软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(9):3939−3940 [doi: 10.13328/j.cnki.jos.006880]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

AI 软件系统工程化技术与规范专题前言*

张 贺[1,2], 夏 鑫[3], 蒋振鸣[4], 祝立明[5], 李宣东[1,2]

[1](南京大学 软件学院, 江苏 南京 210093)

[2](计算机软件新技术国家重点实验室 (南京大学), 江苏 南京 210023)

[3](华为技术有限公司, 浙江 杭州 310007)

[4](Electrical Engineering & Computer Science, York University, Toronto M3J 1P3, Canada)

[5](Computer Science and Engineering, University of New South Wales, Sydney NSW 2015, Australia)

通信作者: 张贺, E-mail: hezhang@nju.edu.cn

中文引用格式: 张贺, 夏鑫, 蒋振鸣, 祝立明, 李宣东. AI软件系统工程化技术与规范专题前言. 软件学报, 2023, 34(9): 3939–3940. http://www.jos.org.cn/1000-9825/6880.htm

近年来, 人工智能产业的热度逐步提升, 市场规模持续扩大, 全球各行各业的组织机构都正在或试图通过人工智能对原有的产品和服务赋予新的能力. 最先进的人工智能系统正在迅速从实验室环境迁移到工业环境, 并主要以软件为承载形式渗透到社会应用的方方面面. 然而开发、测试和运维工业化的人工智能软件系统会遇到一些不同于传统软件系统的工程问题. 例如, 在基于人工智能的系统中, 规则和系统行为是从训练数据中推断出来的, 而不是被开发者编写的程序代码所定义; 人工智能系统的需求具有较大的不明确性; 人工智能系统的演化过程中需要关注不断变化的数据集和相关的基础设施; 人工智能系统开发和运维需要数据科学家和软件工程师的跨专业协作; 人工智能系统的开发面临伦理、道德和法律的约束, 且这些约束的更新速度正受到飞速发展的人工智能技术和产业的挑战. 如果不能及时解决这些挑战所带来的问题, 最终可能会开发出大量带有严重技术债务的糟糕的人工智能系统应用. 在这种局面下, 非常有必要探索面向开发和运维人工智能系统的软件工程理论、方法和实践, 以应对这一跨专业领域中, 数据科学家和软件工程师面临的新的软件工程挑战. 专题重点关注人工智能系统的软件工程挑战、技术探索、最佳实践、质量属性、工程规范等, 收录国内外在解决人工智能系统的软件设计、开发、测试、运维、重构、迁移等难题和挑战过程中所取得的理论、技术、实验等方面的创新性、突破性的高水平研究成果.

本专题采取公开征稿的方式, 共收到 14 篇投稿并通过了形式审查. 特约编辑邀请了 20 余位领域专家参与审稿, 每篇稿件至少邀请 2 位评审专家, 历时近 6 个月并经过两轮审稿. 共计 9 篇稿件通过第 1 轮评审, 并在 CCF 中国软件大会上进行了报告. 经过第 2 轮终审, 最终有 8 篇论文入选本专题.

《可信人工智能系统的质量属性与实现: 三级研究》关注于人工智能系统的可信性相关质量属性和实践的研究现状开展三级研究, 通过对 2012 年至 2022 年间发表的相关 34 项二级研究进行筛选、抽取、评价和整合, 提出一个全面系统的可信人工智能系统质量属性框架元模型, 识别了 21 种与可信性相关的质量属性及可信性度量方法和保障实践, 对未来可信 AI 系统领域的研究提供重要参考.

《面向智能计算框架的即时缺陷预测》基于通用的 14 个基本度量元建立智能计算框架的即时缺陷预测数据集, 增加了 LDA 主题模型来提取隐藏的语义特征, 通过 SHAP 对于模型的预测结果进行解释, 从而提高缺陷预测方法的透明性和可解释性.

《嵌入路网图模型的自动驾驶场景描述语言》面向自动驾驶这一人工智能重要应用领域, 提出一种能简洁描述场景路网结构的语言 SceneRoad 来扩展 Scenic 场景描述语言使其能够描述场景道路结构. 通过优化场景生成机制来生成多样化的静态场景, 并利用不同的模型分别在真实和仿真数据集上进行测试, 以验证其生成仿真数据的有效性.

《基于稀疏扰动的对抗样本生成方法》针对深度神经网络提出一种基于稀疏扰动的对抗样本生成方法, 能够依据重要性程度对扰动进行改进以跳出局部最优, 并对梯度值进行迭代排序以选择新增扰动, 最终实现稀疏且小幅扰动并成功进行对抗攻击.

* 收稿时间: 2023-01-19; jos 在线出版时间: 2023-01-19

《源码处理场景下人工智能系统鲁棒性验证方法》提出一种验证 AI 模型鲁棒性的方法 RVMHM, 针对以源码为输入的 AI 模型, 以漏洞预测为场景, 通过提取抽象语法树中的变量名, 并应用 MHM 源码攻击, 计算性能指标下降程度以评估模型鲁棒性.

《深度学习模型中的公平性研究》定义了基于输出标签和基于输出分布的两种个体公平率计算方法, 进一步提出一个提高模型个体公平性的算法, 通过余弦相似度计算样本之间的差异程度, 利用相似临界值筛选出满足条件的相似训练样本对, 并在真实数据集上进行了验证.

《TensorFlow 开源软件社区中贡献修订的实证研究》从 TensorFlow 开源软件社区中收集了拉请求 (pull-request, PR) 信息进行人工分析归类, 发现不同类型修正的关系, 并基于人工标注的修订数据集定量分析了不同修订类型的频率分布、次序分布以及关联关系, 以帮助 AI 开源实践者和研究者更好地理解修订过程, 并引导 PR 的审查和修订行为.

《智能运维的实践: 现状与标准化》对业界的智能化运维现状, 包括运用能力、评估标准等方面开展问卷调研, 在此基础上结合对国内外现行人工智能标准和智能运维标准的梳理, 提出智能运维的能力建设标准框架 AIOps-OSA, 对企业落地智能化运维系统提供指导.

本专题主要面向软件工程、人工智能、数据科学等多领域的研究人员和工程人员, 反映了我国学者在人工智能系统的软件工程领域的最新研究和实践进展. 感谢《软件学报》编委会、CCF 软件工程专委会与系统软件专委会对专题工作的指导和帮助, 感谢专题全体评审专家及时、耐心、细致的评审工作, 感谢踊跃投稿的所有作者. 希望本专题能够对国内面向人工智能系统的软件工程领域的科研工作有所促进.

张贺(1971－), 男, 博士, 南京大学教授, 博士生导师, CCF 高级会员. 主要研究领域为软件工程, 开发运维一体化, 软件研发效能, 软件安全, 经验及循证软件工程, 区块链.

夏鑫(1986－), 男, 博士, 华为软件工程应用技术实验室主任, 软件工程应用技术科学家和首席专家, CCF 专业会员. 主要研究领域为智能化软件工程, 软件仓库挖掘, 经验软件工程.

蒋振鸣(1981－), 男, 博士, 加拿大约克大学副教授. 研究兴趣在于软件工程和计算机系统, 特别是对性能工程、AI 工程、软件分析以及分布式系统的调试和监控方面有深入的研究.

祝立明(1975－), 男, 博士, 澳大利亚联邦科学与工业研究组织 (CSIRO) 软件与计算系统研究所所长, 新南威尔士大学教授. 研究领域包括: 软件工程, 软件架构, DevOps, 区块链, 人工智能系统, 分布式系统, 信息安全与隐私.

李宣东(1963－), 男, 博士, 南京大学教授, 博士生导师, 智能软件与工程学院院长, CCF 会士, CCF 软件工程专业委员会主任, 国家自然科学基金委员会信息科学部专家咨询委员会委员, 国务院学位委员会学科评议组成员 (软件工程). 主要教学与科研工作集中于复杂软件建模与分析、软件测试与验证.