基于人工智能技术的计算机网络安全分析建模研究

白城钟
山东信息工程学院，山东潍坊 261000 18353617033@163.com

摘要

计算机安全技术对人们的日常使用至关重要。黑客和病毒入侵的高频率给用户的隐私带来了危机。人工智能技术正在逐步发展，其在计算机信息技术中的应用比较广泛。多样化的人工智能技术将为计算机网络安全的监督与预测提供技术支持。在日常生活和生产中，越来越多的智能产品出现并占据了重要的地位。 将人工智能技术应用到计算机网络安全管理过程中，可以有效利用人工智能技术更高效的计算能力及其强大的学习和模仿能力，进一步完善计算机系统。本文构建了计算机网络安全分析模型，并对今后计算机网络安全的研究提出了建议。

CCS 的概念

• 信息系统~信息系统应用~过程控制系统

关键字

人工智能;计算机网络安全;病毒入侵

ACM 参考格式:

白城钟。2020.基于人工智能技术的计算机网络安全分析建模研究。2020 年航空安全与信息技术国际会议(ICASIT 2020)， 2020 年 10 月 14 日至 16 日，中国威海。ACM，纽约，美国，4 页。https://doi.org/10.1145/3434581.3434709

ICASIT 2020, 2020 年 10 月 14-16 日，威海市，中国
& # 169;2020 年计算机协会。Acm isbn 978-1-4503-7576-4/20/10…$15.00
https://doi.org/10.1145/3434581.3434709

1 介绍

由于科学水平的不断提高，人工智能的相关技术也取得了显著的成果。当前，计算机信息技术越来越普及，人工智能技术在计算机网络安全管理过程中显示出越来越积极的意义[1]。如今，人工智能技术已经成为科学进步中最值得研究的课题之一。

国内外都给予了足够的重视和极为广泛的应用。在日常生活和生产工作中，越来越多的智能产品被生产出来[2]。与计算机的飞速发展相矛盾的是对计算机网络安全的研究。计算机网络发展越快，软件更新越频繁，计算机网络的安全性就越差。黑客会在计算机上安装的软件中寻找漏洞进行攻击，然后获取保存在计算机中的信息[3]。由于互联网技术的加速进步，旧的模式已经不再适用于当前的互联网环境，计算机空间的安全受到了威胁[4]。侵入计算机网络的渠道和技术更加先进，企业机密和个人隐私可能被泄露。计算机网络安全管理的研究迫在眉睫。在计算机安全管理中借助人工智能技术，将能够充分发挥人工智能技术优越的计算水平和优异的学习模仿特性，有效改善计算机安全管理，提高计算机分析数据的效率和效率，安全保障[5]。

由于科学水平的不断提高，人工智能技术有了很大的进步，计算机信息技术越来越普及，人工智能技术在计算机信息安全管理工作中也越来越显示出积极的意义[6]。人工智能在计算机信息安全管理阶段的应用越来越广泛。由于人工智能技术的快速进步，有效地推动了计算机信息安全管理技术的不断发展[7]。人工智能技术在计算机信息安全管理中的作用是前所未有的具有广泛的应用范围。计算机安全事件日益增多，黑客攻击时有发生。必须建立一种新的安全模式，以确保网络安全，并无限期地减少事故的发生。计算机网络安全分析的建模研究变得越来越重要。只有提高计算机网络的安全性，人们的隐私才不会被泄露[8]。本文分析了计算机信息安全管理资源及其可能对安全产生负面影响的原因，建立了计算机信息安全分析模型，为计算机信息安全管理的发展和研究提供了一定的支持。

2 计算机网络安全分析

2.1 计算机信息安全管理绩效

在计算机发展初期，由于网络数据的连续性和规律性较差，增加了计算机分析数据真实性的难度。这也使得计算机信息安全管理的智能化变得极其重要。人工智能技术的提出，不仅极大地促进了文字、图片、视频的处理，而且使计算机网络更接近人类大脑的思维方式，为解放劳动做出了重大贡献。越来越多的领域都离不开计算机的使用。毫无疑问，电脑确实给我们带来了很多方便和便利，还有很多好处。然而，在其优点之外，也存在一些不可忽视的弊端[9]。随着越来越多的网络犯罪的出现，为了在有效遏制网络犯罪的同时更有效地保证用户信息的安全，敏锐的洞察力和快速的反应能力是计算机所必需的功能。基于人工智能技术建立智能管理系统。

主要具有信息自动采集和网络故障诊断功能，极大地保证了用户的信息安全。

计算机信息系统安全水平的提高，不仅保证存储的数据不被窃取，还包括对个人隐私和公司秘密的保护。人工智能高效处理数据的能力大大提高了人类在使用计算机时的工作效率，促进了整体计划更高效地完成。对于整个计算机网络的整体发展是不可低估的。的驱动效应[10]。任何技术进步都离不开装备保障，两者相互支撑。对转鼓设备进行技术检查，满足工作要求，保存工作信息，确保信息安全管理。计算机技术水平的提高促进了人工智能技术的普及和进步，而人工智能技术的提高对计算机的提高也至关重要

信息安全管理。人工智能技术在计算机信息分析中具有非常积极的意义，其重要性是不可替代的。互联网上的数据资源是巨大的，但不是连续的。它们不规则且难以捉摸。因此，必须在计算机网络技术中引入人工智能，加强监管，从网络数据资源中快速准确地找到目标信息，从而保证信息安全。

2.2 对计算机信息安全管理产生负面影响的原因

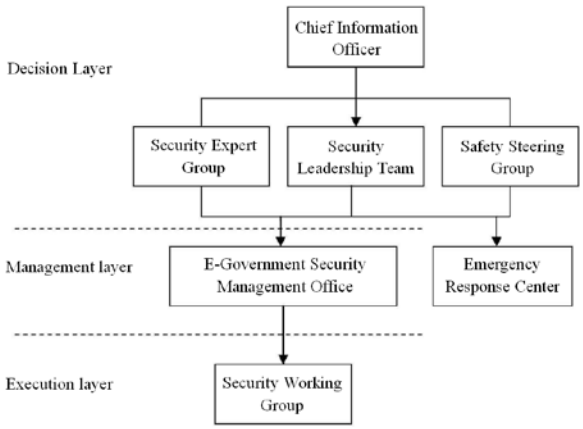
*2.2.1 计算机网络软件和网络漏洞由于*计算机网络存在漏洞或计算机网络中安装的软件存在漏洞，病毒能够攻击计算机网络，黑客能够侵入他人的计算机网络[11]。从目前网络的暂态和动态性能来看，网络管理和系统评估工作在这方面有很大的压力，智能技术的融合确实有效地缓解了这一问题。数据信息是计算机网络保护的对象，因此整个计算机网络系统是信息技术的载体。软件和网络漏洞是指硬件、软件或协议实现和安全设计上的缺陷。在这种情况下，一些非法用户可以未经授权登录系统并进行恶意破坏。当相关公司开发的新计算机网络系统投放市场时，应由专业人员进行系统检查，防止系统在安装过程中出现缺陷。

2.2.2 黑客和病毒的恶意攻击

黑客利用高超的计算机网络技术，不断地攻击别人的网络，从别人的计算机中获取大量的信息，从而获取大量的利润。有些黑客攻击别人的电脑不是为了牟取暴利，而只是为了炫耀。一些病毒软件会检测到计算机网络的弱点，并对这个弱点进行猛烈的攻击。当系统被入侵时，用户无法正常使用信息，无法对系统进行操作。他们只能让病毒侵入他们的私人信息。恶意程序、病毒、木马等工具也是黑客常用的恶意篡改和窃取用户数据的工具，病毒或木马还会影响计算机网络的连通性，影响用户计算机的正常使用。利用人工智能可以提高防火墙和监控系统的智能化程度，实现内部网络和外部网络的有效隔离，更有效地识别病毒，从而有效抵御网络入侵，使用户尽可能免受病毒的攻击。

3 基于人工智能技术的计算机信息安全管理建模

构建智能防火墙后，可以通过概率运算、数理统计、内存识别和智能决策来识别信息数据。电脑



网络安全一直是企业和国家追求的目标。培养专业人员学习信息技术，加强对网络安全的分析研究，采用数学方法，根据实际情况选择合适的数学模型。影响计算机网络安全的最重要因素是黑客和病毒的恶意攻击，人们不能保证自己永远不会受到黑客的攻击。因此，为了提高计算机网络的安全性，有必要设置计算机的访问权限，并且计算机中的重要信息必须只有管理员才能访问[12]。及时提高计算机网络的系统管理能力，对用户的上网感受起着极其重要的作用。

为了实施决策层的决策，还需要一个管理层来管理日常工作，需要一个执行维护层来负责执行安全计划和决策。这形成了一个由 CIO 直接领导的分层信息安全组织，如图 1 所示。

图 1 分层信息安全管理结构

计算机网络数据的共享特性允许不同行业、不同领域共享计算机网络信息。对于计算机犯罪，基于能量的概率模型通过能量函数定义概率分布:

$$\ln(\mathrm{Di})\ a\,\mathrm{bj}=^{n}$$
$$ln(pj)+\sum ri\ln(\mathrm{Y})\ u++$$

对各种信息数据进行分析、分类和管理。智能防火墙的意义体现在防止黑客入侵，有效减少恶意病毒攻击，显著提高局域网的监控和管理，从而充分避免恶意病毒和特洛伊木马的攻击。入侵检测是智能防火墙的主要组成部分，是防火墙提高计算机网络安全性的第二种保护手段。计算机网络中仍然存在许多潜在的危险。犯罪分子的恶意入侵可能导致计算机网络崩溃，重要数据丢失，给个人、企业和国家造成巨大损失[13]。将人工智能技术应用于计算机信息安全管理，可以使计算机系统更加人性化、智能化。与此同时，计算机将能够为人类带来更高质量的服务，更好地满足人们的需求。通过人工智能技术，可以对网络数据进行数据挖掘，更准确地检测内存溢出等问题，从而智能地保证网络的平稳运行。提高计算机安全管理技术，减少漏洞，定期维护计算机及相关设备，可以在一定程度上保证计算机系统的安全性能。

表 1 移动社交网络系统分析结果

网络	节点数量	的数量关系	网络密度	中央潜在的
满足信息	198	237	0.831	0.346
相互信息	181	243	0.657	0.355
加权求和	187	246	0.691	0.322

$j=-1$ (1)

作为多项式核函数:

$$dia=\mathrm{bj}+\ln(\mathrm{pj})\sum_{j=-1}^{n} ri\ \ln(\mathrm{Y})\ u++ \quad (2)$$

随着节点间社会关系的增加，节点间最短路径和整个网络的平均距离都在减小(见图 2)。

基于大数据分析的特点，人工智能技术将在这一过程中发挥重要作用

呈现爆炸性模式。人工智能技术与计算机信息安全管理的共同发展，将显著提高数据分析水平，有效应对计算机数据分析和安全管理问题的复杂性。目前，快速的自动信息检索技术和工具为计算机网络结构的安全管理提供了重要的支持，而评估的课题也致力于在单个主机上对整个信息结构进行综合评估。人工智能技术的改进和应用对于提高网络安全管理水平至关重要。在科学技术不断进步的背景下，人工智能在数据分析、学习效率、互联网保护能力等领域的优势日益被人们所认识。只有不断提高计算机网络的安全性能，才能保证用户的隐私，减少计算机用户的损失。

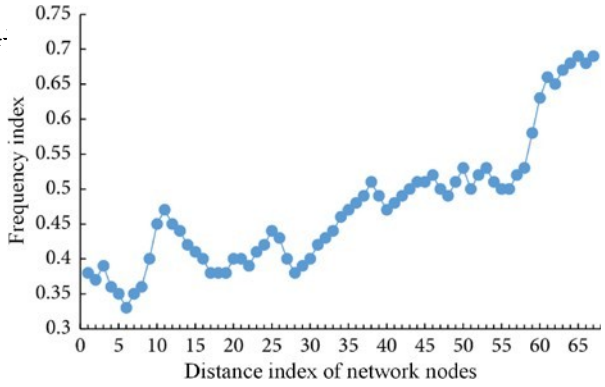


图 2 移动社交网络节点距离分析

4 结论

由于社会和各个层面的日益进步，网络技术和信息技术越来越普及，人们的生活质量和素质也在一定程度上得到了提高。大数据时代，数据处理

参考文献

[1] 王晨曦，王浩，王泉，等。医疗人工智能产品的网络安全探讨。《中国医疗器械》第 33 卷第 33 期。12, pp. 31-34+39, 2018。

[2] 安可英，卢红。人工智能时代网络安全的刑法保护——基于网络犯罪化的视角。杂志

云南民族大学学报(哲学社会科学版)，第 181 卷，第 181 期。6, pp. 145 -156, 2018。

[3] 李信。基于人工智能算法的无线移动通信系统风险评估。现代电子技术，第 43 卷，第 43 期。1, pp. 12-15, 2020。

[4] 王 Qianyun。人工智能背景下数据安全犯罪刑事规制的思考。《法律论坛》，第 34 卷，第 34 号。2，第 27-36 页，2019。

[5] 朱桂明，宾晨忠，顾天龙，等。基于知识图谱的用户偏好神经建模框架。模式识别与人工智能，vol. 32, no。7, pp. 661-668, 2019。

[6] 付鹏，林政，袁凤成，等。基于卷积神经网络和用户信息的微博话题跟踪模型。 模式识别与人工智能，第 30 卷，第 30 期。1，第 73-80 页，2017。

[7] 吴元利，司光亚，罗皮。人工智能技术在网络空间安全防御中的应用计算机应用研究，第 32 卷，第 2 期。8, pp. 2241-2244, 2015。

[8] 廖方圆，陈建峰，甘志旺。人工智能驱动下关键信息基础设施防御研究综述。计算机工程，第 45 卷，第 5 期。7，第 181-187,193 页，2019。

[9] 邱悦，李思琪。人工智能发展与应用中的安全威胁分析及解决策略研究。《信息网络安全》第 213 卷第 2 期。9，第 41-47 页，2018。

[10] 湾清。基于自适应神经网络人工智能的船舶 AIS 航路搜索技术研究。船舶科学技术，第 41 卷，第 41 期。2，第 43-45 页，2019。

[11] 林义伦，戴兴远，李莉，等。人工智能研究的新前沿:生成对抗网络。自动化学报，第 44 卷，第 2 期。5, pp. 775-792, 2018。

[12] 齐斌，邹红霞，王宇，等。自适应网络安全意识评估体系研究综述。四川军队学报，2018 年第 39 卷第 11 期，第 140-146 页。

[13] 高琪琪，刘洋。人工智能时代的城市治理。《上海行政学院学报》第 20 卷第 1 期。2，第 33-42 页，2019。