大数据背景下的计算机网络信息安全

史立杰
内蒙古赤峰市巴林左旗花加拉嘎乡人民政府　内蒙古赤峰　025450

摘　要：随着大数据技术的迅猛发展，计算机网络信息安全面临着前所未有的挑战和机遇。大数据在为各行业带来深刻变革的同时，也使得信息安全问题日益凸显。海量数据的存储、传输和处理过程中，任何安全漏洞都可能导致严重的后果，包括数据泄露、篡改和非法访问等。本文将从大数据的基本特征入手，深入分析计算机网络信息安全防护的积极意义，探讨有效的安全防护技术和策略，以期为提高信息安全水平提供有益参考和实践指导。

关键词：大数据；计算机网络；信息安全

各行业、各领域无不在借助大数据技术的力量，实现更高效的决策、更精准的服务以及更具创新性的发展。然而，大数据在为人类带来便利和机遇的同时，也引发了前所未有的计算机网络信息安全挑战。信息安全问题的复杂性在大数据背景下愈加凸显，传统的安全防护手段和策略在大规模、多样化、高速流动的数据面前显得力不从心。因此，如何在大数据背景下有效保障计算机网络信息安全，已成为学术界、产业界和政府部门共同关注的重要课题。

1　大数据时代计算机网络信息安全的特征

1.1 完整性

数据完整性不仅要求信息在生成、传输和存储过程中不被非授权篡改或破坏，还需要确保数据的一致性和准确性。由于大数据涉及的数据量巨大，且来源广泛，任何数据的不完整或不一致都可能导致决策错误，甚至带来严重的经济损失和声誉风险。因此，保障数据完整性成为信息安全防护的核心环节之一。维护数据完整性的关键在于采用多种技术手段，如数据加密、数字签名、校验码等，确保数据在各个环节的完整性得到有效验证。同时，建立严格的数据质量管理制度，对数据采集、清洗、转换等流程进行规范化管理，确保数据的一致性和准确性。

1.2 隐私性

随着海量数据的生成和收集，个人隐私和敏感信息的保护面临严峻挑战。大数据技术的广泛应用使得数据挖掘和分析更加深入，许多原本看似无害的数据通过交叉引用与分析，可能泄露出个人身份、行为模式甚至生活细节。这种隐私泄露不仅侵害了个人的基本权利，还可能导致声誉受损和财务安全风险。为保障隐私性，各组织和企业亟需建立健全的数据治理机制，明确数据使用的范围和目的。同时，采用数据脱敏技术、访问控制和加密通信等手段，防止敏感信息在传输和存储过程中被不当获取。

2　大数据时代计算机网络信息安全防护的积极意义

2.1 有效保护系统安全

系统安全不仅是指防止外部攻击和数据泄露，还包括维护系统的稳定性和可靠性。大数据环境下，系统面临着多方面的安全威胁，如恶意软件、DDoS攻击、拒绝服务攻击等。通过实施有效的安全防护措施，如防火墙、入侵检测系统、安全信息和事件管理系统（SIEM），可以显著增强系统的防御能力，减少潜在的安全风险。此外，大数据技术的广泛应用推动了许多新技术的出现，如人工智能和机器学习，这些技术在提升数据处理效率的同时，也为安全防护提供了新的手段。机器学习可以用于检测异常行为，及时发现并应对潜在的安全威胁。通过集成多种先进技术，构建智能化的安全防护体系，不仅能提高系统的安全水平，还能改善用户体验，保证业务的连续性和高效性。

2.2 有效防止电脑病毒

电脑病毒作为一种常见的网络威胁，能够迅速传播并破坏系统，导致数据丢失、系统瘫痪甚至财务损失。大数据环境下的复杂性和多样性使得病毒传播更加隐蔽和迅速，传统的防护手段已难以应对。因此，强化信息安全防护措施，如安装和更新防病毒软件、实施网络隔离和访问控制，成为保护系统免受病毒侵害的关键。防病毒软件通过实时监控和定期扫描，能够及时发现并清

除潜在的病毒威胁。同时，大数据技术的发展也为病毒检测提供了新的工具，如基于机器学习的病毒识别系统，能够更准确地识别和分类新型病毒。这些技术不仅提高了检测效率，还增强了防护的全面性和及时性。

3 大数据时代计算机网络信息安全防护策略

3.1 应用生物识别技术，加强身份验证与访问控制

生物识别技术，如指纹识别、面部识别和虹膜扫描，通过独特的生物特征来验证用户身份，提供了比传统密码和令牌更为安全可靠的认证方式。这些技术不仅难以伪造，还能有效防止身份盗用和未经授权的访问。通过集成生物识别技术，组织可以实现多层次的身份验证，确保只有经过严格认证的用户才能访问敏感数据和系统资源。例如，在企业内部，员工可以通过指纹或面部识别登录系统，而外部合作伙伴则可能需要结合多种生物识别手段进行验证。这种多因素认证机制大大提高了安全性，减少了单一认证方式可能带来的风险。生物识别技术还可以与大数据分析相结合，实时监控和分析用户行为，识别异常活动并及时采取措施。通过分析用户的登录时间和地点，系统可以自动触发额外的验证步骤，确保访问行为的合法性。这种智能化的防护策略不仅提升了安全性，还优化了用户体验，使得身份验证过程更加便捷和高效[1]。

3.2 安装防火墙和杀毒软件，建造安全的交流屏障

防火墙作为网络的第一道防线，能够监控和控制进出网络的数据流，通过设定的安全规则，有效阻止未经授权的访问和恶意攻击。其强大的过滤功能可以识别并拦截潜在的威胁，确保内部网络的安全。同时，杀毒软件通过实时监测和定期扫描，能够检测和清除隐藏在系统中的病毒、恶意软件和间谍软件。其持续的更新机制确保了对新型威胁的及时响应和处理，保护数据免受恶意代码的侵害。结合防火墙和杀毒软件，可以构建一个多层次的防御体系，有效抵御各种网络攻击。防火墙负责控制网络流量，防止外部威胁进入，而杀毒软件则专注于清除内部潜在的威胁，确保系统不受病毒侵害。这种双重防护策略不仅提升了安全性，还增强了系统的可靠性，保证了数据的完整性和可用性[2]。

3.3 构建多层级协同防护机制，满足安全防护需求

多层级协同防护机制通过综合运用多种安全防护措施，形成立体化的防御体系，有效应对当前复杂的网络安全威胁。多层级防护不仅涵盖网络边界的防火墙和入侵检测系统，还包括终端安全、数据加密以及用户行为分析等环节，使安全防护更为全面和深入。在这一机制中，网络边界防护作为第一道防线，阻挡外部的潜在攻击，通过规则和策略过滤不安全的访问。这一层次与终端安全相结合，确保每个用户设备都具备必要的防护措施，如安装杀毒软件和保持系统更新，降低终端被攻击的风险。在数据层面，信息加密和数据完整性校验保证了数据传输的安全性，使敏感信息在交换过程中不易被窃取或篡改。协同防护机制还强调各个安全层级之间的协作与信息共享。通过实时监控和日志分析，系统能够及时识别异常活动并迅速响应。在发现威胁时，各层级的安全防护措施能够快速联动，共同形成有效的防堵，确保系统与数据的安全[3]。

结语

大数据背景下的计算机网络信息安全问题复杂多变，传统的安全防护手段已难以满足当前的需求。面对日益严峻的安全形势，我们必须采取更为全面和系统的防护措施，包括技术手段的升级、管理制度的完善以及人员安全意识的提升。唯有如此，才能在大数据时代充分挖掘和利用信息价值，推动社会各领域的健康、可持续发展。信息安全任重而道远，需要我们持续关注和不断努力。

参考文献

[1] 张淑红.大数据背景下的计算机信息安全及防护思路[J].网络安全技术与应用，2023，(07)：64-66.

[2] 倪瑞，梁嬿良，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.

[3] 张磊.大数据视角下计算机网络信息安全防护路径[J].数字通信世界，2023，(05)：179-181.