大数据时代计算机网络信息安全及防护策略研究

唐小沛

国家电投集团贵州金元绥阳产业有限公司，贵州 遵义 563300

摘　　要： 随着我国计算机技术的飞速发展，大数据时代的全面降临，计算机网络信息安全问题已经跃升为行业乃至社会关注的焦点。本文将首先详细阐述大数据时代的独特背景与其鲜明的技术特点，进而深入探讨和分析在海量数据流动与共享的过程中，计算机网络信息安全所面临的严峻挑战与潜在风险。为大数据时代下的计算机网络信息安全提供一套科学、合理且行之有效的防护策略，以期在保障信息流通的便捷与高效的同时，确保信息的安全、保密和完整性不受任何形式的侵害和威胁。这将有助于构建一个安全、可信、可靠的网络环境，为大数据时代的健康发展提供坚实的保障。

关 键 词： 大数据；计算机；网络信息；安全及防护；策略

Research On Computer Network Information Security And Protection Strategy In The Era Of Big Data

Tang Xiaopei

State Power Investment Group Guizhou Jinyuan Suiyang Industry Co., LTD. Zunyi, Guizhou 563300

Abstract: With the rapid development of computer technology in China, the advent of the era of big data, the computer network information security problem has become the focus of the industry and even the society. This paper will first elaborate on the unique background and distinct technical characteristics of the big data era in detail, and then further explore and analyze the severe challenges and potential risks faced by computer network information security in the process of massive data flow and sharing. To provide a set of scientific, reasonable and effective protection strategies for the computer network information security in the era of big data, in order to ensure the convenience and efficiency of information circulation, and ensure the security, confidentiality and integrity of information from any form of infringement and threat. This will help to build a safe, credible and reliable network environment, and provide a solid guarantee for the healthy development of the era of big data.

Keywords: big data; computer; network information; security and protection; strategy

引言

随着信息技术的日新月异，我们迈入了波澜壮阔的大数据时代。在这个时代里，数据已不再是简单的数字集合，而是成为了一种宝贵的资产，对个人生活、企业运营乃至国家发展都具有着举足轻重的价值。然而，正如一枚硬币的两面，数据的丰富性和价值性也带来了前所未有的安全挑战。计算机网络信息安全问题日益凸显，成为了威胁个人隐私、企业机密和国家安全的重要因素。深入探讨和研究大数据时代下的计算机网络信息安全及其相应的防护策略，显得尤为迫切和重要。这不仅是对现有安全体系的挑战，更是对未来信息安全发展方向的探索和预测。通过深入分析大数据时代的特征，我们可以更有针对性地制定防护策略，确保数据的完整性、可用性和保密性，为个人、企业乃至国家的长远发展保驾护航。

一、大数据时代背景与特点

（一）数据量庞大

在当今的大数据时代，数据量的增长已经远远超出了传统的计算范畴，呈现出一种前所未有的爆炸式增长态势。[1] 这种增长不仅局限于某个特定的领域或行业，而是全面覆盖了从科研、医疗、教育到金融、零售、交通等各个领域和行业。这种数据的爆炸式增长，不仅为我们提供了前所未有的洞察力和机会，同时也带来了对数据存储、处理和分析能力的极大挑战。

（二）数据多样性

在当今的信息化时代，数据类型展现出了极为丰富和多样化的特点。首先，结构化数据占据了重要的位置，这类数据具有固定的格式和明确的结构，如数据库中的表格数据，它们易于被计算机读取和处理。其次，半结构化数据也日益受到关注，它们具

有部分的结构性，如 XML 和 JSON 格式的数据，虽不如结构化数据那样严格，但在某些场景中却具有更高的灵活性和适应性。[2] 非结构化数据则更为广泛，包括文本、图像、音频、视频等多种形式，它们没有固定的结构，但蕴含着丰富的信息，需要通过特定的技术手段进行提取和分析。这三种数据类型各有特点，共同构成了当今数据领域的丰富图景。

（三）数据价值高

在当今信息爆炸的时代，数据无疑扮演着举足轻重的角色。在决策层面，数据能够提供精准的信息支撑，帮助企业或国家作出更为明智的选择；在预测领域，数据作为趋势的指针，能够揭示未来的可能走向，为规划提供重要依据；在优化方面，通过对数据的深入挖掘和分析，能够发现潜在的问题与机会，进而推动效率与效益的双重提升。[3] 数据已经超越了单纯的数字集合，成为了企业和国家不可或缺的核心资产，其价值和重要性不言而喻。

二、影响计算机网络安全的因素分析

（一）自然灾害

计算机设备在本质上并不具备直接抵御外部环境带来的各种潜在破坏因素的能力。它们对于诸如强烈震动、环境污染、水灾和火灾等自然灾害的抵御能力相对薄弱。这些自然灾害一旦发生，不仅可能直接导致计算机设备的物理损坏，如电路板断裂、硬盘受损等，还可能间接引发数据丢失、系统崩溃等严重后果。因此，为了确保计算机设备的安全稳定运行，我们需要采取一系列有效的防护措施，以减少自然灾害对计算机设备的潜在威胁。

（二）网络的开放性

计算机网络的开放性如同一把双刃剑，它极大地促进了信息和资源的流通与共享，为全球各地的用户提供了便捷的沟通和获取信息的途径。这种开放性也相应地增加了网络被恶意攻击的风险。[4] 黑客们常常利用网络的这种开放性，通过各种手段和技术手段进行非法入侵，企图窃取、篡改或破坏敏感数据和关键资源。这些攻击行为不仅严重威胁着个人隐私和商业机密的安全，更可能对整个社会的稳定和发展造成不可估量的损失。在享受计算机网络带来的便利的同时，我们也需要时刻保持警惕，加强网络安全防护，确保网络环境的稳定和安全。

三、大数据时代下计算机网络信息安全面临的挑战

（一）数据泄露风险

鉴于数据量的庞大及其蕴含的巨大价值，我们必须充分认识到其重要性。数据，作为企业和个人的核心资产，一旦遭受泄露，其后果将不堪设想。对于企业而言，数据泄露可能导致商业机密被窃取、客户信息泄露、品牌声誉受损等连锁反应，从而严重影响企业的市场竞争力和经营效益。[5] 而对于个人来说，数据泄露可能涉及个人隐私泄露、身份被冒用等风险，给个人的生活和安全带来极大的威胁。因此，保护数据安全成为了当今社会不可或缺的重要任务，必须高度重视并付诸行动。

（二）网络攻击手段多样化

在当今数字化的世界中，网络安全面临着前所未有的挑战。黑客攻击、病毒、木马等网络攻击手段层出不穷，如同暗流涌动的威胁，给网络安全带来了巨大压力。这些攻击手段不仅手段多样，而且技术日益复杂，它们能够悄无声息地侵入计算机系统，窃取敏感信息、破坏数据完整性，甚至操控整个网络。[6] 这种形势对于个人用户、企业组织乃至整个国家的信息安全都构成了严重威胁，因此，加强网络安全防护、提升网络安全意识已迫在眉睫。

（三）移动互联网安全挑战

随着移动互联网的广泛普及和深入渗透，网络攻击的手段和途径变得日益多样化和隐蔽化，这使得个人信息安全面临前所未有的严峻挑战。在数字世界中，用户的个人信息如同宝藏一般，吸引了不法分子的目光。他们利用技术手段，悄无声息地窃取、篡改或滥用这些信息，给用户带来了极大的风险与损失。因此，保护个人信息安全已经成为了一个刻不容缓的问题，需要社会各界的共同努力和持续关注。随着移动互联网的日益普及，人们已经能够享受到随时随地接入网络的便捷性，这种无缝连接极大地丰富了我们的日常生活和工作方式。[7] 移动设备的便捷性，意味着其信息传输更加频繁且广泛，但这同样使它们成为潜在的网络攻击目标。攻击者可以利用移动设备在传输过程中的薄弱环节，进行各种形式的网络攻击，如数据窃取、恶意软件植入等。

四、计算机网络信息安全防护策略

（一）加强安全意识教育

面对日趋复杂的网络安全问题，无论是个人还是公司，都急需增强自身的网络安全意识，增强自我保护意识。个人要重视网络安全，要学会识别网络诈骗，保护好自己的个人隐私，采取行之有效的手段来防止网络攻击。在此基础上，提出了一种基于信息技术的信息安全管理方法。从而保证企业的数据资源的安全性与稳定性。[8]

（二）采用先进的安全技术

随着信息技术的发展，信息系统的安全保护越来越受到人们的重视。要想有效地应对各种类型的网络攻击，就必须利用各种技术方法来增强网络的安全保护。防火墙是网络安全的第一道防线，它主要对网络数据进行监测，并按照预先设定的安全机制对非法用户进行过滤或拦截。随着网络攻击方式的变化，防火墙的技术也得到了进一步的发展。新一代防火墙通过行为分析、机器学习等更加智能的威胁探测方法，可以更加精准地发现并拦截“零天漏洞”以及未知的高层次威胁。入侵检测系统通过采集和分析网络流量、系统日志和用户行为等信息，发现异常和可疑行为。它是一种利用模式匹配，统计分析，以及人工智能的方法来发现和处理网络攻击的方法。入侵检测系统可以对网络的行为进行实时监测，并对其进行预警，从而降低系统的安全风险。入侵检测系统要想更精确地发现网络攻击，就必须搜集更多的信息，提高数据分析的能力。通过与防火墙和路由器等网络设备的联

动，一旦发现有攻击发生，入侵行为就能第一时间切断攻击者，阻止其蔓延。数据加密是一种有效的方法，可以有效地解决数据的安全问题。[9] 使用加密算法和密钥，将明文转化为密文，以防止外人破解。数据加密技术主要包括数据传输的加密，数据存储的加密，数据的完整性认证，以及密钥管理等。这三种方法是从软硬件两个角度来保证数据的安全传输。防火墙技术、入侵检测系统（IDS）以及数据加密技术是增强网络安全保护的重要途径。这三种网络架构各有其自身的特点与优点，可以相辅相成，共同构筑更为安全可靠的网络环境。在对网络设备及软件进行选型时，必须保证其安全性、可靠性。我们要仔细甄别，不要购买没有经过正式认证或来源不明确的网络设备及软件，因为它们一旦被部署到互联网上，就会存在潜在的安全隐患；这将会对网络系统造成极大的威胁。[10] 我们应该选择经过权威机构认证、具有良好声誉和可靠性的网络设备和软件，从而确保我们的网络安全得到最大程度的保障。

（三）加强网络监控和及时响应

为了有效保障网络安全，构建一个完善的网络监控体系至关重要。制定一套全面的网络安全策略，明确安全目标、责任分配和安全规范，确保公司内部人员对网络安全的重要性有充分的认识。对企业的关键资产、业务流程和网络环境进行全面风险评估，识别潜在的安全威胁和漏洞，以便确定安全投入的优先级，并针对性地进行防护。基于风险评估结果，设计符合安全要求的网络架构，包括划分网络区域、部署防火墙、入侵检测系统等安全设备，以及实施网络接入控制等措施。保障操作系统、应用程序、数据库等关键系统的安全，通过安装安全补丁、加固系统配置、实施权限管理等措施，减少系统被攻击的风险。对敏感数据进行加密处理，防止数据泄露。同时，建立严格的身份认证机制，确保只有授权用户才能访问关键资源。部署安全监控系统，实时监控网络活动，检测异常行为。同时，定期进行安全审计，评估安全防控体系的有效性，及时发现并处理网络安全事件。针对可能发生的网络安全事件，制定详细的应急预案，包括事件报告、问题定位、数据恢复、后续改进等内容，确保在发生安全事件时能够迅速、有效地应对。为员工提供网络安全相关知识及技术方面的培训。保证所有员工都知道公司的保安制度，并且遵守公司的规章制度。[11] 网络安全是一项不断进行评估、调整和改善的工作。定期检讨预防与控制系统，找出新的危险及弱点，并作出有目标的调整及最佳化。密切跟踪产业发展趋势，掌握最新的安全科技及先进做法，并运用到自身的安全防护系统中。在此基础上，按照国家有关规定，严格遵守国家有关规定，保证企业在网络安全方面达到规定的要求。为了保证企业网络的安全，我们将逐渐形成一套完整的网络监测系统。

结语

在如今的大数据时代背景下，探讨计算机网络信息安全及其防护策略的重要性愈发凸显。这不仅关系到企业的核心数据安全，更是涉及到国家安全与公共利益的关键问题。因此，深入研究和实施有效的安全防护策略，对于维护网络空间的稳定与繁荣具有深远意义。加强安全意识教育是防范网络信息安全风险的基石。我们需要通过广泛的安全知识普及和培训，提高广大用户和管理者的安全意识，使大家认识到信息安全的重要性和必要性，从而形成全社会共同维护网络安全的良好氛围。采用先进的安全技术是保障网络信息安全的关键。随着技术的不断进步，网络安全威胁也日益复杂多变。因此，我们需要不断引进和研发先进的安全技术，如加密技术、防火墙技术、入侵检测技术等，以应对日益严峻的网络安全挑战。加强网络监控和及时响应是防范网络安全威胁的有效手段。通过建立完善的网络监控体系，实时发现和跟踪网络安全事件，并及时进行应急响应和处理，可以有效地防止网络攻击和数据泄露等安全事件的发生。我们需要持续关注网络安全领域的新技术、新动态，不断完善网络安全防护策略。随着大数据、云计算、物联网等新技术的不断发展，网络安全面临的威胁和挑战也将不断变化。因此，我们需要紧跟技术发展的步伐，不断完善和优化安全防护策略，确保大数据时代下的计算机网络信息安全。大数据时代下的计算机网络信息安全及防护策略研究是一项长期而艰巨的任务。只有我们不断加强安全意识教育、采用先进的安全技术、加强网络监控和及时响应，并持续关注新技术和新动态，才能确保网络空间的稳定与繁荣，为经济社会发展提供坚实的保障。

参考文献

[1] 孙美玲. 基于大数据分析的计算机网络信息安全监测［J］. 信息与电脑（理论版），2023，35（22）：239-241.

[2] 李俊. 计算机网络信息安全中的网络技术运用［J］. 信息记录材料，2023，24（11）：109-111+114.

[3] 孙玮. 大数据背景下计算机网络信息安全及防范策略研究［J］. 数字通信世界，2022，（12）：169-171.

[4] 麻恒瑞. 计算机网络信息安全保障措施研究［J］. 电脑知识与技术，2022，18（29）：71-73.

[5] 袁一帆. 探讨如何实现大数据时代的计算机网络信息安全［J］. 网络安全技术与应用，2021，（12）：174-175.

[6] 杨佳兰. 基于大数据环境下的计算机网络信息安全与防护策略研究［J］. 南方农机，2021，52（23）：132-134.

[7] 于柯实. 探讨大数据时代计算机网络信息安全及防护策略研究［J］. 信息系统工程，2023（09）：130-133.

[8] 刘占凤. 大数据时代如何加强计算机网络信息安全管理［J］. 网络安全技术与应用，2023（07）：162-164.

[9] 倪瑞，梁嫣良，马雯阳. 大数据时代背景下的网络信息安全管理分析［J］. 数字通信世界，2023（06）：188-190.

[10] 郝景昌，徐李阳，赵文华，等. 大数据时代计算机网络信息安全与防护［J］. 数字技术与应用，2023，41（04）：219-221.

[11] 杨晓娇，吴文博，董洁，等. 大数据时代下的网络信息安全保护策略研究［J］. 数字通信世界，2023（02）：4-5+23.