 DOI: https://doi.org/10.12349/iser.v6i8.7024

Level protection and reinforcement strategy of cloud computing platform data storage in the context of Internet security

Zhixiu Gao Jiawei Li

Jinan Sanze Information Security Evaluation Co., Ltd., Jinan, Shandong, 250101, China

Abstract

In the context of continuous digital economic development, cloud computing has become a core technological support for information system construction. However, with the constant evolution of cyber threats, data storage security issues have become increasingly prominent. As a crucial regulatory framework for China's cybersecurity, the graded protection system provides institutional basis and implementation guidelines for cloud platform security. This paper examines current internet security environments, thoroughly analyzes major risks in cloud platform data storage, outlines key requirements under the Graded Protection 2.0 standard, and explores technical strategies for data storage security reinforcement including identity authentication, access control, data encryption, and backup recovery. Research demonstrates that systematic advancement of graded protection alongside technical reinforcement constitutes an effective approach to enhance cloud platform data storage security, carrying practical significance for safeguarding cyberspace security and data sovereignty.

Keywords

cloud computing; data storage; graded protection; information security; reinforcement strategies

互联网安全背景下云计算平台数据存储的等级保护与加固策略

高志修 李佳蔚

济南三泽信息安全测评有限公司，中国 · 山东 济南 250101

摘 要

在数字经济持续发展的背景下，云计算已成为信息系统建设的核心技术支撑。然而，随着网络威胁的不断演化，数据存储安全问题愈发突出。等级保护制度作为我国网络安全监管的重要制度体系，为云平台安全防护提供了制度依据和实施框架。本文立足当前互联网安全环境，深入分析云计算平台数据存储所面临的主要风险，梳理等级保护2.0标准下的关键要求，并探讨数据存储安全加固的技术策略，包括身份鉴别、访问控制、数据加密、备份恢复等方面。研究表明，系统性等级保护建设与技术加固并行推进，是提升云平台数据存储安全水平的有效路径，对保障网络空间安全与数据主权具有现实意义。

关键词

云计算；数据存储；等级保护；信息安全；加固策略

1 引言

伴随信息技术深度渗透于社会各领域，云计算凭借弹性扩展、高可用性与资源共享优势，已成为政府、企业和科研机构普遍采用的基础架构形态。然而，云环境下数据脱离本地控制、运行环境多租户共用、安全边界模糊等特性，使得传统信息安全体系面临挑战。

近年来，针对日益严峻的网络安全问题，我国陆续颁布《网络安全法》《数据安全法》等法律法规，并于 2019 年发布《信息安全技术网络安全等级保护基本要求（GB/T 22239-2019）》，提出等级保护 2.0 标准。该标准在继承传统等级保护制度框架的基础上，扩展了对云计算、大数据、移动互联网等新兴技术形态的适配要求，为新时代信息系统安全建设提供了规范依据。

在这一背景下，如何围绕等级保护制度的核心要求，构建针对性强、执行力高的数据存储安全体系，已成为云计算平台安全防护工作的关键内容。本文以云平台数据存储为研究对象，围绕其在等级保护体系下的合规建设与技术加固问题展开系统探讨，旨在为云平台运营主体提供可行性强、适应性广的安全提升策略。

【作者简介】高志修（1998–），男，中国山东菏泽人，本科，中级网络工程师，从事网络安全研究。

2 云计算平台数据存储面临的主要安全风险

在云计算技术迅猛发展的背景下，越来越多的企业和组织选择将数据存储、处理和管理迁移至云平台，以降低 IT 成本、提升资源利用效率和增强系统弹性。然而，云计算环境下的数据安全问题也随之愈发突出，尤其是数据泄露、数据完整性和可用性风险、安全管理体系不健全等问题日益成为阻碍云计算深入应用的核心障碍。深入剖析云计算环境下的数据安全风险，对于构建健全的数据保护体系、提升企业数字化治理能力具有重要意义。

2.1 数据泄露风险频发

云计算架构具有高度开放性和资源共享性，数据通常被存储于第三方云服务提供商的基础设施中，数据在传输、存储和处理等环节面临诸多安全隐患。由于多租户共享环境下的资源隔离问题，系统一旦存在漏洞，便可能被攻击者利用实现越权访问，从而导致不同用户之间的数据泄露。例如，某租户通过边界验证绕过手段，访问本不应有权限查看的另一租户数据，进而造成敏感信息外泄。

此外，权限控制机制的不完善也是数据泄露的重要诱因。在实际运维过程中，部分云服务平台未能实施精细化的权限划分，用户权限设定过宽或存在默认账号未修改等问题，为不法分子提供了攻击入口。一旦攻击者获得管理员权限，不仅可随意访问、下载数据，甚至能控制平台操作，导致大规模泄露事件。

值得注意的是，云平台所承载的不仅是用户的日常业务数据，还包括大量涉及隐私的个人信息和企业核心资产，如财务报表、商业合同、知识产权文件等。一旦发生数据泄露事件，不仅会直接损害用户权益、引发法律纠纷和监管问责，还将对企业品牌形象与社会声誉造成难以挽回的负面影响。因此，如何在开放共享的云架构中确保数据安全，是当前亟须解决的重要问题。

2.2 数据完整性与可用性受到威胁

除了数据泄露风险，云计算环境下的数据完整性与可用性同样面临严峻挑战。数据完整性是保障数据可信性的前提，一旦数据被恶意篡改或意外损坏，将严重影响业务运行的准确性和科学性。现实中，不法分子可能通过注入恶意代码、伪造请求或利用管理员权限修改、删除关键数据，使系统产生错误决策，甚至导致业务瘫痪。例如在金融领域，篡改交易数据将直接威胁资金安全，带来重大损失。

近年来，以勒索病毒为代表的攻击方式日益猖獗。攻击者通过入侵云平台系统、加密存储在云中的重要数据，然后向用户索要赎金换取解密密钥。这类攻击不仅导致数据短期内无法使用，还可能造成长期的数据不可恢复风险，严重破坏数据可用性。

值得警惕的是，部分数据可用性问题并非源于外部攻击，而是由于平台内部运维管理不善或技术设施不完善所致。例如，服务器硬件故障、存储介质损坏、网络中断、电力异常，甚至是运维人员操作失误，均可能导致数据丢失或系统长时间无法访问。尤其是在未建立有效备份和容灾机制的云环境中，一旦发生灾难性故障，用户数据将面临永久性损毁的风险。因此，加强数据冗余备份、建立自动容灾机制和应急响应流程，是确保云计算环境下数据可用性和业务连续性的关键所在。

2.3 安全管理体系不完善

云计算数据安全问题的深层原因往往在于安全管理体系的滞后与不完善。部分云平台仍处于“以功能优先、安全滞后”的建设思路，缺乏统一、系统的安全管理制度与流程。例如，对用户权限边界缺乏精细化控制，对系统行为未实施持续监控和日志审计，导致安全事件发生后无法有效追踪和溯源。此外，安全事件处置流程不明确，导致攻击行为难以及时发现与阻断，影响了整体风险应对能力。

技术与策略的脱节也是常见问题。某些平台虽部署了防火墙、入侵检测、加密传输等技术措施，但在实际运行中未能与运维管理策略形成联动，导致系统无法动态调整防护策略，对新型攻击手段响应迟缓。此外，不同层级的安全控制策略分散、缺乏统一协调，也导致防护效果不佳。

同时，云服务提供商与用户在安全责任划分上的模糊界限，也为数据安全管理带来新挑战。在“责任共享”模式下，云服务商负责基础设施安全，用户则需自行负责应用和数据层的安全管理。但在实际操作中，部分用户错误地将全部安全责任推给服务商，忽视了自身安全配置与管理职责，从而埋下安全隐患。此外，云服务商未能为用户提供完善的安全服务选项与配置指导，也加剧了风险暴露。

3 等级保护 2.0 标准下的数据存储安全要求解析

3.1 制度背景与政策框架

等级保护制度是我国信息系统安全管理的基本制度，按照信息系统对国家安全、社会秩序、公众利益的影响程度，将信息系统划分为五个安全等级，提出相应的技术与管理要求。2019 年发布的等级保护 2.0 标准在原有框架上新增了对云计算、大数据、物联网等技术形态的适配内容，明确了等级保护对象不再局限于传统实体系统。

对于云平台而言，不论作为服务提供方或租用方，都需按系统定级开展等级保护测评与整改，确保安全控制点的全面覆盖与有效执行。特别是在数据存储方面，标准强调了数据分类分级保护、访问权限控制、传输加密、存储加密、备份与恢复、安全审计等关键控制点。

3.2 数据安全保护的基本要求

等级保护 2.0 在数据安全层面提出“分类分级、全生命周期保护”的理念。对于不同敏感等级的数据，应采取差异化保护措施，实现“重要数据重点保护”的原则。技术措施应覆盖数据生成、传输、处理、存储与销毁全过程，形成闭环式管理。

标准对数据加密存储提出明确要求，敏感数据应采用国家商用密码算法进行加密处理，同时必须配置数据完整性校验机制，以防数据篡改与伪造。对于高等级系统，还需部署专用加密机与密钥管理系统，保障加密体系安全性与可靠性。

3.3 云环境下的差异化保护策略

等级保护 2.0 对云平台特性进行了细化适配，如要求平台运营方具备虚拟化安全、资源隔离、镜像可信验证等能力，用户方则需对其租用服务的系统级别进行定级备案，并按等级要求落实数据保护措施。

此外，标准还强调云平台应具备灵活的资源动态调整能力与统一的安全策略推送机制，以应对复杂多变的网络安全威胁。

4 云平台数据存储加固的关键技术路径

4.1 强化身份认证与访问控制

云平台数据存储安全，首先要筑牢访问者身份识别这道防线。建立基于多因子认证（MFA）的用户身份验证机制是关键，可引入动态令牌、生物识别等先进手段。动态令牌能提供一次性密码，生物识别如指纹、面部识别等具有唯一性，二者结合可极大增强登录安全性，有效抵御暴力破解等攻击。

对于高敏感操作，需设置严格的行为审计与授权审批流程。通过详细记录操作行为，对异常操作及时预警，同时要求多级审批，防范内外部人员越权访问，确保数据操作在可控范围内。

在访问控制上，推行最小权限原则至关重要。基于角色（RBAC）或属性（ABAC）的访问控制模型，可实现精细化权限分配与动态调整。RBAC 根据用户角色分配权限，ABAC 则依据用户属性、资源属性等综合判断，二者都能确保每位用户仅能访问与其职责相符的最小范围资源，避免权限过度分配带来的安全风险。

4.2 完善加密与备份容灾机制

加密是保障数据存储安全的核心手段。对静态数据采用国密对称算法：SM4

等对称加密处理，可有效防止数据在存储过程中被窃取或篡改。对于传输数据，运用 SSL/TLS 等协议保障链路安全，确保数据在网络传输过程中的保密性和完整性。同时，引入哈希算法（如 HMAC-SM3）生成数据摘要，通过对比校验结果实现完整性验证，及时发现数据是否被篡改。

为保障数据可用性与业务连续性，构建多级备份体系必不可少。包括本地实时备份、异地异构备份与云端热备方案，备份数据独立加密存储，并定期进行恢复演练，验证备份文件完整性与恢复路径可行性。在容灾方面，通过主备切换、负载均衡、容器化部署等方式提升系统弹性，对关键数据节点部署 RAID 阵列、分布式存储与副本机制，提高物理层安全性与系统抗故障能力，确保云平台数据存储稳定可靠。

5 等级保护落地中的实践路径与管理机制

在技术加固之外，制度建设与流程规范同样是等级保护工作成功的关键。一方面，组织应成立安全管理委员会，明确等级保护责任人，制定信息安全管理制度与应急预案。另一方面，应通过定期安全审计、自查整改与第三方测评等手段，持续优化安全措施。

此外，还需强化人员培训与安全意识教育，确保操作人员理解等级保护政策与具体操作流程，减少因人为失误导致的安全事件。对于云平台运营商而言，还应建立与用户的安全责任边界协议，明确数据处理权限与安全服务内容。

云平台服务商可借助“安全即服务”（Security as a Service, SECaaS）模式，为客户提供包括数据加密、审计日志、异常监控等在内的托管安全服务，提升整体安全运维效率，缓解中小客户的安全建设压力。

6 结语

在互联网高速发展与数字化转型深入推进的背景下，云计算平台承载的数据类型日趋多样、数据价值日益攀升，数据存储安全问题愈加重要。等级保护 2.0 的出台为新技术环境下的信息系统安全建设提供了清晰框架和标准指引。在此基础上，针对云计算平台的特性，制定系统化的数据存储安全加固策略，是提升平台安全水平与风险应对能力的关键。

本文从风险识别、标准要求、技术路径与管理机制四个层面，系统探讨了云平台数据存储的等级保护实施逻辑与加固措施。实践证明，制度建设与技术手段协同并进，才能构建稳定、高效、合规的数据存储安全体系，为数字经济的健康发展提供坚实保障。未来，需进一步研究人工智能、区块链等新兴技术在数据安全领域的应用，持续推动安全理念与能力的协同演进。

参考文献

[1] 穆端端.提升安全配置管理能力，保障云计算基础设施算力安全[J].中国信息安全,2024,(09):83-86.

[2] 刘秋月,刘佳良.基于云计算的SecaaS发展态势研究与建议[J].网络安全技术与应用,2024,(09):84-87.

[3] 李紫赚.基于云计算的动态网络体系优化与智能路由算法研究[D].昆明理工大学,2024.

[4] 刘菁.基于技术控制能力的云计算服务提供者法律义务分类配置[D].北京化工大学,2024.

[5] 简振城.云计算行业上市企业的投资价值研究[D].广东财经大学,2024.