云计算环境下的数据安全存储与传输协议设计

张浩麒　赵璟璇
中国电建集团华东勘测设计研究院有限公司　浙江　杭州　310000

摘　要：随着云计算的广泛应用，数据安全问题愈发关键。本文聚焦云计算环境，深入剖析其中的数据安全存储与传输协议设计。首先阐述云计算相关概念及特点，分析数据面临的数据泄露、篡改、丢失以及身份认证与访问控制等风险。进而详细探讨数据安全存储协议涉及的加密算法、完整性验证、访问控制、备份恢复策略，还有数据安全传输协议涵盖的加密、完整性保护、身份认证与密钥交换及流量控制等内容。

关键词：云计算环境下；数据安全；存储；传输协议；设计

引言：在当今数字化时代，云计算凭借其强大的资源共享与灵活配置能力，在众多领域得到迅猛发展。然而，与之相伴的数据安全问题却成为制约其进一步拓展应用的重要因素。数据在云计算环境下存储与传输时，面临诸多风险，如泄露、篡改等，严重威胁着用户与企业的利益。鉴于此，深入研究云计算环境下的数据安全存储与传输协议设计意义重大，它不仅能保障数据安全，还能增强用户对云计算服务的信任，推动云计算产业健康、可持续发展，故本文展开相关探讨。

1 云计算概述

云计算是一种基于网络的计算模式，通过虚拟化技术将计算资源、存储资源、网络资源等整合为资源池，以按需服务的形式提供给用户。其具有显著特点，虚拟化技术使物理资源得以抽象和隔离，实现多用户共享；弹性扩展可依据用户需求动态调配资源；按需服务让用户仅为实际使用的资源付费；资源池化则集中管理和分配资源，提高资源利用率。云计算主要有基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）三种服务模型，分别提供基础计算设施、开发平台和软件应用服务[1]。

2 云计算环境下的数据安全风险分析

2.1 数据泄露风险

云计算环境中，数据泄露风险多源。网络黑客常利用云平台系统漏洞，发起恶意攻击以突破安全防线，窃取存储于云端的海量数据。同时，云服务提供商内部管理若有疏忽，如员工权限设置宽泛或缺乏有效监管，可能导致个别人员恶意导出数据。再者，用户端设备若感染恶意软件，其登录云服务的账号密码等信息易被窃取，进而使云端数据面临泄露危机，给企业与个人带来难以估量的隐私与商业机密损失。

2.2 数据篡改风险

数据于云计算环境下的传输与存储过程皆面临篡改风险。在传输时，网络中的中间人可能拦截数据，将原始数据恶意修改后再转发，而接收方难以即时察觉。存储于云端的数据，若存储系统安全机制存在破绽，不法分子便能利用其获取篡改权限，悄然更改数据内容，破坏数据的准确性与完整性，使基于此数据的决策与业务运营产生严重偏差。

2.3 数据丢失风险

数据丢失在云计算场景中有多种诱发因素。云服务提供商的硬件设施一旦突发故障，如存储硬盘损坏、服务器遭遇物理损毁，且其备份机制不完善时，数据极易丢失。软件故障同样不容小觑，如数据库系统崩溃、应用程序错误操作等可能导致数据损坏或被错误删除。此外，不可抗力的自然灾害，如洪水、地震冲击数据中心，若无可靠的异地灾备方案，将造成大量珍贵数据永久性消逝。

2.4 身份认证与访问控制风险

云计算的身份认证与访问控制环节隐患重重。简单的用户名与密码认证极易被攻破，用户设置弱密码或密码遭泄露的情况屡见不鲜。多因素认证若实施存在缺陷，如生物识别不准确或动态验证码被截获，也会使认证失效。访问控制方面，若策略不够精细严密，可能出现权限过度授予或权限更新滞后等问题，导致未经授权的访问以及数据被越权使用，严重损害数据的保密性与安全性[2]。

3 数据安全存储协议设计

3.1 加密算法选择与应用

3.1.1 对称加密算法

对称加密算法使用相同的密钥进行加密和解密操作。例如AES（Advanced Encryption Standard）算法，其加密过程高效快速，能在短时间内处理大量数据。在数

据安全存储协议中，对于云端存储的大规模数据文件，可先运用对称加密算法进行加密，将数据转换为密文形式存储。密钥的生成需遵循强密码学原则，且在存储和传输过程中要严格保密。通常可采用密钥管理系统对其进行妥善保管，仅授权用户或特定安全模块可访问该密钥，从而确保数据在存储时的机密性，防止未授权方获取数据内容。

3.1.2 非对称加密算法

非对称加密算法如RSA（Rivest–Shamir–Adleman）算法，具有公钥和私钥两个不同密钥。公钥可公开，用于数据加密；私钥则由用户秘密持有，用于解密。在数据存储协议里，非对称加密算法可用于用户身份认证，服务器通过验证用户的私钥签名来确认用户身份合法性。同时在密钥交换环节，它能安全地传递对称加密算法所需的密钥。例如，客户端用服务器的公钥加密对称密钥后传输，服务器再用私钥解密获取，保障了密钥传输的安全性，并且数字签名功能可有效验证数据来源和完整性，增强数据存储的安全性与可信度。

3.1.3 混合加密方案

混合加密方案结合了对称加密和非对称加密的优势。首先，利用对称加密算法对数据进行快速加密，生成密文数据。然后，采用非对称加密算法对对称加密所使用的密钥进行加密。在数据存储时，将密文数据与加密后的对称密钥一同存储在云端。当需要访问数据时，先使用私钥解密获取对称密钥，再用对称密钥解密密文数据。这种方式既发挥了对称加密速度快的特点，适用于大量数据处理，又借助非对称加密解决了对称密钥的安全分发问题，提高了整体加密体系的安全性与灵活性，有效保障数据在云计算环境中的安全存储。

3.2 数据完整性验证机制

数据完整性验证机制对于保障云计算环境中数据的准确性与可靠性至关重要。可采用基于哈希函数的消息认证码（MAC）或数字签名技术。在数据存储时，先通过哈希函数对数据进行计算，生成固定长度的哈希值作为数据摘要。若使用MAC，将对称密钥与数据摘要结合生成消息认证码，并与数据一同存储。当读取数据时，重新计算数据哈希值并结合密钥生成新的MAC，与存储的MAC对比，若一致则数据完整。若采用数字签名，数据发送方用私钥对哈希值签名，接收方用发送方公钥验证签名及数据哈希值，相符则数据未被篡改。此机制能有效检测数据在存储过程中是否遭受恶意修改或意外损坏，确保数据的完整性，为云计算数据安全存储提供坚实保障，让用户放心将数据存储于云端。

3.3 数据存储的访问控制策略

数据存储的访问控制策略是云计算环境数据安全的关键防线。基于角色的访问控制（RBAC）模型可依据用户在组织内的角色分配权限，例如管理员、普通用户、访客等角色分别对应不同的数据访问级别，管理员可进行全面管理操作，普通用户仅能读取或修改特定范围数据，访客则仅有浏览权限。属性基访问控制（ABAC）模型则综合考虑更多属性，如用户属性（部门、职位等）、数据属性（敏感程度、所属项目等）以及环境属性（时间、地点等），更加灵活精准地定义访问规则。在数据存储协议中，通过集中式的访问控制管理系统，将这些访问策略进行存储、更新与执行。每次用户请求访问数据时，系统会根据其身份信息与请求的资源属性进行匹配判断，仅当符合既定访问规则时才允许访问，从而有效防止未经授权的访问与数据泄露，保障数据存储的安全性与合规性。

3.4 数据备份与恢复策略

对于备份策略，可采用全量备份与增量备份相结合的方式。全量备份定期对所有数据进行完整复制，虽耗时较长但能提供完整数据基线；增量备份则仅备份自上次备份以来有变化的数据，可减少备份时间与资源消耗。备份周期依据数据重要性与变化频率设定，如关键业务数据可每日全量备份或更频繁的增量备份，非关键数据可适当延长备份周期。备份数据存储于异地数据中心或云存储的不同区域，以防止本地灾难导致数据全部丢失。在恢复策略方面，当数据发生丢失或损坏时，系统依据备份索引与日志快速定位所需备份版本，按照预定恢复流程，将数据逐步恢复至指定位置或系统中，保障业务能在最短时间内恢复正常运行，减少数据丢失造成的损失与影响[3]。

4 数据安全传输协议设计

4.1 传输加密技术

在数据安全传输协议中，传输加密技术是核心要素之一，其中SSL/TLS（Secure Sockets Layer/Transport Layer Security）协议应用广泛。SSL/TLS协议通过复杂的加密算法和密钥交换机制来保障数据传输的安全性。在握手阶段，客户端与服务器首先进行通信协商，确定双方支持的加密算法套件，如AES、RSA等算法的组合方式。随后，服务器向客户端发送数字证书，包含公钥等信息，客户端验证证书的合法性，确保与可信的服务器进行通信。接着，双方利用非对称加密算法交换会话密钥，该密钥用于后续数据传输的对称加密。在数据传输过程中，使用协商好的对称加密算法对数据进行加密，

将明文数据转换为密文传输，有效防止数据在网络传输过程中被窃取或篡改。即使数据被不法分子截获，由于其缺乏解密密钥，也无法获取数据的真实内容，从而确保了数据在云计算环境下不同节点间传输的机密性与完整性，为数据安全传输提供了坚实的保障。

4.2 数据传输的完整性保护

在数据传输前，先利用哈希函数对数据进行处理，生成固定长度的哈希值，该哈希值就如同数据的“指纹”，能唯一地标识数据内容。随后将哈希值与数据一同传输。接收方在收到数据后，以相同的哈希函数对接收的数据再次计算哈希值，并与发送方传来的哈希值进行比对。若两者一致，则表明数据在传输过程中未被篡改；若不一致，则说明数据可能遭受了恶意修改或传输错误。为进一步增强完整性保护的安全性，可结合数字签名技术。发送方使用私钥对哈希值进行签名，接收方用发送方公钥验证签名的有效性，同时验证哈希值。这种双重验证机制能有效抵御中间人攻击等恶意行为，确保数据从源端到目的端的完整性，使接收方能够信任所接收的数据准确性，从而保障基于这些数据的后续业务处理或决策的正确性与可靠性。

4.3 身份认证与密钥交换协议

在身份认证环节，常采用多因素认证方式以增强安全性。例如，除了传统的用户名与密码验证外，还可结合生物特征识别（如指纹、面部识别）或动态验证码（短信验证码、令牌验证码）等。客户端与服务器在建立连接时，首先进行身份信息的交互与验证。客户端向服务器发送包含自身身份标识的请求，服务器则对客户端身份进行合法性检查，确保通信双方真实可靠，防止假冒身份的攻击者介入。在密钥交换方面，常运用Diffie-Hellman密钥交换算法或其改进版本。该算法允许客户端与服务器在不安全的公共网络环境中，通过公开的信息交换，共同协商生成一个会话密钥。其原理基于离散对数问题的复杂性，使得攻击者难以从公开信息中推导出会话密钥。在交换过程中，双方利用各自的私钥和对方的公钥进行计算，最终得到相同的会话密钥。

4.4 传输过程中的流量控制与拥塞避免

采用滑动窗口协议可有效实现流量控制，发送方维护一个发送窗口，窗口大小代表在未收到接收方确认时能够发送的数据量。发送方依据接收方反馈的接收窗口大小以及自身网络状况动态调整发送窗口，确保发送速率与接收方处理能力及网络带宽相匹配。例如，当接收方处理速度较慢或网络拥塞时，接收窗口变小，发送方相应减少发送量，避免接收方缓冲区溢出导致数据丢失。拥塞避免机制则侧重于预防网络拥塞的发生与缓解拥塞程度。常见的如慢启动算法，发送方初始以较小的拥塞窗口发送数据，随后根据收到的确认信息逐步增大拥塞窗口，但增速呈指数递减，防止网络瞬间过载。同时结合拥塞避免算法，当拥塞窗口增长到一定阈值后，进入线性增长阶段，更精准地控制数据注入网络的速率。一旦检测到拥塞（如超时未收到确认或收到特定拥塞信号），则迅速减小拥塞窗口，重新进入慢启动过程[4]。

结束语

在云计算技术蓬勃发展的当下，本研究深入探索了其环境下的数据安全存储与传输协议设计。通过对各类风险的剖析与应对策略的构建，从加密算法、完整性验证、访问控制到备份恢复以及传输中的加密、认证与流量管理等多方面提出了全面的解决方案。虽已取得一定成果，但云计算技术仍在持续演进，未来需进一步关注新兴技术对数据安全的潜在影响，不断优化协议以适应更复杂多变的应用场景，为云计算数据安全保驾护航，推动云计算产业在安全轨道上稳健前行。

参考文献

[1]温俊香.浅析云计算环境下分布式缓存技术在物联网中的应用[J].信息记录材料,2023,24(08):149-151.

[2]王颖.云计算环境下舰船控制系统大数据有效存储方法[J].舰船科学技术,2023,45(13):170-173.

[3]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.

[4]吴云.基于云计算环境分析计算机网络安全技术的优化[J].中国设备工程,2023,(09):113-115.