

人工智能技术在网络信息安全中的应用研究

张宸煦¹, 张晓璇²

1. 中国电子口岸数据中心南京分中心, 江苏 南京 210019

2. 江苏易斯特电子口岸信息科技有限公司, 江苏 南京 210019

DOI: 10.61369/TACS.2026020027

摘 要 : 人工智能技术正深刻变革网络信息安全防护模式, 为应对复杂多变的网络威胁提供了全新手段。基于此, 本文深入探究了 AI 赋能软件自动化测试在网络信息安全中的作用、问题和策略, 旨在更好地揭示人工智能技术如何有效提升网络信息安全防护的效率与精准度, 为构建更加智能、高效、可靠的网络信息安全防护体系提供理论支持与实践参考。

关 键 词 : 人工智能技术; 网络信息安全; 软件自动化测试

Research on the Application of Artificial Intelligence Technology in Network Information Security

Zhang Chenxu¹, Zhang Xiaoxuan²

1.China E-PORT Information Data Center Nanjing Branch, Nanjing, Jiangsu 210019

2.Jiangsu Yisite E-Port Information Technology Co., Ltd., Nanjing, Jiangsu 210019

Abstract : Artificial intelligence technology is profoundly transforming the network information security protection model, providing a new means to address complex and ever-changing cyber threats. Based on this, this paper deeply explores the role, problems and strategies of AI-empowered software automated testing in network information security. It aims to better reveal how artificial intelligence technology can effectively improve the efficiency and accuracy of network information security protection, and provide theoretical support and practical reference for building a more intelligent, efficient and reliable network information security protection system.

Keywords : artificial intelligence technology; network information security; software automated testing

引言

《“十四五”国家信息化规划》的文件中明确指出加快数字化发展, 坚持技术创新和制度创新双轮驱动, 以数字经济引领现代产业体系建设, 有利于推动经济发展质量变革、效率变革、动力变革; 加快数字化发展, 推进国家治理体系和治理能力现代化, 打造共建共治共享社会治理格局, 有利于满足人民群众美好生活新期待; 加快数字化发展, 提升产业基础高级化、产业链现代化水平, 有助于补齐产业基础能力短板, 激发市场主体活力; 坚持合作共赢, 推动信息化对外开放水平向更大范围、更宽领域、更深层次拓展, 有利于支撑构建以国内大循环为主体、国内国际双循环相互促进的新发展格局^[1]。企业应该根据国家的政策性文件发展, 这样才能够更好地促进自身的发展。

一、AI 赋能软件自动化测试在网络信息安全中的作用

(一) 提升漏洞发现精准度

传统的软件测试对漏洞的查找依靠人工的经验和一成不变的漏洞规则, 而面对黑客不断翻新的网络攻击手段和五花八门的攻击方式, 漏洞查找仍然存在很多漏洞死角, 因此存在测试方面的问题。而通过 AI 技术赋能软件自动化测试, 借助机器学习, 进行对成千上万已知漏洞数据的分析学习, 不断训练, 直至掌握漏洞的规律和特征, 建立智能模型, 对软件代码进行扫描, 以点带

面, 不放过每一个细微的异常, 快速、精准地定位软件的安全漏洞死角, 避免人为测试的死角和疏漏, 为网络信息安全筑起坚实的防线^[2]。

(二) 增强安全测试全面性

网络信息安全是指软件在不同种类的攻击下都能够平稳地运行, 从而更好地保证结果的准确性。AI 赋能的软件自动化测试包括软件的各个功能模块、边界条件以及不同用户操作场景等多样化的测试案例, 只有进行多重方式的模拟和操作, 才能够更好地对软件进行全方位的测试, 从而保证软件面对攻击后有一定的抵抗能力^[3]。

二、AI 赋能软件自动化测试面临的问题

（一）数据质量与标注难题

AI 模型的训练依赖于大量高质量的数据，但在软件自动化测试领域，获取符合要求的数据并非易事^[4]。软件测试数据具有专业性和复杂性，不同类型软件的测试数据差异较大，且数据的收集和整理需要耗费大量资源。同时，数据的标注错误或不准确的数据会严重影响 AI 模型的训练效果，导致测试结果不准确，进而影响网络信息安全防护的可靠性。

（二）模型可解释性不足

深度神经网络等一些先进的 AI 模型，虽然能够更好地进行测试，但模型的结果和决策的过程存在着一些问题，这使测试人员即使测试到结果，也很难进行验证与分析，从而降低了测试的效率，阻碍了企业的发展进程^[5]。

（三）技术融合与协同障碍

AI 赋能的软件自动化测试涉及多种技术，如机器学习、自然语言处理、软件测试技术等。不同技术之间的融合和协同存在一定障碍。此外，各技术之间的协同工作机制也需要进一步完善，以确保它们能够高效地配合，共同完成软件自动化测试任务，否则会影响网络信息安全测试的效率和效果。

（四）人才短缺与技能更新压力

目前市场上这类人才相对短缺，企业难以招聘到合适的人员来开展相关工作。同时，随着 AI 技术的快速发展和软件安全需求的不断变化，测试人员需要不断学习和掌握新的知识和技能，以适应技术的发展和工作的要求^[6]。

三、AI 赋能软件自动化测试在网络信息安全中的策略

（一）优化数据管理与标注

一是，建立数据采集体系。通过软件测试公司的测试数据、软件开发公司的内部数据、安全研究机构的实验数据、第三方数据提供商的数据等多渠道、多途径建立广泛的软件测试数据来源，包括软件类型多样、环境多样、攻击手段多样的测试数据，涵盖软件安装、软件运行、软件遭受攻击、软件正常关闭等不同状态的数据。同时，加强数据清洗前处理工作，剔除或修正错误的数据，对数据进行标准化处理，统一数据的格式和编码方式，提高数据的一致性和质量^[7]。二是，数据标注规范。数据标注是机器学习模型训练的基础，因此，建立软件测试数据标注规范非常重要。首先，要建立详细的标注规范，定义标注的规则，避免标注的随意性。其次，采用多人标注和交叉校验的方式，保证标注结果的一致性。最后，建立标注质量稽核和培训机制，定期对标注人员进行稽核，对标注错误的人员进行培训，提高标注人员的标注水平^[8]。也可以采用半自动标注工具，提高标注效率。为人工智能模型训练提供高精度的数据支持，提高软件自动化测试在网络信息安全中的精确度。

（二）提升模型可解释性

选择可解释性较强的模型，如决策树、贝叶斯网络等，这些

模型拥有易于测试人员理解的决策规则和逻辑关系，优先选择此类模型。对于难以解释的模型（如深度学习模型），采用模型解释技术，如特征重要性，决策路径可视化等。特征重要性可以帮助测试人员理解模型在做出某决定时，哪些特征变量起到关键作用。决策路径可视化可以将模型的决策过程以图形的方式呈现出来，测试人员可以更加直观地了解模型如何根据输入的数据进行决策。另外，开展模型可解释性研究，探索新的模型解释方法和技术，提高 AI 模型在软件自动化测试中的可解释性，增加测试人员对模型结果的信任度，从而更好地保障网络信息安全。

（三）加强技术融合与协同

制定统一标准，促进技术融合。相关行业主管部门和行业组织牵头制定人工智能软件自动测试技术标准，明确不同技术之间的接口要求、数据格式等，实现不同技术的衔接和协作。建立沟通机制^[9]。建立机器学习、自然语言处理、软件测试等不同技术团队之间的沟通机制，定期举办技术交流会和培训活动，使不同技术团队的员工相互了解彼此的技术特点和工作流程，促进知识共享。融合技术平台。将不同技术融合到同一个平台，实现不同技术之间的数据共享和流程自动化，提高测试系统的开发和集成效率，降低技术融合难度，增强软件自动测试在网络信息安全中的整体效力^[10]。

（四）培养与引进复合型人才

企业积极与高等院校和职业院校、培训辅导机构开展深度合作，共同制定人才培养方案，在高等院校和职业院校中设置相关专业和课程，将软件测试和人工智能技术紧密结合，培养一批具有扎实软件测试和人工智能技术基础知识的专业人才。积极支持在职人员参加各种形式的培训和进修，邀请有关专家进行讲学和指导，介绍和讲解最新的 ai 技术、软件安全测试方法等，鼓励员工加强业余时间对人工智能技术知识的自我学习，以及参加相关学术交流活动，以开阔视野，拓宽思路。建立健全人才培养激励机制，对在相关领域做出突出贡献的使用人工智能技术进行软件自动化测试的员工，给予相应物质奖励以及提升职务级别，调动员工的积极性和学习的主动性。同时，积极引进外部高素质人才，尤其是具有人工智能和软件测试方面经验的高端人才，为企业引进新鲜血液，为使用人工智能技术进行软件自动化测试在网络信息安全中的应用提供人才保障。

四、人工智能技术在网络信息安全中的应用研究——以 AI 赋能软件自动化测试为例

（一）实验对象

本实验选取两款功能相似、代码量相近的企业级软件作为实验对象。实验组采用 AI 赋能的软件自动化测试方式，借助机器学习算法（如公式，为代码特征向量集）对软件进行全面测试。对照组则运用传统手工测试方法，由经验丰富的测试人员依据测试用例文档逐项执行测试。通过设置实验组与对照组，可清晰地对比 AI 赋能与传统测试在软件自动化测试中的差异，为评估 AI 技术在网络信息安全测试中的应用效果提供依据。

(二) 实验过程

1. 测试用例生成

实验组利用 AI 算法自动分析软件需求文档和代码结构，生成大量多样化的测试用例，数量公式为，其中是软件规模，是需求复杂度。对照组由测试人员根据经验和需求文档手动编写测试用例。

2. 测试执行

实验组将生成的测试用例输入到自动化测试框架中，由 AI 驱动的测试工具自动执行测试，并实时记录测试结果。对照组则由测试人员按照测试用例顺序手动操作软件进行测试，并记录测试情况。

3. 缺陷发现与分析

在测试过程中，实验组通过 AI 模型对测试结果进行实时分析，快速定位潜在缺陷，分析公式为，是测试结果数据，是历史缺陷数据。对照组由测试人员人工检查测试结果，判断是否存在缺陷。

(三) 实验结果

经过一段时间的实践，实践结果如表 1 所示。

对比维度	实验组（AI 赋能）	对照组（传统手工）
测试效率	完成测试时间短，效率提升 60%	完成测试时间长
缺陷发现数量	发现缺陷多 35%	发现缺陷相对较少
测试成本	成本降低 40%	成本较高

由此可见，AI 赋能可以有效提升测试效率与质量，降低成本，在软件测试领域具有较大应用价值。

五、结束语

在当今数字化浪潮下，人工智能技术于网络信息安全领域的应用研究意义深远且重大。通过本次研究，清晰地洞察到其能为网络信息安全带来高效威胁检测、精准风险预测等诸多优势。然而，挑战如技术融合难题、数据隐私保护等仍存在。未来，需持续深化研究，优化技术与安全策略，让人工智能更好地赋能网络信息安全，构建稳固的安全防线，护航数字世界稳健发展。

参考文献

[1] 杨戈, 蔡巧玉, 吕腾波. 构筑网络空间安全主动防御体系——记中国电子科技集团有限公司总师召集人 / 首席科学家中国电子科技网络信息安全有限公司总工程师饶志宏 [J]. 科学中国人, 2024, (12): 16–21.

[2] 漆昊晟. 高校网络信息安全体系建设实践和思考——以江西司法警官职业学院为例 [J]. 中国信息界, 2024, (08): 120–123.

[3] 吴钟灿, 冯展畅. 城市网络信息安全建设的影响因素与组态路径研究——基于 36 个重点城市的模糊集定性比较分析 [J]. 知识管理论坛, 2024, 9(03): 285–302.

[4] 高和平, 宋光信. 数字经济背景下基于 CIPP 模型的网络信息安全人才培养质量评估体系研究 [J]. 无线互联科技, 2024, 21(10): 125–128.

[5] 张晓航, 闫玺玺. 网络信息安全专业课程思政教学实践——以防火墙与入侵检测课程为例 [J]. 焦作大学学报, 2024, 38(02): 93–96.

[6] 朱斌勇. 大数据环境下高校校园网络信息安全隐患与防护措施 [J]. 网络安全技术与应用, 2024, (03): 76–78.

[7] 张君华. 全产业链导向渐进式复合应用型人才培养体系研究——以网络信息安全产业为例 [J]. 高教学刊, 2024, 10(07): 164–167.

[8] 钱祖良, 朱铁良. 大数据技术在计算机网络信息安全问题中的应用——评《计算机网络信息安全》[J]. 应用化工, 2024, 53(02): 511.

[9] 马威. 大学生网络信息安全意识教育现状分析及教育对策——以河南地区为例 [J]. 河南教育 (高等教育), 2023, (12): 31–32.

[10] 谭小伟. 基于人工智能的网络威胁情报分析与网络信息安全防护体系研究 [J]. 信息记录材料, 2023, 24(12): 59–61.