人工智能时代计算机信息安全与防护研究

许应强
云南省工业和信息化厅　云南　昆明　650031

摘　要：随着互联网的迅速演进，人工智能技术在各个行业的运用愈来愈普遍，信息化管理时代早已来临。这些在不一样行业的运用不但可以促进提升各个行业的工作效率，也给电子计算机互联网信息安维护技术产生了考验。互联网中出现的对抗性攻击也屡见不鲜。电子计算机信息互联网的推广，为信息违法犯罪造就了新的方式和手段。互联网信息偷盗和个人互联网信息偷盗倒卖比较严重影响了社会安全性。个人隐私数据安全性已变成人工智能技术总体发展的关键瓶颈，也是互联网时代亟待提升的重要考验。

关键词：人工智能；网络安全；防护

引言：随着我国经济及其高新科技的快速发展，以人工智能技术技术性、云技术性、大数据技术性等为意味着的优秀技术性开始在各领域行业中发挥着愈来愈关键的效果，随着着互联网安全隐患的频发，各领域也提高了对互联网安全防护工作中的关心水平，因此，在人工智能技术时代的大环境下，怎样合理确保电子计算机信息安全性，便变成了电子计算机安全性工作中工作中中务必要要点关心的一个热点，针对这些难题的合理处理也会给人工智能技术技术性在各领域行业中更为完善的应用奠定优良的基本，为我国电子计算机互联网的安全性健康发展，作出应该有成果[1]。

1 人工智能时代下计算机信息安全相关概述

说白了电子计算机信息安全性，关键是指受影响的客户在应用电子计算机系统软件时，其数据和信息有一定的安全性确保，软硬件机器设备不容易遭受外部系统软件和软件的毁坏，信息可以安全性地传送。安全性传播。在人工智能技术时代，电子计算机信息的安全性与确保不但是全部互连网领域亟待解决的难题，更是搭建现代社会和睦发展的根本性难题，理应造成充足的高度重视。电子计算机互联网的应用具备多样性和便捷性的特征，其关键作用不仅是简易的信息互换，也有数据的传送和储存等作用。对于现代社会的发展，电子计算机信息技术性不但合理地提升了数据处理方法的效率，并且为大家的日常生活和工作中造就了一定的便捷标准，这反映了信息技术性的效率。除此之外，互联网是开放的，尽管信息测算持续升级，但也出现一些无法操纵的缺点，比如，一些非法分子结构运用互联网技术性，将毁坏电子计算机互联网系统软件的编码插进到电子计算机程序，给电子计算机客户导致巨大伤害 潜在性的安全风险，运用病毒感染植物窃取客户信息，进而给客户导致经济或盈利损害，毁坏互联网自然环境的平稳发展[2]。因而，它在电子计算机互联网信息安全性和维护技术性中起着十分关键的效果。

2 当前计算机网络安全防护中存在的主要风险

在大数据时代，各种数据之间出现着一定的关联性。在科技发展的环境下，数据信息安全性早已变成一个关键的难题。随着互联网时代的持续拓展，信息的开放度愈来愈高。在方便快捷的信息中，也有木马病毒的伤害。因而，您也更非常容易遭受病毒感染产生的风险的影响。目前，大数据是信息技术性发展和运用的发展前景，相匹配的课题也愈来愈多。科学研究工作人员必须融合信息技术性的自主创新与发展，达到大数据时代信息技术性的具体要求，进而真正提升数据的合理性和安全性性。虽然当前互联网信息安全性出现一些难题，但客户的生活遭受了影响。可是，经过长期性持续的勤奋，电子计算机互联网的信息安全性维护作用将持续健全，进而打造出更为高效、方便快捷、安全性的电子计算机互联网系统软件[3]。

2.1 传统病毒造成的数据风险

传统的电子计算机病毒感染具体上是一个可实行程序或命令编码。该命令编码埋伏在客户电子计算机系统软件的数据资源中，可以持续拷贝和生存，毁坏电子计算机系统软件或数据，影响电子计算机的正常的运作。由于其特点和所历经的全过程，它们与微生物病毒感染十分类似，可以拷贝并被感染，因而而出名“病毒感染”。传统病毒感染通常有三种普遍的传播方法：(1)通过电子邮件或通信软件推送被感染网址的连接或配件开展传播；(2) 运用具体操作系统软件系统漏洞或互联网服务系统漏洞开展传送；(3)通过电脑硬盘、U盘等挪动储存物质传播，普遍的总体病毒感染有：CIH病毒感染、文

档病毒感染。近些年，Nion和WNCRY两种勒索病毒感染变种在全国各地甚至全世界暴发，大量个人、公司和组织客户的计算机感柒病毒感染。目前被攻击的受害人大多数是通过远程桌面弱动态口令、系统软件系统漏洞和应用软件系统漏洞开展攻击。

2.2 个人隐私以及信息被泄露的风险

随着人工智能技术时代互连网的推广，在给大家产生很多便捷的与此同时，也产生了很多安全性方面的安全隐患，与此同时也为很多非法分子结构给予了可乘之机，网络黑客应用。一旦个人信息泄露，不但你会遭受危害，你的亲人、朋友、亲友等也会接到大量的废弃物邮件和源源不绝的销售电話。废弃物邮件通常会夹杂一些病毒感染来窃取你的个人信息。信息，进而申请办理假银行信用卡和身份证交易，将对个人名誉和资产安全性导致比较严重危害。也有一些非法分子结构极为猖狂，会以检察机关的为名运用窃取的信息骗领资产，或是危害群众，声称自己的个人身份涉及到一些极为比较严重的案子，会导致欠佳影响。以做到吓唬吓唬的目地，进而执行行骗。

2.3 计算机网络自身漏洞造成的风险

从理论上讲，电子计算机互联网本身便是由各种种类的数据构成的，这些复杂的电子计算机信息组成在一起构成了各种种类的数据信息数据库，当电子计算机互联网出现安全风险时，数据库便会被故意攻击毁坏。几率会大大的提升，也有数据库系统漏洞或电子计算机互联网信息不正确的状况。除此之外，一些非法分子结构会在电子计算机数据传送全过程中为不法目地窃取或伪造信息，导致电子计算机信息泄露。

2.4 木马造成的数据风险

木马，以自身特性取名，归属于病毒感染，但它与传统病毒感染不一样，它不容易无休止地拷贝传播，也不容易感柒其他文档，它通常仅仅掩藏自己的身份，诱骗客户免费下载运作后，掩藏成一般程序（通常是系统软件程序，不容易被客户发觉）埋伏在客户电子计算机系统软件中，伺机窃取客户信息，毁坏系统软件，乃至查验客户的主机。木马程序通常通过以下四种方法传播：(1)通过电子邮件或通信软件推送，诱骗客户点一下或免费下载；(2)与一般软件关系，客户免费下载应用一般软件时，免费下载木马；(3)通过网址传播，选用网页页面挂马的方法，当客户应用时全自动免费下载到客户计算机上浏览网址；(4)通过电脑硬盘、U盘等挪动储存物质传播普遍的木马关键是“冰河”木马，称得上国内木马的“领头羊”。冰河木马发生于1999年，有别于以往的总体病毒感染一旦发生就会残暴的毁坏电子计算机系统软件，近乎疯狂删掉客户文档，完全毁掉电子计算机，冰河更趋向系统化，在设计方案整体构架、作用设定、具体操作在其他层面有比较大的磁感应性[4]。

3 人工智能背景下计算机信息安全的有效防护措施

在人工智能化环境下，计算机技术总体发展早已较为完善，信息安全性工作人员务必高度重视互联网信息维护，并选用多种合理的方式来实现电子计算机信息维护。在维护工作中中，提升数据安全性技术性，提升信息安全性管理体系基本建设，做好安全性技术性的研发和提升工作中，使人工智能技术技术性环境下的目前互联网自然环境变成很有可能。提升达到互联网信息安全性难题的要求。因而，提议在电子计算机信息安全性维护保养工作中中，采用以下对策，全方位维护电子计算机信息安全性。

3.1 建立计算机信息安全意识

为确保电子计算机信息安全性，首先要塑造自身的电子计算机信息安全性认识，并在认识的幌子下，有针对性、全方位地逐渐健全互联网信息安全性基本建设。仅有在保证的前提条件下电子计算机信息安全性信息化管理认识基本建设 为实现信息维护的基本上技术性发展，而不是只是借助互联网技术工作人员。第二，维护互联网信息安全性关系到我们的日常生活和工作中。要贯彻落实信息安全性发展战略，提升信息管理工作人员的安全性认识和心态，积极主动认识信息安全性对机构的必要性，通过制订行之有效的管理计划和规章制度保证网络安全。最后，为构成互联网信息发展的健康情况，必须创建健全的信息传送机构模型，搭建安全性的互联网构架，以互联网构架为关键，融合互联网发展现况安全性性开展持续的详尽剖析和剖析。把握住和操纵短板，积极主动改善和提升，自始至终围绕网络安全管理体系的合理性进行工作中，防止过度复杂的项目，真正把信息安全技术贯彻落实到互联网信息安全性管理方式的具体运作中。

3.2 运用杀毒软件的技术

目前互联网病毒感染涉及到面很广，假如不开展科学有效的预防，将会造成很多安全风险，在这种状况下，可以在信息安全性管理中有效运用杀毒软件技术性，以做到更强的管理效果。杀毒软件本身具备效果好、应用便捷的特征，客户只需免费下载该软件就可以根据全部文档开展全自动检验，有效排查电子计算机中是不是出现病毒感染，随后采用防护对策，避免病毒感染入侵击中您的电子计算机并导致不必需的毁坏。因

而，承担网络管理的工作人员务必运用杀毒软件技术性，提升网络管理的安全性水准。杀毒软件安装区坐落于机器设备终端，一旦病毒感染入侵电子计算机内部互联网并挨近终端，将对病毒感染开展科学操纵、查杀和阻断，有效确保信息安全性。大部分计算机具体操作工作人员因为安全性认识不强，在日常工作中中很有可能会随便开启一些不著名的连接，免费下载一些不著名的软件，杀毒软件可以针对这些软件和连接中掩藏的一些病毒感染、木马开展消除。

3.3 构建防火墙防护

防火墙是外部互联网和电子计算机本地互联网之间的维护机器设备。它是您的电子计算机与外部互联网联接的合理天然屏障。在电子计算机系统软件的基本电子计算机系统软件中，防火墙的关键效果是维护电子计算机的信息安全性，制订了算法，合理避免外部的非权利信息进到电子计算机。个人电子计算机中的防火墙由电子计算机系统软件中的应用软件和电子计算机处理芯片来发挥效果，电子计算机系统软件遭受电子计算机中处理芯片程序的维护。通常在私网与公网之间或电子计算机的内部网与外网之间设定防火墙，可以合理避免外部信息或工作人员浏览内部网。在启用防火墙的全过程中，电子计算机的速率特性会略微降低。缘故是防火墙已经查验全部传送的数据，这会减慢电子计算机的运作速率。

3.4 重视管理与维护计算机网络环境

电子计算机互联网自然环境关键是指客户应用电子计算机访问互联网时所处的安全性自然环境。为合理确保电子计算机互联网的信息安全性，首先要高度重视电子计算机互联网自然环境的安全性管理。通过对所在互联网的安全性性开展科学剖析，合理避免外部病毒感染的攻击。与此同时，客户必须按时及时查验计算机安全性防护系统软件和计算机杀毒软件。对于一般客户来说，一般的安全性软件就足够达到杀毒防护的必须，假如觉得自己的计算机感染了病毒感染，可以应用很多杀毒软件开展修补，例如360杀毒、金山毒霸、瑞星杀毒等.假如要应用手动式杀毒，必须了解病毒感染的藏身之处，还必须了解病毒感染，由于很有可能涉及到到改动申请注册表等。因而，假如要手动式删掉，必须清晰自己的计算机感柒的是哪种病毒感染，具有一定的电子计算机专业知识，了解病毒感染，才能手动式删掉。

3.5 完善信息安全教育工作

除了以上多样化的安全防护外，相关部门还应积极主动进行信息安全性教育教学，健全信息安全性教育，有针对性、有计划地将信息安全性教育系统软件地列入教育，使有关专业的学者认识到互联网详细性的必要性。并从提升客户网络安全认识和网络安全技术能力两个层面，全方位提高电子计算机互联网客户的安全防范能力。一是以互联网为媒介，全力宣传策划网络安全的必要性。与此同时，在互联网上创建网络安全管理技术性教程，推广安全性管理技术性专业知识。改掉随便访问互联网资源、不留意维护保养安全性等欠佳习惯，提升全网安全性管理水准。

结束语：综上所述，随着互联网信息技术的持续发展，大家对当前电子计算机信息安全性的关心度也愈来愈高，大家慢慢将当前信息技术性科学研究的重心从技术性信息技术性的发展迁移到了电子计算机信息技术性上。科学研究、多元化的信息安全技术持续获得开发设计和运用，也最大水平地推动了电子计算机信息安全技术在日常生活和生产中的推广和合理运用。因而，规定有能力的技术性工作人员在后面工作中中做好信息技术性的信息安全性维护工作中，将信息技术性与人工智能技术技术性相融合，随着当前信息技术性的发展，进而推动信息技术性的发展可持续性。

参考文献

[1]刘仪.人工智能时代计算机信息安全与防护研究[J].网络安全技术与应用，2022(4)：173-174.

[2]佘春燕.大数据背景下计算机网络信息安全防护手段研究[J].软件，2022，43(3)：65-67.

[3]邵奎翔.大数据背景下计算机网络信息安全风险及防护措施[J].信息与电脑(理论版)，2021(12)：220-221.

[4]王魏，赵奕芳.大数据时代计算机网络信息安全及防护策略[J].中阿科技论坛(中英文)，2022(1)：72-75.