 DOI: https://doi.org/10.12349/iser.v7i5.10529

Research on Network Security Protection System and Data Protection Mechanism in Cloud Computing Environment

Yuchen Liu

Xi'an Xidian Anxing Yongdao Information Security Technology Co., Ltd., Xi'an, Shaanxi, 710000, China

Abstract

Focusing on the characteristics of high resource virtualization, highly centralized business systems, and dynamically changing network boundaries in cloud computing environments, this paper systematically analyzes the construction logic of network security protection systems and data protection mechanisms.By examining the cloud computing infrastructure, multi-tenant operation modes, and data flow paths, the primary sources and operational mechanisms of security threats are identified.On this basis, a multi-layered network security protection system is established from the perspectives of identity authentication, access control, threat detection, and encrypted communication.Meanwhile, combined with data classification and grading, backup and recovery, and privacy protection strategies, a data protection mechanism covering the entire data lifecycle is formed.Furthermore, from the perspective of system coordination, the linkage mechanism and dynamic optimization path between security protection and data protection during operation are explored, enabling coordinated enhancement of risk identification, response handling, and data recovery, thus providing systematic technical support for improving overall security and business continuity in cloud computing environments.

Keywords

cloud computing environment; network security protection; data protection mechanism; data backup; collaborative security

云计算环境下网络安全防护体系与数据保护机制研究

刘雨晨

西安西电安行永道信息安全技术有限公司，中国·陕西 西安 710000

摘要

围绕云计算环境中资源虚拟化程度高、业务系统高度集中及网络边界动态变化的特征，系统梳理网络安全防护体系与数据保护机制的构建逻辑。通过分析云计算基础架构、多租户运行模式及数据流转路径，明确安全威胁的主要来源与作用机理。在此基础上，从身份认证、访问控制、威胁检测及加密通信等方面构建多层次网络安全防护体系，同时结合数据分类分级、备份恢复与隐私保护策略，形成覆盖数据全生命周期的保护机制。进一步从体系协同角度出发，探讨安全防护与数据保护在运行过程中的联动机制与动态优化路径，实现风险识别、响应处置与数据恢复的协同提升，为提升云计算环境整体安全性与业务连续性提供系统化技术支撑。

关键词

云计算环境；网络安全防护；数据保护机制；数据备份；协同安全

1 引言

随着云计算技术在政务、金融及工业领域的深入应用，信息系统部署方式由传统集中架构向分布式、虚拟化及服务化模式转变，网络运行环境呈现出高度开放与动态变化特征。资源共享与弹性扩展在提升计算效率的同时，也使安全边界不断弱化，攻击路径更加多样，数据泄露与服务中断风险显著增加。在多租户模式下，不同业务系统之间的隔离要求更为严格，一旦防护措施不足，极易引发连锁安全问题。同时，数据在采集、传输、存储及调用等环节持续流动，保护难度显著提升，对安全防护体系与数据保护机制提出更高要求。构建覆盖网络层、系统层与数据层的协同防护体系，已成为保障云环境稳定运行与数据安全的重要前提。

【作者简介】刘雨晨（1987–），男，中国北京人，在职硕士，从事云安全、数据安全、信息安全管理、信息科技风险管理、网络安全等级保护、商用密码应用安全研究。

2 云计算环境下网络安全防护体系的结构构成

2.1 云计算基础架构与安全边界划分

云计算基础架构由计算资源池、存储资源池及虚拟网络系统构成，通过虚拟化技术实现资源动态调度与弹性扩展。在该环境下，传统基于物理网络边界的安全防护模式被打破，安全边界由单一网络边界向多层逻辑边界转变。通过引入虚拟私有云VPC、子网划分及安全组策略，对业务系统进行逻辑隔离，同时结合软件定义网络SDN技术实现网络流量的精细化控制。边界防护不再局限于外部防火墙，而是延伸至主机层、应用层及数据层，通过微分段技术对不同业务模块进行隔离控制。

2.2 网络安全防护体系的层级架构设计

网络安全防护体系在云环境中呈现出分层化与协同化特征，整体架构涵盖基础设施层、平台服务层及应用服务层。基础设施层依托虚拟化平台与云主机安全加固技术，通过主机入侵防护HIPS与虚拟防火墙实现底层资源的安全防护。平台服务层通过容器安全技术与镜像扫描机制，对应用运行环境进行安全检测，结合Kubernetes安全策略控制容器调度与资源访问。应用服务层通过Web应用防火墙WAF与API网关实现应用访问控制与接口安全防护[1]。

3 云计算环境下网络安全防护关键技术体系

3.1 云网络访问控制与身份认证技术

云网络访问控制依托身份认证与权限管理体系构建精细化控制机制，通过统一身份认证平台IAM实现用户身份集中管理，并结合多因素认证MFA增强身份验证强度。在访问控制层面采用基于角色的访问控制RBAC与基于属性的访问控制ABAC相结合的方式，对用户权限进行动态分配。通过安全令牌服务STS实现临时凭证管理，降低长期密钥泄露风险。在网络访问控制方面，结合安全组策略、网络访问控制列表ACL及零信任网络访问ZTNA技术，对访问请求进行持续验证与动态授权。

3.2 入侵检测与威胁感知技术体系

入侵检测与威胁感知体系通过多源数据采集与智能分析实现对安全威胁的实时识别。网络层部署入侵检测系统IDS与入侵防御系统IPS，对流量特征进行深度包检测DPI，识别恶意攻击行为。在主机层通过终端检测与响应EDR技术对系统进程与文件行为进行监测，实现对未知威胁的动态识别。通过引入威胁情报平台TIP，整合外部威胁情报数据，对攻击特征进行实时更新。利用机器学习与异常检测算法，对日志数据进行关联分析，提升对高级持续性威胁APT的识别能力。结合安全编排自动化与响应SOAR技术，实现威胁检测、分析与响应的自动化处理，缩短安全事件处置时间，提升整体防护效率。

3.3 数据传输安全与加密通信机制

数据在云环境中的传输过程涉及多种网络路径，保障通信安全需要多层加密机制支撑。通过传输层安全协议TLS 1.3实现端到端加密，防止数据在传输过程中被窃取或篡改。在内部服务通信中采用服务网格Service Mesh技术，通过Sidecar代理实现微服务之间的加密通信与身份验证。针对跨区域数据传输，通过虚拟专用网络VPN及专线连接技术实现安全通道构建。在密钥管理方面，利用密钥管理系统KMS与硬件安全模块HSM对加密密钥进行集中管理与安全存储。结合同态加密与安全多方计算技术，实现数据在加密状态下的计算处理，进一步提升数据在传输与处理过程中的安全性[2]。

4 云计算环境下数据保护机制构建路径

4.1 数据分类分级与全生命周期保护机制

数据分类分级是数据保护的基础，通过对数据敏感程度与业务价值进行评估，将数据划分为不同安全等级。基于数据发现与分类工具，对结构化与非结构化数据进行自动识别与标注，结合数据标签技术实现精细化管理。在数据生命周期管理过程中，从数据采集、存储、使用到销毁各阶段均实施差异化保护策略。存储阶段采用透明数据加密TDE与分布式存储加密技术，使用阶段通过数据脱敏与访问审计控制数据使用范围，传输阶段通过加密协议保障数据安全。结合数据防泄漏DLP技术，对敏感数据外泄行为进行实时监控与阻断，形成贯穿全生命周期的数据保护机制。

4.2 数据备份与容灾恢复技术体系

数据备份与容灾体系通过多层级备份策略与高可用架构保障数据安全与业务连续性。采用全量备份、增量备份与差异备份相结合的方式，提高备份效率与存储利用率。在存储架构中引入分布式存储与对象存储技术，通过多副本机制实现数据冗余保护。跨区域容灾通过异地多活与两地三中心架构实现业务连续运行，结合数据同步技术如日志复制与块级复制，确保数据一致性。利用快照技术实现数据快速恢复，同时通过自动化灾备切换系统实现故障情况下的业务快速恢复。结合容灾演练与恢复验证机制，对恢复时间目标RTO与恢复点目标RPO进行持续优化，提升系统整体可靠性。

4.3 数据隐私保护与合规控制机制

数据隐私保护与合规控制在云环境中具有重要意义，通过多种隐私计算与安全技术实现数据可用不可见。采用差分隐私技术对数据分析结果进行扰动处理，防止敏感信息泄露。通过联邦学习技术实现多方数据协同建模，在不共享原始数据的前提下完成模型训练。在数据存储与处理过程中，结合加密存储与访问控制策略限制数据访问权限。通过区块链技术构建数据访问审计链，实现数据操作的可追溯性。结合合规管理框架，对数据处理过程进行审计与评估，确保满足相关法规要求。

5 云计算环境下安全防护与数据保护协同机制

5.1 安全防护与数据保护协同运行架构

云计算环境中安全防护与数据保护需要在统一架构下实现协同运行，通过构建跨层联动的安全控制体系，将网络安全、主机安全与数据安全进行集成设计。在架构层面依托统一安全管理平台，将身份认证系统IAM、访问控制策略引擎及数据保护策略进行集中配置与调度，形成策略驱动的运行模式。通过安全信息与事件管理系统SIEM实现日志集中采集与关联分析，并与数据防泄漏系统DLP及加密管理系统联动，对敏感数据访问行为进行实时监控。结合服务网格与零信任架构，对应用间通信与数据访问进行持续验证，实现从网络层到数据层的纵向贯通。通过接口化与平台化设计，使安全防护策略与数据保护策略在运行过程中实现动态协同，提升整体防护能力[3]。

5.2 安全事件响应与数据恢复联动机制

安全事件响应与数据恢复机制在云环境中需要形成紧密联动关系，通过自动化与流程化手段实现快速处置。在安全事件发生时，依托安全编排自动化与响应系统SOAR对事件进行分类与处置，结合入侵检测系统IDS与终端检测响应EDR技术获取攻击路径与影响范围。通过事件驱动机制触发数据备份系统执行快照保护或数据隔离操作，防止数据进一步损坏。在恢复阶段，利用分布式存储与异地灾备系统进行数据回滚与业务重建，并结合日志重放技术恢复关键数据状态。通过对恢复时间目标RTO与恢复点目标RPO的动态监测，实现恢复策略的优化调整。联动机制将安全响应与数据恢复过程进行融合，提高应对复杂安全事件的整体能力。

5.3 安全策略动态调整与风险预警机制

云计算环境中安全风险呈现动态变化特征，需要通过实时感知与策略调整机制实现持续防护。通过威胁情报平台TIP获取外部攻击信息，并结合机器学习算法对日志与行为数据进行分析，构建风险评估模型。基于分析结果，动态调整访问控制策略与防护规则，实现策略的自适应更新。通过安全态势感知平台对系统运行状态进行可视化展示，对异常行为与潜在风险进行提前预警。结合基于规则与基于模型的双重检测机制，提高对未知威胁的识别能力。在策略执行过程中，通过策略编排引擎实现跨系统联动调整，使安全防护与数据保护策略保持一致性，增强整体安全防护的前瞻性与主动性[4]。

6 云计算环境下网络安全防护体系与数据保护机制优化路径

6.1 安全管理体系与技术体系融合优化

云计算环境中安全管理体系与技术体系需要实现深度融合，通过制度与技术协同提升整体安全水平。在管理层面构建覆盖规划、实施与评估的安全管理体系，结合风险评估方法对系统安全状态进行量化分析。在技术层面将访问控制、加密保护及威胁检测等技术手段进行整合，形成多维度防护体系。通过统一安全策略管理平台，实现策略配置、执行与审计的集中控制。结合日志审计与合规检查机制，对系统运行状态进行持续监督。通过将管理要求转化为技术规则，实现制度约束与技术执行的协同运行，提升安全体系的整体一致性与执行效率。

6.2 自动化运维与智能化安全防护能力提升

自动化运维与智能化技术为云环境安全防护提供重要支撑，通过引入自动化工具与智能分析手段，实现安全管理效率提升。利用基础设施即代码IaC技术对云资源进行自动化部署与配置，降低人为操作风险。通过持续集成与持续交付CI/CD流程，将安全检测工具嵌入开发与部署环节，实现安全左移。结合人工智能与机器学习技术，对安全日志与网络流量进行分析，实现异常行为的自动识别。通过安全编排自动化与响应SOAR技术，实现安全事件处理流程的自动化执行，减少人工干预。自动化与智能化技术的应用，使安全防护从被动响应向主动防御转变，提高系统整体安全能力。

6.3 持续评估与动态优化机制构建

持续评估与动态优化机制是保障云环境安全稳定运行的重要支撑，通过建立全周期评估体系，对安全状态进行动态监测。依托漏洞扫描工具与渗透测试技术，对系统潜在风险进行识别，并通过风险评分模型进行量化分析。结合安全基线检查与配置审计机制，对系统配置进行规范化管理。通过持续监控平台对系统运行数据进行采集与分析，形成安全评估报告，为策略调整提供依据。在优化过程中，通过闭环管理机制，将评估结果反馈至策略制定与执行环节，实现持续改进。动态优化机制使安全防护与数据保护体系能够适应云环境变化，保持长期稳定运行。

7 结语

综上所述，云计算环境下网络安全防护体系与数据保护机制的构建需以体系化与协同化为导向，通过多层防护架构与全生命周期数据保护策略，实现对复杂威胁的有效应对。在技术持续演进与业务规模不断扩展的背景下，安全能力需依托动态监测、自动化运维及智能分析实现持续提升，确保系统运行的稳定性与数据资产的安全性，从而为云计算环境的高效应用与可靠发展提供坚实支撑。

参考文献

[1] 李伟周.基于云计算环境的网络安全防护体系优化方法研究[J].中国信息界,2025,(02):140-142.

[2] 曾婕.云计算环境下网络安全防护机制的创新研究与实践[J].数字通信世界,2024,(12):87-89.

[3] 沈勤丰.云计算环境下的网络安全防护技术发展与应用[J].网络安全和信息化,2024,(11):140-142.

[4] 石永清.云计算环境下的网络安全防护技术探讨[J].信息系统工程,2024,(10):52-55.