大数据云计算环境下的数据安全及防范策略

李欣，邹大伟，张艳鹏 *
绥化学院，黑龙江 绥化 152000

摘　　要： 随着网络技术的飞速发展和应用覆盖范围的逐步扩大，人们的生活和工作越来越依赖于网络，云计算技术也在不断进步和发展。云计算是通过虚拟化技术的应用，提升用户体验，满足更多用户需求的一项新技术。人们可以有选择地在各大网络平台上按需获取计算服务。网络云服务提供商在大数据云计算环境中为广大用户提供网络通信、服务器存储、数据计算、应用分析等功能，所有用户提供的数据共同构成大数据，所有数据管理都在网络云环境中完成。云计算技术一方面提供了更多通信便利，另一方面也带来了各种新安全问题。云安全的两大安全风险和威胁是数据泄露和数据丢失，一个可能导致机密文件泄露，另一个可能破坏数据完整性。

关 键 词： 大数据；云计算；数据安全；防范策略

Data Security and Prevention Strategy in Big Data Cloud Computing Environment

Li Xin, Zou Dawei, Zhang Yanpeng *
Suihua University, Suihua, Heilongjiang 152000

Abstract: With the rapid development of network technology and the gradual expansion of application coverage, people's life and work are increasingly dependent on the network, and cloud computing technology is also constantly improving and developing. Cloud computing is a new technology to improve user experience and meet the needs of more users through the application of virtualization technology. People can selectively obtain computing services on demand on major network platforms. Network cloud service providers provide users with network communication, server storage, data computing, application analysis and other functions in the big data cloud computing environment. The data provided by all users together constitute big data, and all data management is completed in the network cloud environment. On the one hand, cloud computing technology provides more communication convenience, on the other hand, it also brings a variety of new security issues. The two major security risks and threats of cloud security are data leakage and data loss. One may lead to the disclosure of confidential files, and the other may damage data integrity.

Keywords: big data; cloud computing; data security; prevention strategies

一、大数据云计算网络环境的概述

（一）云计算的定义与发展

云计算，即通过互联网提供计算资源和服务的一种模式，其核心理念是将计算资源如处理能力、存储空间等作为按需服务提供给用户。云计算的出现和普及源自信息技术的发展和应用需求的推动。20世纪60年代，John McCarthy最早提出“计算也将成为公众需要的产品”的设想[2]。进入21世纪，随着互联网和虚拟化技术的成熟，云计算逐渐成为现实。

云计算的发展大致经历了三个阶段：初始阶段是简单的应用托管服务和虚拟化资源的提供；中期阶段引入了弹性计算和大规模分布式计算，基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）等服务模式逐渐成型；当前阶段云计算趋向智能化和生态系统化，融合了人工智能（AI）、大数据分析和物联网（IoT）技术，通过智能云服务推动产业升级和业务创新。如今，云计算已成为信息技术的核心组成部分，广泛应用于各行各业，从提供基础设施的AWS、Azure，到专注于SaaS的Salesforce等平台，云计算的潜力和影响力不断扩大，推动了数字经济的蓬勃发展[1]。

（二）大数据的特性与价值

大数据具有体量巨大、类型多样、增长迅速、价值密度低等特点，传统的数据处理技术难以应对如此庞大的数据规模和复杂

课题来源：黑龙江省高校基本科研业务费
课题名称：基于云计算的电子信息产业数据服务优化研究
课题编号：YWF10236240126

作者简介：
李欣（1981.07-），男，汉族，黑龙江省绥化市，本科，绥化学院讲师，研究方向：网络工程、通信工程、物联网；
邹大伟（1979.08-），男，汉族，黑龙江省绥化市，硕士，绥化学院讲师，研究方向：机器学习理论与应用研究；
通讯作者：张艳鹏（1979.03-），男，汉族，黑龙江省绥化市，工学博士，绥化学院副教授，研究方向：混沌保密通信、人工神经网络、机器学习。

性。大数据的特性为数据分析和处理提出了新的技术挑战，但也带来了极大的应用价值。在众多数据的储存、筹划和研究之中，造就了富有吸引力的信息以及知识，刺激了商业智能、科学勘探、公共治理等领域的进步。更是在云计算的背景下，分布式存储与并行计算的技术，使得大数据的处理更加迅速且灵巧，为依赖数据的决策提供实质的支撑。大数据之所以有其价值，便是因其可通过分析挖掘，发现隐藏在数据中的走向和关联，为各个行业的创新与发展提供一股新的活力[2]。

（三）大数据云计算网络环境的特点

谈及大数据云计算网络环境，其优点之一是高度可扩展性，可应对高并发处理，并有资源弹性分配的能力。凭借分布式计算及存储架构，对海量数据进行快捷高效的处理近在眼前。另外，将虚拟化技术运用到实际中，硬件资源的利用率及其之大不言而喻，保证资源的安全共享，实现多租户互不干扰。在云计算环境下，高速读取和存储数据轻而易举，有力的实时数据分析及处理能力，且能迅速响应用户需求。冗余数据和备份制度确保了数据的高可用性和可靠性，使得系统更为稳固，灾难应对能力大大提升[3]。

二、大数据云计算网络环境中的数据安全问题

（一）数据安全的核心要素

数据安全的核心要素在大数据云计算网络环境中至关重要。数据安全性是首要要素，突出在面临恶意攻击或硬件问题等恶劣状况下，系统应确保合法使用者能访问数据资源。数据完整性意在守护传输与储存过程中的数据，应免受非法更改，确认的是数据的真实性及准确度。而讲究数据保密性、确保敏感信息的安全不受损害，未得授权的使用者不能窥视或透露敏感数据。在强调数据隐私保护的同时，应尊重数据中个人隐私信息，在运用数据的过程中，不应侵害数据主体的隐私权。将这些核心元素拧在手心中，数据安全在复杂的大数据云计算网络环境里，能有效对抗各类安全威胁，提高系统的整体稳定性及可靠性[4]。

（二）大数据云计算网络环境下的数据安全挑战

大数据云计算网络环境下的数据安全面临诸多挑战。数据的安全性是首要关注点之一，云环境中的数据存储和传输过程中，不易遭受未授权访问和数据窃取。数据的可用性同样关键，系统故障、网络攻击可能导致数据服务中断，影响用户对数据的正常使用。数据完整性是保证数据不受非授权篡改的重要因素，但在云计算环境下，数据完整性受到恶意攻击和操作失误的威胁。数据保密性也备受关注，云计算涉及多个租户，数据保密性失守可能导致租户数据泄露，从而引发财务、隐私等重大风险。数据隐私保护面临新挑战，数据在多个节点间传递和存储，容易被无关人员访问和使用，隐私泄漏风险增加。这些挑战对数据安全提出了更高的要求，必须在提升数据保护技术和策略上不断创新，以确保大数据云计算环境的安全性。

（三）数据安全事件案例分析与反思

在大数据云计算网络环境中，数据安全事件频繁发生，并带来了严重的后果。某全球知名的云服务提供商曾遭遇大规模的数据泄露事件，数百万用户的敏感信息被非法获取。分析显示，数据未加密存储、访问控制机制不健全以及内部人员操作失误是造成此次事件的主要原因。另一案例是某社交媒体平台的数据泄露事件，黑客通过渗透攻击并利用系统漏洞，成功获取了大量用户的个人信息。此次事件暴露了网络防御体系的脆弱性以及数据加密机制的不足。这些案例表明，数据安全问题不仅源自外部攻击，还涉及内部管理和技术措施的全面性。在探讨这些事件的过程中，反思发现：增强数据加密、完善访问控制、加大内部监控力度，以及加强系统漏洞的检测和修补是提升数据安全的关键措施。上述教训对今后大数据云计算环境中的数据安全防护具有重要的指导意义，需引起足够的重视并采取相应措施加以防范[5]。

三、保障大数据云计算环境下数据安全的对策

（一）数据加密

选择合适的数据加密算法对敏感数据进行加密。常见的加密算法包括对称加密算法和非对称加密算法。对称加密算法使用相同的密钥进行加密和解密，可以提供较高的加密速度和效率。非对称加密算法使用公钥和私钥进行加密和解密，提供了更高的安全性。根据实际需求和安全要求选择适合的加密算法。对于对称加密算法，密钥的安全性至关重要。

采用合理的密钥管理策略，包括生成强密钥、安全存储密钥以及定期更换密钥等措施。对于非对称加密算法，需要安全地管理公钥和私钥，确保私钥的机密性。密钥管理是保证数据加密的基础，需要严格控制密钥的访问和使用权限[6]。

在数据传输过程中，采用端到端加密的方式保护数据的安全。端到端加密是指在数据发送端对数据进行加密，然后在接收端对数据进行解密，中间环节都不会解密或访问数据的明文内容。这样即使在云计算环境中，也能够保护数据的机密性，防止数据被窃取或篡改。

（二）数据验证与日志审计

确保数据在传输或存储过程中没有被篡改或损坏。可以使用散列算法（如 MD5、SHA）计算数据的哈希值，并在传输或存储后验证哈希值是否一致，以确保数据的完整性。确保多个副本或分布式系统中的数据保持一致。可以使用一致性哈希算法或分布式事务管理机制来实现数据的一致性验证。确保数据的内容和格式是正确的。可以使用数据模式验证或规则引擎来检查数据的正确性，例如检查数据类型、范围、格式、约束条件等[7]。记录和监控用户对数据的访问和操作行为。可以记录用户的身份信息、访问时间、访问路径、操作类型等，并建立审计日志用于追踪审计数据的访问和修改情况。记录和监控系统的关键事件和异常行为，如系统启动、配置更改、错误日志、安全事件等[8]。

可以使用日志管理工具收集和分析系统日志，及时检测和响应潜在的安全威胁。通过设置实时警报和监控机制，及时发现并响应异常数据访问行为或系统事件。可以使用入侵检测系统（IDS）、入侵防御系统（IPS）等安全设备来实现实时警报和

监控。

（三）使用安全传输协议

首先，使用HTTPS协议是一项重要且常见的安全传输协议。HTTPS通过建立加密通道，保护数据在传输过程中的机密性和完整性。其采用SSL/TLS协议进行数据加密，同时还提供数字证书验证来确保服务器身份的合法性[9]。

其次，SSH协议也是一种常用的安全传输协议。其主要应用于远程登录和文件传输，通过加密通信和身份验证来确保数据的安全传输。SSH协议是一个安全的传输协议，可以有效防止中间人攻击和数据被篡改的风险。使用VPN协议也是一种重要的安全传输方法。VPN建立了一个加密隧道，通过在公共网络上传输数据时加密数据包，确保数据在传输过程中的隐私和安全。其可以有效地保护云计算环境中数据的机密性和完整性[10]。

（四）数据备份和灾难恢复

制定合适的备份策略非常重要。这包括决定备份频率、备份内容、备份介质、备份存储位置等。根据数据重要性和业务需求，可以选择完全备份、增量备份或差异备份等备份方法。按照备份策略，定期进行数据备份是必要的。可以使用自动化工具或脚本来执行备份操作，并确保备份的数据完整性、一致性和可恢复性。

重要的数据可以进行多重备份，将备份数据存储在不同的地理位置或存储介质中。这样可以提高数据的可靠性和安全性，在发生灾难时有备份可用。备份数据应存储在安全的位置，能够防止未经授权的访问和物理损坏。

可以考虑使用加密技术来保护备份数据的机密性，以防止数据泄露。定期测试和验证备份数据的完整性和可恢复性非常重要。通过还原备份数据或模拟灾难恢复过程进行测试，确保备份数据的可用性和有效性。制定灾难恢复计划是必要的，包括定义灾难的类型和级别、确定恢复目标和时间、指定责任人和恢复流程等。

四、结语

总而言之，云计算服务数据安全防范措施是用户保护个人信息和私人数据的重要手段。云服务提供商也需要保证平台安全，数据的存储和传输有安全保障，为数据访问的合法性奠定基础，从而有效防范各种恶意攻击。因此，云计算服务商必须高度重视云计算服务中的数据安全问题，在了解云计算服务中的数据安全威胁的基础上，积极探索优化数据安全性和更强大防护的方法，尽可能保证云数据的完整性和真实性，为广大用户提供稳定、高效、真实的通信服务。

参考文献

[1]李小聪. 基于大数据云计算网络环境的数据安全问题研究［J］. 网络安全技术与应用，2024,(08):60-61.

[2]邓浩. 解析大数据云计算网络环境的数据安全问题［J］. 通信电源技术，2023,40(06):208-210.

[3]蒋冬冬，孙允恒. 基于大数据云计算网络环境的数据安全问题研究［J］. 通信与信息技术，2023(05):79-82.

[4]冯俙瑀. 云计算环境下的网络安全防护技术发展与应用［J］. 信息与电脑（理论版），2024,36(04):7-9.

[5]程嘉，冒鹏鹏. 云计算环境下网络信息安全技术研究［J］. 无线互联科技，2023,20(14):161-164.

[6]王冰兰，刘洋. 大数据云计算环境下的数据安全探讨［J］. 网络安全技术与应用，2022,(12):42-43.

[7]陈秉乾，周强，刘欣. 云计算时代安全问题探究［J］. 天津科技，2024,51(09):8-11.

[8]刘国强. 云计算背景下数据传输安全优化研究［J］. 兰州职业技术学院学报，2024,40(05):88-92.

[9]王建伟. 云计算时代网络安全技术应用实现及策略［J］. 信息与电脑（理论版），2024,36(17):139-141.

[10]周进学. 云计算技术在网络安全中的应用探析［J］. 软件，2024,45(08):172-174.