大数据环境下计算机技术的网络安全威胁分析

何智超

巴彦淖尔市铭筑建筑构件有限公司，中国·内蒙古自治区　巴彦淖尔　015000

【摘　要】本文聚焦于大数据环境下计算机技术的网络安全威胁。随着大数据的快速发展，计算机技术广泛应用，网络安全面临诸多挑战。本论文概括分析网络安全保障的重要性，如保护数据完整性、隐私性等。阐述计算机技术面临的威胁，包括恶意软件、网络攻击手段多样化等问题。同时探讨解决对策，如强化技术研发、完善管理制度等方面，旨在全面呈现大数据环境下计算机技术网络安全威胁的现状与应对策略，为保障网络安全提供参考。

【关键词】大数据；计算机技术；网络安全威胁

引言

在当今数字化时代，大数据蓬勃发展，计算机技术渗透到各个领域。海量数据的产生、存储和传输成为常态。然而，这一进程也伴随着网络安全风险的急剧增加。网络安全威胁的复杂性和多样性不断攀升，从个人隐私泄露到企业商业机密受损，从系统瘫痪到数据丢失，这些问题严重影响着计算机技术在大数据环境下的正常应用。这一现状促使我们深入探究计算机技术在大数据环境下所面临的网络安全威胁，进而为后续的研究奠定基础。

1　大数据环境下计算机技术网络安全保障的重要性

在大数据环境下，计算机技术的网络安全保障具有不可忽视的重要性。计算机技术是大数据存储、处理和传输的核心支撑，一旦网络安全出现漏洞，可能导致数据的大规模泄露或损坏。网络安全保障有助于维护数据的完整性。在大数据的复杂环境中，数据在各个节点之间频繁流动，任何一个环节的数据篡改都可能引发连锁反应，影响整个数据体系的准确性。保护数据隐私性是网络安全保障的关键任务。大数据包含大量的个人信息、企业机密等敏感数据，这些数据一旦被窃取或不当使用，将对个人和企业造成巨大损失。

2　大数据环境下计算机技术面临的网络安全威胁问题

恶意软件的威胁日益严重，传统的病毒、木马等恶意软件不断进化，新的变种层出不穷。它们能够悄无声息地潜入计算机系统，破坏数据、窃取信息。勒索软件更是成为一大威胁，它通过加密用户数据，勒索用户支付赎金以恢复数据，给用户带来巨大损失。网络攻击手段也呈现出多样化的趋势，DDoS攻击频繁发生，攻击者通过控制大量僵尸网络向目标服务器发送海量请求，使服务器不堪重负，导致网络服务不可用。网络钓鱼也愈发猖獗，攻击者伪装成合法机构，诱导用户泄露账号密码等重要信息，从而获取非法利益。

3　大数据环境下计算机技术网络安全威胁的解决对策

3.1强化网络安全技术研发

强化网络安全技术研发是应对大数据环境下计算机技术网络安全威胁的关键举措。在大数据时代，网络安全技术需要不断创新和升级以适应新的威胁形式。随着数据量的爆炸式增长和网络攻击手段的日益复杂，传统的网络安全技术已显得力不从心。研发新型的防火墙技术是重要方向之一，这种防火墙应具备智能识别能力，能够根据大数据分析结果准确判断网络流量中的恶意行为并及时阻断。入侵检测系统也需要进一步强化，它要能够在海量数据中快速检测到潜在的入侵行为，不仅仅是基于已知的攻击模式，还应具备对未知攻击的预警能力。人工智能和机器学习技术应深度融入网络安全技术研发中，利用其强大的数据分析和模式识别能力，对网络安全威胁进行实时监控和预测。例如，通过机器学习算法对网络行为进行建模，识别异常行为模式，从而提前防范网络攻击。研发高效的数据加密技术也是重中之重，确保数据在存储和传输过程中的安全性，即使数据被窃取，攻击者也无法获取有效信息。网络安全技术研发还应注重安全协议的优化，使其在大数据环境下能够提供更可靠的安全保障，防止数据在传输过程中被篡改或窃取。

3.2完善网络安全管理制度

完善网络安全管理制度对于应对大数据环境下计算机技术的网络安全威胁至关重要。在大数据的复杂环境中，没有完善的管理制度，再好的技术也难以发挥其最大效能。企业和组织应建立全面的网络安全管理框架，明确各部门在网络安全中的职责和权限。例如，IT部门负责技术维护和安全策略的执行，而管理层则负责制定网络安全战略和监督执行情况。在人员管理方面，要加强网络安全意识培训，提高员工对网络安全威胁的认识，避免因员工的疏忽导致安全漏洞。如定期开展网络安全培训课程，包括识别

网络钓鱼邮件、正确使用公司网络资源等内容。要建立严格的访问控制制度，根据员工的岗位职能和权限级别，分配不同的数据访问权限，确保数据的安全性。在数据管理方面，应制定完善的数据备份和恢复策略，以应对可能的数据丢失或损坏情况。建立网络安全应急响应机制是必不可少的，当发生网络安全事件时，能够迅速启动应急预案，进行事件的评估、处理和恢复工作，最大限度地降低损失。对于网络安全管理制度的执行情况，要进行定期的审计和评估，及时发现制度执行过程中的问题并加以改进，确保制度的有效性和适应性。

3.3加强数据加密技术应用

在大数据时代，数据的价值愈发凸显，数据的安全性也成为重中之重。数据加密技术通过对数据进行编码转换，使得只有拥有正确密钥的用户才能解读数据，从而保障数据的保密性和完整性。在数据存储方面，应采用先进的加密算法对存储在本地或云端的数据进行加密。例如，对称加密算法具有加密速度快的优点，适用于对大量数据的加密；而非对称加密算法则在密钥管理方面具有优势，可用于加密对称加密算法的密钥，两者结合使用能提供更强大的安全保障。在数据传输过程中，无论是在企业内部网络还是在互联网上传输数据，都必须进行加密处理。例如，使用SSL/TLS协议对网络传输的数据进行加密，防止数据在传输过程中被窃取或篡改。对于移动设备中的数据加密也不容忽视，随着移动办公的普及，移动设备存储和传输大量敏感数据，采用合适的加密技术确保这些数据的安全至关重要。加密技术的密钥管理也是关键环节，应建立安全可靠的密钥管理体系，确保密钥的生成、存储、分发和更新过程的安全性，防止密钥泄露导致数据被解密。

4 建立网络安全监测体系

网络安全监测体系犹如网络空间的预警机，能够对潜在的安全风险进行实时监控与分析。大数据的海量性、多样性和高速性等特点，使得网络攻击手段更加隐蔽和复杂。建立网络安全监测体系首先要部署全方位的传感器，这些传感器能够覆盖网络的各个节点，包括服务器、终端设备以及网络传输链路等。通过对网络流量、系统日志、用户行为等多源数据的采集，为后续的分析提供丰富的数据基础。在数据采集的基础上，需要运用先进的数据分析技术。机器学习和人工智能算法在其中发挥着重要作用。例如，异常检测算法能够通过学习正常的网络行为模式，识别出偏离正常模式的异常活动，这些异常可能是恶意软件的入侵、数据泄露或者是网络攻击的先兆。同时，关联分析技术可以将不同来源的数据进行关联，挖掘出隐藏在数据背后的安全威胁线索，如看似孤立的登录失败事件与特定文件的异常访问可能存在关联，是一次有组织的攻击行为的不同表现。网络安全监测体系还应具备快速响应能力。一旦监测到安全威胁，能够及时向相关的安全管理人员发出警报，并提供详细的威胁信息，包括威胁的来源、类型、可能造成的影响等。

5 促进国际网络安全合作

大数据的全球流动使得网络安全问题不再局限于一国之内。恶意软件、网络攻击等威胁可以迅速跨越国界，影响到多个国家的计算机网络和信息系统。不同国家在网络安全技术、法律法规、管理经验等方面存在差异，这既可能导致网络安全治理的漏洞，也为国际合作提供了互补的空间。促进国际网络安全合作需要在技术层面展开深入交流。各国可以共享网络安全威胁情报，例如，一个国家发现的新型网络攻击手段或者恶意软件的特征码，可以及时分享给其他国家，这样其他国家就能够提前做好防范措施。同时，在网络安全技术研发方面进行合作，共同攻克如大数据加密技术、跨境网络流量监测技术等难题。通过联合研究项目，集合各国的科研力量和资源，提高全球网络安全技术水平。在法律法规方面，国际间应加强协调。由于各国的法律体系不同，对于网络犯罪的定义、惩处标准等存在差异，这给跨国网络犯罪的打击带来了困难。各国应就网络安全相关的法律法规进行交流与协商，寻求建立一些基本的国际准则和标准，如网络犯罪的认定框架、跨境电子证据的获取和使用规则等。这有助于消除法律上的障碍，确保各国在打击网络犯罪时有统一的依据。

结束语

通过分析可知网络安全保障具有多方面的重要性，包括维护数据完整性、隐私性以及系统稳定性等。同时计算机技术面临着恶意软件攻击、网络攻击手段多样化、数据管理与存储风险等诸多网络安全威胁问题。为了更好地应对网络安全威胁，建议企业和组织持续投入资源到网络安全建设中，不仅要关注技术的更新换代，还要重视管理制度的完善和人员安全意识的提升，以构建全面、有效的网络安全防护体系，保障大数据环境下计算机技术的安全稳定运行。

参考文献：

[1]窦也翔,高闪闪.大数据时代及计算机技术的网络安全探究[J].科学技术创新,2019(1):101-102.

[2]陶丽.大数据背景下计算机网络安全问题初步探讨[J].网络安全技术与应用,2022(1):161-163.

[3]葛利,陆琦.浅析大数据网络安全态势感知中的数据融合技术[J].科技创新导报,2022,19(22):70-72.