云计算环境下的信息安全防护技术发展探究

鞠科伟 [1]
JU Kewei

摘 要 随着云计算成为数字基础设施的重要底座，生成式人工智能和大模型正在同步重塑网络攻击与安全防护模式。相较于当前业界更强调零信任、CNAPP 与安全运营自动化协同的实践路径，既有研究仍较多停留于边界防护、漏洞检测等单点控制。文章在分析云计算环境安全风险的基础上，提出纵深防护、合规管理与 AI 驱动安全运营协同联动的路径，强调以意图 / 行为驱动运营衔接模型安全、身份安全与数据安全，并从智能漏洞挖掘、威胁情报分析、异常行为识别和自动化响应等方面论证大模型赋能安全防护的实践价值与创新意义。

关键词 云计算；信息安全；大模型；安全运营

doi：10.3969/j.issn.1672-9528.2026.05.021

0 引言

云计算作为信息技术体系演进的重要成果，其本质上是在资源共享需求不断增长的背景下，对传统 IT 基础设施进行集约化整合与服务化重构，并以按需服务的商业模式向用户提供计算与存储能力[1]。《信息安全技术云计算服务安全指南》将云计算界定为：通过网络访问可扩展、灵活的共享资源池，用户能够按需、自助地获取并管理物理或虚拟资源的服务模式[2]。依托资源池化与虚拟化技术，云计算在动态扩展能力、部署灵活性和系统可靠性等方面展现出显著优势，正在成为数字化基础设施的重要形态。

然而，云计算在提升资源利用效率和服务能力的同时，也使网络系统在开放性、集中化与共享化程度上进一步提高，安全风险由传统单点防护问题转变为跨平台、跨层级的系统性安全问题。系统漏洞利用、恶意代码传播、数据泄露以及多租户环境下的内部安全风险等问题[3]，在云环境中呈现出更强的扩散性与隐蔽性，使得网络安全防护的复杂程度明显提升。随着国家持续推进关键信息基础设施和数据资源保护体系建设，如何在云计算架构下构建与其技术特征相匹配的安全防护机制，已成为信息安全技术领域亟需深入研究的重要课题。围绕云计算环境中的安全风险识别与防护技术演进路径展开系统研究，对于提升云平台整体安全防护能力具有重要的理论价值与现实意义。

2024 年以来，生成式人工智能进入规模化应用阶段，大模型在代码生成、自动代理、智能检索与内容合成方面的能力快速提升，推动企业上云、用云和 AI 原生应用建设同步加速。技术扩散一方面提高了业务敏捷性，另一方面也显著降低了攻击者获取攻击知识、编写恶意代码、构造社工话术和实施多阶段渗透的门槛，使云安全问题呈现出“高自动化、高对抗、高联动”的新特征。因此，将 AI 技术演进因素纳入云计算安全防护体系研究，已经成为提升防护有效性和实践指导价值的重要前提。

1 云计算环境下的信息安全风险分析

2019 年发布的《信息安全技术网络安全等级保护基本要求》标志着我国网络安全等级保护制度进入 2.0 阶段。与以往相比，2.0 阶段在云计算场景下提出了更加系统化的安全要求，不仅强调基础设施层硬件环境、虚拟化平台及云服务层的整体防护能力，同时也将安全控制对象延伸至虚拟机、数据库、中间件、业务应用以及数据全生命周期管理，体现出“云 - 平台 - 应用 - 数据”多层协同防护的理念[4]。

从风险类型来看，云计算安全隐患主要集中在技术风险与治理风险两个方面：一是技术层面，随着网络攻击技术持续演进，勒索软件攻击、0 day 漏洞利用以及 APT 持续性渗透攻击呈现出常态化、专业化和隐蔽化特征，云环境中高度集中化的资源结构使攻击一旦突破关键节点，往往会产生放大效应。同时，SaaS 模式下的应用系统数量庞大、更新频繁，应用软件自身的设计缺陷或配置不当更容易形成新的安全入口，进一步增加了云平台整体暴露面。二是治理层面，尽管我国已陆续出台《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规，但在跨区域数据流动、云服务责任边界划分以及多主体协同监管等方面仍存在制度衔接与实施细化问题，在一定程度上增加了数据安全与合规管理风险。

1. 邵阳市第一中学 湖南邵阳 422000

围绕云计算环境中的安全隐患识别与防护能力提升，学界已开展了多角度探索，并形成了一系列具有代表性的研究成果。相关研究主要集中在攻击检测、隐私保护及安全风险评估等关键方向。例如，从云基础架构层入手，提出基于网络行为特征的攻击识别方法，通过构建应用调用模式并结合入侵检测系统（IDS）机制，实现对异常入侵行为的实时预警与识别[5]；针对云环境中隐私数据流动频繁、关联度高的特点，利用匿名化技术与决策树算法构建隐私数据融合模型，以提升数据处理过程中的隐私保护能力和数据完整性水平[6]；在安全风险评估方面，引入层次分析法与神经网络模型，对云计算环境中的风险因素进行量化分析和预测评估[7]，在一定程度上提升了风险识别的准确性和前瞻性，但与业界零信任、CNAPP 和 XDR/SOAR 协同实践相比，现有研究仍偏重单点算法，对模型安全、身份连续验证和运营闭环关注不足。

就目前 AI 技术的发展情况而言，云安全风险正从传统的漏洞和边界所带来的风险，进一步发展成“模型 - 身份 - 数据 - 业务”耦合风险，攻击者借助大模型可大幅缩短从侦察、伪装到渗透落地所耗费的时间成本，且运用可信身份、SaaS 应用和云基础设施隐藏攻击留下的痕迹，传统凭借固定特征和边界拦截的防护模式压力更大。

大模型接入云平台这个情况后，其输入、输出、工具的使用和权限边界，会直接对访问控制、数据安全与自动化执行安全造成影响，提示词注入、数据投毒、敏感信息遭遇泄露和供应链所具有的脆弱性等问题，进一步体现云安全治理从仅仅保护基础设施延伸到模型使用以及智能代理调用的全过程，如图 1 所示。

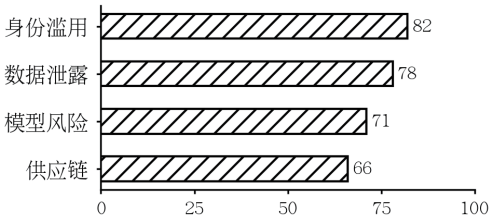

图 1 云安全关键风险暴露面

2 云计算环境下的信息安全防护技术实践

在等级保护制度框架的范畴内，通信网络、区域边界、计算环境和安全管理中心一起构成了云平台纵深防护基础，以这一理念为基础，可于云平台打造覆盖网络接入、系统运行以及数据处理全阶段的安全控制体系：在边界一侧开展准入控制、流量监控和安全审查，在计算环境侧大力强化虚拟机隔离、多因素认证和备份恢复，在运营侧提高监测、判定和联动处置能力[8]。

云计算所拥有的资源池化特征，让计算、存储以及网络资源可以在统一平台中集中管理和动态调配[9]，也为安全能力服务化的部署搭建了条件，凭借着资源池化架构，能够把访问控制、入侵检测、WAF、日志审计等能力一起部署，通过做流量引流、提示风险告警与策略动态变动，达成云上防护能力的持续开展工作。

基于资源池化技术与等级保护纵深防护理念的融合，本文进一步吸收业界零信任、CNAPP 和安全编排响应经验，提出“技术防护—合规治理—智能运营”三维协同框架。本文创新体现在三个方面：纳入模型安全主线、以意图 / 行为驱动运营、贯通技术防护与治理闭环。

2.1 建设纵深安全技术体系

在 IaaS 服务模式下，业务系统通常部署于公有云资源池。针对资源集中、租户共享和边界弱化等特点，纵深安全技术体系应围绕网络边界、资源池安全能力和数据全生命周期保护协同推进[10]，并叠加行为基线、访问意图识别等能力，提升异常访问发现的及时性。

2.1.1 安全区域边界加强网络安全防护与访问隔离

在核心服务器域相关的云安全资源池中部署下一代防火墙平台，把云租户 VPC 跟核心路由设备做安全连接，达成对云上南北向流量的统一管控治理，此平台把防火墙、IPS 和 WAF 的能力予以融合，可实时针对攻击时间、攻击类型和攻击流量做检测与记录，为安全分析和事件溯源提供相关依据。

业务流量先经访问控制策略加以过滤，仅开放业务开展和运维管理必要的端口，并且对访问的来源网段加以限制；由 IPS 对病毒传播、漏洞利用、恶意程序和口令暴力破解等行为予以识别，之后由 WAF 拦截 Web 应用层面的攻击，于入口处缩小攻击面进而保障业务可用。

在业务流量进入云租户 VPC 以后，借助安全组策略搭建第二层安全防护机制，安全组根据白名单访问控制的原则，对访问源地址、协议类型以及端口范围做精细化配置，而且将访问策略与具体业务实例做关联，做到对不同租户之间访问举动的有效隔离。

2.1.2 强化服务器与终端层安全防护能力

在云计算的环境之内，计算节点数量较多、资源调度很常见，要是主机层防护的强度不足，攻击者说不定会借助弱口令、系统漏洞进入平台内部并实施横向渗透，服务器与终端层要同步加大在账户管理、系统加固和主机安全监测的力度：统一实施高要求的口令策略，使默认账户不可用，运用 EDR 持续对暴力破解、恶意程序、异常进程和木马攻击开展监测，结合漏洞扫描以及补丁修复，减少系统被利用的概率，就 AI 辅助造成的异常登录、批量探测和自动提权行为而言，还应凭借主机画像和行为序列分析提高识别的精确性。

2.1.3 强化应用与数据层安全防护机制

在应用与数据有关方面，防护主要是建立起可信身份认证、精细化访问控制以及数据传输和存储的保护机制，各种

安全设备以及业务系统要采用统一身份认证，还利用复杂密码、多因素认证和加密通信，降低账号被盗用及数据在传输当中被窃取、篡改的可能性。

在权限管理相关事宜上，业务系统利用角色权限划分实现有差异的访问控制，给用户分配跟业务职责相匹配的访问权限，还把日志审计系统和数据库审计系统结合起来，全过程记录用户登录、操作以及关键数据访问的相关行为，达成安全审计在各方面的覆盖，鉴别信息在存储方面采用加密算法处理，防止账户凭据泄露产生安全问题。

在数据保护方面，通过建立定期备份与恢复验证机制提升数据安全保障能力。服务器采用快照方式开展周期性全量备份，并定期进行回滚测试验证备份有效性；数据库系统实施周期性全备及恢复演练，确保在系统异常或数据损坏情况下能够快速恢复业务。同时，构建异地实时备份机制，将关键数据同步保存至核心机房或灾备中心，形成多层数据容灾体系，从而在突发事件发生时保障业务系统的连续运行与数据资产的完整性。

2.1.4 以 AI 对抗 AI，构建自适应、自进化的云端防御体系

面对攻击者利用大模型开展定向钓鱼、深度伪造、自动化漏洞利用和低成本横向渗透的新态势，仅依赖静态规则库与人工分析已难以及时应对。与业界向 CNAPP 整合并以 XDR/SOAR 缩短响应链路的趋势相比，云平台更应将机器学习、知识图谱与大模型能力引入检测、分析和处置全流程，形成“AI 对抗 AI”的自适应防御机制。

在具体落地上，第一，可利用大模型和代码语义分析技术开展智能漏洞挖掘，对应用代码、镜像配置、基础设施即代码脚本和开源组件依赖进行自动审查；第二，可对多源日志、告警和外部情报进行关联研判，提升威胁情报分析的归并、去噪和溯源效率；第三，可结合 UEBA 持续识别异常账号调用、跨地域登录、异常权限提升和非常规数据流转；第四，可将检测结果接入 SOAR 流程，自动完成告警分级、主机隔离、账号冻结、访问控制策略下发和工单联动，如图 2 所示。

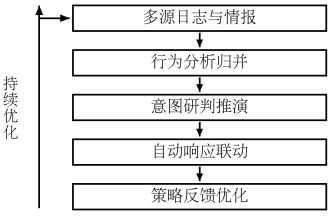

图 2 AI 驱动安全运营闭环

2.2 建设合规安全管理体系

在云计算环境中，单纯依赖安全技术与防护设备难以形成长期稳定的安全保障能力，只有在完善的制度体系与持续运营机制支撑下，技术防护措施才能发挥应有作用。因此，在云计算平台安全建设过程中，应同步推进安全管理体系建设，通过制度规范、流程控制与责任落实，实现安全防护从“设备防护”向“制度化运营”的转变。

2.2.1 完善安全管理制度，夯实制度化防护基础

安全管理制度是网络安全治理体系的核心支撑。大量安全事件表明，安全事故往往并非源于技术缺失，而是由于制度不完善、执行不到位或监督机制缺乏所导致 [11]。因此，在云计算环境中，应以等级保护及数据安全相关法规为依据，建立覆盖系统建设、运行维护和安全运营全过程的安全管理制度体系。

制订统一的信息系统安全管理相关制度文件，界定云平台运行的安全政策、安全目标及安全控制规则，并依靠制度文件形式对安全职责分级落实，制度内容要涵盖信息安全组织架构及岗位职责、人力资源安全管理、信息资产识别与分级管理、系统建设与变更管理、运行维护和操作安全、恶意代码防范、备份与恢复管理、日志审计管理以及安全事件响应管理等核心领域，打造出结构化、可真正执行的信息安全管理制度框架。

确立定期评估和持续改进办法，以内部检查、审计评估及安全演练等方式，对制度执行情形进行跟踪和核查，保证云平台建设和运行过程中安全管理要求落实到位，采用制度建设和执行监督协同推进，可以在技术防护体系之外造就稳定、可持续的安全管理支撑，为云计算环境中信息安全防护技术的长期良好运行提供制度保障。

2.2.2 强化安全管理人员职责，构建责任清晰的安全治理体系

在云计算产生的环境当中，人员管理是安全治理体系重要的组成方面，安全能力不只是取决于技术方面的手段，还和责任的划分以及人员行为规范密切挂钩，要搭建覆盖管理、运维和审计环节的责任体系，并利用常态化培训使关键岗位增强对数据安全、模型安全和账号安全的认知。

在组织管理的范畴当中，要设置统一的信息安全管理领导机制，明确统筹部门以及责任的划分，设置安全、系统、网络、审计管理员等岗位，并做到权限配置和岗位职责相匹配，针对岗位有变动情况，要及时完成审批、权限调整、账号注销并回收资产，防止账户遗留造成的隐患。

2.2.3 强化安全运维管理，提升持续安全保障能力

在安全运维管理这一范畴，要依托云资源池打造标准化流程和持续化监测机制，凭借运维访问控制和审计平台，做到统一身份认证、权限约束和操作留痕；定时对渗透测试、漏洞扫描、系统基线核查和恶意程序检测进行开展，及时针对中高风险问题进行整改，再进一步引入大模型帮忙研判后，可以对大量日志、告警以及工单开展语义归并与优先级排序，

带动安全运营中心从规则触发的途径转向面向意图和行为的联动处置途径。

2.2.4 强化安全风险管理，完善应急响应与持续防护机制

在云计算环境中，安全风险具有突发性强、影响面广、传播快等特点，应依托系统化风险管理机制提升事件预防与处置能力。风险防控可分阶段推进：第一阶段以清理风险、加固基础为重点，通过漏洞排查、集中修复、渗透测试、基线核查与安全培训，降低弱口令和不规范操作造成的隐患；第二阶段以持续监测和动态防护为重点，依托安全监测平台实时掌握云上系统状态，对异常访问行为和可疑攻击源进行分析评估，并按风险等级实施访问限制、主机隔离或策略收敛。在重要业务运行阶段和关键时间点，应制定专项安全保障方案，落实值班制度和应急响应程序。发生突发事件时，应按预案分级响应，第一时间隔离受影响设备或暂停相关服务，完成证据收集、影响评估、恢复处置和报告报送；同时通过常态化应急演练检验预案可操作性，持续优化响应流程与协同机制。

2.3 推动安全运营从“规则驱动”向“意图 / 行为驱动”升级

传统云安全运营多依赖规则、静态阈值和预定义特征库。面对生成式 AI 辅助的低特征、高拟真、快速变形攻击，应在保留关键规则控制的基础上，引入面向身份、资产、会话和业务流程的意图识别与行为建模机制；相较于业界由 SIEM 向 XDR、UEBA、SOAR 协同演进的实践，本文更强调以统一语义和业务上下文实现联动，构建“规则兜底、行为分析增强、意图判断决策”的复合型安全运营框架。

所谓“意图 / 行为驱动”，是指不再仅依据单点日志或单条命中规则判断风险，而是综合账号行为序列、访问链路、调用对象、数据流向、操作结果及其与业务目标的一致性，识别访问行为背后的真实目的。例如，同一账号在短时间内连续触发密钥读取、权限探测、跨区下载与异常外联，即便每一步尚未触发高危规则，也可能体现出明显的数据搜集与外传意图。其论证逻辑在于：攻击行为虽然可伪装单次请求，却难以长期伪装跨主体、跨资源、跨时序的一致性偏离。云计算场景可依托统一身份、资产标签、流量镜像、日志数据和安全知识图谱，建立“人—机—应用—数据—指令”的行为画像与风险评分模型，再由大模型辅助完成告警语义归并、攻击链推演和响应建议生成，如图 3 所示。

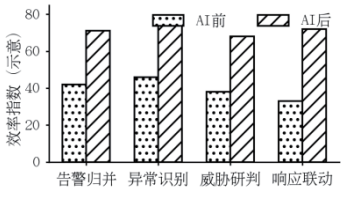

图 3 AI 介入前后处置效率对比

3 结语

在云计算与生成式人工智能深度融合的背景下，云安全防护已由单纯关注网络边界、主机和数据保护，进一步拓展为覆盖模型安全、身份安全、行为安全和运营治理的系统工程。本文在比较业界零信任、CNAPP 与智能 SOC 实践的基础上，提出“技术防护—合规治理—智能运营”三维协同思路。其创新在于将模型安全纳入主线，以意图 / 行为驱动贯通模型、身份与数据安全，形成技术防护与治理闭环。通过引入智能漏洞挖掘、威胁情报分析、异常行为识别与自动化响应能力，可提升系统对新型 AI 攻击的识别、研判与处置效率。

参考文献：

[1] 杨焕增 . 云计算环境下面向内部威胁的虚拟网络安全保护技术研究 [D]. 北京 : 北京工业大学 ,2021.

[2] 国家市场监督管理总局 , 国家标准化管理委员会 .GB/T 31167—2014, 信息安全技术 云计算服务安全指南 [S]. 北京 : 中国标准出版社 ,2014.

[3] 许广彬 . 云计算环境下的信息安全防护技术研究 [J]. 电子元器件与信息技术 ,2023,7(7):121-124.

[4] 叶军军 . 基于云计算背景下的网络安全防护实践 [J]. 信息系统工程 , 2022(4):43-46.

[5] 柴晓东 . 一种在云基础架构中识别基于网络的攻击的新方法研究 [J]. 电子器件 ,2020,43(4):867-872.

[6] 傅江辉 . 基于云计算的社交网络安全隐私数据融合方法 [J]. 济南大学学报（自然科学版）,2021,35(1):29-33.

[7] 郭祖华 , 李杨波 , 徐立新 , 等 . 面向云计算的网络安全风险预测模型的研究 [J]. 计算机应用研究 , 2015, 32(11): 3421-3425.

[8] 安国新 . 云计算背景下的计算机信息安全技术应用分析 [J]. 信息与电脑 (理论版), 2024, 36(18): 119-121.

[9] 李昂 . 云计算环境下网络信息安全技术发展探究 [J]. 网络安全技术与应用 ,2022(7): 61-63.

[10] 党超辉 , 马志伟 , 李树新 , 等 . 浅谈网络安全等级保护 2.0 下的云计算安全风险 [J]. 计算机与网络 ,2021,47(10):54-55.

[11] 冯俙瑀 . 云计算环境下的网络安全防护技术发展与应用 [J]. 信息与电脑 (理论版),2024,36(4):7-9.

【作者简介】

鞠科伟（1980—），男，湖南邵东人，本科，工程师，研究方向：网络技术。

（收稿日期：2026-03-26 修回日期：2026-04-30）