

云计算环境下开放式网络数据安全存储方法

郭广朋

潍坊职业学院 山东 潍坊 261000

摘要: 云计算开放式网络具备动态接入、跨域交互与资源共享等特点,使其数据存储面临泄露、篡改、非法访问等多重安全威胁,传统安全存储方法存在适配性弱、管控僵化、预警滞后等诸多缺陷。本文结合云存储技术原理与安全评价标准,提出动态加密、精细化访问控制及全流程溯源监控的优化方案。实验证明,该方法可有效规避各类存储风险,平衡安全防护与运行效率,能够较好适配开放式网络的数据存储应用需求。

关键词: 云计算环境; 开放式网络; 数据安全; 存储方法

引言: 数字化时代下,云计算技术广泛普及,开放式网络打破传统网络边界限制,实现多主体、跨平台的数据交互与资源共享,极大提升了数据存储与流转效率。但开放性、动态性的网络特征导致云存储安全边界模糊,各类网络攻击与数据安全问题频发,现有防护机制难以适配复杂动态的存储场景。为此,本文深入分析存储安全风险与现存问题,探索科学可行的安全存储优化方法,为云数据安全防护提供有效技术支撑。

1 云计算开放式网络数据安全存储相关理论与技术基础

1.1 云计算与开放式网络核心概念

(1) 云计算架构模式分为IaaS、PaaS、SaaS三层架构,分层实现资源虚拟化、按需调度与共享交付。其存储服务具备虚拟化、分布式、弹性扩容、按需付费的核心特性,可突破传统存储硬件局限,适配海量网络数据存储需求。(2) 开放式网络是打破封闭局域网壁垒、支持多主体接入的开放式互联网络形态,具备开放性、异构性、动态性、互联互通的特征。网络节点可自由接入退出,依托通用协议实现跨平台、跨区域数据交互,运行机制灵活且去中心化。(3) 云环境下开放式网络数据存储采用“网络传输+云端分布式存储”运行模式,外部网络数据经安全校验后接入云平台,分散存储于多节点服务器,依托云端调度机制实现数据统一管理、动态调用与实时更新。

1.2 数据安全存储核心技术

(1) 数据加密存储技术是安全存储的基础,核心原理是通过加密算法转换数据明文,仅授权主体可解密读取。主要分为对称加密、非对称加密及混合加密,分别适配批量数据加密、密钥安全传输等不同场景。(2) 数据备份与容灾恢复技术通过定期全量、增量备份留存数据副本,针对网络故障、硬件损坏、恶意攻击等风险,

依托异地容灾、快速恢复机制,保障数据意外丢失后可快速复原,维持存储服务连续性。(3) 数据访问控制与身份认证技术通过账号权限分级、身份核验机制,甄别访问主体合法性。结合密钥认证、多因素认证等方式,杜绝非法接入与越权操作,从访问源头规避数据泄露、篡改风险^[1]。

1.3 云环境数据安全存储评价标准

(1) 数据安全以保密性、完整性、可用性为核心评价指标。保密性保障数据不被非法获取,完整性防止数据被篡改破坏,可用性确保合法用户可随时正常调取数据,三项指标共同构成云存储安全效果的基础评价体系。(2) 开放式网络数据传输与存储安全规范,明确了数据加密传输、节点接入审核、流转日志留存、数据共享管控等要求,规范跨网络、跨节点的数据交互与存储行为,有效规避传输拦截、数据篡改等安全问题。(3) 云计算平台安全合规相关标准涵盖数据隐私保护、安全审计、风险管控、合规存储等内容,对云平台的存储架构、防护机制、操作规范进行约束,确保数据存储、管理与流转全过程符合行业规范与安全监管要求。

2 云计算环境下开放式网络数据存储安全风险与现存问题

2.1 开放式网络数据存储安全风险类型

(1) 数据泄露与非法窃取风险。开放式网络具备接入自由、数据交互频繁的特点,边界防护较为薄弱。在云数据存储与传输过程中,黑客可通过网络漏洞、爬虫抓取、恶意节点接入等方式窃取用户隐私数据与业务核心数据。同时开放式网络多主体共享资源的模式,使得数据在流转、共享、同步环节极易出现外泄问题,一旦防护疏漏,会造成大规模数据泄露,引发隐私泄露、信息滥用等安全问题。(2) 数据篡改与损坏风险。云平台数据多采用分布式存储模式,数据分散存储在多个节

点设备中。开放式网络环境下,非法攻击者可利用网络协议漏洞、节点安全缺陷入侵存储系统,恶意篡改、删除数据内容。此外,网络波动、设备故障、病毒攻击等突发问题,也会导致存储数据出现损坏、缺失、错乱等情况,直接破坏数据完整性,影响数据后续使用价值。

(3) 非法访问与越权操作风险。开放式网络接入主体繁杂、终端类型多样,缺乏固定安全边界。部分非法用户可通过破解账号、伪造身份等方式绕过基础防护机制访问云端存储数据。同时系统内部授权管理不完善,易出现用户权限冗余、权限混用问题,合法用户越权访问、调取、修改非权限内数据的情况频发,严重威胁云存储数据安全。

2.2 现有安全存储方法存在的缺陷

(1) 传统加密技术适配性不足,无法适配开放式网络动态特性。传统加密算法多适用于封闭、静态的网络存储场景,加密解密流程固定。而开放式网络节点动态增减、数据实时流转、交互场景多变,传统加密技术密钥更新滞后、加密模式固化,难以适配动态数据存储需求,易出现加密失效、解密卡顿等问题。(2) 访问控制机制僵化,精细化管控能力缺失。当前多数云平台沿用静态访问控制策略,权限分配多为一次性配置,无法根据用户身份、访问场景、数据等级动态调整权限。针对开放式网络复杂的访问行为,无法实现最小权限管控,对临时访问、跨域访问等特殊场景缺乏有效约束,管控漏洞较多^[2]。(3) 数据动态监控与风险预警能力薄弱。现有安全系统多以事后检测、被动防护为主,对云端数据流转、节点访问、数据操作等行为的实时动态监控力度不足。难以提前识别异常访问、数据批量传输、恶意篡改等风险行为,风险预警滞后,往往在安全问题发生后才能发现,无法实现事前预防、事中管控。

2.3 云环境下数据存储安全管理痛点

(1) 多租户场景下数据隔离难度大。云计算平台支持多租户资源共享,多个用户、企业数据存储于同一云端硬件架构。部分云平台隔离技术不完善,逻辑隔离强度不足,容易出现租户数据交叉泄露、数据混淆等问题,难以彻底实现不同租户数据的独立存储与安全隔离。(2) 开放式网络数据流转追踪困难。开放式网络数据跨节点、跨平台流转频繁,数据共享、传输、复制路径复杂且动态多变。现有管理体系缺乏全流程溯源机制,无法精准记录数据流转轨迹、操作主体与操作行为,数据出现安全问题后难以定位风险源头,追责与整改难度较大。(3) 安全防护与存储效率难以平衡。高强度的加密、监控、隔离等安全防护手段会占用大量云端

算力与网络资源,降低数据存储、调取、传输速率。若侧重提升存储效率、保障数据交互速度,又会简化安全防护策略,产生安全漏洞,导致云存储系统长期存在安全与效率难以兼顾的矛盾问题。

3 云计算环境下开放式网络数据安全存储优化方法

3.1 适配开放式网络的动态加密存储方法

(1) 基于场景自适应的混合加密算法优化。针对开放式网络动态接入、数据流转频繁、场景复杂多变的特点,本文优化传统单一加密模式,构建场景自适应混合加密算法体系。结合对称加密高效解密、非对称加密高安全的双重优势,根据网络负载、数据体量、传输场景自动切换加密模式。针对海量普通数据采用轻量化对称加密提升效率,针对核心涉密数据采用非对称加密强化防护,有效解决传统算法适配性差、安全与效率失衡的问题,适配开放式网络动态运行特性。(2) 数据分层分类加密存储策略设计。依据云端数据的保密等级、应用价值、使用频次,对存储数据进行分层分类划分,实施差异化加密存储策略。将数据划分为公开数据、普通业务数据、核心隐私数据三个层级,分别匹配不同强度的加密标准与存储方案。低层级数据简化加密流程、保障存取效率,高层级数据采用多重加密叠加防护,杜绝高强度加密资源浪费,实现精细化、差异化的安全存储管控^[3]。(3) 加密密钥动态管理与更新机制。针对传统密钥固定、易泄露、难管控的缺陷,搭建动态密钥管理体系。依托云端算力实现密钥定时自动更新、随机迭代,针对跨网络传输、高频访问、异常操作场景触发密钥实时刷新,避免密钥长期使用产生破解风险。同时建立密钥分级存储、授权调取机制,规范密钥使用权限,杜绝密钥泄露、滥用问题,全方位提升加密存储安全性。

3.2 精细化动态访问控制存储机制

(1) 基于用户角色与场景的多级权限划分。结合开放式网络多主体接入的特征,摒弃传统静态权限分配模式,构建角色、场景、数据三维多级权限体系。按照用户岗位、身份、业务职能划分访问角色,匹配最小权限原则分配操作权限,同时结合访问时间、终端设备、网络环境动态调整权限范围,杜绝权限冗余、越权预留漏洞,实现精准化权限管控。(2) 开放式网络数据访问行为实时管控。针对开放式网络访问行为繁杂、场景多变的问题,搭建全维度访问行为管控机制。对用户的数据查询、下载、修改、共享、删除等操作进行实时记录与合规校验,针对跨域访问、批量数据调取、陌生终端接入等特殊行为强化管控力度,实时约束用户操作行为,规避违规操作带来的数据安全风险。(3) 异常访问行为

识别与拦截机制。依托大数据分析 with 智能算法,构建异常访问识别模型,精准识别暴力破解、频繁试错、异地异常登录、批量窃取数据等风险行为。系统可对异常操作进行实时拦截、访问冻结,同步推送风险提示,主动阻断非法访问路径,从源头防范非法接入与恶意操作,提升云存储访问安全防护能力^[4]。

3.3 数据全流程安全监控与溯源存储方法

(1) 数据存储、传输、调用全流程监控体系构建。围绕数据上云、存储、传输、调用、共享、下线全生命周期,搭建全方位动态监控体系。实时监测云端节点运行状态、数据流转轨迹、用户操作行为,全覆盖排查网络漏洞、设备故障、异常操作等安全隐患,改变传统事后防护模式,实现数据安全事前预防、事中管控、事后留存的全流程防护。(2) 基于区块链的数据存储溯源技术应用。利用区块链去中心化、不可篡改、可全程追溯的技术特性,将数据存储、访问、流转、修改等所有操作信息实时上链存证。每一项操作均生成唯一溯源标签,全程记录操作主体、时间、内容、路径,数据信息不可篡改、可永久查询,有效解决开放式网络数据流转追踪难、责任界定模糊的问题,实现数据安全可溯源、可追责^[5]。(3) 安全风险实时预警与应急处置策略。构建智能化风险预警模型,整合监控数据、访问日志、网络状态等信息,通过算法实时研判安全风险等级,针对数据泄露、篡改、异常访问等隐患实现分级预警。同时配套完善应急处置方案,针对不同安全风险启动对应防护预案,快速隔离风险、修复漏洞、恢复数据,最大限度降低安全事故造成的损失。

3.4 优化方法性能与安全性验证

(1) 实验环境与评价指标设置。为验证优化方法的可行性与优越性,搭建模拟云计算开放式网络实验环境,配置多租户节点、动态网络接入场景、海量模拟存储数据。从安全性能与存储效率两大维度设置评价指标,安全指标包含数据保密性、完整性、抗攻击能力、风险拦截率;效率指标包含数据加密速率、存取响应时

间、资源占用率,为实验测试提供标准化依据。(2) 安全性能对比测试与结果分析。将本文优化方法与传统安全存储方法进行对比测试,模拟网络攻击、非法访问、数据篡改、数据泄露等多种风险场景。测试结果表明,优化后的动态加密与访问控制机制,可有效抵御各类网络攻击,异常行为拦截率显著提升,数据篡改、泄露风险大幅降低,数据存储的保密性与完整性得到有效保障,安全防护能力优于传统方法。(3) 存储效率与实用性验证分析。通过多组对比实验检测优化方法的资源占用、数据存取速率、加密解密耗时等核心指标。实验证明,该优化方法在强化安全防护的同时,通过自适应加密、精细化权限管控减少了无效算力消耗,有效平衡了安全防护与存储效率,适配开放式网络动态、高频、跨域的数据存储场景,具备良好的实用性与落地应用价值。

结束语

本文系统分析云计算开放式网络数据存储的安全风险与技术短板,从动态加密、访问管控、全流程监控溯源三个维度构建完整的安全存储优化体系,有效解决了传统方案防护僵化、溯源困难、安全与效率失衡等问题。实验验证该优化方法防护性能优异、实用性较强。后续将持续优化智能预警与容灾机制,适配更多复杂网络场景,进一步提升云平台数据存储的智能化安全防护水平。

参考文献

- [1]田瑞.云计算环境下的数据安全与隐私保护[J].电子元件与信息技术,2024,8(4):163-165.
- [2]胡雅茹.云计算环境下网络安全数据存储系统设计[J].网络安全和信息化,2023,10(5):43-45.
- [3]饶超影,赵金萍.云计算环境下数据存储安全问题的研究[J].数码世界,2023,23(12):73-74.
- [4]梁仲峰.云计算环境中的数据安全与隐私保护方法[J].长江信息通信,2025,38(6):167-169.
- [5]周小燕.云计算技术在计算机网络安全存储中的应用研究[J].电脑知识与技术,2022,18(15):28-33.