混合云环境下重要数据多层加密研究

王 斌[1]
WANG Bin

摘 要 随着云计算技术飞速发展，混合云作为新型云服务模式，其数据隐私保护与安全应用问题愈发突出。文章聚焦混合云架构，剖析现存数据保护痛点，从公有云、私有云双维度，系统阐述数据安全加密方案。创新提出混合云通信隐私数据多层加密方案，通过分层加密机制，强化混合云环境下通信隐私数据的加密防护能力，保障数据传输全流程安全。经理论推导与模拟验证，该方案有效提升混合云数据安全水平，为云计算领域安全发展提供技术支撑与实践参考，助力构建更可靠的混合云数据安全生态。

关键词 混合云；通信隐私；多层加密；同态加密；数据安全应用

doi：10.3969/j.issn.1672-9528.2025.07.026

0 引言

云计算作为一种新兴的高效计算模式，为企业和政府部门等众多用户提供了弹性可扩展、按需付费的资源服务，确保各类业务系统和数据应用场景的实现。混合云结合了公有云和私有云的优势，既保证了数据的安全性，又降低了成本。然而，在混合云环境下，数据的传输和存储涉及多个不同的网络和服务提供商，数据隐私泄漏风险增加。因此，如何确保混合云环境下通信隐私数据的安全应用成为亟待解决的问题。

1 混合云架构中的数据传输加密研究现状

混合云架构为用户提供了灵活性和可扩展性，但在数据安全性方面确实面临诸多挑战。尤其是如何有效保护在公有云和私有云之间数据传输数据的安全性。数据传输安全包括传输加密算法和密钥管理两大部分。其中，密钥作为加密传输的核心，其存储、传输和调用的安全性极为重要。为解决以上问题，实现密钥的统一管理是保障其在整个混合云架构中的安全使用和存储的有效手段之一[1]。

混合云环境中的数据保护示意图如图 1 所示。混合云架构的安全性是企业实施云计算策略时的核心关注点，为确保数据在公有云和私有云之间安全传输，可信传输线路或加密传输信道可有效隔离公共网络的不安全因素，保证传输数据的机密性和完整性。密钥管理在整个混合云安全体系中至关重要，在混合云架构中所有密钥统一由私有云端的密钥管理系统（key management system, KMS）管理和保护。

1. 山东省济南市消防救援支队 山东济南 250101

[10] 李建华 , 郝炘 , 牛明雷 , 等 . 基于卷积神经网络的农作物病害识别 [J]. 中国农业信息 , 2019, 31(3): 39-47.
[11] 丁士宁 . 基于 ResNet50 的水稻病虫害识别 [J]. 现代信息科技 , 2024,8(16):127-130.
[12] 赵晋飞 . 面向田间复杂环境的水稻叶片病害识别算法研究 [D]. 广州 : 广东技术师范大学 ,2023.
[13] 胡志伟 , 杨华 , 黄济民 , 等 . 基于注意力残差机制的细粒度番茄病害识别 [J]. 华南农业大学学报 , 2019, 40(6): 124-132.
[14] WANG Q L, WU B G, ZHU P F,et al. ECA-Net: efficient channel attention for deep convolutional neural networks[C]//2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway:IEEE, 2020: 11534-11542.
[15] SUNIL C K, JAIDHAR C D, PATIL N. Cardamom plant disease detection approach using EfficientNetV2[J]. IEEE access, 2021, 10: 789-804.
[16] SANDLER M, HOWARD A, ZHU M L,et al. MobileNetV2:-inverted residuals and linear bottlenecks[EB/OL].(2019-03-21)[2024-09-25].https://doi.org/10.48550/arXiv.1801.04381.

【作者简介】
龚瑾（2000—），女，湖北荆州人，硕士研究生，研究方向：机器学习与人工智能。
崔艳荣（1968—），女，湖北仙桃人，博士，教授、研究生导师，研究方向：网络安全和信息处理。

（收稿日期：2025-02-15 修回日期：2025-07-10）

KMS 作为安全基石，采用高安全性的加密算法和严格的访问控制策略，维护密钥的全生命周期安全。私有云端的业务系统调用 KMS API 获取密钥，可有效降低密钥泄露的风险。

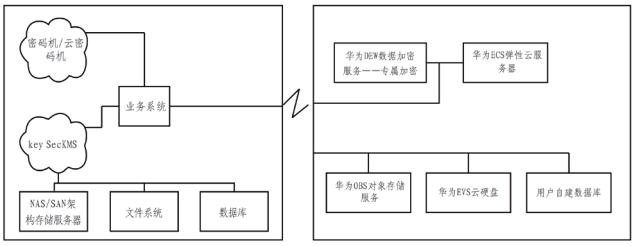

图 1 混合云环境中的数据保护示意图

为保证加密运算的效率和安全性，业务系统并不直接进行加解密操作，而是调用密码机或云密码机的接口，利用专业的硬件密码设备完成数据的加解密工作，提高加密性能，确保加密过程的安全性，同时释放业务系统端的计算资源，使其更专注于业务逻辑的实现。在数据传输到公有云之前，私有云端会先加密处理数据，建立的可信传输线路或加密传输信道等安全通信通道传输到公有云端。公有云端只负责存储加密后的数据，不参与任何解密过程，从而注重数据在公有云环境中的安全性 [2]。

当公有云端的业务系统需要使用这些数据时，私有云端的 KMS 会为其开通相应的权限，并严格控制该业务系统可获取或调用的密钥范围。业务系统与 KMS 之间的通信基于数字证书进行认证，强调通信双方的身份合法性。在密钥调用的过程中，利用 SSL（secure sockets layer）通道展开传输，保证密钥在传输过程中的安全性。业务系统将获取到的密钥导入专属的加密服务中，该服务采用高性能的密码运算能力，高效执行加密和解密过程。同时，专属加密服务还提供密钥的安全存储和调用机制，注重密钥在使用过程中的安全性。

2 混合云架构下的通信数据加密

2.1 公有云厂商是否具备合适的认证资质

用户在选择公有云服务商时，应遵守国家相关的法律法规，保障数据存储在中华人民共和国境内，同时应重视其是否具备相应的安全资质，旨在证明服务商在信息安全、云平台管理、用户数据保护等方面的能力。例如，涉及信用卡支付的业务需要服务商具备 PCI DSS（payment card industry data security standard）认证——全球最严格的金融数据安全标准，需明确公有云服务商是否履行了国家等级保护制度和商用密码管理制度，并对公有云平台进行等级保护定级、备案、等级保护测评及商用密码安全性评估，测评结果满足国家标准要求。常见的安全资质包括 ISO 20000、ISO 27001、ISO 22301 等，分别代表 IT 服务管理、信息安全管理和业务连续性管理等方面的标准。服务商拥有的资质种类越多，意味着其更重视基础建设、用户服务、信息安全和法规遵循，从而能提供更优质的服务 [3]。

2.2 私有云安全防护能力建设

在混合云环境中，保护通信隐私数据至关重要。多层加密策略作为一种有效的保护手段，能够保证数据在传输和存储过程中的机密性、完整性和可用性。通过采用多种加密技术和手段，对数据生命周期不同层次的保护，其涵盖了传输层加密，利用 TLS/SSL 等协议确保数据传输安全，防止数据被截获或篡改。数据层加密对存储在云环境的数据采用强大的加密算法（如 AES）、国产密码算法进行加密，即使数据被非法访问，攻击者也无法轻易解密和利用。应用层加密通过对敏感数据进行加密处理，如用户密码、信用卡信息等关键数据，进一步增强数据安全性。密钥管理采用服务器密码机等专门的密钥管理系统对密钥进行全生命周期管理，此外，同态加密和多方计算技术为在加密状态下处理和验证数据提供新的解决方案，避免数据泄漏风险。基于实施多层加密策略，企业在云环境中全面保护通信隐私数据，提高数据安全性，满足合规性要求，增强数据应用效果，进而提升用户的市场竞争力。私有云安全防护能力建设思维导图如图 2 所示。

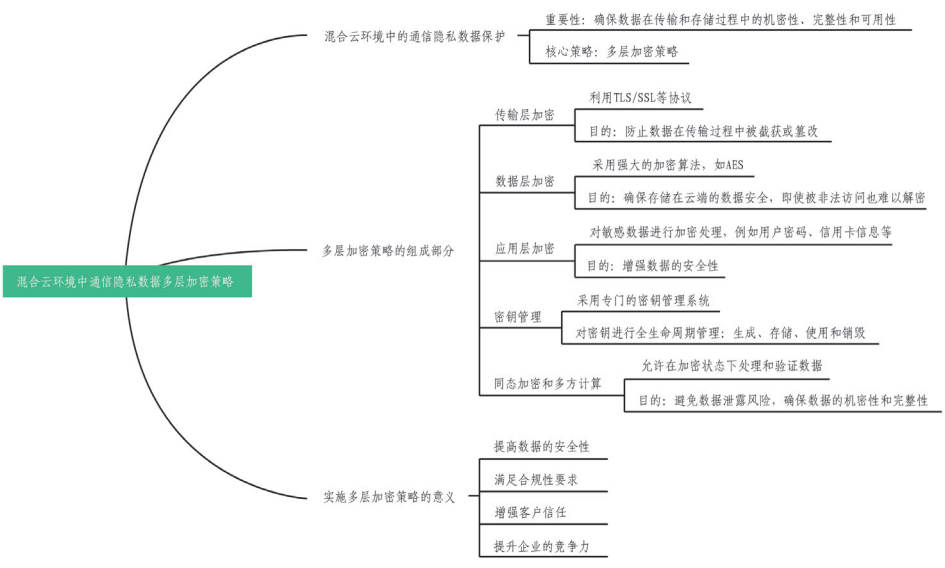

图 2 私有云安全防护能力建设思维导图

2.3 混合云环境下的数据安全挑战与应对

在混合云环境中，数据在公有云和私有云之间流动，跨域的数据传输和存储增加了数据被非法监听、窃取或篡改的风险。尽管公有云厂商提供诸如数据加密、密钥管理、数据库审计和防火墙等安全服务，但云服务提供的多租户、资源共享的服务意味着即使是技术上的安全措施也可能因为人为因素或外部攻击而出现漏洞。除外部威胁，公有云服务自身的稳定性和可靠性也是企业担忧的问题。一旦出现服务器宕机或服务中断等事故，云用户的数据安全将受到严重威胁，甚至可能导致数据丢失。因此，许多用户在实际应用中更倾向于将敏感数据存储在私有云环境中，以保障数据的安全性和可控性 [4]。

面对混合云环境带来的数据安全挑战，用户必须采取可靠且全面的措施。建立完善的数据安全管理体系，保障数据在其从生成到销毁的全生命周期内受到严密保护。实施数据分类与分级管理策略至关重要，需要细致梳理和分类企业内部的所有数据，依据数据的重要性和敏感程度进行分级，并为不同级别的数据制定相应的保护策略，确保关键和敏感信息得到最高级别的安全应用保障。在数据传输环节，加密技术的运用不仅能保证数据的机密性，还能维护其完整性，同时需构建安全的传输通道，有效防止数据在传输过程中被非法截获或篡改。对于数据存储，加密存储技术是防范未经授权访问和窃取的有力武器，而定期数据备份则是应对意外事件、避免数据丢失的有效措施。在数据处理环节，严格控制数据访问权限，要求仅授权人员能处理数据，并建立数据处理审计机制，全面监控和记录数据处理过程，有助于追溯和发现问题。此外，用户在制定数据安全策略时，必须充分考虑合规性要求，遵循相关的数据安全标准、法律法规和行业规定，有助于降低违规风险，也有助于提升用户的公信力和市场竞争力。

2.4 统一的混合云安全管理和运营平台

混合云架构为各类用户带来了业务灵活性和数据安全的双重优势，但随着技术的不断进步和业务的日益复杂，这一架构下的信息安全运维与运营管理也面临着前所未有的挑战。在混合云环境中，用户需面对公有云和私有云中各种安全产品和技术的整合问题，如何在数据不被泄露的同时，提高运维和运营效率成为一个难题。传统的安全管理方法在这种环境下显得力不从心，因此，一个能够集中管理公有云和私有云安全设备和服务的统一平台变得至关重要。

统一平台降低运维的复杂性，更能通过自动化和智能化手段，减少人工错误，提升运维效率。目前，尽管有公有云厂商和硬件安全厂商提供了解决方案，但都存在一定的局限性，无论是对于公有云厂商的依赖还是对硬件安全厂商产品体系的完善程度的担忧，都使用户在选择时需谨慎权衡。对于选择原生 OpenStack 或基于其二次开发的私有云平台的用户，构建一个统一的混合云安全管理平台的任务尤为艰巨，涉及众多技术难题和开发工作 [5]。

3 混合云通信隐私数据多层加密解决方案建议

3.1 多层加密解决方案

为保证混合云环境下数据生命周期的安全性和隐私性，提出了一种多层加密解决方案，从数据生成、传输、存储和处理等多个环节对数据进行全面保护。

在数据生成阶段，采用 AES-256、SM1 等强加密算法对数据进行初始加密。AES-256 是一种高级加密标准，具有极高的安全性和抗破解能力。SM1 加密强度与 AES 相当，该算法不公开，调用该算法时，需要通过加密芯片的接口进行调用。通过使用强大的密钥和加密算法，即使数据在后续环节中被截获，攻击者也无法轻易解密，保证了数据的安全性和隐私性。

在数据传输中，基于 SM2 数字证书进行身份鉴别，采用 SM3、SM4 算法保障通信数据完整性及保密性，采用密码产品自身安全保护机制实现网络边界访问控制信息完整性。例如使用国密 IPSec VPN 实现端到端的加密传输；使用国密 SSL VPN 实现点到端的加密传输；部署安全认证网关，业务终端安装国密浏览器，采用国密 HTTPS 协议访问业务应用系统。也可采用符合国家密码管理要求的国际密码算法对数据传输信道进行加密。

数据存储环节，采用 SM4 算法对重要数据进行加密后存储；采用 SM3-HMAC 或 SM2 数字签名技术，对访问控制信息、重要数据进行存储完整性保护。防止未经授权的访问和数据泄露。即使存储介质被盗或丢失，攻击者也无法直接访问数据，为数据的长期存储提供了强有力的保障。也可采用符合国家密码管理要求的国际密码算法对存储的数据进行加密。

在数据处理过程中，采用同态加密或安全多方计算（secure multi-party computation, MPC）等先进技术，实现在加密状态下对数据进行处理和计算。同态加密允许对加密数据进行计算并得到加密结果，而 MPC 则允许多个参与方在不泄露各自数据的情况下进行协同计算，避免了数据泄露的风险。

3.2 关键技术与实施步骤

在混合云环境中，密钥管理是保障数据安全的核心环节。为有效管理密钥并增强其安全性，企业应构建一套集中

化的密钥管理系统，负责密钥的生成、存储、分发和销毁等全生命周期管理。为进一步增强密钥的安全性，用户应采用服务器密码机等专用设备或服务存储和管理密钥，有效防止密钥被窃取或滥用。在密钥管理系统中，应实现密钥的隔离与分权管理，即不同的密钥应由不同的管理员或角色负责，保持单个个体无法获得完整的密钥信息，从而降低内部泄露的风险。

选择合适的加密算法是保障数据安全的关键，云环境下数据加密关键技术主要包括对称加密技术、非对称加密技术、同态加密技术等。在选择加密算法时，对于需要高性能且数据敏感性相对较低的应用，可采用 AES、SM4 等对称加密算法，提高加密和解密速度快，但要求密钥的安全传输和管理。对于需要高安全性的场景，如重要数据的传输和存储，采用 RSA、SM2 等非对称加密算法，使用公钥和私钥进行加密和解密，安全性较高，但性能相对较低。同态加密技术允许在密文上进行特定的计算，而无需先解密，计算结果解密后与在明文上进行相同计算的结果一致。这在云环境中对于需要在加密数据上进行数据分析和处理的场景非常有用，能有效保护数据隐私。为了兼顾安全性和性能，企业采用混合加密算法，即使用非对称加密算法加密对称算法的密钥，然后使用对称算法加密实际数据。

制定合适的加密策略是确保数据安全的基础，在制定加密策略时，不同的业务对数据的安全性和性能要求不同，用户应根据业务需求确定哪些数据需要加密以及加密的强度。遵守相关的法律法规和行业标准，控制加密策略符合合规要求。例如，对于涉及个人隐私的数据，应采用高强度的加密算法和严格的密钥管理措施。在制定加密策略时，还应考虑技术可行性，即用户应评估现有的技术能力和资源是否能够支持所制定的加密策略，如图 3 所示。

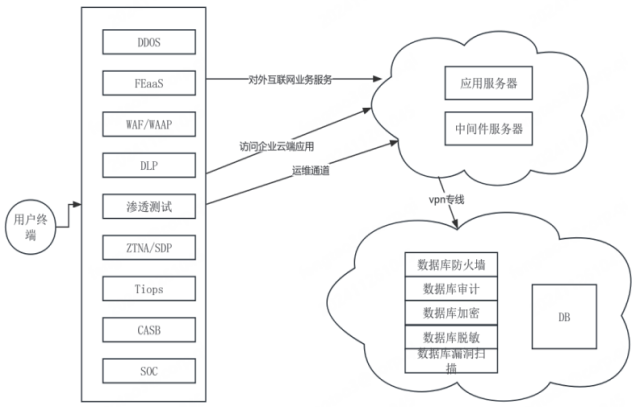

图 3 混合云基础安全 / 加强安全防范和服务能力

在实施多层加密解决方案时，用户应对其与混合云架构的集成进行全面的测试和验证，包括功能测试、性能测试和安全测试等，判断方案的可行性和有效性。同时，还应制定详细的应急预案，以便在出现问题时能够迅速响应和恢复。为了应对不断变化的安全威胁和需求，应建立一套完善的监控机制，综合实时监测和分析混合云环境中的安全事件和威胁，及时发现并应对潜在的安全风险。根据监测结果持续改进和优化加密策略和技术也是至关重要的，包括定期评估现有加密算法的安全性、更新或更换过时的加密技术、调整加密策略的参数等。

4 结语

混合云环境下通信隐私数据多层加密研究，是应对当前复杂网络安全威胁的关键手段。对数据生成、传输、存储和处理等环节实施多层加密，提高数据在混合云环境中的完整性和机密性。采用强加密算法、安全传输协议和同态加密等先进的加密技术和策略，可以为数据提供全面的安全保护。密钥管理的完善、加密算法的选择以及加密策略的制定，都是保障加密效果的重要环节。基于集成与测试，验证多层加密解决方案的可行性和有效性，持续监控与改进则确保了方案能够适应不断变化的安全需求。总体而言，该研究为混合云环境下的数据安全和应用提供了有力保障，推动云计算领域的安全发展。

参考文献：

[1] 杨昌尧 , 翁云峰 . 基于大数据的用户隐私数据多层级加密及仿真研究 [J]. 通信技术 ,2021(3):693-697.

[2] 闫攀 , 周莉 , 闫会峰 . 混合云存储下物联网隐私数据保护模型研究 [J]. 计算机仿真 , 2023,40(2):530-534.

[3] 王建成 . 混合云存储数据访问隐私保护研究 [J]. 电脑知识与技术 ,2021,17(15):69-71.

[4] 唐彭舟 . 混合云环境下整体安全防护体系探讨 [J]. 现代电视技术 ,2021(1):110-114.

[5] 杨昌尧 , 翁云峰 . 基于大数据的用户隐私数据多层级加密及仿真研究 [J]. 通信技术 ,2021,54(3):693-697.

【作者简介】

王斌（1977—），男，山东郓城人，硕士，高级工程师，研究方向：消防通信及信息化，email: wangbin_119@126.com。

（收稿日期：2025-02-16 修回日期：2025-07-03）