处理者财富两方面最佳平衡，使所有人都达到最理想境况，从而有效、合理、科学地使用个人信息资源，促使信息资源效用最大化，实现个人信息领域的社会福利最大化。

3.3 “比例原则”下个人信息合理使用判定的操作指南

个人信息合理使用的“双清单”均为开放清单，灵活性与模糊性并存。在进行合理性判定时，应灵活权衡公权与私权，精准拿捏分寸。比例原则作为成本效益分析的形式，常被用于解决利益冲突。比例原则要求行为应适合预期目的，采用最缓和的手段，且收益应大于风险，这与信息合理使用的“平衡”精神相契合。结合比例原则的要旨，可以对个人信息合理使用的判定设置三项审查流程，分别对应目的、行为和结果，具体应用可按照以下流程逐步推进。

第一，启动情形审查。法院在未释明“合理使用情形”情况下，判定应先将行为与“信息合理使用条款”列举的情形进行比照，再依兜底条款向其他部门法或《民法典》第九百九十九条寻求依据。为配合必要的扩大解释，需抽象出信息合理使用的底层逻辑，辅助启动情形认定。是否存在紧迫、优阶利益致使知情同意失灵是规则启动的关键，故可以考虑正当利益甄别、价值位阶对比和知情同意失灵三要素。正当利益并非权益让步的万能理由，例如，2020 年，杭州市计划利用码进行常态监

测，其所维护的“公共”不具有现实紧迫性，行为难称合理。价值位阶具有流动性，预先确定的高阶利益仅有相对优先性，应坚持一案一判，采用“先验标准+具体场景”方式，结合职业伦理、专业知识进行判定。由于合理使用对信息主体具有利益减损性，不应被作为处理个人信息的一般手段，仅当知情同意失灵会导致特定目标无法实现，才可进行合理使用。

第二，行为限度审查。个人信息具有非竞争性，合理使用通常不会限制信息的实际使用，但由于主体通过特定语境控制自身信息流向，若使用行为超出主体合理期待，则会干扰信息的潜在使用。合理期待理论于美国 *Katz v. United States* 案中被确立，法官认为若公民表现出对自身隐私的保护期待，且被社会认可，则这种期待需被保护。合理期待理论起初用于约束公权力对公民隐私的侵入，后被广泛应用个人信息场景中。例如，在“谭某诉乐动花开案”中，法院认为原告因经营需求公开其电话号码，对私生活不受侵扰仍保有期待，被告的摄制行为导致原告遭受大量电话骚扰，构成不当侵权。为兼顾权利保护的民主性和有限性，合理期待理论分设主观和客观要件，两项要件于内部相互制约。

第三，结果均衡审查。信息侵权中，主体对于风险损害的诉求可归纳为三点，即信息风险激增、为预防风险支出的合理费用以及因风险激增产生的不良情绪。从逻辑上看，风险激增是“因”，合理费用和负面情绪是“果”，风险损害的审查应分为两步进行。一方面，由于风险增幅与个人信息的敏感性呈显著正相关，法官可依信息敏感性，结合信息暴露程度、被误用的迹象、与其他信息聚合的可能性以及缓解措施的有效性等要素，判定风险是否突破安全阈值。由于个人信息的潜在用途巨大，风险证必须建立在法官谨慎的自由心证之上，谨防肆意发散。另一方面，考虑到主体为预防风险所支出的合理费用本质上是一种制止侵权行为的支出，这项支出客观且真实，因为无不当使用便无此项支出，可将其纳入损害结果的范畴。同时，主体对于颇具敏感性的个人信息泄露感到焦虑是一种理性反应，情感的平静本就是值得保护的法益。依据我国《民法典》的规定，精神损害应符合“严重性”要求，且为避免滥诉，“严重性”要件应当保留。

4 个人信息合理使用判定的具体路径

在个人信息合理使用判定的方案探寻中，“合理”是信息合理使用的核心限定词，解决的是“判定什么”的问题，而明确其具体内涵是明确合理性判定内容的关键。在此基础上，在私利与公益的双重法益中使用“分离性标准”，并在特定场景下使用“三步检验法”，从而实现判定路径的具体建构。

4.1 以“合理”为核心限定词

“合理”作为一项法学概念，最早出现于行政法领域。英国“*Wednesbury*”案的法官曾阐释了“合理”的内涵，认为权力主体在行使权力时应综合考量相关要素，并给予适当权重以实现平衡。信息合理使用效果来自立法的“赋权”，是信息处理者行使的抽象“自由裁量权”，平衡是其“合理”的关键^[11]。在平衡精神的指导下，应进一步明确合理性判定的具体

标准。

“卡—梅框架”下，个人信息合理使用中汇集多方利益，使得实践中审判者往往难以兼顾各方。通过结合“帕累托最优”原理的评价方案，避免可预见的损害，将不可避免的损害降至最低，实现利益盈余。“信息合理使用条款”中的“限权”要件对认定结果均衡具有掣肘作用，“必须”要件强调合理使用的绝对必要，规则取向以保障主体信息权益为先，收益应绝对大于风险，而“合理范围”要件侧重于强调信息主体对合理使用的容忍义务，要求处理者对于合理使用保持“合理谨慎”，风险和收益间不存在明显不平衡即可。

4.2 双重法益下“分离性标准”的使用

私利与公益是两大法益，通说认为公益在位阶上更优。但概念的模糊极易导致利益的抽象，故应将双重法益转化为获取疫苗接种数据、医药研发资源、劳工个人简历等具象形态。而因个人利益间有时并无明显位阶，其权重应考虑主体期待^[12]。此外，商业利益作为私利的分支，其正当性应得到认可。但无论如何，双重法益本质上并无根本性冲突，均是社会长效发展过程中不可或缺或平衡要素。个人利益与公共利益应相互协调，避免过度偏向任何一方^[13]。

在“分离性标准”合理性界定的最后，是对公共利益与个人利益的平衡。以分离性标准界定个人信息合理使用时，不仅应关注信息的主体关联性与处理行为的法律效果，最大限度地保护信息主体的人格利益，还应充分利用与主体无关联的个人信息的可

转让性^[14]，积极进行个人信息的“可分离”处理，为社会创造更多财富。例如，可依托利益平衡理论贯彻于“产业发展+权利保障”的双线路径、责任规则优于财产规则与特定公共利益的实现，为个人信息合理使用的正当性提供理论支撑。

4.3 情景特定化下“三步检验法”的使用

场景决定行为的全局表达。在应用“三步检验法”时，需要依托我国对于个人信息保护的规定，结合具体情景。我国《个人信息保护法》第六条通过“明确”和“合理”两项要件设置“目的限制”原则。个人信息价值呈现多依靠二次利用，“特定”绝非要求处理目的固定不变。

以健康信息为例，应依信息类型、处理者等要素，将场景具体至医生调阅、强制检疫、商保对接等，以细化场景树状图。借助 Nissenbaum 的“场景理论”，为信息主体、信息类型、处理规则等要素搭建处理场景，并进行严格保护，充分保障信息安全。此外，处理者原则上不应变更处理目的，但若结合“语境”中的各项要素证明新目的与原始目的存在合理关联，且不会改变处

理场景，造成风险的重大变动，则应允许其适度拓展处理目的。

结语

个人信息合理使用尊重个人安宁的同时，兼顾信息交融流通带来的经济利益。当前，个人信息保护的司法判定方案尚不完善，极易导致处理者利用法律监管的真空地带不当侵入主体私人空间。通过实证分析发现，个人信息合理使用领域的司法冲突时有发生，根源在于个人信息类型划分不周延、司法裁判场景抽离和论证方式缺乏标准范式。针对这些问题，依次探索路径建构方案。首先，从类型化视角出发，以“三步检验法”处理未公开敏感信息、以“去标识化”安置未公开非敏感信息，为个人信息类型划分不周延提供框架。其次，将法官假设为“无知之幕”下的自利理性人，以“帕累托最优”为价值追求和社会资源分配的内在逻辑，并以比例原则作为其具体判定的操作指南，促进法官消除成见、在判定时融入场景。最后，以“合理”为核心判定词、将“分离性标准”纳入双重法益的考量、关注“三步检验法”的特定场景，为个人信息合理使用的判定提供范式遵循，从而筑牢我国个人信息保护之网。^[5]

引用

[1] 彭诚信,刘海安.个人信息保护法[M].上海:上海交通大学出版,2024.

[2] 申卫星.数字权利体系再造:迈向隐私、信息与数据的差序格局[J].政法论坛, 2022(3):89-102.

[3] 王锡锌.国家保护视野中的个人信息权利束[J].中国社会科学,2021(11):115-134.

[4] 王苑.敏感个人信息的概念界定与要素判断——以《个人信息保护法》第28条为中心[J].环球法律评论,2022(2):85-99.

[5] James C.Cooper;Joshua Wright.The Cambridge Handbook of Consumer Privacy[M].Cambridge University Press,2018:465.

[6] 郭传凯.敏感个人信息处理规则的反思与修正.政法论坛,2024(3):102-113.

[7] 蔡蔚然.去标识化个人信息分级处理的规则体系[J].山东社会科学,2023(2):185-192.

[8] 王良顺,李想.“合理使用”公开的个人信息出罪路径的法教义学建构——从最高人民法院第194号指导性案例切入[J].西安交通大学学报(社会科学版),2024(10):1-16.

[9] 杨伟清.重思罗尔斯的无知之幕[J].伦理学研究,2023(5):81-89.

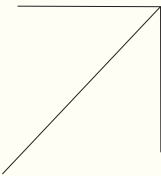
[10] Sun J,Li GL. An end-to-end Learning-based Cost Estimator[J].Proc. of the VLDB Endowment,2019,13(3):307-319.

[11] 李杨.著作权侵权认定中的转换性使用理论适用阐释[J].北方法学,2023(3):42-56.

[12] 彭诚信.论个人信息的双重法律属性[J].清华法学,2021(6):78-97.

[13] 程啸.论公开的个人信息处理的法律规制[J].中国法学,2022(3):82-101.

[14] 丁晓东.法律如何调整不平等关系?论倾斜保护型法的法理基础与制度框架[J].中外法学,2022,34(2):445-464.





数据要素

Data Elements

数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通、消费和社会服务管理等各环节，深刻改变着生产方式、生活方式和社会治理方式。

数据要素是指以电子形式存在的、通过计算的方式参与到生产经营活动并发挥重要价值的数据资源。在数字经济中，数据被视作与土地、劳动力、资本、技术并列的五种生产要素之一。数据要素是推动数字经济发展的核心引擎，是赋能行业数字化转型和智能化升级的重要支撑，也是国家基础性战略资源。

2023 年正式成立的国家数据局，负责协调推进数据基础设施建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等，不仅体现了对数据资源的战略性管理和规范化利用的需求，也体现了国家层面对数字经济发展和数据治理的重视。

大数据技术在健康管理中的应用研究

文 ◆ 四川通信科研规划设计有限责任公司 刘 砧

引言

随着科技的快速发展，健康数据的采集和管理逐渐从单一的医学诊断向多维度、多层次的大数据挖掘与分析转变。基于物联网、云计算以及智能穿戴设备的技术支持，健康数据涵盖了生理指标、行为数据、基因信息以及环境因素等多种维度，为健康管理提供了更为详尽和动态的信息基础。大数据技术的兴起为健康管理带来了颠覆性的变革，不仅显著提升了数据存储与处理能力，还推动了个性化医疗和精准健康服务的发展，使健康管理从被动响应逐步向主动预防转型，为健康干预提供了更科学的决策支持。本研究旨在探讨大数据技术在健康管理中的应用，阐述通过物联网和可穿戴设备实时采集健康数据，并利用云计算和机器学习方法进行数据处理和风险评估，构建个性化健康管理模型。

1 大数据技术在健康管理中的特点

首先，数据量大（Volume）是大数据的核心特点。健康管理

涉及大量的生理、心理和环境数据，来源包括医疗记录、可穿戴设备数据、基因检测结果、体征数据和日常生活信息等。如此巨大的数据量使传统的存储和处理方法难以满足日益增加的需求，而大数据技术能够支持对以 PB 甚至 EB 计算的海量数据进行高效存储和分析^[1]。

其次，类型多样（Variety）体现在健康数据的复杂性和多样性方面。健康数据不仅包括结构化数据，还包括大量非结构化数据和半结构化数据，包括文本（医生记录）、图像（CT、MRI 影像）、视频监控数据、地理位置数据以及由可穿戴设备生成的实时数据^[2]。这种多样性要求大数据技术应具备强大的数据处理和整合能力，以全面分析健康信息。

再次，处理速度快（Velocity）对于健康管理中的实时性需求至关重要。由于健康数据的产生速度越来越快，而通过云计算和流处理等技术，能够实现数据的即时处理，确保健康管理系统能够快速响应用户健康状态的变化。这一特点尤其适用于健康监测和疾病预警系统，确保在数据异常时及时做出反应。

最后，数据的潜在价值高（Value）是大数据在健康管理中应用的驱动力。健康数据的深度挖掘有助于识别潜在健康风险、预测疾病趋势、优化医疗资源分配，并为个性化健康管理提供科学依据^[3]。通过大数据分析，可以发现不同群体的健康行为模式，评估个体或群体的疾病风险，从而提供早期干预方案。

2 大数据技术在健康管理中面临的挑战

大数据技术在健康管理中的应用尽管带来了显著的效率提升，但也伴随着一系列实践中的挑战，需要在技术和管理层面进行深入研究。

首先，健康数据的安全性与隐私保护问题尤为突出。健康数据通常包含患者的敏感信息，如诊断记录、基因信息等，一旦泄露会对患者隐私造成无法挽回的损害。随着数据量和数据交互的增加，数据存储和传输的安全风险也随之加剧。传统的访问控制与加密方法已难以应对当前复杂的数据安全需求，亟须发展基于零信任架构和同态加密的新型安全

【作者简介】刘砧（1994—），女，山西吕梁人，硕士研究生，高级系统规划与管理师，研究方向：智慧医疗、大数据应用。

策略。同时，法律与伦理层面的规范尚不完善，大数据技术的实际应用还需与患者隐私保护法规深度结合，以确保数据处理的合法性与合规性。

其次，数据标准化与整合的挑战限制了数据分析的深度与广度。医疗健康数据的异构性极高，来源包括医院电子健康记录（EHR）、可穿戴设备数据、基因组数据以及患者自填问卷等，这些数据在格式、结构、语义等方面差异显著。如何通过数据标准化模型（如 FHIR 标准或 HL7 协议）统一数据结构以及借助数据清洗和语义整合技术提升数据质量已成为大数据技术在健康管理领域的重要研究方向。此外，数据孤岛现象依然存在，不同机构间缺乏数据共享机制，导致分析结果的片面性，阻碍了跨机构数据价值的最大化利用。

最后，高效数据处理的复杂性问题也对技术架构提出了更高要求。尽管 Hadoop 和 MapReduce 等技术能够显著提高大规模数据处理的效率，但面对持续增长的数据规模和多样化的分析需求，现有架构在实时性和灵活性上依然存在不足。一方面，系统扩展性的设计需要优化存储与计算资源的动态分配，以适应数据流动的非线性增长。另一方面，实时数据处理框架（如 Apache Flink 或 Spark Streaming）的应用正在成为研究热点，但如何在高吞吐量的同时保障低延迟和高精度分析，仍需进一步优化。分布式计算中因节点失效或通信延迟导致的性能瓶颈也是一个待解决的问题，尤其是在处理健康数据这样高维度、低容错的敏感数据时，对架构设计提出了更加苛刻的要求。

3 大数据技术在健康管理数据方面的应用

首先，大数据技术在健康管理中，通过多层次数据采集与整合，构建了全面而精细的健康数据体系，涵盖了宏观、中观和微观 3 个层次。宏观层次的数据关注外部环境因素，包括气候条件、地理位置、空气质量以及社会经济状况等，这些因素通过影响个体的行为模式和生活习惯间接作用于健康。中观层次的数据集中于生理和心理指标，如血压、心率、体温、血糖水平和情绪状态，这些数据为健康状态的精准评估提供了直接依据。微观层次的数据深入到分子和基因水平，包括基因组序列、生化指标、代谢产物以及蛋白质组信息，为疾病的精准诊断、早期干预和个性化治疗提供了科学基础^[4]。智能设备如可穿戴传感器、射频识别设备（RFID）、条码扫描器和 GPS 定位设备等，通过与物联网技术结合，实现了健康状态的实时监控、数据采集和多维度整合。这些设备以无缝方式整合不同层次的数据，提升了数据采集的效率与准确性，为动态健康管理提供了多维度的科学决策支持。

其次，在数据处理环节，云计算技术通过高效的数据存储与分析，完成了从数据采集到评估的全面管理。云平台集成了多种先进的机器学习与数据挖掘算法，能够对健康数据进行聚类分析、关联规则挖掘以及时间序列预测。例如，通过分析相似个体的健康特征，云平台可以分组识别高危人群；通过挖掘数据间的隐性关联，揭示健康行为与疾病风险之间的关系；利用时间序列模型则能够动态追踪个体健康状态的变化趋势^[5]。基于这些分析结果，系统生成个性化健康评估报告和风险模型，在早期风险出现时及时发出预警，为健康干预提供科学指导。

最后，健康管理系统的基础架构依赖实时监控与动态更新的能力。借助传感设备（如激光扫描器、智能传感器和 GPS 定位设备），系统全天候采集用户的生理、心理和活动数据，不仅包括传统健康指标，还包括通过整合社会、文化和自然环境的背景数据，以此为健康评估提供更广阔的背景支持。例如，用户所处环境的气候变化或空气质量波动可以被记录并纳入健康评估体系中，从时间和空间维度全方位呈现个体健康状态。通过这些技术手段，大数据技术构建了更具科学性和前瞻性的健康管理模型，使健康管理从静态评估转向动态调整。

4 大数据技术在健康管理流程中的应用

在健康管理流程中，大数据技术贯穿于健康状态监测、数据整合、动态评估、风险预警、干预调整以及效果再评估的全生命周期，形成闭环的动态健康管理體系。这种方法不仅实现了对个体健康状态的实时监控，还通过整合多源数据和动态反馈机制，为个性化健康管理提供了坚实的技术支撑。

首先，物联网与智能可穿戴设备在数据采集中发挥关键作用。通过智能手表、心率带、血压计等，系统实时采集个体的生理参数（如心率、血压、血氧）以及生活行为数据（如睡眠质量、运动量、步数）。这些数据通过传感器与互联网连接，实时传输至云端，形成标准化数字记录。健康管理系统将数据标准化后存储在电子健康档案中，每个档案以唯一编号管理，确保数据的独立性、完整性和可追溯性。电子档

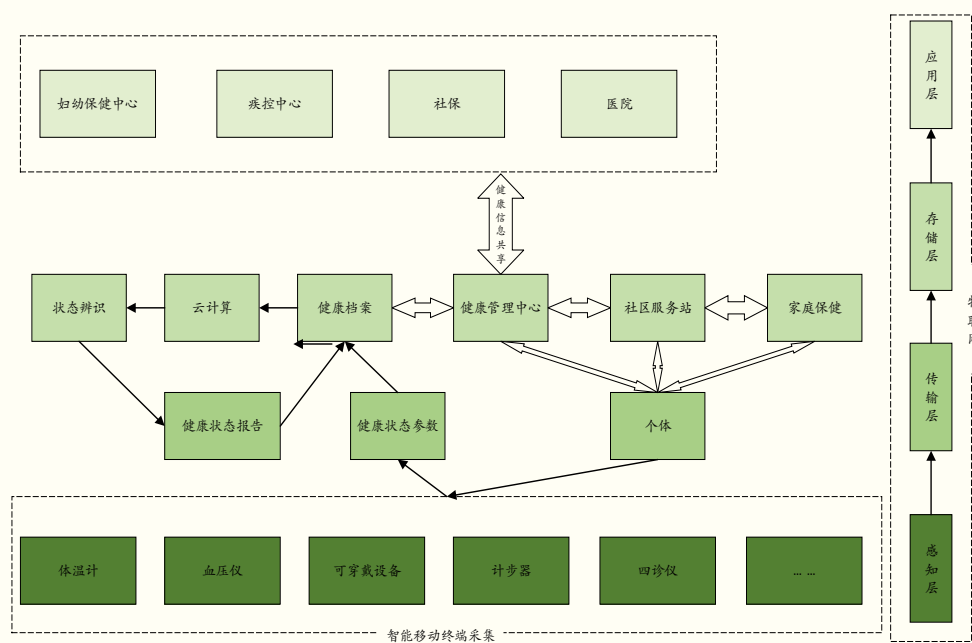


图 1 健康管理大数据技术运用示意图

案包含时间序列数据、体征趋势以及历史健康记录，为精准分析和个性化干预提供支持。

其次，在健康数据分析中，大数据技术通过状态辨识、数据挖掘以及高级算法模型支持动态评估和科学决策。健康管理系统利用回归分析、深度学习和聚类算法，将原始数据转化为健康状态评估指标。例如，回归分析量化健康状态变化趋势，神经网络预测慢性病发病概率，聚类算法根据健康特征分组并识别高危群体。整个流程按风险等级分组管理，并提供分层干预措施，同时通过数据反馈实时监控干预效果，动态调整策略，确保干预的有效性。

最后，云计算技术在健康管理中提供了强大支持，特别是在数据存储与共享方面。通过云平台，社区医疗站、健康管理中心和个人智能终端实现了无缝协作和实时数据同步。数据通过分布式存储与计算框架高效管理，支持海量数据动态更新与并行处理。云平台集成数据挖掘算法（如频繁模式挖掘、关联规则分析、时间

序列预测），从健康数据中提取潜在的行为规律。例如，频繁模式挖掘揭示不良生活习惯对慢性病的影响，关联分析捕捉健康指标与环境因素之间的联系。这些分析结果有助于优化个性化健康管理方案，并为公共卫生策略提供科学依据。健康管理大数据技术运用示意图如图 1 所示。

结语

大数据技术在健康管理中推动了传统医疗模式向智能化、个性化服务的转型。借助物联网、云计算和数据挖掘技术，健康管理系统能够整合并分析个体的生理、心理、环境等多维数据，实现实时监测、精准评估和动态干预。不仅为健康管理提供广泛的数据支持，还推动了预测和预防为主的健康管理模式，使服务更加主动、个性化。未来，大数据将扩展至健康行为引导与重塑，如通过健康数字孪生技术模拟健康状态，提前发现风险并提供干预建议；强化学习与行为心理学，为用户定制健康激励计划，潜移默化改变健康习惯。健康管理的未来是科技与人文交织的整体健康系统，既是技术进步，也是健康认知的深度变革。

引用

[1] 李子俊.基于CiteSpace知识图谱“健康中国”背景下健康大数据领域研究[J].中国现代医生,2023,61(24):62-67+73.

[2] 马欣欣,万生芳,魏昭晖,等.医疗大数据背景下的人工智能在中医诊断中的应用研究[J].世界中医药,2023,18(11):1579-1582.

[3] 黄江发,刘志国,李金峰,等.大数据下老年膝关节病中医健康管理模式的应用[J].现代医药卫生,2023,39(12):2145-2149.

[4] 蔡全福.大数据技术在医疗健康管理的应用与设计[J].安徽电子信息职业技术学院学报,2022,21(6):1-6.

[5] 杨娅,吕国卿,马培元,等.基于大数据的医院健康管理平台的构建与实践[J].济宁医学院学报,2022,45(3):189-191.

基于深度学习的 实时大数据流处理框架优化与性能分析

文 ◆ 苏州高博职业学院 陈永平

引言

随着信息技术的迅猛发展，大数据和人工智能技术在实时数据处理领域的应用日益广泛。深度学习作为人工智能的重要分支，通过强大的特征提取和模式识别能力，显著提升了实时大数据流处理的效率与精度。然而，深度学习模型的复杂性和高计算资源需求对实时大数据流处理框架的优化提出了新的挑战。本文旨在研究基于深度学习的实时大数据流处理框架的优化方法与性能分析。通过对大数据流处理的基本概念和主流框架的介绍，分析了现有框架的优缺点，探讨了深度学习在数据流处理中的应用，包括数据预处理、特征提取和预测分析。研究表明，引入深度学习技术有助于提升实时大数据流处理框架的性能，但同时也需应对模型复杂性和资源管理的挑战。本文为实时大数据流处理框架的优化提供了理论依据和实践指导，具有重要的参考价值。

1 实时大数据流处理框架概述

1.1 大数据流处理的基本概念

大数据流处理（Big Data Stream Processing）指的是对持续生成的海量数据进行实时或近实时的处理和分析^[1]。与批处理不同，流处理强调低延迟、高吞吐量的数据处理能力，能够在数据产生的瞬间进行处理，适用于需要即时响应的应用场景，如金融交易监控、网络安全防护、实时推荐系统等。大数据流处理框架通过分布式计算和并行处理技术，能够实现对数据流的高效处理和实时分析，确保数据在生成后能迅速被处理并反馈结果^[2]。

1.2 主流实时数据流处理框架介绍

目前，主流的实时大数据流处理框架主要包括 Apache Storm、Apache Flink、Apache Spark Streaming 以及 Google Dataflow 等。这些框架各具独特的架构设计和功能特性，能够满足不同应用场景和业务需求的多样化要求。

2 深度学习在数据流处理中的应用

2.1 深度学习的基本原理

深度学习是机器学习的一个重要分支，基于人工神经网络，通过多层结构实现对数据的特征提取和表示学习^[3]。深度学习模型通过反向传播算法，自动调整网络权重，从而实现了对复杂数据模式的识别和预测。典型的深度学习模型包括卷积神经网络（CNN）、循环神经网络（RNN）和生成对抗网络（GAN）等。

反向传播算法用于训练神经网络，通过计算损失函数对网络权重的梯度，实现权重的更新。损失函数通常采用均方误差（MSE）或交叉熵损失（Cross-Entropy Loss）。计算公式如式（1）所示。

$$\frac{\partial L}{\partial W} = \frac{\partial L}{\partial a} \cdot \frac{\partial a}{\partial z} \cdot \frac{\partial z}{\partial W} \quad (1)$$

式（1）中， L 表示损失函数， W 表示权重， a 表示激活值， z 表示加权输入。

2.2 深度学习与数据流处理的融合点

深度学习技术与实时数据流

【作者简介】陈永平（1981—），男，山西大同人，本科，高级工程师、高级网络规划设计师、高级系统规划与管理师、高级信息系统项目管理师，研究方向：数字化校园与企业信息化建设、云计算、大数据、人工智能、网络安全工程项目实施与技术研究应用。

处理的融合，主要体现在数据预处理、特征提取和预测分析等环节。通过在数据流处理框架中集成深度学习模型，可以实现对实时数据的智能分析和处理，提升数据处理的自动化和智能化水平^[4]。

数据预处理是深度学习模型应用的前提，包括数据清洗、归一化和数据增强等步骤。在实时数据流处理框架中，可以利用深度学习模型。深度学习与数据流处理的融合点如表 1 所示。

3 实时数据流处理框架的优化设计

实时数据流处理框架的优化设计旨在提升系统的处理能力和性能，确保实时性和准确性。本文将从系统架构的优化和深度学习算法的优化两个方面进行详细探讨。

3.1 系统架构的优化

系统架构的优化是提升实时数据流处理框架性能的基础。合理的架构设计能够有效提升数据处理的并行性和分布式计算能力，降低系统延迟。

3.1.1 数据输入层优化

数据输入层作为实时大数据流处理系统的前端入口，承担着数据采集与预处理的关键职责。优化数据输入层不仅能够显著降低数据传输延迟，还能提升整个系统的数据处理实时性和响应速度。

采用高效的数据采集协议和传输机制是优化的基础^[5]。Apache Kafka 和 RabbitMQ 等分布式消息队列系统因其高吞吐量和低延迟特性，被广泛应用于实时数据流的传输。Kafka 通过其分区和复制机制，实现了高可用性和横向扩展能力，适合处理大规模、高频率的数据流；RabbitMQ 则以灵

表 1 深度学习与数据流处理的融合点

融合环节	深度学习应用	主要技术
数据预处理	数据清洗、归一化、数据增强	CNN, RNN
特征提取	自动特征提取、降维	CNN, Autoencoders
预测分析	实时预测、分类、异常检测	LSTM, GAN, Transformer

活的路由机制和多协议支持，适用于复杂的消息传递场景^[6]。通过合理配置消息队列系统，可以确保数据的高效传输和系统的稳定运行。

数据输入层优化方案比较如表 2 所示，对比了不同数据输入层优化方案的优缺点。

表 2 数据输入层优化方案比较

优化方案	描述	优点	缺点
Kafka	分布式消息队列系统	高吞吐量、低延迟	配置复杂
RabbitMQ	消息代理软件	灵活性高、支持多种协议	吞吐量相对较低
数据压缩技术	使用 GZIP、Snappy 等压缩数据	减少带宽占用、加快传输速度	增加 CPU 负担
数据预处理模块	实时数据清洗和格式转换	减少后续处理负担	增加数据处理延迟

3.1.2 数据处理层优化

数据处理层是数据流处理系统的核心，负责数据的实时处理和分析。优化数据处理层可以提升系统的计算效率和并行处理能力，确保数据处理的实时性和准确性。

首先，采用分布式计算框架，如 Apache Flink 和 Spark Streaming，能够实现数据的并行处理，提升系统的计算能力^[7]。其次，利用内存计算技术，如 Spark 的内存缓存机制，减少磁盘 I/O 操作，提高数据处理速度。最后，优化数据处理算法，采用高效的并行算法和数据结构，能够进一步提升数据处理的性能。例如，利用图计算算法进行实时图分析；采用流式机器学习算法进行实时预测和分类。数据处理层优化技术比较如表 3 所示。

表 3 数据处理层优化技术比较

优化技术	描述	优点	缺点
分布式计算框架	使用 Flink、Spark Streaming 等框架	高并行性、高可扩展性	配置和管理复杂
内存计算技术	使用内存缓存机制	提高数据处理速度	内存消耗较大
高效并行算法	采用流式图计算、并行机器学习算法	提升计算效率	算法设计复杂
数据结构优化	使用高效的数据结构，如哈希表、B 树等	提高数据访问和处理速度	增加实现复杂度

3.1.3 数据输出层优化

数据输出层负责将处理后的数据传输到下游系统或存储系统，优化数据输出层可以减少数据传输的延迟，提升系统的整体性能。

首先，采用高效的数据传输协议和存储接口，如 HTTP/2、gRPC 等，加快数据传输速度，降低传输延迟。其次，利用异步数据传输机制，避免数据传输过程中的阻塞，提高系统的吞吐量。最后，优化数据格式，

如使用 Protobuf、Avro 等高效的序列化格式,有利于减少数据传输的开销,提高数据传输的效率。

3.2 深度学习算法的优化

深度学习算法的优化是提升实时大数据流处理框架性能的关键。通过优化深度学习模型的结构和训练方法,可以显著提高模型的推理速度和准确性,满足实时数据处理的需求。

3.2.1 模型压缩与加速

深度学习模型通常具有庞大的参数量和复杂的计算结构,直接应用于实时数据流处理框架时,会导致推理速度过慢,无法满足实时性要求。因此,模型压缩与加速技术成为优化的关键。

模型剪枝是通过去除神经网络中冗余的连接和神经元,减少模型的参数量和计算量来实现。量化技术则是通过降低模型参数的精度,如将 32 位浮点数转换为 8 位整数,减少模型的存储需求和计算开销来实现。知识蒸馏是将一个复杂的教师模型的知识迁移到一个较小的学生模型中,保持模型性能的同时降低模型复杂度。

模型剪枝后的参数量计算公式如式(2)所示。

$$P_{pruned}=P_{original}\times(1-r) \quad (2)$$

式(2)中, P_{pruned} 表示剪枝后的参数量, $P_{original}$ 表示原始模型的参数量, r 表示剪枝率。

3.2.2 在线学习与增量更新

在线学习与增量更新技术使深度学习模型能够在数据流处理过程中持续学习和更新,有利于适应数据分布的动态变化,提升模型的适应性和准确性。

在线学习指的是模型在接收到新数据时,能够立即进行学习和更新,无需重新训练整个模型。增量更新则是指在已有模型的基础上,通过少量新数据进行更新,保持模型的最新状态。计算公式如式(3)所示。

$$\theta_{new}=\theta_{old}-\eta\nabla_{\theta}L(\theta;x,y) \quad (3)$$

式(3)中, θ_{new} 表示更新后的模型参数, θ_{old} 表示原始模型参数, η 表示学习率, $\nabla_{\theta}L(\theta;x,y)$ 表示损失函数对参数的梯度。

3.2.3 资源调度与负载均衡策略

在实时大数据流处理框架中,深度学习模型的训练和推理需要大量的计算资源。合理的资源调度与负载均衡策略能够优化资源的利用率,提升系统的整体性能和稳定性。

资源调度指的是动态分配计算资源,以满足不同任务的需求,确保系统的高效运行。负载均衡则是指将任务均匀分配到不同的计算节点,避免资源的过载和闲置,提高系统的吞吐量和响应速度。

结语

本文研究了基于深度学习的实时大数据流处理框架的优化与性能分析。首先,介绍了实时大数据流处理的基本概念,强调了其在低延迟和高吞吐量数据处理中的重要性,并概述了当前主流的实时数据流处理框架,如 Apache Storm、Apache Flink、Apache Spark Streaming 和 Google

Dataflow,分析了各自的优缺点。

在实时数据流处理框架的优化设计部分,本文从系统架构优化和深度学习算法优化两个方面进行了深入探讨。系统架构优化包括数据输入层、数据处理层和数据输出层的优化,通过采用高效的数据采集协议和传输机制、分布式计算框架、内存计算技术以及高效的数据传输协议和数据格式,实现了系统的高并行性和低延迟。深度学习算法优化则涵盖模型压缩与加速、在线学习与增量更新以及资源调度与负载均衡策略,通过模型剪枝、量化技术、知识蒸馏等方法,降低了模型的计算复杂度和存储需求,同时提升了模型的推理速度和适应性。^[8]

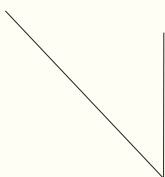
引用

- [1] 杨知玲,谭树杰.不确定大数据流分类的决策树模型构建仿真[J].计算机仿真,2024,41(5): 532-535+542.
- [2] 成伟.基于BMRC-细粒度情感分析的电影推荐系统设计与实现[D].石家庄:河北经贸大学,2024.
- [3] 蒋稷峰.基于剖分的大湾区高分卫星时空数据立方体[D].广州:广州大学,2024.
- [4] 韩畅.数据安全态势感知关键技术的研究与实现[D].成都:电子科技大学,2024.
- [5] 王靖.基于增强现实(AR)、深度学习与大数据技术的分布式水电站智慧检修系统研究[J].水电与抽水蓄能,2023,9(6):55-59+91.
- [6] 叶盛.IoT感知的服务组合动态调整及质量优化研究[D].北京:北方工业大学,2023.
- [7] 明智涛.基于Spark Streaming的电网运行数据分析系统研究与实现[D].扬州:扬州大学,2023.

RPA 与 AI 技术融合

在企业智能决策支持系统中的作用研究

文 ◆ 中铁十二局集团有限公司财务共享服务中心 耿 倩



出了显著的应用价值。借由精准把控线程并行度、学习率等关键参数，不但提高了企业的数据处理效率，还强化了决策的精准性与反馈的实时性。基于此，本文深入研讨了 RPA 与 AI 技术在企业智能决策支持系统中的深度融合以及实际应用的价值。从数据整合、决策模型优化以及全流程自动化执行这 3 个层面展开分析，以明晰此技术组合对企业智能决策的效率与质量实现全面提升的推动作用。就数据整合而言，RPA 凭借其高效的数据采集与处理，再加之 AI 对非结构化数据的解析能力，达成了跨平台的数据整合以及实时更新。在决策模型优化方面，AI 的动态学习能力同 RPA 的快速部署能力相互结合，促使决策系统迅速适应环境变化并持续进行迭代改进。而在执行这一环节时，RPA 与 AI 协同达成了从决策生成至执行反馈的全流程自动化，有力保障了决策的精准性与响应速度。因此，RPA 与 AI 的融合为企业赋予了创新的智能决策支持，成为数字化转型的关键驱动力。

引言

伴随数字化与智能化的迅猛发展，企业对于高效决策支持系统的需求正愈发强烈。RPA（机器人流程自动化）可对重复性任务予以自动化处理，进而提升数据处理效率，而 AI（人工智能）凭借强大的算法能力能对复杂场景给予深度分析，二者的融合给企业智能决策支持系统带来了极具革命性的变革。近些年来，RPA 与 AI 的协作应用已由单一流程自动化逐步拓展至多场景决策支持领域，如财务管理、供应链优化以及客户服务等，均凸显

1 RPA 与 AI 技术融合在企业智能决策支持系统中的作用

1.1 数据驱动的决策优化

企业智能决策支持系统基于传统数据分析，通过 RPA 与 AI 技术的融合，达成了更为高效的数据处理以及决策优化的目的。RPA 技术在处理大量结构化数据方面表现出色，如财务报表、库存信息等，而 AI 则借助深度学习以及自然语言处理能力，从非结构化数据中提炼出有价值的信息。这种融合打破了过去单一数据来源的局限性，让决策模型涵盖更为广泛的信息维度。在供应链管理情境下，此种数据驱动的优势极为显著。例如，RPA 能够自 ERP 系统里抽取库存数据，并与 AI 针对市场趋势所做的预测分析相结合，进而给予最优的采购和库存策略^[1]。如此实时且高效的整合之力，不仅减少了因信息滞后引发的决策失误，还降低了企业的运营成本。特别是处在动态的市场环境中，AI 的预测算法可依据历史数据与实时信息持续对预测模型予以调整，而 RPA 则凭借其自动化能力迅速将这些模型运用至实际业务流程当中，达成闭环决策优化。另外，RPA 与 AI 的结合在决策执行方面亦发挥着重要作用。例如，

【作者简介】耿倩（1990—），女，山西平遥人，硕士研究生，工程师，研究方向：计算机、网络安全。

当 AI 系统对市场供需变化进行预测时，RPA 可以自动生成订单、调整生产计划或者向相关部门发送通知，缩减了决策至执行的时间间隔。总体而言，此种数据驱动的优化机制促使企业的智能决策支持系统由“分析型工具”向“行动型助手”转变。

1.2 异常检测与风险管理

RPA 与 AI 的结合在企业智能决策中为异常检测与风险管理提供了崭新的思路。AI 算法的强大学习能力，能够在海量历史数据中萃取正常模式，且可以实时甄别偏离此等模式的异常状况，而 RPA 技术则可以迅速针对这些异常施行相应举措，以保障决策链条的完整性与及时性。以金融领域为例，在信用风险管理中，基于历史交易数据与信用评分系统，AI 模型能够对潜在的违约风险予以预测。当 AI 侦测到异常交易时，RPA 可以即刻冻结相关账户，触发风险应对流程并向有关部门予以通知。此外，在复杂的供应链情境下，RPA 能够迅速抓取合同订单、物流以及付款数据，与 AI 的模型分析相结合，以识别潜在的延迟风险或欺诈行为，助力企业适时调整策略。这种技术融合亦化解了传统风险管理系统所存有的两大问题，其一为响应速度，其二为识别精度。传统系统通常依靠手动操作以及静态规则，难以对动态变化做出及时响应^[2]。RPA 与 AI 的结合借由自动化与智能分析，提升了实时性与准确性，规避了因响应迟缓或规则滞后所导致的损失。总之，此种融合为企业构筑起了更为可靠和主动的风险管理体系。

2 RPA 与 AI 技术融合的应用现状分析

2.1 自动化流程中的应用深化

RPA 与 AI 技术的融合正促使企业自动化流程由规则驱动朝着智能化转变。传统的 RPA 主要依据固定规则来实施操作，如数据录入、文件处理等，虽效率有所提升，但在应对复杂多变的场景时却显得颇为乏力。AI 技术的引入使自动化流程在应对非结构化数据、动态环境以及多变量决策时呈现出更强的适应性能。在财务报账管理流程中，这一整合展现了巨大的效益。传统的自动化工具能够快速录入员工提交的报销单据中的基本数字信息，但对于非标准格式的资料（如收据照片、手写备注或是通话录音等），其应对能力相对薄弱。然而，借助先进的 OCR（光学字符识别）技术与自然语言理解功能，AI 技术能够精准捕捉报销材料中的核心要素，如发票详情中的商品与服务项目、手写说明中的特殊事项或通话录音中确认的报销理由，并将这些信息转换为自动化流程软件可解析的格式，从而实现从资料提交到审批支付的全程自动化^[3]。这一创新结合不仅显著减少了人工审核的工作量，还极大加速了报账流程，增强了员工的报销体验与满意度。

2.2 数据分析与决策支持的创新实践

在建筑施工领域，此类技术融合取得了显著进展。AI 模型能够预测施工过程中的能源与资源需求波动，通过分析设备运行数据来识别潜在的机械故障或效率低下问题，而 RPA（机器人流程自动化）技术则将这些预测结果与实时监控的施工数据相结合，自动生成并执行优化的资源调度与施工计划。例如，在大型基础设施项目的施工高峰期，系统能

依据 AI 预测调整各施工区域的能源与材料分配计划，同时利用 RPA 自动触发施工机械的启停或调整作业班次，以确保施工进度顺利推进以及设备使用效率的最大化。这种智能化的分析与执行能力，不仅显著提升了施工管理的决策效率，还大幅减少了人工干预带来的误差与延误。

3 RPA 与 AI 技术融合在企业智能决策支持系统中的应用

3.1 数据整合智能化的提升

对于企业智能决策支持系统而言，RPA 与 AI 技术融合的核心价值展现在数据整合能力智能化的提升方面。在企业的日常运营中，数据往往分散于不同的系统和格式里，如 ERP、CRM、Excel 文件以及邮件附件等。传统的数据整合方式不但耗时长久，精度较低，而且难以契合动态变化的需求。然而，RPA 技术凭借其自动化与高效性，与 AI 的数据分类以及处理能力相结合，致使数据整合不再受限于规则设定，而能够动态适应各种不同的场景与需求。在企业预算管理的应用中，这一技术优势体现得尤为突出。预算编制需要对来自诸如财务报表、项目数据、历史成本记录等多种渠道的信息予以整合，传统的人工操作不但效率低下，还极易因格式不一致或者人为疏忽而造成数据遗漏^[4]。RPA 能够通过脚本自动从不同系统中提取数据，同时可调用 AI 对文本和表格内容进行智能解析，如识别发票中的供应商名称、交易金额等关键信息。经 AI 建模处理所提取的数据，可生成跨部门一致的预算模型，且能借由 RPA 进一步分发至相关

决策者，达成了从数据采集至整合再到应用的全流程自动化。

3.2 决策模型的动态优化

RPA 与 AI 融合后的另一重要应用体现于对决策模型的动态优化能力方面。这种优化既展现在模型准确性的提高方面，又涵盖模型对外部环境变化的快速适应能力方面。传统的决策模型往往依据历史数据构建，其规则一经设定便不易调整，然而 RPA 与 AI 的结合促使模型能够伴随时间和环境的变化持续进行迭代与改进。于供应链管理情境中，AI 通过对历史交易数据和实时市场信息的分析，能够预测未来的需求趋势，而 RPA 则把这些预测结果自动整合至现有的决策模型当中。

3.3 决策执行的全流程自动化

RPA 与 AI 技术地融合在决策执行环节彰显出全流程自动化的显著优势。传统意义上的决策执行，通常需要诸多环节中人工

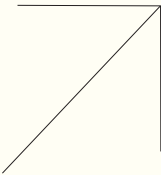
的参与，涵盖从决策下达、任务分配至具体操作，流程繁杂且易受人为因素干扰。RPA 技术借助流程自动化，促使决策执行由手动操作向系统驱动转变，同时与 AI 对执行结果进行的实时反馈以及优化相结合，令整个过程更为高效且形成闭环。同时，扩展至建筑行业经营承揽方面，当企业规划好经营承揽策略后，需迅速在各类市场渠道进行布局，并实时跟踪承揽项目的进展与成效^[5]。当前，RPA 与 AI 技术的结合正深刻改变着建筑行业经营决策支持系统的运作方式。AI 能够深度分析潜在客户的项目需求与行为模式，从而推荐出最佳的项目承揽渠道与时机，而 RPA 则根据 AI 的指引自动完成项目信息的录入、承揽参数的设定以及资源的初步分配。承揽工作启动后，RPA 还能实时收集各渠道的反馈信息，如项目咨询量、中标率等关键指标，并通过 AI 模型评估是否需要调整承揽策略。若 AI 发现某一渠道的承揽效果不佳，RPA 能立即减少在该渠道的投入，并将资源调配至效率更高的渠道，整个过程紧密配合，无需人工直接参与，确保了建筑行业经营承揽的精准性和高效性。这种全流程自动化的执行模式，不但大幅提升了执行效率，还有力确保了执行结果与决策意图的高度相符性。尤为重要的是，通过 AI 对执行过程中数据的实时监控，企业可在过程中动态优化决策，避免资源浪费或者机会损失。

结语

对于数据整合的智能化提升，决策模型的动态优化、决策执行全流程自动化等技术结合不但赋予企业以更高决策效率，还增强其对复杂多变环境的适应能力。借由将自动化与智能化实现无缝衔接，企业既可降低运营成本，又能在市场竞争中占据更为主动的位置。未来，伴随技术的持续演进，RPA 与 AI 的应用潜力会进一步得以释放，为企业造就更多创新场景与价值增长点。同时，在这场数字化转型的浪潮中，对 RPA 与 AI 融合的拥抱会成为企业智能决策发展的重要驱动力。^[6]

引用

[1] 英璐,王强.基于智能制造的工艺决策支持系统研究[J].阀门,2024(7):870-872.
[2] 徐铭蔚.会计信息系统与智能决策支持系统的集成研究[J].财会学习,2024(9):97-99.
[3] 佟佳梦.企业财务分析与决策支持系统研究[J].大市场,2024(4):115-117.
[4] 付艳玉.人工智能在财务决策支持系统中的应用研究[J].大市场,2024(8):10-12.
[5] 冯雪.电力企业人事档案管理中的人工智能应用与实践[J].现代企业文化,2023(29):38-41.



ChatGPT 应用于医学图书馆 咨询服务的建设路径与策略研究 *

文 ◆ 南方医科大学图书馆 贾司渤

引言

ChatGPT 作为目前代表性的生成式人工智能工具，为图书馆咨询服务的发展注入了新的技术活力。本文在分析 ChatGPT 应用方向的基础上，探讨了 ChatGPT 为医学图书馆带来的机遇和挑战。聚焦 ChatGPT 在医学图书馆咨询服务中的应用，提出了从准备、测试、评估、反馈 4 个阶段开展对医学图书馆咨询服务的建设路径探索以及设置检索指令、制定医学提示词、验证生成信息、馆员提供指导的建设策略。

1 研究背景

医学图书馆作为医学信息资源的重要载体，通过为医务人员提供包含最新研究成果、临床实践指南在内的专业文献资源，以实现最佳的诊疗支持。传统依靠搜索引擎和数据库的信息获取方法无法充分保证用户对于医学信息资源的准确性、相关性和可访问性等方面的要求。具体表现在传统搜索引擎缺乏语义理解能力，无法理解用户的检索意图并与上下文信息关联，因此难以准确处理用户的检索要求。而数据库由于其高昂的订购价格以及复杂的检索方式则对用户提出了更高的使用要求。

2022 年 11 月，由 OpenAI 开发的自然语言处理模型 ChatGPT 在回答用户提问时所展现出的准确性、快速性、互动性、丰富性^[1]，迅速在语言翻译、文本生成、智能客服等领域开展广泛应用^[2]。ChatGPT 在多个领域的成功实践成为图书馆业界关注的焦点。ChatGPT 依托的大型语言模型可以基于大量数据进行自主知识学习，帮助用户解决实际问题，与图书馆的服务属性具有较高的契合度^[3]。尽管现阶段 ChatGPT 在医学图书馆的实践案例较少，对其开发应用也有待进一步探索，但 ChatGPT 在改进信息检索、用户体验和知识传播等方面存在着巨大潜力。

2 ChatGPT 的应用方向

2.1 文本生成

ChatGPT 是一种基于深度学习技术的自然语言处理模型，通过分析大量

的语料库，可以学习到人类语言的规则和模式，从而生成符合语法和语义规则的文本内容。该技术在图书馆领域具有广泛的应用前景，可以帮助图书馆员更快地查找并生成特定信息，提高工作效率。

2.2 问答系统

ChatGPT 凭借其强大的语言生成能力，构建出高效的问答系统。根据用户提问，快速生成解决方案。在教育领域，ChatGPT 作为教学辅导工具在课堂教学中使用，根据教师或学生提出的问题或案例进行解答，帮助教师以多种方式呈现课程内容以及为学生提供课程以外的补充信息和延伸阅读材料。

2.3 资料搜集

用户在向 ChatGPT 请求特定主题或领域的信息时，ChatGPT 可以基于自身的预训练模型从庞大的语义数据库中抓取符合用户需求的信息资料。例如，在学术写作中，ChatGPT 可以根据研究人员提供的关键词，针对某一主题的学术文献、研究报告或案例进行提取和梳理，为研究人员归纳出符合研究方向的论点论据。

*【基金项目】本文为广东省医学科学技术研究基金项目 2024 年度立项项目“基于 UTAUT2 的医学相关人员利用大语言模型工具辅助学习与科研的意愿及影响因素分析”的研究成果之一（A2024271）

【作者简介】贾司渤（1994—），男，黑龙江牡丹江人，硕士研究生，助理馆员，研究方向：用户信息服务研究。

3 ChatGPT 对于医学图书馆的价值

目前，ChatGPT 在客服与支持系统中得到广泛应用，而在图书馆咨询服务领域也同样具有应用潜力。其基于自然语言、语义理解以及上下文推理功能，在参考咨询、资源导航、科研支持、馆藏编目与分类等方面具有独特优势。

与传统的图书馆咨询服务模式不同，ChatGPT 作为一种知识支持系统，具备的信息处理和交互能力在为用户提供个性化信息支持方面具有独特优势。根据现有研究，ChatGPT 在不同类型的图书馆中开展了多种应用探索，包括回答读者咨询问题、提高文献检索和数据处理效率、辅助教学等方面表现出色^[4]。但 ChatGPT 也存在局限性，如缺乏理解情感的能力，在回答用户所提出的复杂问题时呈现错误或过时的信息等^[5]。

现阶段医学领域的快速发展对医学图书馆提出了更高的要求，包括对已有知识进行整合，挖掘新的医学知识资源，为用户评估信息资源质量，协助进行医学文献和数据管理以及指导用户使用不同类型的技术工具开展科研活动等。因此，ChatGPT 在医学图书馆中的应用潜力巨大，对其研究和开发应着眼于如何充分发挥其技术优势，从而为用户提供更加高效、智能和个性化的服务，推动医学信息管理和服务的现代化进程。

4 ChatGPT 为医学图书馆带来的机遇与挑战

4.1 机遇

4.1.1 优化检索质量

通过自然语言处理和机器学习技术，使咨询系统能够更准确地理解用户的需求并提供相关的信息资源，提升用户信息获取效率。当 ChatGPT 用于文献检索时，有助于研究人员快速找到相关的文献资源。医学研究人员通过与 ChatGPT 进行对话，提出关于特定主题的问题，ChatGPT 根据问题的语义理解，提供相关的文献推荐。

4.1.2 提升编目效率

ChatGPT 有助于提升医学图书馆编目的效率和质量，包括利用 ChatGPT 进行自动化编目和智能分类。借助 ChatGPT 的自然语言处理技术，自动抓取文献资源的关键信息，如标题、作者、出版日期等，形成初步的书目记录。通过分析医学文献内容，自动分配主题词、分类号和关键词，提高编目的准确性。

4.1.3 提供研究支持

整合 ChatGPT 与医学图书馆馆藏系统，可为医务人员开展研究工作提供资源支持。根据医务人员的研究方向与检索记录，生成不同研究主题的文献推荐列表，提供科研支持。同时，分析馆藏数据，构建知识图谱，揭示不同文献之间的关联，帮助医务人员更快锁定符合其研究需求的特定资源。

4.2 挑战

4.2.1 准确性、真实性尚待改善

信息资源的权威性和真实性是发挥图书馆价值的基础，生成内容本身和引用的各种文献资料必须准确无误。而自然语言生成模型建构在语料库中在形成文本时无法做到字斟句酌，无法注明引用信息来源。同时，所使用的数据来源庞大且质量参差不齐，甚至包含虚假内容。在基于这些数据生成回答时，必将对用户产生误导^[6]。因此，图书馆应指导用户辨别信息的可信度和来源，避免过度使用人工智能而产生的技术依赖。

4.2.2 隐私数据泄漏

OpenAI 在隐私政策中提到，ChatGPT 会收集用户账户信息、对话等相关的所有内容、互动中网页内的各种隐私信息（如 Cookies、日志、设备信息等），这些信息会被共享给供应商、服务提供商以及附属公司，数据共享过程会有未经授权的攻击者访问模型相关的隐私数据，导致在图书馆使用中，用户群体会对使用 ChatGPT 等大型语义模型产生包括对数据泄露、未经授权访问用户数据以及用户数据被用于图书馆之外的目的的担忧。

4.2.3 信息道德界定模糊

ChatGPT 本身的功能缺陷可以通过收集丰富的语料库、提高训练和优化的效率和质量以及开发人工智能检查和修改的工具来改善，但是更深层次的著作权保护、信息道德约束也是图书馆需要思考的问题。目前 ChatGPT 能够在用户的引导下，基于数据库内容的学习快速生成创造性内容。但是否会构成对被抓取作品的侵权、生成的文本内容是否具有著作权以及版权是否属于该用户等一系列问题的答案尚不明确，容易引发知识产权纠纷问题^[7]。

5 ChatGPT 应用于医学图书馆咨询服务的建设路径

5.1 准备阶段

首先,确定评估标准。该标准应将 ChatGPT 运用于医学图书馆时生成内容的准确性、连贯性以及上下文理解程度作为评估的核心部分。其次,构建可以反映医学图书馆用户各种检索行为的测试数据集,使其能够在多种应用场景下进行完整测试和评估,确保测试的全面性。

5.2 测试阶段

创建模拟医学图书馆环境中用户互动的现实场景,包括常见的参考咨询问题,较为专业和复杂的医学知识检索、诊疗方案支持以及医学论文写作等。邀请图书馆员、教师、医务人员、医学生群体参与到测试中,根据自身的学习和科研需求向 ChatGPT 提出各类咨询问题,以便对 ChatGPT 进行效果和有效性评估。

5.3 评估阶段

在完成测试后,应评估 ChatGPT 生成内容的准确性和关联性,确保其符合用户的使用需求。评估 ChatGPT 在医学领域内,是否能够理解用户检索需求并生成逻辑结构清晰的答案以及对于专业医学知识的检索能力,确保语言模型能够满足医学图书馆用户专业化的信息需求,使 ChatGPT 具备处理专业问题的能力。

5.4 反馈阶段

通过图书馆员、教职工以及不同专业的学生群体所提供的 ChatGPT 的使用反馈,详细记录各种用户群体关于 ChatGPT 使用的优缺点和改进建议。汇总从语言模型评估中获得的各项数据,系统记录评估结果。总结用户的使用反馈,形成具有可行性建议的文字报告。

6 ChatGPT 在医学图书馆咨询服务中的建设策略

6.1 设置检索指令

明确在医学图书馆的使用背景下,ChatGPT 会接收到的用户检索请求,设置具体的检索指令,使 ChatGPT 能够准确识别用户提出的具体服务要求,如处理病例查询或提供医学文献资源推荐。

6.2 制定医学提示词

考虑医学术语的复杂性,为了便于用户明确表达检索需求,应针对医学知识体系,制定全面、专业、具有关联性的检索提示词,以确保 ChatGPT 能够准确理解并回答医学领域的相关问题。

6.3 验证生成信息

虽然借助 ChatGPT 可以快速获取和生成信息资源,但医学图书馆必须对于生成内容进行逻辑性和真实性的检查验证。因此,应利用馆藏图书、各类数据库等较为权威的信息源对 ChatGPT 所生成信息进行交叉验证,以确保用户获取信息的准确性和可靠性。

6.4 馆员提供指导

图书馆员应提醒用户在依据 ChatGPT 的生成内容做出决策判断之前,对关键和特定信息进行查证。鼓励用户在使用 ChatGPT 时,从多方面佐证所要获取的医学信息资源,指导用户使用 ChatGPT 时符合信息道德规范。

结语

ChatGPT 作为人工智能背景下的代表性技术成果,为图书馆领域展现了巨大的应用价值。医学图书馆应充分认识到 ChatGPT 的技术特点及其为自身所带来的机遇与挑战,探索 ChatGPT 如何有效应用到医学图书馆业务工作中,发挥 ChatGPT 的技术优势和医学图书馆的资源优势,持续推动医学图书馆服务向纵深发展。^[8]

引用

- [1] Van Dis E A M,Bollen J,Zuidema W,et al.ChatGPT:Five Priorities for Research[J].Nature,2023,614(7947).
- [2] Hutson M.Could AI Help You to Write Your Next Paper?[J].Nature,2022,611(7934):192-193.
- [3] 吴若航,茆意宏.ChatGPT热潮下的图书馆服务:理念、机遇与破局[J].图书与情报,2023(2):34-41.
- [4] Verma M.Novel Study on AI-based Chatbot(ChatGPT) Impacts on the Traditional Library Management[J].International Journal of Trend in Scientific Research and Development,2023,7(1):961-964.
- [5] Adetayo A J.ChatGPT and Librarians for Reference Consultations[J].Internet Reference Services Quarterly,2023,27(3):131-147.
- [6] 李雅丽.ChatGPT在学术出版中的应用与影响[J].传播与版权,2024(16):20-22.
- [7] 冯雨隼.ChatGPT在教育领域的应用价值、潜在伦理风险与治理路径[J].思想理论教育,2023(4):26-32.

一种基于深度学习及 AI 语音识别的工业软件大模型 *

文 ◆ 陕西空天超算中心有限公司 刘 琨 成李博 房庆龄
陕西空天动力研究院有限公司 刘 霞

引言

近年来，运用 AI 辅助 CAE 仿真分析成为新的热点。目前，AI 已在多个分析领域进行了初步探索和应用，其技术的应用将大幅缩短数据分析及优化时间。同时，机械仿真设计软件是利用数值理论方法对工程中一系列问题求解的重要工具，长期以来面临着理论不完备和计算能力不足的挑战，导致大量工程问题难以得到快速、准确的求解。此外，软件操作的复杂性也限制了技术人员的使用。本文所提出的技术，通过将 AI 技术应用于工程软件，能有效加速求解速度，并结合语音识别降低技术人员的应用门槛，从而加速工业软件行业的智能化发展。

1 人工智能和深度学习概述

AI 即人工智能的简称，是一门研究和开发用于模拟、延伸和扩展人类智能的理论、方法、技术以及应用系统的技术科学^[1]。其通过计算机程序和算法，模仿并扩展了人类智能的多个方面，包括感知、学习、推理和决策等^[2]。AI

包括多个分支，如机器学习、深度学习、自然语言处理、计算机视觉等。深度学习是机器学习的一种形式，利用具有多个层次的神经网络来处理和学习数据^[3]。通过对数据进行层次化的抽象，深度学习使计算机能够更准确地识别和解释复杂的数据结构。人工智能、机器学习、深度学习及神经网络关系图如图 1 所示。神经网络是深度学习的基础（算法），深度学习是机器学习的一种形式，而机器学习则是人工智能的重要组成部分。

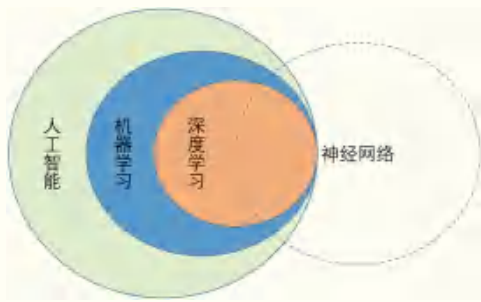


图 1 人工智能、机器学习、深度学习及神经网络关系图

2 深度学习与 CAE

CAE 是用计算机辅助求解复杂工程和产品结构强度、刚度、屈曲稳定性、动力响应、热传导、三维多体接触、弹塑性等问题的分析计算以及结构性能优化设计等问题的一种近似数值分析方法。

深度学习是通过多层神经网络算法从大量数据中自动归纳逻辑或规则形成模型，并根据模型对新数据进行预测。

两者既有共性又有差异，共性在于都是基于给定的输入条件或参数来分析或预测相应的响应。差异性在于 CAE 分析时包含了结构、流体、电磁等学科的理论知识，在给定条件下，分析结果精度较高。而深度学习则不考虑数据间的逻辑关系和学科知识，单纯地就输入和输出数据通过归纳总结的方式分析自变量与因变量之间的关系，一般来说，预测结果精度没有 CAE 高。

然而，对于 CAE 分析来说，复杂的结构和工况条件往往需要较长

*【基金项目】西安市科学技术局“科学家+工程师”队伍建设项目“服务质量驱动的并行作业智能调度方法”（NO.23KGDW0033-2023）
【作者简介】刘琨（1996—），男，陕西咸阳人，本科，研究方向：计算机科学与技术。

的计算周期，如非线性的碰撞、跌落分析或电磁散射分析，通常需要若干天甚至若干周的时间。而深度学习模型一旦训练完成，就可以在分钟甚至秒级的时间内完成快速预测，进而极大地缩短设计周期。

因此，可以建立一种数据预测模型，该模型不是基于明确清晰的物理原理和几何特征，而是依赖于大量的历史数据^[4]。通过数据不断训练模型，最终形成基于 CAE 工程验证数据的大模型，从而对设计参数进行预测，实现参数驱动的产品设计。数据预测模型思路如图 2 所示。

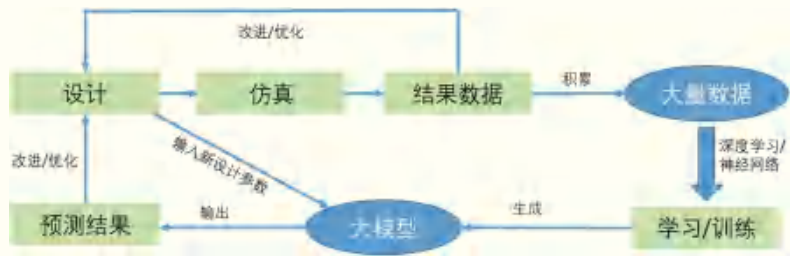


图 2 数据预测模型思路图

3 Chat—CAX 智能识别机械仿真设计软件大模型

近年来，随着工业软件的飞速发展，各类工业软件百花齐放，软件功能日益强大，但随之而来的是设计仿真人员对软件的高学习成本。面对繁重的工作任务，如何最大化地减少学习软件所需的精力和时间，在保证结果可靠性的前提下实现产品的快速迭代是值得思考的问题。针对行业痛点，提出了 Chat—CAX 大模型（见图 3），即基于 AI 智能识别的工业软件大模型，并针对智能识别、人机实时交互、商业软件二次开发、工程问题超算场景、深度学习以及神经网络进行相关技术实践和模型测试，该模型已完成首轮技术迭代。



图 3 Chat—CAX 智能识别机械仿真设计软件大模型

作为人工智能的一大分支，AI 语音识别技术现阶段在各个领域已有广泛应用，如语音助手、电话客服、自动驾驶等。其持续发展使人机交互变得更加智能、便捷和个性化，极大改善了人们的生活和工作体验^[5-7]。

Chat—CAX 将 AI 语音识别系统、人机实时交互系统以及商业软件二次开发进行深度结合，工程师的人机交互从鼠标 / 键盘的繁琐操作转换为语音指令或对话的形式，通过独立或连续的语音指令直接驱动软件操作和数据交互。借助超算的持续数据赋能，结合深度学习模型，实现了语音人机交互的全流程工程数据预测和验证。

Chat—CAX 大模型带来了一个更为便捷、智能的场景，使交互体验变得更为自然、高效，同时也提供了更多个性化、定制化的软件选择，推动了工作方式向更为智能化、数字化的方向发展。

结语

CAE 在工业领域的多年应用已积累了大量数据，为深度学习提供了

基础。随着 AI 技术的不断成熟与深入，AI 仿真分析已成为 CAE 行业发展的大趋势。本文提出的 Chat—CAX 基于 AI 智能识别的机械仿真设计软件大模型，能够针对智能识别、人机实时交互、商业软件二次开发、工程问题超算场景、深度学习以及神经网络进行相关技术实践和模型测试，并完成了首轮技术迭代。相信未来 Chat—CAX 将涌现出更多极具突破性的应用成果，为不断加快的工业发展注入新的能量。

引用

[1] 郝江.人工智能在计算机网络技术中的应用探究[J].品牌与标准化, 2024(6):215-217.

[2] 李英华,李体新.人工智能在计算机网络技术中的应用探究[J].网络安全技术与应用,2024(12):8-10.

[3] 高徐辉,黄宋魏,陈永春,等.深度学习在矿物识别中的应用现状与展望[J/OL].化工矿物与加工,1-10[2024-12-04].<http://kns.cnki.net/kcms/detail/32.1492.TQ.20241129.1036.004.html>.

[4] 卢宁.飞机制造行业数字化转型背景下的AI驱动创新模式研究[J].中国高新科技,2024(8):92-94.

[5] 中国工业互联网研究院通用人工智能与工业融合创新中心.AI大模型工业应用模式及其实现[J].中国工业和信息化,2024(4):20-25.

[6] 钱童心.从特斯拉到富士康 数字仿真技术成为AI工厂“标配” [N].第一财经日报,2023-10-24(A01).

[7] 沈嘉玮,才大业,杨国青,等.大规模脉冲神经网络动态加载仿真方法[J/OL].系统仿真学报:1-9[2024-05-31].<https://doi.org/10.16182/j.issn1004731x.joss.23-1220>.

人工智能安全框架下信息安全防护机制的探索

文 ◆ 公安部第三研究所 山东大学 张少昌

引言

人工智能作为当今科技领域的核心驱动力之一，正以前所未有的速度改变着人们的生活。从智能语音助手到自动驾驶汽车，从医疗诊断辅助系统到金融风险预测模型，人工智能的应用场景无处不在。然而，这种广泛应用也伴随着严峻的信息安全挑战。此外，人工智能算法本身也存在安全隐患。算法偏见会导致不公平的决策，如在招聘、信贷审批等领域对特定群体产生歧视性结果。面对日益严峻的信息安全问题，构建完善的信息安全防护机制成为人工智能发展的当务之急。

1 人工智能安全框架概述

人工智能安全框架是一套全面且系统的规范体系，用于保障人工智能系统全生命周期的安全稳定运行，其涵盖多方面关键要素。在架构设计上，采用分层隔离、冗余容错等技术确保系统结构稳固。在数据层面，运用加密算法与隐私保护技术维护数据安全。在算法方面，结合公平性检测、可解释性增强以及鲁棒性提升来降低风险。此外，还包括实时监测系统性能、数据流量与安全事件以及具备应急响应流程与策略以

应对突发威胁，各要素协同作用，为人工智能的安全应用筑牢基础^[1]。

2 人工智能应用中的信息安全风险

2.1 数据隐私泄露风险

在人工智能系统的数据收集过程中，存在未经授权收集数据、收集数据范围过大或数据来源不合法等问题。一些移动应用在用户不知情的情况下收集大量个人信息，包括位置信息、通讯录信息等，这些信息存在被用于非法活动的风险^[2]。此外，在物联网环境中，各种智能设备持续收集数据，但设备的安全防护能力参差不齐，容易导致数据在收集源头就被窃取。同时，数据存储环节面临着存储设备安全漏洞、数据加密不足等风险。如果存储设备被黑客攻击，且数据未进行有效的加密处理，那么黑客将轻易获取大量敏感数据。

2.2 算法偏见与可解释性问题

人工智能算法的偏见主要源于训练数据的偏差以及算法设计本身的缺陷。如果训练数据存在偏向性，且数据集中在某些群体的样本数量过少或数据质量不高，那么训练得到的算法会对这些群体产生不公平的对待。在人脸识别算法中，如果训练数据主要来自白人，那么该算法在识别其他少数族裔时会出现较高的错误率。此外，算法设计过程中的一些假设和简化也会导致偏见的产生，如在信用评估算法中，将某些地区或职业作为风险评估的重要因素，对来自这些地区或从事这些职业的人群产生歧视性结果。

2.3 恶意攻击与对抗样本

恶意攻击类型主要包含数据投毒、模型窃取和对抗样本攻击。攻击者在训练数据中注入恶意数据，破坏人工智能系统的训练过程，使训练得到的模型偏离正常预期。在垃圾邮件检测系统的训练数据中添加大量伪装成正常邮件的垃圾邮件数据，导致模型在检测垃圾邮件时准确率大幅下降。同时，攻击者试图获取人工智能模型的参数或结构信息，复制或利用该模型进行非法活动。对云服务上的人工智能模型进行多次查询，分析查询结果推断模型的内部结构和参数，从而窃取模型。此外，攻击者对输入数据进行微小的、精心设计的修改，使原本正确分类或处理的样本被人工智能系统误判。在图像识别系统中，给一张正常的熊猫

【作者简介】张少昌（1994—），男，河北晋州人，本科，研究实习员，研究方向：网络安全、人工智能、信息安全。

图片添加一些人眼难以察觉的噪声，就可使图像识别系统将其误判为长臂猿。对于对抗样本，存在严重威胁着人工智能系统的可靠性和安全性。例如，在自动驾驶领域，对抗样本导致车辆对道路标志、行人或其他车辆的误判，引发交通事故；在金融领域，对抗样本使欺诈检测系统失效，导致金融诈骗得逞；在安全监控领域，对抗样本使监控系统无法识别真正的威胁，产生安全漏洞。

3 人工智能安全框架下信息安全防护机制的构建要素

3.1 安全的人工智能架构设计

3.1.1 分层架构与隔离机制

设计人工智能系统时采用分层架构，将数据处理、模型训练、决策执行等不同功能模块分层部署，并在各层之间设置严格的隔离机制。将数据存储层与模型训练层分离，通过防火墙、访问控制列表等技术限制不同层之间的非法访问，防止数据泄露和恶意攻击在不同层之间传播。这样，即使某一层遭受攻击，也能够有效限制攻击的影响范围，保护其他层的安全。

3.1.2 冗余与容错设计

在人工智能架构中引入冗余设计，包括硬件冗余、软件冗余和数据冗余。采用多个相同功能的硬件设备，如服务器、存储设备等，当其中一个设备出现故障或遭受攻击时，其他冗余设备能够自动接管工作，确保系统的不间断运行。在软件层面，采用多版本的算法或模型，当主版本出现问题时，切换到备用版本。同时，对数据进行冗余存储，如采用分布式存储技术，将数据存储多个节点上，即使部分节点数据丢失或损坏，也能够通过其他节点的数据恢复完整信息，提高系统的容错能力。

3.1.3 安全启动与更新机制

建立安全的启动机制，确保人工智能系统在启动过程中加载的软件和数据完整且未被篡改。采用数字签名技术对系统启动文件和关键数据进行签名验证，只有通过验证的文件和数据才允许被加载。在系统更新方面，制定严格的更新流程，对更新包进行安全检测和验证，防止恶意更新包被安装到系统中。更新过程中采用增量更新技术，减少更新过程中的数据传输量和风险，同时在更新完成后对系统进行全面安全测试，确保更新不会引发新的安全漏洞。

3.2 数据加密与隐私保护技术

3.2.1 数据加密算法选择

根据数据的重要性和敏感性，选择合适的加密算法对数据进行加密。对于高度敏感的数据，如个人身份信息、金融交易数据等，采用高级加密标准（AES）、RSA 等强加密算法。AES 算法具有加密速度快、安全性高的特点，适用于对大量数据进行加密；RSA 算法则基于公钥加密体制，常用于数字签名和密钥交换等场景，能够提供更高的安全性保障。在数据传输过程中，采用 SSL/TLS 等加密协议对传输通道进行加密，确保数据在传输过程中的保密性和完整性。

3.2.2 密钥管理策略

建立完善的密钥管理策略是数据加密的关键环节。密钥的生成、存

储、分发、更新和销毁都需要遵循严格的安全规范。采用密钥分层管理机制，将主密钥与工作密钥分离，主密钥用于保护工作密钥，工作密钥则直接用于数据加密和解密操作。在大型企业的信息系统中，主密钥由专门的密钥管理服务器进行安全存储和管理，工作密钥则根据不同的业务部门和数据类型进行分配和使用。同时，定期更新密钥，有利于降低密钥被破解的风险，且在密钥使用过程中采用密钥托管、密钥备份等措施，防止因密钥丢失导致数据无法解密。

3.2.3 隐私保护技术应用

除了数据加密，还需采用多种隐私保护技术来保护数据隐私。采用数据脱敏技术，对敏感数据进行模糊化或替换处理，使数据在保持原有数据特征的基础上，无法识别出具体的个人身份信息或敏感内容。在数据共享和发布过程中，采用差分隐私技术和在数据中添加噪声的方式，在保证数据统计特性的前提下，保护数据提供者的隐私。此外，还可采用同态加密技术，允许在加密数据上直接进行计算，而无需先解密数据，在保护数据隐私的同时，实现数据的有效利用，如在云端进行加密数据的机器学习计算。

3.3 算法安全增强措施

3.3.1 算法公平性检测与修正

在算法开发过程中，建立算法公平性检测机制，对算法存在的偏见进行检测和评估。采用统计分析方法，如计算不同群体在算法决策结果中的比例差异、分析算法对不同特征的敏感程度等，判断算法是否存在偏见。一旦发现算法存在偏见，及时采取修正措施。通过调整训练数据的

分布，提高少数群体的样本数量或质量，对算法模型进行优化，修改算法中的决策规则或权重分配，以减少偏见的影响，确保算法的公平性。

3.3.2 算法可解释性增强技术

为提高人工智能算法的可解释性，采用多种可解释性增强技术。对于决策树、贝叶斯网络等相对简单的算法，可直接展示其决策过程和依据，如决策树的分支条件和节点信息。对于深度学习等复杂算法，采用可视化技术，如特征图可视化、注意力机制可视化等，展示算法在处理数据过程中的内部机制。此外，开发可解释性模型，如局部可解释性模型（LIME）和沙普利值解释模型（SHAP）等，这些模型在不改变原算法的基础上，对其决策结果进行近似解释，帮助用户理解算法的决策过程和依据。

3.3.3 算法鲁棒性提升

利用多种方式提升算法的鲁棒性，提高其抵御恶意攻击和对抗样本的能力。在算法训练过程中，采用对抗训练技术，将对抗样本纳入训练数据，使算法学习对抗样本的特征，从而提高对对抗样本的识别和抵御能力。在图像识别算法训练中，生成大量的对抗图像样本，并将其与正常图像样本一起进行训练，使算法在面对对抗样本时做出正确判断。同时，采用模型正则化技术，限制模型的复杂度，防止模型过拟合，从而提高模型的泛化能力和鲁棒性。此外，对输入数据进行预处理，如数据清洗、数据标准化等，去除数据中的异常值和噪声，减少对抗样本的产生机会。

3.4 实时监测与应急响应体系

3.4.1 监测指标与技术

建立全面的实时监测体系，确定一系列监测指标，包括系统性能指标、数据流量指标、安全事件指标等。监测人工智能系统的 CPU 使用率、内存占用率、模型准确率等系统性能指标以及网络数据流量的大小、来源和去向等数据流量指标，同时关注是否有异常的登录尝试、数据访问请求等安全事件指标。采用多种监测技术，如入侵检测系统（IDS）、入侵防范系统（IPS）、安全信息和事件管理系统（SIEM）等，对系统进行全方位监测。IDS 检测到网络中的入侵行为并发出警报，IPS 则能够在检测到入侵行为后及时采取措施阻止攻击，SIEM 系统能够收集、分析和关联各种安全事件信息，提供全面的安全态势感知。

3.4.2 应急响应流程与策略

制定完善的应急响应流程和策略，当监测到安全事件发生时，迅速启动应急响应机制。应急响应流程包括事件确认、事件评估、事件遏制、事件根除和系统恢复等环节。当发现数据泄露事件时，首先确认事件的真实性和影响范围，评估事件的严重程度，采取措施遏制数据泄露的进一步扩大，如切断网络连接、暂停相关业务等。其次，深入调查事件原因，根除安全隐患，如修复系统漏洞、更换被攻击的设备等。最后，恢复系统的正常运行，并对整个事件进行总结和分析，完善信息安全防护机制。在应急响应策略方面，根据不同类型的安全事件制定相应的应对策略，如针对数据投毒攻击，采用数据清洗和重新训练模型的策略；针对对抗样本攻击，采用更新算法模型和加强输入数据检测的策略等。

3.4.3 安全态势感知与预警

结合实时监测体系收集的大量数据，构建安全态势感知平台，对人工智能系统的安全态势进行实时分析和预测。采用数据挖掘、机器学习等技术，从海量的监测数据中提取有价值的信息，识别潜在的安全威胁和风险趋势。分析网络数据流量的异常变化、系统性能指标的波动等信息，预测潜在的安全事件，如大规模的 DDoS 攻击或数据泄露事件，并提前发出预警。安全态势感知平台能够为安全管理人员提供全面的安全态势视图，帮助他们及时作出决策，采取有效的预防措施，降低安全事件的发生概率和影响程度。

结语

随着人工智能技术的持续演进，信息安全防护需不断创新。应加大跨学科研究投入，培育复合型人才，以攻克技术难关。同时，呼吁立法机构加速完善相关法律法规，监管部门强化监管力度，为人工智能信息安全保驾护航，确保其在各领域的安全应用与长远发展。

引用

[1] 黄健.人工智能时代下网络信息安全问题 and 防护策略[J].网络安全技术与应用, 2024(7):124-126.

[2] 黄杰,宁雪冰.人工智能时代下的企业信息安全防护[J].科教导刊-电子版(下旬),2019(5):285.

人工智能机器学习 行为情景下的合理使用制度因应

文 ◆ 江苏师范大学法学院 毛宇涵

引言

人工智能机器学习存在复制权侵权和演绎行为侵权的风险。传统的合理使用情形难以完全适用于人工智能的机器学习行为。数字时代应重新检视合理使用制度目的，不具有明确指向性、不与原数据使用目的完全相同的人工智能机器学习行为均属于合理使用范畴。对于人工智能机器学习行为情景下的合理使用制度，不宜通过修改著作权法规制，但可纳入人工智能法或数据法规制范畴。

1 问题的提出

人工智能发展需要大规模使用文字、图像作品，若涉侵权会严重威胁其生存发展基础，这种法律不确定性会给产业带来阻碍，故需审视著作权侵权风险并制定应对措施。人工智能生成物是机器学习产物，应重新审视著作权原理及条款以赋予其合理权利取得路径。面对技术创新，现有合理使用制度如何适应机器学习技术发展是现实问题。

2 人工智能机器学习行为侵权风险

人工智能在进行机器学习时需要大批量收集素材以供自身学习使用，这种技术被称为文本与数据挖掘（TDM）。欧盟《数字单一市场版权指令》认为，其是指任何旨在对数字格式的文本和数据进行分析的自动分析技术，以便生成包括但不限于模型、趋势、相关性等在内的信息。机器创作需要人类事先提供海量数据的“母乳”，而从事自主深度学习的主体是作为智能机器的“孩子”自己^[1]。在人工智能执行机器学习活动时，通常会涉及复制和类似演绎的行为，此类行为会引发侵权风险。

2.1 人工智能机器学习的复制权侵权风险

人工智能机器学习在输入阶段所进行的复制行为并不能归入传统复制行为的定义中，传统的复制权是将复制的终点放置在作品的最终形成上，即对作品的永久复制，却并没有区分“永久复制”与“附随性复制”。

附随性复制通常指的是在进行其他活动时，不可避免地产生的对作

品的临时性复制行为。这种复制并不是为了复制作品本身，而是作为技术过程中的一个必要步骤。具体到人工智能的机器学习行为中，无论是接收控制者所提供的“学习资料”后，还是自主从网络中寻找“学习资料”，人工智能都会对这些材料进行分析。这一过程包括根据学习目的寻找关键词，将有关资料临时储存，再对这些临时储存的资料进行进一步分析，最后输出结果。无论采用何种技术，都会对数据进行临时复制。然而，我国相关法律法规并未对“临时复制”的性质作出说明，这主要是因为禁止临时复制的症结在于终端用户的在线作品使用行为，而禁止终

【作者简介】毛宇涵（1998—），男，江苏徐州人，硕士研究生，研究方向：民商法学。

端用户进行非营业性的作品使用在实际操作中不具有可行性^[2]。

2.2 人工智能机器学习演绎行为的侵权判定

此处所指的演绎行为并非一项单独的行为，而是一种行为集合，其中包括翻译行为与改编行为等。人工智能无法直接理解原始素材，所以需要数据预处理，清洗并转换为模型可用的格式。这一过程涉及对目标文本的识别和转码，而转码行为是改变、编排目标对象的表达形式，从而形成新的研究样本^[3]。有学者认为，此种行为与著作权法规定的改编行为有一定同质性^[4]。从字面意义上理解，这种看法确实有一定道理，但我国著作权法所规定的改编行为最终要形成的是一种作品，而“转码”行为只是人工智能输出结果的一个中间过程，因此改编行为只具有行为上的相似性而不具有结果上的同质性。

此外，人工智能进行学习时所涉及的“改编行为”在机器学习的训练阶段进行，而我国著作权法所规定的改编行为与翻译行为都是将作品的产生作为拥有权利的起点，人工智能在训练阶段尚处于创作“作品”的状态，此时“作品”尚未出现，因此，从结果论的角度来看，对此时的“改编行为”或“翻译行为”并不需要负相应责任。

3 著作权合理使用制度在机器学习视角下的适用困境

合理使用制度是指在符合法律规定的条件下，未经著作权人许可，他人可以自由使用著作权人的作品。《中华人民共和国著作权法》第二十四条规定了合理

使用的情形，从字面意义上看，机器学习所适用的类型为个人学习和研究使用以及为科学研究供科研人员使用，但深入探究，机器学习与这两种合理使用情形并非完全吻合。

第一，为个人学习和研究使用的合理使用并不能够完全适用于人工智能的机器学习行为。随着硬件设施的快速进步，硬件的算力也在快速攀升，目前个人电脑已经可以承担起一般规模的机器学习项目，但这并不意味着为个人学习和研究使用的合理使用能够完全适用于人工智能的机器学习。因为人工智能机器学习的训练往往需要大量数据和计算资源，这些资源的获取和维护对于个人来说通常不切实际。此外，机器学习模型的开发和优化是一个持续的过程，需要团队合作和专业知识的积累，个人难以独立完成。

第二，当前为科学研究供科研人员使用的合理使用目的与人工智能的机器学习行为发展方向不符。该款的立法原意，实质上是通过限制著作权来实现公共利益。在此背景下，科研机构以及科研人员应限定为国家设立的教育、科研公共事业单位，如经主管部门批准设立的学校、全额财政拨款的国家科研机构等^[5]。因此，在现阶段人工智能技术主要由各科研机构以及大型科技公司共同推动发展的背景下，为科研工作提供的合理使用场景实际上并未满足人工智能发展的实际需求。此外，即使试图重新阐述该条款的立法初衷，该条款仍存在主体限制，仅适用于教学与科研人员。

4 数字时代合理使用制度的优化进路

4.1 对合理使用制度目的地再检视

数字时代的著作权合理使用制度重构需要平衡创作者的权益保护和公众的利益，同时考虑技术发展和社会实践的变化。从著作权角度看，合理使用制度更应考虑如何平衡权利人与社会公众的利益，以促进创新和技术进步，而不是损害权利人的利益以成就产业的快速发展。《中华人民共和国著作权法》第一条开宗明义指出本法促进科学文化事业的发展和繁荣。以公益性视角观之，著作权法赋予权利人垄断权只是手段，促进知识增值才是目的^[6]。著作权法的制定初衷，并非仅仅是为了给予权利人绝对的垄断地位，而是期望通过这种方式，激励权利人进行更多的知识创造和文化创新。这种知识增值不仅有助于提升整个社会的科学文化水平，还能够为经济发展和社会进步提供强大的动力支持。

4.2 我国合理使用制度的因应

不具有明确指向性的人工智能机器学习行为属于合理使用。输出结果中出现相似风格的语言或图像，并不一定能认为对训练材料的“抄袭”。具体来说，若出现完全相同的句子或图像，则可以认定为完全复制，构成侵权。若是特殊的表达性机器学习，其学习行为具有明确的指向性，目的也较为明确，应当认为构成侵权，不属于合理使用的范畴。而若是仅在风格、遣词造句、色彩使用以及画面布局等有相似之处，不宜武断认定为“抄袭”。人工智能的生成行为不宜简单视为“缝合”。人工智能具有“记忆”和“泛化”能力，能够模仿人类的基本记忆与创造能力。虽然人工智能的这些能力较为幼稚，但与人类的记忆与创造过程

相符。例如，人类阅读后会记住美好或有感触的语句，并会在写作中融入其风格。人工智能记忆能力强，能“过目不忘”，且可在不同提示词下输出不同风格语句。生成式人工智能需要大量长时间训练材料，若因会输出“相似”文字就认定侵权，有因噎废食之嫌，会影响行业发展。

不与原数据使用目的完全相同的人工智能的机器学习行为属于合理使用。一般来说，人工智能的机器学习行为并不一定是为了与原数据持有人在同一领域进行竞争。人工智能的机器学习需要海量数据，具有表达性的机器学习又可分为普通的表达性机器学习与特殊的表达性机器学习。特殊的表达型机器学习指机器学习旨在输出表达性内容，且用于算法训练的作品全部来自特定作者^[7]。对于特殊的表达性机器学习而言，所有的训练数据都来源于同一来源，具有较为明显的目的性，因此这类机器学习可以认为不属于合理使用。而对于普通的表达性机器学习，其训练所需的数据来源于不同领域的不同主体，因此生成的内容即使风格与某一原材料相似，也不能直接认为会与该原材料在同一领域发生冲突，不合理地损害著作权人的合法权益。

我国针对人工智能的发展和利用，出台了《生成式人工智能服务管理暂行办法》（以下简称《办法》）。《办法》要求人工智能机器学习行为所使用的数据来源应合法，对该规定应理解为“只要是通过合法途径从公开渠道获取的材料就认为合法，而不必要求事先获得著作权人的许可”。这一理解与《办法》的制定目的相吻合。但即便能够进行这样解读，《办法》依旧不属于《中华人民共和国著作权法》第二十四条所规定的行政法规，而只是部门规章。而《中华人民共和国著作权法》在2020年刚进行过修改，为保持法律的稳定性，不宜在短时间内再次进行修改。我国已在为人工智能法以及数据法的出台做准备，实践中也出台了《中华人民共和国数据安全法》等法律规章为人工智能法以及数据法的出台打下深厚基础。因此，既然可以认为不具有明确指向性、不与原数据使用目的完全相同的人工智能机器学习行为属于合理使用范畴，且不宜在《中华人民共和国著作权法》中进行规定，则应将这部分内容纳入人工智能法或数据法的规制范畴，并加快出台相关法律的步伐。

结语

在当前的法律框架下，对于人工智能机器学习行为的侵权风险，需要结合具体情况进行细致分析。不仅不能忽视人工智能在创作过程中会产生的创新价值，还必须保护原著作权人的合法权益。合理使用制度的适用困境要求对现行法律进行深入检视。在数字时代，合理使用制度的优化路径应当考虑技术发展的新特点以及人工智能在创作和学习过程中所展现的独特性。通过立法和司法实践的不断探索，有望找到平衡著作权保护与技术进步的合理路径。最终，随着人工智能法和数据法的逐步

完善，以期能够为人工智能的健康发展提供更加明确和有力的法律支持。^[8]

引用

[1] 吴汉东.人工智能生成作品的著作权法之问[J].中外法学,2020,32(3): 653-673.

[2] 张建华.《信息网络传播权保护条例释义》[M].北京:中国法制出版社,2006:107-108.

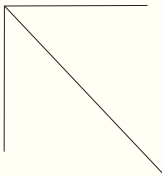
[3] 董凡,关永红.论文本与数字挖掘技术应用的版权例外规则构建[J].河北法学,2019,37(9):148-160.

[4] 吴高,黄晓斌.人工智能时代文本与数据挖掘合理使用规则设计研究[J].图书情报工作,2021,65(22):3-13.

[5] 李明德,管育鹰,唐广良.《〈著作权法〉专家建议稿说明》[M].北京:法律出版社,2012:251-252.

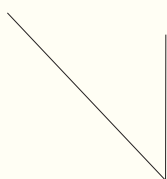
[6] 周文康,费艳颖.生成式人工智能创作使用作品的合理使用调适[J].科技与法律(中英文),2024(3):77-87.

[7] 李安.机器学习作品的著作权法分析——非作品性使用、合理使用与侵权使用[J].电子知识产权,2020 (6):60-70.



新质生产力背景下的 大模型与数据要素 在政务服务问答图谱中的协同作用研究

文 ◆ 中电科大数据研究院 杨迪丹



引言

在数字化国家建设的新动力不断推进下，政府服务的信息化转型已成为推动国家治理体系现代化的关键。依据《数字化国家建设的全面规划》，一个高效协作的数字政务发展方案已清晰勾画。不仅扩展了数字政府概念，还成为提升治理能力的核心工具。数字化政务在技术应用、流程改善以及制度创新方面面临迫切变革需求。为此，需以创新制度为引领，借助数字思维推动党政机关的数字化转型，促进跨部门合作和数据共享，构建可持续治理循环体系。数字政务问答图谱的构建对于满足企业与民众的需求至关重要。通过大模型与数据要素的深度协作，可显著提高

问答图谱在智能化、精细化以及个性化服务中的应用效率^[1]。在此背景下，本文将聚焦四大关键技术，即基于增量索引技术的 Lucene 索引器、基于知识图谱的深度学习排序模型、基于关键词的知识图谱语义搜索方法和基于表示学习的知识图谱语义搜索，探讨其在政务服务问答系统中的应用潜力和协同机制，挖掘数字化创新的实际价值，以期为未来政务服务的发展提供科学性、实用性并兼具前瞻性的思路。

1 大模型与数据要素的交融共振之必然

1.1 满足高效智能化的政务需求

在新质生产力背景下，政务服务问答系统必须快速满足用户需求，实现信息检索和处理的智能化与精确性。统计显示，在传统系统中，未结合大模型和数据要素时，用户平均响应等待时间为 5 ~ 10s，信息检索准确性约为 70%，用户满意度得分为 3.8（基于 5 分制）。大模型和数据要素的结合有效弥补了传统系统在处理复杂政务内容中的不足^[2]。大模型在语言理解和推理方面表现出色，能处理含糊表述和复杂意义，为政务咨询奠定智能化基础^[3]。数据要素支撑，如结构化的知识图谱和多维度数据标注，使系统在解答过程中捕捉潜在需求，形成多层次问答体系，进一步提高信息的准确性和权威性。在协同技术下，系统响应时间缩短至 2s 以内，检索准确率提高至 90%，满意度提升至 4.5。这种整合不仅提升了用户体验，还增强了问答系统的应用性和可扩展性，确保政务服务达成“智慧化、便捷化”目标，打造出可持续优化的信息服务生态。

1.2 实现资源优化配置与信息共享的精准应用

在多元化管理需求下，政府服务亟须构建跨部门的数据共享和资源分配体系，凸显了大模型与数据要素协同作用的优势。协同合作促进了数据共享和资源优化配置，使大模型能根据实时数据调整服务策略。这样的问答图谱不仅具备回答问题的功能，还可进行预测和分析。在知识图谱中，对数据资源进行系统化整合，保障政务信息在多个维度上应用，为跨领域的信息共享提供支持^[4]。在实际操作中，通过融合深度学习的排序模型和知识图谱，实现了对经济、民生、司法等领域数据变动

【作者简介】杨迪丹（1994—），女，四川内江人，硕士，工程师，研究方向：计算机科学与技术。

的实时监控，及时向用户提供最新资讯。大型模型在多元数据输入下展现出卓越的计算能力，使资源得以高效整合，显著提升政务服务的响应速度和处理能力。

2 四大技术驱动下的政务服务问答图谱创新实践

2.1 增量索引技术下的 Lucene 索引器：提升数据更新效率与检索速度

在政务服务问答图谱中，快速数据更新与精准检索是核心需求。利用增量索引技术，Lucene 索引器只对新增数据部分更新索引，避免全量索引带来的资源浪费，使系统快速响应数据更新请求。数据表明，在实施增量索引技术后，系统的索引更新速度实现了约 50% 的提升。同时，平均检索响应时间被有效压缩至 1s 以下。针对多源政务数据，Lucene 索引器采用增量索引技术实现跨部门、跨层级数据的即时处理。这一技术能迅速生成新索引，缩短检索响应时间。在政策法规频繁变动的情况下，增量索引保障用户查询能够获取到实时、精确的信息，避免因数据更新滞后而导致决策失误。在实际运用中，该技术显著提高了搜索的速度与精确性，并且改善了系统资源的利用效率，从而实现了政府数据的持续、高效动态管理，为智能化政务提供了坚实的技术支持。

2.2 基于知识图谱的深度学习排序模型：实现多层次智能排序与推荐

面对多样化的用户需求，基于知识图谱的深度学习排序模型将信息相关性与用户潜在需求智能结合，提供精细化服务。数据显示，当该模型被实施后，查询结果的点击率有所提高，大约增加了 40%，同时用户满意度的评分也上升了约 30%。政务信息经知识图谱语义结构化处理，深度学习排序模型则依据用户查询历史和偏好等特征，优先展示最相关的信息。例如，当用户查询“创业补贴政策”时，排序算法会呈现最新政策、热门分析以及常见问题解答。该模型不仅能够准确识别用户需求，还能把握需求优先级，确保服务高度吻合用户需求。通过该技术，政务服务逐步实现个性化和高效的智能服务模式，增强了用户体验的便捷性和满意度。

2.3 基于关键词的知识图谱语义搜索方法：提升语义识别能力，深化信息检索层次

传统的关键词匹配难以应对多层次、复杂的政务信息查询需求。基于关键词的知识图谱语义搜索方法则能弥补这一不足，通过对关键词进行语义扩展，实现了对查询意图的深度挖掘。知识图谱在这一过程中发挥了关键作用，其使系统能够将词汇意义与语境联系，实现上下文推理。例如，当用户查询“落户政策”时，系统不仅能够搜索相关政策，还能动态呈现与“人才引进”“户籍变更”等相关内容，提升信息全面性。此技术在复杂查询场景下表现优异，使用户即使不详细描述，也能获得所需信息，因此提升了检索的准确性和效率，为数字政务服务体系构建提供语义理解的基础。

2.4 基于表示学习的知识图谱语义搜索：突破信息孤岛，实现跨部门数据整合

表示学习技术将知识图谱中的政务实体和关系转化为低维向量，实

现跨部门数据资源的智能融合。应用表示学习后，部门间数据互调频率增加约 45%，查询速度提升约 60%。表示学习驱动的知识图谱在语义搜索领域表现出数据映射与关系挖掘的优势，使问答系统在数据领域之间实现流畅互联互通，消除信息孤岛。例如，当企业查询“社保缴纳情况”时，表示学习模型可将社保部门、税务系统和企业注册等多数据源内容整合展示，提供统一查询结果。该技术推动智能政务从单一职能向跨职能领域延展，实现“信息一体化”在政务服务问答图谱中的有效落实。

3 协同共振的机制探索与实现路径

3.1 构建跨层级数据共享机制：打通信息壁垒，实现数据全链条管理

政务服务问答图谱的构建依赖于大模型与数据要素的有效协作。为了实现这一目标，首先需要建立健全的跨层级数据共享体系。通过实施统一的数据标准和协议，可解决部门间信息孤岛问题，实现全链条数据管理与调用。基于增量索引技术的 Lucene 索引器在该机制中发挥核心作用。通过动态增量更新，Lucene 索引器能快速捕获政策、法规等数据变动，提供实时信息检索，避免信息滞后。该共享机制要求政务数据从“部门所有”向“共享共治”转变，在遵循数据安全和隐私合规的前提下，建立统一的数据管理和分级分类框架，促进多源数据融合。此外，知识图谱深度学习排序模型在此机制中以语义智能筛选和匹配高关联信息，实现跨部门信息的联动推

送，为用户提供更全面、准确的信息。通过这一机制，不同层级的政务部门高效协同，充分利用大模型和数据要素协同带来的优势，使信息透明化、可得化，提升服务效能和用户体验。

3.2 打造基于语义搜索的智能决策支持路径：增强信息检索精准度与决策辅助能力

构建政务服务问答图谱的目的不仅在于提供信息查询功能，还是实现信息检索与智能化决策支持的循环。基于关键词的知识图谱语义搜索方法和基于表示学习的知识图谱语义搜索在此路径中形成了有力的技术支撑。知识图谱语义搜索方法可将用户输入的关键词进行语义扩展，提升信息匹配精准度。表示学习技术则在此基础上通过向量化数据表征，关联不同数据源内容，便于跨领域信息的关联分析。例如，当用户查询“医疗补贴申请条件”时，语义搜索技术不仅能够检索到直接相关信息，还能关联展示相关申请渠道、时间要求等。进一步地，表示学习技术为决策支持提供强大数据基础，通过构建各类主题信息库和跨部门数据资源池，系统可快速响应、深度分析，支持科学决策，满足政务治

理的复杂性需求。在智能化决策支持路径的加持下，政务服务系统不仅能够高效解答用户问题，还具备预测和引导能力，有力推动政务服务的精细化管理和科学化决策。

4 政务服务智能化的未来图景与展望

4.1 构建个性化服务生态：从“标准化”到“精准化”服务升级

未来，政府服务的智能化将超越仅提供规范化服务的范畴，依托大模型和数据要素的共同协作，达成定制化服务的目标。此外，深度学习排序模型，依托于知识图谱，扮演着至关重要的角色。该模型通过剖析用户行为和历史数据，能够精确预测用户需求，进而提供贴合个人需求的服务。大模型和知识图谱的协同作用，使政务服务不仅能解答用户问题，还可主动提供高匹配度的个性化内容，为用户创造“千人千面”的政务服务新生态。

4.2 构建智慧治理体系：数据驱动的预测与辅助决策

随着增量索引技术和表示学习的持续进步，政务服务将逐渐向智慧治理体系转型。实时更新和部门间共享的政务数据，使系统能够运用关键词和语义搜索技术来监控、分析以及预测社会经济信息，从而为政府决策提供支持。政府通过建立一个多层次、多主题的政务信息库，可以实现对社会变迁的敏捷反应，这一切都得益于数据驱动。深度学习模型与大数据分析相结合，使系统能够实时掌握民生、经济等各方面的数据走向，生成预警报告或辅助建议，为治理能力现代化奠定坚实基础。

结语

通过大模型和数据要素的协同创新，政务服务问答图谱实现了从传统信息检索到智能化、个性化服务的转变，充分展示了新型生产力在数字政务领域的深入应用。政务问答系统借助增量索引技术、深度学习对知识图谱的排序、关键词的语义搜索以及表示学习，不仅实现了数据更新的高效率和信息精确性的提升，还满足了在多种层次和场景下的服务需求。这样的协同机制为政务治理和决策提供了切实可行的支持路径，使智能化问答图谱成为数字政务高质量发展的核心力量。这一体系将不断适应未来多元需求，推动政务服务朝着智慧治理和全面覆盖的方向进化，实现政府服务效能的全面提升。

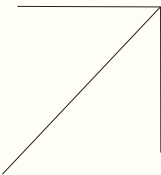
引用

[1] 汪波,牛朝文.从ChatGPT到GovGPT:生成式人工智能驱动的政务服务生态系统构建[J].电子政务,2023(9):25-38.

[2] 朱宗尧.政务图谱:框架逻辑及其理论阐释——基于上海“一网通办”的实践[J].电子政务,2021(4):40-50.

[3] 华斌,吴诺,李若瑄.基于知识图谱的电子政务项目评价方法研究与实践[J].情报理论与实践,2021,44(2):147-153+146.

[4] 王钦敏.全面建设数字政府统筹推进数字化发展[J].行政管理改革,2022(1):4-7.



人工智能生成内容可版权性路径探索

文◆贵州大学法学院 袁 宇

引言

生成式人工智能在文本、图像等创作领域的应用日益广泛，引发了关于版权适用的复杂讨论。现有法律框架以自然人创作假设为基础，对人工智能生成内容（Artificial Intelligence Generated Content, AIGC）的作者身份认定、独创性要求以及保护路径设计均提出了挑战。本研究旨在探讨如何通过“人机合作作品”的路径，克服 AIGC 作品在版权化过程中的障碍。本文假设，适度放宽对作者身份的限制，并从功能主义角度出发，更全面地认定人工智能在创作中的贡献，从而为其作品的版权归属和保护提供可行的法律路径。通过这一研究，以期 AIGC 作品的版权化提出前瞻性的建议，推动法律适应科技发展的步伐。

1 中美对 AIGC 作品的实践立场及评析

1.1 美国版权局的实践

美国版权法明确要求作品必须通过“登记—审核”进行注册，且必须由人类创作才能获得版权保护。这一原则在《美国版权法》第一百零

二条第 1 款中体现为“版权保护适用于由一名或多名作者创作的原创作品。”同时，美国版权局在 2022 年发布的《版权注册实践：作者和作品的识别》中明确指出“版权法保护的作品必须是由人类作者创作的，纯粹由机器或机械过程生成的作品不符合这一要求。”基于上述标准，美国版权局拒绝了数次人工智能生成内容的版权登记申请，其中较为有代表性的有以下 3 个案件。

（1）“太空歌剧院”（Théâtre D'opéra Spatial）版权申请登记案。Stephen Thaler 申请为其 AI 生成的作品《A Recent Entrance to Paradise》登记版权，但因作品缺乏人类创作，版权局驳回申请。尽管 Thaler 声称其在人机协作中做出了创造性选择，版权局依然认为该作品的主要创作来自 Midjourney AI，而非人类。

（2）“黎明的扎利亚”（Zarya of the Dawn）案。该案中，Kashtanova 的漫画《黎明的曙光》最初获得版权，但因图像部分为 AI 生成，版权局随后撤销版权，认为缺乏必要的人类创作。

（3）“离天堂最近的入口”（A Recent Entrance to Paradise）案。



【作者简介】袁宇（1995—），男，贵州贵阳人，硕士，研究方向：知识产权。

美国版权局审查委员会认为作品“必须含有人类创造性要素”而非仅由申请人“指挥”人工智能创作，“人类的创造力是作品的必要组成部分”。

1.2 中国法院的实践

在中国版权自动取得的规则下，法院承担起了处理著作权纠纷的重任。而在人机协作逐渐占据主流的时代，我国法院很好地通过释法解决了许多难题。

（1）菲林诉百度案。法院认为，“自然人创作完成仍应是著作权法上作品的必要条件……即使威科先行库‘创作’的分析报告具有独创性，该分析报告仍不是著作权法意义上的作品，依然不能认定威科先行库是作者并享有著作权法规定的相关权利。^[1]”

（2）“春风送来了温柔”案。法院坚持著作权法仅保护“自然人的创作”，认为人工智能模型不具备自由意志，无法成为法律上的“作者”。此外，基于诚实信用原则和公众知情权，相关主体应标明所使用的人工智能技术或模型^[2]。本案不同于前案之处在于，涉案人工智能模型更具“智能”，且原告智力投入更多，因此具备进一步适用著作权法保护的基础。本案判决延续了前案的主客体二分原则，不承认人工智能的著作权主体资格，但认可其生成内容具备作品外观，可构成智力成果。

1.3 综合评析

中美在 AIGC 作品确权上的差异反映了两国在法律基础和政策理念上的不同。美国版权局坚持“人类作者”要求，严格限制 AI 生成内容的独立版权资格，仅认可“人类创作”作品，从而维持传统版权框架，但使部分

具有创意的 AI 生成内容无法获得法律支持，不利于 AIGC 的长期发展。相比之下，中国采取“工具论”赋予 AI 用户创作主体地位，将 AIGC 的独创性归于自然人，为 AIGC 确权提供了较宽松的法律依据。然而，随着 AI 在复杂人机协作中展现出超越工具属性的自主性，“工具论”面临适用困境。

因此，中美现行实践均未有效应对 AIGC 作品在版权保护中的复杂性，尤其在作者身份和独创性认定上，现有版权框架的局限性明显。本文将从作者身份与独创性认定等角度，探讨 AIGC 版权化的具体挑战，为路径探索提供理论与实践支持。

2 人工智能生成内容版权化困境：作者身份与独创性之障

根据功能主义贡献论，当人工智能对生成内容的“独创性表达”作出主要贡献，而人类仅对其思想或惯常性表达作出贡献时，现行著作权法对其的保护将会遇到瓶颈^[3]。主要体现在两个方面，一是随着人机协作时代的到来，著作权法在作者身份认定上面临障碍；二是独创性认定上也存在相应的问题。

2.1 生成式人工智能的作者身份认定障碍

根据美国版权局的观点，作者身份的认定不仅以创作行为为基础，还依赖于自然人的格要素。因此，人工智能因缺乏独立的人格和意志，无法成为法律意义上的作者，更不能成为享有著作权的主体。这种“自然人作者观”在涉及单位作品的立法中有一定程度的调整。尽管单位本身无法进行创作活动，但为了确定著作权的归属，法律仍然将单位视为作者。表面上看，这似乎突破了传统自然人作者的观念，但实际上，单位仍是自然人的集合，其意志来源于集体，可以行使权利和承担责任。然而，AIGC 作者身份尚未得到法律确认，且其与著作权人的身份存在高度一致性，人工智能无法行使权利，更无法承担侵权责任，因此不可能成为权利主体。在这种情况下，作者身份的认定变得无从谈起，导致其生成的内容被视为缺乏作者的“无主作品”，在侵权责任的认定以及权利保护机制的构建上将面临难以克服的法律障碍。因此，AIGC 作者身份认定的最大障碍源自其行为能力的缺失，这直接影响了其权利行使的可能性，从而使有关人工智能生成内容可版权性的问题在权利主体层面上难以进一步探讨。

2.2 人工智能生成内容独创性认定障碍

首先，在以作者为中心的著作权理论中，作者的人格表达被视为创作行为的核心意义。因此，作品的独创性寄托于作者的独立创作行为中。由于人工智能生成内容并非人类的智力成果，其独创性不可能脱离作者身份而进行讨论。传统的独创性标准强调创作的“独立性”和人类的“智力活动成果”，然而，人工智能生成过程主要依赖于算法驱动和数据训练，并不具备真正的创作意图。其生成内容只是基于训练模型和算法规则的自动化输出，缺乏人类创作所需的独立意志与思想表达。即使是在“创作”过程中，人工智能的贡献无法被忽视，其运算过程本质上是对已有数据的排列组合，缺乏真正的创造性决策。因此，这类生成内容不应被视为具有法律意义上的独创性。总之，人工智能的作者身份与

权利主体认定均面临障碍，单独讨论人工智能生成内容的独创性并不符合著作权法的立法目的，其可版权性亦难以进一步讨论。

其次，实践中的观点与前述一致。美国版权局否认未有充分人类参与的 AI 生成内容的独创性，中国法院则在将 AI 视为工具时才承认其独创性。现有法律框架缺乏针对人工智能生成内容独创性的明确标准。同时，著作权法旨在保护人类劳动与智力成果，但 AIGC 作品不具备“人类劳动”的概念，赋予其版权不但无法激励创作，反而会削弱对人类创作的保护。

3 人工智能生成内容版权化的法律路径探索

3.1 合作作品路径：人工智能作者身份认定的可能方案

为解决生成式人工智能的作者身份认定障碍，调整现有的“作者—著作权人”路径，将人工智能拟制为与自然人合作的“事实作者”。根据现行法律，合作作品指两人或两人以上共同创作且各自作出相应贡献的作品。在人机协作的情境中，合作作品即自然人作者与机器作者的共创作品。尽管人工智能生成内容在一定程度上可视为合作创作，但版权归属依然在人类创作者手中。这种处理方式既维护了传统版权法的核心原则，又适应了技术发展的新趋势，避免版权保护机制因技术进步而陷入困境。

3.1.1 人机合作作者的理论基础

人工智能生成内容版权化的首要难题在于主体确定。传统的“作者—作品”理论范式无法将作者身份与权利主体完全分离，但在结构主义理论的影响下，作者身份与著作权人之间并非绝对对应关系。我国著作权法中已存在职务作品、委托作品、视听作品等作者与权利主体不完全重合的情形。基于上述制度设计，结合当前人机合作中人工智能逐渐主导创作的发展趋势，解除作者身份与自然人的绑定成为现实要求。在可以预见的后人类时代，人在与非人、人机合体之人、法人等的竞争之中，会作为一种弱者出现^[4]。但应当认清，在人工智能深度参与的创作活动中，作者身份与著作权相分离的构想并非要推翻以人为本的人本主义思想，而是对人机协作实然状态的描述。

从法律拟制的法理学角度来看，法人以及非法人组织之所以能够成为权利主体，是因为从“个人”到“类人”的行为抽象是基于对“个人行为”的经验判断归纳而来的“类人”一般行为模型的概然性推断^[5]。而人工智能的“类人化”程度发展超出了预期，为其拟制为主体提供了理论基础。然而，考虑其在权责统一上的现实障碍，建议将其仅拟制为合作作者，而不作为著作权人。

3.1.2 人机合作作者的制度设计

在著作权法中增设人机合作作品条款。首先，条款需明确自然人在合作作品中的主导地位，即便人工智能在创作中的贡献增加，仍须确保人类因素作为作品构成中的必要成分。人机合作作品应当作为一种特殊的合作作品类型，其版权保护的前提条件是自然人始终作为权利主体之一。其次，条款应对人工智能的拟制身份进行规定，即在赋予人工智能“作者”身份的同时，明确其不得作为权利主体，这是对智能创作事实

的一种法律确认^[6]。最后，在权属分配上，除应保障自然人创作者权利之外，可以由实际创作的自然人与“投资者”（技术公司）通过协商一致，共同享有并行使著作权，承认人工智能技术公司拥有著作权，其所产生的激励作用，不仅体现在激励人工智能技术公司进一步优化算法、提升人工智能软件的效能方面，还体现在激励人工智能技术公司积极解决数据素材的版权问题、使用正版内容数据、支付版权费用、保护数据内容原创作者的权利方面^[7]。

3.2 基于读者中心论的人工智能生成内容独创性障碍解决路径

3.2.1 从“作者中心”到“读者中心”：AIGC 作品独创性认定的理论变革

AIGC 作品版权化过程中独创性的障碍源于以作者为中心的理论范式。然而，随着结构主义的兴起，作者中心主义逐渐被消解，读者中心主义逐步进入学者的视野。读者中心主义强调作者的思想是否实际传达给读者具有不确定性，读者会根据自身理解对作者的思想作出假设。除非作者本人明确表达，否则“作者的思想”实际上是读者基于作品文本自身的结构和符号系统的推测，最终作品的意义可以脱离具体作者，由读者即社会公众所赋予。在此背景下，作品的独创性与作者的人格表达相分离，更关注作品本身的创造性，使获得公众认可的生成内容均列入著作权法保护范围，达到激励创作的法律目的。

此外，在人工智能生成内容中，既应反映读者中心主义在其版权化中起到的决定性作用，又不能一味斩断作者与作品的全

部联系。完全由用户评价决定 AIGC 的独创性并不妥当，必须体现自然人创作者对该内容的核心地位和实质贡献。如果对人的核心地位采取否定和置疑的立场，那么著作权法的价值追求将面临冲击，人工智能的发展也会背离“以人为本”的宗旨^[8]。人机合作作品是自然人和人工智能共同创作且自然人在创作中作出实质性贡献的作品。“实质性贡献”应为自然人在创作过程中，通过其独立的智力活动和创作意图，对作品内容、形式所作出的决定性投入，确保生成的内容具备其独特的个性化特征。在独创性认定的标准中，应摒弃对于作者思维、身份重度依赖的桎梏，从而解决独创性标准与人类主体创作过程高度绑定的障碍。

3.2.2 明确自然人“实质性贡献”的制度设计与操作标准

为保障人机合作作品的独创性认定符合现有法律框架的要求，必须在制度设计中建立清晰、可操作的“实质性贡献”标准，以确保自然人对 AIGC 的核心贡献得到认定。自然人在创作过程中的“实质性贡献”应体现在对作品主题、结构、核心元素等方面具有关键性和决定性选择的能力，并应通过列举加兜底条款的

方式具体化。不仅能够保障在不同类型作品中的适用性，还可以使各类创作行为所需的自然人贡献有明确的规范依据。

首先，传统著作权法中的独创性标准建立在人的智力成果基础之上，旨在鼓励和保护人类的创作行为。因此，若生成内容中未体现自然人的创造性判断，则难以满足独创性认定标准。以自然人的智力投入为前提，“实质性贡献”标准将自然人创作中的核心要素——独立意志、审美判断以及价值取舍等作为必要条件，从而确保 AIGC 符合著作权法的独创性要件。

其次，通过列举法设计条文对“实质性贡献”进行细化，明确自然人对内容主题、表现形式的决定性贡献，如用户对内容主题、构图方式、风格等选择，体现人类的实质介入。此外，兜底条款涵盖新兴创作形态，为“实质性贡献”提供灵活适用的标准，确保条文在实践中的适用性与开放性。

最后，制度设计不仅是理论层面的建构，还是实践中的操作指引。将“实质性贡献”标准具体化为自然人在创作中的决策控制权、对内容要素的选择性贡献以及操作的主导性等标准，不仅为实践中区分自然人贡献与 AIGC 提供了重要依据，还明确了自然人在生成过程中的主导作用。

结语

本文对中美在人工智能生成内容著作权保护问题上的不同实践路径进行了对比分析，揭示了现行法律框架下人工智能生成内容版权化的诸多障碍。通过分析美国版权局对人机协作的否定与中国法院“工具论”在权利归属上的实践差异发现，传统的“自然人作者观”与“工具论”在人工智能深度参与创作时已显局限。为应对未来创作格局中的技术与法律挑战，本文从合作作品路径与读者中心论视角出发，提出了将人工智能拟制为合作作者，并重视其在作品中的实质性贡献等新思路，为人工智能生成内容的版权化路径提供新的理论依据。

引用

[1] 朱阁.“AI文生图”的法律属性与权利归属研究[J].知识产权,2024(1):24-35.

[2] 郑海味,张伟君.人工智能生成图片中用户的独创性贡献——以“AI文生图”著作权案判决为例[J].中国出版,2024(12):52-57.

[3] 丁文杰.通用人工智能视野下著作权法的逻辑回归——从“工具论”到“贡献论”[J].东方法学,2023(5):94-105.

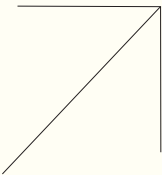
[4] 於兴中.后人类时代的社会理论与科技乌托邦[J].探索与争鸣,2018(4):18-23+28+141.

[5] 俎璐.人工智能法律拟制主体地位再探——面向拟制哲学视角下的法律主体制度[J].北京理工大学学报(社会科学版),2024,26(4):152-163.

[6] 吴汉东.论人工智能生成内容的可版权性:实务、法理与制度[J].中国法律评论,2024(3):113-129.

[7] 徐小奔.论算法创作物的可版权性与著作权归属[J].东方法学,2021(3):41-55.

[8] 王国柱.人工智能生成物可版权性判定中的人本逻辑[J].华东师范大学学报(哲学社会科学版),2023(1):133-142+205.



实践探索

Practical Exploration

近年来，我国信息化事业不断发展，在“全面提高信息化水平，推动信息化和工业化深度融合，加快经济社会各领域信息化”等战略方针的指引下，做出了大量的实践与探索，延伸到了社会、经济、政治、文化、军事等各个领域。移动互联网、云计算、大数据等技术的不断发展和普及，为信息化实践的推进提供了有力支持。此外，智慧城市与数字强国的建设需求也推动了信息化的探索进程，符合时代的要求与趋势。

信息化对经济发展的作用一直是较为重要的课题，在电子政务、电子商务、企业数字化转型、大数据分析应用等各个领域均取得了重大成果。同时，信息化实践探索的工作一直秉承着突破性与创新性齐头并进的态势向前发展。未来将继续以信息化实践与探索为基石，不断推动国民经济和社会信息化事业发展，加快释放信息化发展的巨大潜能，以信息化驱动现代化，全面建成社会主义现代化强国。

计算机软件 Java 编程特点 与技术应用分析

文 ◆ 广州商学院 陈敬宗

引言

为了确保网络环境的稳健安全，优化软件性能及其运行稳定性至关重要。Java 编程语言因其出色的安全性和稳定性特征，已成为程序员们的首选工具。为了全面发挥 Java 编程语言的潜力，编程人员需深入把握其独特属性。本文就计算机软件 Java 编程进行简单介绍，分析其特点，并就其技术应用进行探究。

1 计算机软件 Java 编程

Java 编程是软件开发界的佼佼者，自问世便以跨平台、高效能著称，引领编程技术新风尚。其不仅是一种语言，还是一个强大的技术生态系统，秉持“编写一次，处处运行”的原则，颠覆了传统编程的平台限制，大幅提升了开发效率与灵活性^[1]。

Java 的精髓在于其简洁性、面向对象特性、卓越的可移植性以及坚固的安全性和稳定性。其语法精炼，逻辑清晰，为开发者提供了友好的学习曲线；面向对象的设计理念让代码结构更加清晰，维护成本降低；Java 虚拟机

(JVM) 的引入，则确保了 Java 应用能在各类平台上流畅运行，真正实现了跨平台的梦想。同时，Java 内置的安全框架和自动内存管理机制，为应用的稳健运行筑起了坚实的防线。现阶段，Java 编程已深度渗透至企业级应用、移动开发、大数据处理、云计算等多个关键领域，成为驱动数字化转型、推动智能创新的核心力量^[2]。

2 计算机软件 Java 编程特点分析

在编程语言中，Java 以其独特的魅力和广泛的应用场景，成为软件开发领域的璀璨明星。Java 不仅继承了前辈语言的优秀基因，还在简单性、面向对象性、可移植性、安全性与稳定性等方面展现出了卓越的性能，为程序开发人员提供了强大的工具，推动了软件技术的不断进步^[3]。

2.1 简单性

对于大多数程序开发人员而言，学习编程往往从 C 语言开始。Java 与 C 语言在语言类型、编程规则与语法上的高度相似性，使初学者能够轻松上手，快速掌握编程的基本概念和技巧。Java 在继承 C 语言优点的同时，也对其进行了大胆的改进和优化，摒弃了 C 语言中烦琐、低频使用或难以理解的部分，如某些复杂的语法结构，降低了编程的门槛，提高了开发效率。

此外，Java 还引入了诸多实用功能，如引用功能、自动垃圾收集等，这些特性极大地简化了编程过程，减轻了开发者的负担。与 C++ 相比，Java 的语法更加简洁明了，逻辑更加清晰，使程序更易于阅读和维护^[4]。这种简单性不仅体现在语言本身，还体现在 Java 提供的丰富库和框架上，使开发者能够更快地构建出功能强大的应用程序。

2.2 面向对象性

Java 是一种典型的面向对象编程语言，其通过将现实世界中的事物抽象为对象，并通过类和接口来定义这些对象的属性和行为，从而实现了复杂系统的有效建模。Java 的面向对象特性不仅体现在其语法结构上，还体现在编程思想上。其鼓励开发者以对象为中心来思考问题，将

【作者简介】陈敬宗（1984—），男，畲族，广东河源人，本科，讲师，研究方向：计算机应用和数据科学与大数据技术。

问题分解为多个相互独立又相互关联的对象，通过对象之间的交互来实现系统的功能^[5]。

Java 的面向对象特性方面还体现在其强大的继承机制上。通过继承，开发者可以创建出具有共同属性和行为的“类”，从而避免了代码的重复和冗余。同时，Java 还支持接口的多重继承，使“类”可以灵活地实现多个接口的功能，进一步增强代码的复用性和可扩展性。这种面向对象的设计方法不仅提高了代码的可读性和可维护性，还使开发者更容易地理解和修改系统。

2.3 可移植性

Java 的可移植性是其最引人注目的特性。Java 程序可以在任何支持 Java 虚拟机的平台上运行，无需对源代码进行任何修改。这一特性得益于 Java 语言的中立性设计和 Java 虚拟机的强大功能。Java 详细规定了各种基础数据类型的长度和行为，确保了程序在不同平台上的一致性^[6]。

Java 的可移植性不仅体现在跨平台运行上，还体现在其丰富的库和框架上。这些库和框架提供了大量的通用功能和工具，使开发者能够快速构建出适用于不同平台和环境的应用程序。此外，Java 还支持 Web 程序的开发，使构建出的 Web 应用能够在不同的浏览器和服务器的上运行，无需进行额外的适配和修改。

2.4 安全性与稳定性

在互联网时代，安全性和稳定性成为软件开发的首要考虑因素。Java 编程语言在安全性方面做了大量的工作，以确保程序在复杂的网络环境中能够安全、稳定地运行。Java 提供了多种安全机制，如访问控制、加密技术、异常处理等，这些机制共同构成了 Java 程序的安全防线^[7]。

其中，加密技术是 Java 安全性的重要组成部分。Java 通过密钥技术对相关编程语言进行加密处理，只有持正确密钥的用户才能解密和访问程序。这种加密机制有效地防止了网络木马病毒对程序的破坏和非法访问。同时，Java 还能够处理各种突发状况，如当检测到计算机环境发生变化时，自动断开与互联网的连接或终止网络数据的传输，从而保护计算机上的信息不被非法窃取或篡改。除了安全性外，Java 还以其卓越的稳定性著称。Java 虚拟机（JVM）作为 Java 程序的运行环境，具有强大的错误处理和资源管理能力，能够自动管理内存的分配和回收，避免内存泄漏和内存溢出等问题的发生。同时，JVM 还提供了丰富的调试和诊断工具，使开发者能够快速定位和修复程序中的错误。此外，Java 还重视与操作系统的协同工作。通过与操作系统的紧密集成，实现了对系统资源的有效管理和利用。这种协同工作机制不仅提高了程序的运行效率，还增强了程序的稳定性和可靠性。

3 计算机软件 Java 编程技术应用

3.1 在企业信息化发展中的应用

在数字化转型大潮中，Java 编程语言以其独特的优势，成为企业和行业信息化发展的重要推手。众多企业纷纷采用 Java 技术模型构建应用软件和服务器，不仅提高了软件的开发效率，还降低了维护成本，增强了系统的兼容性和可扩展性。Java 的跨平台特性，使企业能够轻松实现跨

地域、跨系统的业务整合，促进了信息的流通和共享，加速了企业信息化的进程。

在教育领域，Java 编程语言与计算机专业的深度融合，催生了一系列具有实用价值的软件平台和教学工具。以清华大学为例，该校计算机专业结合 Java 编程语言和 Web 技术，研发了多个软件平台，不仅为师生提供了便捷的教学和学习环境，还被众多大型企业采用，推动了产学研的深度融合，促进了科技成果的转化和应用。

3.2 在嵌入式设备中的应用

在当今科技日新月异的时代，嵌入式系统作为计算机技术的重要分支，已经渗透到生活的方方面面，成为现代电子设备不可或缺的一部分。从智能家居到工业控制，从医疗设备到汽车电子，嵌入式系统的身影无处不在。我国作为全球最大的电子产品生产基地，计算机装机中嵌入式系统的应用更是普及且深入，其强大的实用性和广泛的应用范围，使嵌入式技术成为推动信息化、智能化进程的关键力量。

嵌入式系统的核心在于其可定制性和高效性。技术人员通过剪裁法，根据特定应用需求对嵌入式设备的软件和硬件进行二次加工，这种灵活性不仅满足了不同设备对资源消耗的差异化需求，还极大地提升了设备的性能表现^[8]。嵌入式设备以其高工作效率和快速响应能力，在接收到信号后能迅速完成指定任务，确保了系统的实时性和可靠性。然而，嵌入式系统的使用寿命受限于其硬件特性和软件更新速度，如何延长系统寿命、提高系统效率成为亟待解决的问题。

Java 编程语言的引入为嵌入式系统带来了新的生机。Java 以其平台无关性、跨平台能力、丰富的 API 集以及强大的异常处理能力，成为优化嵌入式系统性能、提升任务执行效率的理想选择。通过 Java 编程，嵌入式系统能够更加高效地响应信号，精确执行各项任务指标，不仅提高了系统运行效率，还增强了系统的可扩展性和可维护性。此外，Java 的垃圾回收机制有效管理了内存资源，减少了内存泄漏的风险，进一步延长了嵌入式系统的使用寿命。

3.3 在无线 Java 与移动设备中的应用

随着移动互联网的飞速发展，移动设备已成为人们日常生活中不可或缺的一部分。Java 编程语言作为移动互联网时代的基石，其重要性不言而喻。所有的移动设备都支持 Java 编程语言，不仅是因为 Java 提供了强大的编程框架和丰富的库函数，还在于其持续的创新和改进，使 Java 在宽带、速度、稳定性等方面不断突破，为用户带来更加流畅、高效的使用体验。

移动设备早期多采用封闭式操作系统，用户对于手机软件 and 应用程序的选择受限于生产厂家。而 Java 编程语言的广泛应用，打破了这一局限，使移动设备变得更加开放和灵活。通过 Java，开发者可以创建各种第三方应用，用户可以根据自己的需求自由选择安装，极大地丰富了移动设备的功能和应用场景。同时，Java 的安全机制也为移动设备的数据安全提供了有力保障。

为了推动 Java 在移动设备中的广泛应用，众多生产厂家纷纷加大投入，不仅在资金上给予支

持，还在技术上进行深入研究，推动了 Java 技术的不断进步。可以预见，随着 5G、物联网等新技术的兴起，Java 在移动设备领域的应用将更加广泛，为智能移动时代的到来奠定坚实基础。

3.4 在网络教学中的应用

随着互联网的普及和教育信息化的不断推进，网络教学已成为教育领域的一大亮点。Java 编程语言凭借其强大的跨平台性、丰富的 API 集以及高度的可扩展性，在网络教学系统的开发中大放异彩。编程人员巧妙运用 Java 技术，将网络教学系统与教学平台深度融合，不仅实现了教学资源的优化配置与高效共享，还极大地满足了学生日益多样化的学习需求。

目前，很多高校已经开发应用交互式电站仿真系统，这一创新成果充分展现了 Java 在教育领域的巨大潜力。该系统以 Java 编程语言为核心，通过高精度仿真技术，生动模拟了锅炉膛火和电站锅炉的复杂运行过程。学生们无需亲临现场，就能通过系统直观地了解电站的工作原理、操作流程以及故障处理等知识。更为难得的是，系统还支持模拟操作功能，学生们可以在虚拟环境中进行实践练习，不仅加深了对理论知识的理解，还极大地提高了实践能力和应急处理能力。总体来看，基于 Java 的网络仿真技术，极大地丰富了教学手段，还推动了教育模式的创新。打破了传统教学的时空限制，使学习变得更加灵活、便捷。此外，通过模拟真实场景，增强了学习的趣味性和互动性，激发了学生的学习兴趣 and 积极性。

结语

计算机软件 Java 编程在很多领域都有应用，其应用价值突出。本文对计算机软件 Java 编程的简单性、面向对象性、可移植性、安全性与稳定性进行分析，并就其具体应用进行探究，为深化技术应用和发展提供一些思路。

引用

[1] 徐海燕.JAVA编程在计算机应用软件中的应用特征与技术[J].电子技术与软件工程,2023(3):29-32.

[2] 王南.Java编程在计算机应用软件中的应用特征与技术研究[J].信息记录材料, 2022,23 (4):130-132.

[3] 田甜.计算机软件Java编程特点及其技术研究[J].无线互联科技,2022,19 (3):30-31.

[4] 郭阳,常英贤.浅谈Java语言在计算机软件开发中的应用[J].数字通信世界, 2022(1):88-90+94.

[5] 王可.计算机软件JAVA编程特点及其技术应用分析[J].电子世界,2021(18): 176-177.

[6] 赵子昂,黄钧露.JAVA编程在计算机应用软件中的应用特征与技术研究[J].电子测试,2021(18):83-84.

[7] 诸彩红.浅探Java编程语言在计算机软件开发与应用[J].电子世界,2021(12): 27-28.

[8] 丁琼.计算机软件开发Java编程语言及应用分析[J].长江信息通信,2021,34 (5):73-75.

风机塔筒平台盖板 自动开合技术的未来发展与挑战

文◆新疆能源（集团）哈密清洁能源有限责任公司 王东 杨志龙 黄超 马俊财

引言

作为可再生能源体系内的关键构成部分，风电在全球能源格局中的地位日益显著。确保风机的安全性和运维效率是维系风电稳定产出的核心要素。然而，传统依赖人工操作的风机塔筒平台盖板开闭方式，不但潜藏安全风险，而且工作效率低下，因此，研发自动化盖板开合技术成为该领域不可阻挡的发展趋向。

1 技术背景与应用需求

1.1 技术背景

在全球能源体系向可持续方向转型升级的宏观趋势下，风能作为清洁能源的关键支柱，其发展态势迅猛^[1]。这一进程加剧了对风力发电设施，特别是风机塔筒在安全性能与运维便捷性上的更高标准需求。在常规的风电场管理实践中，塔筒平台盖板的开启与闭合操作大多仍旧依赖人力实施。此传统模式不仅在作业效率上显得滞后，还在高海拔作业场景埋下了重大的安全风险，涵盖了作业人员遭遇的高空跌落危险以及在恶劣气候环境下的操控难度问题^[2]。

鉴于技术的不断进步与安全规范的提升，手动操作模式在应对当代风电场所追求的高效与安全双重要求上显得力不从心。因此，研发一项既能适应风电领域特有环境挑战，又能满足特定操作需求的自动化、智能化盖板开关技术，已成为该行业发展的必由之路。这项技术被期待能在如强风、低温等严苛气候环境下维持稳定作业，同时保证操作过程的极度安全以及高效性^[3]。

1.2 应用需求

传统的开启闭合手段在实际操作过程中显露出多方面的不便与安全风险。首先，该方式依赖人力施力，要求操作人员在高空环境中作业并投入体力，尤其在遭遇强风或不良天气条件时，提升了发生安全事故的风险。其次，从效率层面考量，手动操作效率低下，特别在面临紧急情况，急需封闭盖板以保护设备免受损害的时刻，其响应迟缓，难以适应紧急情况下的时效性要求。

自动化开合技术通过集成传感设备、控制单元和执行机制，能有效应对上述挑战。传感设备持续监测风速、温度等关键参数以及盖板的开启闭合状况，确保所有活动都在一个安全的环境设置下展开。控制单元依据传感设备反馈的信息，运用高级算法进行分析并发出指令，实现盖板开合的自动化调控。执行机制则承担着精准执行这些开合动作的任务，其设计需平衡力量输出与动作精密度，以保证操作的高效率与安全性。

另外，自动开合技术系统应集成远程监控与操控特性，使运维人员得以在控制室界面实现盖板开启与闭合状态的直接监管与控制，极大增强了作业的便捷度与安全性。此特性不仅缩减了现场人员直面恶劣环境的必要性，降低了安全事故发生的概率，还显著提升了对风电场的综合管理水平以及运维响应时效性^[4]。

2 技术优势分析

2.1 安全性提升

风机塔筒平台盖板的自动开启与闭合技术在增强安全性方面

【作者简介】王东（1987—），男，甘肃武威人，本科，工程师，研究方向：新能源运行与维护。

展现出了明显的优势。该技术通过融合高精度传感设备与智能化控制系统，达成了盖板开闭操作的自动化，大幅减少了风电场技术人员执行高空作业的频次。传感系统持续监控风机运行状况以及周遭环境参数，保证所有动作均在安全先决条件下自动实施。控制系统基于传感系统收集的信息，进行严密的数据分析与评估，从而制定出稳妥的操作策略，确保设备与人员的双重安全保障。

当传感器识别到强风或其他构成危险的天气状况时，系统将自行采取措施延缓或中止开启过程，以防止非妥当操作引起的意外事件。此智能化评判机制不仅有赖于实时数据的高速处理能力，还得益于前沿的预判算法，使系统能够预知风险并及时调整操作方案。另外，通过实施自动开关技术，大幅减少了人工直接干预的需求，从而在根本上减少了由人员操作差错或判断偏差引起的安全风险。融入自动化控制系统，不仅简化了操作步骤，缩减了人为干预的变量，还为风电场的安全管控水平带来了显著提升。

2.2 合规性保障

在设计与实施自动开合系统的过程中，应严守国家规定与行业准则，以保障设备操作的合法性和可靠性。这些规范全面涉及设备设计的初始阶段、生产制造、安装调试、功能验证以及后续运营维护等所有步骤，力保系统各组成单元均能满足相关法律条款和行业高标准。通过融合尖端的自动化控制技术，风电场运营者能确保所有作业流程精确符合环境保护、工业安全以及职业健康等法规导向。

在系统功能性层面，自动开合系统集成了一个高级的记录与报告功能模块，能够自动生成详尽的操作日志和维护报表，方便了合规审查过程。不仅强化了数据处理的高效性，还提升了数据的精确度与全面性，为审计阶段的追溯验证工作创造了有利条件。另外，自动化系统的普及应用大幅减少了人工介入的需求，减轻了因偏离操作规范而导致的合规风险敞口。

借助合规性管理与自动化技术的融合，风电场运营的合规性在多维度上得以增强。这种融合措施不仅保障了运营环节中所有操作的合法性与规范性，还大幅减少了法律和监管风险，从而巩固了企业声誉，提升了其在市场中的竞争力。

2.3 效率提升

自动开启与闭合技术的应用提高了风电场运维工作的效率，与以往的手动操控模式相比，不仅缩减了操作周期，还在面临突发状况时表现出更加快捷的响应能力。传统手动操控方式，由于其耗时较长且反应迟缓，往往会对风电场的整体运营效能以及电能产出造成不利后果。相反，自动开合系统凭借高级的控制算法与高效率的执行机制，对操作程序进行了优化，从而大幅减少了盖板开启与闭合过程所需时间。

当系统辨识到故障状态或面临亟须紧急干预的情景时，自动化启闭技术能即刻执行盖板的开启与闭合动作，确保设备得到及时维护，从而缩减由设备故障引发的停产时间。这一迅速反应机制保证了风电场供电的连续性，不受设备故障影响，进一步巩固了电网的稳定性和可靠性。

此外，自动化系统运用的效益显现减弱了对人工介入的依赖性，进而缩减了人力资源的成本消耗以及由人为失误引发的操作偏差。通过优化减少人为因素的干预，运维作业的总体效能与稳定性得到了增强，同时减轻了运维复杂度与潜在风险。不仅促使风电场实现了更优的产能效率，还大幅削减了运维开销，从而为整个系统注入了更强的经济效用与市场竞争优势。

3 技术实现的挑战

3.1 系统的适应性

在设计自动开合系统以适应风机塔筒平台盖板时，务必详尽考量各风机品牌与型号间的独特设计以及结构差异。设计人员面临的挑战在于创造一个兼备广泛适用性和高度灵活性的系统，确保其能在多样化的风机平台上稳健运行。通过引入标准化接口以及模块化构建策略，系统能够实现跨机型的灵活部署，无需经历大幅度的重新设计过程，此举措既增强了系统的互配性，又有效控制了因个性化定制而额外增加的成本。

3.2 技术的可靠性

在风机塔筒平台盖板自动化开关系统的研究与开发进程中，技术可靠性构成了确保该系统能在多样化的环境情境下维持稳健运行的核心基础。系统设计需满足在极端天气状况（如极热或极寒气温、高强度湿度环境）以及复杂地理布局（如海上风力发电厂、高山风能站等）中保持高效作业的能力。实现这一愿景，离不开对系统进行严格的环境适配性评估，涵盖耐久性试验与环境应力测试，旨在确认其在各类工况下的稳

定性与长久使用性能。此外，融入前沿的故障防御策略是至关重要的环节，通过部署冗余架构与错误容忍机制，即使面对关键组件故障，系统亦能维持平稳运行，保证在不利情境下的持续工作能力。此类可靠性设计策略不仅巩固了系统的综合效能，还大幅减少了由意外故障引发的停机时间与维护开销，为风电场的高效持续经营提供了有力保障。

3.3 维护与监控

系统的持续运行不仅需要依赖一套完备的维护策略，还需要借助实时监控机制的效力。维护策略应涵盖周期性的系统审查、预先采取的维护措施和故障诊断流程。至于实时监控机制则需要部署多类型传感器并配合运用数据分析工具，以便传感器能够即刻搜集系统运行参数，而数据分析工具则负责处理这些信息，迅速辨明任何会引致系统性能衰减或中断的先兆。

4 解决策略与未来发展

4.1 研发通用接口

为了推动风机塔筒平台盖板自动化开启与闭合技术的广泛应用，开发一种既标准化又模块化的接口体系显得极为关键。该接口设计需全方位考量其与不同型号和品牌风机系统的匹配度，旨在大幅缩减技术部署的繁琐程度和经济投入。具体来说，应采用开放式的架构设计通用接口，以促进各类硬件与软件的高效集成。这样的开放性特征，既促进了不同系统间的流畅交互，又加快了创新技术的普及与实践步伐。

4.2 强化系统稳定性

确保风机塔筒平台盖板自动开启与闭合技术的持续稳定性是达成该系统可靠运行的核心要求。提升此系统稳定性需采纳多元化的综合性策略。首先，对防护措施进行全面增强。涵盖了从实体防护（如构造加固以及防水构造的设计）到电子防护领域（如电磁干扰的屏蔽效应与超负荷保护机制的实施），确保了系统在严峻环境中的正常运转。其次，改进控制算法是加速系统响应速度与增强其处理效能的至关重要的方法。融合前沿的控制理论与算法，如模糊控制理论与神经网络控制技术的应用，系统自适应性能与错误容忍度将得到显著提升。最后，系统稳定性增益亦有赖于精准的传感器数据输入与即时数据处理能力。

4.3 智能维护系统

智能维护系统的实施是保障风机塔筒平台盖板自动化开闭技术持续稳定运行的关键支柱。该系统融合了云计算与物联网的先进技术，实现了设备状态的即时监控、潜在故障的自动诊断与预警，有效预防了系统性故障的发生。具体实施策略涉及智能维护系统布置多类型高精度传感器以采集核心运行参数，如温度、压力和振动等信息。这些数据借助物联网技术被迅速且稳定地传送至云端平台，随后在云环境中进行深度数据分析。云端平台运用前沿的机器学习算法开展数据模式识别与故障先期预测，确保了能及时发现影响系统性能的潜在风险^[5]。

结语

风机塔筒平台盖板自动开合技术创新的进步，不仅增强了风力发电系统维护的安全属性与作业效率，还彰显了风电领域技术革新的发展趋势。展望未来，行业内部必须持续加大研发力度，克服技术应用过程中遇到的种种难题，以促进该创新技术的普及与深化应用。^[6]

引用

- [1] 高务文,段智.风机塔筒螺栓在线监测装置[J].企业管理,2023(S2): 356-357.
- [2] 李舸.风机塔筒外挂式可升降安装平台设计与施工[J].云南水力发电, 2023,39(8): 40-44.
- [3] 胡磊.风机塔筒阻尼索减振理论与试验研究[D].湘潭:湖南科技大学,2023.
- [4] 黄青松,王晓兵,赵东霞.风电项目现浇混凝土风机塔筒施工技术[J].科学技术创新, 2023(8):225-228.
- [5] 王琛.海上风机塔筒倾斜监测应用与数据分析[J].工程技术研究,2022, 7(7):12-15.

基于无监督学习的 软包锂电池边角外观缺陷检测*

文 ◆ 广东省科学院电子电器研究所 蔡浩聪
广州理工学院 周亚梅
广东省科学院电子电器研究所 张焕文
广东省电子技术研究所 袁 勇 曾伟康

引言

软包锂电池作为新一代储能电源，具有优越的性能和广泛的应用前景，其产能迅速增长。在双碳等环保政策的推动下，全年电力储能项目大幅增加。同时，2025 年后的中国和全球电池产能将面临巨大缺口，其生产质量和生产效率需要进一步提高^[1]。软包锂电池使用的铝塑膜外壳材料质地较软，容易受损，因此在生产过程中常常会出现外观缺陷。其中较大的缺陷会对电池的安全性构成严重威胁，导致电池内部电解质泄漏，甚至引发火灾等安全事故。因此，软包锂电池外观缺陷检测是锂电池生产过程中重要的环节，软包锂电池外观检测技术水平直接决定了电池产品的质量和安全。目前，软包锂电池厂家大多采用人工操作进行产品外观缺陷检测，受主观因素影响较大，且无法较长时间稳定检测，检测效率和准确率较低。少数基于传统机器视觉方案的系

统由于可靠性不足，未能达到验收标准，导致难以实现量产。因此，软包锂电池外观缺陷的自动检测国内仍有很大的提升空间。

王正家^[2]提出一种检测软包锂电池外观缺陷的方法，有效代替人工目检，提高了工作效率，但其检测准确率较低。郑魁敬等^[3]提出一种子图像遍历的方法来处理锂电池检测方面的缺陷，该方法并不适用于反光特性较高的软包锂电池的检测。许海彪^[4]使用改进后的 YOLOv3-x 深度学习网络对锂电池壳表面缺陷进行分类检测，但基于有监督学习的方法存在实际工业现场较难覆盖所有类型的缺陷，容易发生漏报的弊端，并且标注成本高昂。邓红红^[5]结合机器视觉与工业检测技术，利用霍夫变化以及基于最小二乘法改进的算法，有效排除了奇异点的干扰，开发了一套手机锂电池表面检测系统，实现锂电池外观尺寸缺陷、顶峰封印异物缺陷以及喷码不良的自动检测，但其受软包锂电池轻微变形和反光影响较大。刘飞飞等^[6]提出 Gabor 重建图像的皮革检测方法应用到软包电池上，软包电池表面的反光特性影响检测的精度。综上，对软包锂电池外观缺陷检测方法的研究具有较高的研究价值。

目前，国内的速博达（深圳）自动化有限公司基于康耐视的深度学习视觉软件 VisionPro Deep Learning，开发出软包锂电池表面缺陷检测系统。该系统主要技术指标在行业处于领先地位，设备单片检测时间小于 4s、检测准确率大于 96%、人工替代率超过 70%、漏检率小于 0.05%、过检率小于 5%。但该系统核心算法依赖于国外厂家康耐视，据网络搜索结果显示国内厂家暂无较成熟算法，软包锂电池外观缺陷检测仍然存在一定程度的“卡脖子”问题。本文通过研究无监督学习的核心算法，并进行方案实现，致力于为该领域核心技术研发提供有价值的参考方案，以期解决该领域的“卡脖子”问题。

针对上述情况，本文提出了一种基于修改的 DiffusionAD 的软包

*【基金项目】地方科技项目 / 广东省科技计划其他项目（0824149001001）“基于无监督学习的 AI 视觉缺陷检测技术研究及锂电池边角外观缺陷检测应用系统开发”

【作者简介】蔡浩聪（1986—），男，广东揭阳人，硕士，工程师，研究方向：计算机视觉。

【通讯作者】张焕文（1974—），男，广东梅州人，学士，高级工程师，研究方向：电子电器技术及机器视觉应用。

锂电池边角外观缺陷检测方法，设计并搭建软包锂电池边角外观缺陷检测系统实验平台，对检测系统进行方案设计和实验分析。通过优化 DiffusionAD 模型，在保持较高精度的基础上，减少模型参数量，降低对算力的要求，并能在 RTX 4060 等中低端显卡上推理。在自制软包锂电池边角外观数据集上，总体识别准确率高达 97%，验证了本文所提方法的有效性。

- 综上所述，本文的主要贡献如下。
- (1) 针对软包锂电池场景中外观成像困难的问题，设计一种能够解决反光问题并较均匀打光的图像采集系统。
 - (2) 构建了软包锂电池的边角外观缺陷检测的自制数据集。
 - (3) 采用 DiffusionAD 模型优化，在不降低模型准确率的情况下，降低模型参数量，从而降低算力需求，满足在 RTX 2060 等中低端显卡上运行。
 - (4) 提出基于无监督学习软包锂电池边角外观缺陷检测方法，并通过实验得到较好结果，在后续的软包锂电池全面外观缺陷检测中具有一定的参考与应用价值。

1 相关工作

1.1 扩散模型

扩散模型是一种基于热力学原理的图像生成模型，其通过逐步添加高斯噪声将输入数据转变为纯高斯噪声，然后逐步去噪生成新的图像。扩散模型基于数学中的马尔可夫性质，即在给定当前状态的情况下，一个随机过程的未来状态仅依赖于当前状态。在扩散模型中，首先通过不断向初始图像中添加高斯噪声，使其逐渐变成纯噪声图像。由于图像的参数已知，因此前向加噪过程可控。与前向过程中添加噪声不同，逆向

过程是对纯噪声图像进行去噪，从而生成新的图像。这个去噪过程需要扩散模型通过神经网络进行学习。

扩散模型的原理主要依赖两个核心过程，即前向扩散过程（Forward Diffusion Process）和反向扩散过程（Reverse Diffusion Process）。扩散模型的前向和反向过程如图 1 所示。其中， X_0 为初始图像， X_T 为经过 T 次加噪后符合高斯分布的纯噪声图像。实线箭头方向为前向扩散过程，虚线箭头方向为反向扩散过程。前向过程逐步给数据添加噪声，经过 T 次加噪声操作后，图像就会变成一幅符合标准正态分布的纯噪声图像 X_T 。在反向扩散过程中，目标是训练一个神经网络，使其执行 T 次去噪操作，将 X_T 还原为 X_0 。神经网络的学习目标是确保 T 次去噪操作能够抵消对应的加噪操作。在训练完成后，只需从标准正态分布中随机采样一个噪声，通过反向过程中的神经网络将该噪声还原为一幅图像，从而生成新的图像。

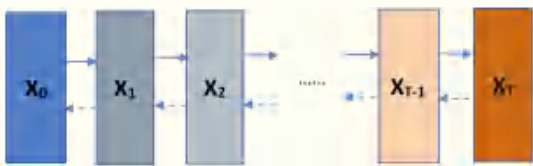


图 1 扩散模型的前向和反向过程

1.2 DiffusionAD 模型

DiffusionAD 模型^[7]是基于扩散模型的无监督学习图像异常检测模型，其核心思想是利用扩散

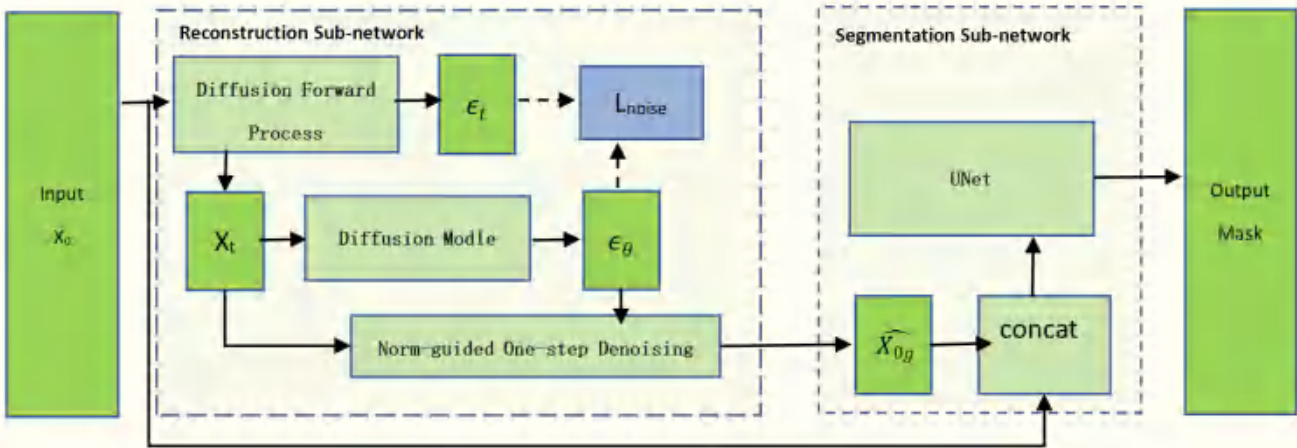


图 2 DiffusionAD 模型框架图

模型来学习正常图像的分布，并通过在逆向过程中的重建误差来检测异常。DiffusionAD 模型作者提出了一种由重构子网络和分割子网络组成的新型异常检测网络，并且重构子网络没有像传统扩散模型逐步加噪恢复图像，而是通过一步加噪直接恢复原始图像，这样可以节约大量运算时间。DiffusionAD 模型框架图如图 2 所示。

DiffusionAD 模型的重构子网络的损失函数如式（1）所示，其中， $y=0$ 为正常样本，网络向训练图像输入两种的噪声 ϵ_{ts} 和 ϵ_{tb} ， ϵ_{ts} 为符合正态分布的弱噪声， ϵ_{tb} 为符合正态分布的强噪声， $\epsilon_{\theta}(x_{ts},t)$ 为模型预测的弱噪声， $\epsilon_{\theta}(x_{tb},t)$ 为模型预测的强噪声。

$$L_{nosie}=[(1-y)||\epsilon_{ts}-\epsilon_{\theta}(x_{ts},t)||^2+||\epsilon_{tb}-\epsilon_{\theta}(x_{tb},t)||^2]/2$$

(1)

分割子网络的损失函数如式（2）所示，其中， M 为真实的 Mask， $\hat{M}$ 为预测得到的 Mask， γ 为权重超参数，用于控制 L_{focal} 的权重。

$$L_{mask}=SmoothL_1(M,\hat{M})+\gamma L_{focal}(M,\hat{M})$$

(2)

因此，DiffusionAD 模型的总体损失函数如式（3）所示。

$$L_{total}=L_{nosie}+L_{mask}$$

(3)

DiffusionAD 模型中将检测方法分为基于结构的检测方法和基于纹理的检测方法。基于结构的

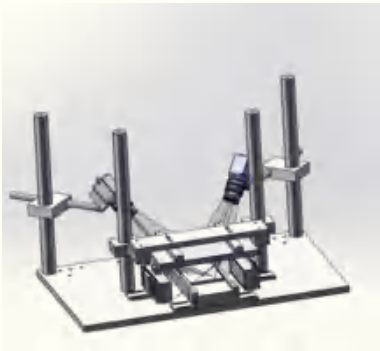


图 3 系统总体硬件示意图

检测方法需要在训练前通过标注工具将产品图像区域从整张图像中分割出来，作为 Mask 图片保存到 DISThresh 文件夹中，供训练时使用。基于纹理的检测方法使用了开源的 Mask 图像，作为模拟缺陷的区域，不需要使用标注工具进行制作。本文的软包锂电池边角外观由于不具备规律的纹理，因此选择了基于结构的检测方法。

2 模型修改

本文算法由 DiffusionAD 模型修改而来。DiffusionAD 模型通过训练正常样本的图像数据集，获得能够识别图像异常区域的权重参数。在预测过程中，DiffusionAD 模型将缺陷产品图像重建为合格产品图像，并将缺陷产品原图和重构后的合格产品图像输入到分割子网络中，预测出缺陷的区域。

本文将原始的 DiffusionAD 模型中 GroupNorm32() 中的 num_groups 由原来的 32 修改为 16，base_channels 由原来的 128 修改为 32，减少了模型的参数量（见表 1），降低显存的要求，在 RTX2080Ti 显卡上训练，通过修改模型参数，重建子网络参数量由 131.6M 下降到 8.2M，模型的总参数量由原来的 159.9M 降低到 36.5M，总参数量是原来模型的 1/4。

表 1 改进前后的模型参数量

子网络	原始总参数量 (M)	裁剪后总参数量 (M)
重建子网络	131.6	8.2
分割子网络	28.3	28.3
总和	159.9	36.5

模型的超参数设置如下。img_size=256，Batch_Size=4，EPOCHS=2000，加噪的步数为 $T=1000$ ，重构扩散模型的学习率设置为 diffusion_lr=1e-4，缺陷分割子网络的学习率设置为 seg_lr=1e-5，多注意力头设置为 num_heads=4。

3 系统设计

3.1 硬件设计

根据客户需求，软包锂电池总共有 8 个边角，由于底部 4 个边角被硬铝包装起来，不容易造成损坏，因此客户只要求检测上面软包部分的 4 个边角。系统总体硬件示意图如图 3 所示，软包锂电池从产品滑槽推进，到达拍照位置后，触发传感器控制边角 2 侧工业相机拍照，同时采集 2 个边角的图像，2 个工业相机成水平 30°~45°角拍照。光源系统如 3.2 搭建清晰的成像采集系统所述。工业相机的高度、远近、角度可根据实际成像效果进行调整。

3.2 图像采集系统

由于软包锂电池的外壳是铝塑膜材质，表面易受表面光斑、随机弹性形变等外界因素干扰，导致局部成像亮暗不一致，因此需要设计一个最大程度降低反光影响的光学成像系统。本文采用了带漫射板的工业白光光源，锂电池上方使用面光源进行打光，侧面使用白光条形光源进行打光，通过调节距离和亮度，达到最佳的打光成像效果。

3.3 软包锂电池边角数据集

图3中，由于左右2个工业相机采集的2张图像是水平镜像的效果，因此将右边相机采集的图像进行水平镜像图像预处理后，可得到和左边相机采集相同方向的图像，以训练同一套模型参数对左右2个相机的图像进行识别，减少图像数据集采集数量，降低研发难度。

本文通过搭建消除较强反光的高清图像采集系统，使用1200万像素的工业相机和微距镜头，获取480张合格的软包锂电池边角图像数据集和80张带有产品缺陷的图像数据集，产品缺陷数据集中包含变形缺陷、凹坑缺陷、划痕缺陷、脏污缺陷等不合格产品图像。各类型缺陷的示意图如图4所示。

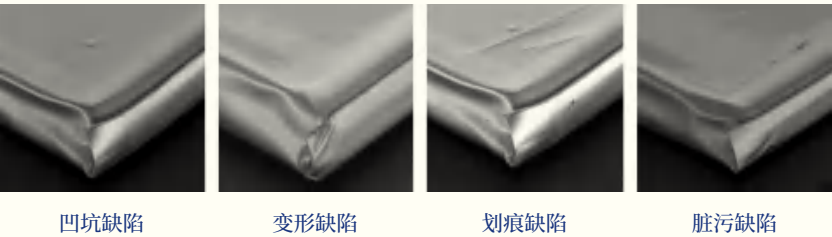


图4 各类型缺陷的示意图

3.4 软件系统

本文将训练和推理代码分开，设计了一个带有人机交互界面的推理软件，可以在 RTX2060 显卡上推理。推理软件主界面如图5所示。

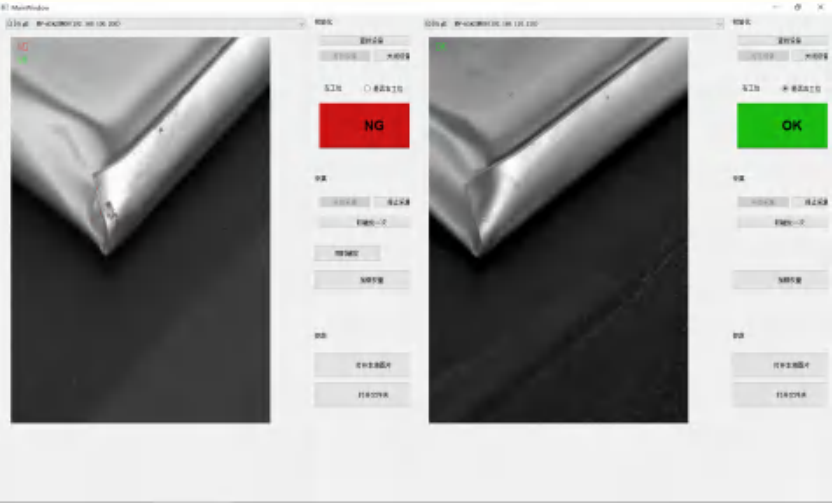


图5 推理软件主界面

软件可以选择每个工位对应的工业相机，调节相机的曝光参数等，并且可以手动选择需要的模型参数。软件上有触发相机拍照的按键，当按下按键后，工业相机抓拍图像，并将图像传送到工控机中处理，工控机根据选择的模型，对图像上软包锂电池边角图像进行检测，若发现有缺陷区域，便将该区域叠加到原始图像上，输出 NG 信号。若未发现缺陷区域，则输出 OK 信号。

系统软件的处理流程如图6所示。通过界面上的按键触发相机拍照，并将采集的图像送入 DiffusionAD 模型中推理，若为不合格产品（NG 产品），则界面输出叠加了缺陷区域的图像，在主界面上提示“NG”字样；若为合格产品（OK 产品），则主界面上提示“OK”字样。

4 实验与分析

本文将软包锂电池边角外观数据集分成正常产品图像数据集和缺陷产品图像数据集，其中缺陷产品图像数据集中的缺陷分成变形、凹坑、划痕、脏污4个类别。实验中将软包锂电池边角外观数据集分为训练数据集和验证数据集。从正常产品图像数据集中随机选取87.5%的数据作为训练数据集（420张OK图像），剩下的12.5%的正常图像（60张OK图像）和NG图像（80张NG图像）作为验证数据集，验证数据集用于验证模型的性能。

本文使用修改 DiffusionAD 模型基于结构的检测方法进行训练。使用该方法，需使用标注工具，将产品的区域从背景中分割出来，本文使用百度的 EISeg 图像分割工具（见图7），能够较快地将训练数据集中的软包锂电池的边角图像区域从整体图像中分割出来。同时，将分割出来的 Mask 图片放置到 DISThresh 文件夹中，在模型训练过程中使用。

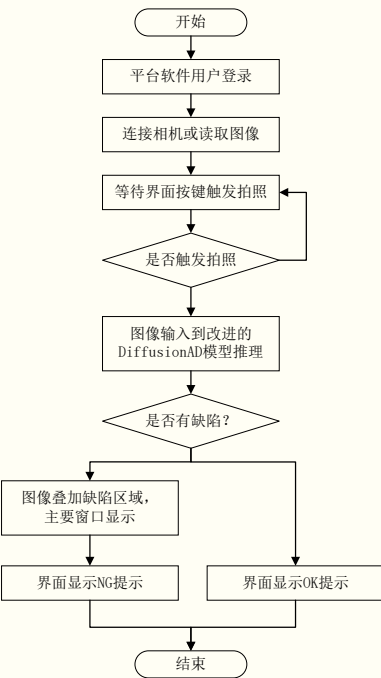


图6 系统软件的处理流程

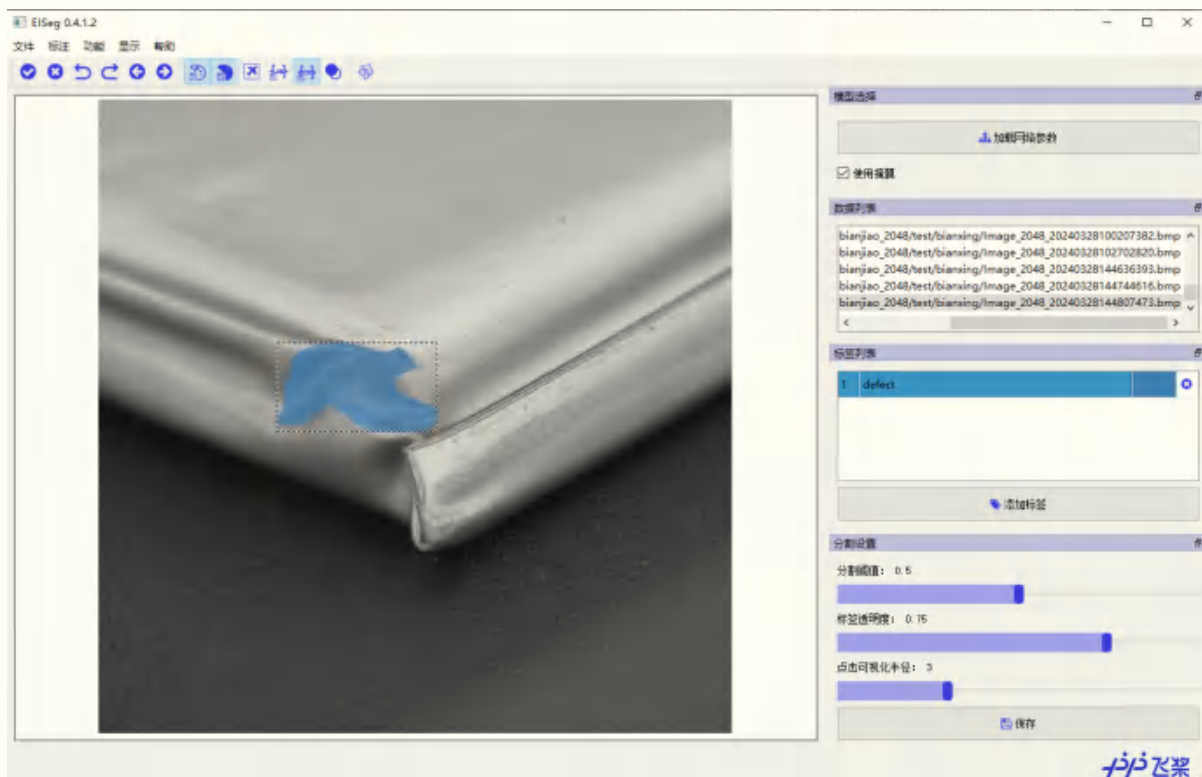


图 7 EISeg 图像分割工具

修改的 DiffusionAD 模型训练使用 420 张 OK 图像作为训练数据集，训练的超参数如“2.2 修改 DiffusionAD 模型裁剪”中的设置，训练完成得到模型权重，再对验证数据集进行验证，得到各类缺陷的检出结果（见表 2）。

修改后 DiffusionAD 模型 AUR OC 和 AUPRO 结果表如表 3 所示。

各类型缺陷的实验结果图如图 8 所示。

轻微变形漏检情况如图 9 所示，从实验结果来看，漏检的重构图已经把缺陷区域重构了，热力图上也有所响应，但响应微弱，未能检测出来。

合格产品误检情况如图 10 所示。

实验结果表明，本文修改 DiffusionAD 模型在自制数据集上获得较高的准确率，达到 97.1%；从验证实验结果看，本文在凹坑、划痕、脏污、较大变形类型

图 8 各类型缺陷的实验结果图

表 2 各类缺陷检出结果统计表

缺陷类型	检测个数	正确检出个数	误检 / 漏检个数	准确率 %
变形	25	24	1 (漏检)	96
凹坑	25	25	0	100
划痕	10	10	0	100
脏污	20	20	0	100
合格产品	60	57	3 (误检)	95
总体	140	136	4	97.1

表 3 修改后 DiffusionAD 模型 AUROC 和 AUPRO 结果表

检测指标	Image-AUROC (%)	Pixel-AUROC (%)	Pixel-AUPRO (%)
修改 DiffusionAD	99	97.2	94.6

图 9 轻微变形漏检情况

图 10 合格产品误检情况

缺陷上都有较好表现，只是在较小变形情况下存在漏检情况。本文存在正常产品的误报情况，关于该问题，后续需优化算法，增加正常样本的数据集，降低模型的误报率。

结语

本文提出了一种基于无监督学习的软包锂电池外观缺陷检测方法，具体是一种基于修改的 DiffusionAD 模型的软包锂电池外观缺陷检测方法。通过实验和数据分析，证明了该方法的有效性，为软包锂电池外观缺陷检测提供一种有价值的参考方案。但本文的实验结果仍存在不足之处，与 MVTec AD 等开源数据集^[8]的准确率相比，本文准确率还有待提

升，模型对微小变形缺陷存在漏检情况和对合格产品存在误报情况。同时，本文实验数据集中，各类型的缺陷数据集较少，划痕数据集只有 10 张。后期应多采集 NG 数据图片，提高基于无监督学习的软包锂电池外观缺陷检测系统的准确率。^[8]

引用

[1] 官云龙,柴文帅.全球碳中和背景下的锂市场发展趋势[J].中国资源综合利用,2021,39(7):92-96.

[2] 王正家,咎傲,谷峰.基于Gabor滤波的软包电池表面缺陷检测[J].组合机床与自动化加工技术,2023(11):146-149.

[3] 郑魁敬,刘学超,王萌萌.基于机器视觉的手机电池表面缺陷检测[J].制造技术与机床,2020(4):105-112.

[4] 许海彪.基于深度学习的锂电池壳表面缺陷视觉检测研究[D].秦皇岛:燕山大学,2021.

[5] 邓红红.锂电池表面缺陷检测研究[D].哈尔滨:哈尔滨工业大学,2018.

[6] 刘飞飞,孙合锐,王潇男,等.基于Gabor滤波的重建图像法检测皮革表面缺陷[J].传感器与微系统,2022,41(3):139-141,144.

[7] Zhang H,Wang Z,Wu Z,et al.DiffusionAD:Norm-guided One-step Denoising Diffusion for Anomaly Detection[J].arXiv preprint arXiv:2303.08730,2023.

[8] Tao X,Gong X,Zhang X,et al. Deep Learning for Unsupervised Anomaly Localization in Industrial Images:A Survey[J].IEEE Transactions on Instrumentation and Measurement,2022(71):1-21.

基于用户视角的 用电用能服务触点分析与优化策略

文 ◆ 云南电网有限责任公司 陈 婷 孟维丽娅 汤 迪

引言

在现代社会中，电力已经成为人们日常生活和工业生产中不可或缺的重要资源。随着智能电网和大数据技术的广泛应用，用电用能服务也在不断向智能化、个性化方向发展。然而，用电用能服务涉及多个环节和多个主体，任何一个环节处理不当都会导致客户的不满和投诉。因此，深入分析用电用能服务中的关键触点，基于用户视角的用电用能服务触点分析，探索用户在电力消费过程中的每一个交互节点，从需求感知、服务接入、使用体验到反馈机制，全面理解用户的真实需求与潜在期待。不仅能够揭示现有服务体系中的盲点与痛点，还为优化策略的制定提供了坚实的数据支撑与洞察基础。通过精准定位服务触点，实施包括智能化升级、个性化定制、便捷性增强在内的优化策略，不仅能有效提升用户满意度与忠诚度，还能促进能源的高效利用与可持续发展，构建更加和谐、绿色的用电用能新生态。

1 用电用能服务触点分析

服务触点是指在服务过程中，供应者与接收者之间相互作用和联系的关键点。在用电用能服务中，服务触点可以分为多个层面，包括供电企业的内部运营触点、与客户互动的服务触点以及电力设备的运行维护触点等。

1.1 供电企业内部运营触点

供电企业内部运营触点主要涉及企业内部的各个业务流程和部门之间的协作。例如，营销部门与生产计划部门的协同工作，可以确保电力供应的稳定性和可靠性；客户服务部门与运维部门的合作，可以快速响应客户诉求，提高服务效率。

（1）营销与生产计划协同

营销部门主要负责与客户进行沟通和互动，了解客户的需求和诉求，并将其传递给生产计划部门。生产计划部门根据客户需求和电网运行情况，制定合理的发电和供电计划。然而，在实际操作中，由于信息不对称和沟通不畅等原因，营销部门与生产计划部门之间的协同工作常常存在问题。例如，营销部门未能及时将客户的高频诉求反馈给生产计划部门，导致供电计划无法及时调整，从而引发客户投诉。

（2）客户服务与运维协作

客户服务部门是供电企业与客户之间的桥梁，负责接收和处理客户的诉求和投诉。运维部门则负责电力设备的运行维护和故障抢修工作。当客户遇到用电问题时，客户服务部门需要将诉求传递给运维部门，并跟踪处理进度，确保问题得到及时解决。然而，在实际操作中，客户服务部门与运维部门之间的协作常常存在问题。例如，客户服务部门未能及时将客户诉求传递给运维部门；运维部门未能及时响应和处理客户诉求，导致客户的不满和投诉^[1]。

1.2 与客户互动的服务触点

与客户互动的服务触点主要涉及供电企业与客户之间的直接沟通

【作者简介】陈婷（1977—），女，云南昆明人，硕士研究生，高级工程师，从事电力市场营销、客户服务以及电力技术与装备研究工作。

和互动。触点包括用电业务办理、客户服务热线、投诉处理、电费缴纳等。

（1）用电业务办理

用电业务办理是客户与供电企业之间最直接的互动触点。客户在办理用电业务时，需要了解相关的政策、规定和流程，并按照规定提供相关的资料和信息。然而，在实际操作中，由于业务流程繁琐、信息不明确等原因，客户在办理用电业务时常常遇到困难。例如，客户在申请新装电表时，需要填写大量的资料和表格，并且需要经过多个部门的审核和审批，导致办理时间过长，影响客户的用电体验。

（2）客户服务热线

客户服务热线是客户与供电企业之间沟通的重要渠道。客户通过拨打客户服务热线，咨询用电问题、查询电费账单、报修电力故障等。然而，在实际操作中，客户服务热线常常存在诸多问题。例如，客服人员的专业素养和服务态度不够优秀，无法准确回答客户的问题；客服人员数量不足，导致客户等待时间过长；客服系统的稳定性和可靠性不够高，导致客户无法正常接入等。

（3）投诉处理

投诉处理是客户对供电企业服务质量和效率的重要评价依据。当客户遇到用电问题时，如果无法通过其他渠道得到解决，那么就会选择向供电企业投诉。然而，在实际操作中，投诉处理常常存在诸多问题。例如，投诉处理流程繁琐，导致处理时间过长；投诉处理结果不够公正和合理，导致客户的不满和抱怨；投诉处理信息的反馈不够及时和准确，导致客户无法及时了解处理进度和结果等。

（4）电费缴纳

电费缴纳是客户与供电企业之间最基本的经济交易。客户需要按照规定的时间和方式缴纳电费，以确保用电的连续性和稳定性。然而，在实际操作中，电费缴纳常常存在诸多问题。例如，电费账单的信息不明确和不准确，导致客户无法及时了解电费金额和缴纳方式；电费缴纳渠道不够丰富和便捷，导致客户需要花费更多的时间和精力去缴纳电费；电费缴纳系统的稳定性和可靠性不够高，导致客户无法正常缴纳电费等。

1.3 电力设备运行维护触点

电力设备运行维护触点主要涉及电力设备的运行状态监测、故障预警和故障抢修等工作。这些触点直接影响电力供应的稳定性和可靠性，进而影响客户的用电体验。

（1）运行状态监测

运行状态监测是电力设备运行维护的基础工作。通过对电力设备的运行状态进行实时监测和分析，可以及时发现潜在的故障和问题，并采取相应的措施进行处理。然而，在实际操作中，运行状态监测常常存在诸多问题。例如，监测设备的精度和可靠性不够高，导致监测数据不准确；监测系统的稳定性不够高，导致监测数据无法及时上传和分析；监测人员的专业素养和责任心不够强，导致监测工作不到位等^[2]。

（2）故障预警

故障预警是电力设备运行维护的重要环节。通过对电力设备的运行

状态进行监测和分析，可以预测设备出现的故障和问题，并提前采取相应的措施进行处理。然而，在实际操作中，故障预警常常存在诸多问题。例如，预警系统的灵敏度和准确性不够高，导致预警信息不准确；预警信息的传递和处理不够及时和有效，导致故障无法及时处理等。

（3）故障抢修

故障抢修是电力设备运行维护的紧急工作。当电力设备出现故障时，需要迅速组织抢修人员进行抢修工作，以确保电力供应的稳定性和可靠性。然而，在实际操作中，故障抢修常常存在一些问题。例如，抢修人员的专业素养和应急能力不够强，导致抢修时间过长；抢修设备和工具不够齐全和先进，导致抢修效果不佳；抢修信息的传递和处理不够及时和准确，导致抢修工作无法顺利进行等。

2 基于用户视角的用电用能服务优化策略

2.1 精细化分类分析与超前服务

为了更精准地满足用户的用电需求，应实施精细化分类分析，将用户按照用电行为、用电需求、用电场景等多维度进行分类。通过对各类用户的用电数据进行深入挖掘和分析，了解各类用户的用电特点和用电规律，进而为制定个性化的用电优化策略提供有力支撑。

超前服务则是在精细化分类的基础上，通过预测用户未来的用电需求和行为，提前为用户提供相应的服务和支持。例如，对于经常遭遇用电高峰困扰的用户，可以提前通知其调整用电计

划。此外，超前服务还包括对用户用电设备的实时监测和预警。通过对用户用电设备的实时监测，及时发现设备的异常情况，提前进行预警和维修，避免设备故障对用户的用电造成影响。同时，通过对用电数据的分析，预测设备的寿命和更换周期，为用户提供更加精准的设备维护建议，延长设备的使用寿命和降低维护成本。

2.2 服务流程优化与高效响应

在快速变化的用电用能服务环境中，服务流程的优化与高效响应成为提升客户满意度的核心要素。为了实现这一目标，应从以下 4 个方面进行深化实践。

第一，简化服务流程，去除繁琐环节。通过对现有服务流程的全面梳理，识别并剔除不必要的步骤，实现流程的精简和高效。例如，在电费缴纳、故障报修等环节，引入自助服务终端、移动应用等数字化工具，减少用户等待时间，提升服务效率^[3]。

第二，加强内部协同，实现信息的快速传递和响应。建立跨部门协作机制，确保用户诉求在各部门间得到及时、准确地传递和处理。引入项目管理、敏捷开发等先进管理理念，提升内部团队的响应速度和执行力，确保用户需求得到快速满足。

第三，注重服务过程的透明化和可视化。通过实时监测服务

进度，为用户提供清晰的反馈和预期，增强用户对服务过程的信任感和满意度。例如，在故障报修过程中，通过短信、移动应用等方式实时告知用户维修进度和预计完成时间，让用户随时掌握服务动态。

第四，建立服务质量和效率的评估机制。收集用户反馈、分析服务数据，对服务流程进行持续优化和改进。同时，设立服务质量指标和考核体系，对服务团队进行定期评估和激励，确保服务质量和效率持续提升。

2.3 多目标用电优化策略

旨在通过综合考虑用户的不同需求与能源使用场景，实现用电效率、成本节约与环境保护等多重目标的平衡与最大化。

首先，多目标用电优化策略注重个性化需求的满足。每个用户的生活、工作模式和用电习惯各异，因此，策略应能够根据用户的用电历史数据、偏好设置以及未来计划，智能推荐最优的用电方案。例如，调整家庭电器的使用时间，以避免高峰电价时段。其次，该策略强调成本效益分析，帮助用户在保障用电质量的同时，实现能源成本的最小化。通过实时监测用电数据，结合实时电价信息以及历史用电模式，智能系统能够为用户提供定制化的节能建议，如使用能效更高的电器、调整恒温器的设定等，从而在不影响生活质量的前提下，有效控制用电成本。最后，多目标用电优化策略还致力于环境保护，鼓励用户采用绿色、可再生的能源。通过整合智能电网技术，策略能够优先调度用户安装的太阳能板、风力发电等可再生能源产生的电力，减少对传统化石能源的依赖，从而降低碳排放，促进可持续发展。

2.4 构建多元化增值服务体系

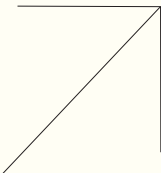
在当今智能化、个性化的服务趋势中，基于用户视角的用电用能服务优化策略正逐步向构建多元化增值服务体系迈进。不仅能够满足用户基本的用电需求，还能够通过技术创新与模式创新，为用户提供一系列丰富、便捷的增值服务，提升用电体验，增强用户粘性。

结语

基于用户视角的用电用能服务触点分析与优化策略是提升电力服务质量和用户满意度的重要途径。通过深入剖析用户在电力消费过程中的实际需求与痛点，精准定位服务优化的关键点，从而制定出更加符合用户期望的服务策略。未来，随着技术的不断进步和用户需求的日益多样化，应持续关注服务触点的动态变化，不断创新服务模式，以更加智能化、个性化的服务满足用户的多元化需求。同时，加强用户教育与互动，提升用户的能源管理意识和能力，共同推动构建更加绿色、高效、和谐的能源消费生态。^[4]

引用

[1] 杨欢.智能电力营销环境下供电企业提高服务质量的措施探析[J].营销界, 2024(14):63-65.
[2] 颜以伦.B供电局供电服务质量优化策略研究[D].南宁:广西大学,2024.
[3] 黄文珏.指向客户满意度的电力系统营销服务质量管理[J].现代商业研究, 2024(6):134-136.



智能单元门系统设计探讨

文◆奥飞久通智能科技（上海）有限公司 陈晓亚

引言

城市化和居民安全需求的增长使社区单元门系统越来越重要，但现有系统存在技术、服务和管理问题，如布线难、功能单一、兼容性差和管理困难，影响用户体验和社区安全。智能单元门系统能提供高效、安全的出入管理，提升社区安全和居民生活质量。本文旨在提供一定理论和实践指导，以期推动社区安全管理向智能化、安全化发展。

1 系统的总体设计

本系统分为总后台管理系统（简称“总后台”）、维修 App、后勤管理系统（简称“后勤 PC”）、后勤 App 以及业务 App。以上系统采用 SaaS 模式，软件应用程序部署在云端服务器上，并通过互联网向用户提供服务。硬件包括门体门框、门体驱动装置、控制器、门口机等^[1]。

2 系统的设计方案

本系统方案主要由以下 5 个子系统以及智能单元门硬件组成。

（1）总后台。支持对所有设备（控制器、门口机等）在线管理，监控设备运行状态，修改设备操作与模式，查看设备运行记录，实时接收设备的故障报警信息，设备维修工单审批分配。（2）后勤 PC。支持物业人员对小区内的所有设备在线管理，监控设备运行状态，设备操作与模式修改，查看设备运行记录，实时接收设备的故障报警信息，设备工单维修提交等。（3）维修 App。支持维修人员对设备在线管理，监控设备运行状态，设备操作与参数调试，查看设备运行记录，实时接收设备的故障报警信息，设备维修工单接收与维修后提交。（4）后勤 App。支持物业人员对小区内的所有设备在线管理，监控设备运行状态，设备操作与模式修改，查看设备运行记录，设备工单维修提交等。（5）业主 App。支持小区的业主对绑定房屋的单元门进行远程开门操作，对故障进行在线报修等。

3 系统的硬件设计

本系统智能单元门包括门体门框、门口机、控制器、门体驱动装置、电源、电锁、五金等。其中，核心硬件为门口机、控制器和门体驱

动装置。

3.1 门口机设计

门口机是智能单元门系统的重要硬件组成部分（见图 1）。为解决传统门口机需要布线的问题，在门口机基础上增加 4G/5G 无线通信模组。将原来的局域网管理中心的功能转移到云平台软件管理系统中，实现支持 SaaS 平台模式。使用 X9 核心板模块，核心板使用 Cortex-A7 双核处理器，数据和指令分别走不同的流水线，以确保 CPU 运行速度达到最大化^[2]。配备 8GB 的 Flash 存储和 512MB 的 DDR3 内存。人脸识别模块使用双目摄像头进行识别，包括彩色和红外摄像头，增强了识别准确性。822W_CSD 读卡模块使用韦根 34 接口和主板通信，兼容支持 UART 通信或韦根 26/34 接口，能够读取多种类型的卡片。无线通信模块采用搭载 ASR 平台的 CLP700 V1.1 设备，支持 LAN 网口、WiFi 等功能。RD58MT 是 5.8GHz 微波模块，可以有效感应移动物体。模块上有内置高精度算法单元主控芯片，稳定性好，可有效滤除环境干扰。

3.2 控制器设计

3.2.1 控制器结构设计

控制器是智能单元门系统的

【作者简介】陈晓亚（1990—），男，上海人，硕士，中级工程师，研究方向：计算机与信息技术应用。

核心控制单元，主要由以下 5 个模组组成。

- (1) 输入模组。编码器、门禁 / 雷达输入、安全光线输入等。
- (2) 输出模组。电机驱动、NPN 输出、电锁输出等。
- (3) MCU 处理器。芯片型号为 STM32F411，是一款高性能的 ARM Cortex-M4 微控制器，用于实现复杂的控制逻辑和数据处理。
- (4) 通信模组。采用 NBIoT 模块 -BC26，通过移动网络将采集到的数据上传至云端服务器。
- (5) DC-DC 模组。为 MCU 和其他模组提供稳定的电源，即使在输入电压波动时也能保持稳定输出。

3.2.2 控制器功能设计

- (1) 开关门功能。控制器通信模组与门口机 4G 通信模块联网，接收各端传来的操作指令，通过控制门体驱动装置完成开关门流程。
- (2) 门运行模式切换。联网后，控制器接收各端传来的操作指令，控制门体驱动装置完成门运行模式的切换流程。运行模式包括常开、常闭、自动、单向等模式。
- (3) 遇阻反弹。智能单元门在运行过程中遇到阻力或障碍物时，控制器触发遇阻反弹功能，操作门体自动停止或反向运动，以保护设备和避免对人员或物品造成伤害。
- (4) 故障报警。智能单元门在运行过程中产生异常，控制器获取异常代码指令，将故障信息上传至云服务器。

3.3 门体驱动装置设计

门体驱动装置包括电机、减速器、吊轮、皮带或者连杆等。以平移门为例，控制器联网后，接收各端传来的操作指令。控制器的电机驱动模块控制电机运行，电机通过减速器降低转速，增加扭矩，以适应门体移动的速度和力量要求。

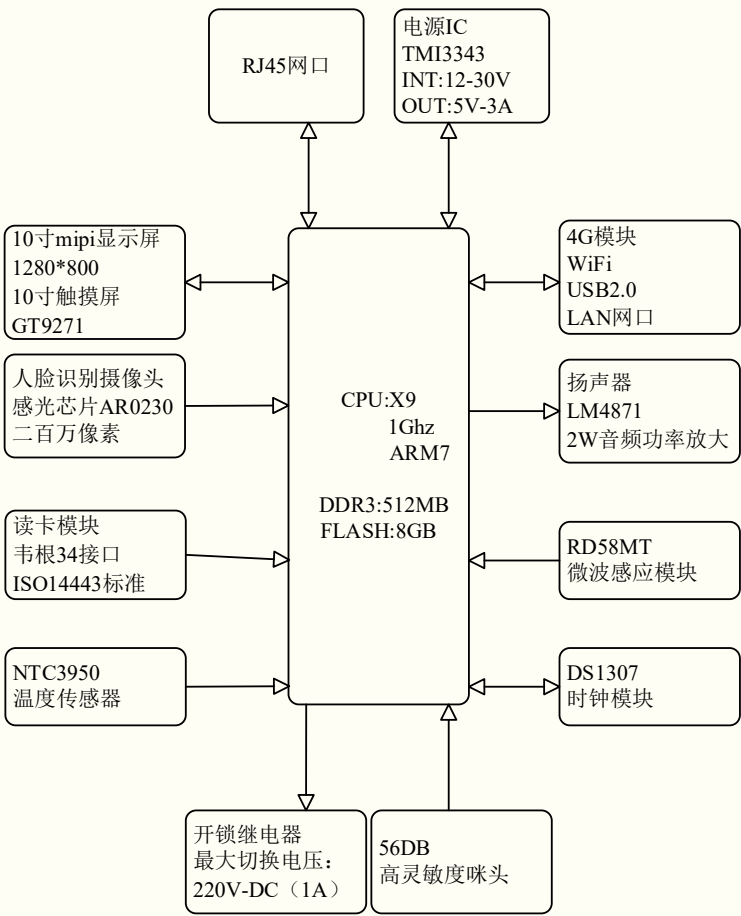


图 1 门口机结构示意图

度和力量要求。减速器带动皮带转动，皮带将动力传递给吊轮，门体在吊轮的牵引下开始开启或关闭动作。平开门则是减速器与连杆连接，通过连杆牵引门体的开关动作。

4 系统的软件设计

4.1 架构设计

本系统软硬件之间的交互基于“HTTP+MQTT”协议模式。本系统软件采用前端 VUE.js 架构，后台 SpringCloudAlibaba 架构，并结合 SpringSecurity、AOP 和 Quartz 等组件，使用 Redis 作为缓存层，处理高频次的数据访问。大幅提升系统的读写性能，减少数据库压力。使用阿里云 OSS 作为文件服务器，存储非结构化数据，如图片、视频、文档，MySQL 数据库主备架构、读写分离、数据库分库分表和消息队列等技术，构建了一个高度集成、功能丰富的分布式微服务架构，从而使系统具备强大的扩展性、可靠性和安全性。

4.2 数据库设计

良好的数据库设计可以提高数据的一致性、可维护性等性能。在数据库设计时，应遵循以下基本设计原则。

- (1) 需求分析。设计前彻底理解业务需求和数据使用场景。
- (2) 规范化。通过规范化减少数据冗余，为字段选择合适的数据类型以优化存储效率和查询性能。
- (3) 索引、主外键约束。在经常作为查询条件的字

段上设计索引。使用主键来唯一标识表中的每条记录，使用外键来维护表之间的关系。(4) 优化、可扩展。减少表之间的复杂关联查询，使用视图和存储过程来封装复杂的业务逻辑，提高代码的重用性。考虑未来业务增长的情况，确保数据库架构可以灵活扩展。(5) 安全性设计。实施适当的安全措施，如权限控制、数据加密和审计日志，确保数据库支持事务，维护数据一致性和完整性。制定数据备份和恢复策略以应对潜在的硬件故障、数据丢失或其他灾难情况。

4.3 业务流程设计

4.3.1 基本管理模块

管理员登录总后台完成角色与账号创建，导入设备信息和小区客户信息。管理员登录维修 App 完成设备新增、设备配置后，在总后台将指定的设备分配给后勤 PC。物业人员登录后勤 PC 同样完成角色、管理员账号、小区房屋结构创建，导入该小区的业主信息，将分配的设备按照编号一一对应绑定在小区房屋节点，然后录入 IC 卡、人脸信息等。小区业主通过实名制认证后登录业主 App，在房屋管理中进行房屋匹配绑定。以上各端在进行基本流程操作后，均可以对设备进行操作。

4.3.2 工单维修模块

业主通过业主 App 创建工单将故障问题进行描述上报，物业人员登录后勤 PC 确认后补充信息后继续上报至总后台。总后台管理员接到报修后进行审核分配维修人员，维修人员通过维修 App 接收任务，完成任务后进行结果提交。最终在后勤 PC 中由物业人员验收完成，该工单流程关闭。同时，物业人员可以在后勤 App 直接创建工单上报故障问题，管理员也可以在总后台直接创建工单上报故障问题。

4.3.3 开门管理模块

业主通过 IC 卡、人脸识别、登录业主 App 等方式开门。物业人员可以登录后勤 PC 或后勤 App 打开小区内各单元的单元门，对门运行模式进行设置，运行模式包括常开、常闭、自动、单向等。访客可以通过门口机进行对讲呼叫，业主可以通过业主 App 接收对讲，物业人员可以通过后勤 App 接收对讲。同时，App 远程对讲呼叫功能替代了传统的室内机、管理机功能，解决了老旧小区综合布线的问题。

4.3.4 故障报警模块

控制器通过收集门的运行状态和实时门体位置以及故障报警等数据，通过 MQTT 协议将数据传送至云服务器，并通过各端看到相关设备实时数据。故障类型包括电机故障、电压故障、强行扒门、多次遇阻、

自检故障等。故障报警功能有效遏制了老旧小区强行扒门等不良行为，加强了小区的安全管理。

5 系统测试

系统测试包括硬件测试、软件测试与整机测试，其中软件测试又包括 App 和 PC 端测试、后端测试、前后端接口联调测试^[3]等。根据业务流程，对各个模块的功能操作进行模拟场景综合测试，各项功能均测试通过。

结合实际使用场景，本系统中仅业主 App 在实际使用中会有高并发场景。针对业主 App 远程开门功能进行性能测试。使用 JMeter5.4.1 工具进行测试，测试结果良好，远程开门测试如表 1 所示。

结语

本文通过对智能单元门系统的整体设计，结合功能和性能测试，验证了该系统在提升社区安全管理方面的有效性。测试结果表明，智能单元门系统在可靠性、稳定性和效率方面均表现出色，能够有效应对传统单元门系统在技术、服务和管理方面的不足。■

引用

[1] 杨彰成,常可望.基于ARM的智能门开闭控制系统设计[J].工业控制计算机,2024,37(9):153-155.
[2] 周运道,周海军,宛熊飞,等.基于STM32的可视化智能门控系统设计[J].电脑知识与技术,2017,13(19):140-141.
[3] 王越,瞿少成,陈青松.基于人脸识别技术的社区智能门禁系统的实现[J].电子测量技术,2018,41(16):70-73.

表 1 远程开门测试

并发开门数 / 次	开门成功数 / 次	平均响应时间 / s	开门成功率 / %
1	1	0.85	100.00%
100	100	0.96	100.00%
300	299	1.21	99.67%
700	696	1.43	99.43%
1000	992	1.78	99.20%

基于优化 XACML 与信任值的零信任架构设计

文 ◆ 成都理工大学 丁奕涵 宋 飞

引言

随着人工智能、云计算等技术的发展，基于网络边界的传统网络模型逐渐暴露出许多安全问题。零信任网络架构作为一种新的网络安全理念，能够弥补传统模型的诸多不足，提升系统安全性。主流的零信任架构普遍通过对主客体进行安全状态评估的结果以及可拓展访问标记语言（XACML）来实现对应请求的策略决策。本文提出多角度的 XACML 的策略优化方法，设计 XACML-TV 并行模型来实现系统决策，结合国产商用算法提高检索效率的同时，计算信任值以实现高细粒度的访问控制效果。通过两者并行，企业能够更好地实现零信任架构，保障系统的高可用性与高安全性。

1 关键技术与算法

1.1 零信任

零信任是一种新型网络安全理念，包括 IAM（身份识别与访问管理）、SDP（软件定义边界）、MSG（微隔离）三大技术，贯彻持续验证、动态授权、全局防御的概念，确保身份可信、设备可信、应用可信、链路可信。2010

年，J. Kindervag^[1]正式提出零信任（Zero Trust）这一专业术语。“从不信任，始终验证”作为零信任的工作信条，要求对所有用户以及设备进行严格的身份验证、访问控制，对资源进行加密与保护。

美国国家标准技术研究所（NIST）于 2020 年 8 月发布《零信任架构》，并给出了抽象零信任访问模型（见图 1）^[2]。不受信任区域试图访问隐式信任区域的内容或向系统获取服务时，通过策略决策点 / 策略执行点（PDP/PEP）进行策略决策和执行，并最小化访问特权，从而避免内部攻击。

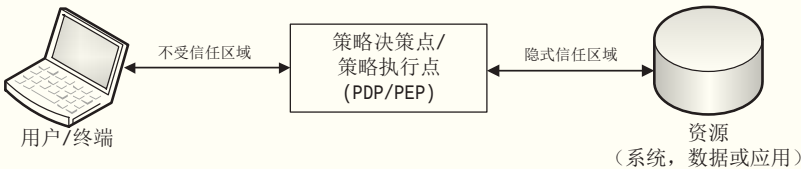


图 1 抽象零信任访问模型

1.2 XACML

XACML（eXtensible Access Control Markup Language）是以 XML 为基本形式的四元组，包括主体、目标对象、动作、规定。XACML 通过规则与决策来决定对象以及属性对资源访问^[3]。

XACML 广泛用于策略定制以及访问控制模型中，但其自身有关的优化却没有得到很大突破。SunPDP 采用暴力检索适用规则；Enterprise XACML^[4]通过属性来建立索引，面临属性较多、同一属性的策略较少的场景时效率低下；Pietro 等人^[5]指出 XACML 在资源集成时面临的策略冲突、优先级确定和效率等问题，并给出了一种集成算法，初步点明了可优化的方向；王雅哲等人提出了一种树型优化算法，处理规则冲突与冗余并取得较大的效率提升；郑楷^[6]等人则从规则聚类 and 规则重排序两方面进行了优化，更符合原生策略习惯，提升了检索性能。

1.3 SM3 算法

SM3 是国家密码管理局于 2010 年发布的一种密码散列标准，被广泛用于金融、政府等单位。在商用密码体系中，SM3 主要用于数字签名和验证、消息认证码生成和验证、随机数生成等，其安全性和效率与 SHA-256 相当^[7]。

【作者简介】丁奕涵（2000—），男，四川成都人，研究生，研究方向：零信任、SDN 网络等。

【指导老师】宋飞（1982—），男，四川成都人，博士，工程师，研究方向：网络安全技术等。

2 XACML 的多维优化

在主流的零信任网络架构中普遍存在时延高且效率低等问题。XACML-TV 评估引擎并行模型如图 2 所示，图 2 中的并行模型在解决性能问题的同时，通过组合函数还能达到更高级别的细粒度访问控制。

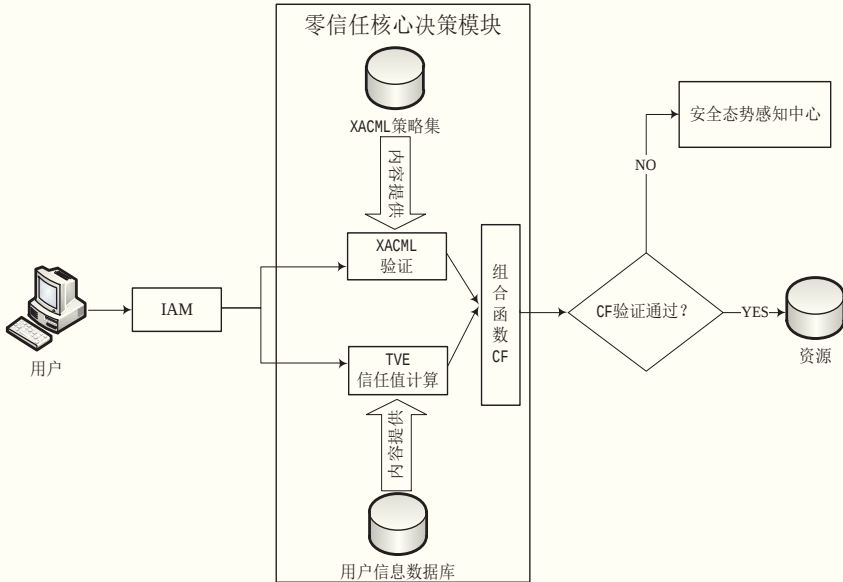


图 2 XACML-TV 评估引擎并行模型

2.1 属性数值化

XACML 主要基于属性的值和类型进行逻辑比较。若类型和数值种类复杂且不统一，所进行的匹配时间也会大幅延长，严重影响 XACML 的匹配效率。

基于 SM3 的属性数值转换图如表 1 所示，通过 SM3 算法，将杂凑的字符串转换为字节数组，更新 SM3 哈希对象获取杂凑值 hash_value，再将杂凑值 hash_value 转为字符串 hash_hex，最后通过类型转换 hash_hex 得到独一无二的整数来进行属性的唯一标识。

由于 SM3 得到的为 256bit 的哈希值，因此需要进行缩减且考虑哈希冲突，通过对 256 进行模运算并检验，保证其唯一性。通过这种方式得到的“数值型”属性，能够大幅降低因为字符串和不同种类属性带来的 XACML 匹配延迟，避免盲目取值造成的数值混淆与可能的网络攻击行为，同时为后续遍历搜索以及建立索引提供便利与依据。

表 1 基于 SM3 的属性数值转换图

属性	SM3 取模散列值
人力资源部	201
产品部	137
研发部	82
售后部	245

2.2 规则状态空间聚合与去冗余

XACML 具有多个集合及其属性，将这些属性进行笛卡尔乘积，能得到其状态规则空间，其中每个属性的最大值相乘，能够得到其最大状态规则空间 S_{max} ，对属于这个集合的任意属性及其值相乘，得到的空间 S ，有 $S \leq S_{max}$ 。可得任意两个空间 S_1 和 S_2 ，存在相交、覆盖和无关 3 种关系。

通过空间的角度，以企业部门为索引（3.1 节已进行属性数值化），建

立标准的 XACML 格式，存在 Subject、Resource、Action 共 3 个属性。状态空间简化表如表 2 所示。

表 2 状态空间简化表

状态空间简化表					
Rule	Rule ₁	Rule ₂	Rule ₃	Rule ₄	Rule ₅
Sub	1	1	1	2	2
Res	1	1	2	1	2
Act	1	4	3	4	4

Sub 为访问主体信任权限等级，Sub 越高则该访问主体信任权限等级越高；Res 为对应资源所属等级标签，Res 越高则为所需权限更高的深层资源；Act 为用户请求操作，数字 1，2，3，4 分别对应 Read、Create、Update、Delete 共 4 个权限。为进一步减少冗余，增强可读性，对 Sub 再建立索引，以不同信任等级为依据进行聚合。

首先，以 Sub=1 为例，对于表中 Sub 为 1 的 3 个访问策略，第一列与第二列空间存在覆盖关系，因为 $Sub_1=Sub_2, Res_1=Res_2$ ，但 $Act_1 < Act_2$ ，因此第一列规则是冗余，需要删去。Rule₂ 和 Rule₃ 存在相交关系，策略为 $\langle sub \rangle 1 \langle /sub \rangle, \langle res \rangle 1, 2 \langle /res \rangle, \langle act \rangle 3 \langle /act \rangle$ 以及 $\langle sub \rangle 1 \langle /sub \rangle, \langle res \rangle 1 \langle /res \rangle, \langle act \rangle 4 \langle /act \rangle$ ，此时引入 Rule₄，由于 $Sub_4 \neq 1$ ，此时聚合策略为 $\langle sub \rangle 1 \langle /sub \rangle, \langle res \rangle 1, 2 \langle /res \rangle, \langle act \rangle 3 \langle /act \rangle; \langle sub \rangle 1 \langle /sub \rangle, \langle res \rangle 1 \langle /res \rangle, \langle act \rangle 4 \langle /act \rangle$ 以及另一索引 $\langle sub \rangle 2 \langle /sub \rangle, \langle res \rangle 1 \langle /res \rangle, \langle act \rangle 4 \langle /act \rangle$ 。引入 Rule₅，存在覆盖 Rule₄ 的关系，整合策略为： $\langle sub \rangle 1 \langle /sub \rangle, \langle res \rangle 1, 2 \langle /res \rangle, \langle act \rangle 3 \langle /act \rangle; \langle sub \rangle 1 \langle /sub \rangle, \langle res \rangle 1 \langle /res \rangle, \langle act \rangle 4 \langle /act \rangle; \langle sub \rangle 2 \langle /sub \rangle, \langle res \rangle 1, 2 \langle /res \rangle, \langle act \rangle 4 \langle /act \rangle$ 。

将表 2 的策略依据规则状态空间关系进行规则整合，将原来 5 条规则，共计 $2 \times 2 \times 4 = 16$ 次比

对变为3条规则，共计 3×3 次=9次比对，整合效果明显，在该场景中理论提升达78%。

2.3 动态重排序

动态重排序是在聚合的基础上，引入优先级这一因素来提升常用规则的检索次序，以减少资源浪费、提升检索效率。优先级的设置可以通过分析用户历史数据来得到，依据不同等级的用户对不同等级资源执行不同操作的频率来进行设置。例如，如Sub=1的用户经常访问、修改或删除Res=1的资源，则提升 R_2 的规则优先级，使 $R_{2_prior} > R_{1_prior}$ 。通过设置优先级，能够在识别到对应Sub的用户访问时，优先匹配对应规则，提升匹配效率。

3 信任值的主客观赋权计算

XACML能够保证用户“去哪里”是否符合要求，而信任评估则能保证用户能否“去那里”，两者结合能够实现路径和过程安全。信任值计算方面则通过主客观结合的方法，让信任值兼具可

解释性和科学性，具有安全参考意义。

3.1 主客观赋权计算

过多的决策层因素会导致主客观矩阵检验、计算较慢以及打分存在理论偏差等问题，将各因素进行归纳与计算，得到网络属性、流量属性、应用层属性、访问情况属性、个人属性共五大因素的信任值。

在用户进入系统试图得到系统服务时，会通过层次分析法、熵值法对该用户五大因素下的各项决策层因子进行计算。得到熵值法以及AHP的权重结果后，将两者进行二次组合计算。主客观权重结果表如表3所示。

表3 主客观权重结果表

因素	熵值法权重 EM_i	AHP 权重 AHP_i
网络情况	0.28	0.15
流量情况	0.23	0.26
应用层情况	0.06	0.11
访问情况	0.23	0.19
个人属性	0.20	0.29

由于专家和企业有关人员对零信任架构有关因素熟悉情况不同，评估指标不同，进而导致主观与客观权重的重视程度也存在差异。引入主客观权重矩阵 W 、客观权重因子 α_1 、主观权重因子 α_2 ，分别于与 EM_i 、 AHP_i 构成的权重矩阵相乘，得到主客观结合的组合权重。计算公式如式(1)所示。

$$W = \alpha_1 EM^T + \alpha_2 AHP^T \tag{1}$$

客观权重 α_1 和主观权重 α_2 若采用加法或乘法的合成法组合赋权，存在过于呆板、可解释性低等问题，后者在两者数值差异较大时甚至会导致“倍增问题”。因此，选用基于博弈论的方法求解纳什均衡点。

为避免客观权重 α_1 和主观权重 α_2 在组合时出现冲突，如结果差异过大导致出现负值的情况，需在组合前通过距离函数进行一致化校验。计算公式如式(2)所示。

$$d(EM, AHP) = \sqrt{\frac{1}{2} \sum_{i=1}^q (EM_i - AHP_i)^2} \tag{2}$$

若 $0 \leq d(EM, AHP) \leq 1$ 则一致性校验通过，此时以求最小离差为目标，建立目标函数如式(3)所示。

$$f(x) = \min \left| \sum_{p=1}^n \alpha_p w_p^T - w_p \right|_2 \tag{3}$$

其中， $w_1=EM$ ， $w_2=AHP$ ， $n=2$ 。根据矩阵微分性质，将上式 $f(x)$ 等价变化为如式(4)所示的优化一阶导数条件的线性方程组。

$$\begin{bmatrix} EM \times EM^T & EM \times AHP^T \\ AHP \times EM^T & AHP \times AHP^T \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} = \begin{bmatrix} EM \times EM^T \\ AHP \times AHP^T \end{bmatrix} \tag{4}$$

得到客观权重 α_1 和主观权重 α_2 后，进行归一化处理，得 $\alpha_1^*=0.59$ ， $\alpha_2^*=0.41$ ，最后通过式(5)得组合赋权结果表(见表4)。

$$W = \alpha_1^* EM^T + \alpha_2^* AHP^T \tag{5}$$

3.2 组合函数 CF

在得到各个因素的组合权重之后，通过该权重与其对应安全状态的具体得分(如考虑正态分布的得分模式)相乘，得到不同主体的信任值

表4 组合赋权结果表

因素	组合赋权
网络情况	0.2267
流量情况	0.2423
应用层情况	0.0805
访问情况	0.2136
个人属性	0.2369

表5 组合函数 CF(TV, XD, RTV) 伪代码

组合函数 CF(TV, XD, RTV)
def CF(TV, XD, RTV):
if TV >= RTV:
if XD== "Permit":
return "Permit"
elif XD== "Deny":
return "Deny"
else:
return "Not Applicable"
else:
return "Deny"

TV，TV 越高则说明其所有用户中相对安全状态越好。

在并行的 XACML 和信任评估的系统中，TV 决定了用户在进入系统时是否为安全的状态，通过设计组合函数 $CF(TV, XD, RTV)$ ，能够综合考虑访问主体的安全程度、主体对客体关系的合规以及对客体的实时安全和等级评估。组合函数 $CF(TV, XD, RTV)$ 伪代码如表 5 所示。

XD 即 XACML DECISION，即 XACML 决策结果，结果表示为同意 Permit，拒绝 Deny 和不适用 Applicable。若该访问为不适用，则移交服务端处理并制定新规则。

RTV 即 Resource Trust Value，即资源要求信任值。零信任对整体安全提出了要求，即对网络中的任何事物都秉持“永不信任，持续验证”的工作信条，因此对客体即资源应定期持续、动态地进行安全评估。不同资源对应不同的 RTV，理论上资源重要程度越高，所需的安全级别也越高，需要及时且持续地调整其对应的 RTV 至合适的数值，保障资源安全。

4 实验结果与分析

4.1 XACML 优化效果

实验模拟 16G 内存，双核 CPU，在 Windows 10 的操作系统中，JRE 版本为 1.8.0。

将本文方法与 SunPDP 直接检索、Enterprise XACML 属性聚类以及规则聚类和重排序 3 种方法进行对比，测试集为某企业的访问规则集合。访问时间对比表如表 6 所示。

表 6 访问时间对比表 (ms)

策略集数 (条)	100	200	400	800
SunPDP	98.2	195.3	393.8	781.1
Enterprise XACML	70.3	133.7	249.4	448.4
规则聚类和重排序	57.4	97.6	168.7	298.1
本文	48.8	90.1	155.3	251.9

随着策略规则集的数量增多，后两者的“聚合 + 重排序”带来的效率提升逐渐突出。与规则聚类和重排序相比，由于空间、匹配过程以及属性数值化的多维优化，本文在 800 条的策略集合时，效率较“聚类 + 重排序”的方法提升了 15.5%，效果明显。

4.2 优化 XACML-TV 并行效果

遵循上节环境，本节分别以 XACML、TV、XACML-TV 以及优化 XACML-TV 模型对随机产生的相同请求在不同次数下进行处理时间的比对。处理时间对比表如表 7 所示。

当访问请求次数分别为 2 次和 32 次时，提升效率为 19% 和 22%，差距变大的原因是 XACML 的多维优化使其面临多次调用时，较未优化 XACML 的处理时间更为稳定。同时，优化 XACML-TV 模型较单个 XACML 或 TV 的处理时间差异较小，保证系统高安全性的同时，保障了高可用性。

结语

零信任作为一种新型网络安全架构，旨在改善传统网络模型的诸多缺点，现逐渐被广泛采纳和迁移。本文提出了一种可以实现的 XACML-TV 并行系统方案，并对 XACML 的策略制定、TV 的赋权计算分别进行

表 7 处理时间对比表 (ms)

访问请求次数	2	8	32
XACML	137.9	528.3	2040.4
TV	106.3	414.2	1649.2
XACML-TV	149.8	623.3	2337.7
优化 XACML-TV	121.3	455.7	1801.2

了优化，并结合国产商用密码进一步改进。实验证明优化并行模型在安全性、可用性上均得到保障，能够较好实现零信任网络安全架构。

引用

[1] Kindervag J.Zero Trust Network Architecture with John Kingdervag-video[EB/OL].[2020-05-31].https://www.paloaltonetworks.com/resources/videos/zero-trust.

[2] Rose S,Borchert O,Mitchell S, et al.Zero Trust Architecture [R].Gaithersburg:National Institute of Standards and Technology, 2020.

[3] 王雅哲,冯登国.一种XACML规则冲突及冗余分析方法[J].计算机学报,2009,32(3):516-530.

[4] Enterprise XACML[OL]. http://code.google.com/p/enterprise-iava-xacml/, 2008.

[5] Mazzoleni P,Crispo B,Sivasubramanian S,et al.XACML Policy Integration Algorithms[J].ACM Transactions on Privacy and Security,2008,11(1):4.

[6] 郑楷,田秀霞,卢官宇,等.基于聚类和重排序的XACML策略评估优化方法[J].计算机仿真,2022,39(10):519-525.

[7] Lamberger M,Mendel F. Higher-Order Differential Attack on Reduced SHA-256[J].IACR Cryptology ePrint Archive.2011(1): 37.