



多云存储关键技术研究进展

鲍禹含¹, 付印金^{1,2}, 陈卫卫¹

(1. 陆军工程大学 指挥控制工程学院, 南京 210001; 2. 军事科学院 系统工程研究院, 北京 100039)

摘 要: 传统单云存储在数据安全与服务弹性方面存在数据隐私泄漏及难以满足在线实时应用需求等缺陷, 而多云存储技术能够通过虚拟化集成多个云供应商的在线存储服务实现统一存储、性能调优、数据安全与隐私保护等一系列功能, 最大化地挖掘云存储资源价值。介绍多云存储技术的概念、系统架构及其优势, 阐述多云存储技术在数据可用性、完整性、一致性和安全性方面存在的主要技术挑战, 重点分析并总结多云存储各项关键技术的国内外研究现状, 包括纠删码容错技术、数据完整性证明机制、并发控制方法以及安全重删技术, 在此基础上, 指出现有多云存储技术研究中存在的不足, 并对未来发展方向进行探讨和展望。

关键词: 多云存储; 纠删码; 完整性证明; 并发控制; 安全重删技术

开放科学(资源服务)标志码(OSID):



中文引用格式: 鲍禹含, 付印金, 陈卫卫. 多云存储关键技术研究进展[J]. 计算机工程, 2020, 46(10): 18-32, 40.

英文引用格式: BAO Yuhan, FU Yinjin, CHEN Weiwei. Research progress on key technologies of multi-cloud storage[J]. Computer Engineering, 2020, 46(10): 18-32, 40.

Research Progress on Key Technologies of Multi-Cloud Storage

BAO Yuhan¹, FU Yinjin^{1,2}, CHEN Weiwei¹

(1. College of Command and Control Engineering, Army Engineering University of PLA, Nanjing 210001, China;

2. Institute of System Engineering, PLA Academy of Military Sciences, Beijing 100039, China)

[Abstract] Traditional single-cloud storage leads to data security and service flexibility problems, such as data privacy leakage and difficulty in meeting the needs of online real-time applications. Multi-cloud storage technology uses virtualization to integrate the online storage services of multiple cloud providers, so as to realize functions such as unified storage, performance tuning, data security and privacy protection, maximizing the value of cloud storage resources. This paper introduces the concept of multi-cloud storage technology, as well as its system architecture and advantages. Then the paper describes the main technical challenges of multi-cloud storage technology in data availability, integrity, consistency and security. And it focuses on analyzing and summarizing the research status of key techniques of multi-cloud storage, including erasure code-based fault tolerance, proof mechanism of data integrity, concurrency control method and secure deduplication technique. Finally, according to the weaknesses of the current research works on multi-cloud storage technology, this paper analyzes several potential further research directions.

[Key words] multi-cloud storage; erasure code; integrity proof; concurrency control; secure deduplication technology

DOI: 10.19678/j.issn.1000-3428.0058345

0 概述

云存储是利用集群计算、虚拟化、效用计算和分布式文件系统等技术将网络中大量不同类型的存储设备通过应用软件集合起来协同工作, 共同对外提供在线数据存储和业务访问功能的系统^[1]。用户可

随时通过网络连接按需使用云端存储资源^[2], 不仅在数据管理和维护上更为便捷, 还能较好地解决本地存储自身的不可扩容、不方便携带、数据丢失恢复困难等问题。然而, 随着云存储的发展与广泛应用, 传统单一云存储服务固有的缺陷逐渐暴露出来^[3]。首先, 企业和用户会遇到供应商锁定问题, 过分依赖

基金项目: 江苏省自然科学基金面上项目(BK20191327); 陆军工程大学基础前沿科技创新项目(201933)。

作者简介: 鲍禹含(1992—), 女, 硕士研究生, 主研方向为云存储、服务计算; 付印金, 讲师、博士; 陈卫卫, 教授。

收稿日期: 2020-05-18 修回日期: 2020-06-29 E-mail: yinjinfu@gmail.com

于单一供应商的产品和服务,在不产生大量切换成本的情况下无法进行灵活迁移。其次,企业和用户将数据全部交给一个供应商保管,失去对数据的控制权,若供应商内部人员出现问题,很容易获取用户的所有信息,数据隐私泄漏在所难免。再次,若供应商停止服务或遭遇故障,客户将面临数据全部丢失的风险,造成不可挽回的经济损失。此外,智能终端设备迅猛发展,对数据处理时延和网络带宽的需求越来越高,单云存储很难满足在线实时应用的需求。通过多个云存储提供商进行对等协作服务,能够较容易地解决以上问题。

多云协作服务思想为企业提供云计算模式。2008 年, Cisco 公司提出 Inter-Cloud^[4], 试图通过使用其他云服务提供者的计算、存储或其他任意类型的资源, 解决单一云服务提供者物理资源有限或地理上难以实现无处不在的覆盖等所带来的服务质量问题。2013 年, Multi-Cloud 概念被提出^[5], 旨在通过更多云服务提供者共存的软硬件基础设施冗余优化容错能力, 降低云用户数据丢失或云计算环境中局部构件失效所引起的宕机等情况下产生的服务中断风险, 提高性能, 避免云平台锁定。2015 年, 欧盟开展 SuperCloud 项目研究^[6], 强调以用户为中心, 试图跨多个云服务提供者构建全套透明的计算、存储和数据通信服务, 权衡安全性、可用性、成本开销和处理突发负载等因素。Federated Cloud 项目^[7]在多个未建立信任关系的云服务提供者之间, 通过部署和管理多个内外部云计算服务来匹配业务需求, 支持若干个独立云平台合作完成一个目标任务。另外, Cloud Service Broker^[8]为云服务提供者与云服务消费者提供咨询、集成和协商谈判服务, 不仅可通过对云服务提供者的服务集成与定制, 为云服务消费者提供更优质的云服务, 还可通过创新渠道和市场机会, 为云服务提供者增长销量。国内王怀民院士团队近年提出的云际计算 (JointCloud Computing) 概念^[9]是以多个云服务实体之间开放协作为基础, 通过多方云资源深度融合, 方便开发者通过“软件定义”方式定制云服务, 创造云价值的新一代云计算模式。

随着多云协作计算模式的发展, 多云存储成为围绕多个云存储服务进行协作的新一代云存储技术。国内外学术界和工业界的学者已经对多云存储开展大量研究, 并取得较多研究成果。本文主要介绍多云存储技术的概念、系统架构、优势以及主要技术挑战, 并分析和总结多云存储中 4 项关键技术的国内外研究现状。

1 多云存储技术

1.1 多云存储技术概念

多云存储通过代理将多个供应商的不同云存储服务虚拟化联合管理, 实现统一存取、性能调优、安

全可靠等一系列功能, 以此来降低存储成本、提高效率, 最大化地挖掘数据价值, 保证高可用的业务连续性。在部署上既可以使用物理/虚拟的公有云或私有云进行部署, 也可以实现两者的混合部署。多云存储能很好地改善单云存储存在的供应商锁定、数据丢失、隐私保护、性能瓶颈等方面的局限性。

1.2 多云存储系统架构

目前, 国内外学者已提出了多种多云存储系统架构, 依据存储代理布局差异, 本文将其大致分为集中式代理架构和地理分布式代理架构。多云存储集中式代理架构如图 1 所示。为能够统一协调优化所有用户的数据, 并确保数据隐私安全, 通常将多云存储代理部署在本地或私有云等可信任的位置, 连接用户和不可信的各大云存储供应商。该系统大致分为数据处理层、选取存储策略层以及数据库层 3 个部分。数据处理层负责对用户上传的数据进行分块、加密、重删等操作; 选取存储策略层负责根据实际情况和不同策略计算出数据最佳存储策略; 数据库层负责存储元数据以及缓存热数据。SafeStore^[10]、NCCloud^[11]、Hybris^[12]、StoreSim^[13]、F2MC^[14]等都属于集中式代理架构。

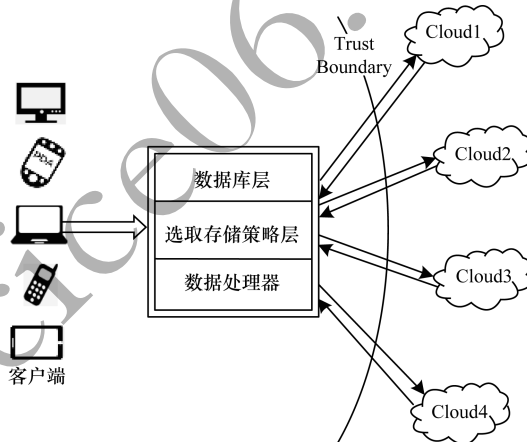


图 1 多云存储集中式代理架构

Fig. 1 Centralized agent architecture of multi-cloud storage

海量数据迅速增长和地理位置分散的特点, 使得集中式架构中负载集中和远距离传输的缺陷渐渐暴露出来, 越来越高的响应延迟导致一个中心代理无法满足用户对性能的需求, 因此, 地理分布式代理架构应运而生。根据代理功能布局差异, 本文将多云存储的地理分布式代理架构分为半集中式代理架构和分散式代理架构。多云存储半集中式架构如图 2 所示, 根据地理位置部署多个代理系统, 每个多云代理系统帮助管理分发其附近用户的数据到各大云供应商, 各代理间通过中心协调服务统一协调传递信息, 保持数据一致性。半集中式代理架构相比集中式代理架构具有更好的扩展性, 且对地理分散的用户依然能保持良好的性能。RACS^[15]、SPANStore^[16]等都属于半集中式代理架构。

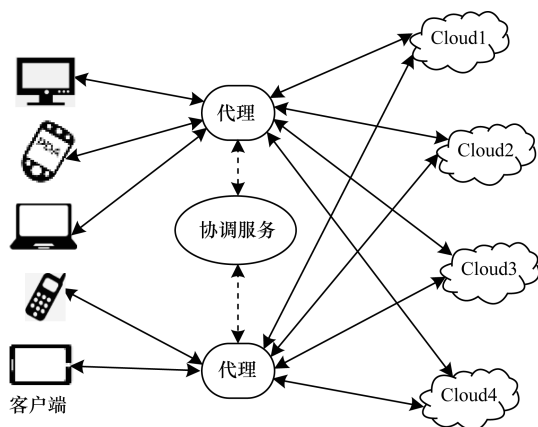


图 2 多云存储半集中式代理架构

Fig.2 Semi-centralized agent architecture of multi-cloud storage

然而,半集中式架构随着数据量的进一步增长依然会面临中心协调服务的性能瓶颈,去中心化的分散式架构显然有更好的发展前景。多云存储分散式架构如图 3 所示,按地理位置部署多云存储代理系统,同时为每个代理附加协调器组件,协调器定期交换状态,无需中央控制。MetaStorage^[17]属于分散式代理架构。

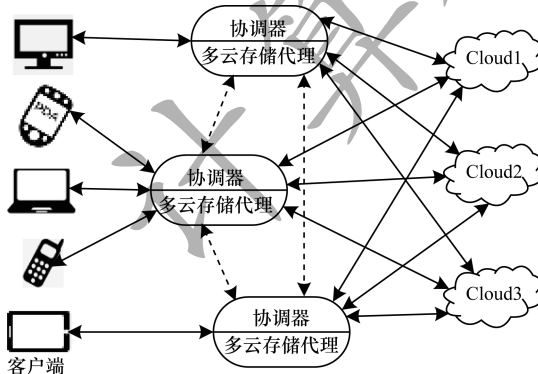


图 3 多云存储分散式代理架构

Fig.3 Decentralized agent architecture of multi-cloud storage

上述 3 种多云存储架构在管理难度、地理范围和扩展性方面各有不同。如表 1 所示,多云存储集中式代理架构方便管理文件元数据信息,但不适合地域跨度大的多云部署,扩展性差。而地理分布式代理架构方便用户访问最近的副本数据,减少时间延迟和带宽资源,但同时保持数据一致性变得更加困难。

表 1 多云存储架构对比分析

Table 1 Comparative analysis of multi-cloud storage architecture

架构	管理难度	地理范围	扩展性
集中式	容易	小	差
半分散式	中等	中等	中等
分散式	困难	大	好

1.3 多云存储技术的优势

多云存储技术对于海量数据的迅猛增长具有更好的扩展性和灵活性,单云存储的固有缺陷也在多云存储技术的应用中得到解决,越来越多的企业和用户倾向于选择多云服务来存储数据。多云存储技术的优势主要有以下 6 个方面:

1) 业务连续性

采用多云存储能够实现单个云供应商无法达到的冗余级别,有助于在灾难发生时仍能确保业务连续不中断。用户将云资源分散部署在多个云供应商,若某个特定的云供应商遭受攻击或故障后,则托管于其他云供应商的资源不会受影响。

2) 数据可靠性

将数据存储在多个云中能够显著提高数据可靠性,从而降低因云失效引起的数据丢失而产生的风险。通过复制或纠删码的方式将数据存储在多个云中,即使某个云存储服务整体故障,也可以通过其他云存储服务恢复完整数据,通过一定的云存储成本换取数据服务更高的可靠性。

3) 访问性能

多云存储能充分利用每个云供应商的优势,即在不同云供应商之间灵活做出最佳选择,获得最佳的云服务。多云存储代理可能会发现某个云供应商擅长于对象存储,而另一个供应商的强项是目录服务,从而根据客户的需求将不同客户的数据发送给不同的云供应商。

4) 安全隐私

由于隐私问题,许多用户不愿将其最敏感的数据托管到公共云中,减轻隐私担忧的方法之一就是使用纠删码来跨多个云存储服务分发数据。这样就能确保任何单个云供应商都不会拥有数据的完整内容,无法读取和恢复原始数据。同样,如果少数云供应商遭遇安全漏洞攻击,攻击者也将无法获得完整的数据集。

5) 管理灵活性

由于每个供应商的云存储服务在服务质量和价格方面存在差异性,多云存储能够灵活运用多个云供应商,根据每个云的价格以及擅长的特定服务来选取多个云的使用策略,提高用户使用体验和降低使用成本,避免供应商锁定。

6) 云存储成本

云服务供应商设置了每种服务的使用资费,根据资费情况,使用多个云的客户可以为不同的服务选择资费最合理的云供应商。例如,某个供应商的每 GB 存储资费可能比另一家便宜 2 美分,而另一家云供应商则在数据传输服务项目上提供更低的资费。如果从多个云供应商订购服务,就可以为使用的每一项服务实现最大的成本效益。

1.4 多云存储技术挑战

尽管多云存储技术拥有上述诸多优点,但面对指数增长的数据和用户越来越高的性能需求,其仍面临着许多技术层面的严峻挑战,主要表现在以下4个方面:

1) 数据可用性

由于大数据体量大且增长速度飞快,多云存储系统的规模需要不断扩大,这对其性能和可用性提出了挑战。研究者针对单云存储中普通商用服务器构建的分布式存储系统节点失效常态化问题,提出通过数据冗余提高可用性的方法^[18-21],但多云存储具有数据距离跨度大、智能终端异构化、网络需求高速化、云容错技术差异化等特点,用户和应用程序与多云存储连接起来的复杂网络存在速度缓慢或不可靠风险,容易导致高延迟率甚至宕机,系统性能和可用性大大降低。因此,在多云存储下数据容错技术仍然面临着不同冗余机制转换和集中式编码实现方法引发的性能瓶颈,以及网络存储节点分散所需的可扩展性挑战。多云存储中数据可用性问题需要同时兼顾可扩展性和性能,这值得研究人员关注和深入研究。

2) 数据完整性

云存储的核心理念是资源租用、应用托管和服务外包,使用户以较低廉的价格获得海量的存储能力。但当用户选择将数据交给单云平台保管的同时,也失去了对数据的控制权,从而无法保证数据的完整性,可能会面临因软件失效或硬件损坏导致数据丢失、被其他用户恶意攻击导致数据损坏,以及被供应商内部人员为经济利益擅自删除不常访问的数据导致数据丢失等问题。为解决上述问题,PDP^[22]、POR^[23]等多种远程数据完整性验证方案被提出。在多云存储中,云用户数量庞大且更加依赖云存储服务,用户在数据完整性检测过程中更加注重用户体验,比如支持数据动态操作、个人隐私保护和无限高效检测等性能。同时,多个云服务供应商也导致数据在验证中更容易出错以及验证开销巨大等问题,给数据完整性验证增加了难度。因此,及时识别存储在多云中的数据是否损坏至关重要,如何使多个云服务供应商协作存储和维护客户数据完整性更是一个难点,数据完整性控制作为多云存储的重要安全技术之一,逐渐受到业内关注。

3) 数据一致性

随着用户对多云存储系统的存储容量和地理位置部署广度的需求不断提高,多云存储往往采用分布式的系统架构,利用多地点多台存储服务器分担存储负荷,提高了系统的可靠性、可用性、扩展性和存取效率,降低了耦合性。但同时也带来了部署、架

构、运维复杂的考验,不同的云存储服务系统可能使用不同的存储类型、编码方式、加密方法、安全级别以及可能相互冲突的不同API,使得数据在多云基础架构的不同系统间不能有效地跨云移动。因此,如何保证庞大的多云存储系统数据一致性,值得深入研究。

4) 数据安全性

多云存储系统的便捷性越来越受到用户的青睐,导致用户群的类型、领域范围和数量不断增加,更容易成为黑客攻击的对象。而多云技术要求海量用户参与,资源以远程、虚拟或租用的形式提供给用户,虽然相比单云存储数据,安全性得到一定提高,但要保证数据在多云环境下整个生命周期中的安全性,防止数据被泄露和窃取仍然比较困难。目前学者们针对多云存储中数据的安全性与隐私性提出了很多技术,如保护用户数据隐私的数据加密和对应的密文搜索机制^[24-26]、隐藏用户数据访问模式的隐藏存储技术^[27-29]、保证用户数据安全销毁的确定性删除技术^[30-31]以及提高用户服务性能和安全性的安全重删技术等。本文主要对安全重删技术进行重点阐述。云存储中数据的高冗余特点使得重复数据删除技术必不可少,而重删技术的大量应用会引发加密阻碍、非授权访问、侧通道攻击等诸多安全问题。安全重删技术成为云存储下保证数据性能和安全性的关键技术之一。多云存储环境下的安全重删技术还需要面临提高重删系统的可扩展性、协调多云中不同加密方式和编码方式、跨云重删以及如何抵御不同攻击类型等挑战。因此,制定更加安全高效的重删机制保证数据的隐私安全性尤为关键。

1.5 国内外多云存储管理平台

随着云存储在各个行业中变得越来越普遍,不同企业的云服务不断涌现,多云存储管理平台的建设也逐渐引起企业的关注。

国外著名的多云厂商有谷歌的Anthos^[32]、IBM Cloud Pak^[33]和MultCloud^[34]等。谷歌作为云厂商的三大巨头之一,本身就拥有数千公里长的光缆、庞大的开源项目、大数据收集和分析能力等巨大优势,其多云管理平台Antos以谷歌首创的多项开源技术(Kubernetes、Istio和Knative等)为基础构建而成,支持对现有应用现代化改造、构建新应用、安全运行应用等功能,但目前Antos只与AWS和Azure协同工作,不支持其他公有云。IBM Cloud Pak是适用于企业的容器化软件解决方案,有助于在多云管理功能中提供一致的可见性、自动化和治理,支持多集群管理、事件管理、应用程序管理和基础架构管理等功能。企业可以利用IBM Cloud Pak来帮助提高由智能数据分析和预测黄金信号驱动的运营效率,并获

得对合规性管理的内置支持。MultCloud 是一款功能强大的多云存储管理器,实现在一个虚拟层下管理来自多个云的在线文件,支持多云文件传输、多云文件同步、多云文件管理器等功能。MultCloud 不仅提供了一种通过基于 Web 的应用程序访问和管理文件的简便方法,而且还提供了流畅的用户体验和直观的界面。通过成功实施多云战略,85% 的企业在多云环境中开展运营,各大厂商已经成功降低了用户的成本增长率,提高了应用程序的可靠性。

目前,国内提供多云管理平台的厂商主要有行云管家^[35]、FIT2CLOUD^[36]和贝斯平^[37]等。行云管家的发展较为迅速,主要提供跨云厂商的云管理方案,包括云服务器管理、混合云管理、微信监控告警、成本分析与优化建议、健康负载与安全体检、云堡垒机、自动化运维等功能。FIT2CLOUD 主要致力于解决企业在多云环境下的服务化和管理、安全及数据库服务交付难题,以统一的方式帮助企业在多云环境下实现自动化、自助式的服务交付,支持企业从传统 IT 渐进无缝地过渡到多云战略。贝斯平推出的 OpsNow 提供了对公有云、私有云、容器、裸金属服务器的统一接入管理,为用户隐藏各云商的差异,提供统一的资源抽象,进而提供一致性的体验。国内多云管理平台市场尚处于早期阶段,但仍然面临资源孤岛、复杂运维以及运营缺失等诸多问题。随着我国企业云行动的快速推进,多云环境安全性、多云管理一致性、多云间数据层可靠性和完整性等问题需要研究者进一步研究与探讨。

2 多云存储关键技术

针对多云存储技术在数据的可用性、完整性、一致性和安全性上存在的技术挑战,本文重点分析和总结多云存储在纠删码容错技术、数据完整性证明机制、并发控制方法以及安全重删技术等方面的国内外研究现状。

2.1 纠删码容错技术

在多云存储中为防止数据丢失、故障、中断以及供应商锁定等损失,往往需要提高数据的容错能力。目前常见的数据容错技术有两种^[38],即多副本容错技术^[39]和纠删码容错技术^[40]。与多副本容错技术相比,纠删码容错技术可以在显著降低存储空间消耗的同时,提供相同甚至更高的数据容错能力。纠删码容错技术的基本原理是将数据分割成数据块,对数据块进行编码生成编码块,使得每个编码块都是所有数据块的线性组合,然后将编码块存储在不同的位置,达到容错的目的。若某个块失效,则通过对剩余可用块进行线性组合计算来恢复。具体的编码实现主要包括集中式和分布式

两种^[41]。在集中式编码实现方法中,所有编码工作都由一个编码节点来单独完成。编码节点从存储节点下载数据块,编码计算校验块,然后再把校验块发送到其他存储节点上。

文献[15]提出 RACS 代理在多个供应商中使用纠删码容错技术进行冗余存储,使客户避免供应商锁定,更好地容忍供应商的中断和故障。收到 Put 请求后,RACS 将传入的数据拆分为 m 个大小相等的块(即每个数据块是原始数据大小的 $1/m$),其中 $m < n$ 是可配置参数。然后,RACS 使用纠删码容错技术创建额外的 $(n - m)$ 个编码块,总共 n 份。编码块与数据块的大小相同,任何 m 个编码块的集合足以重建原始数据,每个块都发送到不同的存储库。相反,当客户端发出 Get 请求时,RACS 将获取 m 份并重新组装数据。RACS 将问题上升至多云,试图解决供应商锁定,降低切换供应商的成本,更好地容忍中断和故障。但其使用的纠删码是传统的 RS 码^[42],并未提高纠删码的性能,也没有解决多云存储的安全问题。

文献[11]结合网络编码的思想设计一种再生码——MSR 码,提出了使用 F-MSR 在多个供应商中冗余存储:将文件划分为 A、B、C、D 4 个数据块,并且通过数据块不同的线性组合形成 8 个不同的编码块 P_1, P_2, \dots, P_8 。每个数据块大小相同 ($M/4$),每个编码块也具有相同的大小 ($M/8$),每 2 个编码块合并成一个代码块存储在一个节点中。任意 2 个节点可以用来恢复初始的 4 个数据块。假设某个节点故障,代理从每个幸存节点收集一个编码块,每次下载大小为 $M/8$ 的 3 个编码块,则代理由 3 个编码块的不同线性组合重新生成 P_1' 和 P_2' 2 个编码块。注意, P_1' 和 P_2' 仍是数据块的线性组合。然后代理将 P_1' 和 P_2' 写到新节点。在 F-MSR 中,存储大小是 $2M$,但是修复流量是 $0.75M$,比 RAID6 节省了 25%。F-MSR 的重点是试图高效修复云故障,极大减少了修复时的传输数据量,但其要求节点不仅具有存储转发的简单功能,还需要具有可编程性。同时,由于 F-MSR 只保留代码块,而不是原始块,要访问某个文件的单个块,需要为特定块下载和解码整个文件。因此,F-MSR 只适用于长期存档应用。

文献[14]将收敛加密、重复数据删除、压缩与缓存等技术和纠删码相结合,提出 F2MC。F2MC 与 RACS^[9]一样都使用 RS 码,将一个加密的文件数据分解成 m 个大小相等的原始碎片,再将 m 个碎片映射到 n 个碎片的集合 ($n > m$),用少量存储成本换来了数据的容错性。同时,F2MC 在雾节点中对数据进行重删、压缩、编码和加密,再将加密后的数据分散到多个云供应商,不仅进一步节省了数据流量和

存储空间,而且增强了多云存储的弹性和安全性。同时,雾节点支持数据缓存,以提高客户端读取操作的性能,但该方案没考虑改善纠删码性能,且集中式编码方案也导致其不适用于大规模部署。

以上的集中式编码实现方法的优点是简单且易于实现,其缺点是在大规模多云存储中存在较为严重的性能瓶颈和网络传输瓶颈,从而影响编码实现效率。分布式编码实现方法是将编码实现的网络传输负载和计算负载分布到多个节点上,并行执行子任务。相对于集中式编码实现方法,分布式编码实现方法可以在数据不断增长且分布范围广的现状下提升编码实现的性能。

文献[4]针对在实际情况中不同供应商可能使用不同的冗余机制来存储数据(纠删码容错技术、RAID 技术、多副本容错技术等)的问题,提出一种使用基于信息分层的纠删码方案 SafeStore。该方案通过公开存储服务供应商(Storage Service Provider, SSP)内部可接受的冗余选项,对 SSP 内部冗余进行额外的控制,允许系统在 SSP 内部和 SSP 之间有效地划分存储冗余,降低网络带宽和存储成本。混合使用多种纠删码可以同时发挥多种纠删码的优势,但是如果使用完全不同种类的纠删码,每次动态转换都相当于重新进行一次编码,成本极高。在同一种纠删码的不同参数之间转换,可以减少转换需要重新产生的校验数据以及数据的读取量和传输量,SafeStore 的实现阶段就使用了这种方式,采用(3,2)MDS 码以及三副本来跨 SSP 冗余存储数据。SafeStore 试图提高将故障限制在特定节点组的可能性,并有效地在 SSP 内部和跨 SSP 部署存储以解决此类故障,但其并不考虑提高纠删码的性能,且安全性较低。

文献[43]提出了分布式文件系统 NCFS,它支持在分布式存储设置中进行常规的读写操作,并在节点故障期间启用数据修复。它的特别之处是支持一种 E-MBR 码的特定重新生成编码方案,跨不同存储节点透明地对数据进行条带化,而无需在修复过程中对存储节点之间进行协调,试图最大程度地减少修复带宽。在此之前对于再生码的分布式存储研究多数是理论上的,该方案第 1 次使用实用的分布式文件系统评估重新生成代码的性能。相比于 NCcloud,NCFS 需要耗费更多的存储开销,但不要求节点具有编码性,可扩展性更高。总而言之,再生码可以有效地降低数据修复开销,但是再生码的存储空间利用率明显低于其他类别纠删码,所以不适用于存储成本要求较高的大规模存储系统,而更加适合对于带宽成本敏感的系统。

文献[44]考虑到数据的安全性,提出一种将对称加密、秘密共享和纠删码相结合的 DEPSKY 方案。数据使用随机密钥加密,防止个别云泄露数据;密钥

使用秘密共享进行划分,每个服务器接收加密数据块和密钥的共享,确保不会有错误的云重建数据;纠删码技术减少每个云中数据的大小。DEPSKY 不需要节点具有可编码性,且相对于 RACS 增强了数据的机密性和安全性。但 DEPSKY 没有试图通过利用供应商之间的差异来寻求最小化成本。

表 2 从编码实现方法、纠删码类别、节点可编程性和扩展性等方面对几种纠删码方案进行了对比分析。类似 HAIL^[45]的单云存储中数据可靠性主要依靠多副本容错技术和纠删码容错技术的集中式编码方法,实现起来相对简单,但随着数据量的增长容易引起网络拥塞和单点故障。网络编码思想^[46]是在节点上进行编码以提高信息传输率,但多数网络节点是使用“存储-转发”机制的路由器,不能对数据进行编码操作,扩展性不高。在多云存储中,RACS、NCcloud 和 F2MC 方案借鉴了单云存储中集中式编码方式和网络编码思想,因而限制其扩展性。面对指数增长的海量数据,未来的多云存储系统将越来越庞大,更倾向于使用 NCFS、SafeStore 和 DEPSKY 等采用分布式编码的方案来提高数据可靠性。但分布式编码实现方法需要多个不同节点相互协调合作,带来大量数据传输,占用较多网络资源。因此,相对于集中式编码,分布式编码的重点已从降低运算复杂度转换到了降低网络资源消耗和一致性保证,同时对安全性和性能有更高要求。

表 2 多云存储纠删码方案对比分析

Table 2 Comparative analysis of multi-cloud storage erasure code schemes

方案	编码实现方法	纠删码类别	节点可编程性	扩展性
RACS	集中式	RS 码	否	一般
NCcloud	集中式	MSR 码	是	差
F2MC	集中式	RS 码	否	一般
NCFS	分散式	MBR 码	否	一般
SafeStore	分散式	MDS 码	否	好
DEPSKY	分散式	RS 码	否	好

2.2 数据完整性证明机制

数据完整性证明机制^[47]可以根据是否对原数据采用容错预处理技术,分为数据持有性证明 PDP 机制和数据可恢复证明 POR 机制。PDP 机制能快速地判断远程节点上的数据是否损坏,更多地注重效率。POR 机制不仅能识别数据是否损坏,并且能够恢复已损坏的数据。两种机制有不同的应用需求,PDP 机制主要用于检测大数据文件的完整性,而 POR 机制则用于确保重要数据的完整性。

文献[48]提出了一种有效的多副本 PDP 方案(MR-PDP),可确保存储服务存储多个唯一副本。初始化阶段对输入文件进行“一次”预处理,创建适用于 PDP 的 t 个唯一且可区分的副本,然后客户端

将副本和验证标签存储在服务器上,并保留少量恒定的信息。质询阶段客户可以执行单个挑战或完整挑战来确定服务器是否仍然拥有文件副本并通过复制阶段来维护所需的副本。该方案可动态创建新副本,而无需再次预处理文件,且检查 t 个副本的开销比检查单个副本开销便宜 t 倍,但不能支持动态的数据操作。

文献[49]提出了动态可证明数据持有(DPDP)技术的定义框架和有效构造,它扩展了PDP模型以支持对已存储数据的可证明更新,在块级别上进行插入、修改、删除等操作,而这些在传统PDP机制是无法实现的。当动态更新操作时,用户首先发出更新请求,服务器分以下2个阶段进行更新:1)解析请求中的更新操作,若删除操作,则直接删除所在数据块;若修改操作,则更新制定数据块内容和块签名标签;若插入操作,则在制定位置插入数据块和块标签;2)辅助用户更新跳表的根哈希值,服务器返回每个指定节点的认证路径,用户利用认证路径更新根节点的哈希值。该方案可以完全支持动态操作,但其认证路径过长,每次认证过程中需要大量的辅助信息支持,计算和通信开销较大。

文献[50]提出了一种支持保护隐私的公共审计的PPDP方案。该系统将基于公钥的同态线性身份验证器(HLA)^[51]与随机掩蔽技术集成在一起,在审计时无需检索整个数据的副本,不仅大幅减少通信和计算开销,而且确保TPA在审核过程中不会学习有关存储在云服务器中的数据内容;并将保护隐私的公共审核协议进一步扩展为多用户设置,同时应对可能来自大量不同用户的多个审核委派,大幅提高了工作效率。该方案虽然可以确保数据的隐私,但对于POR机制而言,采用这种方法将使得验证者无法再通过抽取器去恢复损坏的原文件。

文献[52]提出了一种基于哨兵的PORs机制,用户无需下载存储在云上的数据即可验证其完整性,不仅能判断其是否被删除或修改,并且可以恢复一定程度的数据。在存入云中的数据中预先植入一些被称为“哨兵”的检验数据块,并在本地存储好这些检验数据块。远程服务器无法区分检验数据块与数据,若数据被损坏,则会相应损坏到检验数据块。通过对比存储在本地的检验数据块,就能判断出数据完整性以及出错部分所占的概率。结合纠错码对文件进行容错预处理,使得验证机制可以恢复一部分损坏的数据。虽然POR机制最先考虑到数据恢复问题,但该机制不支持公开验证,且只能进行有限次验证。

文献[53]提出了一个健壮的动态远程数据检查方案DPOR提高鲁棒性,同时支持动态更新。该方案采用Cauchy RS线性编码进行数据预处理,只需

要奇偶校验符号和新符号即可更新代码字。仅检索奇偶校验符号使得更新通信量显著减少,有效地提高了恢复错误的效率,但更新操作需要云服务器重新生成所有的辅助容错信息,导致计算代价较高。

文献[54]提出一种针对多云环境的完整性和零知识特性(IVCZKP)方案,用户对数据进行预处理后将数据索引发送到受信任的第三方(TTP),将数据块和标签发送给组织者,组织者将数据分发到多个云供应商。同时,用户可通过索引哈希表对数据块进行动态更新,如数据修改、插入和删除。在验证时用户向TTP发送请求验证,TTP向组织者发起挑战,组织者向云供应商发起相应挑战,组织者汇总CSP质询相应信息并发送给TTP,TTP执行完整性验证并将结果告知用户。该方案运用零知识来确保挑战云供应商进行数据完整性验证无需任何秘密信息,同时支持动态更新,但所有验证都需要经过组织者分发和汇总,频繁更新和验证容易引起性能瓶颈。

文献[55]提出一种多云环境的数据完整性验证和恢复方案(MRVR),利用同态、双线性图和二进制聚合树(BAT)技术实现公共审计和快速恢复。在准备阶段,用户借助受信任的权威(TA)对数据进行分块生成密钥、副本和标签。在完整性验证阶段,诚实云供应商(HCSP)将多云证明汇总到单个响应中,并将其发给审核员验证,审核员验证后将结果通知用户。若数据已损坏,则进入数据恢复阶段,MRVR将查找损坏数据并借助BAT技术进行恢复。该方案可以在多云环境下实现很高的数据可恢复性和可用性,但审核员的公正性很难保证,且HCSP依然存在集中式引发的性能瓶颈问题。

表3对7种完整性机制从服务器计算复杂度、用户计算复杂度、通信复杂度、数据恢复、支持动态操作、验证次数等方面进行了对比分析。虽然POR机制可以对数据进行一定的恢复,但其用户计算复杂度也随着分块数 n 的增加以幂函数增长,对于大文件来讲性能不佳。全动态操作和POR机制无限次验证的实现仍然是完整性控制的难点。在单云存储中,数据完整性方案尚不成熟,很难兼顾数据恢复、动态操作和无限次验证的要求,且扩展性不高,虽然DPOR方案兼顾了以上要求,但在数据更新过程中需要大量的辅助信息支持,使用性能不佳。在多云环境下数据分布广且复杂,完整性验证和恢复过程更注重安全性,且时间复杂度和空间复杂度都不能过高才有实现的可能。但目前IVCZKP和MRVR 2种方案都需要一个组织者来频繁分发和汇总各个云的数据,扩展性有限。整体来说,目前多云存储在数据完整性研究方面还不成熟,尚未建立起一套完整的理论体系,需要更多学者进行深入研究。

表 3 多云完整性检测机制对比分析

Table 3 Comparative analysis of multi-cloud integrity detection mechanisms

机制	服务器计算复杂度	用户计算复杂度	通信复杂度	数据恢复	支持动态操作	验证次数
MRPDP	$O(c)$	$O(n)$	$O(1)$	否	是	无限
DPDP	$O(c)$	$O(n)$	$O(1)$	是	部分是	无限
PPDP	$O(c)$	$O(n)$	$O(1)$	否	是	无限
PORs	$O(1)$	$O(n^2)$	$O(1)$	是	否	有限
DPOR	$O(1)$	$O(n^2)$	$O(1)$	是	是	有限
IVCZKP	$O(c)$	$O(n)$	$O(1)$	否	是	无限
MRVR	$O(\log_a n)$	$O(1)$	$O(1)$	是	是	无限

2.3 并发控制方法

分布式环境下多任务并发处理不当将会导致时间和数据上的不一致,而时间及数据的不一致将导致集群效率和性能较低,甚至分布式任务的失败。多云存储系统需要保证数据在多任务并发的情况下全部正确写入,不会出现错乱或遗漏,同时保证写操作执行成功后,在可接受的时间内所有的用户可以获取到最新的数据。

目前用来解决并发问题的使用最广泛的分布式组件是 Zookeeper^[56]。Zookeeper 相当于集群的管理者,监视着集群中各个节点的状态,根据节点提交的反馈进行下一步合理操作。最终,将简单易用的接口和性能高效、功能稳定的系统提供给用户。文献[12]提出了 Hybris,该方案结合公有云和私有云两者的优点,将元数据保存在受信任的私有云上,而将数据分散到多个不受信任的公共云上。私有云上元数据的更新,便是在 ZooKeeper 上使用无等待并发控制来实现,进一步提高了 Hybris 相对于基于锁的系统的可伸缩性。但 Hybris 将元数据服务器限制在单个地理位置,扩展性差。

文献[16]提出一种 SPANStore 方案,该方案统一协调地理位置分散的多个供应商,最大限度降低传播时延和存储成本,由一个中央位置管理器(PMan)绘制存储服务的统一视图,决定哪些 SPANStore 虚拟机为哪些位置的用户提供 PUT/GET 请求服务。在初始化阶段,所有的 SPANStore 虚拟机都将应用程序的工作负载和延迟的摘要传输给 PMan,PMan 根据对下一个时段中应用程序的工作负载以及应用程序的延迟、一致性和容错需求的估计,计算应用程序对象使用的最佳复制策略。然后,PMan 将新的复制策略传递给所有数据中心上的 SPANStore 虚拟机。这些复制策略规定了 SPANStore 应该如何在下一个时段中为应用程序的 Put 和 GET 操作提供服务。尽管 SPANStore 试图最大限度地降低多云存储的使用成本,但也有一个显著的缺点,就是所有工作负载和延迟数据都需要传输到 PMan,这在数据量和传输量庞大的情况下必然会出现性能瓶颈和单点故障的问题。

为了避免中央协调组件成为瓶颈,文献[17]采用一个分散的解决方案 MetaStorage。该方案为每个多云分发代理附加了一个协调器组件,该组件负责在代理之间定期交换状态。代理的分发机制基于键值哈希的首选列表,根据首选云存储服务及其在首选列表中的顺序存储在前 N 个节点上,从而分布到多个提供者。该方案的思路为一个主协调器确定所有其他协调器的状态。若主协调器故障,则无法在一段时间内到达其余协调器,其余协调员都会让主协调器离线并将其从协调员名单中删除。因此,第 2 号成为新的第 1 号,即主协调员。由于协调员了解所有其他协调员及其具体顺序,他们每个人都可以决定新主人是谁以及何时成为主人,无需中央控制。MetaStorage 通过分散机制避免了单点故障,但在每个分发代理上添加了一个额外的层而遍历每个服务调用会导致一定的延迟,而且 Dynamo^[57]风格的复制协议放松了一致性的保证。

文献[58]提出一种 Scalia 方案,该方案依靠多版本并发控制(MVCC)来处理并发更新,是一种没有锁的替代方法,更新操作不会删除旧数据,而是用新数据覆盖旧数据。旧数据被标记为过时并且添加了新版本,导致存储多个版本的数据,其中只有一个是最新版本。如果在多个数据中心同时更新条目,则数据库将检测冲突。系统将提示用户决定哪个版本是好的版本,Scalia 将删除其他版本,也可以自行决定只保留最新版本。该方案对比锁机制不会阻塞读操作,大幅优化了读效率。但在云存储供应商发生短暂故障的情况下,Scalia 需要将故障供应商托管的块移动到其他供应商,为了移动故障供应商的块,需要从剩余的块重建数据对象并再次拆分成块。此时,若最具成本效益的供应商集合的阈值 m 不同,需要重写所有块,这一过程的成本相对较高。

文献[59]针对不同云之间的兼容问题,提出一个多云文件写作系统 CoCloud,该系统通过在每种流行云附近部署一个或多个代理来有效访问 Web API;同时设计了统一的代理间高级传输协议,包括重复删除技术、压缩、多级捆绑,以便利用文件版本

之间的相似性提高整体协作效率;另外设计了相关控制机制优化客户端和控制服务器,以保证及时性并消除文件协作期间的冗余更新。尽管 CoCloud 解决了跨云文件的协作问题,但该方案并未考虑安全和隐私问题。

文献[60]针对多云环境下副本选择问题,提出一种基于带宽和等待时间的副本选择机制 BLRS,以避免潜在的网络过载问题。该方案采用多副本管理器(RM)和分析模块(AM)来应对分散式分析和框架。当用户发出请求时, RM 将在执行单元中创建实例请求并发送环境分析请求(EAR)给云提供商中相应的 AM;AM 将收集的延迟和带宽情况进行评估,生成环境信息反馈(EIF)返回给 RM;根据收到的 EIF, RM 将为此实例生成一份副本选择选项,若网络过载或副本不可用, RM 可根据副本重建机制自动创建副本到合适的位置。该方案基于对网络指标的评估,去中心化地选择更合适的副本路径,可以显著增加并发运行实例数量,并平衡带宽使用。但该机制中 RM 只和云提供商中的 AM 直接联系, RM 间并未协调统一,且未考虑安全性和隐私问题。

文献[61]针对多云复合应用程序部署问题,提

出一种混合遗传算法 HGA,该算法综合考虑了多云中性能优化和预算控制,在 GA 框架下增加了服务聚类机制、修复算法、解决方案表示、种群初始化和遗传算子的新算法技术,以实现有效的多云应用程序部署。该算法将多云复合应用程序部署问题定义为约束优化问题,在预算约束下大大缩短了响应时间,但并未考虑一些新的云范例,且只设置了一个代理连接应用程序与多云,扩展性有待提高。

表 4 对几种并发控制机制从并发处理、锁机制、中央控制以及核心特征等方面进行了比对分析。Scalia 适用于多读场景,冲突发生较少,省去锁开销可以增大系统的吞吐量;而多写机制会经常产生冲突,导致上层应用不断进行重试,反而降低了性能,使用带锁机制的方案更合适。从表 4 可以看出,能否进行分散架构的并发控制仍是一个值得深入研究的问题。并发控制问题的处理是分布式多云存储的基本任务之一,也是分布式任务完成度以及性能好坏的关键所在。随着多云存储业务的不断丰富,越来越多的用户认可并投入使用,不断扩大的数据规模和用户对多云存储服务需求使得并发控制问题越来越具有挑战性,成为多云存储研究的重点和难点。

表 4 多云并发控制机制对比分析

Table 4 Comparative analysis of multi-cloud concurrency control mechanisms

机制	并发处理	锁机制	中央控制	核心特征
Hybris	ZooKeeper	需要	需要	结合公有云和私有云
SPANStore	PMan	需要	需要	能生成统一视图
MetaStorage	Dynamo	需要	不需要	采用分散架构管理
Scalia	MVCC	不需要	需要	优化数据放置
CoCloud	Notification Handler	需要	需要	兼容不同版本
BLRS	Replica Selection/Re-Creation	需要	不需要	分散式优化副本选择
HGA	Service Clustering/Greedy Heuristic	需要	需要	约束优化复合应用程序部署问题

2.4 安全重删技术

随着数据量的飞速增长,存储空间和传输速率成为当前网络存储领域的一大瓶颈,其中对相同相似数据的优化处理成为一个研究热点。据研究,在所有备份的数据中,高达 80% 以上的数据是冗余的^[62-63],利用数据高度冗余的特性,研究者提出了重复数据删除技术,该技术是一种数据缩减技术,它的算法流程是对数据进行分块,计算每个块的特征值并加入特征值列表,新加入的块通过对比特征值列表来确定是否重复,若不重复,则建立索引保存该块特征值和映射关系到特征值列表并存储原始块到数据库,若重复则只添加映射关系。而安全重删是在此基础上加入纠删码、加密等技术,增强了数据在全周期内的安全性,不仅降低了数据管理所需的存储空间,实现更快更频繁的存取,而且实现数据的安全防护和高效传输。

文献[64]提出一种基于重复数据删除技术的云中云存储系统,该系统充分挖掘复制和纠删码数据

布局的优点,并结合重复数据删除技术中数据引用机制,消除云存储系统中的冗余数据量;然后基于数据块引用率将数据块以复制和纠删码两种数据布局方式存储在多个云中。用复制方式存储高引用数据块,用纠删码方式存储其他数据块,从而使系统整体性能和成本大幅提高。该方案通过结合混合纠删码和重删技术提升多云性能,但并未从安全和隐私方面对数据进行保护。

文献[65]提出一种在多云环境下提高成本效益的信息简化计划 CHARM,用最小的费用将信息灵敏放置到不同的云中。在 CHARM 中,工作负载不断收集并处理用户存储数据的信息,将统计信息发送到预测器,预测器根据接收到的信息预测文件访问频率并发送给存储模式切换 SMS, SMS 根据预测器输出决定对存储数据使用纠删码还是多副本方式存储。数据在数据托管单元中通过放置启发式算法计算出成本最小的多云策略,并进行重删以进一步减小成本。该方案结合纠删码、重删和放置启发式

算法将数据灵活存储在多云中,大幅降低了存储成本,但对于预测器的设计没有深入研究,且未提及安全和隐私风险。

文献[66]提出一种基于口令认证的密钥交换协议的服务器端重复数据删除方案,用户相互比较私密信息共享密钥,不需要额外的服务器即可实现跨用户重删。该方案不仅允许用户在本地客户端加密数据,而且可以通过限制单个文件访问次数来防御恶意用户或服务器发起的暴力攻击。但针对一些热数据,用户同样需要将其对称加密,并与其他用户运行 PAKE 协议,增加了计算开销。

文献[67]提出一种 CDStore 方案,该方案综合考虑安全和成本效率,将秘密共享和两阶段重复数据删除技术相结合,用源自原始数据的确定性加密哈希替换传统秘密共享的随机输入,使其能够在客户端去重后再编码发送到不同的云上,节省上传带宽,然后在服务器端对不同用户的数据进行重复数据删除,进一步节省存储空间。但 CDStore 采用的收敛加密技术仍可能遭受离线的暴力攻击。

文献[68]提出一种 CloudS 方案,该方案为获得更好的用户体验以及安全性和性能之间的平衡,通过压缩、加密和编码方案的各种组合提供了多个安全级别。同时提出了基于异或操作 XOR 的隐私保护码 PPC,在此基础上提出一种适用于完全并行化的重删友好型分散算法 HCE-PPC,以及变体压缩 PPC 和压缩 HCE-PPC,以适应不同用户的不同需求。HCE-PPC 算法与传统算法相比,在实现近似安全性的基础上提供了更好的性能。但 HCE-PPC 算法难以抵抗双重错误。

文献[69]提出一种 CloudShare 方案,该方案通过区块链与收敛加密的结合,将每个云存储系统相融合构成一个巨大的联盟云,跨用户进行加密重复数据删除。CloudShare 分为两层:上层采用区块链记录跨云用户的存在和所有权,不可更改和删除;底层由云供应商及其相应用户组成,每个用户将数据存储所在的云中,但可以访问多个云的数据。不同的云资源可以获得有效的集成和分配,显著降低了每个云的存储成本,并节省了用户的上传带宽,确

保了数据的保密性和一致性。但由于区块链技术实施机制的原因,只能处理比较少的并发任务,一旦超过阈值,则会产生性能瓶颈。

文献[14]利用云雾计算的互补性提出一种 F2MC 方案,该方案将本地雾计算与远程云计算相结合,把关键数据处理功能放在雾节点中完成,利用重复数据删除技术、压缩技术、纠删码以及缓存在多个云供应商之间分散存储加密数据,增强了服务质量,提高了数据流量和空间效率,进一步增强了多云存储的弹性和安全性。但该方案属于多云存储集中式架构,随着数据量的增长,将数据处理功能都放在一个雾节点上容易产生性能瓶颈,不适宜进行大规模部署。

不同于上述都是对相同数据进行处理以达到优化性能目的的方案,文献[12]考虑到相似数据跨多个云可能引起信息泄露,提出了一种多云信息泄漏感知存储系统 StoreSim,采用基于聚类的存储计划生成算法,将语法相似的数据存储在同一个云上,从而最小化用户跨多个云的信息泄漏。但该方案只能针对语法相似度进行划分,基于语义的优化存储隐私算法还需要进一步研究。

表 5 对基于重复数据的防护机制在算法、数据去重级别、抗攻击类型、第三方服务器、重删范围等方面进行了对比分析。文件级去重模式易管理,相比之下块级去重模式具有更高的灵活性和可靠性,在数据库环境下更倾向于块级去重模式。引入第三方服务器可以提高安全性,实现对密钥的有效管理,但同时存在实用性低、重删效率低、扩展性差且不能保证与云服务器合谋的缺点,对于海量数据并不适用,多云方案都未使用第三方服务器。多云环境下同领域用户增多,更加迫切需要在保证数据安全性的前提下对相同或相似数据进行删减优化^[70],目前多云重删方案大都局限于客户端重删和云内部重删,云与云之间重删实现困难,CloudShare 打破了多云屏障,通过区块链降低了每个云的存储成本,但该技术尚不成熟,对于并发任务并不友好。目前,对相同或相似数据的研究虽有一定的成果,但还不够完善,跨云安全重删和相似数据研究等方向值得当今学术界和产业界重点关注。

表 5 基于重复数据的防护机制对比分析

Table 5 Comparative analysis of protections mechanism based on duplicate data

机制	算法	数据去重级别	抗攻击类型	重删范围
PAKE	PAKE	文件级	蛮力攻击	用户间
CDStore	CE + AONT-RS	块级	侧信道攻击	客户端/用户间
CloudS	HCE-PPC	块级	侧信道/蛮力攻击	用户间
CloudShare	CE + DS	块级	侧信道/女巫攻击	用户间
StoreSim	Minhash + SPClustering	块级	单点攻击	用户间
F2MC	CE + SFTC	块级	侧信道攻击	用户间

3 多云存储未来研究展望

本节结合多云存储的实际应用需求和研究现状,总结多云存储的研究趋势。

3.1 多云间数据迁移

目前云存储服务市场蓬勃发展,国外比较著名的有亚马逊、微软、谷歌等,国内有阿里、腾讯、华为等,多个云存储服务给企业带来更多的选择。为避免供应商锁定,利用就近计算优势以及提高业务应用的全域服务能力,企业更倾向于将自己的服务应用部署到多个地域、多个云存储供应商的数据中心内^[71-72],越来越多的企业基于多云架构提升灵活性和成本效益。然而,不同云平台之间并不是无缝衔接的,不同的生产环境、操作系统、数据库以及中间件等,都会导致多云间难以实现数据的及时传输和分析,形成一座座信息孤岛,使得企业的业务进程不能正常推进。因此,如何科学有效地提高企业在多云间迁移和管理数据的能力变得尤为重要。不同云平台的数据迁移情况复杂,实现困难,既要保证数据在迁移过程中的隐私性、完整性和一致性,又要维持迁移过程中业务的可用性、稳定性和性能。同时,应用数据在迁移前需要基于不同云平台做兼容性部署,甚至要对应用系统重新拆分、设计架构和构建,才能更好地贴合不同云架构和实际需求。因此,迁移准备中的兼容调整和测试验证、迁移过程中的传输秩序和安全保障机制以及迁移后的运维等,都是多云间数据迁移必须直接面对的机遇和挑战。

3.2 多云间数据一致性

随着多云存储业务的不断丰富,投入使用的云用户越来越多,导致云数据量激增,分布式云存储架构越庞大,部署也越来越复杂。而多云间数据一致性问题分布式多云存储的核心问题之一,也是分布式任务完成程度以及性能好坏的关键所在。数据一致性的出现,引出分布式系统的核心理论——CAP理论^[73],后又在一致性和可用性的权衡下逐步演化为BASE理论^[74],该理论减弱了数据一致性的约束,提出服务基本可用,数据存在软状态,但能确保最终一致的方案^[75]。常见的数据一致性协议有2PC^[76]、3PC、Paxos^[77]、Zab^[78]和Raft^[79]等,这些协议有些实现简单,能够保证数据的强一致性,但降低了系统的可用性;有些实现复杂,能够保证系统较高的可用性,只实现数据的最终一致性。而多云存储系统涉及到多个云存储系统之间的相互协调调用,情况更为复杂,需要从需求背景出发选择最合适的数据一致性方案。目前企业更倾向于选择去中心化程度更高的分散式多云存储系统来避免数据容量和带宽流量冲突造成的性能瓶颈,导致一致性保证变得更为艰难。现有工作虽然能够完成分布式任务,并针对实际情况遇到的问题提出一些改进方法,但大多采用集中式管理方式。随着数据量上升,弊端

也逐渐暴露出来,与人们对多云存储性能的预期还有很大差距。多云间数据一致性的保证涉及数据安全、资源消耗、工作效率以及服务质量等方面,是多云存储研究的重点和难点。

3.3 云端协同的隐私防护

云存储在为用户带来便利的同时,也造成了数据所有权和控制权的分离^[80]。供应商可能搜索、获取用户存储在云端上的数据,也可能因为系统故障导致用户数据丢失,同时也可能存在黑客通过攻击云端的服务器获取用户的数据等,这些都是信息泄露、数据丢失的潜在风险。而使用多云存储会增加攻击面的数量以及数据受损的可能性,用户使用的云存储服务越多,风险就越大。多云存储带来的安全问题不仅局限在一维层面,它涉及到设备维度、网络维度、系统维度、云端维度等多个方面,任何一点疏漏都可能导致整体的安全防护功亏一篑,各个云供应商必须全面分析并着手解决面临的各种安全和隐私问题,才能使用户放心地将自己的数据交付于多云^[81]。现有工作利用数据加密、身份验证、访问控制级别、秘密共享、纠删码、数据压缩处理等技术,在一定情况下减少了信息泄漏风险,改进了多云存储的安全性能。但每个云存储供应商对多云平台的可见性有限,只针对自身系统应用设计账户管理模式和数据防护方案,不同的防护工具和流程使得多云安全性更加复杂,模式不兼容和规则漏洞的情况时有发生。若不同的云存储平台能理解不同体系结构的模式和规范,采用全面一致的防护策略,数据安全风险将大幅减小,但这显然并不容易。制定多云协同的隐私安全和治理策略还需要投入更多的努力去探索。

3.4 基于云际计算的跨用户重删

云数据的迅猛增长使得网络空间和带宽资源都变得日趋紧张,而利用数据高度冗余的特性,重删技术能够极大降低存储空间开销和网络带宽,并进一步降低能耗和管理成本。凭借在数据缩减上的优势,目前重删技术主要应用于备份、容灾、归档、虚拟机环境下的主存储系统、内存性能优化^[82]和延长SSD使用寿命^[83]等环境中。尽管现有工作利用重删技术节省了一定网络资源,且具备一定的防御能力,但仍然不容乐观。多云数据的重删度极高,随着数据的增长元数据将会十分庞大,从而影响数据查找效率,因此调整元数据的组织结构和数据布局提高重删性能十分必要。多云存储的兴起使得企业更倾向于在云端进行跨用户重删,若能打破多云壁垒实现多云间重删,数据缩减将有质的提升。但同时用户的隐私可能会因此受到极大威胁,而且企业对重删的偏爱会导致用户数据安全性降低,如何平衡尚有待解决。基于云际计算的跨用户重删还有很多尚待解决的问题等待人们去研究和挑战。

3.5 基于区块链的云际资源调度

近几年,区块链作为一项新兴技术引起了人们的广泛关注。区块链分为公有区块链、联盟区块链、私有区块链^[84-85],具有去中心化、开放性、独立性、安全性、匿名性等特点^[86],众多优势可以很好地解决现有技术所面临的瓶颈问题,使其迅速成为学术界的热门研究话题之一,目前已经渗透到全球多个行业应用领域。云际资源调度^[87-88]是多云存储中至关重要的一环,多云平台接收到用户的服务请求后,会根据用户的要求(时间、效率、成本等)给出最优的资源调度组合,从而在满足用户要求的同时,极大地提高了资源利用率。而将区块链与云际资源调度相结合,不仅可以促进云际资源调度领域的一些突破,实现更经济、更高效、更安全的分布式多云存储,而且可以解决区块链技术因信息爆炸而产生的存储容量不足的问题^[89],为大规模应用奠定基础。但基于区块链的云际资源调度发展尚不完整,还存在如下挑战:在资源调度中针对具体的分布式特性与管理需求采取合适的偏好决策^[90];解决区块链的计算能力及响应速度不能满足应用领域实时计算的要求;改善区块链记账方式效率不高和资源耗费严重的问题^[91];解决区块链技术只能添加,不可删除,导致数据增长不可逆的问题;打破多云屏障实现去中心化。基于区块链的云际资源调度仍然是一个开放的课题。

3.6 基于多云环境的“智慧地球”

当前世界科学技术迅猛发展,大数据、物联网、人工智能、多云存储等技术的广泛应用不断推动社会生产方式发生变化。2008年,IBM在外国关系理事会上提出“智慧地球”概念,意在使用先进信息技术改善商业运作和公共服务^[92]。“智慧地球”就是把感应器嵌入和装备到铁路、电网、供水系统、油气管道等各种物体中,普遍连接形成物联网,然后通过多云环境将物联网数据整合起来用人工智能进行分析,植入“智慧”的理念,人们能够以更加精细和动态的方式管理生产和生活,达到全球“智慧”状态。“智慧地球”克服了信息技术应用中零散的、各自为战的现状,从一个总体产业或社会生态系统出发,调动该生态系统中的各个角色,充分发挥先进信息技术的潜力以促进整个生态系统的互动,以更加智慧的方式解决当今世界的重大问题。目前人们普遍接受这一理念,并从“智慧城市”与“智慧企业”做起,逐步向“智慧地球”靠拢,但距离实现目标还很遥远。首先,多云存储技术发展尚不完善,而物联网技术中传感器收集的数据具有海量、异构、移动的特点,很难实现及时处理以适应动态调整。其次,“智慧地球”的实现存在很多安全威胁,可感知、互联互通和更加智能化意味着一切更加透明,更易被操控。最重要的是,实现“智慧地球”需要制定统一的技术框

架和规则,各个国家不会轻易接受其他国家的技术、产品、管理方式和运行模式,都想建立自己的智慧系统,但实际技术水平差异巨大,很难统一。因此,基于多云环境的“智慧地球”还需要不断尝试和探索。

4 结束语

多云存储是目前广受关注的热点研究领域。本文简述了多云存储的概念、体系结构、技术优势、挑战及相关产品,对多云存储相关技术中的数据可靠性保障、数据完整性证明、并发控制方法以及安全重删技术的最新研究进展进行了深入分析和讨论,并展望了多云间数据迁移、数据一致性保证、隐私防护、跨用户重删、云际资源调度、基于多云环境的“智慧地球”应用等若干未来潜在的研究方向。鉴于多云存储技术应用上的复杂性,目前大量研究成果仍停留在理论和试验阶段,未来更为成熟的先进技术推广应用值得期待。

参考文献

- [1] FU Yingxun, LUO Shengmei, SHU Jiwu. Survey of secure cloud storage system and key technologies[J]. Journal of Computer Research and Development, 2013, 50(1): 136-145. (in Chinese)
傅颖勋, 罗圣美, 舒继武. 安全云存储系统与关键技术综述[J]. 计算机研究与发展, 2013, 50(1): 136-145.
- [2] FENG Chaosheng, QIN Zhiguang, YUAN Ding. Techniques of secure storage for cloud data[J]. Chinese Journal of Computers, 2015, 38(1): 150-163. (in Chinese)
冯朝胜, 秦志光, 袁丁. 云数据安全存储技术[J]. 计算机学报, 2015, 38(1): 150-163.
- [3] ZHOU Yuezhi, ZHANG Di. Near-end cloud computing: opportunities and challenges in the post-cloud computing era[J]. Chinese Journal of Computers, 2019, 42(4): 677-700. (in Chinese)
周悦芝, 张迪. 近端云计算: 后云计算时代的机遇与挑战[J]. 计算机学报, 2019, 42(4): 677-700.
- [4] BUYYA R, RANJAN R, CALHEIROS R N. Inter-Cloud: utility oriented federation of cloud computing environments for scaling of application services[C]//Proceedings of the 10th International Conference on Algorithms and Architectures for Parallel Processing. Berlin, Germany: Springer, 2010: 13-31.
- [5] TSAMOURA E, GOUNARIS A, TSICHLAS K. Multi-objective optimization of data flows in a multi-cloud environment[C]//Proceedings of the 2nd Workshop on Data Analytics in the Cloud. New York, USA: ACM Press, 2013: 6-10.
- [6] SuperCloud Consortium. Welcome to SuperCloud[EB/OL]. [2020-04-10]. <https://supercloud-project.eu>.
- [7] PETRI I, DIAZ-MOINTES J, ZOU M, et al. Market models for federated clouds[J]. IEEE Transactions on Cloud Computing, 2015, 3(3): 398-410.
- [8] MATEUSE G, ALICJA G, PASCAL B, et al. Cloud brokering: current practices and upcoming challenges[J]. IEEE Cloud Computing, 2015, 2(2): 40-47.

- [9] SHI Peichang, WANG Huaimin, ZHENG Zibin, et al. Collaboration environment for JointCloud computing [J]. SCIENTIA SINICA Informationis, 2017, 47(9): 1129-1148.
- [10] KOTLA R, ALVISI L, DAHLIN M. SafeStore: a durable and practical storage system [C]//Proceedings of the 12th USENIX Annual Technical Conference. Berkeley, USA: USENIX Association, 2007: 129-142.
- [11] CHEN H C H, HU Y C, LEE P P C, et al. NCCloud: a network-coding-based storage system in a cloud-of-clouds [J]. IEEE Transactions on Computers, 2014, 63(1): 31-44.
- [12] DOBRE D, VIOTTI P, VUKOLIĆ M. Hybris: robust hybrid cloud storage [C]//Proceedings of ACM Symposium on Cloud Computing. New York, USA: ACM Press, 2014: 1-14.
- [13] HAO Z, RANMAN R, PAN H, et al. Optimizing information leakage in multicloud storage services [EB/OL]. [2020-04-10]. <https://www.researchgate.net/publication/323348778>.
- [14] FU Yinjin, QIU Xiaofeng, WANG Jian. F2MC: enhancing data storage services with fog-to-MultiCloud hybrid computing [C]//Proceedings of the 38th IEEE International Conference Performance Computing and Communications. Piscataway, USA: IEEE Press, 2019: 1-6.
- [15] ABULIBDEH H, PRINCHHOUSE L, WEATHERSPOON H. RACS: a case for cloud storage diversity [C]//Proceedings of the 1st ACM Symposium on Cloud Computing. New York, USA: ACM Press, 2010: 453-467.
- [16] WU Z, BUTKIEWICZ M, PERKINS D, et al. SPANStore: cost-effective geo-replicated storage spanning multiple cloud services [J]. ACM SIGCOMM Computer Communication Review, 2013, 43(4): 545-546.
- [17] BERMBACH D, KLEMS M, TAI S, et al. MetaStorage: a federated cloud storage system to manage consistency-latency tradeoffs [C]//Proceedings of the 4th IEEE International Conference on Cloud Computing. Piscataway, USA: IEEE Press, 2011: 452-459.
- [18] GHEMAWAT S, GOBIOFF H, LEUNG S T. The Google file system [J]. ACM SIGOPS Operating Systems Review, 2003, 37(5): 29-43.
- [19] BONVIN N, PAPAIOANNOU T G, ABERER K. A self-organized, fault-tolerant and scalable replication scheme for cloud storage [C]//Proceedings of the 1st ACM Conference on Cloud Computing. New York, USA: ACM Press, 2010: 205-216.
- [20] LIAO Bin, YU Jiong, SUN Hua, et al. A QoS-aware dynamic data replica deletion strategy for distributed storage systems under cloud computing environments [C]//Proceedings of the 2nd International Conference on Cloud and Green Computing. Piscataway, USA: IEEE Press, 2012: 219-225.
- [21] JIA Yaru, LIU Xiangyang, LIU Shengli. Decentralized secure distributed storage system [J]. Computer Engineering, 2012, 38(3): 126-129. (in Chinese)
贾亚茹, 刘向阳, 刘胜利. 去中心化的安全分布式存储系统 [J]. 计算机工程, 2012, 38(3): 126-129.
- [22] ATENIESE G, BURNS R, CURTMOLA R, et al. Provable data possession at untrusted stores [C]//Proceedings of ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2007: 146-157.
- [23] SHACHAM H, WATERS B. Compact proofs of retrievability [J]. Journal of Cryptology, 2013, 26(3): 442-483.
- [24] CAO Ning, WANG Cong, LI Ming, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data [J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(1): 222-233.
- [25] WANG Liangmin, YANG Zhengdong, SONG Xiangmei, et al. SHAMC: a secure and highly available database system in multi-cloud environment [J]. Future Generation Computer Systems, 2017(105): 873-883.
- [26] PRAVIN A, JACOB T P, NAGARAJAN G, et al. Robust technique for data security in multicloud storage using dynamic slicing with hybrid cryptographic technique [J]. Journal of Ambient Intelligence and Humanized Computing, 2019(17): 1-8.
- [27] FAN Yijie, QIAO Zhen, XIAO Mingzhong, et al. One cloud: a secure and anonymous multi-cloud oblivious storage architecture [J]. Applied Mechanics and Materials, 2014(556): 5591-5596.
- [28] BINDSCHAEDLER V, NAVEED M, PAN X, et al. Practicing oblivious access on cloud storage: the gap, the fallacy, and the new way forward [C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM Press, 2015: 837-849.
- [29] LIU Zheli, LI Bo, HUANG Yanyu, et al. NewMCOS: towards a practical multi-cloud oblivious storage scheme [J]. IEEE Transactions on Knowledge and Data Engineering, 2020, 32(4): 714-727.
- [30] XUE Liang, YU Yong, LI Yannan, et al. Efficient attribute-based encryption with attribute revocation for assured data deletion [J]. Information Sciences, 2018(479): 640-650.
- [31] VANITHA M, KAVITHA C. Secured data destruction in cloud based multi-tenant database architecture [C]//Proceedings of International Conference on Computer Communication and Informatics. Coimbatore, India: [s. n.], 2014: 1-6.
- [32] Google Cloud. Anthos: a modern application platform for your business [EB/OL]. [2020-04-10]. <http://cloud.google.com/anthos>.
- [33] IBM Corporation. IBM Cloud Pak for multicloud management [EB/OL]. [2020-04-10]. https://www.ibm.com/support/knowledgecenter/SSFC4F/product_welcome_cloud_pak.html.
- [34] MultCloud Corp. MultCloud-focus on transferring across clouds [EB/OL]. [2020-04-10]. <https://www.multcloud.com>.
- [35] Xingyun Blooming Technology Co., Ltd. Cloud steward cloud management platform [EB/OL]. [2020-04-10]. <https://www.cloudbility.com>. (in Chinese)
行云绽放科技有限公司. 行云管家云管理平台 [EB/OL]. [2020-04-10]. <https://www.cloudbility.com>.
- [36] FIT2CLOUD Information Technology Co., Ltd. FIT2CLOUD [EB/OL]. [2020-04-10]. <https://www.fit2cloud.com>. (in Chinese)
飞致云信息科技有限公司. FIT2CLOUD [EB/OL]. [2020-04-10]. <https://www.fit2cloud.com>.

- [37] Bepin Global Technology Co., Ltd. BESPIN GLOBAL [EB/OL]. [2020-04-10]. <https://www.bespinglobal.cn>. (in Chinese)
贝斯平云科技有限公司. BESPIN GLOBAL[EB/OL]. [2020-04-10]. <https://www.bespinglobal.cn>.
- [38] ZHENG Liming, LI Xiaodong. Low-cost multi-node failure repair method for erasure codes [J]. Computer Engineering, 2017, 43(7): 110-118, 123. (in Chinese)
郑力明, 李晓冬. 面向纠删码的低成本多节点失效修复方法[J]. 计算机工程, 2017, 43(7): 110-118, 123.
- [39] WANG Yijie, LI Sijun. Research and performance evaluation of data replication technology in distributed storage systems [J]. Computers and Mathematics with Applications, 2006, 51(11): 1625-1632.
- [40] PLANK J S, THOMASON M G. An exploration of non-asymptotic low-density, parity check erasure codes for wide-area storage applications [J]. Parallel Processing Letters, 2007, 17(1): 103-123.
- [41] WANG Yijie, XU Fangliang, PEI Xiaoqiang. Research on erasure code-based fault-tolerant technology for distributed storage [J]. Chinese Journal of Computers, 2017, 40(1): 236-255. (in Chinese)
王意洁, 许方亮, 裴晓强. 分布式存储中的纠删码容错技术研究[J]. 计算机学报, 2017, 40(1): 236-255.
- [42] SOLOMON I S R. Polynomial codes over certain finite fields [J]. Journal of the Society for Industrial and Applied Mathematics, 1960, 8(2): 300-304.
- [43] HU Y, YU C M, LI Y K, et al. NCFS: on the practicality and extensibility of a network-coding-based distributed file system [C]//Proceedings of 2011 International Symposium on Network Coding. Piscataway, USA: IEEE Press, 2011: 233-245.
- [44] BESSANI A, CORRIA M, QUARESMA B, et al. DEPSKY: dependable and secure storage in a cloud-of-clouds [J]. ACM Transactions on Storage, 2013, 9(4): 12.
- [45] BOEERS K D, JUELS A, OPREA A. HAIL: a high-availability and integrity layer for cloud storage [C]//Proceedings of the 16th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2009: 187-198.
- [46] AHLWEDE R, CAI N, LI S Y R, et al. Network information flow [J]. IEEE Transactions on Information Theory, 2000, 46(4): 1204-1216.
- [47] TAN Shuang, JIA Yan, HAN Weihong. Research and development of provable data integrity in cloud storage [J]. Chinese Journal of Computers, 2015, 38(1): 164-177. (in Chinese)
谭霜, 贾焰, 韩伟红. 云存储中的数据完整性证明研究及进展[J]. 计算机学报, 2015, 38(1): 164-177.
- [48] CURTMOLA R, KHAN O, BURNS R, et al. MR-PDP: multiple-replica provable data possession [C]//Proceedings of the 28th International Conference on Distributed Computing Systems. Piscataway, USA: IEEE Press, 2008: 411-420.
- [49] ERWAY C C, PAPAMANTHOU C, TAMASSIN R. Dynamic provable data possession [J]. ACM Transactions on Information and System Security, 2015, 17(4): 1-29.
- [50] WANG Cong, WANG Qian, REN Kui, et al. Privacy-preserving public auditing for data storage security in cloud computing [C]//Proceedings of IEEE INFOCOM'10. Piscataway, USA: IEEE Press, 2010: 1-9.
- [51] ATENIESE G, BURNS R, CURTMOLA R, et al. Provable data possession at untrusted stores [C]//Proceedings of the 14th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2007: 598-609.
- [52] JUELS A, JR B S K. PORs: proofs of retrievability for large files [C]//Proceedings of ACM Conference on Computer & Communications Security. New York, USA: ACM Press, 2007: 108-119.
- [53] CHEN B, CURTMOLA R. Robust dynamic remote data checking for public clouds [C]//Proceedings of 2012 ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2012: 1043-1045.
- [54] CAO Laicheng, HE Wenwen, LIU Yufei, et al. An integrity verification scheme of completeness and zero-knowledge for multi-cloud storage [J]. International Journal of Communication Systems, 2017, 30(16): 3324-3335.
- [55] PEI Xin, LIN Jiuchuan, JIN Bo, et al. Ensuring replication-based data integrity and availability in multicloud storage [C]//Proceedings of the 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. Piscataway, USA: IEEE Press, 2016: 687-692.
- [56] LEVY D. Zookeeper [C]//Proceedings of ACM SIGGRAPH Conference on Computer Animation Festival. New York, USA: ACM Press, 2011: 458-469.
- [57] DECANDIA G, HASTORUN D, JAMPANI M, et al. Dynamo: amazon's highly available key-value store [J]. ACM SIGOPS Operating Systems Review, 2007, 41(6): 205-220.
- [58] PAPAIOANNOU T G, BONVIN N, ABERER K. Scalia: an adaptive scheme for efficient multi-cloud storage [C]//Proceedings of International Conference on High Performance Computing, Networking, Storage and Analysis. Piscataway, USA: IEEE Computer Society Press, 2012: 20-31.
- [59] E Jinlong, CUI Yong, WANG Peng, et al. Cocloud: enabling efficient cross-cloud file collaboration based on inefficient Web APIs [J]. IEEE Transactions on Parallel and Distributed Systems, 2017, 29(1): 56-69.
- [60] XIE Fei, YAN Jun, SHEN Jun. A bandwidth and latency based replica selection mechanism for data-intensive workflow applications in the multi-cloud environment [C]//Proceedings of Australasian Computer Science Week Multi-Conference. New York, USA: ACM Press, 2020: 1-8.
- [61] SHI Tao, MA Hui, CHEN Gang, et al. Location-aware and budget-constrained service deployment for composite applications in multi-cloud environment [J]. IEEE Transactions on Parallel and Distributed Systems, 2020, 31(8): 1954-1969.
- [62] FU Yinjin, XIAO Nong, LIU Fang. Research and development on key techniques of data deduplication [J]. Journal of Computer Research and Development, 2012, 49(1): 12-20. (in Chinese)
付印金, 肖依, 刘芳. 重复数据删除关键技术研究进展[J]. 计算机研究与发展, 2012, 49(1): 12-20.
- [63] XIONG Jinbo, ZHANG Yuanyuan, LI Fenghua, et al. Research progress on secure data deduplication in cloud [J]. Journal on Communications, 2016, 37(11): 169-180. (in Chinese)
熊金波, 张媛媛, 李风华, 等. 云环境中数据安全去重研究进展[J]. 通信学报, 2016, 37(11): 169-180.

- [64] MAO Bo, YE Geyan, LAN Yanjia, et al. A data deduplication-based primary storage system in cloud-of-clouds[J]. Journal of Computer Research and Development, 2015, 52(6): 1278-1287. (in Chinese)
毛波, 叶阁焰, 蓝琰佳, 等. 一种基于重复数据删除技术的云中云存储系统[J]. 计算机研究与发展, 2015, 52(6): 1278-1287.
- [65] RADE P, BARKADE V M. A cost efficient multi-cloud data hosting using heuristic data placement algorithm [C]// Proceedings of the 2nd International Conference on Inventive Systems and Control. Piscataway, USA: IEEE Press, 2018: 403-407.
- [66] LIU Jian, ASOKAN N, PINKAS B. Secure deduplication of encrypted data without additional independent servers [C]// Proceedings of ACM SIGSAC Conference on Computer & Communications Security. New York, USA: ACM Press, 2015: 132-147.
- [67] LI Mingqiang, QIN Chuan, LI Jingwei, et al. CDStore: toward reliable, secure, and cost-efficient cloud storage via convergent dispersal [J]. IEEE Internet Computing, 2016, 20(3): 45-53.
- [68] SHEN Lu, FENG Shifang, SUN Jinjin, et al. CloudS: a multi-cloud storage system with multi-level security [J]. IEICE Transactions on Information and Systems, 2016, 99(8): 2036-2043.
- [69] LI Yandong, ZHU Lichuang, SHEN Meng, et al. CloudShare: towards a cost-efficient and privacy-preserving alliance cloud using permissioned blockchains [C]// Proceedings of International Conference on Mobile Networks and Management. Berlin, German: Springer, 2017: 339-352.
- [70] XIAO Liang, LI Qiangda, LIU Jinliang. Survey on secure cloud storage [J]. Journal of Data Acquisition & Processing, 2016, 31(3): 464-472. (in Chinese)
肖亮, 李强达, 刘金亮. 云存储安全技术研究进展综述[J]. 数据采集与处理, 2016, 31(3): 464-472.
- [71] SHI Weisong, SUN Hui, CAO Jie, et al. Edge computing-an emerging computing model for the internet of everything era [J]. Journal of Computer Research and Development, 2017, 54(5): 907-924. (in Chinese)
施巍松, 孙辉, 曹杰, 等. 边缘计算: 万物互联时代新型计算模型 [J]. 计算机研究与发展, 2017, 54(5): 907-924.
- [72] ABDELBAKY M, DIAZ-MONTES J, PARASHAR M, et al. Docker containers across multiple clouds and data centers [C]// Proceedings of the 8th International Conference on Utility and Cloud Computing. Piscataway, USA: IEEE Press, 2015: 368-371.
- [73] BREWER E A. Towards robust distributed systems [C]// Proceedings of the 19th Annual ACM Symposium on Principles of Distributed Computing. New York, USA: ACM Press, 2000: 768-779.
- [74] PRITCHETT D. Base: an acid alternative [J]. Queue, 2008, 6(3): 48-55.
- [75] LI Zhenhao. Design and implementation of cloud platform supporting multi-cloud collaboration [D]. Beijing: Beijing University of Posts and Telecommunications, 2019. (in Chinese)
李振豪. 支持多云协作的云平台的设计与实现 [D]. 北京: 北京邮电大学, 2019.
- [76] GRAY J, LAMPORT L. Consensus on transaction commit [J]. ACM Transactions on Database Systems, 2006, 31(1): 133-160.
- [77] LIU Y A, CHAND S, STOLLER S D. Moderately complex Paxos made simple: high-level executable specification of distributed algorithms [C]// Proceedings of the 21st International Symposium on Principles and Practice of Programming Languages. New York, USA: ACM Press, 2019: 15-29.
- [78] JUNQUEIRA F P, REED B C, SERAFINI M. Zab: high-performance broadcast for primary-backup systems [C]// Proceedings of IEEE/IFIP International Conference on Dependable Systems & Networks. Piscataway, USA: IEEE Press, 2011: 589-594.
- [79] ZHANG Chendong, GUO Jinwei, LIU Bozhong, et al. High availability implementation based on Raft [J]. Journal of East China Normal University: Natural Science, 2015, 2015(5): 172-184. (in Chinese)
张晨东, 郭进伟, 刘柏众, 等. 基于 Raft 一致性协议的高可用性实现 [J]. 华东师范大学学报 (自然科学版), 2015(5): 172-184.
- [80] LI Hui, SUN Wenhui, LI Fenghua, et al. Secure and privacy-preserving data storage service in public cloud [J]. Journal of Computer Research and Development, 2014, 51(7): 1397-1409. (in Chinese)
李晖, 孙文海, 李风华, 等. 公共云存储服务数据安全及隐私保护技术综述 [J]. 计算机研究与发展, 2014, 51(7): 1397-1409.
- [81] KE Changbo, HUANG Zhiqiu. Privacy requirement description and checking method in cloud computing [J]. Journal of Computer Research and Development, 2015, 52(4): 879-888. (in Chinese)
柯昌博, 黄志球. 云计算环境下隐私需求的描述与检测方法 [J]. 计算机研究与发展, 2015, 52(4): 879-888.
- [82] KOLLER R, RANGASWAMI R. I/O deduplication: utilizing content similarity to improve I/O performance [J]. ACM Transactions on Storage, 2010, 6(3): 211-224.
- [83] CHEN Feng, LUO Tian, ZHANG Xiaodong. CAFTL: a content-aware flash translation layer enhancing the lifespan of flash memory based solid state drives [C]// Proceedings of the 9th USENIX Conference on File & Storage Technologies. Berkeley, USA: USENIX Association, 2019: 77-90.
- [84] LIU Yining, ZHOU Yuanjian, LAN Rushi, et al. Blockchain-based verification scheme for deletion operation in cloud [J]. Journal of Computer Research and Development, 2018, 55(10): 2199-2207. (in Chinese)
刘忆宁, 周元健, 蓝如师, 等. 基于区块链的云数据删除验证协议 [J]. 计算机研究与发展, 2018, 55(10): 2199-2207.
- [85] CHEN Weili, ZHENG Zibin. Blockchain data analysis: a review of status, trends and challenges [J]. Journal of Computer Research and Development, 2018, 55(9): 1853-1870. (in Chinese)
陈伟利, 郑子彬. 区块链数据分析: 现状、趋势与挑战 [J]. 计算机研究与发展, 2018, 55(9): 1853-1870.

(上接第 32 页)

- [86] HE Haiwu, YAN An, CHEN Zehua. Survey of smart contract technology and application based on blockchain[J]. Journal of Computer Research and Development, 2018, 55(11): 2452-2466. (in Chinese)
贺海武, 延安, 陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 2452-2466.
- [87] WANG Binfeng, SU Jinshu, CHEN Lin. Review of the design of data center network for cloud computing[J]. Journal of Computer Research and Development, 2016, 53(9): 2085-2106. (in Chinese)
王斌锋, 苏金树, 陈琳. 云计算数据中心网络设计综述[J]. 计算机研究与发展, 2016, 53(9): 2085-2106.
- [88] SHI Xuelin, XU Ke. Utility maximization model of virtual machine scheduling in cloud environment[J]. Chinese Journal of Computers, 2013, 36(2): 252-262. (in Chinese)
师雪霖, 徐恪. 云虚拟机资源分配的效用最大化模型[J]. 计算机学报, 2013, 36(2): 252-262.
- [89] KURDI H, ALSALAMAH S, ALATAWI A, et al. Healthybroker: a trustworthy blockchain-based multi-cloud broker for patient-centered ehealth services[J]. Electronics, 2019, 8(6): 1-17.
- [90] LI Zhiyong, CHEN Shaomiao, YANG Bo, et al. Multi-objective memetic algorithm for task scheduling on heterogeneous cloud[J]. Chinese Journal of Computers, 2016, 39(2): 377-390. (in Chinese)
李智勇, 陈少森, 杨波, 等. 异构云环境多目标 Memetic 优化任务调度方法[J]. 计算机学报, 2016, 39(2): 377-390.
- [91] PAN Chen, LIU Zhiqiang, LIU Zhen, et al. Research on scalability of blockchain technology: problems and methods[J]. Journal of Computer Research and Development, 2018, 55(10): 2099-2110. (in Chinese)
潘晨, 刘志强, 刘振, 等. 区块链可扩展性研究: 问题与方法[J]. 计算机研究与发展, 2018, 55(10): 2099-2110.
- [92] XU Ye, MENG Hong, CHENG Jiayu, et al. The stratagem of IBM's smarter planet and china's countermeasures[J]. Forum on Science and Technology in China, 2010(4): 20-23. (in Chinese)
许晔, 孟弘, 程家瑜, 等. IBM“智慧地球”战略与我国的对策[J]. 中国科技论坛, 2010(4): 20-23.

编辑 索书志