人工智能技术在计算机软件安全防护中的具体应用路径

张奕卉
中国信息通信研究院，北京 100191
DOI:10.61369/TACS.2025080043

摘　　要： 在信息处理与交互中，计算机软件发挥的作用不可替代。但是，其在日常应用中仍旧会面临各种各样的安全威胁，常见的有病毒入侵、黑客攻击、木马植入等，这除了对数据安全与信息隐私带来直接威胁外，更严重的情况下还可能造成经济损失甚至危及国家安全。而人工智能技术的应用能为计算机软件构筑自检测到评估再到响应的闭环防护体系，有利于整体提升计算机软件系统的安全性。基于此，本文将研究目光对准计算机软件安全防护，首先简单说明计算机软件安全的重要性，继而总结分析计算机软件常见的几大安全问题，根据问题，深入探究人工智能技术在计算机软件安全防护中的具体应用路径，希望能为保障计算机软件安全提供理论与实践层面的启发和参考，为计算机行业的健康、持续发展贡献微不足道的力量。

关 键 词： 人工智能技术；计算机软件；安全防护；应用路径

Specific Application Paths of Artificial Intelligence Technology in Computer Software Security Protection

Zhang Yihui
China Academy of Information and Communications Technology, Beijing 100191

Abstract: Computer software plays an irreplaceable role in information processing and interaction.However,it still faces various security threats in daily applications,such as virus intrusion,hacker attacks,and Trojan implantation.These threats not only pose direct risks to data security and information privacy but may also cause economic losses or even endanger national security in more serious cases.The application of artificial intelligence technology can build a closed-loop protection system for computer software,covering from self-detection and evaluation to response,which is conducive to improving the overall security of computer software systems.Based on this,this paper focuses on computer software security protection.It first briefly explains the importance of computer software security,then summarizes and analyzes several common security issues of computer software.According to these issues,it deeply explores the specific application paths of artificial intelligence technology in computer software security protection.It is hoped to provide theoretical and practical inspiration and reference for ensuring computer software security,and make a small contribution to the healthy and sustainable development of the computer industry.

Keywords: artificial intelligence technology; computer software; security protection; application paths

引言

无论是在日常工作还是学习中，计算机软件均扮演着不可替代的角色。尽管如此，计算机软件安全问题不容忽视，其除了威胁用户隐私、数据安全外，还可能造成不可挽回的经济损失，在现实中，无论对企业还是用户个人均带来了巨大困扰。研究表明，传统的防护技术在应对新型攻击方面已显得力不从心。可喜的是，人工智能技术在这方面的优势显著，效果突出，能保障整个计算机软件系统的安全性。因而，本文将研究目光对准人工智能技术在计算机软件安全防护中的具体应用，希望能有效应对日益复杂的安全威胁，为计算机软件安全防护提供新思路和新方法。

一、计算机软件安全的重要性

下面主要从国家以及企业和个人两个层面重点阐述计算机软件的重要性。第一，国家层面。在建设信息化国家的进程中，计算机软件发挥的作用不可小觑。当今时代，国家与国家间的竞争很大程度上是科技实力的彼此较量。计算机软件是否安全，

也可能直接影响整个国家的安全性。在国民经济各领域对信息化技术的依赖日益加深的背景下，软件的安全性成为关注的焦点。软件本身任何隐性及显性的漏洞、功能缺陷、任意代码篡改等均会给整个系统造成致命打击，继而可能会引发一系列不可逆转的连锁反应[1]。第二，企业及个人层面。众所周知，计算机的整体性能与软件的安全性息息相关。尤其在这个移动支付、电子商务等飞跃式发展的新时代，当前及未来，人民群众对计算机软件的依赖程度有增无减。全面提升企业及个人的计算机安全管理能力，一方面，是对企业负责的具体体现，另一方面，也是保障行业健康、有序发展的内在需求，当然，对保障企业及个人信息安全也发挥着积极作用，从而进一步促进数字经济的繁荣发展。

计算机软件安全标准，具体指的是保证计算机及其软件系统即便处于复杂网络环境中依然能在不被外来非法干扰的条件下有序且可靠运行的一系列准则与规范。第一，从用户的视角出发，计算机软件安全指的是使用过程既安全又可靠，同时，操作起来也比较便捷；第二，从计算机软件开发者而言，计算机软件安全指的是在满足终端用户安全需求的基础上保护计算机软件研发人员的知识产权，其核心目的为防止核心技术被窃取、仿冒等事件发生，同时，避免不法分子恶意利用软件系统牟取暴利[2,3]。

总而言之，计算机软件安全并非一个狭窄的概念，而是内涵丰富且具有综合性显著特征的宽泛概念，它除了包括系统运行安全外，还不断向软件自身及其开发权益不被侵害等更广阔的领域延伸。

二、计算机软件常见的安全问题分析

第一，病毒入侵。计算机病毒具有极强的传播性和自我复制能力，是恶意软件程序的典型代表。它对数据具有极强的破坏能力，同时，还能干扰系统的正常运行，也能窃取敏感信息。电子邮件附件、网络下载资源、移动存储介质等均是病毒的重要传播载体。一旦被激活，病毒可以立即执行诸如破坏用户数据、篡改正常程序功能、占用系统资源等一系列恶意操作，严重的情况下，可能致使系统瘫痪，甚至会造成服务中断[4]。最近几年，一系列新型病毒相继出现，它们不仅传播起来的隐蔽性更强，而且还具有较高的抗反病毒软件能力，对于计算机软件安全防护而言，面临着前所未有的挑战。第二，黑客攻击。其指的是攻击者利用非法手段强行访问计算机系统，目的是非法访问系统数据，窃取、篡改数据或破坏系统。黑客攻击对数据安全将造成直接威胁，同时，还会导致巨大的经济损失，甚至还会损坏名誉，严重威胁国家安全。第三，木马植入。木马程序指的是一种伪装成合法软件的恶意代码，其能在悄无声息中执行非法操作。木马的传播途径多样，比如诱导用户下载捆绑软件或者让他们点击恶意网络广告等。一旦木马被激活，攻击者便能远程操控被攻击者的计算机并执行一系列非法操作，常见的有监控屏幕、窃取敏感文件等[5]。现如今的木马兼具智能化、隐蔽化特征，这给计算机软安全防护带来了巨大的挑战。

三、人工智能技术在计算机软件安全防护中的具体应用

（一）基于时序神经网络的异常行为检测

时序神经网络在提升软件系统异常行为监测方面的优势显著。具体来讲，第一步，依托先进的词嵌入技术转化时序数据。常见的时序数据包括 API 访问日志、系统调用序列等。通过将其转化为128维的稠密特征向量，便于后续的深度特征学习。接着，捕捉时序依赖关系。模型可以采用双向 LSTM 结构分别从正向和逆向两个角度对序列的上下文信息进行编码。下一环节为特征提取。模型通过引入 MHA 机制对 LSTM 输出的时序特征进行多角度加权并设置8个并行计算的注意力头，之后，基于查询—键—值三元组运算方式计算权重。这里的权重具体指的是不同时间步特征分配差异化的重要性权重。动态滑动窗口技术被应用于处理长度不一的输入序列中[6,7]。根据序列复杂程度的差异性，动态调整窗口大小。时间步最小为50，最大为200。自适应调整的窗口大小有利于进一步增强模型的适应性，使其在面对多变的输入规模时依然有效。与此同时，层次化最大池化操作也至关重要。在提取特征环节，其能聚焦两个粒度（局部窗口和全局序列）进行，目的是实现由微观到宏观多尺度行为模式的捕捉。最后，异常监测模块发挥作用。其构成主要为全连接神经网络，主要负责特征映射，具体指的是将融合后的深层特征映射至异常评分空间，在此基础上，基于 S 型激活函数输出一个介于0到1之间的异常概率值，以此为依据便能准确判定系统状态。该模型的核心优势在于能精准且及时识别异常行为，具有极强的敏感度。

（二）基于集成学习的多层级风险评估

为了有效提升计算机软件应对安全风险的评估水平，增强评估的精准度，可以构建集成学习框架。该框架的核心为 GBDT 和 DNN，混合性特征显著。基于集成学习的多层级风险评估主要分为两个阶段，分别为特征提取阶段和模型融合阶段。在第一阶段，即特征提取阶段，首要步骤为提取并构建多源异构数据特征，其涵盖的维度多样，比如协议类型、数据包长度分布、流量突发性等。在进行该操作的同时，还需要同时提炼并解析语义特征，常见的包括用户操作序列模式、权限变更历史等。接着，严格按照标准处理特征数据，之后，利用 XGBoost 模型评估特征的重要性[8]。在第二阶段，即模型融合阶段，采用特征交叉策略，促进新特征与原始特征交互。其中，新特征由 GBDT 部分所生成的每一棵决策树的叶子节点输出。通过将新特征与原始特征融合随后输入下游 DNN，能为更深层次的表征学习奠基。之后，综合特征的重要性、时效性与环境相关性三个维度构建评分函数并形成最终的风险评估模块。该模块自动聚焦当前与威胁紧密相关的关键特征组合，通过输出介于0-100之间的连续风险评分值，为制定科学有效的安全决策提供更直观的依据[9]。

基于集成学习的多层级风险评估框架的训练方式以端—端为主。众所周知，软件系统的安全特征具有显著的差异性，而该

框架通过交替优化 GBDT 与 DNN 的参数，让模型的自适应特征更明显。研究表明，该框架对常见威胁具有精准且高效的识别能力，特别表现在对 DDoS 攻击、SQL 注入等高危安全威胁层面。

（三）基于深度强化学习的自适应防御决策

为了提升计算机软件安全防护的质量和效率，制定并实施自适应防御决策显得格外重要。其中，深度学习技术发挥的作用不可替代。通过构建基于深度强化学习的智能防御与决策系统，能进一步提升防护的有效性和时效性，提高响应速度，立即响应决策。该系统致力于将复杂的安全防护问题建模为马尔可夫决策过程，目的是实现序列化决策下的长期安全收益最大化。此模型的状态空间被定义为一个23维的复合特征向量，其涵盖多维统计指标，比如通用漏洞评分系统评分、实时攻击行为特征、网络流量等，这样，便能全面且客观地反映计算机软件系统的宏观安全态势[10]。除了状态空间外，此模型还涉及动作空间。该空间被定义为包含8类具体防御措施的动作集合，诸如补丁部署优先级调度、访问控制策略实时更新、网络流量清洗强度调节等。奖励函数由三个关键组件组成，分别为安全收益项、系统开销项和稳定性项。为了进一步提升深度学习的效率并确保其稳定性，系统还采用基于优先级采样的经验回放缓冲区机制，这样，模型就能优先学习过往具有更高价值的经验，从而加速优化和改进。值得一提的是，该系统引进了先进的动作屏蔽机制，目的是提高决策的可行性，通过自动过滤掉现下无法执行的防御行为，有效避免无效操作或者动作冲突等事件发生。最为关键的是，该系统还在状态编码中额外引入 LSTM 组件，目的是早期预测某些潜伏期的攻击行为并为制定科学有效的早期干预对策提供坚实有力的支持。

四、结语

由上文可知，计算机软件安全无论对国家还是对企业和个人均具有深远的影响。然而，伴随着计算机软件安全问题的日益复杂化、多元化，人工智能技术凭借其突出的优势在计算机软件安全防护中应用的前景广阔且效果突出。它的应用，对提升计算机软件安全防护的精准性、有效性、实时性并提升系统的自适应能力均具有深远影响。本文提出了基于人工智能技术的“检测—评估—响应”闭环防护体系，分别从基于时序神经网络的异常行为检测、基于集成学习的多层级风险评估、基于深度强化学习的自适应防御决策三个维度构建了由威胁感知到智能处理的完整技术链条。未来，希望有越来越多专业人士加入相关课题的研究行列，进一步探索人工智能技术在计算机软件安全防护领域应用的更多可能性，切实助推计算机行业向更高阶层迈进。

参考文献

[1] 杨永红 . 基于人工智能技术的计算机网络安全防御系统研究 [J]. 网络空间安全 ,2024,15(4):306-309.

[2] 张袖斌 , 谌颃 , 黄永健 . 生成式人工智能信息安全问题研究 [J]. 数码设计 ,2024(14):40-42.

[3] 钟宜宏 . 人工智能在计算机软件开发中的运用 [J]. 电子元器件与信息技术 ,2024,8(12):47-50.

[4] 王青峰 . 人工智能技术在网络安全防御中的应用研究 [J]. 网络安全技术与应用 ,2020(5):8-9.

[5] 何挺 . 计算机软件开发中安全技术的应用研究 [J]. 电脑校园 ,2019(7):3867-3868.

[6] 冯莉莉 . 大数据时代计算机软件技术的运用研究 [J]. 电子元器件与信息技术 ,2023,7(6):34-36,41.

[7] 江诗敏 . 浅谈计算机软件的安全问题及其防护 [J]. 信息记录材料 ,2023,24(8):62-64.

[8] 余伟 . 计算机软件安全问题及防御对策研究 [J]. 软件 ,2022,43(4):168-170.

[9] 叶伟 , 高丽芬 . 生成式人工智能在软件安全领域的应用分析 [J]. 网络空间安全 ,2024,15(2):82-86.

[10] 胡学龙 . 移动端人工智能软件的隐私保护与数据安全策略 [J]. 数码设计 ,2024(24):81-83.

