基于云计算的中小企业数据管理与安全策略分析

张宇峰

网思科技股份有限公司　江苏苏州

【摘要】随着云计算技术的快速发展，中小企业纷纷将其作为提升数据管理效率的重要手段。数据安全问题也随之凸显。本文深入分析了基于云计算的中小企业数据管理现状，探讨了数据安全面临的威胁，并提出了针对性的安全策略。通过研究发现，合理的数据分类、加密技术的应用以及严格的访问控制是保障数据安全的关键。研究旨在为中小企业在云计算环境下优化数据管理与安全防护提供参考，促进其数字化转型的稳健发展。

【关键词】云计算；中小企业；数据管理；数据安全；安全策略

【收稿日期】2025 年 3 月 5 日　　【出刊日期】2025 年 4 月 6 日　　【DOI】10.12208/j.jer.20250154

Data management and security strategy analysis of SMES based on cloud computing

Yufeng Zhang

Wangsi Technology Co., Ltd, Suzhou, Jiangsu

【**Abstract**】With the rapid development of cloud computing technology, small and medium-sized enterprises have taken it as an important means to improve the efficiency of data management. However, data security issues have also highlighted. This paper deeply analyzes the current situation of data management of small and medium-sized enterprises based on cloud computing, discusses the threats of data security, and puts forward targeted security strategies. It is found that reasonable data classification, the application of encryption technology and strict access control are the key to ensure data security. The research aims to provide reference for small and medium-sized enterprises to optimize data management and security protection in the cloud computing environment, and promote the steady development of their digital transformation.

【**Keywords**】Cloud computing; Small and medium-sized enterprises; Data management; Data security; Security strategy

引言

在数字化时代，中小企业面临着海量数据的管理和安全挑战。云计算技术以其灵活性和成本效益成为中小企业数据管理的首选。数据泄露、恶意攻击等安全威胁频发，严重影响企业运营。研究基于云计算的中小企业数据管理与安全策略具有重要意义，旨在探索如何在充分利用云计算优势的保障数据的安全性和完整性。

1 中小企业数据管理现状

在云计算环境下，中小企业数据管理呈现出复杂多样的特点。云计算平台以其强大的存储和计算能力为中小企业带来了前所未有的便利。通过云服务，企业能够快速获取海量的存储空间，满足日益增长的数据存储需求，同时借助云计算的高性能计算资源，中小企业可以高效地处理和分析复杂的数据集，从而更好地支持业务决策和创新。这种高效的数据处理能力为中小企业在市场竞争中赢得了时间和优势，使其能够更灵活地应对市场变化和客户需求[1]。数据管理的另一面也带来了诸多挑战。数据的分散存储和动态管理使得数据一致性难以保证。在云计算环境中，数据可能分布在多个服务器和数据中心，不同节点之间的数据同步和更新需要精确的协调机制。

数据的动态变化要求企业能够实时监控和管理数据状态，以确保数据的准确性和完整性。这种复杂的数据管理需求对中小企业来说是一个巨大的考验，尤其是在缺乏专业技术和管理经验的情况下。数据备份与恢复也是中小企业亟待解决的问题。在云计算环境下，数据丢失或损坏的风险依然存在，无论是由于硬件故

作者简介：张宇峰（1989-）男，汉，江苏苏州，本科，研究方向为信息技术应用与管理。

障、软件漏洞还是人为错误，都可能导致数据不可用。中小企业需要建立完善的备份策略，确保数据在发生意外时能够快速恢复，以减少业务中断带来的损失。中小企业在数据管理过程中还面临着技术和管理方面的双重困境。一方面，中小企业往往缺乏专业的技术人才。数据管理涉及复杂的云计算技术、网络安全知识以及数据分析技能，而中小企业通常难以吸引和留住具备这些专业技能的人才。

这使得企业在数据管理的各个环节，如数据架构设计、安全防护措施实施以及数据分析应用等方面，都可能面临技术瓶颈。另一方面，中小企业往往缺乏完善的管理制度。数据管理需要明确的流程、规范的操作和严格的监督机制，但中小企业可能由于规模较小、管理经验不足等原因，未能建立起完善的制度体系。这导致数据管理的随意性较大，数据安全和合规性难以保障。在数据访问权限管理方面，如果没有严格的制度约束，可能会出现数据泄露或滥用的风险。在数据备份与恢复的执行过程中，缺乏制度保障可能导致备份工作的不规范和不及时，进而影响数据恢复的效果[2]。这些技术和管理方面的不足进一步加剧了中小企业在云计算环境下数据管理的复杂性，使得企业在享受云计算带来的便利的也面临着较高的数据管理风险。

2 数据安全面临的威胁

在云计算环境下，中小企业数据安全面临着诸多复杂且严峻的威胁。外部攻击者往往将云平台作为攻击目标，利用其潜在的安全漏洞，试图窃取或篡改企业数据。云平台的开放性和广泛的用户基础使其成为网络攻击的热点区域。攻击者可能通过恶意软件、钓鱼攻击或其他网络攻击手段，突破云平台的防护机制，获取企业存储在云端的敏感信息。一些攻击者可能会利用云平台的配置错误或软件漏洞，绕过安全防护措施，直接访问企业的数据存储区域，从而导致数据泄露或被篡改。这种外部攻击不仅会对企业的商业机密和客户信息造成严重损害，还可能导致企业在市场竞争中处于劣势地位，甚至面临法律诉讼和声誉损失的风险。

内部人员的不当操作或恶意行为也是导致数据泄露的重要因素。在中小企业中，员工可能由于缺乏足够的安全意识或培训，误操作删除或泄露数据，或者在使用云平台时违反安全规定，将敏感数据共享给未经授权的人员。更严重的是，内部人员可能出于个人利益或恶意动机，故意窃取企业数据并将其出售给竞争对手或第三方。由于内部人员通常具有合法的访问权限，他们的行为往往更难以被发现和防范[3]。中小企业在管理和监督内部人员操作方面可能缺乏完善的机制，进一步增加了数据泄露的风险。一些员工可能会在个人设备上存储企业数据，而这些设备可能没有足够的安全防护措施，容易被外部攻击者入侵，从而导致数据泄露。

云计算平台的多租户架构也给数据安全带来了新的挑战。在多租户环境中，多个企业共享同一云计算基础设施，这使得数据隔离成为关键问题。如果云平台的数据隔离机制失效，不同企业之间的数据可能会相互干扰或被错误地共享。一个企业的数据可能会被错误地存储在另一个企业的存储空间中，或者一个企业的应用程序可能会意外访问到其他企业的数据。这种数据混淆不仅会导致数据的混乱和不可用，还可能引发严重的隐私和安全问题[4]。数据在传输和存储过程中的加密不足也是数据安全的重要隐患。许多中小企业可能没有意识到加密的重要性，或者由于成本和技术限制，未能对数据进行充分的加密处理。未加密的数据在传输过程中容易被截获或篡改，而在存储过程中也可能被未经授权的人员访问。加强数据加密措施，确保数据在传输和存储过程中的安全性，是中小企业在云计算环境下必须重视的问题。

3 数据安全管理策略

在云计算环境下，中小企业面临着多种数据安全威胁，因此必须采取综合性的数据安全管理策略。数据分类管理是基础且关键的一步。中小企业应根据数据的重要性和敏感性，将其划分为不同等级。核心业务数据、客户个人信息等属于高敏感性数据，需要制定最为严格的安全策略；而一些公开信息或低价值数据则可以采用相对宽松的管理措施[5]。通过这种分类方式，企业能够更精准地分配安全资源，确保关键数据得到重点保护。数据分类也有助于明确数据的使用权限和存储方式，从而提高整体数据管理的效率和安全性。

加密技术是保障数据保密性的核心手段。在云计算环境中，数据在传输和存储过程中都可能面临被窃取或篡改的风险。中小企业必须采用先进的加密算法，对数据进行全程加密处理[6]。在数据传输过程中，可以使用 SSL/TLS 等加密协议，确保数据在互联网上的安全传输；而在数据存储时，应采用对称或非对称加密技术，对数据进行加密后再存储到云平台。企业还需要定期更新加密密钥，防止密钥被破解而导致数据泄露。

访问控制机制和数据备份与恢复策略是数据安全管理的重要保障。建立严格的访问控制机制，能够有效限制对数据的访问权限，防止未经授权的人员接触到敏感数据。企业应根据员工的职责和权限，为其分配相

应的数据访问权限，并定期审查和更新权限设置。采用多因素认证等技术，进一步增强访问控制的安全性。定期进行数据备份与恢复演练也是必不可少的。中小企业应制定详细的备份计划，定期对重要数据进行备份，并将备份数据存储在安全的位置。定期进行恢复演练，验证备份数据的完整性和可用性，确保在数据丢失或损坏时能够快速恢复业务，降低数据安全事件对企业运营的影响。

4 结论与展望

云计算技术的迅猛发展为中小企业带来了前所未有的机遇。它不仅提供了强大的计算和存储能力，还极大地降低了企业的运营成本，使得中小企业能够以较低的门槛快速实现数字化转型。通过云计算，企业可以轻松地获取和处理海量数据，从而更好地支持业务决策和创新。数据安全问题也随着云计算的广泛应用而日益凸显。数据是企业的核心资产，一旦泄露或被篡改，将给企业带来巨大的损失。中小企业必须高度重视数据安全管理，采取有效的措施来保障数据的安全性和完整性。

在云计算环境下，中小企业可以通过多种方式来提升数据安全水平。合理的数据分类是基础。企业应根据数据的敏感性、重要性和使用频率，将数据划分为不同的等级，并为每个等级制定相应的安全策略。对于涉及企业核心机密和客户隐私的高敏感数据，应采取最严格的安全措施，如加密存储、访问权限严格限制等。加密技术的应用至关重要[7]。数据在传输和存储过程中都应进行加密处理，以防止数据在传输过程中被窃取或在存储设备中被非法访问。严格的访问控制机制也是保障数据安全的关键。企业应建立完善的用户身份认证和授权体系，确保只有经过授权的人员才能访问相应的数据，并且对访问行为进行严格的审计和监控。

展望未来，云计算技术将继续保持快速发展的态势，数据管理与安全策略也需要与时俱进。随着云计算架构的不断演进和新技术的不断涌现，如人工智能、区块链等，数据安全面临的威胁将更加复杂多样[8]。中小企业必须持续关注技术发展趋势，及时调整和完善数据安全管理策略。利用人工智能技术进行安全威胁检测和预警，利用区块链技术实现数据的不可篡改和溯源等。

5 结语

云计算为中小企业提供了高效的数据管理手段，但数据安全问题亟待解决。通过合理的数据分类、加密技术的应用和严格的访问控制，中小企业能够在云计算环境中有效保障数据的安全性和完整性。未来，随着云计算技术的持续发展，数据管理与安全策略需不断优化，以应对日益复杂的安全威胁。中小企业应积极关注技术动态，灵活调整安全策略，确保在数字化转型中稳健前行，实现可持续发展。

参考文献

[1] 姜威. 基于数据中台的中小企业数据治理路径研究 [J]. 信息技术与标准化, 2024, (12): 70-75.

[2] 李文岩,刘利娜,贾学志. 基于大数据技术的中小企业项目决策辅助研究 [J]. 中小企业管理与科技, 2024, (19): 119-121.

[3] 刘瑶. 精准营销策略在中小企业本地化市场中的战略管理路径探讨 [J]. 营销界, 2024, (21): 137-139.

[4] 王鹏洋. 数字化时代中小企业市场营销管理面临的困境与对策 [J]. 中国管理信息化, 2024, 27 (22): 104-106.

[5] 梅艺川. 中小企业财务管理数字化转型路径探索 [J]. 中小企业管理与科技, 2024, (22): 185-187

[6] 张雨. 大数据背景下中小企业人力资源管理优化策略 [J]. 经营管理者, 2025, (02): 72-73.

[7] 杜峰. 算网协同提升供给 降低中小企业用算成本[N]. 通信信息报, 2025-03-12 (002).

[8] 安容蒂. 云计算视角下科技档案信息化管理策略探究 [J]. 兰台内外, 2025, (09): 32-34.