云计算环境下通信信息存储与管理的创新模式

赵　坚
内蒙古电信股份有限公司通辽分公司　内蒙古　通辽　028000

摘　要：通信信息数据量爆发式增长使传统存储与管理模式陷入容量、效率、成本困境，云计算为突破这些难题提供新路径。探索其环境下的创新模式，既能实现数据存储弹性扩展与管理流程高效协同，突破传统局限，又能为通信行业数字化转型提供技术支撑。这项研究可丰富云计算在通信领域的应用理论，还能帮助企业优化信息资源配置、提升数据价值挖掘能力，为通信行业在数字时代实现高质量发展提供实践参考。

关键词：云计算；通信信息；存储创新模式；管理创新模式；数据安全

引言

当前通信行业信息数据呈现海量性、实时性、异构性特点，5G、物联网技术普及更使数据量呈指数级增长，传统存储模式因固定容量限制面临扩容难题，管理流程也因数据类型复杂导致效率低下，难以满足行业发展需求。云计算具备资源共享、弹性伸缩、成本优化等优势，可灵活适配通信数据存储与管理需求，为模式创新提供技术可能。但二者融合中存在模式适配不足、安全风险等问题，因此构建科学创新模式框架，推动通信信息管理升级，对行业发展意义重大。

1 云计算环境下通信信息存储的创新模式设计

1.1 基于混合云架构的分层存储模式

基于混合云架构的分层存储模式，关键是按照通信信息的重要程度与使用频次划分存储层级。对于涉及用户隐私、业务核心的敏感数据（像用户身份信息、核心网络配置数据），采用私有云存储，凭借私有云专属资源池、独立访问权限的特性，确保数据安全性与可控性；对于非核心、访问频次低的数据（如历史通信日志、非关键业务备份数据），则存入公有云，利用公有云海量存储资源与按需付费模式，降低企业硬件投入与运维成本。

在此基础上，通过建立统一的混合云管理平台，实现私有云与公有云之间的数据动态迁移与协同管理。当私有云存储资源接近饱和时，系统自动将部分低频访问数据迁移至公有云，释放私有云空间用于存储更关键的数据；当需要访问公有云中的特定数据时，又能通过安全通道快速调取，确保数据的可用性与及时性。同时，该模式还支持多租户环境下的资源隔离与权限控制，不同业务部门可根据自身需求分配独立的存储空间与访问权限，避免数据交叉干扰，提升整体存储效率与管理水平。

1.2 面向实时通信数据的动态弹性存储模式

面向实时通信数据（如 5G 语音通话数据、物联网设备实时传输数据）的动态弹性存储模式，核心在于 “按需调整、智能分配”。依托云计算的弹性伸缩技术，当数据流量高峰到来（如节假日通信高峰、大型活动数据传输峰值），系统可自动扩容存储资源，增加服务器节点与存储容量，避免数据拥堵或丢失；当流量回落时，自动缩减资源规模，减少闲置浪费。同时，结合智能负载均衡算法，将实时数据分散到不同存储节点，平衡各节点负载压力，保障数据写入与读取速度，满足实时通信业务对存储延迟的严格要求。

为实现这种动态调整，系统需配备实时流量监测模块，持续收集并分析数据流量变化趋势。通过机器学习算法对历史流量数据进行训练，预测未来流量走向，为资源扩容或缩减提供决策依据。此外，该模式还应具备智能故障转移功能，当某个存储节点出现故障时，能迅速将数据迁移至其他正常节点，确保数据存储的连续性与稳定性。通过这些技术手段，面向实时通信数据的动态弹性存储模式能够有效应对数据流量的不确定性，提升存储资源的利用率与通信业务的服务质量。

1.3 结合边缘计算的分布式存储模式

结合边缘计算的分布式存储模式，重点解决通信数据“就近存储、快速响应”的问题。在通信网络边缘部署边缘节点（如基站边缘服务器、区域边缘云），对本地产生的实时数据（如智慧城市终端数据、工业物联网设备数据）进行本地化存储，减少数据向远端云端传输的延迟，提升业务响应速度，尤其适用于自动驾驶、远程医疗等对时延敏感的通信场景。同时，边缘节点与云端建立协同备份机制，边缘存储的数据定期同步至云端，形成“本地存储+云端备份”的双重保障，既确保数据实时可用，又避免因边缘节点故障造成的数据丢失。

为进一步优化这种分布式存储模式，边缘节点采用

轻量级存储架构设计，降低硬件资源消耗与部署成本。通过分布式哈希表（DHT）技术，实现数据在边缘节点间的快速定位与访问，无需依赖中心化索引服务器，提升系统可扩展性与容错性。同时，边缘节点内置数据预处理模块，对采集的原始数据进行初步筛选、压缩与加密，减少无效数据传输与存储开销，保障数据安全性。此外，结合软件定义存储（SDS）技术，实现边缘存储资源的虚拟化管理与动态调配，根据业务需求灵活分配存储空间与计算资源，提升资源利用率。通过这些技术手段，结合边缘计算的分布式存储模式能够有效满足低时延、高可靠性的通信业务需求，推动通信网络向智能化、边缘化方向发展。

2 云计算环境下通信信息管理的创新流程构建

2.1 数据全生命周期的智能化管理流程

数据全生命周期的智能化管理流程，覆盖通信信息从产生到销毁的完整环节，通过云计算与 AI 技术实现各环节自动化。在数据采集阶段，借助云平台接口对接各类通信设备，自动采集语音、文本、视频等异构数据；清洗阶段利用 AI 算法识别并剔除冗余、错误数据，统一数据格式；分析阶段通过云算力支撑大数据分析模型，提取数据价值；归档阶段根据数据重要性自动分类存储至对应云存储层级；销毁阶段按照预设规则，对过期或无用数据执行安全删除，全程无需人工干预，大幅提升管理效率，减少人为操作误差。

在数据存储阶段，智能化管理流程会依据数据的使用频率、重要性以及安全需求等指标，将数据分配到最合适的存储位置，如高频访问数据存于高速缓存层，重要且不常访问数据存于冷存储层，确保存储资源的优化配置。同时，利用区块链技术实现数据存储的不可篡改与可追溯，增强数据的安全性与可信度。在数据共享阶段，通过智能合约技术自动执行数据访问权限控制，确保只有授权用户或系统能够访问特定数据，且访问行为被完整记录，便于审计与追溯。此外，智能化管理流程还支持跨云平台的数据共享与协同，打破数据孤岛，促进通信信息的流通与价值最大化。通过这些技术手段，数据全生命周期的智能化管理流程能够显著提升通信信息的管理效率与安全性，为云计算环境下的通信业务提供有力支撑。

2.2 多主体协同的权限管理模式

多主体协同的权限管理模式，针对通信行业涉及运营商、合作企业、用户等多主体的特点，构建精细化权限体系。采用基于角色的访问控制（RBAC）机制，为不同主体分配专属角色，例如运营商管理员拥有数据管理全权限，合作企业仅获取授权业务数据访问权限，用户仅可查看个人通信数据。同时，建立跨部门数据共享授权流程，当不同部门或合作方需要共享数据时，通过云平台提交授权申请，经审批后生成临时访问权限，权限到期自动回收，既满足数据共享需求，又防止数据越权访问，维护数据安全与隐私。

为进一步强化权限管理的灵活性，该模式引入动态权限调整机制。根据主体角色变化、业务需求变动或安全风险评估结果，系统自动调整权限配置，例如当合作企业业务范围扩展时，其数据访问权限可同步更新；若检测到异常访问行为，立即限制或撤销相关权限。此外，通过多因素身份认证技术（如生物识别、动态令牌等）增强权限验证强度，确保只有合法主体能够获取对应权限。在权限审计方面，利用区块链技术记录所有权限分配、调整及访问行为，形成不可篡改的审计日志，支持实时查询与追溯，为安全合规提供可靠依据。这种多主体协同的权限管理模式，有效平衡了数据共享与安全防护的需求，为云计算环境下的通信信息管理提供了精细化、动态化的安全保障。

2.3 基于大数据分析的信息价值挖掘管理模式

基于大数据分析的信息价值挖掘管理模式，依托云计算强大算力，深度挖掘通信信息的潜在价值。通过构建用户行为分析模型，分析用户通信时长、业务偏好、地域分布等数据，为运营商精准推送套餐、优化服务提供依据；针对业务数据，通过趋势预测模型分析通信流量变化、网络负载波动，提前规划网络资源配置，避免网络拥堵；还可挖掘数据中的异常模式，如异常通话行为、数据传输异常，为反欺诈、网络安全防护提供预警支持，将通信信息从“存储资产”转化为“决策资产”，提升企业核心竞争力。

该模式还注重数据的关联性分析，通过整合不同来源、不同类型的通信信息，发现数据间的潜在联系。例如，将用户的社交网络数据与通信消费数据相结合，能够更全面地了解用户的社会关系和消费习惯，为个性化营销和服务定制提供更丰富的依据。同时，利用机器学习算法对海量通信数据进行深度挖掘，不断优化分析模型，提高信息价值挖掘的准确性和效率。在数据更新方面，基于大数据分析的信息价值挖掘管理模式能够实时捕获新的通信信息，并及时将其纳入分析体系，确保挖掘结果的时效性和实用性。此外，该模式还支持与外部数据源的对接和融合，引入行业报告、市场调研等外部数据，拓宽信息价值挖掘的视野，为通信企业提供更具前瞻性和战略性的决策支持，助力企业在激烈的市场竞

争中占据优势地位。

3 云计算环境下通信信息存储与管理的安全保障体系

3.1 数据传输与存储过程中的加密防护机制

数据传输与存储过程中的加密防护机制，从 “端到端” 全链路确保通信信息安全。传输阶段采用 TLS/SSL 协议对数据进行加密，确保数据在通信设备与云平台、边缘节点与云端之间传输时，即便被截取也无法解密；存储阶段采用分布式加密存储技术，将数据分割为多个片段，每个片段用不同密钥加密后存储在不同云节点，单一节点泄露无法还原完整数据。

同时，引入同态加密技术，允许在加密数据上直接进行计算操作，无需解密即可获取计算结果，既保障了数据安全性，又满足了数据处理需求。为应对密钥管理难题，采用密钥分层管理与分发机制，主密钥由安全中心统一管理，工作密钥由各节点独立生成与更新，并通过安全通道分发，确保密钥的安全性与可用性。此外，建立数据完整性校验机制，在数据传输与存储过程中，利用哈希算法生成数据指纹，定期比对校验，及时发现数据篡改或损坏情况，确保数据的完整性与一致性。这种全方位的加密防护机制，为云计算环境下的通信信息存储与管理构建了坚实的安全防线。

3.2 面向云平台的实时安全监控与风险预警体系

面向云平台的实时安全监控与风险预警体系，通过多维度监测及时发现安全威胁。利用云平台自带的安全监控工具，实时采集存储节点、管理系统的运行数据，如数据访问日志、资源占用情况；借助 AI 异常检测算法，识别异常行为，如高频次数据访问、非授权 IP 登录、异常数据传输量，一旦发现异常立即触发预警；同时，定期对云平台进行漏洞扫描，检测系统漏洞与配置缺陷，生成漏洞修复报告，指导运维人员及时修补，形成 “实时监控 - 异常预警 - 漏洞修复” 的闭环防护，保障云平台安全稳定运行。

为进一步提升风险预警的精准度，该体系还引入了威胁情报共享机制。通过与行业内的安全组织、其他云平台建立情报交互渠道，实时获取最新的威胁情报信息，如新型攻击手段、恶意软件特征等。将这些外部情报与内部监测数据相结合，利用大数据分析技术进行深度挖掘，能够更准确地判断安全威胁的类型、来源和潜在影响范围，提前制定针对性的防范策略。此外，针对不同级别的安全预警，设定了差异化的响应流程。对于一般性安全事件，系统自动记录并通知相关运维人员关注；对于重大安全威胁，则立即启动应急响应机制，自动切断相关网络连接，阻止威胁进一步扩散，并通知安全专家团队进行深入调查和处理，确保云平台在面对各种安全挑战时能够迅速、有效地做出应对。

3.3 基于合规要求的数据备份与灾难恢复机制

基于合规要求的数据备份与灾难恢复机制，依据《数据安全法》《个人信息保护法》等法规，构建完善的数据保障体系。采用多副本备份策略，将通信数据在不同地域、不同云存储介质（如对象存储、块存储）中生成多个备份，避免单一存储介质故障导致数据丢失；制定跨地域容灾方案，在远离主数据中心的区域建立灾备中心，当主中心遭遇自然灾害、网络攻击等灾难时，灾备中心可快速接管业务，恢复数据访问。

4 结论

云计算环境下通信信息存储与管理创新模式，以存储创新为基础、管理创新为核心、安全保障为支撑，三者协同作用形成完整体系。存储模式通过混合云分层、动态弹性、边缘分布式设计，解决数据存储容量与效率问题；管理流程借助全生命周期智能管理、多主体权限协同、大数据价值挖掘，提升数据管理效率与价值；安全体系通过加密防护、实时监控、备份容灾，保障数据安全与业务连续。创新模式需遵循 “技术适配、安全优先、价值导向” 原则，兼顾行业特性与数据保护需求。

参考文献

[1]梁雷.基于Reactor模式的通信信息安全存储多重加密方法[J].长江信息通信,2024,37(12):143-145+154

[2]殷文霞.区块链技术下大规模电子通信信息存储方法[J].机电产品开发与创新,2023,36(06):86-88

[3]付鋆,刘俊荣,周泽元.基于双混沌映射的通信信息安全存储多重加密[J].信息技术,2023,(07):87-91