文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

人工智能时代计算机信息技术安全与防护策略

耿亚涛
郑州电力职业技术学院
DOI:10.12238/acair.v2i2.7389

[摘　要] 伴随我国科技的持续进步,电脑已经变得对我们的日常生活和教育有着重大影响。在这个人工智能的世界里,许多潜在的风险正在对电脑系统的使用造成威胁,因此确保电脑系统的正常运转,降低非法侵入、恶意破坏、数据篡改的风险,以及确保电脑信息的完备,以及电脑系统的稳固,已经变得是这个时期的主要职责。针对这个问题,需要进行一个简要的计算机网络安全的评估,深入理解其带来的各种影响,然后进行主动的调查与研究,以便制定有效的信息安全保障与管控策略,从而促进在人工智能时期的创新科技的普及。
[关键词] 人工智能；计算机；信息技术；安全；防护；策略
中图分类号：G623.58　**文献标识码**：A

Security and protection strategy of computer information technology in the era of artificial intelligence

Yatao Geng
Zhengzhou Electric Power Vocational and Technical College

[Abstract] With the continuous progress of science and technology in our country, computers have become a significant impact on our daily life and education. In this world of artificial intelligence, many potential risks are a threat to the use of computer system, ensure the normal operation of computer system, reduce the risk of intrusion, malicious damage, data tampering, and ensure that the computer information is complete, as well as the computer system, has become the main responsibility of this period. In view of this problem, we need to conduct a brief assessment of computer network security, in-depth understanding of its various impacts, and then active investigation and research, in order to develop effective information security and control strategies, so as to promote the popularization of innovative technology in the period of artificial intelligence.
[Key words] artificial intelligence; computer;information technology; safe; protect; tactics

引言

目前,人们对计算机IT的安全和防护策略的研究非常关注。因此,为了满足现代生活的需求,我们需要着重解决计算机IT应用的安全问题,以降低信息泄露等问题的发生几率,提高信息安全的水平。显然,通过从安全威胁的识别和安全态势的感知两个角度出发,可以为计算机IT的安全和防护提供支持。

1 计算机网络安全问题概述

网络安全的核心问题主要包括信息保护和网络保护两个领域。信息保护是指在网络传输过程中,信息数据可能遭到篡改、盗取、破坏或伪造等行为,从而使得信息的完整性和真实性遭到破坏,并被他人使用。网络安全主要涵盖了由于网络系统运作引发的威胁以及电脑自身的安全隐患,这些威胁包含了硬件设施、各种应用程序、数据库、网络服务等。

2 人工智能时代计算机网络信息不安全带来的危害

2.1个体的关键资料与个人隐私受到侵犯

尽管互联网的广泛应用为我们创造了许多方便,但它却引发了许多潜在的安全风险,并为许多恶意攻击者创造了一个更广阔的作战空间。如果个体资料被侵犯,受害的将是你本身,甚至是你的家庭成员、同事、朋友,各种垃圾邮件、推销电话都会频繁出现。对于那些被恶意利用的垃圾文档和电子邮件,混入了一些恶性软件,一旦获得了你的隐私,就会利用它们制作伪造的身份证、信用卡,随心所欲地进行消费,从而对你的资金和声望造成了威胁。有些更为猖獗的犯罪分子假冒公安部门的名义,利用你被盗取的个人信息进行欺诈,或者利用你的身份牵涉到一些恶劣的案件,对你未来的生活产生了一些影响。

2.2对国家政治安全以及社会经济安全构成威胁

随着全球互联网的发展,各个国家的关系日益紧密,一点点

的国际经济变化都可能威胁到他们的财政稳定。从一个角度来看,全球互联网极易受到黑客和病毒的侵袭,总有一些别有用心的人试图对本身存在缺陷的全球互联网进行攻击,对各国的政治和经济安全构成威胁。另一方面,一些拥有先进网络技术的国家有能力利用互联网的漏洞窃取其他国家的经济数据,破坏社会主义市场经济的规则,对一些发展中国家构成了严重的威胁。在一定程度上,国家对信息传播的传统控制权已经被削弱。鉴于全球互联网的普遍性和开放性,国家和政府正在面对来自非政府组织甚至个人的挑战和威胁。

3 人工智能时代计算机信息安全问题

3.1网络攻击和网络病毒多样性

随着计算机科技和网络科技的飞速进步,人工智能与信息安全之间的联系也在逐渐建立。一方面,我们利用智能科技实现了人机互动,从而使得各种活动的智能化程度持续增强;另一方面,为了适应“互联网+ ”所带来的新变革,我们正在深入研究数据加密、安全防护、访问控制等技术,以确保计算机信息的安全性。随着对人工智能技术的深度探索,我们已经看到了人工智能技术的运用和计算机信息安全管理的进步,但是依然面临着信息安全的威胁和网络安全的挑战。尤其是网络病毒和网络攻击,它们的出现频率和形式都非常多元。

在互联网环境中,黑客攻击已经变得频繁,通过对其入侵途径的分析,我们可以看出,黑客攻击的主要形态包括:首先,他们会利用恶意插件和木马病毒进行攻击,通过嵌入含病毒的广告或者插件,从而破坏电脑系统,并且为病毒的侵入提供了可能。其次,通过发布短信,网络恶意攻击者能够诱使用户在接收到富含诱惑性的消息后,把与其个人隐私相关的数据泄漏出去,从而使得用户陷入数据的威胁以及财务的破坏。最后,PUP种类的AP,利用广告和无效的软件,直接把病毒嵌入到电脑中。一旦用户进行二维码扫描、下载非法的AP、搜索网页等操作,病毒便可能进入到计算机系统,从而干扰到计算机的正常运行。这同样可能引发安全风险与危险。

3.2网络信息和数据的脆弱性

电脑的信息被保存在规模宏大的数据库里,其中涵盖了各种子系统,这导致了数据库的信息量巨大。通常,由于网络数据库具备一定的密封特性,因此不太可能面临信息外泄的危险。然而,当信息被公开或者传播时,非法人员可能会针对信息的重要环节发起攻击,寻找数据库的结构漏洞,这可能导致数据的混淆、完整性的减弱,从而引发数据和信息的外泄。另一方面,因为互联网信息本质上的敏感度,它们极其可能遭到攻击或窃取。当遇到这些安全威胁或问题时,电脑系统以及相应的管理工具,仅能够轻微地警告一些表面的危险,而无法立即发现潜伏的更大的安全威胁。一些网络恶意软件无法迅速定位其根源,这导致了互联网信息的滥用风险日益增加,并给个体的隐私权利、保护以及社会经济稳定带来了潜在的危害。

4 计算机网络安全风险控制措施

4.1优化计算机硬件设备

在处理电脑网络的安全问题上,优化电脑配置显得尤为关键。电脑配置构成了电脑系统的根本,必须适时地进行保养与更新,以增强电脑系统的承受压力,如果没有这样做,电脑的运作可能会变得不稳定、卡顿,甚至可能会出现故障。在电脑网络环境下,硬件设施对于信息数据的流通与保留有着重要的作用。如果这些设施发生故障,电脑网络系统就会无法顺利工作,同时,所保留的信息的完好度与精确度也会遭遇损害,可能会导致数据遗漏、信息处理不当等情况。如果电脑系统年代久远,它的操作性将相对降低,存在大量的缺陷,有些甚至无法承受一些软件的工作,这样一来,当遭遇病毒攻击的时候,它们将更加容易受到攻击,从而产生负面影响。

4.2对网络信息进行加密

随着AI的普及,电脑网络的信息数据流动和储备显著提升,因此,确保这些信息不会遭到干扰、偷窃或损害变得至关紧要。在这个过程中,我们需要使用加密技术来处理关键的文档信息,以此来降低其在网络交流时遭到解读或者偷窃的风险,从而避免信息泄漏的情况发生。当我们挑选加密方法的时候,我们需要深思熟虑诸如信息的关键性、加密的复杂性、加密的过程以及解码的困难性等各种因素。我们需要在保障信息数据的安全性的前提下,最大限度地降低电脑网络的压力,以便它们能够顺利地进行数据的交流与日常操作。为确保信息的安全性,在计算机网络系统的内部管理过程中,我们需要合理地设定用户权限和口令,并对计算机用户进行分级管理。同时,我们还需要利用信息技术、统计技术、密码学等科技手段,来实现信息的加密传输和储存。对于各级别的用户,应当赋予他们不同的权限,并且要重视SK交接流程的保密性,以防止SK丢失或泄露,从而保障电脑网络信息的安全。

4.3优化防火墙设置

恶意的外部攻击给电脑使用者的利益带来了巨大的风险,因此,建立防火墙就显得尤为关键,它可以阻止电脑系统受到非法的侵犯。通过在电脑的主干线路和局域线路之间建立防火墙,我们可以分隔主干线路,筛选出主干线路的信息,阻止任何形式的非法访问和不安全的服务,仅发布安全的数据,以此来保护个人隐私,并且可以增强主干线路的安全性,从而达到主干线路的安全互动。

4.4利用人工智能的优势优化安全管理工作

将人工智能技术的优越性和独特性结合在网络安全管理任务上,既能够提升工作效能,也能给予网络安全更强的防护。利用人工智能技术,深入研究网络攻击的属性与模式,揭示过去的网络攻击的普遍与独特之处,探讨恶意软件及其攻击策略的进步路径,以此提升网络攻击的抵抗能力与精确度。

将人工智能的尖端科学技术融入到网络安全的实践中。同时,我们也需要增强对于感知科学、深度学习、机器学习等人工智能方案的开发投入,以此来增强方案的理论阐述、信息公开以及操作效果。首先,我们需要增强在人工智能领域的漏洞探索、安全验证、风险预警、侵入侦查以及紧急响应等网络安全技术

的研发，以增进人工智能在安全状况的感知、测验评价、风险数据的公开以及紧急响应的能力。其次，我们需要推动应用技术的探索，特别是在对抗型的机器学习领域的深入研究，以便更好地理解这种对抗型的攻击如何影响到人工智能系统。

4.5引进各种先进的信息技术手段，严格把控计算机信息安全

在人工智能的背景下，为了确保信息安全管理工作的高效进行，我们必须加大对计算机信息安全的保护力度。这需要我们引入各种专业且先进的IT手段，并针对性地开发数据安全技术。在此基础上，我们必须对电脑信息安全实施彻底的监督与保护，严密地管理电脑信息安全，以保障电脑网络系统的安全性和稳定性，防止电脑信息安全事件的发生。第一，我国的政府部门应当充分发挥其职能，为电脑信息安全技术的研究提供必要的经济支持，从而为引入更多的尖端电脑技术和设备设施提供充足的经济支持。第二，我们需要主动运用数字加密技术来维护隧道技术，加强对数据传输过程的加密防护，以确保数据在传递过程中不会遭到损害或泄露。第三，通过数字签名与文件加密技术，我们可以确保电脑数据的安全，避免数据遭到窃取或篡改。这两种技术在某种程度上具有共通点，即它们均源自对电脑数据的非平衡设计，旨在增强电脑数据的安全性与隐私。当计算机用户进行重要资料的储备与控制时，必须在互联网上注册一个特殊的帐号与密码，这样才能避免其他人的不当访问。为了避免这些密码被他人轻松获取，我们应该尽量简化这些密码，一般会选择“数字+字母+符号”的形式，同时也需要定期修正已经设立的密码，这样才能保证资料的安全。第四，采用更为全面的计算机人工智能技术，以此有效地提升计算机网络信息安全性。在实际操作过程中，我们可以利用人工智能的自动识别功能，准确地发现电脑网络内的隐蔽安全缺陷，同时进行逆向跟踪，跟踪不合规的攻击者，观察他们的不当活动，然后把攻击者的相关资料自动上传至网络监控单位，让该单位进行处理，从而达成对电脑信息安全的有力保障。第五，借助人工智能技术构筑电脑信息的监督架构，以便于实现对数据的即时跟踪。通过该架构的自动化数据采集功能，可以向有关的管理者提供更加精确的电脑信息安全的检查报告，从而确保电脑信息的安全稳固。

5 结束语

简而言之，在人工智能的背景下，我国的计算机信息安全和防护领域已经实现了显著的进步，技术层面也进行了大幅度的提升和刷新。许多计算机专家也热衷于网络信息安全系统的研究和技术探讨，从而为计算机信息安全问题提供了强有力的保障。另外，有关的机构也需要肩负起确保电脑信息安全的责任，增强网络信息安全的建设投入，对那些非法获取网络信息的人员进行严格的惩罚，对电脑网络中可能存在的安全隐患和风险进行深入的分析和监控，减少电脑网络的使用风险。通过各方的协作，研究网络信息安全的目标，以便更有效地应对电脑信息的安全威胁，创造一个安全的电脑网络环境。

[参考文献]

[1]付鹏.大数据背景下计算机网络安全及防范措施分析[J].科技创新与应用,2022(1):123.

[2]王梁.计算机网络安全及防火墙技术分析[J].中国管理信息化,2021(12):11.

[3]朱亚兵.计算机网络安全问题及防范策略[J].产业与科技论坛,2021(10):14.

[4]周晓娟.人工智能视角下计算机信息安全防护探讨[J].电脑编程技巧与维护,2021(03):171-173.

[5]胡玲芳,徐晨瑶,赵秀丽.人工智能时代计算机信息安全与防护[J].信息通信,2020(06):192-193.

作者简介：

耿亚涛(1978--),男,汉族,河南郑州人,硕士研究生,工程师,郑州电力职业技术学院,研究方向：计算机信息管理,信息管理与信息系统。