 DOI: https://doi.org/10.12349/iser.v5i11.3607

The Application of Artificial Intelligence Technology in Big Data Network Security Defense

Su Zhang

Beijing Ruubypay Science and Technology Co., Ltd., Beijing, 100088, China

Abstract

With the rapid development of the Internet, network security issues have become the focus of global attention. In this era when data is king, the flow of massive information through the Internet brings endless opportunities and breeds endless security threats. The network attack means are becoming increasingly complex, and the traditional security defense means have become inadequate. Artificial intelligence technology, with its powerful computing ability and learning ability, is becoming the new favorite technology of network security defense. It can not only quickly analyze massive amounts of data, but also continuously improve its defense level through self-learning. Therefore, exploring the application of artificial intelligence in the big data environment has become an important topic at present.

Keywords

artificial intelligence technology; big data; network security defense; application research

人工智能技术在大数据网络安全防御中的应用

章苏

北京如易行科技有限公司，中国 · 北京 100088

摘　要

随着互联网的快速发展，网络安全问题已成为全球关注的焦点。在这个数据为王的时代，海量信息在网络中流动而带来了无尽的机遇，也滋生了层出不穷的安全威胁。网络攻击手段日趋复杂，传统的安全防御手段已经显得力不从心。人工智能技术以其强大的计算能力和学习能力正在成为网络安全防御的新宠，它不仅能够迅速分析海量数据，还能通过自我学习不断提高防御水平。因此，探索人工智能在大数据环境下的网络安全防御应用，已经成为当前的重要课题。

关键词

人工智能技术；大数据；网络安全防御；应用研究

1 引言

如今的网络世界，安全威胁如影随形。面对这日益严峻的形势，传统的防御手段已经显得苍白无力，依靠人工去处理庞大的安全数据显然跟不上攻击者的节奏。而就在这样的背景下，人工智能技术逐渐崭露头角。它能在短时间内处理海量数据，还能识别出那些常规防御措施无法发现的异常活动，这像是给安全专家配备了一个超级助手，聪明且精力无限。人工智能的应用前景不可估量，特别是在网络安全领域，它的潜力已经开始被业界广泛认可。智能化的网络安全防御将不仅仅是对现有技术的优化，而是一次真正的革命。

2 大数据环境下的网络安全挑战

在大数据时代，网络安全正面临着前所未有的挑战。这些挑战看似平静无波，实则暗藏危机。数据的爆发式增长让网络安全防护犹如在海量信息中寻找一根针，每秒钟都有成千上万的数据点产生，它们有的关乎隐私，有的涉及商业机密，而这些数据在传输和存储过程中都可能成为黑客的目标。面对如此庞大的数据量，传统的安全防护措施显得力不从心。数据类型的多样化让网络安全的防线捉襟见肘，以前可能只需要保护几种特定的数据格式，但现在，从文字到图片、从视频到实时数据流，每一种数据都有可能成为攻击者的突破口，每一种数据类型都需要不同的保护方式。在应对这些纷繁复杂的数据形式时，安全措施却有时漏洞百出。而且，这些数据之间的相互关联性也让风险进一步扩大，牵一发而动全身，一旦有一个环节被攻破，整个系统都可能受到牵连。在这庞大复杂的数据生态系统中，安全威胁的隐蔽性也随之上升。黑客们不再像过去那样简单粗暴，而是变得更加狡猾和隐蔽。他们利用大数据技术将攻击伪装得毫无痕迹，甚至会让人误以为是正常的数据流动。这种隐蔽性让检测变得极为困难，传统的防护手段在这种新型威胁面前，就

【作者简介】章苏（1977–），男，中国浙江鄞县人，硕士，从事大数据、网络安全和人工智能领域的研究。

像是白昼里打着手电筒找人一样无效。最后，随着物联网设备的普及，网络安全的边界也被无限扩展。每一个联网的设备都是一个潜在的攻击点，这些设备之间相互连接，形成了一个庞大的网络生态系统。曾经，只需保护企业内网和服务器，而现在，从智能手机到智能家居，甚至是智能汽车，都成为了需要防护的对象，如图 1 所示。这些设备通常安全性较低，易受攻击，犹如一个个敞开的城门让黑客轻而易举地找到突破口。整个网络世界因此变得如同一张千疮百孔的渔网，防不胜防 [1-3]。

3 人工智能在网络安全防御中的应用

智能技术的应用为大数据网络安全防御带来了前所未有的变革，其中，人工智能技术在这一领域的表现尤为亮眼。尤其是在利用机器学习进行异常检测、深度学习在恶意软件识别中的应用，以及自然语言处理在威胁情报分析中的应用这三个方面。纵观这几个方面的应用，犹如给网络安全加上了一层铜墙铁壁（见表 1）。

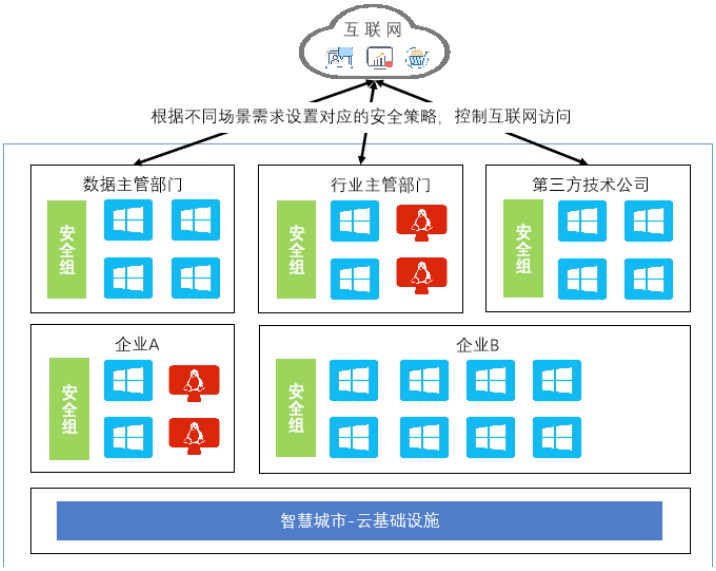

图 1 互联网安全监管系统

表 1 人工智能在网络安全防御中的应用一览表

应用领域	主要技术	关键指标	备注
异常检测	机器学习	分类准确度 85%~99%	通过大量数据训练行为模式
恶意软件识别	深度学习	准确度 99.5% 以上	使用 CNN 和 GANs 等模型分析
威胁情报分析	自然语言处理（NLP）	情报解析准确度 95%	解析文本数据提取有价值情报

机器学习在网络安全中的应用，尤其是在异常检测方面堪称一大亮点。传统的检测方法往往防不胜防，但机器学习可以通过大量历史数据进行训练而生成复杂的行为模式，从而准确识别出网络中潜藏的异常活动。异常检测应用中的一个关键指标是“分类准确度”，通常范围是 85%~99%，这一技术的运用使得网络可疑行为无处遁形。不同于普通的检测系统，深度学习能够深层次地分析数据特征，从而对恶意软件进行更加精准的识别和分类。例如，卷积神经网络（CNN）可以通过图像分析精准识别恶意代码的特征，此类方法在一些实验中显示出了 99.5% 以上的准确度。与此同时，生成对抗网络（GANs）也可以生成近似恶意代码的样本用于训练检测模型，使得模型在面对新型恶意软件攻击时更加游刃有余。网络攻防之间的信息不对称，往往使得防御工作应接不暇。NLP 可以解析网络中大量的文本数据，从中提取出有价值的威胁情报，进行实时分析。通过对社交媒体、论坛、黑客论坛、研究报告等数据源进行情感分析及关键字过滤，NLP 能够提前捕捉到潜在威胁。一个关键指标是情报解析准确度，预计未来可以达到 95% 以上。这无疑让网络防御站在了一个制高点上，提前布控，及时响应 [4,5]。

4 人工智能技术增强网络安全的策略

4.1 智能化安全监控系统的构建

构建智能化安全监控系统是一项复杂而精细的任务，其目标是创建一个能够全面监控网络环境并及时响应安全威胁的系统。这一系统的核心在于利用人工智能技术来提升对异常活动的识别能力，这种能力在速度和准确性上远超人类分析者。系统首先必须建立一个高效的数据收集机制，以确保能够从网络流量、日志记录、用户行为等多个维度收集数据。这些数据是构建智能监控系统的基础，它们为系统提供了必要的信息以识别和分析潜在的安全威胁。智能监控系统应通过机器学习算法进行训练，以识别正常与异常的行为

模式。这一过程涉及到对大量数据的分析，以训练模型识别出潜在的异常行为，如图 2 所示。随着深度学习等高级 AI 技术的应用，系统能够自动适应新的威胁模式，提高其对新型攻击的识别能力。当系统检测到异常行为时，它不仅会发出警报，还会自动采取一系列措施，如隔离受感染的系统部分、调整防火墙规则或启动额外的安全扫描，以迅速响应并减轻威胁的影响。而且，AI 哨兵不是一成不变的，它们会从每一次的威胁中学习和进化，这一过程需要不断地调整算法、更新模型，以确保哨兵能始终保持最强的状态。人工智能技术的加入让网络安全系统从被动防御转向主动出击，智能化安全监控系统的构建不仅仅是技术的累加，更是一次网络安全思维的革新。

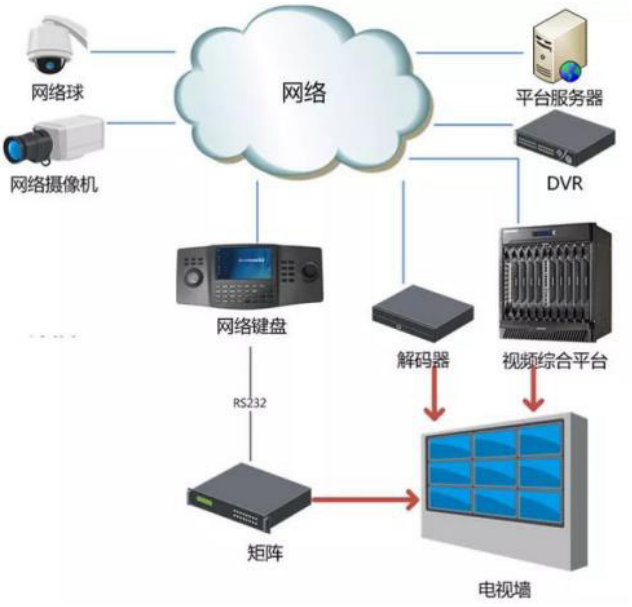

图 2 智能化网络安全监管覆盖

4.2 预测性网络安全防御策略

人工智能技术在预测性网络安全防御策略中展现出无可替代的优势，这是因为传统的网络安全防御往往依赖于已知威胁的特征和模式来进行拦截，而面对日益复杂和不断演化的网络攻击，单纯依靠过去的经验显然已经捉襟见肘。预测性防御策略则通过利用人工智能的强大计算能力和机器学习算法，提前识别潜在威胁，并在它们成为实际攻击之前采取行动。在具体操作过程中，人工智能首先通过大数据技术获取和处理海量的网络流量数据，这些数据包括用户行为日志、网络通信记录以及设备操作历史。然后，机器学习算法深入分析这些数据，建立多维度的威胁模型，挖掘出正常行为和异常行为之间的细微差异。深度学习技术更是能够识别出那些隐藏在海量正常数据背后的“零日攻击”，这些攻击由于没有明确的特征，往往是传统防御的盲区。当潜在威胁被识别出来后，人工智能系统并不仅仅是发出警报，更会通过自动化的决策引擎采取预防性措施，比如实时阻断可疑流量、调整防火墙策略、隔离受感染的节点等。AI 还会不断更新和优化自己的模型，确保应对未来的新型威胁。这个过程中，人工智能并不是孤立工作的，它与整个网络安全生态系统紧密配合，形成了一个动态、智能的防御体系，如图 3 所示。每一次防御行为的反馈都会反哺至模型之中，使得系统的预测能力和反应速度不断提升。通过这种方式，预测性网络安全防御策略不仅能够显著降低攻击成功的可能性，更能将威胁扼杀在萌芽状态，让安全防线始终处于主动而非被动的状态。在这个过程中，人工智能展示了其卓越的自适应能力与学习能力，这种不断进化的特性使得网络安全防御不再是静态的屏障，而是一道能够“思考”的智能防线，为数字世界的安全保驾护航。

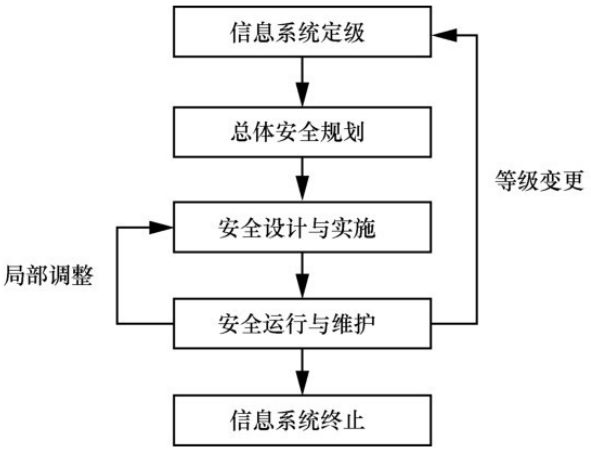

图 3 AI 预测性安全防御流程

4.3 人工智能辅助的应急响应机制

人工智能辅助的应急响应机制为网络安全领域的中坚力量，此机制的核心在于其能够通过机器学习和深度学习算法，快速识别、定位并响应异常行为，实现从被动防御到主动预防的转变。人工智能的作用不仅限于检测异常，还包括实时分析入侵的模式与路径，深度挖掘历史数据，人工智能可以建立异常行为的模型，这些模型能够帮助识别潜在的威胁。在遭遇攻击时，系统会迅速调用预先训练的模型，分析流量的特征和变化，进而识别攻击类型和攻击源。一旦检测到可疑活动，系统能够立刻触发自动化的响应流程，这种速度是传统手段无法企及的。传统的威胁情报依赖于人工收集和分析，效率低且容易受到信息的滞后影响。而人工智能可以通过自然语言处理技术实时分析海量的威胁情报数据，包括网络日志、社交媒体信息、暗网活动等，迅速过滤出与当前网络环境相关的威胁信息，形成动态的威胁画像。这种动态更新的威胁情报库可以为应急响应提供及时而精准的参考，使得响应团队能够在第一时间采取有效的应对措施。人工智能还能够协助进行应急响应中的漏洞修补，传统的漏洞修补过程需要人工逐一排查和验证，而在面临大规模的攻击时，这种方式显得力不从心。借助人工智能的自动化分析能力，系统能够快速识别潜在的漏洞位置和影响范围并生成修复建议。结合历史攻击数据和当前的攻击特征，人工智能还

能预测未来可能出现的攻击方式和路径，为网络安全防御策略的优化提供数据支持。应急响应机制的另一个关键在于事件后的分析与复盘，这也是人工智能大显身手的领域。通过深度学习算法，人工智能能够分析攻击者的行为模式，识别出攻击链中的每一个环节。这有助于理解攻击者的意图和手段，提升系统的整体防御能力。通过不断学习和进化，人工智能辅助的应急响应系统能够不断适应新的威胁，形成一种动态、适应性强的防御体系。

4.4 自动化漏洞检测与修复

面对层出不穷的安全威胁，人工智能技术在自动化漏洞检测与修复方面展现出了前所未有的潜力，它通过机器学习和大数据分析能够在海量数据中精准定位潜在的安全漏洞，甚至在这些漏洞被利用之前就能及时加以修复。相比传统的手动检测方式，人工智能的自动化检测不仅效率高、速度快，更具备实时性，能够随时监测并识别网络中的异常活动。自动化漏洞检测的核心在于其自我学习和进化的能力，人工智能算法不断地分析历史攻击数据以自动更新自己的检测规则和防护策略，这种动态的学习机制使得防御系统能够应对不断变化的攻击手段，无论是零日漏洞还是高级持续性威胁，人工智能都能够在第一时间响应，并采取有效的防御措施。大数据环境下的数据量庞大且复杂，人工智能可以迅速从中挖掘出隐藏的威胁模式，通过关联分析，找出看似无关的事件之间的联系，从而预判可能发生的攻击。修复方面，传统的漏洞修复往往需要人工介入，既耗时又容易出错，而人工智能则可以自动生成修复方案并进行快速部署。更为重要的是，人工智能还能通过仿真技术，在实际修复之前模拟修复后的效果，确保修复不会影响系统的正常运行。

4.5 行为分析与异常检测

在面临数据规模急剧膨胀的挑战下，人工智能可以在海量数据中捕捉到微小的异常并及时识别潜在的威胁，从而有效地提升网络安全防御的精准度和响应速度。在实际操作中，行为分析的核心是对用户和系统的正常行为进行深度学习，通过大量的历史数据建模而建立起一个精细的行为基线。当系统运行过程中出现偏离该基线的行为时，人工智能算法便能够迅速检测到这些异常。举例来说，若某用户账号突然频繁尝试访问未授权的敏感数据，或者在非工作时间段出现大量的数据传输，这些异常行为很可能预示着恶意攻击或数据泄露的企图。此时，人工智能系统会立即发出警报，并可以自动采取响应措施，如限制访问权限、隔离受影响的节点或进一步加强监控。在大数据环境下，攻击者的手法变得更加多样化，而通过不断的学习和进化，人工智能可以逐步更新其行为模型，识别出那些未曾见过的新型攻击模式。这种动态的、智能化的防御策略能够大大降低被攻击成功的风险，提升安全系统的整体效率。

5 结语

随着网络威胁的不断升级和复杂化，人工智能将成为安全防御的中坚力量。不论是通过机器学习来发现潜在威胁，还是利用深度学习识别恶意软件，抑或是通过自然语言处理进行威胁情报分析，这些技术都在逐步改变网络安全的格局。技术的发展离不开实践的指导，要想充分发挥人工智能的优势，企业和组织必须在安全策略中主动融入这些新兴技术，建立更加智能化的安全防御体系。未来的网络安全必将是一场智能与智能的对抗，谁能在这场对抗中占据上风，将决定未来网络世界的安全格局。

参考文献

[1] 李根.网络安全防御中的人工智能技术运用[J].电子技术,2023,52(6):216-217.

[2] 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.

[3] 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(3):83-84.

[4] 于淏璇.大数据时代人工智能技术在网络空间安全中的应用研究[J].无线互联科技,2021,18(24):110-111.

[5] 周春萍,徐长棣.人工智能技术在大数据网络安全防御中的应用探究[J].网络安全技术与应用,2021(11):61-63.