软件所在开源软件合规性分析方面取得进展

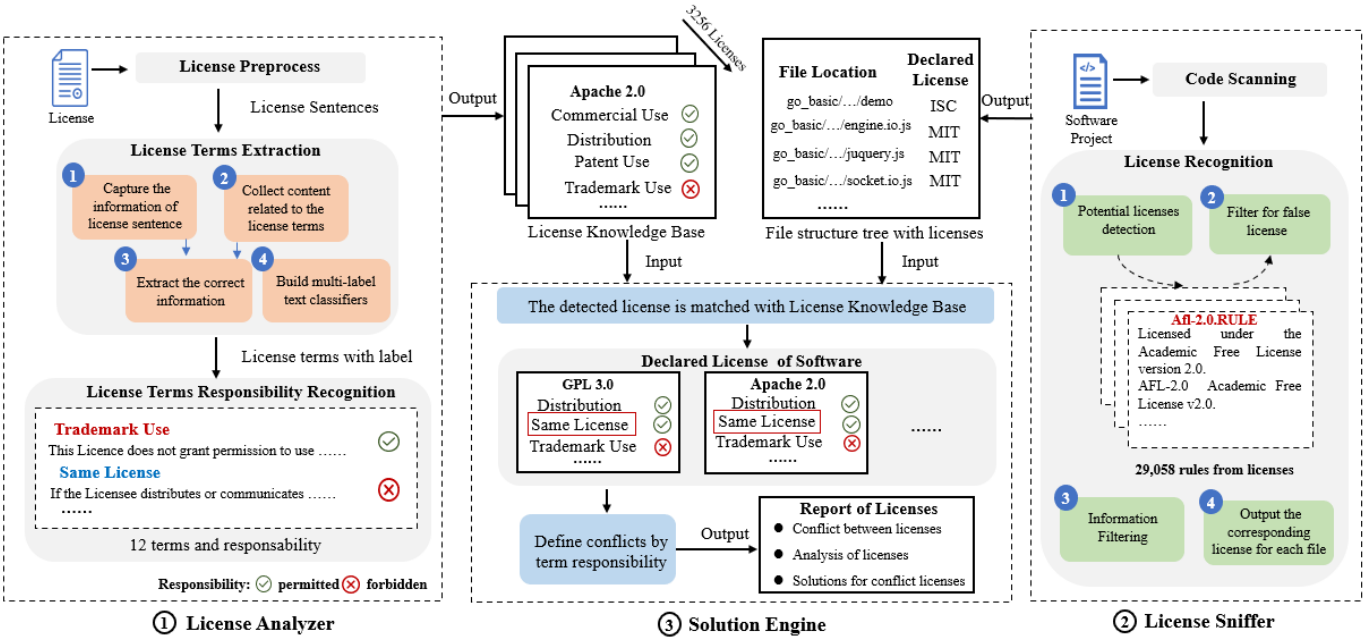
文章来源： | 发布时间：2023-02-06 | 【打印】 【关闭】

近日，中国科学院软件研究所智能软件研究中心团队基于“源图”开源软件供应链重大基础设施平台开展的开源许可证（Open Source License）合规性分析工作取得进展。该项研究提出了基于人工智能技术的开源软件许可证风险分析方法与工具，实现了许可证声明条款自动提取，条款倾向智能判断以及条款冲突精准识别。该成果论文“An Empirical Study of License Conflict in Free and Open Source Software”已被软件工程领域的国际顶级会议ICSE-SEIP 2023接收，第一作者为智能软件研究中心工程师崔星，通讯作者为吴敬征研究员。

近年来,开源软件的创新发展已经形成全球化趋势,在软件开发及应用领域发挥着重要作用。开源软件许可证规定了软件开源的使用权力与义务，从而保障开发者与使用者的合法利益。然而，每个开源软件及组件都可能通过不同许可证和不同条款来发布。在复杂的软件供应链中，当开源软件或组件所使用的许可证与整个项目所使用的许可证条款相互冲突时，将会存在许可证兼容性问题，从而导致开源软件的违规使用风险。

“源图”团队聚焦开源软件供应链中的许可证冲突问题，设计了一种检测开源许可证并分析冲突的自动化工具，通过自然语言处理技术构建了一个包含3256个开源许可证的冲突关系知识库，借助该知识库，实现软件许可证扫描、冲突行为识别，并为这些风险提供可行的消解方案。研究成果已经在“源图”开源软件供应链重大基础设施平台进行应用，目前已累计分析开源项目超过140万款，检测时长超过14,000小时，已发现超过24万个项目存在合规性风险。此外，该工具还支撑软件成分分析（SCA）、软件物料清单（SBOM）分析、OpenChain认证等应用，并在知识产权纠纷、企业软件许可分析、科研软件合规性研判等领域得到实践应用，有效管控了软件项目中的开源许可证风险。

“源图”开源软件供应链基础设施平台，旨在应对开源软件供应中的风险，突破软件领域关键核心技术，建设知识化的软件图谱、供应链安全分析、供应链集成推荐一体化设施，打造服务全球的开源代码知识图谱和开源软件供应链体系，保障软件供应安全和产业创新发展。目前，“源图”平台已在2022年11月发布2.0版本，累计发现超过80万个存在维护性风险的项目；24万个存在许可证冲突的项目；773 个被“投毒”成功的项目，其中已获得145个PyPI漏洞编号，12个Kernel漏洞编号。本次研究成果显著拓展了“源图”平台的能力，在开源合规分析上超越了国外同类竞品，可为开源项目全球范围的大规模推广应用提供合规性支撑。



许可证冲突分析工作流程

电话：86-10-62661012　传真：86-10-62562533　电子邮箱：info@iscas.ac.cn