云计算环境下的数据安全与隐私保护研究

陈悦君[1] 张国星[2] 江 长[1] 郑博仑[3] 马汉杰[4]
1. 国网浙江省电力有限公司丽水供电公司 浙江 丽水 323000
2. 国网浙江省电力有限公司青田县供电公司 浙江 丽水 323000
3. 杭州电子科技大学 浙江 杭州 310000
4. 浙江理工大学 浙江 杭州 310000

摘 要：本文旨在系统研究云计算环境下数据安全与隐私保护的核心内涵、关键技术、法规框架、现实困境及未来演进趋势。文章首先剖析了云安全模型的责任共担原则，并详细阐述了当前面临的数据泄露、身份认证、合规性等多重风险。随后，深入探讨了以零信任架构、隐私增强计算（PEC）和云原生安全为代表的关键技术解决方案。文章进一步指出了在AI驱动攻防对抗、量子计算威胁以及供应链安全等新兴背景下，云安全所面临的深层挑战，并提出了构建全域协同、主动自治的安全防御体系的对策建议。最后，展望了可信执行环境（TEE）、机密计算与AI深度融合等未来发展方向，以期为构建安全、可信、合规的云上数字生态提供理论参考与实践指导。

关键词：云计算；数据安全；隐私保护；零信任架构；隐私增强计算

引言

我们身处数据爆炸时代，IDC预测到2025年全球数据总量将达175ZB，传统IT架构难以应对海量数据处理需求，云计算凭借资源池化和服务模式灵活等优势，成为承载数据洪流的核心平台，众多企业都将业务和数据迁移至云端。但云计算带来便利的同时也伴随着风险。企业核心数据置于第三方云服务商管理的虚拟化环境，失去对物理基础设施的直接控制，数据在全生命周期面临外部黑客、内部威胁及云服务商自身等潜在风险。近年来，Capital One、Verizon等云数据泄露事件频发，凸显云安全形势严峻。在此背景下，如何在享受云计算红利的同时，保障数据安全与用户隐私，满足复杂合规要求，成为学界、业界和监管机构共同关注的核心命题，本文将围绕此展开系统性研究。

1 云计算环境下的安全模型与核心挑战

1.1 责任共担模型

理解云安全的第一步是厘清责任边界。主流云服务商（如AWS、Azure、GCP）均采用“责任共担模型”。该模型明确划分了云服务商与云用户各自的安全责任：（1）云服务商负责“云的安全”：即保障底层物理基础设施（服务器、网络、存储硬件）、虚拟化层以及云平台本身的安全。（2）云用户负责“云上的安全”：即保障自身部署在云上的操作系统、应用程序、数据、身份认证、访问控制以及网络安全配置的安全。这一模型的核心在于，云服务商提供了安全的“地基”和“建筑材料”，但如何设计、建造和维护自己的“房屋”（应用与数据），则完全取决于用户自身[1]。大量云安全事故的根源并非云平台存在漏洞，而是用户未能正确配置其云上资源，这凸显了用户安全能力建设的极端重要性。

1.2 核心安全与隐私挑战

1.2.1 数据泄露风险

这是最直接、后果最严重的威胁。原因包括但不限于：云存储桶（如S3）的错误公开配置、数据库弱口令、API接口滥用、恶意内部人员窃取、以及针对云管理控制台的钓鱼攻击等。2026年的行业报告显示，超92%的云安全事件源于企业防护体系缺位。

1.2.2 身份与访问管理（IAM）失效

在动态、分布式的云环境中，传统的基于边界的认证方式已不适用。特权账户的过度授权、凭证泄露、会话劫持等问题，都可能导致攻击者获得对关键数据和系统的完全控制。

1.2.3 合规性与数据主权压力

不同国家和地区对数据的存储位置、处理方式、跨境传输有着截然不同的规定。例如，GDPR强调数据主体的权利和长臂管辖，而中国的《数据安全法》则更侧重于数据分类分级管理和国家数据主权。企业在进行全球化业务布局时，必须应对这种复杂的“合规拼图”。

1.2.4 多云与混合云环境的复杂性

为避免供应商锁定和优化成本，越来越多的企业采用多云（Multi-cloud）或混合云（Hybrid-cloud）策略。这虽然带来了灵活性，但也极大地增加了安全管理的复杂度，因为需要在多个异构平台上统一实施安全策略、

监控和响应。

1.2.5 云原生技术的新风险

容器、微服务、无服务器（Serverless）等云原生技术的普及，在提升开发效率的同时，也引入了新的攻击面，如容器逃逸、镜像供应链污染、函数注入等。

2 关键防护技术与解决方案

面对上述挑战，业界和学界正在积极探索并应用一系列创新技术来构筑云上安全防线。

2.1 零信任架构（Zero Trust Architecture, ZTA）

2.1.1 策略决策点（PDP）与策略执行点（PEP）的实现

零信任架构的工程化落地依赖于策略决策点（Policy Decision Point, PDP）与策略执行点（Policy Enforcement Point, PEP）的分离与协同。PEP通常部署在网络入口、应用网关或主机代理层面，负责拦截所有访问请求，并将其元数据（如源IP、目标资源、用户/设备标识、时间戳等）转发给PDP。PDP作为中央大脑，维护着一个动态的信任评估引擎。该引擎会实时查询多个数据源，包括身份提供商（IdP）的认证状态、设备合规性平台（如MDM/UEM）返回的设备健康报告、用户行为分析（UBA）系统生成的风险评分，以及来自SIEM平台的上下文威胁情报[2]。基于预设的策略规则库，PDP综合这些维度的信息，计算出一个实时的信任分数，并据此做出“允许”、“拒绝”、“限制”或“要求二次认证”的决策，再将指令下发给PEP执行。这种架构确保了访问控制决策的集中化、精细化和动态化。

2.1.2 微隔离（Micro-segmentation）的技术路径

微隔离的实现主要有两种技术路径。其一是基于网络的微隔离，通过软件定义网络（SDN）控制器，在虚拟交换机（vSwitch）层面动态下发细粒度的访问控制列表（ACL），实现虚拟机或容器之间的东西向流量管控。其二是基于主机的微隔离，通过在每个工作负载上部署轻量级代理（Agent），利用操作系统内核的包过滤机制（如Linux的iptables/eBPF）来强制执行安全策略。后者的优势在于不依赖底层网络架构，能够提供更精确到进程级别的控制。例如，可以设定策略仅允许特定应用的二进制文件访问数据库端口，即使同一主机上的其他进程也无法进行连接，从而有效遏制横向移动攻击。

2.2 隐私增强计算（Privacy-Enhancing Computation, PEC）

2.2.1 联邦学习中的安全聚合协议

联邦学习的核心挑战在于如何在聚合来自各参与方的模型更新时，防止服务器或其他参与方推断出任何一方的私有数据。安全聚合（Secure Aggregation）协议是解决此问题的关键。一种典型的实现是基于同态加密（Homomorphic Encryption）或秘密共享（Secret Sharing）。在秘密共享方案中，每个客户端在发送其模型梯度更新前，会与其他客户端建立安全信道，并互相交换随机掩码（mask）。这些掩码的设计使得当所有客户端的掩码化更新在服务器端相加时，所有的随机掩码会相互抵消，最终服务器只能得到所有梯度的总和，而无法获知任何一个客户端的原始梯度值。这一过程保证了在模型训练过程中，单个参与方的数据贡献始终处于加密或混淆状态。

2.2.2 可信执行环境（TEE）的硬件安全机制

以Intel Software Guard Extensions (SGX)为例，其硬件安全机制通过CPU内部的内存加密引擎（Memory Encryption Engine, MEE）实现。当应用程序创建一个Enclave时，CPU会为其分配一块专属的EPC（Enclave Page Cache）内存区域。所有进出EPC的数据都会被MEE使用一个由CPU内部生成且永不暴露的密钥进行AES-128加密[3]。此外，SGX还提供了远程证明（Remote Attestation）机制。任何外部实体（如云用户）都可以向运行在SGX Enclave内的应用发起证明请求。Enclave会利用其内置的、由Intel签名的认证密钥，生成一个包含其代码度量值（即哈希值）的证明报告。外部实体通过验证该报告的签名和度量值，即可确信该Enclave运行的是未经篡改的、预期的可信代码，从而建立起对远程计算环境的信任链。

2.3 云原生安全（Cloud-Native Security）

2.3.1 基础设施即代码（IaC）的安全扫描原理

IaC安全扫描工具（如Checkov, tfsec）的工作原理是将声明式配置文件（如Terraform的.tf文件、CloudFormation的.yaml文件）解析为抽象语法树（AST），然后将其与一组预定义的安全策略规则进行比对。这些规则通常以Open Policy Agent (OPA) 的Rego语言或自定义DSL编写。例如，一条规则可能规定：“所有新创建的S3存储桶必须显式设置block_public_acls = true”。扫描器会遍历AST，查找所有aws_s3_bucket资源块，并检查其属性是否包含此项安全配置。若未找到或配置错误，则标记为高风险漏洞。这种在代码提交阶段（CI/CD流水线中）进行的静态分析，能将安全左移至开发源头，从根源上杜绝因配置疏忽导致的安全事件。

2.3.2 云工作负载保护平台（CWPP）的运行时防护

CWPP的运行时防护能力主要通过部署在主机上的轻量级传感器（Sensor）实现。该传感器利用内核模块或

eBPF探针，深度监控系统调用（syscalls）、进程创建、文件读写、网络连接等关键事件。它会将捕获的行为日志与本地或云端的威胁情报库进行实时比对。例如，当检测到一个新进程尝试执行/bin/sh并连接到一个已知的恶意C2服务器IP地址时，CWPP会立即将此行为识别为典型的勒索软件活动模式，并根据预设策略采取行动，如终止该进程、隔离受感染主机或向安全运营中心（SOC）发送高优先级告警[4]。此外，CWPP还能对容器镜像进行完整性校验，监控容器逃逸尝试（如利用Dirty COW等内核漏洞），为动态变化的云工作负载提供纵深防御。

3 新兴挑战与未来发展趋势

云安全领域正处在一个快速演化的十字路口，未来将面临更多元、更复杂的挑战。

3.1 AI驱动的攻防对抗

AI已成为攻防双方的核心利器。攻击者利用AI自动化生成钓鱼邮件、探测系统漏洞、发起隐蔽攻击；而防御方则利用AI进行异常行为分析、威胁情报关联、自动化响应（SOAR），形成“攻击自动化、防御智能化”的双向博弈格局。

3.2 量子计算的潜在威胁

量子计算机理论上能在极短时间内破解当前广泛使用的RSA、ECC等公钥加密算法。这使得今天在云中加密存储的敏感数据，未来可能面临“先窃取、后解密”的风险。后量子密码学（PQC）的研究与标准化已成为各国战略重点。

3.3 软件供应链安全

Log4j等开源组件漏洞事件表明，现代云应用高度依赖第三方库和开源软件，任何一个环节的污染都可能导致整个系统沦陷。软件物料清单（SBOM）的普及和供应链安全治理将成为云安全的重要组成部分。

3.4 从被动防御到主动自治

未来的云安全将不再是孤立的、被动的点状防御，而是朝着“全域协同、主动自治”的方向发展。通过整合零信任、云原生安全、隐私计算等技术，构建一个能够自我感知、自我学习、自我修复的智能安全生态系统。

4 结语

云计算环境下的数据安全与隐私保护是一项复杂的系统工程，它横跨技术、管理、法律等多个维度。责任共担模型明确了用户在云安全中的主体责任，而零信任架构、隐私增强计算和云原生安全等技术则为履行这一责任提供了强有力的武器。在全球数据保护法规日益趋严的背景下，企业必须将合规要求内化为产品设计和业务流程的一部分。展望未来，随着AI、量子计算等颠覆性技术的发展，云安全的攻防战场将更加激烈。唯有秉持“安全与发展并重”的理念，持续投入技术创新，深化合规治理，并积极拥抱如机密计算等前沿范式，才能在享受云计算无限可能的同时，牢牢守住数据安全与用户隐私的生命线，为构建一个繁荣、可信的数字未来奠定坚实基础。

参考文献

[1]王雨鑫.云计算环境下的数据安全与隐私保护机制研究[J].信息与电脑,2026,38(06):1-3.

[2]魏钰灵.云计算环境下的数据安全与隐私保护技术探讨[J].信息与电脑,2026,38(06):13-15.

[3]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.

[4]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.