 DOI: https://doi.org/10.12349/iser.v6i8.7009

Research on Building a Cybersecurity Protection System for Data Center Cloud Environments in the Financial Industry

Xiawei Zhuang

People's Bank of China Clearing Center, Beijing, 100080, China

Abstract

With the widespread adoption of cloud computing technology in the financial sector, cybersecurity challenges in data center cloud environments have become increasingly prominent. This study systematically analyzes major security risks in cloud environments based on practical financial industry needs, proposing a comprehensive cybersecurity protection framework. The system comprises four core components: infrastructure security, data security, access control, and security management. Through multi-layered and multi-dimensional protective measures, it effectively addresses various security threats in cloud environments. Research demonstrates that this protection system significantly enhances the cybersecurity capabilities of financial industry data center cloud environments, providing reliable safeguards for financial institutions' digital transformation.

Keywords

Financial Industry; Data Center; Cloud Computing; Cybersecurity; Protection System

金融行业数据中心云环境下的网络安全防护体系构建研究

庄夏唯

中国人民银行清算总中心，中国 · 北京 100080

摘　要

随着云计算技术在金融行业的广泛应用，数据中心云环境下的网络安全问题日益突出。本文从金融行业实际需求出发，系统分析了云环境下面临的主要安全风险，提出了一套完整的网络安全防护体系构建方案。该体系包含基础设施安全、数据安全、访问控制和安全管理四个核心组成部分，通过多层次、多维度的防护措施，有效应对云环境中的各类安全威胁。研究表明，该防护体系能够显著提升金融行业数据中心云环境的安全防护能力，为金融机构的数字化转型提供可靠保障。

关键词

金融行业；数据中心；云计算；网络安全；防护体系

1 引言

近年来，金融行业数字化转型步伐不断加快，云计算技术凭借其弹性扩展、成本优化等优势，在金融行业得到广泛应用。据统计，超过 80% 的金融机构已经或正在将业务系统迁移至云平台。然而，云环境的开放性和共享特性也给金融数据安全带来了新的挑战。金融行业作为国民经济的重要支柱，其数据中心的安全直接关系到金融稳定和社会经济安全。

传统的数据中心安全防护措施难以完全适应云环境的特点。云环境中的资源共享、动态调度等特性，使得安全边界变得模糊，传统的基于边界防护的安全模型面临严峻挑战。同时，金融行业对数据安全、业务连续性等方面有着极高的要求，这进一步加大了云环境安全防护的难度。

【作者简介】庄夏唯（1994–），男，中国江苏邳州人，中级，从事网络安全研究。

2 金融云环境面临的主要安全风险

2.1 基础设施安全风险

云环境的基础设施安全是整体安全的基础。在虚拟化环境下，物理服务器的安全直接影响所有租户的安全。常见的风险包括虚拟化软件漏洞、资源隔离失效、虚拟机逃逸等。有些虚拟化平台曾曝出严重的漏洞，攻击者可以利用这些漏洞突破虚拟机的隔离机制，访问同一物理服务器上的其他虚拟机，从而窃取敏感数据或破坏系统运行。

此外，云平台的网络架构与传统网络存在显著差异，软件定义网络虽然提供了灵活的配置能力，但也带来了新的攻击面。SDN 控制器作为网络的核心管理节点，一旦被攻击，可能导致整个网络的控制权被窃取，攻击者可以随意修改网络配置，甚至发起大规模的网络攻击。

2.2 数据安全风险

数据是金融机构的核心资产，云环境下的数据安全面临诸多挑战。首先，数据在传输、存储和使用过程中都可能

面临泄露风险。例如，在数据传输过程中，如果未采用强加密协议，攻击者可能通过中间人攻击窃取敏感数据；在数据存储环节，如果加密措施不到位，存储设备丢失或被非法访问可能导致数据泄露 [1]。

多租户环境下数据隔离问题突出，云平台共享硬件资源，若数据隔离机制设计不当或云存储配置出错，不同租户数据可能被其他租户访问，造成泄露。同时，数据备份和恢复机制也影响数据安全，若备份数据未加密、策略不合理，或存储于未受保护的第三方云服务，就可能导致数据丢失、篡改，备份数据也有泄露风险。

2.3 身份认证与访问控制风险

云环境中的用户身份复杂多样，包括内部员工、合作伙伴、客户等，如何确保正确的用户以适当的方式访问特定资源是重要挑战。传统的基于 IP 的访问控制策略在动态变化的云环境中难以有效实施 [2]。例如，云环境中的虚拟机可能随时迁移，IP 地址也会随之变化，基于固定 IP 的访问控制策略将失效。

同时，权限管理不善可能导致权限滥用或特权提升等问题。员工如果被授予过高的权限，一旦其账户被攻击，攻击者可以利用这些权限进行非法操作。此外，特权账户的管理也是一个难点。特权账户通常拥有系统的最高权限，如果管理不善，可能导致系统被完全控制。

2.4 安全管理风险

云环境的安全管理面临诸多新问题。首先，责任共担模型使得安全责任划分变得复杂。在云计算环境中，安全责任通常由云服务提供商和金融机构共同承担，但具体的责任划分可能不明确，导致安全漏洞无法及时修复 [3]。

云服务快速弹性特性要求安全管理动态适配，云环境资源可随时增减，安全策略若不能及时调整，便会引发新安全漏洞。另外，多云或混合云环境下的统一安全管理也是难题，金融机构常同时采用多个云服务提供商服务，或公有云与私有云并用，怎样达成不同云环境间安全策略统一，成为亟待攻克的关键问题。

3 网络安全防护体系构建

3.1 基础设施安全防护

基础设施安全是整体防护体系的基础。在物理安全层面，需要确保云数据中心符合相关安全标准。数据中心应具备完善的物理访问控制措施，如门禁系统、视频监控等，防止未经授权的人员进入。同时，数据中心应具备冗余的电力、网络和冷却系统，确保在发生故障时能够快速恢复 [4]。

虚拟化安全上，要采用安全技术，定期更新虚拟化平台补丁，严格隔离资源，用硬件辅助虚拟化技术防虚拟机逃逸攻击，还需定期评估以修复漏洞。网络层面，部署新一代防火墙、入侵检测系统等设备，实施网络微分段，限制非必要访问。还可采用软件定义边界技术，将网络划分成多个安全区域，限定特定流量通过，降低攻击风险。

3.2 数据安全防护

数据安全防护需贯穿全生命周期。数据传输时，采用强加密协议，如 TLS 1.3 加密传输，防中间人攻击，还要定期更新加密算法与密钥。数据存储要加密，用 AES-256 算法，配合硬件安全模块严格管理密钥，即便设备丢失或被非法访问，数据也难被窃取。数据使用中，运用数据脱敏技术，如替换数据库敏感字段，降低敏感信息泄露风险。此外，要建立完善的数据备份与灾难恢复机制，采用 3-2-1 备份策略，即 3 份副本、2 种介质、1 份异地存储，且定期开展灾难恢复演练，保障数据可用性与完整性，确保灾难时能快速恢复业务。

3.3 访问控制体系

建立完善访问控制体系是保障云安全的关键。采用多因素认证机制，融合密码、短信验证码、指纹识别等，增强身份验证安全性。实施基于角色的访问控制，遵循最小权限原则，为每个用户分配特定角色，赋予完成工作所需最低权限，降低权限滥用风险。对特权账户加强管理，建立严格审批和审计机制，实时监控操作、记录日志并定期审计。此外，建立持续身份验证机制，利用行为分析技术实时分析用户操作，发现异常立即要求重新验证，确保云环境安全。

3.4 安全管理体系

完善的安全管理体系是技术措施有效实施的保障。应建立专门的云安全管理组织，明确各岗位的安全职责。设立首席信息安全官 (CISO)，负责统筹整个机构的信息安全工作；设立安全运营中心 (SOC)，负责日常的安全监控和事件响应。

制定覆盖云服务全生命周期的安全管理制度和流程，包括风险评估、安全运维、应急响应等方面。在云服务采购阶段进行安全评估，确保云服务提供商的安全能力符合要求；在云服务使用阶段，定期进行安全检查和漏洞扫描，及时发现和修复安全漏洞 [6]。

同时，建立安全审计机制，定期检查安全措施的执行情况。聘请第三方安全审计机构，对云环境的安全状况进行全面评估，发现潜在的安全风险。

此外，还应加强安全意识培训，提升全员的安全防护能力。定期组织安全培训，提高员工的安全意识，防止因人为疏忽导致的安全事件。

4 实施建议与展望

4.1 分阶段实施策略

建议金融机构在构建数据中心云环境下的网络安全防护体系时，采用分阶段推进的实施路径，以契合金融行业对安全性、稳定性与合规性的高要求。第一阶段应聚焦基础设施安全与基础防护能力建设，重点部署虚拟化安全防护、网络隔离与边界防护机制，完成云平台底层架构的安全加固，

为后续防护体系搭建奠定基础；

第二阶段需围绕数据全生命周期安全与精细化访问控制展开，通过数据分类分级保护、加密传输存储、多因素认证等技术手段，构建覆盖数据采集、传输、存储、使用、共享及销毁的全链路防护网，同时建立最小化授权访问模型，防范数据泄露风险；

第三阶段则需构建涵盖安全策略管理、风险监测预警及应急响应机制的全面安全管理体系，通过制定统一的安全标准与操作规范，结合实时安全态势感知与自动化响应技术，形成“预防 - 检测 - 响应 - 恢复”的闭环管理能力。每个阶段均需设定可量化的目标与评估指标（如安全漏洞修复时效、访问控制覆盖率、风险事件处置效率等），确保各阶段防护措施有效落地，最终形成层次化、协同化的云环境网络安全防护体系，为金融行业数字化转型提供持续可靠的安全支撑。

4.2 技术与管理并重

云环境的安全防护需要技术和管理的有机结合。从技术层面来看，要综合运用多种先进的安全技术手段。比如在基础设施安全方面，采用虚拟化安全防护技术，防止虚拟机逃逸等安全风险；在数据安全领域，运用加密算法对敏感数据进行加密处理，保障数据的保密性和完整性；访问控制上，实施多因素认证和细粒度授权策略，严格限制用户对资源的访问权限。

而管理制度则是保障技术措施有效执行的关键。需制定完善的安全策略和操作规范，明确人员在网络安全中的职责和权限。同时，建立严格的监督和审计机制，对技术措施的执行情况进行定期检查和评估。

只有技术与管理制度相辅相成，才能构建起一个全方位、多层次的网络安全防护体系，有效应对金融行业数据中心云环境下的各种安全威胁，为金融机构的稳定运营和数字化转型提供坚实保障。

4.3 持续改进机制

在金融行业数据中心云环境下，网络安全威胁正呈现出动态演变、复杂多样的特征，这对防护体系的适应性和前瞻性提出了更高要求。为确保防护体系的有效性和先进性，建议金融机构建立三维度持续优化机制：首先，构建常态化的风险评估框架，采用定性与定量相结合的评估方法，每季度对防护体系进行全面体检，重点关注新型攻击手段的防御能力；其次，设立专门的技术跟踪团队，密切关注零信任架构、机密计算等新兴安全技术的发展趋势，定期将经过验证的最佳实践纳入防护体系 [5]；最后，建立安全事件智能分析平台，通过机器学习技术对历史安全事件进行归因分析，形成可复用的防御策略知识库。特别需要强调的是，这种持续优化机制应当与金融行业的监管要求保持同步演进，确保技术措施与管理规范的有机统一。

4.4 未来发展趋势

在金融云安全领域，技术发展正推动着防护体系的深刻变革。未来金融云安全将呈现四大显著趋势：其一，人工智能技术将深度融入安全防护，通过机器学习算法实现威胁的智能识别与实时响应，大幅提升检测效率；其二，零信任架构将成为主流安全范式，打破传统边界防护思维，实现 " 永不信任，持续验证 " 的安全模式；其三，安全运营自动化水平将持续提升，实现安全事件的自动响应与处置；其四，监管合规要求将日趋严格，特别是针对数据跨境流动和隐私保护的规定将更加细化。面对这些趋势，金融机构应当未雨绸缪，一方面加强 AI 安全、零信任等前沿技术的研究与应用，另一方面注重培养复合型安全人才，为数字化转型筑牢安全根基。

5 结论

本文针对金融行业数据中心云环境的特点，构建了一套完整的网络安全防护体系。该体系从基础设施安全、数据安全、访问控制和安全管理四个维度出发，通过多层次、多维度的防护措施，有效应对云环境中的各类安全威胁。研究表明，该防护体系能够显著提升金融行业数据中心云环境的安全防护能力，为金融机构的数字化转型提供可靠保障。

金融云安全是一个持续演进的过程，需要金融机构、云服务提供商和安全厂商的共同努力。建议金融机构根据自身实际情况，参考本文提出的防护体系框架，制定适合自身的安全建设方案。同时，应保持对新技术、新威胁的关注，持续优化安全防护措施，确保金融业务在云环境下的安全稳定运行。

参考文献

[1] 高幻幻,冯梓洋,张春晖.网络安全运营体系在金融业的应用研究[J].金融科技时代,2024,32(09):16-20+24.

[2] 陈妍,常媛媛,周家晶,等.网络安全态势感知标准在金融行业云场景下的应用实践[J].信息技术与标准化,2024,(S1):56-60+66.

[3] 乔梦梦,李彦彪,王嘉源.数字化转型背景下金融数据安全面临的风险及对策建议[J].金融科技时代,2023,31(12):76-80.

[4] 袁靖,詹丹丹.加强金融行业关键信息基础设施安全保护，有效防范网络安全风险[J].中国信息安全,2023,(09):58-61.

[5] 刘晨亮,卢宏旺,吴斌.零信任安全防护体系落地实践[J].中国金融电脑,2022,(07):63-66.

[6] 熊建宇.网络金融的特点及安全体系构建[J].科技信息,2010,(31):799-800.