ISSN：3078-8994
EISSN：3104-4492

基于密码技术的云数据访问控制安全加固策略

田茂君

联通数字科技有限公司，北京 100176

摘　要：文章以密码技术应用于云数据访问控制为研究对象，首先对对称密码技术、非对称密码技术、哈希算法和数字签名技术进行云数据访问控制基础分析，阐述了它对保证数据机密性、完整性、身份可信等方面所具有的巨大价值；然后结合目前云计算环境的安全要求，着重讨论了细粒度访问控制中基于属性加密和基于身份密码的用户认证技术，采用基于密钥管理的数据安全防护、数字签名为基础的数据完整性保护，以及基于零信任框架的动态访问控制等多种安全强化手段。研究得出多种密码技术协同应用可有效提高云数据访问控制安全性、可靠性及智能化水平等结论，可为可信云安全体系建设及云数据安全防护机制的完善提供理论借鉴。

关键词：密码技术；云数据；访问控制；安全加固

DOI：10.64649/yh.shfzykjcx.issn3078-8994.202608001

0 引言

云数据运行于开放的网络环境与多租户架构中，面临着数据泄露、非法访问、身份冒用、权限滥用、数据篡改等诸多安全风险，传统的访问控制机制已经很难适应复杂的云环境对数据安全的要求。密码技术是信息安全的一个重要依据，它通过数据加密、身份认证、密钥管理、数字签名和完整性验证等多种技术手段为云数据访问控制的实现提供可靠安全保障，并且可以有效地增强数据的机密性、完整性、可用性和可追溯性。伴随着属性加密、身份密码、零信任架构等新的密码技术的发展，云数据的访问控制已经从静态授权逐步演变为动态、细粒度、智能化的控制。

1 密码技术在云数据访问控制中的应用基础

1.1 对称密码技术与数据加密保护

对称密码术（又称秘钥密码术）是一种使用相同密钥进行加密和解密的加密技术，根据密钥形式可分为分组密码与流密码两种类型。它具有了快速的加密能力、较低的计算成本以及适应大规模数据处理的特点[1]。在云计算的环境下，用户在将数据上传到云服务器之前，可以采用 AES、SM4 等对称加密技术对数据进行加密处理，确保数据始终以加密文本的形式存储在云端，即使云服务器受到攻击或者出现数据泄露的情况，攻击者仍然很难获得数据的原始数据，因此数据的机密性得到了有效的保证。同时对称密码技术可以满足云平台对海量数据实时加密的要求，在云存储、云备份和数据共享等业务场景下有着很高的应用价值。但由于对称密码对密钥安全的依赖性，一旦发生密钥泄露就会直接造成数据保护的失败，综合运用安全的密钥分发、密钥更新和访问权限等控制机制进行研究，实现了数据加密和密钥保护协同管理，持续提高了云数据访问控制体系整体安全性，并为之后的身份认证和权限控制奠定了可靠数据安全基础。

1.2 非对称密码技术与密钥管理机制

非对称加密，亦称公钥加密，是一种使用公钥与私钥配对进行加密和解密的密码技术。用户可以使用公钥来完成数据加密或者密钥加密，通过私钥对其解密，从而实现了开放网络上密钥的安全传递，有效地减少密钥泄露的危险。云计算环境中的非对称密码技术更多地用于密钥交换、身份认证和数字证书管理，并通过建立公钥基础设施来实现，对用户、设备和服务器进行可信认证。云平台可以与密钥生命周期管理机制相结合，实现密钥的产生、分发、存储、更新、撤销和销毁等整个过程的统一管理，从而避免了由于长时间使用相同密钥带来的攻击风险的加大[2]。

1.3 哈希算法与数据完整性验证

哈希算法是一种将任意长度的数据输入映射到固定长度的散列值的函数[3]。它具有单向性、抗碰撞性和高效计算的特点，在云数据访问控制中，它主要负责数据完整性验证的重要功能。用户可以通过 SHA-256、SM3 和其他哈希算法产生唯一的数据摘要后再将数据上传到云平台上，进行哈希值的计算，再进行分享或者移植，通过和原始摘要的比较来判断是否存在篡改数据。在数据内容有任何微小变化的情况下，由于哈希值的显著不同，从而可以迅速检测出非法修改的行为并提高数据完整性检测的效率。同时哈希算法计算快速，且不参与数据加密解密过程，且对系统性能几乎没有影响，非常适合海量云数据实时完整性校验。在实践

ISSN：3078-8994
EISSN：3104-4492

中，哈希算法一般会和数字签名和消息认证码一起协同工作，既能验证数据的完整性又能进一步证实数据来源是否真实，为云数据访问控制，加强云平台总体安全防护能力提供了一种可靠数据验证机制。

1.4 数字签名技术与身份可信认证

数字签名技术是从非对称密码技术中发展起来的一种重要的安全认证技术，它主要使用发送方的私钥产生签名，由相应的公钥来完成对签名的认证，由此达到身份认证、数据完整性验证和不可否认性保障的目的。在对云数据进行访问控制时，数字签名可以有效地证实数据发送者的身份合法与否，避免身份伪造、非法授权和数据篡改的安全性。在用户接入云资源、分享敏感数据或者进行重要业务操作等情况下，该系统可以先对数字签名进行验证，只有经过身份认证后的用户才可以获取对应的访问权限，从而有效地减少了非法访问的风险。数字签名可以将数据在生成和传输时的责任主体记录在案，从而为安全审计、责任追踪和争议处理等提供可信的依据。

2 云数据访问控制面临的安全挑战

2.1 云环境下数据泄露与非法访问风险

云计算环境以资源共享、多租户部署和开放网络互联为主要特征，提高数据使用效率，但也加大了数据泄露和非法访问等安全风险。海量敏感数据在云平台上集中保存，当身份认证机制出现缺陷，访问权限分配不合理或者系统受到网络攻击时，攻击者就有可能采取权限提升和账号盗用等手段、恶意程序的植入和其他手段对数据的非法获取造成了用户的隐私泄露和重要业务信息的泄露。云服务提供商、第三方运维人员以及内部管理人员如果没有有效的监督，还会因为权限滥用或者违规操作等原因导致数据泄露。当数据进行传输、共享和跨区域迁移时，如果没有有效的加密保护措施也极易受到中间人攻击、数据监听和篡改等安全威胁。

2.2 传统访问控制机制在云计算环境中的局限性

传统的访问控制机制大多是以固定身份、角色或者访问列表为基础来进行权限管理，这种设计理念比较适合于一个封闭而又稳定的信息系统，并且在动态开放云计算环境下也渐渐显露出许多缺陷。传统的访问控制策略一般都是静态授权，很难随着用户的身份改变、终端设备的状态、访问环境以及业务风险等因素的不同而做出动态的调整，易产生权限被长时间保留或者被过度授权的情况。多租户、大规模分布式云平台下用户数量与资源类型不断增加，而传统权限管理方式存在分配复杂、维护费用高等问题，很难满足跨部门、跨组织与跨平台对数据共享的要求。传统的访问控制更注重访问控制之前的认证，对访问控制期间的连续身份验证和行为监测比较欠缺，在账号盗用、内部人员越权限访问控制以及高级持续性攻击的安全威胁下防护能力欠缺。它与密码技术的结合度有限，在数据加密保护、密钥管理、完整性验证等方面的支持不到位，很难实现数据、身份、权限等一体化的安全保护。

3 基于密码技术的云数据访问控制及安全加固策略

3.1 基于属性加密的细粒度访问控制策略

属性加密（Attribute-Based Encryption, ABE）通过结合访问权限和用户属性来对数据访问权限进行细粒度控制是目前云数据访问控制研究的一个重要方向。相对于传统的以角色或者身份为中心的授权方式，属性加密可以依据用户部门、职位、权限等级、业务职责和时间地点等多维属性来构造访问策略，使得只有符合访问策略的用户才能够顺利地对数据进行解密，从而有效地避免了权限过大的问题。在云计算环境下，数据访问策略可以直接内嵌到密文当中，从而达到对数据和访问权限的同时保护的目的，甚至可以把数据保存到不可信的云服务器上进行访问，不会因为服务器权限过高造成数据泄露的问题。同时系统要与动态属性管理机制相结合，针对用户属性的改变及时进行访问权限更新、支持属性撤销、权限调整和策略重构等功能，以规避岗位变动或者权限失效带来的安全风险。通过建立以属性加密为核心的细粒度访问控制体系可以显著提高云数据在共享时的安全性，灵活性以及最小权限管理水平。

3.2 基于身份密码技术的用户认证强化策略

身份密码技术（Identity-Based Cryptography,IBC）以用户身份信息直接生成公钥，无需依赖传统数字证书管理体系，有效简化了密钥管理流程，提高了身份认证效率。在对云数据进行访问控制时，可以以用户邮箱、身份证号和工号为公钥进行唯一身份标识，使用户身份和密码体系紧密融合，降低了证书申请、发布和维护所产生的管理成本。同时将动态口令、生物特征识别和多因素认证技术相结合，构建多层次的身份认证机制，不断对用户登录、数据访问和敏感操作等关键环节的身份

ISSN：3078-8994
EISSN：3104-4492

真实性进行认证，减少账号盗用和身份伪造的危险。

3.3 基于密钥管理的云数据安全保护策略

密钥，作为密码技术的关键组成部分，其在安全管理方面的表现直接决定了云数据访问控制的总体性能。要建立一个涵盖密钥产生、发布、存储，更新、备份、撤销和销毁等全生命周期的管理机制，以保证密钥时刻保持在安全可控的范围内。密钥生成阶段要使用高强度随机数算法来增强密钥的复杂度；在密钥的存储过程中，采用硬件安全模块（HSM）或可信执行环境（TEE）来实施密钥的隔离保护，确保密钥不被非法窃取；使用密钥时，要结合最小权限原则进行分级授权和建立定期轮换机制以降低因长时间使用相同密钥而造成的安全隐患。同时还可以引入密钥托管、密钥恢复和分布式密钥管理等技术来增强设备故障或者灾难恢复时系统数据的可用性。

3.4 基于数字签名的数据完整性保障策略

数字签名在实现身份认证的同时也为云数据的完整性提供了源源不断的保障。当云数据被上传、分享、下载和更新时，用户私钥可以用于签名数据摘要，接收者可以通过公钥来证明签名是否真实，从而证实了数据的传输和储存过程中没有受到非法篡改[4]。数据内容一改变，签名验证就会马上失效，系统能及时发现数据的异常，防止损坏数据的持续扩散。同时要结合数字签名和哈希算法、时间戳技术以及日志审计机制等构建数据全生命周期的完整性保护体系，以达到数据来源可查证，操作过程有记录，责任主体可溯源的目的。在多用户协同办公与跨组织数据共享的场景下，通过数字签名可以精确地确定数据的创建者与修改者的身份，避免责任推诿与恶意篡改的发生，增加了云平台数据管理透明度与可信度，对云数据访问控制有了更完善的保障。

3.5 基于零信任架构的动态访问控制策略

零信任架构以“永不默认信任、始终持续验证”为核心理念，强调任何用户、设备及应用在访问云数据前均需完成身份验证和权限评估，为云数据访问控制提供了新的安全防护思路[5]。零信任模式中的系统要结合密码技术构建持续认证机制来实时监控用户的身份、终端设备、网络环境和访问行为，并且根据访问风险对授权策略进行动态的调整，而不是对长期授权进行一次性认证。同时可以使用加密通信、数字证书、身份密码和行为分析来实现数据访问整个过程的安全防护，对于异常登录，越权访问和可疑操作可以及时地进行权限收缩、访问阻断或者重新认证。要将最小权限原则、微隔离技术与持续风险评估机制相结合，针对不同的业务资源进行差异化的访问控制，做到动态授权、动态调整与动态审计，持续增强云数据访问控制系统对复杂网络攻击、内部安全风险等综合防护能力。

4 结论

面对发展变化的网络攻击手段以及越来越复杂的应用场景，仅靠传统的访问控制机制已难以适应现代云环境下的安全要求，密码技术保护数据的核心作用有待发挥。通过综合运用对称密码、非对称密码、哈希算法和数字签名等基本密码技术，结合属性加密、身份密码、密钥生命周期管理和零信任动态访问控制新安全机制，实现对数据、身份、权限以及访问过程等各方面的防护，进一步提高了云数据访问控制系统主动防御能力以及持续安全保障能力。

参考文献：

[1] 宋永立，贾娟，吴习沫，等．基于密码技术的智能制造网络安全保障体系研究 [J]. 电脑知识与技术，2024,20(24):10-13.

[2] 罗文兵，崔宁宁，徐海波．浅议基于商用密码技术加固视频监控安全 [J]. 中国设备工程，2022,(5):212-213.

[3] 康茜．基于改进哈希算法的网络信息安全溯源体系研究 [J]. 信息技术与信息化，2026,(3):113-116.

[4] 夏刚．互联网信息安全加固技术探讨——HTTPS 技术介绍与应用 [J]. 中国金融电脑，2018,(6):65-67.

[5] 王倩．关于密码技术的“加密包”模型假想 [J]. 计算机产品与流通，2017,(11):6.

作者简介：田茂君（1996.05—），男，汉族，山西晋中人，硕士研究生，研究方向：网络安全，数据安全。