人工智能驱动的网络安全漏洞自动发现与修复技术研究

冉文端　周学永
河北方维网络技术有限公司　河北　石家庄　050000

摘　要：自动发现和修复网络安全漏洞是目前网络安全领域中一个重要的研究方向。文章旨在探索将人工智能技术应用于网络安全漏洞的自动发现及修复，为网络安全防护工作提供一种新思路、新方法。本文首先对网络安全漏洞定义，分类，危害及现有检测技术进行综述，对人工智能技术检测网络安全漏洞进行展望。对基于人工智能自动发现网络安全漏洞技术进行了系统研究，提出了一种自动检测网络安全漏洞的方法，并将人工智能技术运用于网络入侵检测。对人工智能驱动下网络安全漏洞自动修复技术展开论述，主要内容包括人工智能对网络安全漏洞修复的影响，基于人工智能技术的服务器端集群安全漏洞发现方法和工业互联网安全漏洞管理及人工智能技术等。最后对整篇论文进行总结，着重指出人工智能技术应用于网络安全领域有着广泛的前景，但是还需要不断地优化和改进才能建立一个较为安全的网络环境。

关键词：人工智能；网络安全漏洞；自动发现；自动修复；技术研究

引言

数字化时代背景下，网络安全漏洞自动发现和修复技术变得格外关键。随着人工智能技术的快速发展，人工智能技术在网络安全领域中的应用也渐渐成为人们关注的焦点。但现有技术还需要在自动化和智能化上进行改进，尤其是对漏洞进行快速检测和精准修复，而现有的方法也面临着很多挑战。文章旨在探索将人工智能技术应用于网络安全漏洞的自动发现及修复，为网络安全防护工作提供一种新思路、新方法。

1 网络安全漏洞概述

1.1 网络安全漏洞的定义与分类

网络安全漏洞就是指计算机网络系统中因设计，实现或者配置等方面存在缺陷而导致系统安全性下降，并有可能因为恶意使用而获得未经授权访问或者实施攻击等弱点。网络安全漏洞有很多分类方法，可从各个角度对其加以分类。按照漏洞产生的根源，网络安全漏洞可划分为软件漏洞，硬件漏洞以及通信协议漏洞。软件漏洞，主要是指操作系统、应用程序和其他软件产品上的不足；计算机硬件设备，例如CPU和内存，都可能存在硬件漏洞；网络通信协议中的缺陷被称为通信协议漏洞。[1]

网络安全漏洞又可按其性质及影响范围分为本地漏洞与远程漏洞。本地漏洞即要求对目标系统有一定的权限或者接入能力才可使用，远程漏洞可远程使用，不需要对目标系统进行直接接入。另外，网络安全漏洞按其严重性可划分为高危、中危与低危。高危漏洞使用后，会造成严重安全事件发生，例如对系统进行全面管控，数据大量外泄；中危漏洞与低危漏洞影响程度比较低，但是仍需充分重视。

1.2 网络安全漏洞的危害与影响

网络安全漏洞指计算机系统、网络设备或者应用程序等方面的不足或者薄弱之处，可供恶意用户使用以破坏系统安全，盗取敏感信息或者进行非授权操作。一是网络安全漏洞会造成个人敏感信息外泄。伴随着互联网的广泛使用，网络上储存了越来越多的个人数据，例如身份信息，财务信息和通信记录。一旦非法获取这类信息，不仅会侵犯个人隐私，也会诱发身份盗窃和金融诈骗犯罪行为；二是网络安全漏洞也会给企业的经营带来很大的影响。企业在日常运营中高度依赖网络，这包括但不限于客户关系的维护、供应链的管理以及财务报表的编制。网络安全漏洞一旦被钻了空子，就会造成商业机密的泄露，客户信任度的损失，经济损失乃至法律责任的承担；另外，网络安全漏洞也会威胁国家安全。关键基础设施，例如电力网，交通系统和通信网络，都离不开网络技术；三是网络安全漏洞也会引起连锁反应从而影响到整个网络的稳定可靠。鉴于现代网络系统的高度复杂性和互联性，任何一个系统的安全缺陷都有可能对其他系统，乃至整个网络系统造成影响。

1.3 现有网络安全漏洞检测技术

目前，网络安全漏洞的检测技术主要涵盖了静态分析、动态分析、模糊测试以及渗透测试等多种方法。静态分析则通过查看软件代码或者配置文件，找出可能存在的安全漏洞。该方法具有无需运行软件、能迅速检测出编码存在逻辑错误、编码实践不够安全等优点；动态分析通过对软件的执行和对软件行为的监测，检测出安

全漏洞。在进行动态分析时，通常会利用如动态二进制插件（DBI）这样的工具来搜集实时运行的数据；模糊测试就是将随机或者半随机的数据输入到软件中，从而检测出安全漏洞。该方法能够检测出由于输入处理不当而造成的各种漏洞，例如格式字符串攻击和缓冲区溢出。模糊测试具有自动化程度高、能检测出某些不可预知漏洞等优点；渗透测试通过模拟攻击者行为，对系统进行安全性评价。该方法能够检测出系统配置缺陷和访问控制漏洞。

2 人工智能驱动的网络安全漏洞自动发现技术

2.1 基于人工智能的漏洞挖掘技术

漏洞挖掘在网络安全领域中具有重要意义，传统方法主要靠人工进行分析，存在效率低、易遗漏等问题。以人工智能为基础的漏洞挖掘技术可以通过机器学习和深度学习从海量代码中自动化发现潜在安全漏洞。这一技术核心是构造高效的特征提取与分类模型来提高漏洞挖掘精度与效率。[2]

首先要对目标软件源代码或者二进制文件预处理并提取可供分析的特征。这些属性可表现为代码结构信息，语法信息和语义信息。接着，通过机器学习算法训练特征并构造漏洞和非漏洞分类模型。在完成模型的训练之后，将需要检测的代码输入到模型中，并根据模型输出的数据来判断是否有潜在的安全缺陷。另外，将深度学习技术运用到漏洞挖掘方面也有明显效果。深度学习模型可以对代码高层次特征进行自动学习，并进一步提升漏洞挖掘精度。例如，像卷积神经网络（CNN）和循环神经网络（RNN）这样的模型已经在二进制代码的漏洞检测中得到了成功的应用。

2.2 模糊测试在工控协议漏洞挖掘中的应用

工业控制系统（ICS）被视为现代工业生产的关键部分，它的安全性对生产的安全性和社会的稳定性有着直接的影响。但在工业互联网飞速发展的今天，工控系统安全问题也越来越凸显。模糊测试是挖掘漏洞的有效手段，对工控协议安全性分析有很大的应用。模糊测试是指通过自动产生大量随机或者半随机测试数据来检测目标系统是否可能存在异常行为或者崩溃。在工控协议漏洞挖掘上，模糊测试可用于协议各层，包括语法、语义及时序。首先要搭建工控协议测试框架，该框架由协议解析器，测试数据生成器以及异常检测器三部分组成。测试数据生成器的主要职责是产生与协议标准相一致的测试数据，这包括合法的和有意为之的非法数据。接着，把产生的测试数据导入工控系统并观察其反应与行为。

2.3 基于人工智能的网络安全漏洞自动检测方法

在网络安全的领域中，人工智能技术的应用为漏洞的自动化检测开辟了新的途径。传统漏洞检测方法主要依靠签名匹配、规则引擎等技术，它们面对新的、未知攻击模式常常显得无能为力。人工智能技术特别是机器学习算法可以通过对海量网络行为数据进行学习来发现异常模式以达到发现未知漏洞。[3]例如，通过深度学习中的卷积神经网络（CNN）来分析网络流量，能够有效地区分恶意流量和正常流量之间的区别。除此之外，如循环神经网络（RNN）和长短期记忆网络（LSTM）这类算法在处理时间序列数据上展现了卓越的性能，它们能够有效地识别持续的网络攻击行为。但人工智能在自动检测网络安全漏洞时也遇到了数据标注难和模型泛化能力欠缺的难题。

2.4 人工智能技术在网络入侵检测中的应用

网络入侵检测在网络安全领域起着至关重要的作用，它旨在对网络异常行为以及潜在威胁进行及时的发现与反应。人工智能技术应用于网络入侵检测主要有以下几点：一是利用机器学习算法实时分析网络流量，能够自动识别恶意行为例如DDoS攻击和SQL注入；二是采用深度学习技术建模网络行为，能够更加精确地识别复杂攻击模式；三是人工智能技术也能辅助人工分析并通过智能推荐系统给安全分析师决策支持。但是在网络入侵检测过程中人工智能的运用也有其局限性，例如模型训练对标注数据要求较高，检测系统有可能受到恶意攻击者的回避。

2.5 人工智能在网络安全漏洞修复中的作用

修复网络安全漏洞对于抵御网络攻击具有重要意义。传统漏洞修复方法大多依靠人工分析与手动修补相结合的方式，该方式效率较低，难以处理越来越复杂的网络环境。[4]将人工智能技术运用于网络安全漏洞修复能够显著提升修复效率与质量。人工智能可通过如下途径来协助漏洞修复工作：一是使用机器学习算法分析漏洞数据并自动识别其特征与规律，从而为修补工作奠定基础；二是利用深度学习技术建立漏洞修复策略模型并自动产生修复方案；三是人工智能也能辅助自动化测试来验证修复方案。但是人工智能在漏洞修复方面也遇到了一些难题，比如模型训练对数据要求较高，修复方案会出现安全隐患。今后的研究还需在改善模型准确性和加强修复方案安全性上下功夫。

3 人工智能驱动的网络安全漏洞自动修复技术

3.1 人工智能在网络安全漏洞修复中的作用

人工智能技术对于网络安全漏洞的修复有着举足轻重的作用。一是人工智能可以快速地对漏洞进行识别与

定位，提升漏洞检测效率与准确性。二是人工智能可以自动产生修复方案以减少人工干预和修复成本。[5]另外，人工智能可以对网络环境进行实时监测，发现和修补新漏洞，增强网络安全防护实时性。

人工智能对网络安全漏洞修复具有如下功能：漏洞快速识别与定位：人工智能借助深度学习及其他技术手段，本发明可以对网络流量及系统日志进行快速分析，确定可能存在的漏洞及异常行为；自动产生修复方案：人工智能可以根据漏洞特点及上下文信息自动产生修复方案，其中包括修补代码和更新配置；降低修复成本：人工智能自动化修复能力、减少人工分析修复工作量、降低修复成本；增强实时性：人工智能可以对网络环境进行实时监测，发现和修补新漏洞，增强网络安全防护实时性。

3.2 基于人工智能的服务器集群安全漏洞检测方法

服务器集群在现代网络架构中占据着举足轻重的地位，它的安全与否直接影响着整个网络系统是否安全。基于人工智能技术的服务器集群安全漏洞检测方法可以有效地提高服务器集群运行的安全性。所述方法包括如下步骤：数据采集：从服务器集群中采集日志数据，配置信息和网络流量，作为基础数据进行后续分析；特征提取：采用人工智能技术对采集的数据进行异常访问模式和配置错误这类安全漏洞的相关特征提取；漏洞识别：根据提取到的特征通过分类算法识别服务器集群中的漏洞并判断安全漏洞；漏洞修复：对确定的漏洞人工智能系统可以自动产生修复方案并且在需要时自动修复。

3.3 工业互联网安全漏洞管理与人工智能技术

工业互联网是新一代信息技术和制造业的深度融合，安全显得格外重要。将人工智能技术运用于工业互联网安全漏洞管理可以有效地提升安全管理效率与成效。人工智能应用于工业互联网的安全漏洞管理主要有如下几方面内容：漏洞发掘：运用人工智能技术对工业互联网系统的软，硬件和协议进行深入分析，发掘潜在安全漏洞；漏洞评估：评价挖掘出来的漏洞并判断危害程度及影响范围，以便后续修补；漏洞修复：针对漏洞具体情况，人工智能系统可以自动产生修复方案并且在需要时自动修复；安全策略优化方面：人工智能技术可以针对工业互联网对安全的要求与特点对安全策略进行优化，提升整体安全性。

4 结束语

通过对人工智能技术自动发现和修补网络安全漏洞的深入探究，揭示出其对于提高网络安全防护能力所具有的巨大潜能。国内外学者一般认为人工智能技术可以有效地提高网络安全漏洞检测速度与精度，减少人工分析的复杂性与代价。

研究结论显示人工智能技术对于网络安全漏洞自动发现及修复有明显的优势，同时也面临着一些局限性及挑战。比如人工智能算法在泛化能力，数据隐私保护以及算法可解释性方面还有待深入研究与解决。另外，人工智能技术在实践中需要结合当前网络安全防护体系形成协同防御机制。

人工智能技术在为网络安全漏洞自动发现和修补提供全新解决方案的同时，也提出了全新的挑战与难题。要积极应对上述挑战，并不断地进行探索与创新，促进人工智能技术进一步运用到网络安全领域中，助力于更安全可靠网络环境的建设。

参考文献

[1]郝宁.基于人工智能技术的网络安全管理应用研究[J].信息记录材料,2024(2):66-68.

[2]李成.基于人工智能理论的网络安全管理技术应用研究[J].计算机应用文摘,2024(6):80-81.

[3]李流丽.基于人工智能的网络安全监测与防御技术研究[J].移动信息,2024(4):158-160.

[4]范康康,王颖慧.基于人工智能技术的网络安全漏洞挖掘应用研究[J].网络安全和信息化,2023(12):48-50.

[5]李永杰,侯昊,王广硕,等.人工智能技术在网络安全漏洞挖掘中的应用[J].数字技术与应用,2023(3):55-57.