

数据环境下云存储数据安全探讨

郭鹏飞

中华通信系统有限责任公司河北分公司 河北 石家庄 050000

摘要: 云存储作为数据环境下的重要存储方式,正面临着数据安全的多重挑战。公有云存储和内部云存储虽各具优势,但数据保密性与完整性、身份认证与访问控制等方面的问题日益凸显。为保障云存储数据安全,需采取一系列策略,包括加强数据加密与密钥管理、完善身份认证与访问控制机制,以及提升数据备份与恢复能力。这些措施共同构成了云存储数据安全防护的坚实屏障。

关键词: 数据环境;云存储;数据安全

引言

随着信息技术的飞速发展,云存储已成为数据环境下不可或缺的存储方式。公有云存储以其灵活性和可扩展性受到广泛关注,而内部云存储则更注重数据的安全性和可控性。然而,在享受云存储带来的便利的同时,我们也必须正视其数据安全方面的挑战。数据保密性与完整性、身份认证与访问控制等问题,已成为制约云存储进一步发展的关键因素。

1 云存储概述

1.1 公有云存储

公有云存储作为云计算领域的重要组成部分,近年来得到了广泛的关注和应用,在这一领域中,亚马逊和Nutanix是率先采用并提供公共云存储服务的先驱之一。亚马逊凭借其先进的云存储技术,成功与全球范围内的分销商构建了稳定且高效的数据共享与交付平台。该平台不仅提升了数据处理的效率,还允许供应商为每位客户量身定制独立的私有存储服务,从而确保了数据的安全性和隐私性。在个人云存储领域,Dropbox无疑是公有云存储技术的先行者和佼佼者,作为该领域的代表企业,Dropbox不仅率先将其云数据存储产品推向市场,还通过不断创新和优化,为用户提供了便捷、高效的云存储解决方案。Dropbox的成功不仅在于其技术的领先性,更在于其对用户需求的深刻理解和精准把握。尽管中国在云数据存储领域的发展起步较晚,但近年来却展现出了惊人的发展速度和潜力,随着云计算技术的不断普及和应用,中国市场上涌现出了一批优秀的公有云存储软件,如百度网盘、乐视网盘、金山快盘、坚果云和微云等。这些软件不仅提供了丰富的存储功能和便捷的操作体验,还通过不断优化和升级,满足了用户日益多样化的存储需求。公有云存储技术已经成为当前云计算领域的重要发展方向之一,随着技术的不断进步和应用场景

的不断拓展,公有云存储将在未来发挥更加重要的作用,为用户提供更加高效、便捷、安全的云存储解决方案。

1.2 内部云存储

内部云存储,作为一种专为企业或组织设计的云数据共享解决方案,相较于公有云存储,展现出了其独特的优势,它以安全办公私有云、联想网盘等先进产品为代表,致力于满足企业对数据安全与高效管理的双重需求,这类云存储技术代表了当前云存储领域的最前沿发展。它巧妙地依托公有云平台,通过设立不同权限级别的账号体系,实现了公有云与私有云之间的无缝融合,这种融合不仅提升了数据存储的灵活性,还为企业提供了更为精细化的数据管理手段。在实际应用中,企业可以根据自身的业务需求,灵活地使用不同权限级别的帐户,通过这种方式,企业可以将公有云上的部分存储容量划分为私有云区域,从而确保敏感数据的安全隔离。这种划分还使得企业能够为不同的部门或团队设置不同的数据使用权限,进一步提升了数据管理的精细度和安全性。内部云存储技术的引入,不仅提升了企业数据存储的效率和安全性,还为企业提供了更为便捷的数据共享和协作方式。它使得企业能够充分利用公有云的资源优势和私有云的安全优势,实现数据的灵活管理和高效利用。内部云存储技术已成为当前企业信息化建设中的重要组成部分,为企业的发展提供了有力的支撑。

2 数据环境下云存储数据安全现状分析

2.1 数据保密性与完整性挑战

在大数据环境下,云存储的数据保密性与完整性确实面临着复杂且多维度的挑战。第一,云存储服务供应商作为数据的托管方,其权限和职责的界定往往模糊不清,这为用户数据的隐私保护带来了潜在风险。具体而言,供应商可能出于各种目的,如数据分析、商业利益或法律合规等,而查询用户存储的数据。用户往往难

以有效监控和约束供应商的行为,从而无法确保数据不会被擅自读取或滥用,这无疑增加了数据隐私泄露的风险。第二,云存储的数据传输和存储过程高度依赖于互联网,而网络环境本身的安全威胁不容忽视。服务中断、数据破坏、信息被窃取和篡改等安全事件时有发生,这些都会对云存储中数据的安全性构成严重威胁。特别是在数据传输过程中,由于数据需要在多个节点间进行传输和交换,因此更容易成为攻击者的目标。第三,云存储系统自身的特点也增加了数据保护的难度,例如,安全域的划分在云存储环境中往往难以有效实施,不同用户的数据可能存储在同一个物理节点上,这增加了数据泄露的风险。云存储系统的分布式架构也使得数据的备份和恢复变得更加复杂,进一步影响了数据的完整性和可用性。因此,如何确保数据的机密性、完整性和可用性,成为云存储数据安全领域亟待解决的重要课题。这要求我们在技术层面不断创新和完善,如采用加密技术、访问控制机制、数据完整性校验等手段,以提高云存储数据的安全性。也需要加强法律法规的制定和执行,明确云存储服务供应商的责任和义务,为用户数据的隐私保护提供更加有力的法律保障^[1]。

2.2 身份认证与访问控制漏洞

身份认证与访问控制作为云数据安全防护体系的核心策略,其重要性不言而喻。在实际应用中,这些机制却存在着诸多不容忽视的漏洞。身份认证机制若未能达到足够的严密程度,将可能导致未经授权的用户轻易绕过安全防线,进而访问到敏感数据。这种情况的发生,往往源于认证方式的单一性、密码策略的宽松或身份凭证管理不善等原因。访问控制策略的制定与实施同样至关重要。若策略设定不合理,将可能出现权限划分不清、角色定义模糊等问题,进而引发水平越权、垂直越权等漏洞。水平越权使得攻击者能够访问到与自己相同权限但无权访问的其他用户的资源;而垂直越权则允许攻击者突破权限层级,访问或修改更高权限级别的资源。这些漏洞的存在,无疑为攻击者提供了可乘之机。目录遍历漏洞也是身份认证与访问控制领域的一大威胁,攻击者利用此漏洞,可以绕过正常的访问控制机制,直接访问服务器上的任意文件。这不仅可能导致敏感数据的泄露,还可能为攻击者提供进一步入侵系统的机会。目录遍历漏洞的成因多样,可能涉及输入验证不足、路径解析错误或文件访问权限设置不当等,为了有效防范数据泄露等安全风险,我们必须加强身份认证机制的严格性和访问控制策略的合理性。具体而言,应采用多因素认证、定期更换密码、强化身份凭证管理等措

施来完善身份认证机制;应明确权限划分、细化角色定义、加强访问日志审计等,以构建更加严密的访问控制体系。

2.3 数据备份与恢复能力

数据备份与恢复能力在云存储数据安全体系中扮演着至关重要的角色,在大数据环境下,这一能力面临着前所未有的挑战,随着数据量的快速增长,备份过程变得愈发耗时且资源密集。传统的备份方式已难以满足高效、全面的需求,而频繁的全量备份又会导致存储资源的极大浪费。因此,如何在保证数据完整性的同时,实现备份过程的高效性和灵活性,成为了一个亟待解决的问题。备份数据的完整性和可用性验证也是一大难题,若未能定期对备份数据进行检查,确保其未受到损坏或篡改,那么在关键时刻进行恢复时,可能会遇到无法顺利读取或恢复的情况。这不仅会导致数据丢失的风险增加,还可能对业务的连续性和稳定性造成严重影响。建立多层次、高效的备份与恢复机制显得尤为重要。第一,应采用增量备份、差异备份等高效备份方式,以减少备份过程中的资源消耗和时间成本。第二,应建立完善的备份数据验证机制,定期对备份数据进行完整性和可用性检查,确保其能够在需要时顺利恢复。还应考虑备份数据的异地存储和容灾备份策略,以提高数据的安全性和可靠性。数据备份与恢复能力是云存储数据安全不可或缺的一环,只有建立高效、可靠的备份与恢复机制,才能确保关键数据在遭受攻击或意外丢失后能够及时恢复,从而保障业务的连续性和稳定性^[2]。

3 数据环境下云存储数据安全策略

3.1 加强数据加密与密钥管理

在大数据环境下,加强数据加密与密钥管理对于确保云存储数据的安全性至关重要,具体策略可细化为以下几点:(1)采用先进的加密算法对数据进行加密处理。这是保障数据安全的第一道防线。通过应用如AES、RSA等高强度加密算法,可以对存储在云端的数据进行加密,确保数据在传输和存储过程中的保密性。即使数据被非法获取,未经授权的用户也无法轻易读取或利用这些数据,从而有效防止数据泄露和滥用。(2)建立严格的密钥管理制度,覆盖密钥的全生命周期。密钥的生成、存储、分发、更新和撤销等环节均需遵循严格的安全规范。例如,可以使用硬件安全模块(HSM)或密钥管理服务(KMS)来安全地存储和管理密钥,防止密钥被未经授权的访问或泄露。应定期更新密钥,以降低密钥被破解的风险,确保数据的安全性始终保持在较高水平。(3)推动同态加密技术的发展与应用。同态加密技

术允许在不解密数据的情况下对数据进行计算和分析,这为解决大数据处理中的隐私保护问题提供了新的思路。通过应用同态加密技术,可以在保护数据隐私的同时,实现高效的数据处理和分析,进一步提高数据处理的安全性和效率。这一技术的发展和运用,将为大数据环境下的数据安全提供更加全面和有效的保障^[3]。

3.2 完善身份认证与访问控制机制

在云存储数据安全治理中,完善身份认证与访问控制机制是不可或缺的环节,其具体措施可概述为以下三个方面:(1)构建严格的身份认证机制是基础。为了确保用户身份的真实性和可靠性,应采用多因素身份验证技术。这不仅包括传统的密码验证,还应引入指纹、面部识别、令牌等生物特征或物理凭证,形成多层次的认证体系。这样的设计能够大幅增加非法入侵的难度,有效防止身份冒用和数据泄露的风险。(2)实施基于角色的访问控制策略是关键。根据用户在组织中的角色和职责,为其分配相应的访问权限,确保用户仅能访问其工作所需的数据资源。这种权限分配机制能够避免越权访问和数据泄露的情况发生,同时提高数据使用的合规性和效率。通过持续监控和定期审计访问控制策略的合理性和有效性,可以及时发现并纠正潜在的安全漏洞和异常行为。(3)利用单点登录和身份提供者技术提升整体安全性。单点登录技术允许用户通过一次身份验证即可访问多个应用或服务,降低了用户密码管理的复杂性,同时提高了系统的安全性。身份提供者技术则能够集中管理用户身份和访问权限,实现跨系统、跨平台的身份认证和访问控制,进一步降低数据泄露的风险,同时提升用户体验的便捷性。

3.3 提升数据备份与恢复能力

在云存储数据安全治理领域,提升数据备份与恢复能力是一项至关重要的策略,具体可从以下几个方面着手:(1)科学规划备份频率与方式。根据数据的重要性和变动频率,制定合理的备份策略,例如,对于频繁变动的业务数据,可采用每日增量备份的方式,以减少备份数据量并提高效率;而对于相对稳定的系统数据,则

可每周进行一次完整备份。应结合使用多种备份方式,如全量备份、增量备份和差异备份,在保证数据安全性的前提下,提升数据恢复的效率。(2)构建异地备份机制以增强数据容错能力。为避免自然灾害或区域性故障对数据造成毁灭性打击,应将数据备份存储在与主要数据中心相隔较远的地理位置。这种异地备份机制能够确保在灾难发生时,仍有可用的数据副本可供恢复,从而最大限度地减少数据丢失的风险。(3)强化备份数据验证与测试流程。定期对备份数据进行完整性校验和恢复测试,是确保备份数据可用性的关键步骤。通过这一流程,可以及时发现并修复备份数据中的潜在问题,避免因备份数据损坏或不可用而导致的恢复失败。在灾难或数据丢失事件发生时,应迅速启动恢复流程,并根据业务需求和数据的重要性,制定合理的恢复优先级,确保关键业务能够尽快恢复正常运行。采用先进的备份与恢复技术,如快照技术、重复数据删除技术和云备份解决方案等,可以进一步提升数据备份与恢复的效率和可靠性^[4]。

结语

综上所述,数据环境下的云存储数据安全是一个复杂而重要的问题。通过加强数据加密与密钥管理、完善身份认证与访问控制机制,以及提升数据备份与恢复能力,我们可以有效地应对云存储数据安全面临的挑战。未来,随着技术的不断进步和应用的深入拓展,云存储数据安全防护体系将更加完善,为数据的存储和传输提供更加坚实的保障。

参考文献

- [1]马秀秀.大数据环境下云存储数据安全探讨[J].中国设备工程,2022(6):39-40.
- [2]王少泓,彭俊利.云存储数据安全技术研究[J].网络安全技术与应用,2023(6):69-72.
- [3]李瑞青,平措措姆.大数据环境下云存储数据安全探析[J].数字技术与应用,2023,41(6):228-230.
- [4]李艳红.大数据背景下云存储数据安全研究[J].网络安全技术与应用,2022(9):70-71.