Exploration of Engineering Technology, 工程技术探索(30)2023, 5
ISSN:2737-4114(Print) 2705-1242 (Online)

大数据在通信网络安全领域的运用

李新刚
中移铁通有限公司陕西分公司 陕西 西安 710068

【摘 要】随着云计算以及大数据技术的进步，信息科技与互联网平台共同促使我们进入 5G 时代。同样，信息化时代的到来也彻底改变了我们的工作和生活，加快了人们的生活节奏。通过互联网平台和数据科技的助力，物联网思想以及智慧城市的构想逐步成形，为我们的日常生活带来了更便利和更高效的工作方式。大数据技术作为信息科技深度应用的展现，每天创造海量数据，通过对这些数据的收集与深度分析，我们得以找寻出相互关联的信息，进而为公司或为用户带来更为精确的数据参考。目前，大数据已在我国的各个行业得到广泛应用。大数据技术为我们的生活带来更准确的数据指导和更便捷的工作模式，也带来无法忽视的网络安全问题。因此，本文对通信网络安全中存在的问题进行分析，同时提出相应的建议。

【关键词】大数据时代；网络安全；技术应用

1 网络安全概述

网络安全涉及的范围很广，包括保护组织机构的网络和关键基础设施免受未经授权的使用、网络攻击、数据丢失和其他安全威胁。近年来，网络安全形势并不乐观，网络安全威胁事件频发，累计损失持续上升。网络安全形势的日益严峻，使国家对网络安全产业的重视程度日益提高。传统的软件工具无法在指定时间内处理庞大的数据集，只有引进新的数据处理方式，才能体现出出色的洞察力、坚强的决策力、快速的增长速度、众多流程的优化能力和多元的信息资源。随着科技进步，大数据技术得到了广泛应用，现已渗透到我国各行各业，为企业的发展提供了更多的信息获取渠道，同时提高了人们的工作效率。提升数据处理能力，增强数据的应用价值，是大数据对当今社会的明显贡献 [。大数据以其低密度、巨大价值、多样模式的特质改变着人们的生活，同时具有快速生成和数量庞大等特点，在大数据时代，正确理解大数据的内涵和特点。将帮助人们适应大数据时代的发展潮流，充分发挥大数据的积极影响。

2 大数据环境中通信网络安全存在的问题

在大数据环境中，通信网络安全面临着网络病毒的威胁。网络病毒具有自我复制、传染性以及毁灭性等特点，会导致计算机系统被破坏。例如，木马病毒是用户在上网过程中最难防备的病毒之一，经常出现在网络开放终端中，影响计算机数据的安全性。大数据环境下的安全管理难度较大。如果安全管理制度不健全或执行不严格，可能会导致安全漏洞的产生，给黑客提供可乘之机。大数据环境下需要进行身份认证和授权访问控制，但这些机制可能存在漏洞，导致未经授权的用户获取敏感信息或进行恶意操作，从而造成安全问题。

3 大数据在通信网络安全领域的运用措施

大数据环境下通信网络安全是指通过采用各种技术和管理措施，保障数据的机密性、完整性、可用性和可控性。它涉及计算机硬件、软件和数据等各个方面的安全。在大数据时代，数据量巨大且种类繁多，因此网络安全问题也变得更加复杂和严峻。黑客攻击、病毒传播、网络犯罪等问题不断出现，给企业和个人带来巨大的损失。保障通信网络安全已成为大数据环境下必须解决的重要问题之一。因此，深入研究大数据环境下通信网络安全技术是具有现实意义的。

3.1 防火墙技术的应用

目前，利用防火墙技术来维护网络信息安全是一种主要策略，主要有两种形式:应用级防火墙和包过滤防火墙。应用级防火墙主要在原计算机环境下实现实时疏通，能够在较大程度上抵御病毒入侵，切断病毒的扩散途径，以在底层防止病毒对网络安全的破坏。包过滤防火墙像是在计算机系统边缘设置一个保护壳，能够针对入侵的病毒进行检查，识别和过滤潜在的危险病毒并进行应对，从而避免病毒侵入。防火墙技术实际上是一种在计算机和网络中间产生保护作用的软件。所有的网络数据都会经过防火墙，防火墙会审查所有流入的信息，拦截任何有攻 3.2 网络安全保密技术

在通信网络安全科技上，RSA 与 DES 被视为两种主导的加密技术。它们通过用密码对原始数据进行加密处理，确保用户信息的安全。用户需搭配设置有效的密码，才能进行加密。另外，这种技术也可以被用来加密和控制搜索关键信息，从而对电脑网络安全提供更强的防护。

3.3 数据的信息恢复、匿名化技术和水印技术

在大数据背景下，计算机网络环境受多种不安全因

素干扰，可能导致信息的丧失、外泄或缺乏完整性等。然而，通过技术性的信息恢复和补救手段，可将用户的损失降至最低。数据的信息恢复、匿名化技术和水印技术是保护通信网络安全的重要技术手段。数据的信息恢复是指通过一定的技术手段，将丢失或损坏的数据还原到原始状态。数据丢失和损坏可能是由病毒攻击、误操作等原因导致的。信息恢复技术可以恢复数据，避免数据丢失和损坏带来的安全隐患。匿名化技术可以有效地保护个人隐私，同时满足数据使用需求。水印技术是一种数字版权保护技术，通过在数据中嵌入版权信息，可以防止盗版和侵权行为。水印技术可以用于音频、视频、图像等多媒体数据的版权保护，也可以用于文件和软件的版权保护。通过水印技术，可以追踪和识别盗版和侵权行为，保护版权所有者的利益。

3.4 建立安全管理体系

加强员工的安全意识和安全素养培训，建立紧急响应机制，及时应对网络攻击和安全事件。同时，要加强与相关安全机构的合作，及时获取最新的安全策略和漏洞修复方案，提高整体的安全防范能力。通过采用对称加密算法或非对称加密算法对数据进行加密，确保数据传输过程中的机密性。同时，应建立完善的访问控制机制，对访问大数据的人员和设备进行有效的身份认证和权限管理。

4 结语

在大数据时代，强化通信网络安全稳定的重要性不言而喻。新技术持续的推动对网络安全系统构成了巨大挑战为确保网络服务正常高效地运行，有必要持续优化网络安全系统。这不仅需要优化网络安全技术，也需要增强网络用户的安全意识，把网络安全问题当作一项重要任务来对待。

【参考文献】

[1]杨方韬.信息技术发展背景下计算机网络工程建设对策研究[J].信息系统工程,2023(4):113－115.

[2]张玥,胡璨.大数据环境下通信网络安全技术的优化策略[J].中国信息化,2021(4):74－75.

[3]王华英.大数据时代通信网络安全技术[J].电子技术与软件工程,2021(9):249－250.

[4]单超.通信网络安全技术在大数据系统的应用探析[J].网络安全技术与应用,2021(9):82－83.