

探讨计算机网络安全维护中的加密技术与人工智能应用

温 庆

国能包神铁路集团神朔铁路公司 陕西 榆林 719316

摘 要: 在计算机网络安全中, 数据加密技术与人工智能技术的应用, 可以实现数据信息的安全保护。数据加密技术具有高效率、低成本、多功能等优势, 在应用过程中可以确保信息数据的完整性和机密性。人工智能技术能够完成对信息的智能处理, 可以通过网络数据处理系统和计算机网络进行连接, 实现数据信息的传输, 保证信息系统和网络安全。因此, 在实际工作中, 要加强对计算机网络安全管理工作的重视程度, 采取科学的措施进行安全维护。同时, 在实际工作中也要注重加强对计算机网络安全加密技术与人工智能技术的应用, 从而保证计算机网络运行的安全性与稳定性。

关键词: 计算机网络安全; 网络安全维护; 加密技术; 人工智能

引言

计算机网络技术的发展, 对社会经济、文化等各方面产生了重要的影响。与此同时, 也出现了一系列网络安全问题, 给用户的财产和信息安全造成了一定的影响。在当前社会发展中, 人们越来越注重对数据信息的保护, 将数据加密技术应用在计算机网络安全中, 能够有效提升数据信息的安全性。同时, 在实际工作中也要注重对人工智能技术的应用, 从而保障计算机网络运行的安全性与稳定性^[1]。当前, 计算机网络在人们生活、工作中得到了广泛的应用, 为人们的生活、工作带来了便利, 但计算机网络也存在着一定的安全隐患, 需要加强对网络安全的重视程度, 采取科学的措施进行网络安全管理, 从而保障计算机网络运行的安全性与稳定性。本文对计算机网络安全管理中数据加密技术与人工智能技术应用进行了探讨, 分析了当前计算机网络存在的安全问题, 提出了数据加密技术与人工智能技术在计算机网络安全管理中的应用, 目的是促进我国计算机网络的安定运行, 同时为相关工作人员提供一定的参考和借鉴, 提高数据信息保护水平。

1 计算机网络安全维护概述

1.1 计算机网络安全概念

计算机网络安全是指计算机网络系统在受到外部因素或者内部因素影响时, 不会出现信息泄露、破坏或丢失的情况, 保障其系统和信息的完整性和保密性。计算机网络安全是计算机网络系统正常运行的基本保障, 能够保证计算机系统、数据以及信息的安全性, 不会受到黑客攻击或其他意外情况。目前, 计算机网络安全已经成为国家重点关注的领域之一。国家政府机构、企业、单位等都会借助计算机网络, 实现对数据信息的管理和传递。通过

对数据进行加密处理, 保证数据信息在传输过程中不会受到黑客攻击或其他意外情况影响, 确保其安全性。

1.2 网络安全威胁与挑战

网络安全威胁与挑战主要表现在以下几个方面: 第一, 黑客攻击。黑客利用网络进行攻击, 导致数据信息的泄露、丢失和篡改, 给用户带来较大的经济损失和精神损失; 第二, 病毒攻击。病毒入侵会影响计算机网络安全, 导致数据信息无法正常传输; 第三, 不良信息。不良信息会影响计算机网络安全, 使用户对其产生信任危机, 导致其财产、信息被泄露; 第四, 非法入侵。非法入侵会对计算机网络造成较大的破坏和影响, 导致用户的财产、信息被泄露或窃取; 第五, 系统漏洞。计算机网络系统中存在着一些漏洞, 如果这些漏洞没有得到及时处理, 就会使计算机网络安全受到威胁。

1.3 网络安全维护的重要性

网络安全维护能够对用户的财产、信息进行保护, 使用户的信息和数据在传输过程中不会被泄露、破坏或窃取, 保护其财产和信息。同时, 网络安全维护还能够提高用户对计算机网络的信任度, 使用户更加相信计算机网络的安全性和稳定性, 使用户更加信任计算机网络。因此, 网络安全维护具有重要的意义。随着计算机网络技术的发展, 计算机网络应用范围越来越广, 使其成为人们生活中必不可少的一部分。随着信息化时代的到来, 数据信息也越来越多, 如何保证数据信息的安全性就显得尤为重要。

2 加密技术在网络安全中的应用

2.1 加密技术概述

加密技术在计算机网络安全中应用, 是指通过密码算法、加密算法等将信息进行加密, 对信息进行一定程

度的处理,从而保证数据信息的安全。信息安全包括两个方面:一是保密性,二是完整性。保密性就是保障信息不被泄露;完整性是确保数据在传输过程中不被篡改。这两个方面的安全是相辅相成、互相影响的,一条链上任何一个环节出现问题都会影响另一条链的正常运行。加密技术通过对数据信息进行加密处理,确保信息数据的完整性和保密性,以此来保障计算机网络的安全运行。在计算机网络中应用加密技术,可以对用户信息进行有效保护,避免因信息泄露而遭受损失。

2.2 对称加密和非对称加密

对称加密是指使用同一把密钥对信息进行加密,同时使用两个密钥来完成数据的加密,实现数据信息的单向传输。对称加密具有简单、高效等特点,但是不能实现对数据信息的加密保护,容易被攻击者破解。非对称加密是指使用不同的密钥对数据信息进行加密,确保数据信息的安全。非对称加密不需要对数据信息进行对称计算,在实现数据信息加密时需要两个密钥,一个用于接收方使用,一个用于发送方使用。非对称加密方式可以在同一时间完成对数据的传输,确保数据的安全性。

2.3 数字签名和数字证书

数字签名和数字证书是网络通信中最重要的两项技术,数字签名主要用于验证信息的真实性,数字证书是用来证明信息发送方和接收方的真实身份,通过数字签名和数字证书能够有效确保数据信息的安全性。在计算机网络通信中应用加密技术,主要是对数据信息进行加密处理,确保数据信息在传输过程中不被窃取,提高了数据信息的安全性。通过对数据进行加密处理,可以保障数据信息的安全性,防止因数据泄露而遭受损失。在实际工作中,将加密技术应用在计算机网络安全中,可以确保网络通信安全,有效防止网络通信被窃取,从而保障用户的信息安全。

2.4 加密技术在网络通信中的应用

在计算机网络通信中应用加密技术,主要是为了确保信息传输的安全性。在网络通信中应用加密技术,可以有效地解决网络通信中的信息泄露问题。信息在传输过程中一旦被窃取,会给用户带来严重的经济损失。在实际工作中,网络通信过程中使用了大量的数据信息,将加密技术应用在计算机网络安全中,可以对数据信息进行有效的保护,从而确保数据信息的安全性。在计算机网络通信中应用加密技术,可以有效地防止用户受到窃取和篡改数据的侵害,从而确保数据信息安全。

3 人工智能在网络安全中的应用

3.1 人工智能概念及分类

人工智能是一种模仿人类的能力,能够对数据进行自动分析和判断,通过数据模拟的方式去完成人类没有能力去完成任务,从而提升工作效率。人工智能的分类:按功能分可以分为感知型人工智能和行动型人工智能;按智能来源分可以分为弱人工智能和强人工智能。弱人工智能是指一种不能执行任务,不具有智能的机器,只能执行一些简单任务;而强人工智能则是指具有智能的机器,它能够像人一样去思考,能完成各种复杂任务。按照是否具有人类思维能力可以分为强人工智能和弱人工智能;按照其是否能够理解语言可以分为通用型人工智能和具体型智能。

3.2 人工智能在网络安全中的作用

在计算机网络安全中,人工智能具有以下几个方面作用:第一,能够帮助进行安全风险分析,人工智能可以通过分析网络系统的漏洞等相关数据来预测网络的安全性,对于一些潜在的危险可以及时预警。

第二,能够实现对网络中的数据进行分析,利用人工智能技术可以自动学习相关数据和信息,从而实现对网络系统的自动检测和控制。

第三,可以实现对数据的分析处理,人工智能技术能够通过分析用户访问行为、活动等相关信息来判断用户行为是否正常,如果有异常行为则进行预警。

第四,在网络安全中应用人工智能技术,可以提高计算机网络安全管理水平。

3.3 人工智能技术在网络攻击检测中的应用

当前,人工智能技术已经应用到很多领域中,主要包括有:第一,在网络安全管理中应用人工智能技术,可以将攻击行为识别出来,从而保护计算机网络系统的安全。第二,在计算机网络安全中应用人工智能技术可以实现自动攻击检测,对于未知的攻击行为可以进行自动识别,并生成攻击响应措施。第三,在计算机网络安全中应用人工智能技术能够实现网络入侵检测系统的自动化运行,并将相关信息存储起来。第四,在计算机网络安全中应用人工智能技术可以实现网络入侵监测系统的升级,使其能够更加智能地进行网络入侵监测和防御工作。

4 加密技术与人工智能的结合应用

4.1 加密技术与人工智能的融合

在计算机网络安全管理中,加密技术与人工智能的融合,可以帮助计算机网络安全管理人员进行更好的安全管理,利用人工智能技术,可以对数据信息进行全面分析,从而可以实现对数据信息的安全分析与处理。在对数据信息进行分析过程中,可以利用人工智能技术

进行分析和处理,在此过程中,人工智能技术会利用一些算法对数据信息进行处理和分析,从而可以让计算机网络安全管理人员根据其分析结果来制定更好的安全管理方案。在对数据信息进行分析和处理的过程中,还需要结合计算机网络安全管理人员的实际情况来进行智能化决策方案的制定。

4.2 加密技术与人工智能联合应用案例分析

在计算机网络安全管理中,加密技术与人工智能联合应用,可以帮助计算机网络安全管理人员实现对网络安全的全面分析和处理,从而可以提高计算机网络安全管理的水平。例如,在某企业网络安全管理中,该企业需要对其内部数据信息进行管理,但企业内部的数据信息很多,如果只是依靠人工来完成,需要花费较多的时间和精力。

5 未来发展方向与挑战

5.1 加密技术与人工智能在网络安全中的前景

随着计算机网络安全的发展,网络安全技术也在不断地发展与创新,传统的网络安全技术已经不能满足网络时代的需求。现阶段,在计算机网络安全维护中使用的加密技术与人工智能技术在未来有着很大的发展空间。首先,人工智能技术与加密技术相结合,可以有效提高计算机网络安全管理水平,在管理工作中提高安全性与准确性。其次,数据加密技术与人工智能技术结合应用,可以有效提高计算机网络安全管理工作效率,为用户提供更加优质的服务。最后,随着计算机网络安全的不不断发展与完善,对计算机网络安全管理的要求也在不断提高,需要加强对加密技术与人工智能技术的研究,从而提高计算机网络安全管理水平^[2]。随着我国经济的不断发展,人们对计算机网络安全管理工作的要求也越来越高,需要在实际工作中不断研究和探索计算机网络安全管理问题。因此,在未来发展中要注重加强对数据加密技术与人工智能技术的研究与应用,提高计算机网络安全管理水平。

5.2 挑战与解决方案

由于计算机网络技术的不断发展与创新,使计算机网络安全管理面临着新的挑战,其中最大的挑战就是网络信息泄露问题。在网络时代,信息泄露已经成为一个严重的问题,给人们的财产、信息等造成了极大的损失。因此,在未来发展中,要不断加强对计算机网络安全

管理工作的重视程度,积极采取科学的措施进行安全管理。同时,在实际工作中也要注重对计算机网络安全技术的研究与应用,提高计算机网络安全管理水平。因此,在未来发展中要不断加强对数据加密技术与人工智能技术的研究与应用,从而保障计算机网络运行的安全性与稳定性^[3]。同时,还需要加强对网络安全管理人员的培训,不断提升网络安全管理人员的专业素质与能力,提高他们的综合素质,从而有效预防和化解网络信息泄露问题。

5.3 相关建议

在未来发展中,要不断加强对计算机网络安全管理工作的重视程度,积极采取科学的措施进行计算机网络安全维护^[4],同时也要注意加强对数据加密技术与人工智能技术的应用研究,提高计算机网络安全管理水平。同时也要注意加强对网络信息的保护,防止信息泄露等问题的发生。在实际工作中,还要加强对计算机网络安全管理工作的投入力度,不断完善计算机网络安全管理系统,提高计算机网络安全管理水平。

6 结语

随着互联网技术的快速发展,计算机网络也得到了广泛的应用,给人们的生活、工作带来了便利,但同时也存在一定的安全隐患,给用户的财产和信息安全造成了一定的影响。因此,在实际工作中,要注重加强对计算机网络安全管理工作的重视程度,采取科学的措施进行计算机网络安全维护,从而保障计算机网络运行的安全性与稳定性。同时也要注意加强对数据加密技术与人工智能技术的应用,从而提升数据信息保护水平。在今后的工作中,还需要加强对数据加密技术与人工智能技术的应用研究,促进我国计算机网络安全管理工作的有序开展。

参考文献

- [1]胡文杰,王涛.论计算机网络安全中的加密技术与人工智能.电子科技大学学报,2014,27(02):438-441.
- [2]张鹏,杨光全.基于大数据的计算机网络安全防护技术研究.计算机工程与科学,2010,18(2):336-337.
- [3]崔玉振.浅谈网络安全防范技术及创新[J].科技创新导报,2012(3):62-68.
- [4]曹凤岐.如何做好计算机网络安全管理工作?[J].信息安全与管理,2015(8):35-39.