云计算环境下数据存储的网络安全保障措施分析

张轩嘉
墨尔本大学　维多利亚州墨尔本市　3010

摘　要：云计算技术快速发展且广泛普及，使得数据安全问题愈发突显并成为限制云计算进一步发展的关键要素，本文聚焦云计算环境中数据存储遭遇的安全威胁深入剖析了保障数据存储安全的关键技术与有效举措，先阐述云计算数据存储的特性与安全挑战如多租户共享、数据分散存贮、跨域访问等情况，再从数据机密性、完整性、可用性三个维度细致探究加密存贮、访问控制、数据备份和恢复等安全保障技术，接着针对云存储里的数据隐私保护问题给出数据脱敏、匿名化处理之类的隐私保护手段，另外本文也解析云存储安全审计、安全评估、安全合规等管理措施的价值，最后借由案例分析归纳当下云存储安全保障措施的应用成效和存在问题并对未来发展趋势予以展望，本研究想要给云计算环境下提高数据存储安全性提供理论依据与实践指导以推动云计算技术健康发展。

关键词：云计算；数据存储；网络安全；加密技术；隐私保护

近年来，云计算作为信息技术核心驱动力在全球广泛应用。数据显示，2022 年全球云计算市场规模破 5000 亿美元，未来五年预计年均增长率超 20%。其高效、灵活、低成本的优势为各行业提供强大技术支持，但数据存储安全性成为关键瓶颈，金融、医疗、政务等行业云环境下数据泄露、篡改、丢失风险更突出，影响用户信任并给行业发展带来潜在威胁。云计算环境下数据存储因多租户共享导致数据隔离难、数据跨域分布提升安全管理需求、数据访问权限控制复杂且网络环境动态变化，使其安全挑战独特复杂，传统网络安全防护手段需新要求。在此背景下，如何结合技术创新与管理优化构建全面有效的安全保障体系，是云计算领域急需解决的问题。因此，本研究旨在深入分析云计算数据存储的安全保障技术和措施，为应对相关挑战提供理论支持与实践指导。

1 云计算环境下的数据存储安全威胁

1.1 数据泄露风险

云计算环境里，数据泄露是最突出的安全威胁之一，因为云平台大多用多租户架构且不同用户的数可能会存于同一物理服务器，这种共享状况让数据泄露的概率增加，并且攻击者能以恶意手段获取其他租户的数据或者借云服务提供商的漏洞搞数据窃取，再者云存储里数据有跨域访问的性质使得风险进一步加大，国际数据传输时尤其如此，由于不同国家的数据保护法规不一样或许会产生新的安全隐患，2023 年行业报告表明全球因数据泄露而遭受的经济损失达 450 亿美元且大概 30% 的事件跟云存储有关。要应对这个问题的话，加密技术的应用就非常重要，端到端加密能在数据传输和存储的时候多加一道保护屏障从而有效降低泄露的风险，另外加强身份认证和访问控制机制对于减少数据泄露也很关键。

1.2 数据完整性威胁

在云计算环境下，数据存储安全以数据完整性为核心要求之一，然而它面临着诸多威胁，如外部攻击、内部误操作、硬件故障等，因为外部攻击者或许会篡改存储数据以破坏数据完整性，而且内部员工误操作也可能让数据意外被修改或者删除，并且由于云存储系统依靠分布式架构，节点间数据同步可能存在一致性错误进而影响数据完整性。为了全面分析这些威胁的影响，表 1 展示了近年来主要数据完整性威胁的类型、发生频率以及潜在损失情况。针对这些问题，基于区块链的分布式账本技术用于数据完整性验证的情况逐渐增多，其具有不可篡改性和透明性，给云存储带来了新解决方案，另外，定期进行数据校验以及备份恢复测试也是保证数据完整的必要手段。

表 1　主要数据完整性威胁及其影响分析

威胁类型	发生频率（年均）	潜在损失（百万美元）	备注
外部攻击篡改数据	15 次	200	包括勒索软件攻击
内部误操作	25 次	150	数据删除或修改错误

硬件故障	30 次	100	存储设备损坏
同步错误	20 次	80	分布式节点间不一致

1.3 数据可用性挑战

在云计算环境里，数据可用性是用户特别关注的一个安全维度，但这一方面面临着不少挑战，像网络中断、服务宕机以及分布式拒绝服务（DDoS）攻击之类的都包含在内，因为云服务提供商的基础设施有可能会由于自然灾害、电力中断或者人的失误而故障，从而使用户没法访问关键数据，并且 DDoS 攻击靠大量伪造请求把带宽资源占了，合法用户就无法正常享用云服务了，统计显示，2022 年全球云服务中断带来的经济损失超 300 亿美元，金融行业受的影响最大，不过要提高数据可用性，冗余存储和负载均衡技术被广泛采用，把数据分散存放在多处地理位置的服务器上能大大减少单个节点故障带来的影响，而且完善应急响应机制和灾备体系也是保障数据可用性的重要举措 [1]。

1.4 隐私保护问题

云计算环境下的隐私保护问题因大数据与人工智能技术的迅猛发展而愈发复杂，因为用户上传到云端的数据可能含有像个人身份信息、健康记录、财务数据之类的敏感内容，一旦泄露势必给个人和社会带来严重后果，并且云服务提供商在数据分析和处理时也可能无意间暴露用户隐私，特别是在数据聚合与挖掘的时候，不过为了解决这类问题，大家普遍采用数据脱敏和匿名化处理技术，即通过去掉或者替换敏感字段来减少隐私泄露的风险，而且差分隐私这种新技术能在数据分析时加入噪声以保护个体隐私，2023 年行业报告显示全球隐私保护市场规模已达 500 亿美元，可见市场对隐私保护技术极为关注，以后随着隐私计算技术愈渐成熟，隐私保护肯定会有更多创新的解决办法。

2 数据存储网络安全保障措施

2.1 加密技术

在云计算环境下，保障数据存储安全的核心手段之一是加密技术，通过将敏感数据经加密处理，即便数据被非法获取也可防止直接读取。这几年量子计算兴起起来，传统加密算法遭遇挑战，而后量子密码学慢慢成了研究热门。在实际应用里，把对称加密和非对称加密结合起来能有效提高数据安全水平且能满足性能需求，例如 AES–256 这种对称加密算法在数据存储方面运用广泛，而 RSA 或者 ECC 这类非对称加密用在密钥交换和身份验证上，这样就能达成多层次安全防护。

2.2 访问控制机制

在云计算环境里，数据靠访问控制机制限制用户权限免遭未授权访问而得以保护，这是必不可少的安全保障举措，其中基于角色的访问控制（RBAC）、基于属性的访问控制（ABAC）是比较流行的两种实现方式，下表为这两种机制的对比分析展示。

表 2 基于角色与基于属性的访问控制机制比较

特性	基于角色的访问控制(RBAC)	基于属性的访问控制(ABAC)
控制粒度	较粗，以角色为单位	更细，支持多维度属性组合
配置复杂度	较低	较高
灵活性	有限	高
适用场景	用户权限较为固定的企业环境	复杂动态环境，如跨组织协作

实际部署时，把两种机制的优势结合起来不但能更好满足不同场景需求，还可削减管理成本与安全风险。

2.3 数据备份与恢复策略

保障数据可用性，数据备份与恢复策略是关键举措，在云计算环境里更是如此，因为云端数据往往分布在多个物理节点上，若单个节点出故障就可能致使数据丢失，所以得制定完备的备份计划。当下，增量备份和差异备份技术广受关注，前者只记录上次备份之后的变更数据能大幅削减存储开支，后者记录全量备份后的全部变更利于快速恢复，而且异地备份策略把数据副本放在不同地理方位可进一步提升容灾能力 [2]。IDC 统计显示，2022 年全球因数据丢失遭受的经济损失达数十亿美元，这凸显完善备份与恢复机制的重要性，并且自动化工具一结合、定期演练一做，数据恢复效率就能大大提高，业务中断风险也能降到最低。

2.4 安全审计与监控

潜在威胁的发现与及时响应离不开安全审计和监控，在云计算环境复杂的情况下更是如此，所以实时监控系统行为就更为必要。部署日志分析工具能够追踪用户操作轨迹、检测异常活动并且生成详细审计报告。这几年人工智能技术被应用到安全监控中使其更智能了，比如用机器学习算法识别异常流量模式就能提前预警可能的攻击行为。统计显示，2021 年到 2023 年这三年间超 60% 的数据泄露事件若有效果好的安全审计和监控就不会发生。不过现在不少企业还存在审计范围不够全面、监控频率不够高的情况从而使安全隐患难以完全消除。因此建议引进统一的日志管理平台整合多

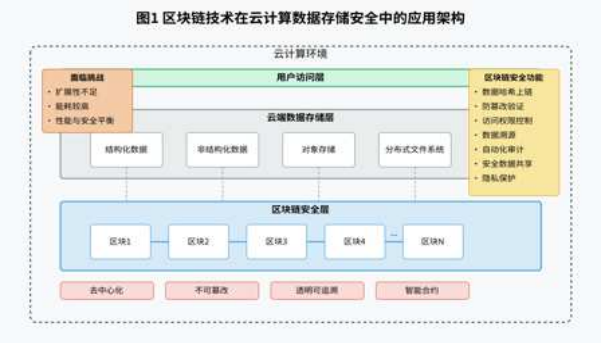
源数据构建全方位安全态势感知体系来不断优化安全防护能力。

2.5 多云存储策略

多云存储策略把数据分散存于不同云服务提供商平台，这既提升系统的冗余性与可靠性又降低被单一供应商锁定的风险，跨国企业与大型组织尤其适用该策略，因其数据常需符合不同国家或地区的法律法规要求，像有些国家就规定公民数据得存放在当地服务器上，多云架构能灵活应对这种合规需求，不过多云存储也带来新挑战，例如数据同步延迟、一致性维护之类的问题，业界针对这些问题提出分布式文件系统、对象存储协议等技术方案来高效管理跨云数据，Gartner 预测到 2025 年超 85% 的企业会用多云战略，这一趋势会进一步推动相关技术发展完善 [3]。

2.6 区块链技术在数据存储安全中的应用

区块链技术具有去中心化、不可篡改以及透明可追溯的特性，在数据存储安全方面有着巨大潜力，于云计算环境里能构建起可信数据存储框架以保障数据完整性与真实性，比如把数据哈希值记于区块链上就能防止数据恶意篡改且能给出完整的修改历史，并且智能合约一用数据访问权限的分配和执行就更自动化、透明化进而减少人为干预产生的风险，这几年好多科技公司在探寻区块链跟云存储相结合的方案，像某个国际著名云服务商推出基于区块链的医疗数据共享平台解决了患者数据隐私保护难题，不过区块链技术在实际运用时仍然存在扩展性差、能耗大等问题，尤其大规模数据存储的时候平衡性能和安全性是急需解决的关键问题，以后随着技术越来越成熟，区块链有望成为云计算数据存储安全保障的重要部分并给行业带来更高效、更安全的解决办法。



3 结论

在信息技术领域，云计算是重要发展方向且这几年全球云计算增长率每年都在 20% 以上，市场规模更是突破数千亿美元大关，不过数据存储安全问题依然是限制云计算进一步普及和应用的关键阻碍。深入分析云计算环境下数据存储安全保障措施后能得出如下结论：加密技术、访问控制、数据备份等核心技术对保障数据机密性、完整性、可用性相当关键，但算法复杂度和计算资源限制仍然影响着这些技术的实施效果。数据脱敏、匿名化处理等数据隐私保护方法给多租户共享环境中解决隐私泄露问题提供有效办法，但实际上操作时得平衡好隐私保护和数据可用性的矛盾。引进安全审计、合规管理措施让云存储整体安全性提高不少，但是相关法规和技术标准还需要进一步完善才能适应行业发展需求。案例分析显示，现在安全保障措施能在一定程度上减轻数据存储面临的安全威胁，但也存在问题，比如技术成本高、跨域协同不够等。以后随着人工智能、区块链等新兴技术融合应用，云计算数据存储安全保障会向着智能化、自动化、标准化发展。这个研究不但给提升云存储安全性提供了理论支持，而且为推动云计算行业健康发展打下了坚实根基 [4]。

参考文献：

[1] 高婷婷 . 区域轨道交通智能服务系统网络安全保障策略研究 [J]. 铁路通信信号工程技术 ,2025,22(01):76–83.

[2] 蒋玥瑶 . 云计算环境下的网络安全风险分析与防护措施 [J]. 信息与电脑 (理论版),2024,36(16):148–150.

[3] 安紫奥 , 李笑天 , 安紫薇 . 云计算环境下网络安全数据存储系统设计 [J]. 信息与电脑 (理论版),2023,35(05):226–228.

[4] 赵鑫宇 , 郭银章 . 云计算环境下数据安全存储的初始划分与分配策略研究 [J]. 计算机与数字工程 ,2023,51(05):1125–1129.