云环境下的数据安全存储与访问控制机制

杜秀玲

贝子府镇人民政府，内蒙古自治区赤峰市，024000；

摘要：数字化大潮下，云计算已经成为数据存储与处理的主要范式，但是也带来了严重的数据安全问题。本文主要研究云端数据安全存储以及细粒度的访问控制方法，从多层加密、分布式存储、属性基访问控制和零信任架构等关键技术入手，给出一个包含数据保护、权限管理、审计的完整的防御体系。通过对不同场景下的加密策略、密钥的全生命周期以及动态、细粒度的访问控制实现路径进行分析，发现将先进的加密技术与情境感知的访问决策深度融合之后，可以构建起从数据存储到使用的全过程纵深安全防护。本研究对于在复杂多变的云环境里保证数据的机密性、完整性以及可用性，创建起可信可控的数据管理生态给予理论支撑和实际参照。

关键词：云数据安全；加密技术；访问控制；安全架构

DOI：10.64216/3080-1508.26.02.031

云计算凭借其弹性伸缩、按需使用和资源共享的特点，正在深刻地改变数据存储、处理、分发的模式。但是集中化、多租户的服务架构虽然提高了效率，但是也使数据面临着前所未有的安全风险。传统的以边界为安全基础的安全模型在云环境的动态性、虚拟化、开放性面前逐渐失效，数据泄露、篡改、越权访问等问题越来越突出。因此构建一套适合于云环境、结合强加密存储、细粒度访问控制、持续监控和合规审计为一体的综合性安全机制，已经成为了保证云上业务可靠运行和数据资产安全的核心基础。本文主要从技术和体系的角度出发，对云数据安全的关键问题进行深入研究，系统地提出数据全生命周期的安全存储技术和智能访问控制技术体系，为构建韧性、智能的云端数据安全防线提供理论基础和实践途径。

1 数据加密与密钥管理关键技术

1.1 多场景适应性加密策略

云计算环境下数据的形态和应用场景存在差异，因此需要对加密方式进行差异化。存储量大、访问频率低的静态数据，一般用高效的对称加密算法来达到安全性和性能之间的平衡。密钥交换、身份认证等场景中，非对称加密技术有独特优势。同态加密等前沿技术计算开销大，但是在密文状态下可以运算，为隐私计算等场景提供了新的可能。加密策略选择要结合数据类型、安全需求、性能损耗等多方面因素，同时在数据生命周期的各个阶段部署相应的加密保护，形成全流程的安全屏障[1]。

1.2 密钥全生命周期安全管理

加密体系的安全性根本上取决于密钥管理的可靠性。必须建立密钥生成、存储、分发、使用、轮换、销毁等各个环节的完整的生命周期管理体系。密钥生成要使用符合安全标准的真随机数发生器，保证密钥的不可预测性。密钥存储要和加密数据物理或者逻辑隔离，优先使用经过安全认证的硬件模块或者专业的密钥管理服务，防止密钥明文泄露的风险。建立定期密钥更换机制，对历史密文进行重新加密，可有效地应对长期使用造成的安全威胁。所有的密钥操作都必须记录完整的审计日志，以便于安全分析以及合规审计。

2 高可靠分布式存储与完整性保障

2.1 基于冗余编码的可靠性增强技术

分布式云存储系统采用冗余来保证数据持久性。纠删码技术由于具有较高的存储效率而成为主流，它在多副本备份的基础上又进一步降低了存储开销。把数据分成若干块进行编码，然后分散存储起来。如果某一部分的存储节点发生故障，还可以从其它数据块中恢复出完整的信息。经过恰当安排数据块同校验块的比例，就能在数据可靠性与存储成本之间求得均衡，以适应不一样的应用场景。对于海量数据在分布式环境下安全存储有着非常重要的意义。

2.2 数据完整性验证与证明机制

云存储环境下数据完整性验证是保证信息安全的重要环节。由于数据托管在第三方平台，用户需要有效的手段来验证其完整性。基于可检索性证明的理论模型使用户能够在不完全下载数据的情况下，利用少量的计算和通信来验证云端数据的完整性。该种机制利用周期性的挑战-应答协议来证明云服务商是否完整保留了用户数据。对实施完整性审计来说，有利于找出可能存在

的数据损坏情况，而且也对服务商起到一定的监督作用，使整个存储系统更加可信。

2.3 防篡改与版本控制技术

为了保证数据不被未授权的修改，云存储系统必须要提供有效的防篡改手段。对象存储服务版本控制功能，在数据被覆盖或者删除的时候会保存历史版本，给错误操作留有回滚的可能，也为审计追溯创造了条件。不可变存储策略就是给一些数据设置保留期限，在这段时间内禁止任何删除或修改操作，这对于满足合规要求和抵御勒索软件攻击有着特殊的意义。区块链技术加入以后，关键数据操作记录得到去中心化存证方法的支持，数据操作历史的可信度与抗篡改性能得以加强。

3 动态与细粒度访问控制模型

3.1 基于属性的访问控制模型应用

传统的基于角色的访问控制在云环境里存在灵活性不够的缺点。基于属性的访问控制模型根据用户、资源、环境、操作等各方面的属性动态判断访问权限，适应云环境动态变化的特点。在该模型中，权限的决策不再只是依据用户的身份数，还会考虑访问的时间、地点、设备的安全状况等环境因素。动态授权机制可以实现更加精细化的权限控制，特别适合多租户、资源多变的云平台环境。策略引擎要能够对复杂的规则进行实时的评估并且高效的执行，来满足大规模部署对性能的要求。

3.2 零信任架构下的持续访问验证

零信任安全理念的核心就是不默认信任、持续验证。在这一架构中，每次访问请求都需要经过严格的身份认证和授权检查，不论请求来源于内部还是外部。访问控制成为持续的过程，系统依照实时的风险评价来改变权限，用户行为异常，设备状况改变或者环境风险加大，就会引发更多的验证需求或者权限收束。动态自适应机制可以较好地解决凭证泄露、内部威胁等传统防护无法解决的问题，是云安全架构的重要发展方向。其实施要依靠完整的身份基础设施和实时的风险分析能力的支持。

3.3 多因素认证与强身份鉴别

强化身份认证是实施有效的访问控制的前提。单一的密码认证已经不能满足现在的攻击手段了，多因素认证结合知识凭证、持有物、生物特征等多种因素，大大提高了身份认证的安全性。云环境下访问敏感数据或者执行特权操作的时候，强制进行多因素认证，尤其是管理员账号以及高权限的用户。生物识别技术融合应用，在提高安全性的基础上也提升了用户体验，指纹、人脸等生物特征与密码、令牌的组合使用已经成为高安全场景下的标配，身份验证过程需要产生详细的审计日志供之后分析追踪使用[2]。

4 权限最小化与会话安全管理

4.1 最小权限原则的实施方法

权限最小化原则是指只给予完成工作任务所必须的最低权限。云身份管理中这就意味着不能使用宽泛的内置角色，而应该根据具体职责来定义细粒度的自定义角色。即时权限提升机制用工作流审批和时间限制来控制高权限访问：用户只有在需要的时候申请提升权限，在任务完成之后或者预设时限到达之后权限自动回收。这样就大幅减少了高权限账号的攻击面，也限制了破坏的影响范围。权限配置要定时查看，及时清除不用的权限，保证权限分配准确又及时。

4.2 细粒度资源与数据级授权

现代云访问控制要超越服务层面的授权，深入到数据内部进行精细控制。数据库系统通过行级安全、列级安全策略，可以限制用户只能访问某一些数据行或者字段。对象存储服务允许使用详细的存储桶策略、对象级别的访问控制列表来精确设定每一个文件的操作权限。微服务架构下，服务间互相调用时也需要严格控制，服务网格技术可以为每一个服务之间通信提供细粒度的认证与授权。多层次、多维度的授权体系就构成了云数据保护的纵深防线。

4.3 会话令牌与凭据安全管理

用户认证成功之后得到的访问令牌以及会话凭证应当妥善保管。短期有效的令牌配合刷新机制可以减少凭证被盗用的时间窗口。服务器需要具备实时吊销令牌的能力，在发现异常行为或者用户主动注销的时候立刻撤销相关的凭据。长期访问凭证（API 密钥等）应该建立定期轮换制度，严禁在应用程序、配置文件中硬编码。所有凭证使用情况要全部记录下来，包括签发时间、使用次数、最后一次使用时间等数据，供安全审计和异常检测使用。

5 安全存储与访问控制的协同机制

5.1 加密与授权的深度绑定

数据加密同访问控制有效配合，这才叫做端到端安全。最理想的情况就是把解密能力直接同访问授权关联起来，只有用户的访问请求通过全部策略检查并且得到许可之后，对应的解密密钥才会被安全地释放[3]。该种

策略决定密钥的方式保证了只有被授权的主体才能访问明文数据。要达成这种深入的整合，密钥管理系统同访问控制策略引擎就得密切配合，从而形成起从身份验证一直延伸到数据解密的一条完整信任链。此种情况比较适合于对高敏感度的数据加以保护，即便存储基础设施遭到攻击，加密过的数据也不会轻易外泄。

5.2 集中化策略管理与统一审计

对于多云、混合云越来越普遍的情况，统一安全策略管理以及集中审计就显得越发重要。安全策略应该在中央策略管理平台统一定义和维护，再分发到各个云环境执行，保证策略的一致性以及合规性。所有和数据安全有关的事件，包括密钥操作、访问尝试、策略变更等都应该被记录到集中化的安全信息与事件管理平台。通过分析这些日志可以发现异常模式、追溯安全事件根源，为合规报告提供依据。统一策略管理、统一审计可以很大程度上降低多云环境安全管理的复杂度、运营成本。

5.3 隐私增强技术与合规性支撑

随着全球数据保护法规的日趋完善，云数据管理要满足越来越严格的合规要求。数据脱敏、匿名化技术可以在保证数据可用性的同时降低隐私风险，可以用于开发测试、数据分析等场景。差分隐私等高级技术给统计数据的发布提供理论上的安全保障。对要求本地化存储的地区和行业来说，云平台能通过区域化存储选项满足法规的要求。除此之外系统还要支持数据主体权利的行使，比如访问、更正、删除个人数据的功能也应该纳入统一的访问控制和审计体系。

6 前沿挑战与发展趋势

6.1 后量子密码学迁移准备

量子计算的发展给现有的公钥密码体系带来了潜在的危险。虽然实用化的量子计算机还要等上一段时间，但是对需要长期保密的数据来说，未雨绸缪还是很有必要的。国际标准组织正在积极推进后量子密码算法的标准化工作。云服务提供商和用户需要开始评估向后量子密码迁移的方案，尤其是对那些需要长期保存的敏感数据使用混合加密等过渡策略，为未来密码体系平滑升级做准备。

6.2 机密计算与可信执行环境

可信执行环境技术给云上数据处理提供了一种新的安全范式。处理器层面创建隔离的安全区域，即使操作系统或者虚拟机监控器被攻破，TEE 内代码和数据的机密性、完整性也不会受到破坏。该技术允许敏感数据可以在云端被计算，但是不会泄露给云平台，这给金融分析、医疗研究、多方安全计算等场景打开了新的一扇门[4]。硬件支持以及软件开发工具越来越完善以后，TEE 能够在更多的云服务中被使用，从而成为保护用户数据的重要技术手段。

6.3 智能化安全运维与自动化响应

人工智能、机器学习技术正在改变安全运维的模式。通过对海量的访问日志、行为数据进行分析，可以建立正常行为的基线模型，进而对偏离基线的异常活动进行实时检测。根据风险评估的结果，系统可以自动执行响应动作，例如需要附加认证、限制访问范围或打开调查工单。AI 可以辅助权限治理，通过对实际使用模式的分析来识别并清除过度的权限配置。智能化的、自动化的安全运营可以大幅度提高威胁检测和响应的效率，减少安全团队的工作量，是云安全未来发展的主要趋势。

7 结论与展望

云环境下的数据安全是系统工程，必须采用加密、访问控制、审计监控等多种技术手段，建立多层次的防御体系。核心就是构建以数据为中心的保护策略，将加密保护和动态授权相结合，不断开展风险评估和权限治理。新技术的发展和法规环境的改变使得云安全领域不断向前发展。未来要重视后量子密码迁移、机密计算实用化以及智能安全运维这些方面，持续优化云数据安全防护能力。企业在选择云服务的时候，要明确安全责任边界，善用云平台的安全工具，建立符合自己需要的云数据安全管理体系，才能在使用云计算的便利性的同时，保证数据资产的安全。

参考文献

[1]李戈.基于HDFS的大数据安全存储技术研究与实现[D].西安电子科技大学,2023.

[2]迟松特.云环境下数据存储安全技术研究[J].中国管理信息化,2021,24(18):197-198.

[3]赵鑫宇.云计算数据安全存储的初始布局与动态调整策略研究[D].太原科技大学,2021.

[4]董义明,贾丽芳.云环境下的数据存储安全技术[J].电子技术与软件工程,2020,(10):250-251.