

云计算环境下网络信息安全技术发展

齐 明

潍坊职业学院 山东 潍坊 261000

摘 要：本文围绕云计算环境下网络信息安全技术展开系统研究。首先分析了云计算环境在网络边界模糊化、资源共享安全耦合性、数据存储集中化三方面的安全特征，指出当前存在虚拟化防护薄弱、数据全生命周期安全风险突出、身份认证与访问控制存在漏洞等核心问题。在此基础上，论述了虚拟化安全防护、数据安全防护、身份认证与访问控制三类核心技术的原理与应用，并提出构建全方位虚拟化防护体系、完善全周期数据安全管控、优化智能安全监测与响应能力三项优化策略，为提升云计算环境安全防护水平提供技术路径。

关键词：云计算；网络信息安全；安全防护技术

引言：云计算已成为支撑现代信息社会运转的核心基础设施，广泛应用于政务、工业、金融、医疗等行业领域。然而，云环境在网络边界、资源共享、数据存储等方面呈现出与传统网络截然不同的安全特征，虚拟化防护薄弱、数据安全风险突出、身份认证漏洞等问题日益严峻，严重制约了云计算技术的安全落地与推广应用。本文系统分析了云计算环境的网络安全特征与核心问题，阐述了虚拟化安全防护、数据安全防护、身份认证与访问控制三大核心技术，并从构建虚拟化防护体系、完善数据全周期管控、优化智能监测响应三个维度提出优化策略，旨在为云计算网络信息安全的技术升级与实践应用提供参考。

1 云计算环境的网络安全特征

云计算环境相较于传统网络环境，在架构模式、资源分配方式、用户访问机制上存在显著差异，由此衍生出独特的网络安全特征，这也是云环境网络安全风险频发的核心诱因，具体体现在以下三个核心方面。（1）网络边界模糊化。传统网络具备固定的物理边界，局域网与外部网络的划分清晰，安全防护可依托防火墙、入侵检测系统、物理隔离设备实现边界管控。而云计算采用分布式虚拟化架构，资源池跨越多个物理设备与网络节点，用户可通过互联网随时随地访问云端资源，物理网络边界彻底消融，基于固定边界的传统防护模式失去防护效力，安全管控难度显著提升。（2）资源共享带来的安全耦合性。云计算的核心优势在于多租户资源共享，同一物理服务器可通过虚拟化技术虚拟出多个云主机实例，为不同用户、不同业务提供并行服务。各租户之间的网络通道、存储空间、计算资源相互关联、共用底层设施，单一租户的安全漏洞、配置缺陷或网络入侵问题，极易通过共享资源池扩散至其他租户，引发连锁

性、大范围的安全风险。（3）数据存储集中化。云计算将海量用户的业务数据、个人隐私数据集中存储于云端服务器集群，数据高度集中的特点使云端成为网络攻击的核心目标。一旦安全防护机制失效，将造成大规模数据泄露、非法篡改与永久丢失等严重后果，其影响范围与危害程度远超传统分散式存储模式^[1]。

2 云计算环境下网络信息安全存在的核心问题

2.1 虚拟化环境安全防护薄弱

虚拟化技术是云计算的核心支撑技术，虚拟机、虚拟网络、虚拟交换机等虚拟化组件，构建了完整的云端虚拟运行环境，但当前针对虚拟化环境的安全防护体系存在明显短板。一方面，虚拟网络缺乏专属防护机制，传统网络安全设备仅能防护物理网络流量，无法监测虚拟网络内部的流量交互，虚拟机之间的非法访问、数据窃取、内网攻击行为难以被及时发现。另一方面，虚拟机存在逃逸、漏洞穿透等安全风险，部分不法分子可利用虚拟化技术漏洞突破虚拟机隔离机制，访问同一物理设备下的其他虚拟机数据，破坏租户隔离的安全边界。同时，虚拟机动态创建、销毁、迁移的特性，会导致安全防护策略无法实时同步，出现临时安全防护空白区域，给网络攻击提供可乘之机。

2.2 云端数据安全风险突出

数据是云计算环境的核心载体，数据安全也是网络信息安全的核心内容，当前云端数据在存储、传输、使用全生命周期中均存在安全隐患。在数据存储环节，多租户数据混合存储于云端资源池，若数据隔离技术不完善，极易出现不同用户数据交叉访问、数据泄露的问题，同时云端海量数据的存储架构复杂，碎片化存储、多节点备份的模式，增加了数据溯源与安全管控的难度。在数据传输环节，云端与终端、云端节点之间的数

据交互频繁,部分数据传输未采用高强度加密技术,明文或弱加密传输的方式,容易被非法截取、篡改。在数据使用环节,缺乏精细化的数据权限管控,内部人员越权访问、违规下载数据的行为无法有效约束,内部数据泄露风险难以规避。

2.3 网络访问与身份认证存在漏洞

云计算环境支持多终端、多用户远程接入,开放式的访问模式大幅提升了身份认证与访问管控的难度。当前多数云平台的身份认证方式较为单一,多采用账号密码登录模式,缺乏多维度、动态化的认证机制,账号被盗、暴力破解、仿冒登录等问题频发。同时,云平台的访问权限分配粗放,多采用批量授权、固定授权的方式,未根据用户岗位、业务需求、访问场景进行精细化权限划分,最小权限原则落实不到位,容易出现权限过剩、越权访问的情况。此外,针对异常访问行为的监测能力不足,无法实时识别批量登录、异地异常访问、高频数据下载等风险行为,难以及时拦截非法访问攻击^[2]。

3 云计算环境下核心网络信息安全技术

3.1 虚拟化安全防护技术

虚拟化安全防护技术是针对云计算环境虚拟架构的专属安全防护技术,核心用于解决虚拟网络、虚拟机层面的安全风险,筑牢云平台底层安全屏障。该技术主要包含虚拟网络隔离、虚拟机安全监测、虚拟化漏洞修复三个核心方向。(1)虚拟网络隔离技术。通过虚拟局域网划分、微隔离等技术手段,将同一物理资源池内的不同租户、不同业务虚拟机进行严格的逻辑隔离,阻断虚拟机之间的非法流量交互,避免单点安全风险向其他租户扩散。微隔离技术可将隔离粒度精准到单个虚拟机实例、单个业务端口,实现细粒度的网络访问控制,有效解决传统边界隔离模式在云环境中失效的问题。(2)虚拟机安全监测技术。依托虚拟化层监控模块,实时采集虚拟机的运行状态、资源占用情况、网络流量数据,精准识别虚拟机逃逸、漏洞利用攻击、异常进程启动等风险行为,实现安全风险的实时感知与预警。(3)虚拟化漏洞修复技术。针对虚拟化管理平台、虚拟交换机等组件的安全漏洞进行常态化扫描与自动补丁更新,同时通过虚拟机快照、镜像备份等技术手段,实现虚拟机故障与安全事件发生后的快速恢复,保障虚拟环境的持续稳定运行。

3.2 数据安全防护技术

数据安全防护技术覆盖云端数据全生命周期,是保障云计算网络信息安全的核心技术体系,主要包含数据加密、数据脱敏、数据备份与恢复三类核心技术。(1)

数据加密技术分为传输加密与存储加密两个阶段。传输阶段采用SSL、TLS等高强度加密协议,对云端服务器与用户终端之间的交互数据进行全程加密传输,有效杜绝数据在传输过程中被窃取、监听与篡改。存储阶段采用对称加密与非对称加密相结合的混合加密算法,对云端静态数据进行加密存储,即使数据被非法获取,也无法在短时间内破解有效信息,保障数据的机密性。(2)数据脱敏技术针对云端存储的个人隐私数据、敏感业务数据,通过字符掩码、数值替换、泛化处理等方式,在不影响数据正常分析与使用的前提下,隐藏数据中的核心敏感信息,有效降低数据泄露后被恶意利用的风险。(3)数据备份与恢复技术通过多节点异地备份、增量备份与全量备份相结合的方式,对云端核心业务数据进行定时自动备份,同时建立数据快速恢复机制,在数据误删、非法篡改、存储损毁等异常情况发生时,能够迅速完成数据还原,保障云端数据的完整性与可用性^[3]。

3.3 身份认证与访问控制技术

身份认证与访问控制技术主要用于规范云平台用户的访问行为,拦截非法接入与越权操作,构建精细化的访问安全体系,是云计算环境下保障用户身份可信与操作合规的关键技术手段。(1)多因素身份认证技术摒弃单一密码认证模式,整合账号密码、设备指纹、人脸核验、短信校验、动态令牌等多种认证方式,根据访问场景的安全等级自动匹配认证强度。在低风险场景中采用单因素快速认证,在高风险场景中强制启用多因素联合认证,有效防范账号被盗用、身份仿冒登录等安全风险。(2)精细化访问控制技术基于最小权限原则,结合用户身份角色、业务场景类型、访问时段限制、终端设备状态等多维度条件,制定差异化的权限分配与动态调整策略,实现用户权限的精准管控,杜绝权限过剩与越权访问问题。结合行为审计技术,全程记录用户的登录行为、操作行为、数据访问行为,实现所有操作可溯源、可审计,及时发现并拦截异常访问、违规操作等行为,全面提升云平台的访问安全等级。

4 云计算网络信息安全技术优化应用策略

4.1 构建全方位虚拟化安全防护体系

针对虚拟化环境安全防护薄弱的问题,需搭建覆盖虚拟底层、虚拟网络、虚拟机终端的全方位防护体系,实现虚拟架构各层面的安全管控。(1)强化虚拟化底层安全管控。定期对虚拟化平台、服务器硬件、虚拟管理组件进行全面安全检测,重点排查底层固件漏洞、配置缺陷与潜在后门,及时修补安全隐患,杜绝底层风险向上层扩散。(2)全面部署微隔离防护机制。打破传统物

理隔离模式的局限,按照业务模块、租户类型、数据安全等级划分隔离区域,实现虚拟机之间的精细化网络隔离,阻断非法横向流量交互,避免单点安全风险向其他租户蔓延。(3)建立虚拟化动态防护机制。适配虚拟机动态创建、在线迁移、快速销毁等运行特点,实现安全防护策略的自动同步与动态适配,消除虚拟环境因资源变动产生的安全防护空白,确保虚拟化环境全程可控、可防护^[4]。

4.2 完善全周期数据安全管控机制

结合云端数据集中存储、全程流转的特点,需建立覆盖数据采集、传输、存储、使用、销毁全生命周期的安全管控机制,确保各环节数据安全可控。(1)在数据采集阶段,严格校验数据来源的合法性与完整性,过滤恶意数据、病毒携带数据及异常格式数据,从源头规避数据污染与安全风险。(2)在数据传输阶段,全程启用高强度加密防护,对跨节点、跨终端传输的数据进行加密封装与完整性校验,防止数据在流转过程中被篡改、窃取或伪造。(3)在数据存储与使用阶段,落实数据脱敏处理与细粒度权限管控,针对不同安全等级的敏感数据实施差异化防护策略,禁止未经授权人员访问、导出、复制敏感数据。(4)在数据销毁阶段,采用专业数据粉碎与多次覆写技术,彻底清除废弃数据及其备份副本,避免残留数据被非法恢复与利用,全方位保障云端数据的机密性、完整性与可用性。

4.3 优化智能安全监测与响应能力

依托智能化技术升级传统被动防护模式,构建主动监测、快速响应的智能安全防护体系,是提升云计算环境安全防护水平的关键路径。(1)引入人工智能、大数据分析技术,搭建云端智能安全监测平台,实时采集并分析云平台的网络流量数据、用户操作行为、设备运行状态等多维信息,精准识别隐藏的网络攻击、异常访

问、数据泄露等安全风险。相较于传统人工监测模式,智能监测可大幅提升风险识别的效率与准确率,实现安全威胁的早发现、早预警。(2)建立标准化的安全应急响应流程,针对监测平台发现的安全风险,自动触发预警通知、访问隔离、流量拦截等处置操作,快速控制安全隐患扩散范围,降低安全事件造成的实际损失。(3)定期开展安全风险复盘工作,系统总结各类网络攻击与安全问题的特征规律,持续优化智能监测模型与防护策略,不断提升云平台安全防护的主动性、精准性与适应性^[5]。

结束语

云计算环境下网络信息安全技术的发展,是保障各行业数字化转型顺利推进的核心支撑。本文从安全特征、核心问题、关键技术、优化策略四个层面展开系统分析,明确了虚拟化防护、数据全周期管控、智能身份认证三大技术方向,并提出了场景化、精细化、智能化的优化路径。面对云计算应用规模持续扩大、安全威胁不断演进的趋势,技术团队需持续深化核心安全技术的研发与落地,强化智能化监测与动态防护能力建设,推动云计算网络信息安全防护体系向主动化、精准化方向持续升级,切实保障云端数据安全与业务稳定运行。

参考文献

- [1]王洪波.云计算背景下网络信息安全技术发展探索[J].网络安全技术与应用,2023(5):73-75.
- [2]李鹏.基于网络信息安全技术管理的计算机应用[J].网络安全技术与应用,2022(1):167-168.
- [3]莫善朋.云计算环境下网络信息安全技术发展研究[J].中国宽带,2026,22(01):69-71.
- [4]杜轻.云计算环境下网络信息安全技术发展研究[J].产业创新研究,2025,(14):63-65.
- [5]郑小辉,郭金涛.云计算环境下网络信息安全技术发展分析[J].数字通信世界,2024,(08):119-121.