基于AI技术的软件供应链安全治理研究

丁汉栋
联通（山西）产业互联网有限公司　山西太原　030032

摘　要：信息化和数字化发展背景下，软件供应链逐渐成为各行业在数字化转型期间的关键技术手段，随着软件供应链在信息系统中的应用不断深入，软件的安全性也将对整个信息系统运行效果造成影响。为此，企业在数字化与信息化转型期间，需要将AI技术的软件供应链进行全面普及，加强软件安全治理工作的全面开展，从多个方面加强AI技术的应用效果。本文主要以AI技术为主，分析软件供应链安全治理的效果，期望能为后续AI技术在软件供应链安全治理中的应用提供参考。

关键词：AI技术；软件供应链；安全治理；治理策略

引言

软件供应链作为现代信息系统的核心框架，在开源软件的普及、第三方组件对复杂供应链网络的依赖，都让软件生态系统逐渐脆弱。根据目前的统计情况来看，开源软件的高危缺陷密度不断提升，其中Log4j2漏洞就导致全球超过6万个开源项目和70%以上企业面临系统远程命令执行风险。为加强软件供应链的安全治理，AI技术作为重塑软件供应链安全治理的全新给予，不仅可以通过机器学习模拟实时分析代码元数据、识别潜在漏洞，还能结合区块链技术确保软件在更新期间的完整性和可追溯性。因此，加强AI技术在软件供应链安全治理中的应用，也是今后软件供应链安全治理的主要方向。

一、AI技术在软件供应链安全治理中的应用现状

（一）威胁检测

1.恶意代码识别

AI技术通过机器学习算法，能够对软件代码进行静态和动态分析，经过对大量现存恶意软件代码特征模式的学习，AI模型可以针对供应链中潜在的恶意代码进行识别。目前部分安全厂商会利用深度学习算法，对代码的语言结构、函数调用关系等进行分析，从中对代码隐蔽恶意逻辑关系进行检测[1]。

2.异常行为监测

软件在运行的过程中，AI技术可以对软件运行的行为模式进行监测，通过对正常行为模式的学习，当软件出现异常的网络连接、文件访问或者系统调用的情况下，AI系统可以及时发出警报信息。利用AI技术的行为分析技术，检测软件是否在未经过授权的情况下，与外部服务器进行通信，减少软件供应链受到攻击后恶意软件师徒传输数据的情况。

（二）漏洞管理

1.漏洞预测

AI技术在应用期间可以针对历史漏洞数据、代码变更记录以及开发期间各项指标进行检测，预测软件中可能会出现漏洞的部位和类型，帮助软件开发团队及时对软件漏洞进行修复，提升软件使用的安全性。通过AI技术的机器学习模型对软件代码的复杂性、复用等情况进行分析，评估软件模块安全漏洞的风险点，确保软件保护的实际效果[2]。

2.自动化漏洞修复

部分AI系统在使用期间可以根据漏洞检测的情况，结合软件代码上下文以及编程规范，为软件开发人员提供自动化的漏洞修复建议和方向，加快漏洞修复的速度，减少在漏洞修复期间人为错误带来的影响。同时，在系统修复期间，结合自动化技术的使用，进一步为漏洞修复工作提供便利条件。

（三）供应链风险管理

1.供应链风险评估

AI技术在使用过程中，可以综合对软件供应链中的各项风险因素进行评估，包括供应商的信誉、历史安全信息、代码质量以及软件开发流程等，构建供应链风险评估模型。通过AI技术对各种因素的量化分析，评估软

作者简介：丁汉栋（1978—），男，汉族，陕西汉中人，研究生，研究领域包括工业互联网、能源互联网、网络安全、数字经济、5G+物联网、云计算、图计算、边缘计算、区块链、数字孪生、信息系统项目管理师（高级）等。

件供应商以及整个供应链的安全状况，帮助企业识别风险的合作活动和关键风险环节，自动生成风险防控措施。

2.风险情报分析

借助AI自然语言处理功能，能够对软件供应链中涵盖的大量风险情报数据进行实时分析和处理，从多个渠道中提取关键信息数据，识别最新的攻击趋势和恶意软件代码特征等，帮助软件供应链企业及时了解外部风险信息，加强风险防范[3]。

二、软件供应链安全治理的市场需求

（一）政策驱动

针对企业发展的需求，软件供应链的安全作为保障企业转型发展的关键，在目前对于软件供应链安全治理情况分析，各个国家针对软件供应链使用情况，出台相关的政策法规，对软件供应链安全治理工作提出明确的标准和要求。我国在“十四五”规划中强调供应链安全，按照企业发展情况，保证相关政策均能满足企业合规经营要求，加强软件供应链安全治理工作的投入。

（二）安全事故频发

软件供应链在目前的使用期间，受到网络攻击、自然灾害等多种意外因素的影响，经常会导致软件供应链断裂情况的产生，给企业带来较为严重的经济损失。企业在数字化和信息化转型发展期间，产品的研发将信息技术、软件技术等电子技术进行使用，如若不能加强对软件供应链的安全治理，都会导致企业经营停滞，引起严重经济损失。

（三）供应链环节复杂

随着现阶段信息技术与数字化技术的广泛使用，软件供应链呈现出复杂的发展趋势。在全球化发展的背景下，软件供应链需要涵盖多个参与方，在参与方信息阻滞、协调困难的影响下，供应链安全治理工作的难度不断提升，进一步加重安全风险的产生。这种情况下，企业在对软件进行使用期间，应当积极采用合理有效的手段，加强对软件供应链的保障，提升各个参与方的协同效果。

三、软件供应链安全治理的挑战

现阶段，供应链安全治理工作已经全面进入“高风险+强合规”的全新研究阶段。根据市场发展趋势来看，软件供应链在发展期间，依旧会面临四个方面的挑战，需要在软件开发中不断进行优化。

（一）开源代码风险不断提升

开源代码作为软件在现阶段开发期间的基本框架，开源代码的使用充分提升开发技术人员对软件开发的效率，让软件能够更快地进行开发和应用。但是，由于开发技术人员在对开源代码使用期间，对代码的安全性了解不够充分，导致开源代码的风险严重危害软件系统在使用期间的安全。目前，开源代码被攻击的情况不断增多，开源代码风险也已经成为软件供应链在应用期间需要应对的主要风险。

（二）应用程序编程接口风险

随着各类软件的普及应用，应用系统在近几年来也从单一的架构转变为低耦合、高内聚的网络服务框架。应用程序变成接口作为保障软件开发共享核心效果的关键，在目前各类应用系统中有着良好交互效果。数字化进程的快速推进，让应用程序变成接口的数量不断提升，在不安全因素下，应用程序编程接口的程序逻辑或者敏感数据，都会因为各类风险因素暴露在公共网络环境中，给软件供应链的安全带来严重危害。

（三）威胁和漏洞点持续增多

互联网技术的发展，让云计算、AI技术等多种新型数字化技术的使用逐渐广泛，为满足互联网技术使用需求，信息系统的形式也将产生明显转变。目前，信息系统包括微服务、无服务、程序变成接口等，都让各类数字化技术的创新得到基础条件。但是，在全新数字化技术使用期间，也会让软件在应用期间的漏洞和威胁不断提升。在对软件应用程序和应用服务使用期间，安全漏洞、供应商风险、企业自身漏洞等，都会给软件供应链安全带来巨大的影响。

（四）软件安全治理工作困难

软件供应链安全治理工作开展期间，企业并没有制定用户软件供应链安全治理相关的管理体系和机制内容，软件在开发、安全测试以及开源组件等多个环节中，风险问题的修正依旧缺少明确指导。同时，企业对于软件资产信息的掌握不够充分，在软件自身复杂性的特性下，企业在掌握软件信息方面存在较为明显的困难，在软件资产和新增软件资产信息采集期间，数据信息采集不全面、整合效果不理想，都会影响后续供应链安全治理工作的开展。除此之外，软件供应链安全漏洞在识别期间，由于软件的结构复杂，漏洞存在多样性的情况。加上多数软件在升级期间需要考虑兼容性的问题，由于软件不能兼容，导致的软件修复无法开展的问题格外明显。

四、AI技术的软件供应链安全治理策略

（一）AI技术下的安全检测与防护策略

1.漏洞扫描与修复

软件供应链中漏洞是造成供应链安全问题的主要因素，AI技术在使用期间能通过对代码和系统的分析，自动对软件供应链中潜在的安全风险进行识别，经过大数据技术的帮助，自动生成漏洞修复方案，借助自动化系统对漏洞进行修复。当软件供应链受到攻击后，AI技术可以通过智能安全防护引擎，提升漏洞检测和拦截的能

力，避免各类安全风险问题的产生。

2.恶意代码检测

AI技术通过深度学习算法和模式识别等技术，可以精准地对代码中存在的风险、异常行为进行判断，及时将潜在的安全漏洞和危害风险进行拦截。在AI技术的恶意代码检测系统中，可以保证对软件供应链的实时监测与分析，发现代码中潜在恶意行为，提供精准有效的修复建议。在AI技术的帮助下，不仅可以全面提升恶意代码检测的精确和有效，还能为软件供应链的安全提供全面保障。

3.入侵检测与防御

在软件供应链安全治理工作的分析期间，入侵行为作为安全风险的常见方式。AI技术通过对网络流量和数据的分析，及时发现在互联网运行期间存在的网络攻击现象，加强对入侵攻击的防御力度。在AI技术的入侵检测系统中，可以精准捕获和分析网络中存在的异常数据，加强对异常数据的拦截分析，提升入侵检测的精准和有效，为软件供应链的安全提供保障。

（二）风险情报与预警机制建立

1.加强数据整理

AI技术自身具备较为强大的数据收集统计与分析能力，借助AI技术对网络流量信息、恶意软件行为等多源数据的整合，经过深度学习和机器学习算法，数据可以转变为具有实际价值的风险情报，为后续供应链安全治理提供识别、响应以及评估的基础需求。

2.建立预警机制

AI技术在对各项风险数据的整合分析后，可以根据数据情报的分析结果，实时预警可能会出现的软件供应链入侵攻击时间。在预警机制建立的过程中，应当优先对预警阈值和预警规则进行确定，确保后续AI技术使用期间可以及时对异常行为进行捕获，快速发出预警信息，有效防止因为入侵攻击引起的安全问题，保障软件供应链的安全。

（三）开源软件的安全治理策略

1.创新开源软件安全技术

使用“揭榜挂帅”的方式加强对开源软件安全检测研发的支持，对开源软件中存在的风险进行保障，重点游湖代码库、指纹库、组件库等基础资源库，确保能够对开源软件安全检测、代码质量评估、许可证风险等因素进行识别。同时，在安全技术创新期间，要针对开源供应链的物料清单进行风险把控，通过在关键基础数据库中的风险把控，减少安全风险问题的产生。

2.建立开源软件安全标准

为进一步加强开源软件风险安全治理的效果，应当全面推进开源软件评估、应用以及管理等工作的开展，适当更新我国相关标准，建立动态化工作机制。同时，建立国际级、行业级软件的安全风险分析示范平台，积极引入AI技术，保障安全风险识别工作更加标准，提升软件供应链安全风险的识别效果。

五、AI技术在软件供应链安全治理的发展

（一）深度学习的应用

深度学习作为AI技术使用期间的关键技术方式，在软件供应链安全治理工作中，通过AI的深度学习方法，对软件供应链进行自动化监控与监测，提升软件供应链安全治理的效率和效果。同时，深度学习算法可以对开源代码、二进制文件等复杂数据展开深度解析，精准识别文化或者代码中潜在风险。此外，深度学习算法还能将传统静态分析与动态分析结合，加强对软件供应链的全面识别和监控，为软件供应链安全治理工作提供有力支撑。

（二）跨领域融合的应用

跨领域融合主要是将AI技术与其余多项技术融合，共同为提升软件供应链安全治理效果提供保障，积极应对安全治理期间存在的各项问题。在跨领域融合期间需要借鉴国际先进的技术经验，加强对软件供应链安全风险的监控与调查，通过技术标准的修订，为我国软件供应链安全治理工作提供有效支持。

结束语

软件供应链安全治理期间，加强对AI技术的使用，是促进安全治理工作数字化与信息化转型的关键。在本次研究工作开展期间，结合目前市场对软件供应链安全治理的需求，分析软件供应链安全治理中存在的挑战，制定AI技术的使用策略，积极应对开源代码风险造成的危害，通过对AI技术的使用，及时识别风险和漏洞，降低软件供应链中的安全漏洞和风险，建立预警机制后加快风险和漏洞的识别，以AI技术为基础，将软件供应链安全治理从“被动”转向“主动”，进一步推动我国AI技术的使用。

参考文献

[1]辛晓华，郭昕竺，许智鑫，赵娆.推动我国开源供应链安全保障体系建设的风险挑战与对策建议[J].数字化转型，2025，2（06）：63-68.

[2]沈滨，柳雪雅.数字赋能跨境电商供应链发展路径研究——SHEIN案例[J].上海管理科学，2025，47（03）：59-71.

[3]高铁林，孙淼.基于CiteSpace的供应链金融文献可视化分析[J].物流研究，2025，（03）：41-46.