机械工程 (4)2024,6
ISSN: 2661-3530(Print); 2661-3549(Online)

基于人工智能技术的计算机网络安全防护系统设计

解晓丽

（宁夏财经职业技术学院学院　宁夏银川　750021）

摘　要：随着网络攻击手段的不断演进，传统的网络安全防护技术已经难以应对日益复杂的威胁形势。本文提出一种基于人工智能的网络安全防护系统设计方案。该系统利用机器学习算法分析海量网络数据，快速识别异常行为模式，及时发现威胁并自动采取防御措施。通过自主学习和模型优化，系统可提高对未知威胁的识别能力，实现智能化防护。同时，该系统自动化了许多安全防护流程，降低了运营成本。该设计方案旨在提高网络安全防护的智能化水平，增强威胁检测和响应能力，为计算机网络带来更加可靠的安全防护。

关键词：人工智能技术；计算机网络；安全防护；系统设计

引言：

在当今信息时代，计算机网络已经无处不在，成为了现代社会的重要基础设施。从政府机构到企业组织，从金融系统到交通运输，无不依赖于计算机网络的正常运转。然而，随着网络技术的快速发展，网络安全威胁也日益增多，给计算机网络的安全运行带来了巨大挑战。基于人工智能技术的计算机网络安全防护系统，就是在这一背景下应运而生。它利用机器学习、大数据分析等人工智能技术，能够快速识别异常行为模式，及时发现潜在威胁，并自动采取相应的防御措施，从而为计算机网络带来更加智能化和主动式的安全防护。

一、计算机网络安全防护技术的现状

（一）网络安全威胁的多样化

当前，网络安全威胁已经呈现出多样化的态势，给计算机网络安全带来了前所未有的挑战。最典型的威胁包括网络蠕虫、计算机病毒、黑客攻击、钓鱼网站、电信诈骗以及恶意二维码等。这些威胁具有隐蔽性强、传播速度快、破坏力大、追求非法利益等特点。网络蠕虫和计算机病毒能够自我复制和传播，在短时间内感染大量主机，造成系统瘫痪和数据损坏。黑客攻击手段也日益专业化，包括网络入侵、拒绝服务攻击、数据窃取等，对关键基础设施和重要信息系统构成严重威胁。另外，钓鱼网站、电信诈骗等社会工程学攻击则是针对人的弱点，诱骗用户泄露敏感信息或支付钱财。近年来，恶意二维码等新型攻击手段也开始出现，进一步增加了网络安全的防护难度。

（二）网络安全防护技术的局限性

传统的网络安全防护技术，如防火墙、入侵检测系统等，在应对当前日益复杂的网络攻击时，已经显现出了明显的局限性。这些技术大多基于已知的攻击模式和规则，对未知的新型攻击手段往往无能为力。防火墙主要通过访问控制策略来阻挡已知的恶意流量，但面对隐蔽性强的攻击很容易被绕过。入侵检测系统虽然能够监测网络异常行为，但其依赖于预先定义的攻击特征，难以及时发现新型攻击。另外，这些被动式的防护技术在发现威胁后，通常需要人工干预才能采取相应的防御措施，响应效率较低。此外，传统防护技术也缺乏对大量异构数据的处理能力，无法对海量的网络流量、日志信息等进行深入分析，从而难以发现隐藏在背后的攻击痕迹。

（三）网络安全意识的不足

尽管网络安全威胁日益严峻，但许多用户和企业对网络安全的重要性认识仍然不足，缺乏必要的网络安全防护意识和措施。这为攻击者可乘之机，导致网络安全漏洞的普遍存在。一方面，普通用户对网络安全知识的了解有限，容易被钓鱼网站、恶意软件等攻击手段所欺骗，泄露个人隐私信息或感染病毒。另一方面，部分企业为了追求短期利益，忽视了网络安全投入，导致系统存在严重漏洞，一旦遭到攻击将付出沉重代价。此外，一些组织内部缺乏完善的网络安全管理制度和应急响应机制，网络安全意识在员工中没有得到充分重视和贯彻。一旦发生安全事件，往往无法及时发现和有效应对，从而加剧了事态的严重性。

二、人工智能技术在计算机网络安全防护中的重要性

（一）提高威胁检测和响应能力

人工智能技术可以通过机器学习算法分析海量网络数据，快速识别异常行为模式，及时发现潜在威胁。具体来说，人工智能系统可以利用深度学习、聚类分析等算法，对网络流量数据、日志信息、安全设备告警等异构数据源进行多维度分析，自动挖掘出可疑的数据模式，实现对已知和未知威胁的主动发现。同时，该系统还可以通过对历史数据的学习，不断优化威胁检测模型，提高对新型攻击手段的识别能力。另一方面，基于人工智能的网络安全防护系统不仅能够发现威胁，还可以根据威胁情况自动采取相应的防御措施，大大提高了网络安全防护的响应速度和效率，有效降低了人工干预的需求。

（二）增强安全防护的智能化水平

传统的网络安全防护技术往往依赖于预先定义的规则和签名，难以应对不断变化的网络攻击手段。而基于人工智能的安全防护系统则可以通过自主学习，持续优化威胁检测模型，提高对未知威胁的识别能力，实现真正的智能化防护。具体来说，人工智能系统可以利用机器学习算法对大量的网络数据和攻击样本进行训练，自动学习到网络攻击的特征模式和规律，而不需要人工预先定义规则。另外，人工智能系统还可以通过持续的模型优化和迭代，不断提高对未知威胁的检测能力。当发现新的攻击手段时，系统可以自动将

其纳入训练样本，重新训练模型，从而实现对新型威胁的快速适应和响应，跟上网络攻击手段的快速演进。

（三）降低网络安全防护的运营成本

人工智能技术可以自动化许多网络安全防护的流程，如数据收集、分析、决策等，减轻人工干预的需求，从而降低网络安全运营的人力和资源成本。传统的网络安全防护工作需要大量的人工参与，如安全分析人员审计海量日志数据、运维人员配置防护策略、应急响应人员处置事件等，这些工作不仅耗费大量人力，而且效率低下、容易出错。而基于人工智能的网络安全防护系统则可以自动完成大部分流程，如自动收集分析数据、识别潜在威胁、自动调整防护策略等，极大减轻了人工干预的需求。此外，人工智能技术还可以应用于网络安全态势感知、预警预判等环节，提高安全运营的前置性和主动性，从而降低事后处置的成本。

三、基于人工智能技术的计算机网络安全防护系统设计

（一）数据收集和预处理模块

数据收集和预处理模块负责从各种来源收集相关数据，并对原始数据进行清洗、标准化和特征提取等预处理，为后续的分析和建模做准备。该模块需要从网络流量数据、各类主机和安全设备日志、安全设备告警信息等多个异构数据源采集数据。收集到的原始数据通常存在格式不统一、冗余、噪声等问题，需要进行数据清洗，如去除无效数据、格式转换等，以确保数据的完整性和一致性。接下来，需要对清洗后的数据进行标准化处理，将其转换为统一的数据格式，方便后续的特征提取和分析。特征提取是数据预处理的关键环节，旨在从原始数据中提取出对于威胁检测和分类有意义的特征，如 IP 地址、端口号、协议类型、文件哈希值、用户行为模式等。特征提取可以采用基于规则的方法，也可以利用机器学习算法自动挖掘特征。不同类型的数据需要提取不同的特征，因此需要针对不同数据源设计合理的特征提取策略。经过预处理后的数据将被输入到后续的威胁检测和分类模块，为网络攻击行为的识别和威胁类型的判断提供数据支撑。数据预处理的质量直接影响到整个系统的检测和防护效果，因此需要在该模块投入足够的精力。

（二）威胁检测和分类模块

威胁检测和分类模块是基于人工智能网络安全防护系统的核心模块，利用机器学习算法对预处理后的数据进行分析，识别潜在的网络攻击行为和威胁类型。该模块可以采用多种机器学习算法，如决策树、支持向量机、深度神经网络等，根据具体场景和数据特征选择合适的算法。首先，该模块需要基于已知的攻击样本和正常数据对机器学习模型进行训练，使其学习到网络攻击行为的特征模式。在训练过程中，可以采用有监督学习、无监督学习或者半监督学习等不同的学习方式，并通过特征选择、模型优化等技术提高模型的准确性。训练完成后，该模块可以对实时的网络数据进行分析和预测，识别出潜在的网络攻击行为，如垃圾邮件发送、恶意扫描、网页挂马、数据窃取等，并对攻击行为进行分类，判断具体的威胁类型，如病毒、蠕虫、木马等。该模块还需要具备持续学习和自我优化的能力。一方面，它可以将新发现的攻击样本不断纳入训练集，重新训练模型，从而提高对未知威胁的检测能力；另一方面，它还可以根据模型的实际检测效果，自动调整算法参数和特征选择策略，持续优化模型性能。

（三）威胁响应和防御模块

威胁响应和防御模块是基于人工智能的网络安全防护系统的执行模块，根据威胁检测和分类的结果，自动采取相应的防御措施，如阻断恶意流量、隔离受感染主机、更新安全策略等，从而实现对网络攻击的快速响应和主动防御。该模块需要与网络基础设施和安全设备深度集成，如防火墙、入侵防御系统、VPN 网关、反病毒系统等，以便能够直接下发并执行相应的防御策略和指令。例如，一旦发现恶意 IP 地址，该模块可以直接在防火墙上添加阻断规则；一旦检测到主机中毒，可以通知隔离主机并调用反病毒软件进行病毒查杀等。同时，该模块还需要具备智能决策能力，能够根据威胁类型、危害程度、响应成本等多个因素，自主选择最优的防御策略。例如，对于低危但频发的攻击，可以采取自动化的防御措施；而对于高危攻击，则需要发出预警并等待人工确认后再执行相应的防御操作。此外，该模块还可以通过反馈机制，将新发现的威胁信息用于模型优化和知识库更新。具体来说，一旦发现新的攻击手段，该模块可以将其作为新的训练样本，反馈给威胁检测模块，以提高对未知威胁的检测能力；同时还可以将新的攻击特征和防御策略更新到知识库中，为后续的威胁分析和响应提供支持。

结束语

综上所述，基于人工智能技术的计算机网络安全防护系统具有广阔的应用前景和发展空间。未来，该系统将融合更多人工智能技术，如深度学习、强化学习、知识图谱等，提高对复杂威胁的理解和分析能力，同时引入自动化机器人技术，实现网络空间的主动防御。另外，随着 5G、物联网、云计算等新兴技术的发展，该系统必将在更广阔的领域发挥重要作用，为网络空间的安全可控性提供有力保障。总之，基于人工智能的网络安全防护技术正在开启新阶段，必将为构建更安全、可靠的网络环境做出重要贡献。

参考文献：

[1]高义升.基于人工智能技术的计算机网络安全防护系统设计[J].网络安全和信息化，2024（04）：127-128.

[2]孙瑜.基于大数据及人工智能技术的计算机网络安全防御系统设计分析[J].网络安全和信息化，2024（02）：143-145.

[3]施雪清.基于人工智能技术的计算机网络安全风险评估系统设计[J].信息与电脑（理论版），2023，35（23）：199-202.

[4]吴晓倩.基于人工智能技术的计算机网络安全防御系统设计[J].信息记录材料，2023，24（10）：67-69.

[5]徐楚原.大数据及人工智能技术的计算机网络安全防御系统设计分析[J].数字技术与应用，2023，41（07）：216-218.

作者简介：解晓丽（1978.10.29-），女，汉族，宁夏中卫，宁夏财经职业技术学院，副教授，大学，研究方向：人工智能，网络安全