基于云计算平台的大数据加密技术在信息安全中的应用

梁 涛
新疆天山职业技术大学 新疆 乌鲁木齐 830017

摘 要：云计算依托分布式架构实现资源池化，但也面临虚拟化层逃逸等安全风险。大数据安全涵盖保密性、完整性等多层次需求。加密技术分对称、非对称和哈希三类，各有适用场景。云计算环境下，大数据加密关键技术包括数据传输、存储、计算加密及密钥管理。其应用场景广泛，涉及企业级云存储、医疗大数据隐私保护等。未来，云计算与大数据加密技术将多技术融合，应用场景也将不断拓展，释放更大社会价值。

关键词：云计算；大数据加密；信息安全；同态加密

引言：在数字化浪潮席卷的当下，云计算凭借其资源池化与弹性扩展优势，成为推动各行业数字化转型的关键力量，大数据也在众多领域广泛应用。然而，云计算的分布式架构在带来便利的同时，也使数据面临诸多安全威胁。信息安全成为重中之重，大数据加密技术作为保障数据安全的核心手段，在云计算环境下发挥着不可或缺的作用，深入研究其应用具有重要意义。

1 云计算与大数据安全基础理论

1.1 云计算平台的安全特性与风险

云计算平台依托分布式架构实现资源池化与弹性扩展，其安全特性体现在多租户隔离机制、动态访问控制和集中化安全管理等方面。多租户隔离通过虚拟化技术划分独立运行环境，避免租户间数据泄露；动态访问控制依据用户角色实时调整权限，降低未授权访问风险；集中化管理则实现安全策略统一部署与漏洞批量修复。但平台也面临多重风险，虚拟化层存在逃逸攻击隐患，攻击者可突破隔离边界窃取其他租户数据；共享资源池易受资源耗尽攻击，影响服务可用性；第三方服务商的运维操作增加数据泄露风险，且跨地域部署导致数据合规性管理难度提升，需结合技术防护与管理规范构建安全体系[1]。

1.2 大数据安全的核心需求

大数据安全围绕数据全生命周期，形成多层次需求体系。保密性确保数据在各环节不被未授权访问，防敏感信息泄露；完整性靠校验机制保障数据不被篡改，避免误导决策；可用性保证授权用户及时获取数据，应对攻击保障服务稳定；可追溯性实现数据操作全程留痕，为溯源提供依据；隐私保护用去标识化等技术规避个人隐私泄露，在个人信息场景尤为关键。这些需求相互关联，构成大数据安全核心框架。

1.3 加密技术分类与适用场景

加密技术分对称、非对称和哈希加密三类，适用场景不同。对称加密用相同密钥，加密快、效率高，适用于大数据存储、实时传输加密等，如AES、DES，AES安全性高，多用于金融、电商；非对称加密公钥加密、私钥解密，密钥管理便捷，适用于密钥交换、数字签名等，如RSA、ECC，ECC在移动设备等资源受限场景优势明显；哈希加密将数据转固定长度哈希值，不可逆，适用于完整性校验和密码存储，如用户密码加密、数据传输验证，SHA-256抗碰撞性强，是主流选择。

2 云计算环境下的大数据加密关键技术

2.1 数据传输加密

数据传输加密是保障云计算环境中数据在终端与云端、云端各节点间安全传输的关键技术，核心在于构建端到端加密通道并强化传输过程防护。主流技术包括SSL/TLS协议加密、虚拟专用网络加密和传输层安全防护等。SSL/TLS协议通过握手过程协商加密算法与密钥，对传输数据进行分段加密，确保数据在公网传输中不被窃听或篡改，广泛应用于云服务访问、大数据采集上传等场景。虚拟专用网络加密利用隧道技术封装数据，通过加密算法对隧道内数据进行保护，适用于企业分支机构与云端数据中心间的大规模数据传输。传输过程中还需结合身份认证机制，如双因素认证验证传输双方身份，同时采用数据分片传输与校验技术，应对传输中断与数据丢失问题，通过多重技术组合实现传输过程的机密性与完整性保障。

2.2 数据存储加密

数据存储加密针对云计算环境中数据静态存储阶段的安全防护，通过对存储介质或数据本身加密，防止数据被非法窃取或泄露。根据加密对象不同，分为存储设备加密、文件系统加密和数据库加密三类。存储设备加密采用硬件加密芯片对磁盘、存储阵列等设备进行加

密，实现数据物理层面的安全防护，即使设备被盗也无法获取数据，适用于云端核心存储设备防护[2]。文件系统加密通过加密文件目录和元数据，对不同用户数据进行权限隔离加密，支持细粒度访问控制，适用于多租户云存储场景。数据库加密针对结构化数据，采用透明加密技术对数据列或行进行加密，在不影响应用系统使用的前提下保障数据安全，同时结合数据脱敏技术，对非必要场景下的敏感数据进行处理。加密过程中需同步考虑密钥与数据分离存储，避免密钥泄露导致加密失效，通过分层加密架构提升存储数据的整体安全等级。

2.3 数据计算加密（同态加密应用）

数据计算加密是解决云计算环境中“数据可用不可见”的核心技术，其中同态加密技术应用最为关键，其允许对加密后的数据直接进行计算，计算结果解密后与原始数据计算结果一致，彻底改变传统加密需解密后计算的模式。同态加密分为部分同态、层次同态和全同态加密，部分同态仅支持加法或乘法单一运算，适用于简单统计分析场景；层次同态支持有限次数的加法和乘法运算，可满足多数数据分析需求，如金融数据的加密统计；全同态加密支持任意复杂运算，但目前计算开销较大，主要应用于高安全需求的小规模数据计算。在实际应用中，常结合隐私保护集合求交、安全多方计算等技术优化性能，如在跨企业数据联合分析中，通过同态加密对各方数据加密后进行联合计算，既保障数据隐私又实现价值挖掘，随着算法优化，其应用场景正逐步从实验室走向实际业务。

2.4 密钥管理技术

密钥管理技术是云计算环境下大数据加密体系的核心支撑，涵盖密钥生成、分发、存储、更新、销毁全生命周期管理，直接影响加密体系安全性。密钥生成采用密码学安全的随机数生成算法，确保密钥唯一性与不可预测性，针对不同加密场景生成不同长度密钥。密钥分发通过安全通道实现，如采用非对称加密算法加密对称密钥后传输，避免分发过程中泄露。密钥存储采用硬件安全模块、密钥管理系统等方式，实现密钥与数据分离存储，硬件安全模块可提供物理级防护，防止密钥被非法读取。密钥更新根据加密等级和使用周期定期执行，避免长期使用同一密钥增加泄露风险。密钥销毁采用安全擦除技术，确保销毁后无法恢复，同时建立密钥管理审计机制，对密钥操作全程留痕，保障管理过程可追溯。

3 基于云计算的大数据加密应用场景分析

3.1 企业级云存储安全

企业级云存储安全依托多层次加密体系，保障企业核心数据在云端存储与使用过程中的安全，满足企业数据管理与合规需求。在数据上传阶段，通过SSL/TLS协议对传输数据加密，防止传输过程中被窃听；存储阶段采用文件级与块级双重加密，结合多租户隔离技术，确保不同企业数据独立存储且加密保护，同时对敏感数据采用脱敏处理后再存储。访问控制层面，基于角色的访问控制机制分配不同权限，仅授权人员可访问对应数据，结合多因素认证提升身份验证安全性。数据备份过程中，采用加密备份技术，确保备份数据安全，同时定期进行加密数据恢复测试，保障数据可恢复性。针对企业数据共享场景，采用基于密钥的访问控制，通过动态密钥分发实现数据共享权限管理，避免共享过程中数据泄露。

3.2 医疗大数据隐私保护

医疗大数据包含患者个人信息、病历数据、检查结果等敏感信息，其隐私保护需在数据利用与隐私安全间实现平衡，加密技术是核心保障手段。数据采集阶段，采用匿名化处理去除患者标识信息，同时对采集数据进行传输加密，确保数据从医疗机构终端安全上传至云端。存储阶段，采用数据库透明加密技术对病历、检查数据等结构化数据加密，结合存储设备加密，防止数据静态泄露；针对医学影像等非结构化数据，采用文件加密技术保障安全[3]。数据使用阶段，采用同态加密与安全多方计算结合的方式，实现多医疗机构间数据联合分析，如疾病诊断模型训练时，各方加密数据后联合计算，无需暴露原始数据。针对数据共享场景，采用基于属性的加密技术，根据访问者属性分配访问权限，仅授权人员可访问特定数据。同时，严格遵循医疗数据相关法规，建立数据访问审计机制，对数据操作全程记录，确保数据使用合规，通过加密技术与管理规范结合，实现医疗大数据隐私保护与价值挖掘的双赢。

3.3 物联网（IoT）数据安全

物联网（IoT）设备数量庞大且分布广泛，数据传输频繁且设备资源受限，其数据安全需采用轻量化加密技术，保障数据从设备端到云端全流程安全。设备端数据采集阶段，采用轻量级对称加密算法对数据加密，如AES-128算法，在保障安全的同时降低设备计算开销；设备与网关间传输采用SSL/TLS精简版协议，建立安全传输通道，防止数据被拦截。网关与云端传输阶段，采用标准SSL/TLS协议加密，结合数据分片传输与校验技术，应对物联网数据海量、实时的传输特点。云端存储阶段，针对物联网数据多格式特点，采用分类加密策略，结构化数据采用数据库加密，非结构化数据采用文件加密，同时结合密钥管理系统实现密钥高效管理。针对设备身

份认证，采用基于公钥基础设施的认证机制，确保设备合法性，防止伪造设备接入。

3.4 跨组织数据协作场景

跨组织数据协作场景中，各组织数据隐私保护与数据共享需求并存，加密技术通过构建安全协作框架，实现“数据可用不可见”的协作目标。在数据共享前，各组织对自有数据进行加密处理，采用同态加密或安全多方计算技术，确保数据在加密状态下可进行联合计算。针对协作过程中的数据访问权限，采用基于属性的加密技术，根据协作角色与任务分配不同访问属性，仅满足属性条件的用户可访问对应加密数据。数据传输过程中，采用虚拟专用网络或加密隧道技术，构建跨组织安全传输通道，防止数据传输过程中泄露。为避免密钥管理混乱，建立跨组织统一密钥管理联盟，采用分布式密钥管理架构，各组织保留自有密钥控制权，同时实现密钥协同管理。协作完成后，对相关数据及密钥进行安全销毁，确保数据不被二次利用。另外，建立协作过程审计机制，对数据操作与计算过程全程记录，保障协作过程可追溯与合规性。

4 未来发展趋势

4.1 技术融合方向

未来云计算与大数据加密技术将呈现多技术深度融合趋势，形成更高效、安全的加密体系。人工智能与加密技术融合成为核心方向，通过人工智能算法优化加密参数选择与密钥管理策略，实时识别加密过程中的异常行为，提升加密体系自适应防护能力。区块链技术与加密技术结合，借助区块链去中心化、不可篡改特性，构建分布式密钥管理系统，提升密钥存储与分发的安全性，实现加密操作全程可追溯。边缘计算与加密技术融合，针对物联网等场景中边缘设备资源受限特点，开发轻量化边缘加密算法，实现数据在边缘节点的实时加密处理，降低云端传输压力。量子计算与抗量子加密技术同步发展，针对量子计算对传统加密算法的威胁，研发格基密码、哈希签名等抗量子加密算法，提前布局量子时代加密安全防护，多技术融合将推动加密技术向更智能、更可靠方向发展。

4.2 应用场景拓展

随着加密技术成熟与落地，其应用场景将从现有核心领域向更多新兴领域拓展，覆盖社会经济各层面。在数字金融领域，加密技术将深度应用于数字货币交易、跨境支付等场景，结合智能合约实现加密交易全程安全可控，保障金融数据隐私与交易安全。在智慧城市建设中，针对交通流量、公共安全等海量数据，采用加密技术实现数据共享与隐私保护，支撑智能交通、智能安防等应用落地，同时保障市民个人信息安全[4]。在工业互联网领域，加密技术将应用于工业数据采集、设备通信与生产协同等场景，防止工业敏感数据泄露与生产系统被攻击，保障工业生产安全。在教育领域，针对在线教育数据、学生个人信息等，通过加密技术实现教育资源安全共享与学生隐私保护，支撑教育数字化转型。在政务数据开放共享中，加密技术将实现政务数据安全开放，推动政务服务智能化升级，应用场景的不断拓展将进一步释放加密技术的社会价值。

结束语

云计算与大数据加密技术对信息安全意义重大，在保障数据全生命周期安全方面发挥着关键作用。从关键技术到多样应用场景，都展现出其强大效能与潜力。未来，随着技术融合与应用拓展，该领域将迎来更广阔发展空间。我们需持续关注技术发展动态，不断优化加密体系，以更好地应对日益复杂的安全挑战，为信息安全保驾护航，推动各行业在安全环境下蓬勃发展。

参考文献

[1]吕敬兰.数据加密技术在计算机网络信息安全中的应用[J].科技创新与应用,2024,14(18):185-188.

[2]吴小锋,宋洋,梁旭.基于云计算的信息网络安全技术研究与应用[J].通信电源技术,2023,40(18):159-161.

[3]徐敏,胡聪,王萍,等.基于云计算技术的大规模数据存储策略研究[J].微型电脑应用,2022,38(4):80-83,92.

[4]邬余崎.基于大数据的云计算安全系统设计及系统测试分析[J].科学技术创新,2022(36):99-102.