文章编号：2096-1472(2023)-04-52-05
DOI:10.19644/j.cnki.issn2096-1472.2023.004.012

基于人工智能的网络空间安全防御策略研究

刘邦桂

(广东开放大学人工智能学院，广东 广州 510091)
✉liubanggui@qq.com

摘　要：在网络的攻防博弈中，传统网络空间的安全防御机制在海量网络动态隐藏信息中逐渐落于防守端下风，以目前网络空间安全存在的问题为出发点，首次从攻击与防御、知识与模型、漏洞与利用等角度进行人工智能与网络空间安全融合分析，以此为基础总结了基于人工智能的网络空间安全攻击分类。通过分析决策树、k邻近等深度学习算法的工作机制和适用场景，探讨了在垃圾邮件、恶意软件、网络异常等网络空间安全防御的应用，为网络空间安全在生成对抗网络为热点的环境下，构建有效的智能网络安全动态防御规则，为实现网络安全运维智能化、自动化提供参考。

关键词：人工智能；网络空间安全；生成对抗网络；安全防御机制
中图分类号：TP393.2　**文献标识码**：A

Research on Cyberspace Security Defense Rules based on Artificial Intelligence

LIU Banggui

(*School of Artificial Intelligence*, *the Open University of Guangdong*, *Guangzhou* 510091, *China*)
✉liubanggui@qq.com

Abstract: In the game of network attack and defense, traditional cyberspace security defense mechanism has gradually fallen behind the defense end in the massive network dynamic hidden information. Aiming at the problems of cyberspace security, this paper proposes to carry out fusion analysis of AI (Artificial Intelligence) and cyberspace security for the first time from the angles of attack and defense, knowledge and model, and vulnerability and utilization. On this basis, the classification of cyberspace security attacks based on AI is summarized. By analyzing the working mechanism and application scenarios of deep learning algorithms such as Decision Tree and K-Nearest Neighbor, this paper discusses the application of cyberspace security defense in spam, malware, network anomaly and so on. It provides a reference for cyberspace security to build effective intelligent dynamic defense rules for network security, and realize the intelligence and automation of network security operation and maintenance under the environment of Generative Adversarial Networks as a hot spot.

Keywords: artificial intelligence; cyberspace security; generative adversarial network; security defense mechanism

1 引言(Introduction)

在2021 年公布的十大最新技术排行榜中[1]，人工智能与网络空间安全技术均位列其中。随着网络在经济、政治、文化等领域的全面应用，与网络相关的公共安全问题不断增多，每年全球在网络空间安全上的花费超过数十亿美元，中国、美国、俄罗斯等国家相继出台了针对网络空间安全领域的建设规划。全面加强网络空间安全软件和硬件设施建设，是保障社会稳定、推动国家治理体系和治理能力现代化的基础。人工智能技术的发展令人感到惊叹，它在攻击点多、面广的新型网络中发挥出不可比拟的优越性。以生成对抗网络为代表的人工智能技术和思想在网络空间安全防御策略中的广泛应用，表明人工智能技术有助于构建更加智能、全面的网络空间防御体系，成为网络安全创新发展新的方向。在网络空间安全领域应用人工智能技术，是一次应用上的创新，

基金项目：2022年广东开放大学(广东理工职业学院)双师工作室项目“网络系统集成双师工作室”(12342127).

是对网络空间的一次防御加固，也是未来网络空间安全领域发展的热点和难点，具有现实的研究价值。

2 目前网络空间安全存在的问题(Problems in current cyberspace security)

网络空间安全包含物理、系统、内容等的安全[2]，其中物理安全是指参与连接人和物等要素的安全；系统安全是指构建网络互联及应用的软件设备、硬件设备和通信数据的安全；内容安全是指在网络互联环境中保证通信数据的机密性、完整性、可靠性。新形势下，网络空间安全存在以下问题。一是人工智能技术应用于身份识别、垃圾邮件、拒绝服务、恶意代码等网络攻击中，呈现出攻击手段自动化、智能化、隐匿化、规模化等特点，能有效躲避、绕过防御端的检测；二是网络应用范围越来越广，使其边界急剧扩张，构成网络的结构越来越复杂；三是网络空间具有通信数据出现量大、类型复杂等特点，传统的威胁检测系统和手段已经疲于应付大量数据日志，未能很好地起到保护网络空间安全的作用；四是网络空间安全人才急缺，随着各种新技术错综复杂地融合，技术单一的网络空间安全工程师很难应对目前层出不穷的安全问题，全面型人才是解决安全问题的核心力量；五是传统网络空间安全理念已经不能适应时代发展的要求，要改变以固定规则匹配攻击类型的被动防御方式，不断转变为主动防御方式，并能主动进行规则学习；六是虽然网络在各领域的应用越来越深入，但是使用者用网层次和安全意识不一，大部分使用者的网络空间安全意识淡薄。以上问题都是需要网络空间安全工程师打破传统被动的防御手段，在人工智能技术新环境下勇于创新并实践。

3 人工智能与网络安全关联度分析(Analysis of the correlation between artificial intelligence and network security)

人工智能与网络空间安全是两个交叉学科，两个领域均有非常全面的理论架构和技术体系。认真厘清两个学科之间的逻辑关系，是更好地将人工智能技术运用于网络空间安全的关键。网络空间安全起源于计算机网络技术，人工智能技术与计算机网络技术TCP/IP(Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议)和OSI(Open System Interconnection，开放式系统互联)参考模型的层次对应关系如图1所示。

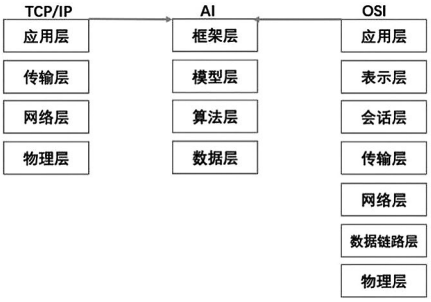

图1 人工智能与网络参考模型的对应关系

Fig.1 Correspondence between AI and network reference model

(1)攻击与防御。网络空间安全是指对网络空间信息在产生、传输、使用、存储处理过程中的安全防护，包含网络系统安全、数据安全、内容安全、行为安全和安全管理。理解网络空间安全的一个重要维度是参与者，即攻击者与防御者，二者之间存在典型的“道高一尺，魔高一丈”关系，因此都迫切需要利用更先进技术应对对方的攻击或防御行为。人工智能具备自动推理、分析识别等能力，是攻击者与防御者都迫切需要的新技术。由此，可以引出人工智能与网络空间安全的重要结合点，即人工智能应用于网络空间攻击与防御[3]。其中，人工智能技术应用于安全防御，是从防御者的角度出发，试图引入人工智能技术加强网络空间安全；而人工智能技术应用于攻击各类网络空间，是从攻击者的角度出发，试图引入人工智能技术提升攻击效率和效果。

(2)知识与模型。可以借助知识层次理解人工智能安全。知识的表示、分析挖掘是人工智能的核心[4]，相比于信息和数据，知识位于更高的层次，而这种层次差异体现在知识的语义特征方面。知识信息具备更强的蕴含表达能力，由此更容易导致一些广泛意义上的网络空间安全问题。此类安全问题主要发生在内容语义层面，涉及伦理道德、隐私性、健康性、公平正义等。微软在线机器人Tay发表偏激言论、人脸识别的滥用、大数据“杀熟”、个人信息的过度索取、算法对物流配送员的控制、推荐算法推荐没有价值的低俗内容等现实的网络空间安全问题，都是内容语义层面表现出来的问题。随着人工智能在网络空间中的应用和推广，迫切需要建立可信、可靠的基于人工智能技术的网络空间安全防御体系，而模型安全是其中的核心。

(3)漏洞与利用。不论哪种形式的安全问题，其根本原因是存在漏洞及可利用的途径。由于信息系统复杂性高，各种软件和硬件存在漏洞不可避免。攻击者与防御者之间的对抗通常都是围绕漏洞的发现、分析、利用与封堵。漏洞被封堵之后就失去了利用价值，因此攻击者热衷于寻找零日漏洞[5]，趁对方毫无防备时发起攻击，而零日漏洞普遍存在于新技术、新系统中。人工智能在网络空间中的应用还处在发展过程，不可避免地存在一些未知漏洞，可能存在于知识处理的模型、算法和平台中。从知识层次来看，相比于信息和数据，以知识处理为中心的新型应用显然为攻防二者开辟了新的对抗战场。因此，人工智能模型、算法和平台的漏洞发现与利用，成为人工智能安全发展的主要推动力。

4 网络空间安全知识架构(Architecture of cyberspace security knowledge)

人工智能被认为是包括机器学习在内的一个广泛的研究领域，机器学习中包含了深度学习。机器学习有监督学习、无监督学习和强化学习三种类型[6]。机器学习技术也可以根据需要解决问题的种类划分为分类、聚类、回归、降维度和密度估计等技术，与此对应的机器算法也就有支持向量机、贝叶斯网络、决策树、随机森林、分层、遗传、相似度等。

在人工智能时代，网络空间攻击的分类如图2所示。其中，分类是根据输入未知数据的特征或特性进行类别区分，因为应用的数据是有标记的，所以是监督学习。在网络安全

框架中，可以用于正确识别同一类的攻击。通过训练数据驱动学习，将合法电子邮件发送给收件箱、垃圾邮件投入垃圾文件夹。同样，基于文本内容网页分类也是分类，例如新闻、广告等网页。聚类与分类不同，属于无监督学习，在分类前没有获得类别的信息情况下就自动识别样本类别，使用数据进行多次迭代，比如基于统一协议的恶意软件攻击、基于不同签名的多态恶意软件。回归主要通过对数据的统计，分析自变量和因变量之间存在关系实现数据预测，特别是对攻击者先前行为日志数据进行分析，预测即将发生的攻击，以此进行必要的防御。此时，必须采用高度动态的算法且需要算法有自动学习能力，比如入侵检测、智能防火墙等。

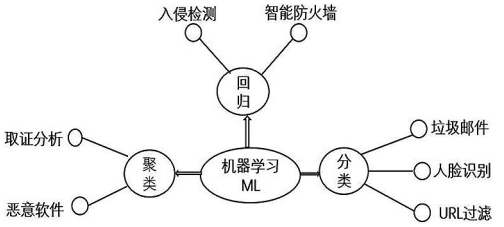

图2 机器学习与攻击种类

Fig.2 Machine learning and types of attacks

目前，Python语言是网络安全人员用于渗透测试与恶意软件分析的最佳选择，它提供了大量用于网络空间安全的库。其中，pefile库用于分析可执行文件，主要在静态恶意软件分析时查找软件是否被破坏或加载恶意代码，类似于用MD5和SHA1摘要算法检测软件的完整性；volatility库是可以编程的实用程序，用来对可执行程序运行内存进行分析，发现存在的恶意软件代码，通常默认安装在恶意软件分析和渗透测试的发行版本中，允许从内存中提取API(Application Programming Interface，应用程序编程接口)挂钩、网络连接、内核模块等进程的重要信息；TensorFlow库主要应用在监测欺诈程序、检测网络异常支付、生物认证、网络用语异常行为等方面，特别是应用在生成对抗网络，可以生成与原生物特征一样的样本，这对传统人脸识别和语音识别提出了挑战。

5 人工智能助力网络空间安全(Artificial intelligence helps cyberspace security)

5.1 检测垃圾邮件

电子邮件是计算机网络诞生时最早的应用，是网络通信最重要的手段，因此电子邮件理所当然地成为网络攻击的主要载体。其中，垃圾邮件是未经用户许可就强行发送到用户邮箱中的任何电子邮件[7]，通常包含广告、病毒等。一般来说，过滤垃圾邮件的方法有知识工程和机器学习[8]。使用知识工程方法时，由于邮件传输流量巨大、需要选取一定数量的关键字、需要选择一个不断更新以区分垃圾邮件的阈值、垃圾邮件发送者会尝试使用不同的策略欺骗过滤器等，导致这种以正则表达式识别垃圾邮件的静态规则已经很难跟上攻击者的步伐，所建立规则的泛化能力也特别差。因此，利用机器学习算法完成这一任务将是必然选择。目前，检测垃圾邮件是AI(Artificial Intelligence，人工智能)在网络安全领域最成功的应用。

5.1.1 感知机

模仿人脑神经元分层结构，将给定输出结果与一个或者多个输入层关联起来。感知机通过预先选择一个适当的阈值，通过线性分类器计算，如果电子邮件分数超过了阈值，就会分类为垃圾邮件。但是，感知机是一个二元线性分类器，局限于线性可分情况下使用，容易在数据周围振荡。

5.1.2 支持向量机

与感知机不同，支持向量机是监督学习方法，所识别的超平面不再局限于感知机线性模型，是感知机的一种扩展。与感知机尽量使分类错误最小化不同，SVM(Support Vector Machine，支持向量机)目标是使超平面与支持向量之间的距离最大化。支持向量机除了以文本方式分类垃圾邮件，还可以通过图片方式检测垃圾邮件，可分为基于内容、非基于内容的过滤，其中前者与本文方式类似，主要采用光学字符识别技术识别图片中的文字，后者主要利用计算机生成正常和垃圾邮件在图片属性上(比如颜色不同)的特征来分类。因此，为了提取图片特征，需要进一步使用神经网络以及深度学习算法。

5.1.3 朴素贝叶斯

通常个人邮件数量不多，很难成为训练样本。由于概率估计原理来源于著名的贝叶斯定理，先验概率可以作为后验概率的输入，以此动态更新概率统计，所以朴素贝叶斯最适合这种只需要很少输入就可以分类的情况，在逐步累加的样本信息中不断优化先前的估计，动态调整预测模型。结合文本分类技术[9]，能够动态检测垃圾邮件中的关键字。

5.1.4 自然语言包

自然语言处理是人工智能的子领域，包含对人类语言的分析和理解，能够从非结构化数据中获得敏感信息，应用在翻译、语音识别、情感分析、信息检索等领域。其中，自然语言工具包可以结合朴素贝叶斯用在垃圾邮件的检测中。

5.2 检测恶意软件威胁

恶意软件是包含对计算机构成威胁代码的文件[10]。恶意软件有木马、僵尸网络、勒索软件、零日漏洞等，可以嵌入可执行文件或隐藏在图片文件中，甚至普通文本文件也可以成为其传播载体。以上方式都有一个共同特点，即破坏原有文件的完整性。所以，文件完整性检测是网络安全体系结构中的一个重要环节，能够有效防止恶意软件的攻击。恶意软件传播速度越快，所构成的威胁就会呈现指数级增长。目前的恶意软件有静态、动态、多态、变态等形式和分类，检测需要有灵活的应对策略，常见的检测手段有哈希文件计算、系统监视、网络监视等。然而，传统基于电子签名和图像文件的哈希检测方法已经不足以应对恶意软件的攻击，引入人工智能技术重要且必要。

5.2.1 *k*均值聚类算法[11]

恶意软件检测过程中，检测方法和检测效率都很重要，正确识别恶意软件的行为相似性很关键，这就需要将恶意软件样本及同类型恶意软件相关联，实现检测自动化。关联性

分析可以利用k近邻算法和k均值算法，将恶意软件的不同特征用距离关联，用来估计其相似性，单个特征作为n维空间中的一个点，选择一个合适的规则计算点与点之间的距离，作为度量。目前，可用来确定距离的度量有欧几里得距离、切比雪夫距离、曼哈顿距离，如果软件特征较多，可以选择欧几里得距离。度量确定后就是选择合适的聚类算法，k均值算法是使用较为广泛的一种无监督算法，该算法可以根据所选欧几里得距离度量将数据分为k个不同子组，最小化由维度空间中点和各自质心之间计算出的度量所表示的代价函数，最后返回对应分组样本。这个过程是选用scikit-learn库中的算法实现的，该方法操作简单，适用于大数据集，但是在n维空间中会以稀疏形式发生维数灾难现象。

5.2.2 决策树

决策树使用二叉树进行数据分析和处理[12]，算法通过一系列if-then-else决策对学习过程进行建模，在迭代过程中把软件样本最终以数值和类别形式进行区分，代表的是一种非线性分类器，无法简化为平面中的直线或超平面。决策树的缺点是会出现过拟合现象，对样本变化会产生比较大的振荡，因此在实际做法中可以使用决策树集合即随机森林让每棵树都有投票权，票数最高的预测就是最后的结果。

5.2.3 隐马尔可夫模型(Hidden Markov Model，HMM)[13]

前面两种方法都是基于静态恶意软件检测方法，如果应用在动态恶意软件，甚至多态和变态恶意软件检测中，会有误报情况发生。对于多态恶意软件以及零日攻击软件的检测，可使用基于HMM机器学习算法，这是一个无法直接观测系统状态的马尔可夫过程，未来状态概率分布取决于当前状态。

5.2.4 卷积神经网络

神经网络模仿人脑学习机制，由输入层、输出层和隐藏层组成。卷积神经网络具有图像识别功能，通过卷积运算提取输入的恶意软件图像特征，将其转换成二进制序列，通过转换灰度图像中存在的布局和纹理相似性，利用图像分类k邻近算法实现分类。这种方法既能识别恶意代码修改部分，使恶意软件整体结构不被破坏，也可以快捷识别同一家族的不同变体。

5.3 网络异常检测

在网络异常检测领域，有基于电子签名异常检测和流量异常检测。其中，基于电子签名的异常检测一般是通过已受攻击的签名知识库来匹配同类攻击，但它有明显的缺陷，即必须通过不断更新签名库来识别新型的网络攻击。基于流量的异常检测主要通过检测时间内主机的连接数、不寻常通信端口的流量、单位时间内突发流量高峰、网络中固定主机占用大量带宽等方式完成检测。

5.3.1 基于人工智能的入侵检测系统[14]

防火墙是一组预先定义的网络规则集合。通常放置于内网和外网边界，进行网络异常检测与防范，经历了包过滤、应用代理、状态检测三个不同的发展阶段。不管在哪个阶段，最关键的都是进行网络异常检测，因此配备入侵检测系统就显得更加重要。根据基于签名库和流量的检测种类，相应出现了基于主机IDS(Intrusion Detection System，入侵检测系统)和基于网络流量IDS。随着人工智能的高速发展，传统检测系统已经无法应对如今的网络攻击。这时，利用监督和无监督学习算法更新检测解决方案就显得必须和重要，基于异常IDS出现了。这种新检测方法需要设置对不同数据进行分离的阈值，让数据集之间存在一定距离，运用聚类算法对数据进行计算，评估其分布规律性，从而实现分类和达到自动检测目的。在这个过程中，我们需要不断分析各种服务日志，并将其转换成有用的数据集；还必须把类似于恶意软件、零日攻击、会话劫持、端口扫描等各种攻击的特征分类出来，为算法提供更加有代表性的数据集。

5.3.2 僵尸网络检测

僵尸网络是基于流量的网络异常检测的难点，是指攻击者试图通过发送木马让网络中的计算机运行，然后不知情地接受攻击者的命令后攻击网络中其他主机的行为。攻击者通常结合分布式计算以及区块连技术让僵尸网络参与发送垃圾邮件、发起DDoS(Distributed Denial of Service，分布式拒绝服务)、密码暴力破解等攻击。僵尸网络通常有三个阶段：一是通过不同方式让网络中的主机运行恶意软件；二是加入僵尸网络；三是将僵尸网络传播到其他主机。在僵尸网络中，受害主机为了接收新的指令，需要不断与远控主机进行信息沟通，并将从受害主机系统上获得的信息发送到服务器中。这个过程的典型特征是需要持续保持会话活跃性且定期进行数据交换。因此，检测僵尸网络最关键的就是数据通信流量，并能图形化地呈现出来。深度学习算法比如k邻近算法、决策树、高斯朴素贝叶斯模型都可以较好地用于僵尸网络检测。

5.3.3 运用高斯分布进行异常检测

高斯分布广泛应用于检测数据分布建模，可识别数据中的离群点。离群点假定的异常元素相对于其他数据存在明显差异，大多数据越是紧密集中在均值附近且方差越小，离群点所假定的异常值就越明显。检测需要导入Python中的numpy、pandas、matplotlib等库，同时加载检测数据流延时和网络吞吐量的值，验证样本分布是否像高斯分布及以图形式显示相应的值，最后将数据绘制在散点图上，用可视化方式识别离群点。

5.4 用户行为异常检测

用户账号是网络安全体系结构中的一个重要环节，主要用来保证网络中数据的完整性和机密性。传统密码在健壮性方面已经做得很好，其组成包括数字、字母、符号等，但是随着各种网络服务平台的增加，密码管理成为用户们最大的困惑。一码通用成为大家的习惯，这就给攻击者提供了可乘之机，一旦密码被破解，全部的网络服务平台就成为攻击者的控制对象。当然，各类网络服务平台都采取了各种保护措施，如密码地理区域限制、动态口令卡二级保护、手机验证码等，还使用了传统密码异常检测方法，如暴力访问尝试次

数控制、同账号同时间异地登录、不同设备登录、用户键盘打字频率等，在一定程度上降低了攻击的成功概率。尽管如此，针对用户身份的攻击依然是网络安全领域的重灾区，传统密码保护措施与安全检测方法之间矛盾越来越大。

5.4.1 采用击键识别用户身份验证

把数据挖掘和机器学习结合起来，从用户关联数据信息中识别出潜在的账号违规行为，并采取相应的防御操作成为新趋势，特别是应用在目前无监督学习和监督学习适用于挖掘数据中潜在的用户可疑行为。把账号风险预测由检测违规行为转换到对正确特征进行监控，以积累用于训练的必要特征。但是，监督学习算法不足，受到分类标签的影响，难以识别新形式的异常活动，即使在后面检测过程中加入了新的检测规则，也不能避免放大先前标签所引入识别的误差。同样，对于无监督学习算法比如k均值算法，正确确定簇数量很重要，因为在实际应用中并不能确定账号分组必需的簇数量，所以不适用于检测用户可疑行为，也不能适用于以二进制分类值形式的用户特征。随着神经网络的发展，使用生物特征检测可疑账号越来越普及，其中击键输入与人脸虹膜、声音、指纹可以作为识别用户的特征。击键过程属于动力学领域，在这一过程中，个人的击键节奏和韵律等动态信息是唯一的生物特征。这个技术过程主要是在清除了各种干扰因素后，将用户相应的原始击键特征数据转换为正确表示用户特征的数据集，在这个基础上运用k邻近、支持向量机、多层感知机算法进行分析，可以根据攻击者击键特征识别出盗取别人账号的行为，并予以制止。

5.4.2 采用人脸识别用户身份

智能手机、平板电脑等终端设备基本配备了采集用户人脸信息的设备，让各种应用采用人脸识别实现登录成为可能。人脸识别是一种分类技术，其中利用线性代数进行“特征脸”识别是最常见的一种，识别分为实时图像识别和已有图像批量导入识别，本研究利用各终端设备摄像头实时采集的用户人脸作为采集数据，将待验证图像与图像集进行比对。在采集过程中受到光线、角度等客观因素和如人脸自然衰老等因素的影响，会出现“撞脸”情况，加上图片是高维数据，在识别过程中模型构建和数据清洗很重要，所以通常利用无监督降维算法、主成分分析法识别出主要代表性变量，从而减少变量数。第一步是去掉各种干扰因素、调整图片位置等归一化和去除噪声预处理，把图片转换成黑白色和用直方图均衡化图片解决因为光线原因导致的明暗度问题。这个过程虽然复杂，但是直接关系到识别速度和准确度；第二步是特征值提取，用k 维特征向量反映人脸图片的特征信息；第三步是用k邻近或者支持向量机等分类器对图片进行分类，并与已训练数据集进行比对后，实现人脸识别。

6 结论(Conclusion)

人工智能技术应用在网络空间安全领域具有独特的优势，如提升网络自动化管理的学习能力、加强识别网络威胁的推理能力、模糊数据的处理能力、创建网络管理机制和协作能力，以及有利于保证大数据处理技术和应用的安全性，有利于改进人工神经网络的整体功能。人工智能与网络空间安全相辅相成，人工智能在对网络攻击的感知、认知、防御、控制等方面都表现出显著的优势，同时其在网络空间安全领域的应用也促进了人工智能的发展。在人工智能和网络空间安全共同发展的历程中，神经网络、深度学习等新技术作用于网络攻防两端，特别是生成对抗网络(Generative Adversarial Network，GAN)[15]的出现，将两者关系更加紧密地联系起来，让网络空间安全进入了全新的发展阶段，也让人工智能展现出前所未有的优势，这将是未来的研究热点。

参考文献(References)

[1] 李荣.2021年应该关注的十大最新技术[J].计算机与网络,2021,47(10):46-47.

[2] 黄光能.数字经济背景下网络空间安全初探[J].办公自动化,2022,27(22):21-23.

[3] 王菲菲.人工智能技术在网络安全防护中的应用优势及策略探究[J].网络安全技术与应用,2022,(12):95-97.

[4]李令方.人工智能技术与网络空间的安全研究[J].通讯世界,2020,27(01):138-139.

[5]庞建波.黑客或利用Chrome零日漏洞展开攻击[J].计算机与网络,2021,47(03):56-57.

[6]方志伟.基于人工智能技术的网络空间安全防御研究[J].电子技术与软件工程,2021(14):240-241.

[7] 王琦,吴钟扬,黄陈蓉,等.基于词嵌入与生成对抗网络的垃圾邮件分类算法[J].南京工程学院学报(自然科学版),2018,16(03):20-27.

[8] 孙劲光,蒋金叶.深度置信网络在垃圾邮件过滤中的应用[J].计算机应用,2014,34(4):1122-1125.

[9] 贺鸣,孙建军.基于朴素贝叶斯的文本分类研究综述[J].情报科学,2016,34(7):147-154.

[10] 魏高山,俞叔刚.基于深度学习的恶意软件检测技术研究[J].计算机工程与应用,2021,57(22):1-14.

[11] 刘光源.基于K-均值聚类的软件测试数据生成算法[J].数字通信世界,2022(11):56-58.

[12] 张莉,丁毛毛,李玮,等.基于决策树算法的客服终端冗余数据迭代消除方法[J].计算技术与自动化,2022,41(4):118-122.

[13] 黄清,方木云.一种基于HMM算法改进的语音识别系统[J].重庆工商大学学报(自然科学版),2022,39(05):56-61.

[14] WANG Z, LIU J, SUN L. EFS-DNN: anensemble feature selection-based deep learning approach to network intrusion detection system[J]. Security and Communication Networks, 2022(22):1-14.

[15] YI S, LIU X, LI L, et al. Infrared and visible image fusion based on blur suppression generative adversarial network[J]. Chinese Journal of Electronics, 2023, 32(01):177-188.

作者简介：

刘邦桂(1983-),男，硕士，讲师.研究领域：人工智能技术，服务器技术，网络空间安全.