The Application of Artificial Intelligence in Network Security Operation and Maintenance Services in the New Era

Bin Yuan

China Aerospace Changchun Control Technology Co., Ltd., Changchun, Jilin, 130000, China

Abstract

The Internet age, artificial intelligence technology, cloud computing technology in the network security operations services played a more and more important role, can realize the automation of network data security, automatic repair network vulnerabilities, intelligent prediction and prevention, network threat to ensure the safety of the network operation, reduce network information security threats, avoid network risk of economic losses to enterprise users, for the overall network security operational service level to provide enhanced technical support. This paper mainly analyzes the key points of the application of artificial intelligence in network security operation and maintenance services in the new era, so as to further improve the protection effect of network security operation and maintenance, reduce the occurrence probability of network security incidents, and optimize the service quality of network users.

Keywords

new era; AI; network security; operation maintenance services

新时代下人工智能在网络安全运维服务中的相关运用

袁彬

中国航发长春控制科技有限公司，中国·吉林 长春 130000

摘　要

互联网时代，人工智能技术、云计算技术等在网络安全运维服务中发挥了越来越重要的作用，可以实现网络数据安全的自动化识别，自动修复网漏洞，对网络威胁智能预测和防范，从而保障网络运行安全，减少网络信息安全威胁，避免网络风险对企业用户造成的经济损失，为整体网络安全运维服务水平的提升提供强化的技术支撑。论文主要对新时代下人工智能在网络安全运维服务中的运用要点进行分析，从而进一步提升网络安全运维防护效果，减少网络安全事件的发生几率，优化网络用户服务质量。

关键词

新时代；人工智能；网络安全；运维服务

1 引言

随着互联网计算机技术的发展，网络安全受到越来越复杂的威胁，如网络漏洞、网络威胁、数据安全、隐私安全等，加大了网络风险事件的发生概率，对企业造成极大的经济损失。基于此，需要对人工智能技术进行优化应用，构建智能化网络安全运维管理系统，进一步提升网络安全运维服务质量，优化网络安全运行环境。

2 网络安全运维服务内容

2.1 健康检测

为了保障网络系统安全，需要有效控制系统故障概率，并延长系统使用时间，在具体实施中需要对系统设备、业务系统的健康状态进行全面性检测，并对系统调配、流量耗用、系统运行状态等安全信息进行全方位搜集，并实现用户系统安全检测的常态化，以便对系统运转情况进行动态了解 [1]。

2.2 安全事件审计

随着互联网技术的发展，网络安全事件逐渐增多，且呈现复杂化、多样化趋势，因此开发了大量的防火墙、IDS、VPN 等网络安全设备，产生大量日志数据，导致网络拥堵现象。基于此，需要持续化搜集网络安全日志，并优化安全审计，完善安全评估。

2.3 网络行为审计

通过该服务的开展，能够对网络用户群体、网络设备配置等情况进行全面审计，尤其可以对网络应用历史进行掌握，同时结合网络运行行为的各类数据，实现网络环境的精准、有效优化，全方位解读用户行为，以此为依据提供动态滑动网络服务。在审计工作中，一旦发现违规行为，需要进

【作者简介】袁彬（1989–），男，中国吉林榆树人，本科，工程师，从事网络安全研究。

行记录，方便事后追查和取证。

2.4 监控与分析

该项内容主要是对网络资源安全进行管理和监控，并对海量网络数据进行深度挖掘，对不同事件的相关性进行构建，并采取针对性的安全监管措施，实现集中管控和智能化分析，实现统一监控，并对网络用户安全风险隐患进行预警处置，保障运维安全 [2]。

2.5 终端安全监控与策略完善

在现代化互联网技术的发展背景下，信息技术逐渐普及，网络用户越来越多，导致网络风险加大，加大了网络安全运维难度。当前企业网络安全监管不到位、病毒库滞后性等缺陷问题，会引起盗号、随意接入网络等安全风险，非常不利于企业网络安全，甚至导致机密信息数据被盗取，对企业造成极大的经济损失。因此，要对人工智能技术进行优化应用，对用户终端安全进行实时监测，并优化安全监管策略，保障主体业务安全。

3 智能化网络安全运维架构

人工智能在网络安全运维服务中的应用架构如图 1 所示。其中，涉及基础层、技术层、应用层。基础层属于核心层，具有计算能力、数据资源等功能，能够进行数据获取、分析和处理；技术层涉及算法、模型和知识库，能够提取数据特征，并构建数据模型，实现模型评估与训练；应用层，即实现人工智能技术与网络安全服务的相互联合，提升运维服务质量 [3]。

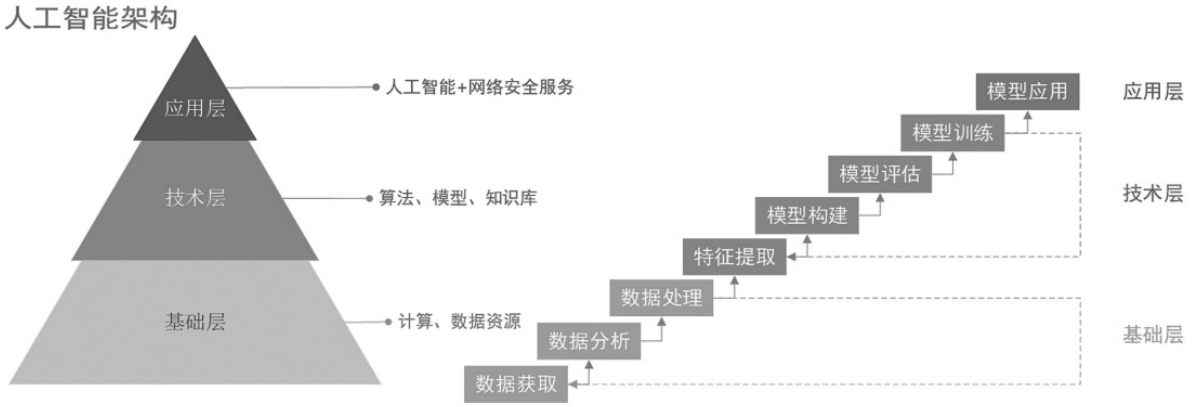

图 1 网络安全运维中的人工智能架构

在人工智能技术支持下，能够利用云加载计算单元，实现中心化运维管理，进一步提升网络安全运维服务质量。其中，涉及事前、事中、事后三个环节，确保人工智能技术能够充分渗透到网络安全运维服务的全过程，构建智慧化安全运维体系，如表 1 所示。

表 1 网络安全运维服务体系架构

网络安全运维阶段	具体事项
事前检测	配置基线、资产态势、漏洞检测、威胁分析
事中运维	安全监控、故障排查、数据备份、异常响应、安全态势
事后分析	日志审计、追踪溯源、安全分析、安全预测

①数据资产态势感知，随着互联网技术的发展，企业日常运营生产中形成的数据量呈现增长趋势，加大了数据处理压力。基于此，为了提升信息数据利用价值，要对 人工智能技术进行优化应用，构建安全数据学习系统，对各类数据综合性采集，在此基础上，形成安全数据态势感知平台，以便对其动态监测，保障安全产品的优化布局。此外，还需要有效提升网络弹性功能，以便对网络安全数据进行动态化分析，精准分类安全报警信息，划分优先级，采取有效性、针对性的处理措施，构建多层次安全报告，保障企业安全管理水平的提高。

②针对网络运维现状，需要对防火墙、IDS 等技术进行优化应用，以便对 APT 高级持续威胁进行积极应对，避免对企业系统运行安全稳定造成威胁。此外，由于 APT 攻击存在一定的隐蔽性，难以进行有效性防控，需要利用人工智能技术，实现各类流量数据的有效性汇集分析，并深度挖掘，掌握攻击者线索。

③软件自动核查，针对企业开源代码的完整性风险，需要利用人工智能技术，全方位识别代码错误，有效控制代码漏洞数量，并进一步提升软硬件防御能力，强化企业对海量代码的分析能力。

④系统动态加固，针对基础设施面临的攻击问题，需要对人工智能技术进行优化应用，即通过自动识别技术，对系统、软件运行中出现的漏洞等进行全方位检测，自动生成补丁程序，并对其持续性修复，强化系统自动防御能力，强化系统加固效果 [4]。

⑤异常动态监测，随着网络技术的发展，网络攻击方式逐渐向多样化、复杂化、动态化、不确定性方向发展，加大了安全防护工作压力。因此，要利用人工智能技术的机器学习功能，在专业算法支持下，对历史数据进行收集分析，构建数据模型，对网络安全事件进行持续性训练、学习，以

便了解运维服务人员的数据需求，为其提供精准情报信息，以便提升响应速度，强化应急处置，减少网络攻击、异常事件造成的损失。

4 新时代人工智能在网络安全运维服务中的应用要点

4.1 自动化漏洞扫描与修复

在网络安全运维服务中，需要对人工智能技术进行优化应用，以便对网络漏洞进行自动化扫描和快速修复，从而强化网络安全防护能力。在具体应用中，需要在人工智能技术支持下，引进多元化的漏洞扫描工具、漏洞评估技术等，实现网络系统、应用程序漏洞的全方位检测，并加快对网络安全事件的响应速度。在机器学习、自然语言处理技术的辅助作用下，能够实现系统漏洞的定期扫描，并对海量漏洞数据全面性分析，并联合大数据技术深度挖掘数据内在关系，及时发现潜在的漏洞风险，并总结漏洞特征、规律，以便对系统漏洞进行精准预测，自动生成修复动作，减少漏洞风险问题的出现几率。自动化漏洞扫描与修复技术具有较强的持续学习和优化能力，能够对历史漏洞数据进行持续性汇总分析，进一步提升系统对漏洞的识别率，并完成自我进化，实现系统漏洞的高效性扫描和修复，保障企业网络安全。

4.2 智能化威胁检测与预警

在人工智能技术支持下，能够对网络流量、系统日志、威胁情报等海量数据进行实时监测，并对可能存在的网络威胁进行全面识别，分析潜在的网络攻击行为，为网络安全防范提供保障。在具体实施中，通过基于深度学习的安全威胁识别技术，对海量网络数据进行训练和学习，构建威胁识别模型，并对异常行为类型进行精准识别，实现潜在威胁的精准检测，并第一时间提取攻击源，形成封堵攻击源的指令，从而对网络攻击行为进行积极响应和防范。通过智能威胁检测和预测技术的应用，能够在机器学习、深度学习算法基础上，对海量数据进行汇集和分析，并提炼特征，利用模式识别、预测技术，对网络安全区域进行动态、精准分析，明确可能出现的攻击事件，保障企业网络安全，减少企业经济损失。此外，该技术还能够对社交媒体、电子邮件等网络数据进行全面性收集和识别，以便对威胁情报进行全方位掌握，强化网络安全监测，进度，进一步保障企业网络安全[5]。此外，在自然语言处理技术的支持下，能够智能化分析文本数据，对可能出现的攻击行为进行精准识别，并对数据内在价值进行深度挖掘，以便对网络钓鱼、勒索软件、恶意软件等威胁进行全面性识别，提出针对性的防范方案。

4.3 隐私保护和数据安全

互联网具有开放性特征，且网络攻击手段逐渐升级，人们数据、隐私安全受到严重威胁，对安全事件响应方法提出了更高的要求。新时代，在网络安全运维服务中引入人工智能技术，如可以利用加密技术、差分隐私技术等进行融合应用，对网络安全风险进行快速识别，并智能化分析风险原因，提出针对性的处置措施，保障网络安全。在具体操作中，要利用深度学习技术，对安全事件进行自动识别，并对其进行精准分类，以便进行快速、针对性响应；利用强化学习技术，形成智能决策系统，同时实现安全事件的智能化分析，有效控制误报率；在差分隐私技术应用中，能够对网络上海量数据进行汇总分析，并精准计算，从而保障用户隐私安全，避免出现信息泄露现象；加密技术的应用，可以利用安全多方计算技术，可以在保障用户私密数据安全的基础上，确保若干个参与者协同计算相应的函数，强化数据共享；同态加密技术的应用，能够在保障数据安全的基础上实现各类数据智能化计算，防护数据安全。在未来发展中，要不断优化算法和模型，保障安全事件的智能化、准确性响应，强化数据安全隐私保护技术，保障安全事件响应和处置工作的智能化开展。

5 结语

综上所述，为了提升企业网络安全运维服务水平，需要对人工智能技术进行优化应用，以便自动识别网络漏洞、智能检测网络威胁、加快安全事件响应速度，强化网络安全防护能力，真正实现网络安全运维管理工作的智能化、高效化，强化降本增效。

参考文献

[1] 宋焱宏.一种基于人工智能的网络安全智能化运维技术解决方案[J].电脑知识与技术,2024,20(6):74-76.

[2] 杨启航.人工智能在网络安全运维服务中的运用研究[C]//中国土木工程学会燃气分会,《煤气与热力》杂志社有限公司.中国燃气运营与安全研讨会(第十一届)暨中国土木工程学会燃气分会2021年学术年会论文集(下册).重庆燃气集团股份有限公司,2021:6.

[3] 方雪琴,符方权,张嘉俊.浅析人工智能技术在电力企业网络安全运维中的应用[J].网络安全技术与应用,2021(3):104-106.

[4] 金景峰.人工智能在网络安全运维服务中的运用研究[J].河南科技,2020,39(25):21-23.

[5] 周利均.人工智能在网络安全运维服务中的应用[J].通信技术,2020,53(2):521-524.