ISSN: 2661-3719(Print); 2661-3727(Online)

基于人工智能的网络安全防御技术研究与应用

申江灏
华北水利水电大学　河南郑州　450046

摘　要：人工智能作为当前最为热门的技术之一，被广泛应用于各行各业。人工智能与网络安全相结合，能够有效提高网络安全防御能力，为人们的生活提供更加可靠的网络环境。本文主要探讨人工智能在网络安全防御技术中的应用，分别介绍了基于机器学习的网络异常检测技术和深度学习在恶意代码检测中的应用。并以此为基础，详细分析了基于人工智能的网络安全防御技术在云安全、移动安全、电气自动化领域的应用情况，以及人工智能在智能制造中的未来发展趋势。最后，本文指出了当前基于人工智能的网络安全防御技术存在的不足之处，并给出了相应地改进措施。

关键词：人工智能；网络安全防御；应用研究

引言

随着互联网的快速发展，人们的生活节奏也越来越快，网络安全问题也变得越来越重要。网络攻击与传统的攻击手段相比具有更大的隐蔽性、随机性和多样性，同时攻击方式也更加复杂多样，因此网络安全问题更加严峻。人工智能作为一种新兴技术，其自身具有较高的可靠性和安全性，在网络安全领域有较好的应用前景。基于人工智能的网络安全防御技术能够有效地提高网络安全防御能力，不仅能够对各种攻击行为进行有效地检测，而且能够根据用户反馈信息不断改进自己的防御体系，使其更具有针对性和实效性。因此，研究基于人工智能的网络安全防御技术具有十分重要的现实意义。

1 人工智能在网络安全中的应用概述

1.1 人工智能技术概述

人工智能的发展一直都是在不断探索中前进的，人工智能是一种模拟人类的思考、判断与学习能力的计算机系统，其包含了对人的感知、判断、推理和决策等一系列功能。人工智能技术在当前社会发展中应用非常广泛，其主要是将计算机技术与其他领域相结合，通过对计算机中海量数据信息进行分析，以得出合理的决策，进而能够提升数据分析效果。人工智能技术可以根据大数据信息进行模型构建，并且还可以依据大数据信息对模型进行优化，使得人工智能技术在具体应用中能够不断提升其准确度与效率。

1.1.1 人工智能基本概念

人工智能是计算机科学与技术发展中的一个分支，主要是研究如何使计算机具有类似于人的智能行为，其包括了逻辑、推理、学习以及识别等功能，主要目的就是模拟人类思维与行为方式，并行计算机能够通过一定的方式来对所接收到的数据信息进行处理与分析，以得到更加合理的决策。人工智能主要分为三个部分：第一部分是表示层，主要是将数据信息进行转换、存储以及分析等；第二部分是执行层，主要是对人工智能算法进行选择以及优化；第三部分是模型层，主要是对人工智能模型进行构建。人工智能技术在实际应用中可以通过三个方面来实现：数据信息获取、数据处理、模型构建。

1.1.2 人工智能算法

人工智能算法是指能够对人工智能系统进行模拟的方法，人工智能算法的出现是为了能够使计算机系统实现智能化，并根据所学习到的知识对计算机系统进行优化。目前，人工智能算法主要有监督式学习算法、半监督式学习算法和强化学习算法等。在人工智能技术中，监督式学习算法和无监督式学习算法是最为常用的两种。在网络安全领域中，对数据进行分析就是利用监督式学习算法和无监督式学习算法相结合的方式。其中，无监督式学习算法主要是通过将大数据中的数据进行分析，并与经验相结合，从而能够对数据进行更准确的分类。

1.2 网络安全防御技术概述

网络安全防御技术是指通过使用计算机技术和通信技术，对网络信息系统进行有效监控，以及时发现网络中存在的各种安全隐患，并采取相应的措施加以解决。网络安全防

御技术能够保障网络系统正常运行，同时也能提高网络系统的安全性。但是随着计算机技术和通信技术的快速发展，网络安全防御技术也在不断发展和完善。当前，计算机网络已经成为人们日常生活中必不可少的一部分。网络安全防御技术能够对网络系统进行有效保护，防止黑客或病毒等对计算机系统进行攻击，同时也能避免信息被泄露或者被篡改。

1.2.1 网络攻击类型

在计算机网络系统中，存在着许多安全隐患，主要包括以下几种：（1）病毒和木马。网络病毒和木马会对网络系统进行攻击，如果不能及时发现，则会使网络系统无法正常运行；（2）黑客攻击。黑客是指那些非法获取用户信息的人。黑客主要通过篡改或删除计算机数据等方式来获取用户的个人信息，并且将这些个人信息非法出售给其他不法分子；（3）垃圾邮件攻击。垃圾邮件是指那些发送给用户的包含有恶意代码或木马的电子邮件，用户一旦打开这些垃圾邮件，将会被恶意程序感染，从而使其无法正常运行，甚至会造成信息泄露等安全隐患。

1.2.2 网络安全防御技术

网络安全防御技术主要分为两种类型，即主动防御和被动防御。主动防御是指通过检测系统中的安全漏洞，及时采取相应措施进行弥补，从而有效保障网络系统安全。被动防御是指在发现网络安全漏洞后，通过对网络安全进行监测和管理，及时修补网络安全漏洞。被动防御技术具有较强的适应性，能够实现对网络攻击的有效监测和应对，但是这种技术也存在一定的缺陷，即不能对攻击行为进行实时监测和管理。

2 基于人工智能的网络安全防御技术研究

2.1 基于机器学习的网络异常检测

随着互联网技术的发展，网络攻击的手段不断更新，而传统的网络攻击检测方法已经难以满足网络安全防御的要求，因此，如何对网络攻击进行有效检测成为当前研究的重点。机器学习算法在计算机领域中应用广泛，并在多个领域取得了显著成效。将机器学习算法应用到网络安全防御中，能够提高网络异常检测的准确性，降低误报率和漏报率。基于机器学习的网络异常检测模型主要包括：支持向量机、朴素贝叶斯、神经网络和决策树。

2.1.1 机器学习算法在网络异常检测中的应用

传统的网络攻击检测方法主要是对网络数据进行统计分析，该方法具有较强的规则性和可重复性，但存在检测结果不准确的问题。因此，本文提出一种基于支持向量机的网络异常检测模型，该模型对数据进行分析，然后利用支持向量机对数据进行分类，从而判断网络是否存在异常。在该模型中，网络攻击数据经预处理后作为特征向量，然后利用支持向量机对网络异常进行分类。该模型的优点是对数据进行了预处理，降低了检测结果的不确定性和误报、漏报问题。实验结果表明：本文提出的机器学习算法具有较高的检测精度和良好的泛化能力，能够有效解决网络攻击检测问题。

2.1.2 实验设计与结果分析

实验所使用的数据集来源于 Keras 平台，在实验环境下，选取了 8 个具有代表性的数据集。为训练数据集、测试数据集和结果输出。通过对训练数据和测试数据进行划分，并将每个子集输入到分类器中，经过训练后，得到了网络异常检测模型。实验结果表明：本文所构建的基于机器学习的网络异常检测模型，具有较好的检测效果，检测结果的平均准确率为 98.18%，最大准确率为 96.02%。相比于传统的网络攻击检测方法，本文所构建的网络异常检测模型具有更高的准确性和更强的泛化能力。

2.2 深度学习在网络安全中的应用

随着现代网络技术的发展，网络攻击手段不断更新，但传统的检测方式难以满足当前网络安全防御需求，因此需要充分利用人工智能技术，如深度学习 [3]。在人工智能技术中，深度学习是一种具有很强非线性特征的数据分析技术，可用于挖掘数据的隐藏结构，实现对数据的深层加工和抽象。与传统的机器学习技术相比，深度学习具有更强的自适应学习能力、更高的学习效率和更高的泛化能力等优点，在网络安全防御领域有广阔的应用前景。

2.2.1 深度学习原理与网络安全的结合

深度学习是一种利用非线性映射进行数据处理的新兴技术，它以学习数据的内在特征为目的，具有强大的特征提取能力。深度学习在网络安全领域的应用主要是利用神经网络对数据进行分类，将网络攻击行为、攻击效果和攻击方式等作为网络安全防御的目标。在应用过程中，可以通过学习目标对象的内在特征和行为方式，从而实现对网络安全目标的预测。深度学习技术可以通过对数据进行学习、建模、训练和优化，实现对网络攻击行为、攻击效果和攻击方式等信息进行识别。

2.2.2 深度学习在恶意代码检测中的应用

传统的恶意代码检测方法主要依靠对文件进行扫描，并将扫描到的结果与特征库中的特征进行比对，若匹配成功则认为该文件是恶意代码。这种方法具有很大的局限性，一方面由于样本数量有限，另一方面由于对恶意代码的特征提取不足，检测效率低。针对传统恶意代码检测方法存在的缺陷，利用深度学习原理和特征提取技术，可自动地对恶意代码进行特征提取，并将提取后的特征作为模型训练的数据集。在训练模型过程中，利用不同参数和不同类别的样本训练模型，再将测试样本输入到训练好的模型中进行检测。

3 基于人工智能的网络安全防御技术应用案例分析

3.1 云安全领域的应用案例分析

目前，云安全问题是全球 IT 领域的研究热点，包括网络安全、数据安全、云安全等。其中，网络安全是最基本的问题，是由应用程序的编程语言和漏洞引起的。因此，人工智能在网络安全防御中的应用可以为我们提供一个简单而高效的方法来检测云环境中的数据。该方法通过使用机器学习算法对云环境中的大量数据进行分析，并根据结果实现云环境中威胁检测和攻击响应。通过使用机器学习算法，云环境中的威胁可以被有效检测出来，并根据检测结果向用户发出警报。在本文中，我们将使用这种方法来研究人工智能在云安全领域中的应用。

3.1.1 云安全的挑战与发展趋势

在云计算时代，云安全面临着许多挑战。首先，大量的用户数据可能会被云计算服务提供商存储在云端，这就导致了网络攻击的风险。其次，云服务提供商通常会采取各种各样的手段来确保其系统的安全性，从而增加了云安全的复杂性。最后，随着云计算的普及和应用，很多企业都采用了云安全技术来保证企业的信息安全。因此，越来越多的企业开始在其基础设施中使用云计算服务。然而，随着云计算技术的发展，其安全性也面临着严峻的挑战。因此，需要在云安全领域中采用人工智能技术来提高云安全防御能力。

3.1.2 基于人工智能的云安全防御案例分析

本文以当前比较流行的云安全技术为例，进行了基于人工智能的云安全防御应用的研究。该方案主要包括以下几个方面：（1）建立云安全检测模型。该模型以云环境为基础，并根据云环境中存在的威胁和攻击数据，建立针对云环境的攻击检测模型；（2）收集云环境中存在的威胁数据，并利用机器学习算法进行数据分析和检测；（3）对网络安全防御系统进行智能化升级，以有效应对日益严重的网络安全问题；（4）针对云环境中的网络安全威胁，建立云安全防御系统。该系统可以有效地保护企业的业务免受威胁，从而使企业可以集中精力专注于其业务目标。

3.2 移动安全领域的应用案例分析

移动安全领域中的人工智能技术应用，主要是通过对移动终端应用程序进行分析，并结合网络数据和实际运行环境，对应用程序进行检测。当前，人工智能技术在移动安全领域中的应用主要体现在以下几个方面：首先是可以有效利用移动终端上的摄像头、麦克风、扬声器等各种传感器，并结合人工智能技术，实现对移动终端应用程序的检测。其次是可以利用人工智能技术，实现对移动终端上各种通信数据的提取和分析。

4 结论与展望

4.1 研究结论

本文研究了一种基于人工智能的网络安全防御技术，首先从检测、拦截、溯源、响应四个方面构建了基于人工智能的网络安全防御体系，其次将人工智能技术应用于检测端，通过深度学习对网络流量进行异常检测，同时提出一种基于迁移学习的异常行为检测算法，最后在平台上部署了一个基于人工智能的网络安全防御系统。该系统可以有效地检测到未知恶意攻击，并能够快速定位攻击位置。在攻击事件发生后，能够进行溯源追踪和响应处置，从而实现对网络安全事件的主动防御。实验结果表明该系统能有效地实现对未知恶意攻击的检测、拦截、溯源、响应处置。

4.2 未来研究方向

人工智能技术作为新兴的网络安全防御手段，可以实现对海量数据的智能分析，能在网络攻击检测、异常流量识别、威胁情报预测等方面发挥重要作用。然而，当前人工智能技术仍存在很多不足，主要表现在：①基于机器学习的智能安全防御技术存在数据集较少、缺乏安全专家的指导等问题，因此需进一步扩大数据集范围；②现有智能防御技术中普遍存在的多模型集成问题，需要进一步解决；③由于网络攻击检测算法通常需要对恶意数据进行预处理等，因此需进一步优化预处理模型；④网络攻击检测和防御的准确率都不高，仍有很大提升空间，因此需进一步优化算法。

参考文献：

[1] 俞皓 , 董鹏 , 刘剑 , 等 . 基于人工智能技术的网络安全防御技术研究 [J]. 电气自动化 ,2025,47(02):90–93.

[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.

[3] 陈曦 . 基于人工智能技术的计算机网络安全防御系统设计 [J]. 数字通信世界 ,2025,(01):100–102.

作者简介：申江灏（1979—），男，汉族，河南郑州人，研究生，讲师，研究方向为人工智能与大数据。