

# 云服务资源管理 方法与技术

吴庆涛 郑瑞娟 张明川 著



 科学出版社

# 云服务资源管理方法与技术

吴庆涛 郑瑞娟 张明川 著

科学出版社

北京

## 内 容 简 介

本书在归纳分析国内外关于云服务资源管理相关研究的基础上,从云服务资源的选择、组合、推荐、评价等角度研究云服务资源的管理机制与方法,并基于信誉评价和安全隔离研究云资源的安全问题。

本书可以作为高等院校计算机科学与技术专业硕士研究生、博士研究生的专业课教材,也可作为云计算研究领域科技人员的参考书。

### 图书在版编目(CIP)数据

云服务资源管理方法与技术 / 吴庆涛,郑瑞娟,张明川著. —北京:科学出版社,2018.6

ISBN 978-7-03-056186-2

I. ①云… II. ①吴… ②郑… ③张… III. ①互联网络-应用-资源管理(电子计算机) IV. ①TP316

中国版本图书馆 CIP 数据核字(2017)第 321174 号

责任编辑:孙伯元 / 责任校对:郭瑞芝

责任印制:张 伟 / 封面设计:蓝正设计

科学出版社 出版

北京东黄城根北街 16 号

邮政编码:100717

<http://www.sciencep.com>

北京中石油彩色印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

\*

2018 年 6 月第 一 版 开本:720×1000 B5

2018 年 6 月第一次印刷 印张:13 3/4

字数:270 000

定价:98.00 元

(如有印装质量问题,我社负责调换)

## 前 言

云计算是以网络服务和应用为中心的新兴服务计算模式,它通过管理、调度与整合分布在网络上的各种资源,以虚拟化的方式为用户提供可缩减或可扩展的计算资源,增加了用户对计算系统的规划、购置、占有和使用的灵活性。在云计算中,用户所关心的核心问题不是计算资源本身,而是所能获取的服务。从这个角度出发,服务问题(即服务的提供和使用)已成为影响和推动云计算技术与产业发展的重要因素。

本质上讲,云计算是以互联网技术为基础,由网络中各类资源(包括计算资源、存储资源、软件资源、平台资源等)组成的一个分布式服务集群系统,其目标是大量用户/终端提供各类在线服务。因此,云服务的管理成为服务提供商、用户和云计算科学研究者共同关注的问题。

从服务提供商的角度来看,面对不断变化的用户需求,在部署、管理和维护海量、异构的软硬件资源的基础上,需要监控并动态重构网络资源,以快速响应用户提交的服务请求,并提供安全、高质量的服务等。

从用户的角度来看,无须大量购置软硬件设备即可方便地获得稳定可靠的专业服务。然而,由于远离数据和计算资源,面对众多可选的云服务以及多租户共享应用服务模式,消费者及其终端用户没有足够的信息来甄别服务的优劣以及服务是否安全可靠;此外,对于云服务是否能够正确、安全、高效地满足自身真实、完整的应用需求,消费者也会有诸多疑问。

从云计算科学研究者的角度来看,云服务是由多种服务聚合成的端到端组合服务。不同的云服务简单组合在一起,虽然能够满足一般性服务需求(主要包括费用、响应时间、可靠性、可用性以及执行成功率等),但是,由于云服务是一种没有集中控制且不提供全局模型的资源组织和服务提供形式,要实现用户的动态需求和云服务提供之间的按需聚合,需要在对其资源属性进行正确分类的前提下,公正合理地评价各类功能互补或重叠的相同或相似云服务的信誉,并优化云服务的资源组合与安全性能。

因而,基于现有海量的云服务,立足满足用户不确定的、动态变化的需求,研究

细粒度的计算资源划分、评估、组合、优化及安全保障,提高云服务的精准性、安全性、有效性和适应性,提升云服务功能分配的自主管理能力,增强用户对云服务的信任度,构建自主的云资源管理技术与方法,成为云服务领域亟待研究的崭新课题。

本书得到国家自然科学基金(61370221,U1404611,U1604155,61602155)的资助,由河南科技大学的吴庆涛教授、郑瑞娟副教授和张明川副教授共同撰写完成。其中,吴庆涛教授完成15万字,郑瑞娟副教授完成了6万字,张明川副教授完成了6万字。在撰写本书的过程中,作者得到了河南科技大学的朱军龙博士、赵海霞副教授、白秀玲副教授、魏汪洋博士以及河南省云计算与信息服务工程技术研究中心的宁召宇、侯敏杰、汪兴、李晨、蔡晓刚、刘娜娜、崔敏、张旭龙、闫金荣、杜娟等研究生的支持与帮助,在这里一并表示感谢。

限于作者水平,本书难免存在不妥之处,望广大读者批评指正。

作者

2017年7月

# 目 录

## 前言

第 1 章 绪论	1
1.1 云服务发展历程	1
1.2 服务体系架构	3
1.2.1 面向服务的体系结构	3
1.2.2 基于云服务 QoS 技术框架	5
1.3 云服务关键技术	6
1.3.1 云数据存储技术	6
1.3.2 虚拟化技术	10
1.3.3 安全访问控制技术	11
1.4 本章小结	13
参考文献	13
第 2 章 云服务选择机制	16
2.1 引言	16
2.2 相关技术	17
2.2.1 服务选择	17
2.2.2 服务描述	18
2.2.3 服务匹配	18
2.2.4 服务分类	19
2.2.5 云服务组合	20
2.3 基于模糊 QoS 的云服务资源选择方法	21
2.3.1 基于 Chord 环的虚拟云服务资源检索	21
2.3.2 QoS 属性的描述及归一化	22
2.3.3 用户 QoS 属性偏好信息的模糊表示	25
2.3.4 QoS 属性匹配矩阵构造算法	26
2.3.5 仿真与结果分析	26

2.4	本章小结 .....	28
	参考文献 .....	29
<b>第3章</b>	<b>基于 QoS 的服务组合机制 .....</b>	<b>32</b>
3.1	引言 .....	32
3.2	基于虚拟 Chord 环的云服务组合算法 .....	33
3.2.1	云服务组合系统模型 .....	33
3.2.2	基于 Chord 环的服务组合算法 .....	36
3.2.3	仿真实验 .....	39
3.3	基于 Map-Reduce 的分布式云服务组合算法 .....	41
3.3.1	QoS 描述 .....	41
3.3.2	QoS 属性值的标准化 .....	43
3.3.3	服务资源的哈希表示 .....	43
3.3.4	Top-k 算法描述 .....	44
3.3.5	Map-Reduce 编程模型 .....	45
3.3.6	基于 Map-Reduce 的 Top-k 服务组合算法 .....	47
3.3.7	实验 .....	49
3.4	基于细菌觅食优化算法的云服务优化组合 .....	51
3.4.1	云服务组合描述 .....	51
3.4.2	基于改进细菌觅食优化算法的服务组合 .....	52
3.4.3	细菌觅食优化算法 .....	53
3.4.4	算法结构 .....	57
3.4.5	仿真实验与分析 .....	58
3.5	本章小结 .....	59
	参考文献 .....	59
<b>第4章</b>	<b>云服务个性化推荐方法 .....</b>	<b>61</b>
4.1	引言 .....	61
4.2	相关技术 .....	62
4.2.1	复杂网络介绍 .....	62
4.2.2	基于二部图的推荐算法原理 .....	63
4.2.3	算法优越性分析 .....	64
4.3	基于 Chord 环的加权二部图推荐算法 .....	65

4.3.1	加权二部图推荐算法 .....	66
4.3.2	云服务推荐机制 .....	67
4.3.3	算法描述 .....	71
4.3.4	仿真与结果分析 .....	73
4.4	云计算环境下加权二部图推荐算法设计 .....	76
4.4.1	资源分配矩阵 $W$ 的计算 .....	76
4.4.2	预测项目评分 .....	78
4.4.3	实验与分析 .....	79
4.5	本章小结 .....	81
	参考文献 .....	81
<b>第 5 章</b>	<b>基于 QoS 的云服务评价方法 .....</b>	<b>82</b>
5.1	引言 .....	82
5.2	基于主成分分析的云服务 QoS 评价算法 .....	83
5.2.1	云服务 QoS 评价指标 .....	83
5.2.2	云服务 QoS 量化评价算法 .....	84
5.2.3	仿真实验及结果分析 .....	87
5.3	基于模糊层次分析法的云服务评价方法 .....	91
5.3.1	相关理论 .....	91
5.3.2	云服务评价方法 .....	94
5.3.3	仿真实验过程及结果分析 .....	96
5.4	本章小结 .....	99
	参考文献 .....	99
<b>第 6 章</b>	<b>云服务的信誉评价机制 .....</b>	<b>100</b>
6.1	引言 .....	100
6.2	基于 QoS 和相似用户推荐的云服务信誉评价模型 .....	101
6.2.1	QoS 的预处理 .....	101
6.2.2	基于相似用户的服务推荐度 .....	102
6.2.3	云服务的信誉度评价模型 .....	105
6.2.4	仿真实验与结果分析 .....	107
6.3	基于用户可信度的云服务资源信誉管理策略 .....	110
6.3.1	面向云服务的信誉评价模型及相关定义 .....	110



6.3.2	云服务信誉值的分布式计算	112
6.3.3	基于用户可信度的信誉修正	112
6.3.4	基于惩罚的信誉评价动态激励机制	114
6.3.5	仿真与结果分析	116
6.4	本章小结	118
	参考文献	119
<b>第7章</b>	<b>云资源虚拟化管理机制</b>	<b>120</b>
7.1	引言	120
7.2	基于擦除码的云存储数据冗余方案	121
7.2.1	简化的云存储系统模型	121
7.2.2	数据编码存储与恢复	122
7.2.3	云存储数据块高效检索	124
7.2.4	实验测试与结果	126
7.3	基于特征相似度的云服务资源分类	130
7.3.1	改进的朴素贝叶斯分类算法	130
7.3.2	分类算法的并行化	132
7.3.3	仿真实验与结果分析	135
7.4	面向云服务的资源虚拟化模型	137
7.4.1	Xen 虚拟化技术	137
7.4.2	虚拟化模型	138
7.4.3	基于 Xen 的 PBS 集群系统	139
7.4.4	仿真实验	140
7.5	本章小结	141
	参考文献	141
<b>第8章</b>	<b>融合信誉评价的云存储安全优化方法</b>	<b>143</b>
8.1	引言	143
8.2	面向云存储服务的自主信誉管理机制	144
8.2.1	云服务信誉机制	144
8.2.2	信誉修正	150
8.2.3	实验与分析	157
8.3	融合信誉机制的云存储模型	160

8.3.1	融合信誉评价的云存储模型 .....	160
8.3.2	安全威胁及分析 .....	167
8.4	高可用的云存储冗余优化方法 .....	168
8.4.1	云存储系统模型 .....	168
8.4.2	数据编码存储与恢复 .....	169
8.4.3	云存储高效检索方法 .....	172
8.4.4	实验与结果分析 .....	174
8.5	本章小结 .....	178
	参考文献 .....	178
<b>第9章</b>	<b>云资源的安全性预测及隔离技术 .....</b>	<b>180</b>
9.1	引言 .....	180
9.2	中国安全墙模型简介 .....	181
9.2.1	中国安全墙模型概述 .....	181
9.2.2	中国安全墙模型数据组织 .....	181
9.2.3	基于中国安全墙模型的访问策略 .....	182
9.3	基于模糊决策树的敏感信息预测方法 .....	184
9.3.1	基于模糊 C 均值聚类算法的单一属性聚类 .....	184
9.3.2	模糊决策树的构建 .....	186
9.3.3	基于模糊决策树的敏感信息预测方法 .....	190
9.3.4	实验结果及分析 .....	191
9.4	基于中国安全墙模型的虚拟隔离技术 .....	195
9.4.1	利益冲突的关系数据模型 .....	195
9.4.2	基于动态分集的中国安全墙模型 .....	197
9.4.3	模型的安全性及其应用 .....	200
9.4.4	仿真实验及性能分析 .....	202
9.5	本章小结 .....	206
	参考文献 .....	206
<b>第10章</b>	<b>云服务的发展 .....</b>	<b>207</b>

# 第 1 章 绪 论

云计算的概念被谷歌公司提出之后,受到世界范围的关注。为了率先占领市场,争夺市场份额,各大公司陆续推出了自己的云计算产品。部分国外公司建立了云计算基地并推出了云计算计划,拥有了私有云和公有云。例如,要在世界多个城市建立云计算中心的 IBM“蓝云”计划;在弹性云计算基础上全面进军云服务的亚马逊网络服务。英特尔、雅虎等公司也都推出自己的云计算产品,抢占市场。目前,云计算已经完成了从抽象到具体的转变,并将概念和理论转化为生产力,推动信息技术的发展。

国内云计算的发展主要为两方面:一方面,很多公司关注云计算,并推出自己的产品服务于大众;另一方面,仍有不少公司由于各种原因并没有加入云计算大军,处于观望状态。虽然云计算的概念从提出到应用于实践是一个漫长的过程,但是云计算模式所体现出来的价值会被更多的公司认知,这就能推动其发展和壮大,因此,云计算前景良好。

## 1.1 云服务发展历程

有别于传统计算的新型计算技术,云计算具有动态性和易扩展性。它依靠网络的互联性,以虚拟化的方式向大众提供服务。它将分散在世界各地的物理资源、软件资源、网络资源等统一管理起来,形成虚拟化资源池。它按照用户个性化需求动态部署安全可靠的虚拟化服务,用户无须了解资源的来源,以很低的费用就能享受到良好的服务。同时,它还是一类由一系列计算机组成的并行分布式系统,能够高效处理大规模的数据,计算能力堪比大型计算机。

云计算体系结构分为四层:物理资源层、资源池层、管理中间件层和面向服务体系架构(service-oriented architecture, SOA)构建层,如图 1-1 所示。

(1)物理资源层包括计算机、存储器、网络设备、数据库和软件等。

(2)资源池层是对物理资源层的一种同构处理,使与物理资源层相同类型的资源转换成同构的资源,便于统一管理。

(3)管理中间件层管理着各种物理资源,统一调整和部署多个服务任务,使对外提供的服务拥有安全性和高效性。

(4)SOA 构建层将各种服务封装成标准的服务,完成服务的注册、查找、访问并建立 workflow。



图 1-1 云计算体系结构

云计算是一种不同于以往互联网应用和单机计算的模式,具有如下特点:

(1)虚拟化技术。虚拟化技术是一种资源管理方法,将各种网络资源和应用进行逻辑化。每一个物理设施和应用都是相互独立的,通过虚拟化方法部署这些应用时,各个应用之间互不干涉。同时,虚拟化管理平台还管理着应用的扩展、迁移、备份和操作。

(2)动态可扩展。动态可扩展建立在虚拟化方法的基础之上。对于已部署的应用,可以将现有服务资源实时地加入当前应用,无须用新应用替换当前的应用,就可提高云计算的能力。

(3)按需部署。不同的用户对资源和计算能力的需求是有差异的,云计算中心可以根据不同的要求,分别提供切合实际的服务。

(4)高灵活性。云计算环境下的服务多种多样,可以很好地兼容不同厂家产品,体现出了很高的灵活性,便于对服务的虚拟化和管理。目前,大部分的软件和硬件都能很好地支持虚拟化技术。在云计算中,软硬件、网络存储和操作系统等都要先进行虚拟化处理,才能通过虚拟化技术提供给用户使用。

(5)高可靠性。高可靠性同样基于虚拟化方法,用户的请求并不是由同一计算节点来完成,而是由多个计算节点共同完成的。当某一计算节点崩溃时,可以通过动态扩展方法将新计算节点加入当前任务,接替原先节点的任务为用户服务。

(6)高性价比。云计算通过虚拟化方法控制所有的物理设施和软件,对单个资源的服务能力要求不高,无须购买昂贵的服务器,使用便宜的计算资源达到的计算能力就可以和昂贵的服务器相提并论。

云计算的崛起使其他行业商业模式发生着重大的变化,其发展趋势可归纳为以下几方面:

(1)标准和技术越来越规范化。云计算的体系结构标准化程度还不够,对云计算的发展有很大的阻力。在研究和推出云计算产品时,不同的厂家采用不同的标准,这导致各个厂家之间的硬件不兼容,无法共同合作推动云计算的发展。只有统一云计算研究和应用的相关标准与技术,才能使云计算更加快速地普及,为用户提供更好的服务,使用户可以在不同的云计算厂商之间自由切换。

(2)数据趋向安全化。云环境下数据安全<sup>[1]</sup>是每个用户高度关注的焦点,体现在两方面:一方面,用户存储在云上的数据会不会遭到损坏,用户能否获得正确的数据;另一方面,数据放在云服务器上会不会被非法访问和盗用。由于云计算是在传统网络技术基础之上发展起来的,增加了很多新技术,因此不仅具有传统的安全问题,还具有新的安全问题。数据安全问题能否得到认真对待关系到用户对云计算的信任程度和使用程度。随着时间的推移,数据安全问题正在逐步解决。

(3)网络性能趋向优化。云计算是一种基于互联网的计算机模式,通过互联网给用户存储、计算的服务,就必然会增加网络通信的压力。要想使用高质量的云计算服务,就要保证接入的网络具有合适的宽带和稳定的网络环境。因此,云计算的成长使网络服务向着安全和稳定的方向发展,从而加速网络性能的优化。

由于没有对硬件和规划做充分的准备,目前云计算在发展中出现了很多问题。借鉴前期实践经验,在云计算后期应用中,很多问题都能找到可行的解决方案。只有不断克服困难,云计算才能快速健康的发展,推动全球信息化,服务于大众。

## 1.2 服务体系架构

### 1.2.1 面向服务的体系结构

面向服务计算(service-oriented computing, SOC)是当前最新的一种计算方式,可以将服务当成最基础的组件支撑快速、低成本的分分布式乃至异构环境的应用。SOC重点关注遍布在各个节点的服务,利用网络之间的连接和沟通,以独立运行方式实现分分布式应用开发与集成。因此,当服务需求和环境参数发生改变时可以进行动态调整。基于服务计算产生了一种高层次的软件开发方法,即面向服务的体系架构,在应用程序中,它可以把有差别的功能单元当成服务,把此类服务相互间的接口和契约关联在一起,选取中立的形式为接口实行概括,接口与实际

的硬件平台、编程语言以及操作系统是相互独立的。面向服务体系架构具有全自动的、基于服务的组织计算资源、松散耦合、间接服务寻址等特点,其协作框架如图 1-2 所示。

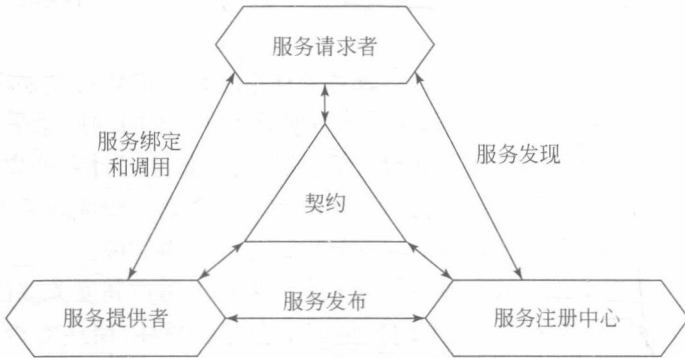


图 1-2 面向服务体系架构的协作框架图

在图 1-2 中,服务提供者发布与平台无关的服务,然后利用互联网在服务注册中心上发布相关的契约以及服务描述文档。服务注册中心在得到相关的文档后,对此文档的数据进行修改来注册服务,对服务的发布、管理起到支撑作用,可以为服务请求者以后的查询服务提供支持。服务注册中心依据服务请求者的服务请求发布描述文档信息,服务请求者能够完成与自身有联系的服务绑定和调用。

对比之前的服务体系结构,SOA 的不同之处在于它的实现技术和业务逻辑无关,表现在以下几个方面:

- (1)松散耦合。云服务相互间的关联度很低,服务逻辑彼此独立。
- (2)可组合性。对于功能不一样的服务,能够彼此组合产生更强功能的服务。
- (3)复用特性。利用复用服务可以处理业务流程和自动化不相关的业务功能。
- (4)互操作性。每个服务之间能够相互操作,服务的信息也能够共享。
- (5)可扩展性。能够采用融合和增加其他服务的方法来扩展已有的服务。

(6)动态演化性。服务的交互关系和数目是根据服务需求变化而变化的,能够对已有的资源重新配置。

SOA 和云计算的概念之间存在着内在联系,云计算应用软件是基于 SOA 系统软件架构的。它致力于解决在网络环境中各种业务架构相互间的问题。云计算就是上述面向服务架构中的一种更适合解决云环境下各类应用问题的方法。当需要合理构建一个信息系统时,SOA 是一种十分合理的架构方法,通过利用 SOA 的机制能够让系统更加合理地运转和协作,使用这种动态虚拟化技术整合网络资源,云服务对于绝大多数用户来说是安全可靠的。

## 1.2.2 基于云服务 QoS 技术框架

本书对云服务给出以下定义:云服务是一个规模巨大的网络资源库,不用进行前期投入,根据用户的服务请求能够获取所需服务,能够保障用户在使用云服务过程中的安全性和可靠性。目前最常见的云服务有以下几种:谷歌公司开发的 Gmail 和 Google App Engine 服务,苹果公司开发的 iCloud 的服务,亚马逊公司的云计算平台服务(Amazon Web service, AWS)等。

服务质量(quality of service, QoS)已经成为目前计算机网络界的热门问题。QoS 是网络技术的核心问题之一。最初对 QoS 的定义是:QoS 是一个综合全面的评价指标,适用于评估服务对用户的满意程度。一般而言, QoS 通常是指服务供应商利用互联网给用户供应服务时要满足的一系列请求。它给 Web 服务提供了多种多样的非功能属性描述。现在,国内外的一些知名学者从多种不同的角度为 Web 服务的 QoS 属性进行了建模,按照他们的理解定义出了很多不同的 QoS 属性。

在云环境中,所有的软件服务一定要在云上运转,用户能够依照自身的需求在网络中租用软件,调节软件个性化设置和所占用的资源。与传统软件相比,在云环境下,软件有以下显著的特点:

- (1)当用户需要使用软件时,请求者不用在自身实际的终端上真正运行软件,只须在网络上进行注册和客户化。
- (2)与之前相比,请求者不具有软件的拥有权,只是软件的租赁者。
- (3)网站的角色在慢慢转变,从传统的信息发布转变成当前的应用软件运行平台,能够同时满足多个租户在此平台上运行软件。
- (4)应用软件的过程不在自身实际的终端上,而是在网络上的数据中心。
- (5)与传统软件相比,云平台软件具有弹性伸缩,依据需求动态调节。
- (6)可定制性。
- (7)发展迅速。

现在,有必要把软件的技术架构和业务模式以及企业组织结构进行深入的改革,以此来处理不停变化的运营环境和服务模式。目前的软件运行管理模式按照用户需求动态供应各个有关联的服务,随着用户对云服务质量的要求越来越高,云应用中一定要持续提升 QoS。

松散耦合、粗粒度、可伸缩特性、动态绑定是云服务的主要特点,而保密性和安全性是云服务的基础前提。因此,云服务对支持软件基础架构平台的性能、可靠性、伸缩性都提出了很高的要求。单一云服务 QoS 可以实现的关键技术方法是云服务 QoS 技术体系,它由很多云服务构成。按照云服务所在的层次不同,云服务又能够分为以下三类。

- (1)云基础设施服务。此类型服务任务是给其他上层服务提供精确可靠的数

据、网络计算以及虚拟化等服务。

(2)云基础服务。基础软件服务层用来支撑云应用服务,为不同类别云服务提供共性信息服务。

(3)云应用服务。对于以前软件响应时间长、规模小、可靠性低等缺陷,云服务在事件采集、关联分析、故障避免等方面都做出了很大的改善,提供了大规模服务和海量存储能力。因此,能够构建大规模的处理平台提升网络性能。

## 1.3 云服务关键技术

### 1.3.1 云数据存储技术

在云服务资源存储中,网络环境复杂多变,如何有效保护云用户个人的信息,以及保障资源数据的完整性、可靠性和可用性,提升存储空间利用率成为需要深入研究的内容。致力于这一研究目标,目前相关的云数据存储技术研究主要包括基于加密的访问控制方法、数据冗余灾备和分布式数据存储。

#### 1. 基于加密的访问控制方法

访问控制<sup>[2,3]</sup>是通过授予一部分用户访问数据的合法权限,而禁止其他的非法用户对数据进行访问的一种安全防范和控制策略。通过访问控制能够实现用户存储数据的机密性,并且保护用户的个人隐私。在复杂多变的云计算环境下,构建一个通用、高效、精确和灵活的访问控制机制<sup>[4]</sup>具有重要的意义。

由于具有弹性服务和无处不在的访问等特点,云计算已经变成最受欢迎的网络应用模式。企业和个人将他们的数据存储迁移至云端,通过访问丰富的云资源来获取可靠的数据服务。云计算产业在带来机会的同时也对用户数据的安全提出了挑战。对云服务用户来说,他们的私人数据不是存储在本地而是在云端,数据的配置和管理,用户拥有信息的数量,数据的存储方式等问题对用户来说都是透明的,对云存储数据进行加密的访问控制成为数据保护的一个重要解决方法。

基于属性的加密(attribute-based encryption, ABE)访问控制将数据的加密和访问控制融合在一起,在不可信的环境下,数据的明文不能泄露给存储服务器,所以为了实现密文的访问控制,数据的加密和限制用户的解密是必要的。基于 ABE 的访问控制,利用传统的基于身份的加密(identity-based encryption, IBE)访问控制<sup>[5]</sup>中身份的概念,将用户的身份定义为一组属性,而加密的数据与访问控制结构相关,用户只有在身份属性满足访问控制结构的前提下才能解密密文。将基于 ABE 的访问控制方法引入云计算中,既满足了细粒度的访问控制需求,又适应了大规模云用户的



动态扩展。数据属主需要提供数据密钥给大量的用户,而巨大的工作负载将会使数据属主在访问控制中遇到瓶颈。为解决这个问题,Bethencourt 等<sup>[6]</sup>基于访问控制方法(attributes based access control for cloud storage, AB-ACCS)提出了 CP-ABE(ciphertext-policy attribute-based encryption),用户直接和属性组相关,数据与属性条件相关,如果数据符合属性条件则用户可以解密数据。数据属主通过控制数据的密文属性来管理访问权限。这种方法在一定程度上减少了访问权限管理的成本。针对云存储的特征和数据共享的安全问题,Zhang 等<sup>[7]</sup>提出了一个基于属性的分布式云访问控制模型,利用 KP-ABE(key-policy attribute-based encryption)<sup>[8]</sup>和 CP-ABE 的特点,构建出了访问控制策略树。模型采用了统一授权方的授权架构,使用公钥基础设施(public key infrastructure, PKI)核实用户身份,提供角色的公钥认证和密钥认证,并分析和证明了该模型可以满足用户不同访问控制策略的需求,同时可以抵抗共谋攻击,保证了数据在转发过程中的机密性。

为了在不可信的服务器之上保护用户敏感数据的机密性,现有方法主要是通过向授权用户公开数据解密密钥。然而,在对密钥的分发和数据管理方面,这些方案给数据属主带来了巨大的计算工作量,尤其是在细粒度的数据访问控制中。Yu 等<sup>[9]</sup>在 KP-ABE、PRE(proxy re-encryption)和 LRE(lazy re-encryption)<sup>[10,11]</sup>等理论基础之上定义和强化了访问控制策略,使用 KP-ABE 在数据属主和数据用户之间管理信息交换的密钥。结合 PRE,在不暴露底层文件内容的情况下,托管大量的密钥计算任务给云服务器。为了减轻云服务器的计算压力,采用 LRE 技术,允许云服务器累积多个系统操作的计算任务来进行批处理计算,在实现细粒度的访问控制基础上,保证了可扩展性、数据安全和用户隐私。

依赖于加密机制的访问控制策略,在很大程度上保证了存储在云端的数据机密性,适应于动态复杂的云网络环境下的趋势,为云端服务器推送给用户服务资源提供了保障。面对海量的云存储数据,加密也成为一個繁重的任务,势必增加计算开销,因此,如何在保证数据安全访问控制的条件下,提高工作效率和系统性能、降低资源能耗是今后研究工作的重点。

## 2. 数据冗余灾备

云计算系统的构成组件非常庞大,底层的基础设施有可能存在着大量的廉价设备,因此在系统运行过程中发生故障实属正常现象。为了保障用户对数据的正常存取,发生故障时不影响用户的使用,为用户提供可靠的数据服务,对数据进行冗余备份在保证数据可用性方面发挥着至关重要的作用。简单来说,数据的冗余备份就是把数据文件复制一份或者多份,并分别放在各个网络节点上进行存储,当一个节点发生故障时,另一个或几个节点立刻接替,并快速进行数据文件的修复。图 1-3 为冗余灾备数据控制过程。