# 人工智能技术在计算机网络安全评估中的应用

刘　宁

[摘要] 进入21世纪后，计算机技术与网络技术快速发展给人们的生活带了更多的便利，计算机网络安全问题也随着应用规模的不断扩大变得越来越多。因而相应的计算机网络安全评估就显得尤为重要。在计算机网络安全评估中，可针对性引入人工智能技术，借助大数据挖掘与深度学习，提前预判各类网络安全问题，有效减少非法入侵等问题。基于此，本文从人工智能概念入手分析了人工智能技术的特点，而后重点探究了人工智能技术在计算机网络安全评估中的应用，希望可以借此给相关研究提供一定的参考。

[关键词] 人工智能；计算机；网络安全评估

## 人工智能概述

（一）人工智能的概念

人工智能的核心在于机器的深度学习，通过大量的数据挖掘与分析使机器能够自己做出判断与决策，实现模拟人类智慧的目的。人工智能技术与计算机技术的快速发展有着密切的关系，随着技术的不断成熟与完善，应用的领域也逐步延伸，目前涉及了语言处理、图像处理、视频处理、文字处理等多个方面。在计算机网络安全评估方面，人工智能也发挥着重要作用，可以精准地识别网络攻击等行为并自主防御网络攻击。相比传统的网络入侵检测方法，人工智能的准确率更高，且能自主发现新的漏洞，对于网络安全评估的现代化发展有着积极的意义。

人工智能技术属于新兴技术，其发展的速度极快，已与很多领域实现了深入融合。在不断的发展中，人工智能随着不断地深度学习，智能化水平也有了显著的提升。在一些应用领域已经完全替代了人工，且比人工更为稳定、高效。另外，人工智能还有着极大的发展空间，目前还未完全发挥出所有功能。相信在后续的发展中，人工智能的应用领域会进一步的拓宽，从而为人们的生活提供更大的便利。

（二）人工智能的基本特征

人工智能的基本特征主要体现在以下几个方面。

（1）较强的自适应性。人工智能在应用中完善行为方式，通过不断地积累经验使其判断更为准确，能更好的适应各类不同环境。在一些全新的领域，人工智能可以在短时间内完成深度的学习，从海量的数据中总结规律从而快速的适应实际需求。

（2）科学的自主决策。人工智能系统可根据采集到的各类信息作出汇总分析，具备自主决策的能力。这也是人工智能的核心特征之一，随着学习的深入，人工智能的决策准确性也会不断的提升。

（3）强大的自推理能力。人工智能系统能根据数据的逻辑推理从海量的信息中得出规律，这是其自推理能力的体现。而且得益于计算机处理速度的日新月异，人工智能系统的自推理能力也愈发强大。

从上述的分析可以看出，人工智能的特征较为明显且具备划时代的意义，让机器代替人工可一定程度减少人力消耗，同时也能保障反映的及时性与正确性。

（三）人工智能技术在计算机网络安全评估中的应用价值

进入21世纪后，计算机在多个领域发挥着重要的作用，人们对计算机的依赖也在不断提升，而互联网的普及也相应带来了一定的问题。计算机网络安全问题日益突出，各类信息泄露与网络攻击层出不穷，所以计算机网络安全评估受到社会各界的广泛关注。人工智能技术为网络安全评估带来了新的思路。

首先，人工智能技术可通过大数据的深入挖掘与分析找到隐藏的规律，进而更加精确的预测各类风险，为网络安全运行保驾护航。在很多实际应用中，人工智能可通过海量的数据进行模拟训练达到识别未知威胁的能力。

其次，人工智能还可以对网络信息进行筛选，进而检测网络上的不当言论，针对性的删除与过滤。此外，人工智能还可以进行网络安全入侵检测。从总体上看，人工智能技术在计算机网络安全评估中扮演着较为重要的角色，对于网络安全的健康发展有着积极的意义。

## 人工智能技术分析

（一）人工智能机器学习技术

人工智能机器学习技术是通过对大量数据的深度挖掘与分析来寻找其中的规律，找到数据背后的特征也就能较大程度提升预测准确性。对于计算机网络安全而言，人工智能技术对数据的分析后，可用于恶意软件的检测，能有效地识别潜在风险与攻击行为。在整个过程中人工智能机器是通过数据的模拟训练来学习技术的，而以往人们进行病毒识别时还需要将病毒的样本输入，通过样本匹配的方式来识别病毒，相比过去效率有了很大的提升。人工智能机器在学习技术过程中不需要人工的干预，可完全自主的学习与识别，整体的检测效果更为可靠与准确。除此之外，人工智能机器学习技术还可用于攻击行为的识别与威胁风险的预测。通过自主分类，对各类攻击与威胁风险进行建模生成概率模型，进而对潜在的风险提前预警。

（二）人工智能深度学习技术

人工智能深度学习技术是基于神经网络的学习方法，借助多层的神经元结构来实现对数据的分类。该训练算法可对特征进行提取和分类，与传统模式相比有着明显的区别。借助这种学习技术可有效解决复杂的问题，预测的精度也能有效的提升。从当前的实际情况来看，人工智能深度学习技术的应用范围极广，如语音识别、语言识别、图像识别、视频识别等，在交通、医疗、金融等领域也有着十分广泛的应用，可为决策系统提供有力支持。

人工智能深度学习技术的优势在于，它能从无序的数据中寻找出特征，通过自主分类、建立模型，预测其发展的趋势。例如，在医学诊断方面，人工智能深度学习技术可用于检测肿瘤细胞。深度学习技术在网络安全领域的应用也十分广泛，它能通过样本数据的识别来归类各类攻击模式，进而针对性查找潜在威胁。此外，人工智能深度学习技术还可用在漏洞扫描和恶意软件检测等方面。

（三）人工智能监测技术

人工智能监控技术是用于异常的识别，借助训练模拟可在短时间内识别到异常行为并告警。这种技术的适应性极强，数据的处理量也较大。另外，人工智能监测技术在计算机网络安全方面还可应用于自动化决策与智能预警，其主要分为基于模式的监控和基于规则的监控两种。基于规则的监控是借助逻辑判断来分析是否有异常情况发生，例如，当某个用户在特定时间内超过登录数的阈值时就会触发系统的告警。基于模式的监控则是用多个因素来进行异常事件的描述，通过神经网络的向量来进行分类预测，能适应更为复杂的场景。

## 人工智能技术在计算机网络安全评估中的应用

（一）计算机网络安全评估的需求分析

计算机网络安全评估意在提高计算机网络的安全性，因此，相应的安全评估首先要具备较高的准确性与更低的漏报率，这样当计算机网络在受到攻击或非法入侵时才能快速地做出反应，并且及时采取处理措施。

其次，网络安全评估还需具备较高的智能化与自动化水平，可快速的处理各类事件，并根据不同的事件做出智能化的分析与处理，为相应的决策提供支持。计算机网络安全评估还需要对各类漏洞信息实现准确的识别与追踪，可有效完善后续的网络安全评估工作。

除此之外，计算机网络安全评估还要有广泛的联动范围与稳定的运行状态。即使发生各类异常，也能有效地进行评估与防护，与主流的网络安全设备进行联动。

（二）人工智能技术在计算机网络安全评估中的应用

人工智能技术有着诸多优势，而且它与计算机网络安全的特性也较为贴合，因此可将两者有效的结合。从当前的实际情况来看，人工智能技术在计算机网络安全评估中的应用可从以下几个方面入手。

（1）智能防火墙。智能防火墙相比于传统的防火墙而言功能更加完善，它不仅具备监测和限制的功能，而且借助人工智能算法与深度学习，可对网络中的异常行为进行预测和识别。其建立的预测模型准确性较高，能够发现潜在的威胁，对于提高网络安全性有着重要的意义。

（2）网络入侵检测。人工智能技术在网络入侵检测中有着极大的作用，目前已经实现的智能化与自动化可以自适应地对各类入侵进行检测。在实际的应用过程中，随着使用时间的增长还能自动的学习网络特征，不断提升预测的准确性。

（3）智能数据分析。智能数据分析是计算机网络安全评估的重要环节，借助人工智能技术可广泛地收集各类数据，同时分析与挖掘其中的特征，进而针对性地识别网络攻击有效的增强网络安全性。

（4）智能风险评估。人工智能技术可对网络安全风险进行智能评估。在具体的应用中海量采集数据，将各类威胁分类、设置各类预警信息，帮助网络管理人员及时发现各类网络风险，进而提前做出防范措施。

（5）恶意软件防护。传统的病毒软件检测是对现有的病毒进行分析汇总制作病毒样本，当检测到与病毒样本相似时进行拦截，这种方式并不能有效地拦截新型病毒。而借助人工智能技术就可通过计算机学习算法进行大量的数据分析与处理，从海量的数据中归类总结恶意软件的特征，便可有效识别新的恶意软件。特别是在恶意软件行为模式分析方面，人工智能还可为相应的网络安全研究人员提供基础资料，这就极大方便了后续的管理与决策。

在实际的应用中，人工智能技术还可自动生成反向工程

代码模拟攻击者的各类行为，通过模拟就能检测系统的漏洞，辅助完成防毒软件的优化与完善。

从上述的分析可以看出，人工智能技术在计算机网络安全评估方面有着极大的优势，目前也应用于很多实践中。随着人工智能技术的不断成熟，计算机网络安全评估与人工智能技术的结合将会更加紧密。

（三）人工智能技术在计算机网络安全评估中应用的局限性

人工智能技术是基于海量的数据进行模拟训练，数据越多其判断的准确性也会进一步提升。但在计算资源与能源有限的情况下，人工智能技术的功能也会受到限制。因此，在一些新的网络安全领域人工智能技术的应用就存在一定的局限。如果能把时间延长，并且不断的补充数据，人工智能仍可以通过模拟训练快速的适应，这也是人工智能技术在当前受到广泛关注的核心原因之一。

## 结束语

近几年，计算机网络安全受到社会各界的广泛关注，但各类网络安全事件却仍层出不穷。因此，需要不断引入新的技术来完善计算机网络安全评估工作。人工智能技术借助其较强的适应性、科学的自主决策、强大的自推理能力，在计算机网络安全评估中能够发挥重要的作用。本文结合实际情况分析了智能防火墙、网络入侵检测、智能数据分析、智能风险评估、恶意软件防护五个方面的具体应用。同时，也针对性地探究了人工智能技术在计算机网络安全评估中的局限性，希望可以借此给人工智能技术与计算机网络安全评估的结合提供一定的参考与启示。

## 参考文献

[1]喻国明，兰美娜，李玮.智能化：未来传播模式创新的核心逻辑——兼论“人工智能＋媒体”的基本运作范式[J].新闻与写作，2017(03)：41-45.

[2]杨坤平，李卫峰.基于人工智能的高校计算机网络信息安全研究[J].长江信息通信，2022，35(09)：137-139.

[3]宋人愚.人工智能时代高校计算机网络信息安全问题研究[J].计算机产品与流通，2019(06)：209.

[4]朱世强，王永恒.基于人工智能的内容安全发展战略研究[J].中国工程科学，2021，23(03)：67-74.

[5]李峰，赵运福，吉翔.计算机网络信息系统安全评估研究[J].信息与电脑(理论版)，2016(12)：195-196.

[6]牛旭.基于粒子优化神经网络的计算机网络安全评估模型[J].电子世界，2018(14)：101-102.

[7]盛海.试论计算机网络安全评估技术[J].青春岁月，2012(16)：367.

[8]胡春.基于神经网络的计算机网络安全评估体系研究[J].电脑知识与技术，2015，11(30)：139-141.

**作者简介：**

**刘宁(1987－)，男，汉族，黑龙江大庆人，硕士，讲师，铁人学院、大庆职业学院，研究方向：物联网教学。**