面向云计算环境的数据加密保护方案探讨

吴兴宇
杭州安恒信息技术股份有限公司　浙江　杭州　310000

摘　要：伴随云计算技术深度普及，数据安全已然成为维系云计算稳健发展的核心要素，云计算场景呈现开放、虚拟与分布式特征，致使数据于存储、传输及处理环节遭遇多重安全隐患，涵盖数据泄露、非授权访问、恶意篡改等情形。数据加密作为捍卫数据安全的关键技术，于云计算场景中彰显出极高应用价值，本文聚焦云计算环境下数据加密的需求与困境，系统剖析传统及新兴加密技术在云计算领域的应用状况，构建一套兼顾数据全生命周期各阶段的加密防护体系，致力于为云计算场景下的数据安全打造更完备、更高效的保障策略。

关键词：云计算；数据加密；保护方案；密钥管理；访问控制

引言

信息技术迅猛革新的当下，云计算作为前沿计算范式，以卓越的运算效能、灵活的资源调配及高效的服务供给模式，应用范畴持续拓展，企业与个人相继将数据及业务迁移至云计算平台，实现成本削减与效率提升。但云计算环境的开放共享特质衍生出诸多数据安全隐患，数据于其中面临遭窃、篡改、滥用等风险，保障数据安全与隐私，成为云计算发展进程中亟需攻克的关键难题。数据加密技术对数据实施加密操作，将明文转化为密文，限定仅授权用户可解密访问，是守护数据安全的关键途径，探究适用于云计算环境的数据加密保护方案，兼具理论价值与现实意义。

1 云计算环境数据加密概述

1.1 云计算环境数据特点

与传统环境相比，云计算环境下的数据呈现独特属性，伴随云计算广泛应用，企业及个人云端存储数据量急剧攀升，类型丰富多元，既包含数据库表格数据等结构化数据，也涵盖文档、图片、视频等半结构化与非结构化数据。数据处于持续变动状态，在云计算环境中不断生成、更新、删除，用户操作频繁且形式多样，其状态与内容始终处于动态演变，云计算平台由众多服务器与存储设备构建，数据分散存储于不同物理位置，处理时需在多节点间传输协作，呈现分布式存储与处理特征。同时云计算平台支持多用户资源与数据共享，用户可经网络随时访问使用数据，这种共享特性无疑加剧了数据安全管理的复杂程度。

1.2 云计算环境数据加密保护需求

在云计算环境里，数据加密保护有着多维度的需求，从机密性角度来看，得保障数据不管是存储、传输还是处理，都不能被没有授权的用户接触到，防止数据遭到泄露。企业的商业机密、用户的个人隐私这些敏感数据，都要靠加密技术来守护，避免被竞争对手或恶意用户获取，而完整性需求要求数据在传输和存储过程中不被篡改、破坏，也不能丢失，这样才能维持数据的真实准确[1]。对于金融、医疗这类对数据精度要求极高的领域，数据完整性尤为重要，稍有篡改就可能引发严重问题，可用性需求强调在确保数据安全的同时，要让授权用户能够随时顺利访问和使用数据，不能因为加密而影响正常操作，访问控制需求则需依据用户身份和权限，细致管控数据访问，只有对应权限的用户才能进行读取、写入、修改等操作，另外密钥作为数据加密的关键所在，其安全地生成、存储、分发和更新，是数据加密保护方案成功落实的重中之重。

2 传统数据加密技术在云计算中的应用

2.1 对称加密技术

作为历史悠久且行之有效的加密手段，对称加密技术运用同一密钥完成数据的加密与解密流程，于云计算场景下，该技术凭借计算效能卓越、加密速率快捷的优势，在处理海量数据加密任务时表现突出。DES、3DES、AES等均属常见的对称加密算法。数据存储环节，可借由对称加密算法对用户数据加密后存于云端服务器，以此防范非授权访问；数据传输进程中，同样能利用对称加密技术保障数据在网络传输时免遭窃取与篡改，不过对称加密技术存在显著弊端，密钥管理面临挑战。因加密解密共用同一密钥，需将密钥安全传递给授权用户，而在密钥存储与分发阶段极易产生泄漏风险，云计算环境下用户与云服务提供商间或存在信任缺失状况，如何实现对称加密密钥的安全管理成为亟待解决的关键问题。

2.2 非对称加密技术

非对称加密技术也被称作公钥加密技术，其运作基于一对密钥——公钥与私钥，公钥能够公开传播，私钥则由用户自行妥善保管，加密时运用公钥处理数据，解密则需对应私钥接入，该技术有效化解了对称加密技术在密钥管理上的困境，无需进行密钥的安全传输，仅公开公钥便能达成目的[2]。RSA、ECC等都是广为人知的非对称加密算法，云计算环境中，非对称加密技术在密钥交换、数字签名等场景发挥着重要作用，用户和云服务提供商可通过非对称加密技术协商密钥，进而生成对称加密密钥，以此对大量数据实施加密传输，提升效率。非对称加密技术用于数字签名，可保障数据完整性与不可否认性，像云服务提供商对所提供服务进行数字签名，以此证实服务的真实合法，不过非对称加密技术存在计算复杂度高的问题，加密解密速度相对迟缓，并不适宜直接用于大量数据加密，一般会与对称加密技术配合使用。

3 新型数据加密技术在云计算中的探索

3.1 同态加密技术

创新性加密技术范畴内，同态加密以独特的属性脱颖而出，其最突出的特性在于能够在数据处于加密状态时，直接执行特定数学运算，无需经历数据解密这一环节，对加密数据进行运算所得到的结果，与先对明文进行相同运算而后再加密所产生的结果完全等同。云计算的应用场景中，同态加密技术在数据处理和分析领域蕴含着巨大的应用潜力，用户可将加密处理后的数据分析指令传输至云服务供应商处，云服务供应商无需解密数据，即可对其进行分析与处理，随后将处理成果反馈给用户，用户利用自身私钥对结果进行解密操作，如此便能在保障数据隐私安全的同时，达成对数据的有效运用[3]。同态加密技术包含部分同态加密与全同态加密两种类型，当前部分同态加密技术已达到相对成熟的程度，并且在诸多实际场景中得以应用，全同态加密技术因面临极高的计算复杂度挑战，仍处于研究探索阶段，尽管同态加密技术具备显著优势，但其计算效率相对较低，对云计算平台的计算资源提出较高要求，致使该技术在现阶段难以实现广泛的大规模应用[3]。

3.2 属性基加密技术

属性基加密作为基于属性的加密技术，其核心理念在于把用户身份信息转换为诸如角色、部门、权限等一系列属性，进而依据这些属性实施数据加密，唯有符合数据加密时所设定属性条件的用户，方可解密并获取数据，凭借此技术，能够达成细粒度访问控制，在云计算场景下多用户数据共享安全管理意义重大。企业可依照员工职位、部门等属性，为不同数据制定差异化加密策略，仅具备相应属性的员工可访问对应加密数据，该技术包含密钥策略属性基加密（KP-ABE）与密文策略属性基加密（CP-ABE），后者在访问控制上更具灵活性，能按照数据内容及用途设定多样访问策略。属性基加密有效应对传统访问控制技术在云计算环境中的动态复杂难题，增强数据访问安全性与灵活性，此技术存在属性撤销棘手、密钥管理繁琐等状况，亟待深入探究与完善。

4 云计算环境数据加密保护方案设计

4.1 数据生命周期各阶段加密策略

数据生成环节，数据敏感状况与重要程度决定加密策略，用户身份信息、金融交易记录这类敏感数据一经产生，随即选用适配加密算法处理，从源头筑牢安全防线，并赋予属性标识，方便后续访问管控与加密策略调配，存储至云端服务器前，对称加密技术可提升存储效能，同时以非对称加密手段保护对称加密密钥。依据数据访问频次与敏感等级，灵活选用不同加密算法及密钥更新方式，访问频繁的数据适配高效对称加密算法且定期更新密钥，访问稀疏的敏感数据采用高安全算法并降低更新频率，数据于云计算平台内部节点间流转，或在用户与云服务商间传输过程中，SSL/TLS协议用于加密传输通道，搭建安全通信链路，抵御数据窃取与篡改风险[4]。结合同态加密技术，既能实现对传输加密数据的安全操作，又不影响传输效率，数据处理阶段，云端分析运算的敏感数据借助同态加密技术保障隐私，无需加密的数据确保仅授权对象可解密，处理完毕后及时重新加密，当数据失去存储使用价值，先行删除加密密钥，再对磁盘等存储物理介质实施格式化、消磁等彻底销毁操作，杜绝数据恢复窃取隐患。

4.2 密钥管理体系

作为数据加密防护的关键所在，密钥管理于云计算复杂网络环境及多用户交互场景中，对保障数据安全意义重大，需构建安全高效的管理体系。密钥生成选用实践检验的可靠算法，借助复杂随机数生成机制保障其随机性与不可预知性，用户既可在本地安全环境下完成生成，也可依托可信密钥管理中心操作，依据加密算法特性及应用场景精确确定生成模式与密钥长度。密钥存储执行严格分级保护策略，用户私钥及对称加密密钥安置于智能卡、硬件安全模块等具备物理防护与加密功能的设备内，严禁以明文形式存储于云端或本地；密钥管理中心生成的密钥采用高强度加密方式存储，仅授权人员凭借多重身份验证方可访问存储系统，以此规避密钥泄漏风险。在密钥分发过程中，对称加密密钥经非对称加

密技术处理后传输，接收端利用私钥进行解密；公钥则由可信证书颁发机构认证，确保其真实性，防范中间人攻击。密钥更新依据使用频次与数据敏感程度制定相应策略，借助过渡协议达成新旧密钥的安全更替。一旦出现用户权限变更或密钥泄露情况，密钥管理中心通过发布撤销列表，或运用属性基加密的属性撤销机制，及时废止相关密钥，有效阻断安全威胁，从而保障数据在整个生命周期内的安全性。

4.3 访问控制机制

云计算环境下，将属性基加密与传统访问控制技术相融合，构建适配的访问控制机制，是保障数据安全的重要举措，准确界定用户和数据属性是关键，用户属性包含身份标识、角色定位、所在部门、权限范围等内容；数据属性则涉及敏感级别、应用方向、归属部门等要素。搭建高可靠属性数据库，运用分布式存储结合实时更新技术，实现属性的高效管理，保证信息准确完整，制定访问策略需综合考量数据与用户属性的多元特征，既可以采用基于规则的方式，规定仅销售部经理有权限访问销售数据；也能够运用基于属性的表达式，实现更精细的权限管控[5]。引入机器学习算法，依据海量访问行为数据对策略进行优化，使其更好地适配复杂多变的业务场景，用户尝试访问数据时，首先通过多因素认证机制，如密码、指纹识别、短信验证码等方式核实身份真实性，系统再根据用户属性与既定访问策略判断其权限，若满足访问条件，系统依据数据加密方式提供相应解密密钥；若不满足，则拒绝访问请求，系统还会记录访问日志，用于后续安全审计与追溯，以便及时防范潜在安全风险。

结语

云计算技术迅猛发展的当下，数据安全问题愈发突出，数据加密保护作为守护数据安全的核心手段，在云计算场景中占据无可替代的地位，本文剖析云计算环境下数据特性与加密防护诉求，探究传统及新型数据加密技术于云计算领域的应用状况，同时构思一套兼顾数据全生命周期各环节的加密保护方案，涵盖数据各阶段加密策略、密钥管理架构以及访问控制机制。此方案致力于为云计算环境中的数据安全提供更周全、更有效的防护策略，增强数据的机密性、完整性与可用性，随着云计算技术持续演进、数据安全需求不断转变，数据加密保护技术亦需持续创新改良。今后有必要深入钻研更高效、更安全的加密算法及技术，攻克密钥管理、访问控制等方面存在的难题，从而契合云计算环境发展与数据安全需求。

参考文献

[1]贺飞翔,程迪.云计算环境下的数据安全与隐私保护研究[J].电脑知识与技术,2024,20(02):69-71.DOI:10.14004/j.cnki.ckt.2024.0123.

[2]刘强兵.云计算环境下的数据隐私保护与访问控制[J].信息记录材料,2023,24(11):207-209.DOI:10.16009/j.cnki.cn13-1295/tq.2023.11.047.

[3]许广彬.云计算环境下的信息安全防护技术研究[J].电子元器件与信息技术,2023,7(07):121-124.DOI:10.19772/j.cnki.2096-4455.2023.7.030.

[4]王芳.云计算环境下计算机网络安全存储系统设计[J].电子技术与软件工程,2021,(22):256-258.DOI:10.20109/j.cnki.etse.2021.22.097.

[5]石玉峰.探讨大数据云计算环境下的数据安全问题[J].信息记录材料,2020,21(07):140-141.DOI:10.16009/j.cnki.cn13-1295/tq.2020.07.087.