人工智能在大数据网络安全防御技术中的应用探讨

平寒
山东职业学院，山东 济南 250104

DOI: 10.61369/TACS.2026020022

摘　　要： 随着数字化进程的加快，网络空间所承载的数据量呈指数级增长，大数据环境在推动价值创造的同时，也成了 APT、零日漏洞攻击等复杂网络攻击的主要阵地。传统的基于规则、特征签名的安全防御技术，在处理海量、多源、高速动态数据的时候，存在滞后、被动、效率低下的缺点。人工智能技术，尤其是机器学习、深度学习和自然语言处理等，因为拥有很强的模式识别、异常检测和预测分析的能力，给创建主动、智能、自适应的新一代网络安全防御体系赋予了关键推动力。本文对人工智能技术在大数据网络安全防御中的价值以及具体策略做系统的论述，分析人工智能的应用价值，最后总结目前的应用问题以及未来的预测。

关 键 词： 人工智能；大数据；网络安全防御

Discussion on the Application of Artificial Intelligence in Big Data Cybersecurity Defense Technology

Ping Han
Shandong Polytechnic, Jinan, Shandong 250104

Abstract: With the acceleration of the digital process, the amount of data carried in cyberspace has grown exponentially. While the big data environment promotes value creation, it has also become a major battleground for complex cyber attacks such as APT and zero-day vulnerability attacks. Traditional security defense technologies based on rules and signature-based detection have shortcomings of lag, passivity, and low efficiency when dealing with massive, multi-source, and high-speed dynamic data. Artificial intelligence technologies, especially machine learning, deep learning, and natural language processing, have strong capabilities in pattern recognition, anomaly detection, and predictive analysis, providing a key driving force for building a new generation of active, intelligent, and adaptive cybersecurity defense systems. This paper systematically discusses the value and specific strategies of artificial intelligence technologies in big data cybersecurity defense, analyzes their application value, and finally summarizes the current application problems and future prospects.

Keywords: artificial intelligence; big data; cybersecurity defense

引言

目前人类社会已经进入了一个由数据成为最主要生产要素的数字经济时代。云计算、物联网、5G 这些技术发展起来之后，全世界的数据量飞速增加，网络空间也由原来的孤立的环境变成了一个十分复杂的“大数据”世界。它给各行各业的数字化转型赋能的同时，也使它遭遇着前所未有的安全威胁，因为它的攻击面大大增广，其攻击手段变得越发专业化、隐匿化以及自动，由此引发了对关键基础设施发动高级网络攻击的恶意行为。面对 PB 级别的海量安全数据，依靠安全专家的人工分析或者传统的基于已知特征的匹配防御方法，就显得如同大海捞针一般，很难实现对潜藏的威胁的及时、准确的发现，并且也很难预知未知的攻击。在这样一种背景之下，人工智能技术的出现给破解大数据环境下网络安全防御困境提供新的可能。人工智能，特别是机器学习 (ML) 和深度学习 (DL)，可以从大量的、高维的、非结构化的安全大数据中自动地学习、抽取复杂的非线性关系以及深层次的模式，并且有超乎人类的持续学习、进化的能力。其主要的价值就是可以对未知的威胁、异常的行为进行智能的感知，可以实现安全态势的实时的评价、可视化、自动化的调查和响应，还可以对未来的攻击趋势做出预测。

一、人工智能在大数据网络安全防御技术中的应用价值

（一）增强威胁检测与识别的精准性与实时性

传统基于签名的检测技术（IDS/IPS）对已经存在的攻击很有效，但是对于零日攻击、变种恶意软件和内部威胁是无能为力的 [1]。人工智能，尤其是无监督学习以及深度学习模型，可以利用大量的网络流量，系统日志和用户行为数据建立基线模型，从而对异常做出自动识别。利用循环神经网络（RNN）、长短期记忆

网络（LSTM）来分析时序性网络连接序列，可以较好地检测出隐蔽的C2通信和数据外泄行为；利用深度学习模型对文件静态特征或者动态沙箱行为进行分析，可以做到比较高的准确率识别未知恶意软件。以行为分析为基础的检测方式大大提高了发现未知威胁、低频攻击的能力，将检测时间由原来的一两个小时或一天减少到了几秒钟，达到了即时检测的目的[2]。

（二）实现宏观与微观相结合的安全态势感知

大数据环境下安全事件会被分散到不同的设备、不同的日志中，不能形成一个全局的视角。人工智能技术可以对网络、终端、应用、云环境等各种不同来源的、不同的安全数据进行分析和融合，从中挖掘出隐藏的安全信息[3]。使用知识图谱技术可以建立实体（IP、域名、用户、资产等）间的复杂关系网络，清楚地展现攻击链的传递途径；用机器学习去剖析历史攻击数据，能对各个资产以及各个地域所面对的风险高低作出量化评定。因此安全运维人员可以对整个系统的安全状况有一个宏观的认识，能够了解攻击者使用的战术、技术以及程序，从而实现由看到一个告警到理解整个攻击过程的飞跃，给决策提供有力的支持[4]。

（三）驱动安全响应的自动化与智能化

面对大量的告警，传统的依靠人工进行研判和响应的方式已经不能满足需要了，而且还会因为疲劳而产生错误的判断。以人工智能为依托的SOAR平台把安全的操作步骤实现自动化地配置和部署，达到自动化的目的。AI模型对告警可以做智能的聚合、去重、排序，从而剔除大量误报、低价值告警[5]。利用剧本（Playbook）、机器学习，可以对威胁信息进行初步调查，也可以直接对感染主机、阻断恶意IP实施自动遏制和修复。既能把安全团队从重复性劳动里解救出来，去从事那些重要的、复杂的安全威胁，又能使平均响应时间（MTTR）由几小时降到几分钟内，有效地缩减了攻击的波及范围。

二、人工智能在大数据网络安全防御技术中的应用策略

（一）构建基于机器学习/深度学习的多层次异常检测模型

网络层异常流量智能检测要充分用上无监督学习算法的优点，比如利用孤立森林，自编码器这些先进的模型，来对网络环境里产生出来的NetFlow数据以及全流量元信息实施深入的建模并开展连续的学习工作[6]。采用此种方式可以很好地识别出分布式拒绝服务(DDoS)攻击、隐藏的端口扫描活动、攻击者在网络内部横向移动渗透所引发的一系列异常流量行为模式，从而达到对网络层威胁主动感知的目的。

用户和实体行为深度分析(UEBA)，使用有监督学习和无监督学习相结合的方法论，给信息系统中每一个用户账号和重要的实体创建出动态且细颗粒度的正常行为基线图谱。通过对用户各种行为日志序列进行持续采集和分析，即用户登录的时间偏好，位置变化，资源使用情况，对敏感数据操作的过程等，并用时序分析方法进行建模。此系统可以对账号凭证被非法劫持、内部授权人员的恶意违规操作、企图窃取核心数据资产等内部安全风险进行准确的识别，从“主体”的角度来进行风险的发现[7]。

文件与内容安全深度研判，用前沿深度学习模型技术，卷积神经网络(CNN)、循环神经网络(RNN)对文件自身静态字节序列编码特征或者沙箱环境下动态执行行为序列做多层次、自动化的特征提取与语义分析。该项能力主要是针对可执行程序文件、各类办公文档、电子邮件及其附件等各类内容载体的判定，对未知类型的恶意代码有较高的准确率，对鱼叉式钓鱼邮件也有较强的识别和拦截能力，构筑起内容安全的屏障。

（二）打造数据驱动的动态智能安全运营平台

安全数据湖创建，冲破数据壁垒，把各种有关的安全日志，网络流量，资产状况，漏洞信息以及外界威胁情报统统纳入一个统一且规范化的安全数据湖之中，从而为AI剖析赋予充沛且优质的“燃料”。

AI模型不断训练、不断优化闭环形成起来的就是模型训练、部署、监测、反馈的完整生命周期管理系统[8]。使用在线学习或者增量学习的方法来保证模型可以适应变化的网络环境、攻击手段，防止模型随着时间推移而出现性能下降的情况发生。

可视化和可解释性增强，用知识图谱加交互式可视化的方式把AI分析结果(攻击链路、关联关系、风险评价)表现出来。同时发展模型可以解释性技术可以让人工智能做出判断的依据被理解，从而加强人与机器之间的互信、合作。

（三）深化智能安全编排与自动化响应实践

告警智能分诊和调查自动化是利用NLP技术分析告警文本、用分类聚类模型对告警自动分类、关联、评分的自动化处理。预设自动化调查剧本，使AI能自动生成初步的证据搜集及上下文联系剖析成果，从而产生带有较多背景资料的“事件摘要”，该种摘要可以作为分析师作出决定的依据[9]。

自适应响应决策支持，在复杂的环境下，利用强化学习可以模拟出各种不同的安全响应方案，给安全人员给出最优或者备用的安全响应方案的建议，从而达到安全效果与业务影响的最佳平衡。

（四）探索生成式AI在防御中的创新应用

第一，安全运营和分析效率的明显提高，得益于它成了一个“智能安全分析员”。它既可以对海量的安全日志、告警进行自动分析，生成出结构清晰、重点突出的事件分析报告，又可以根据分析师的自然语言指令，自动写出准确的调查查询语句（SQL或者Splunk查询）来，从而找出潜在的威胁[10]。除此之外，对于漏洞描述复杂、晦涩的APT攻击报告，LLM可以通过对其快速的理解，把APT攻击技术细节暴露出来，从中提取出有关漏洞的技术特点，使安全分析师更容易找到攻击目标和攻击手段。

第二，模拟攻击和防御测试得到加强之后，生成式人工智能便有了它自己独特的作用。它可以模拟出攻击者的行为模式、思维方式、语言风格，并生成出具有很强的迷惑性、针对性的钓鱼邮件或者社交工程话术脚本。可以直接用在组织内部的“红队”演练、渗透测试、员工安全意识培训及测试上，可以检验并提高整个企业的“人防”水平。从技术防范角度出发，用生成式人工智能可以生成大量的接近真实的恶意网络流量样本、攻击负载和

异常行为数据等。合成数据可以大大增加安全检测模型的训练集，使得模型可以学习到来自于更加多样化的攻击特征变种上，进而明显提高检测未知威胁的能力。

三、结束语

综上所述，人工智能同大数据相互配合，正改变着网络安全防御技术的布局及应用形态。本文研究发现，由于它有数据处理能力强、模式识别准、决策效果好等特点，在威胁检测、态势感知、自动响应以及预测防御等各方面具有无法取代的作用。经过创建分层检测模型，搭建起智能运营平台，深入到自动化响应流程当中，并且尝试采用生成式 AI 等新颖的应用模式去推进这些革新尝试，从而达成将人工智能技术转变成防御手段的实践效果。未来的趋势如下，第一就是向可信 AI 方向发展，强调模型的鲁棒性、公平性以及可解释性；第二就是隐私计算技术会更多地应用到安全数据的协同建模当中来平衡数据利用与隐私保护的关系；第三就是 AI 将会越来越“平民化”，用 SaaS 或者智能化模块的形式来赋能各个不同的组织。

参考文献

[1] 代明，黄辉 . 人工智能技术在大数据网络安全防御中的应用 [J]. 中国宽带 ,2025,21(06):55-57.DOI:10.20167/j.cnki.ISSN1673-7911.2025.06.19.

[2] 杨锐，李茜 . 人工智能技术在大数据网络安全防御中的应用探讨 [J]. 中国宽带 ,2025,21(03):64-66.DOI:10.20167/j.cnki.ISSN1673-7911.2025.03.22.

[3] 宋彦京 . 人工智能技术在大数据网络安全防御中的应用 [J]. 中国信息化 ,2025,(03):80-82.

[4] 郭昕 . 人工智能技术在大数据网络安全防御中的应用 [J]. 中国信息界 ,2024,(04):158-160.

[5] 樊华 . 人工智能技术在大数据网络安全防御中的应用 [J]. 中国高新科技 ,2023,(21):50-52.DOI:10.13535/j.cnki.10-1507/n.2023.21.16.

[6] 周凡 . 人工智能技术在大数据网络安全防御中的应用研究 [J]. 信息记录材料 ,2023,24(06):49-51.DOI:10.16009/j.cnki.cn13-1295/tq.2023.06.010.

[7] 戎亿 . 人工智能技术在大数据网络安全防御中的应用 [J]. 中国宽带 ,2023,19(05):147-149.DOI:10.20167/j.cnki.issn1673-7911.2023.05.043.

[8] 吐逊江·麦麦提 . 人工智能技术在大数据网络安全防御中的应用研究 [J]. 无线互联科技 ,2022,19(11):23-25.

[9] 汤曦 . 人工智能技术在大数据网络安全防御中的应用探究 [J]. 智慧中国 ,2022,(03):83-84.

[10] 耿杨 . 人工智能技术在大数据网络安全防御机制中的应用研究 [J]. 数据 ,2022,(01):48-50.

