云计算环境下的数据安全与隐私保护问题研究

尹青伟
江苏省教育厅教育宣传中心，江苏 南京 210013

DOI: 10.61369/TACS.2026050017

摘　　要： 云计算是推动信息技术发展的动力，是企业数字化转型与信息化建设的支撑。随着云服务的广泛应用，数据安全和隐私保护问题愈发明显，制约了云计算的健康发展。本文基于云计算环境的技术架构，系统性分析当前面临的风险与挑战，并从不同维度出发，提出具有操作性的优化对策。通过加强新技术应用，促进跨行业协同与监管，有助于提高云计算环境下数据安全和隐私保护水平，为云计算可持续发展提供助力。

关 键 词： 云计算；数据安全；隐私保护

Research on Data Security and Privacy Protection Issues in Cloud Computing Environment

Yin Qingwei
Education Promotion Center, Department of Education of Jiangsu Province, Nanjing, Jiangsu 210013

Abstract: Cloud computing is a driving force for the development of information technology and a support for enterprise digital transformation and informatization construction. With the wide application of cloud services, data security and privacy protection issues have become increasingly prominent, restricting the healthy development of cloud computing. Based on the technical architecture of the cloud computing environment, this paper systematically analyzes the current risks and challenges, and puts forward operable optimization countermeasures from different dimensions. Strengthening the application of new technologies and promoting cross-industry collaboration and supervision will help improve the level of data security and privacy protection in cloud computing environments, and provide support for the sustainable development of cloud computing.

Keywords: cloud computing; data security; privacy protection

引言

新时代背景下，以云计算为代表的信息技术融入社会各领域，促进资源分配、服务模式等层面的变革。云计算具有按需服务、成本低等特征，可以促进各领域企业的信息化建设。随着云计算的普及，数据安全与隐私保护问题成为社会性议题，出现了许多云数据泄露事件。基于此，深层次分析云计算环境下数据安全和隐私保护问题，具有重要价值与意义。一方面，可以系统性识别云环境内数据生命周期各环节风险，明确技术、法律等维度挑战。另一方面，可以结合前沿技术趋势，探索可行的防护策略，促进云计算技术发展。

一、云计算环境下数据安全与隐私保护的核心风险与问题

（一）技术层面的安全漏洞与攻击威胁

云计算环境在技术上具有虚拟化、服务化等特征，可以提高工作效率，但也出现新的安全弱点。第一，虚拟化安全风险。云计算的基石是虚拟化，但虚拟层安全的突破，容易造成同一服务器上多租户虚拟机间出现数据泄露。同时，虚拟机逃逸、虚拟网络隔离等问题，很容易成为攻击者冲击的入口[1]。

第二，数据存储与传输风险。云上数据通常借助多副本、分布式的形式，存储到不同地理位置内，而数据传输可以借助公共网络或云服务商内部链路。如果出现存储加密度不足的问题，很容易造成数据的非法访问[2]。

第三，身份认证与访问控制缺陷。在云环境内用户的身份较为多样，访问场景较为复杂，传统的用户密码形式很难应对钓鱼攻击等风险。由于权限设置的宽泛、角色定义不清等问题，很容易出现越权访问或内部的恶意操作。

（二）管理层面的责任模糊与内部风险

在云计算共享责任模型下，服务商和用户需肩负安全义务，但实践过程中，存在责任边界不清，容易带来防护的漏洞。第

一，责任共担模式落地困难。虽当前主流云服务商明确了各层面安全职责，如基础设施、软件等，但用户对自身需要配置的安全选择缺乏理解，容易出现责任空白区域[3]。如用户误以为云服务商全权负责数据的加密，而实际密钥管理需要用户自行实施。

第二，内部人员威胁。其具体涉及云服务商内部员工、用户管理员等内部人员，如果出现疏忽等问题，可以借助合法权益，实施数据窃取、破坏。由于各因素的存在，如权限过于集中、操作行为缺少审计等，造成风险的进一步加剧[4]。

第三，安全运维与应急能力不足。许多组织在迁移至云平台之后，仍采取原有安全运维流程，没有针对云环境进行持续性监控、应急响应的机制，容易出现取证困难、安全事件发展滞后等问题，进一步造成安全损失扩大。

（三）合规与法律层面的隐私挑战

数据跨境流动与多元法律环境使得云计算的合规压力日益增加。第一，数据主权与跨境管辖冲突。云数据中学通常分布于全球的各国家与地区，其中数据可能在用户不知晓状况下，进行跨境传输，触及到不同司法区域的数据本地化要求，如欧盟 GDPR 等。由于法律适用和监管责任尚未明确，很容易给用户与跨国企业造成合规风险[5]。

第二，隐私保护要求升级。随着全球隐私立法的完善，对于个人信息收集、共享以及删除的全生命周期管理要求不断提升。在云计算背景下，多租户架构、数据聚合分析等实践，造成匿名化难度较大，出现隐私泄露风险，用户对于云服务商的信任遭受影响。

第三，审计与举证困境。在云环境中，用户面对底层基础设施控制能力相对有效，当出现安全事件后，往往需依赖云服务商提供日志、证据。如果服务商日志记录不完整、难解读，用户通常面临审计困难、举证不足等问题。

二、云计算环境下数据安全与隐私保护的优化策略

（一）构建全方位、多层次的安全防护体系

第一，深化纵深防御架构。根据云环境的特征，可以构建包含网络、应用等内容的立体防护。从网络层的角度出发，可以借助软件定义边界、微隔离等技术，促进细粒度访问控制的实现。从主机和容器层出发，可以加强镜像安全扫描、运行等过程的保护和漏洞管理，提升数据安全和隐私保护效果[6]。

第二，强化身份与访问管理。面对现代化信息安全防护体系的建设，可以将用户身份作为信息，开展核心安全防护，并实时最小权限原则，保障各用户、应用获取完成工作任务所需的最低访问权限。为了顺利达成该目标，可以综合使用多因素认证方式，强化身份验证可靠性，并借助单点登录提高用户体验和管理效率，适当结合自适应认证机制，结合登录环境和风险动态调整认证的要求[7]。另外，通过整合用户行为分析技术，对用户活动进行持续监控，进而智能地、动态地调整系统和数据访问权限。针对云平台管理接口、应用程序编程接口等高风险目标，可以实施较为严格的控制对策，采取基于安全令牌的短期授权机制，制定和执行精细化控制对策，保障每次访问在严密、动态的监管下，构建其良好的防御安全屏障。

第三，统一安全可视与管控。通过云安全态势管理、云工作负载保护平台等工具，可以对分布与云环境的各种资源，开展统一、高效的安全配置核查和监控，将潜在风险借助直观与可视化方式，更好的呈现出来。同时，可以搭建集合日志聚合与深度分析系统，汇聚不同云平台和地方的日志数据，并实时的识别异常行为与潜在风险，切实提高云环境安全态势感知和主动防御技能。

（二）加强安全管理，提升全员安全意识

确定并且落实责任共担模式。云服务商应该细化责任矩阵，用图示和实例的形式告知用户各自的工作职责。用户要创建云安全责任制，把内部各个部门的数据分类、配置管理、事件响应等工作职责落实到位，防止出现责任不到位的情况[8]。定期对责任模型进行对照审计，没有防护盲区。

第二，创建云原生安全运维体系。推进安全左移，将安全要求放在系统设计阶段就加以考虑。创建专门的云安全运维小组，制订云环境下事件应对方案，定时举办攻防演习。改进云服务公司同其客户之间安全合作的水平，创建事故事件汇报渠道、数据保存、联合处理等系统。

第三，推行安全意识教育的持续性。对开发、运维、业务人员等不同的角色，做有针对性的云安全培训，内容涉及安全配置实践、隐私保护要求、社会工程防范等内容。模拟钓鱼、安全知识竞赛等手段来提高培训效果，培育企业内部安全文化。

（三）推动新兴技术落地应用，提升防护能力

第一，将隐私增强技术集成起来使用。数据融合分析、联合建模这些场景中，用上隐私计算的联邦学习、差分隐私等方法，才能让数据的价值真正被发挥出来。还可以推动可信执行环境在云计算平台上创建起来，给敏感技术提供硬件级的隔离保护。

第二，以人工智能和自动化为主动防御的。利用机器学习算法来分析大量的日志、流量数据，可以快速形成用户的和实体的行为基线，从而有效地提前发出关于异常访问以及内部威胁的警报[9]。用自动化编排和响应平台把威胁响应动作进行剧本化，可以大大缩短响应时间。另外还可以从加强 AI 模型安全防护角度来防止对抗样本攻击。

第三，用区块链赋能审计和溯源。研究区块链在云数据审计和溯源中的应用，把重要操作日志、权限改变、数据访问记录等上链存证，依靠它的不可篡改、可追溯的特点来加强审计证据的可信度，给合规举证和纠纷解决赋予技术支持。

（四）加强行业协同与监管，构建良好生态

为了搭建与优化云计算领域的安全和隐私保障机制，可以从多个角度出发，进行协同促进，构建标准化的认证体系。具体来讲，可以鼓励和引导各行业协会、专业标准化组织促进工作开展，制定和发布有关云计算环境的数据安全和隐私保护评价指南[10]。同时，需要推广基于国际标准的云服务安全认证项目，并借助权威认证，方便用户识别和筛选符合安全要求的合格服务商，有效降低其在市场内的比较和选择成本。

面对行业内部及跨行业信息共享和协同应急响应技能层面，可以建设良好的云安全信息共享平台，包含多企业、跨行业。该平台还需致力于攻击指标、漏洞等安全信息的交换和高效流转。另外，需要推动构建制度化的云安全应急协同机制，保障面临大规模供应链攻击事件时，各方可以快速预警与响应，有效遏制安全威胁的拓展。

通过深化政府部门和企业的交流合作，并重视跨境监管领域的合作，有助于构建良好的生态。政府部门需持续调整适应云计算技术特征与规律的监管框架，清晰划分监管职责，并细化数据出境安全评估流程。同时，可以积极探索创新模式，在可控环境下激励安全新技术测试和应用革新。通过国际间交流、合作，可以推动数据保护规则体系的建设，为企业在全球范围开展业务提供清晰的制度保障。

三、结束语

综上所述，云计算技术的发展，可以赋能数字经济，促进社会革新，为数据安全和隐私保护带来挑战。本文分析云环境下安全风险的特点，如多层次、跨边界等，包括技术、管理等维度，更好的实现有效防护。为了应对相关挑战，需改变孤立、静态思维，积极构建体系化的治理模式。从技术层面出发，可以持续跟踪云架构的演进，促进隐私技术、AI 安全等技术的融合，构建智能弹性防御体系。随着新技术的发展，云计算环境更加复杂，数据安全和隐私保护成为需持续探究的课题。通过技术创新和管理优化的驱动，可以享受云计算红利，打牢数据安全根基，有效保护用户隐私权益。

参考文献

[1] 潘蕊 . 云计算环境下的数据加密与隐私保护技术研究 [J]. 科技与创新 ,2025,(23):113-115+118.DOI:10.15913/j.cnki.kjycx.2025.23.035.

[2] 韦宇星 , 梁荣华 , 莫瑜兴 . 云计算环境下的数据安全与隐私保护研究 [J]. 网络安全和信息化 ,2025,(08):24-26.

[3] 周在彪 . 云计算环境下的数据隐私保护策略 [J]. 数字通信世界 ,2025,(07):92-94.

[4] 梁仲峰 . 云计算环境中的数据安全与隐私保护方法 [J]. 长江信息通信 ,2025,38(06):167-169.DOI:10.20153/j.issn.2096-9759.2025.06.045.

[5] 郑建忠 . 云计算环境下的数据加密与隐私保护技术研究 [J]. 信息系统工程 ,2025,(05):40-43.

[6] 刘银山 . 云计算环境下的数据安全与隐私保护技术研究 [J]. 网络安全技术与应用 ,2025,(05):66-68.

[7] 陈永平 . 云计算环境下的多租户数据隔离与隐私保护技术研究 [J]. 中国战略新兴产业 ,2024,(33):54-56.

[8] 顾睿睿 , 覃露 . 云计算环境下的数据安全保护与隐私保护 [C]// 中国智慧工程研究会 .2024 社会发展与科技创新交流会论文集 . 广西民族大学 ; ,2024:603-605.DOI:10.26914/c.cnkihy.2024.017449.

[9] 田瑞 . 云计算环境下的数据安全与隐私保护 [J]. 电子元器件与信息技术 ,2024,8(04):163-165.DOI:10.19772/j.cnki.2096-4455.2024.4.048.

[10] 钟献坤 . 云计算环境下的数据安全与隐私保护 [J]. 数字通信世界 ,2024,(03):158-160.

