大数据时代背景下计算机网络信息安全防护技术研究

李大勇
北京北方车辆集团有限公司　北京　100072

摘　要：随着大数据技术的快速发展和广泛应用，计算机网络信息安全问题日益凸显。大数据时代下的计算机网络技术具有共享性、便捷性、多元性、实时性等优势，但也存在诸多安全隐患，如黑客攻击、病毒入侵、人为操作失误等。本文研究了大数据时代背景下计算机网络信息安全防护技术，包括防火墙技术、数据加密技术、入侵检测技术等，并提出了相应的防护措施，旨在为计算机网络信息安全提供有力保障。

关键词：大数据时代背景；计算机网络信息；安全防护技术

引言：在大数据时代背景下，计算机网络信息技术的迅猛发展为企业决策、产业转型升级提供了科学依据和技术支撑。然而，随着大数据技术的广泛应用，计算机网络信息安全问题也愈发严重，黑客攻击、数据泄露等事件频发，对个人隐私、企业机密乃至国家安全构成严重威胁。因此，研究大数据时代背景下计算机网络信息安全防护技术，提高信息安全防护能力，已成为亟待解决的重要课题。

1 大数据时代背景下计算机网络信息安全现状分析

1.1 大数据时代的网络信息技术应用及其优势

在大数据时代，网络信息技术得到了前所未有的广泛应用。大数据技术的快速发展，使得企业能够收集、存储和分析海量的数据，从而挖掘出有价值的信息，为决策提供科学依据。大数据技术在电子商务、物联网金融、智能制造等领域的应用，推动了产业的转型升级，提高了生产效率和服务质量。同时，云计算、人工智能等技术的融合应用，进一步增强了大数据技术的处理能力和智能化水平，为数字经济的发展提供了强大的技术支撑。

1.2 当前计算机网络信息安全面临的挑战与威胁

（1）黑客攻击与数据泄露事件概述。随着大数据技术的普及，黑客攻击和数据泄露事件频发，对个人、企业和国家安全构成了严重威胁。黑客利用系统漏洞、恶意软件等手段，窃取敏感数据，进行非法交易或勒索。近年来，多次发生的大规模数据泄露事件，不仅导致用户隐私泄露，还引发了严重的信任危机和法律风险。这些事件暴露出当前计算机网络信息安全防护的薄弱环节，亟需加强安全防护措施。（2）系统漏洞与环境因素的危害。系统漏洞是计算机网络信息安全的重要威胁之一。由于软件设计、编码过程中的疏忽，以及系统更新不及时等原因，导致系统存在漏洞，黑客可以利用这些漏洞进行攻击。此外，环境因素也对计算机网络信息安全构成威胁。如自然灾害、电力故障等，可能导致网络设备损坏或数据丢失，进而影响系统的正常运行和数据的安全性[1]。（3）网络钓鱼、勒索软件等新型攻击手段。网络钓鱼、勒索软件等新型攻击手段的出现，进一步加剧了计算机网络信息安全的风险。网络钓鱼通过伪装成合法的网站或邮件，诱骗用户输入敏感信息，从而窃取数据或进行诈骗。勒索软件则通过加密用户文件或系统，要求支付赎金以换取解密密钥，给用户和企业带来了巨大的经济损失和运营困扰。

1.3 国内外计算机网络信息安全防护现状对比

国内外在计算机网络信息安全防护方面存在一定的差异。国外在信息安全技术研发、法律法规制定以及国际合作等方面相对领先。例如，美国、欧洲等国家和地区在数据保护、网络安全等方面制定了严格的法律法规，并加强了与国际社会的合作与交流。而国内在信息安全技术研发和法律法规建设方面也在不断完善，但与国外相比仍存在一定的差距。同时，国内企业在信息安全防护方面的投入和重视程度也参差不齐，部分企业在信息安全防护方面存在薄弱环节。

2 大数据时代背景下计算机网络信息安全防护技术

2.1 数据加密技术

数据加密技术作为信息安全的基础，其核心在于通过对数据进行编码，使得未经授权的用户无法解读原始数据。这一技术不仅能够有效防止数据泄露，还能在数据传输过程中提供保护。（1）强加密算法的应用。AES（高级加密标准）和RSA是当前最广泛使用的两种加密算法。AES以其高效和安全性著称，适用于大多数数据加密需求，尤其是需要快速加密和解密大量数据的场景。而RSA则以其非对称加密的特性，广泛应用于数字签名和密钥交换，为网络通信提供了更高的安全性[2]。（2）

敏感数据的识别与分类管理。在大数据时代，敏感数据的识别与管理至关重要。企业应对数据进行分类，明确哪些数据是敏感的，哪些是非敏感的。对于敏感数据，如个人隐私、商业机密等，应采用更严格的加密措施，如使用更强的加密算法、定期更换密钥等。同时，还应建立敏感数据的访问权限制度，确保只有经过授权的人员才能访问这些数据。

2.2 防火墙与入侵检测系统

防火墙和入侵检测系统是网络安全的第一道和第二道防线，它们共同构成了网络安全的立体防护体系。（1）防火墙技术的基础构建与安全防护作用。防火墙作为网络安全的门户，通过制定和执行一系列安全策略，对进出网络的数据包进行过滤和检查。它不仅能够阻止未经授权的访问，还能防止恶意软件的传播。防火墙的基础构建包括包过滤、代理服务和状态检测等关键技术，这些技术能够确保只有合法的流量才能通过网络，从而保护内网资源免受外部威胁。（2）入侵检测系统的原理与实时监测功能。入侵检测系统（IDS）则是对防火墙的补充，它通过对网络流量、系统日志等数据进行深度分析和检测，能够发现网络中的异常行为和潜在威胁。IDS的工作原理基于误用检测和异常检测两种模式，误用检测通过匹配已知的攻击模式来发现攻击，而异常检测则通过分析网络流量的正常模式来识别异常行为。实时监测功能是IDS的核心优势之一，它能够在攻击发生前或发生时及时发出警报，为网络安全管理员提供及时的响应和处置时间。

2.3 身份认证与访问控制技术

身份认证与访问控制是确保网络资源安全的重要手段，它们通过验证用户身份和限制访问权限，防止未经授权的访问和操作。（1）身份认证技术的实现与重要性。身份认证技术包括用户名/密码、数字证书、生物特征等多种方式。这些技术能够确保只有合法的用户才能访问网络资源。身份认证的重要性在于，它能够防止恶意用户冒充合法用户进行访问和操作，从而保护网络资源免受非法侵害。（2）基于角色与属性的访问控制策略。基于角色（RBAC）和基于属性（ABAC）的访问控制策略是当前最流行的两种访问控制方法。RBAC将用户划分为不同的角色，并为每个角色分配特定的访问权限。这种方法简化了权限管理，降低了管理成本。而ABAC则更加灵活，它根据用户的属性（如职位、部门等）和资源的属性（如敏感度、重要性等）来动态决定用户的访问权限。这种方法能够更好地适应复杂多变的网络环境，提高访问控制的安全性和灵活性[3]。

2.4 数据备份与灾难恢复技术

数据备份与灾难恢复技术是确保数据安全的重要手段，它们能够在数据丢失或损坏时提供及时的恢复和保障。（1）数据备份的重要性与实施策略。数据备份是指将重要数据复制到另一个物理或逻辑存储设备上的过程。其重要性在于，当原始数据因各种原因（如硬件故障、自然灾害等）而丢失或损坏时，可以通过备份数据进行恢复。实施数据备份时，应考虑备份的频率、备份数据的存储位置和安全性以及备份数据的完整性和可用性等因素。（2）灾难恢复计划的制定与演练。灾难恢复计划是指在灾难事件发生后，为了恢复业务运行和数据安全而制定的详细行动计划。制定灾难恢复计划时，应明确灾难恢复的目标、恢复策略、恢复步骤和恢复时间等关键要素。同时，还应定期对灾难恢复计划进行演练和评估，以确保计划的可行性和有效性。

2.5 新兴安全防护技术探讨

随着大数据和人工智能技术的快速发展，新兴的安全防护技术不断涌现，为计算机网络安全提供了更多的选择和可能性。（1）AI技术在安全防护中的应用。AI技术能够自动识别和分析网络流量中的异常行为，实现对潜在威胁的实时监测和预警。通过机器学习算法，AI能够不断学习和优化自身的检测能力，提高威胁检测的准确性和效率。同时，AI还能与其他安全防护技术相结合，如与防火墙、入侵检测系统等协同工作，形成更加智能化的安全防护体系[4]。（2）物联网设备与5G网络的安全防护策略。物联网设备和5G网络的安全问题日益凸显。为了保障物联网设备和5G网络的安全性，应采取以下策略：首先，加强对物联网设备和5G网络的安全认证和访问控制，确保只有合法的设备和用户才能接入网络；其次，定期对物联网设备和5G网络进行漏洞扫描和风险评估，及时发现并修复潜在的安全漏洞；最后，建立物联网设备和5G网络的安全监测和应急响应机制，确保在发生安全事件时能够迅速做出反应并处置。

3 大数据时代背景下计算机网络信息安全防护的未来发展趋势

3.1 网络安全防护技术的创新方向

（1）新兴技术在安全防护中的潜在应用。在大数据技术的推动下，网络安全防护领域不断涌现出新的技术方法和手段，为信息安全提供了更强大的保障。1）人工智能与机器学习：这些技术能够分析大量数据，识别潜在的安全威胁，并实时响应。通过学习历史数据，AI系统能够预测未来的攻击模式，从而提前采取防护措施。此外，机器学习算法可以不断优化自身的检测能力，适

应新的攻击方式。2）零信任架构：传统的安全模型中，内部网络被视为安全的，而外部网络则被视为不安全的。然而，随着网络攻击手段的多样化，内部威胁的风险也在增加。零信任架构要求对每一个访问请求进行严格验证，无论请求来自内部还是外部，从而有效降低数据泄露和未授权访问的风险。3）量子加密技术：量子计算的快速发展为网络安全带来了新的挑战和机遇。量子加密技术利用量子力学的原理，提供了一种几乎无法破解的加密方式，确保信息在传输过程中不会被窃取或篡改。4）区块链技术：区块链以其去中心化和不可篡改的特性，正在被广泛应用于网络安全领域。通过区块链，数据可以在多个节点之间安全地共享，降低了单点故障的风险，提高了数据的透明度和可信度。5）下一代防火墙：下一代防火墙引入了深度包检测技术，能够对网络数据包的内容进行检查，并根据协议、应用程序及用户行为等信息进行精确过滤，提高了企业网络的安全。（2）安全防护技术的未来发展趋势预测。未来，随着网络攻击手段的不断升级，安全防护技术也将不断进化。预计将有更多智能化、自动化的安全防护技术涌现，如基于行为分析的实时监测系统、自动化的应急响应系统等。同时，量子加密、区块链等新兴技术将逐渐成熟并广泛应用于网络安全防护中，提供更强大的安全保障。

3.2 网络安全法律法规的完善与国际化合作

（1）国内外网络安全法律法规的发展动态。近年来，各国政府和国际组织纷纷出台相关法规，以加强网络安全管理。例如，中国的《网络安全法》《数据安全法》《个人信息保护法》等法律相继颁布实施，确立了网络数据安全的基本制度框架和基本法律原则。而在国际上，GDPR（通用数据保护条例）等法规也要求企业在处理个人数据时采取严格的安全措施。（2）国际化合作在安全防护中的重要作用。网络安全风险的全球化使得任何国家和地区都无法独善其身。国际合作在安全防护中扮演着重要角色，有助于建立全球网络空间的秩序和规则，减少网络冲突和对抗，促进网络空间的和平与稳定。通过加强网络安全情报共享、技术合作、能力建设、打击网络犯罪等方面的合作，各国和地区可以共同应对网络安全威胁，提高整体安全防护能力。

3.3 网络安全人才培养与技能提升

（1）网络安全人才的培养需求与现状。随着网络安全威胁的不断增加，网络安全人才的需求也日益迫切。目前，网络安全人才短缺已成为全球性问题。各国和地区都在积极采取措施，加强网络安全人才的培养和引进。例如，中国通过设立专门的网络安全专业、完善教育体系、加强实践教学等方式，培养具备网络安全意识和技能的学生。（2）技能提升的途径与策略。为提升网络安全技能，个人和组织可以采取多种途径和策略。一方面，可以通过参加培训课程、在线学习、实践演练等方式不断更新知识和技能。另一方面，可以建立校企合作机制，推动产学研一体化发展，加快网络安全人才培养与市场需求的对接。此外，还可以加强与国际知名网络安全机构的合作，引进先进的教育理念和技术，提高网络安全人才培养的水平。

结束语

综上所述，大数据时代背景下计算机网络信息安全防护技术的研究对于保障个人、企业和国家安全具有重要意义。通过数据加密、防火墙与入侵检测系统、身份认证与访问控制等多种技术手段的综合应用，可以有效提升计算机网络信息的安全性。未来，随着技术的不断进步和法律法规的完善，计算机网络信息安全防护体系将更加健全，为大数据时代的可持续发展提供有力保障。

参考文献

[1]石展.浅析大数据时代网络信息安全应对策略[J].网络安全和信息化,2022(08):73-74.

[2]赵占旺.大数据时代网络与信息安全探讨[J].计算机科学与人工智能,2022,(02):29-31.

[3]刘良港.大数据时代计算机网络信息安全及防护策略研究[J].工程技术发展,2021,(03):36-37.

[4]张刚.大数据时代下计算机网络信息安全问题分析与研究[J].计算机应用文摘,2022,(09):90-92.