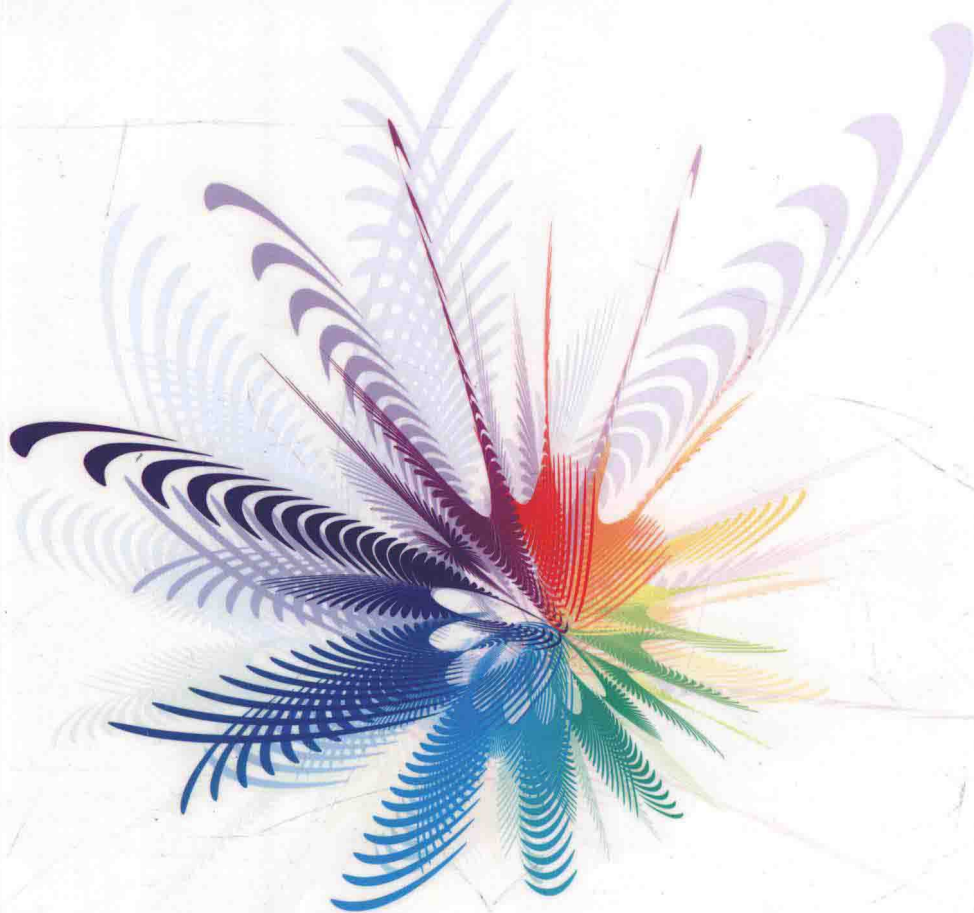




内容广度和深度兼顾，覆盖云安全技术的核心知识点

徐保民 李春艳 编著

云安全深度剖析

技术原理及应用实践

- 深入剖析云安全的关键技术与实现机制
- 秉承实战类图书特色，给出若干实例或思路
- 具有较强的可操作性，便于读者学习和巩固



机械工业出版社
CHINA MACHINE PRESS

云安全深度剖析： 技术原理及应用实践

徐保民 李春艳 编著



机械工业出版社

本书在比较系统地介绍云计算的基础知识、云安全的基本概念及其内涵的基础上,重点讲述了数据的机密性、完整性和可用性,数据的隐私性保护以及云服务的可用性等方面的知识。同时,本书还对云服务风险评估、云安全标准和云测试技术等进行了阐述。

本书内容翔实,通俗易懂,便于讲解和学习,可作为高等院校信息安全、计算机科学与技术等专业的教学用书,也可作为云安全管理工作及工程技术人员的学习和参考用书。

图书在版编目(CIP)数据

云安全深度剖析:技术原理及应用实践/徐保民,李春艳编著. —北京:机械工业出版社,2016.1

ISBN 978-7-111-53353-5

I. ①云… II. ①徐… ②李… III. ①计算机网络—安全技术
IV. ①TP393.08

中国版本图书馆CIP数据核字(2016)第062744号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)

责任编辑:汤枫 责任校对:张艳霞

责任印制:常天培

北京机工印刷厂印刷(三河市南杨庄国丰装订厂装订)

2016年5月第1版·第1次印刷

184mm×260mm·16.5印张·407千字

0 001—3 000册

标准书号:ISBN 978-7-111-53353-5

定价:49.00元

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

电话服务

网络服务

服务咨询热线:(010) 88361066 机工官网: www.cmpbook.com

读者购书热线:(010) 68326294 机工官博: weibo.com/cmp1952

(010) 88379203 教育服务网: www.cmpedu.com

封面无防伪标均为盗版

金书网: www.golden-book.com

前 言

自 2006 年 Google 公司提出云计算概念以来,云计算发展迅速。云计算已经被视为继 Web 2.0 之后,下一波科技产业的重要商机。特别是近年来,随着信息技术的突破和数据科学的崛起,云计算引起了产业界、学术界和政府部门的高度关注。

目前,云计算已经在大多数企业得到普及和应用。其中,伴随着云计算的快速发展,越来越多的用户将数据托管到云端。但是,由于引入虚拟化技术的云计算系统所特有的服务模式以及其前所未有的开放性、复杂性和可伸缩性等特征,传统的安全技术无法完全保证用户托管到云端数据的安全和云计算平台自身的安全。因此,云计算为信息安全领域带来了新的挑战,也为信息系统引入了新的风险。

如今,云安全问题已成为云计算发展的主要障碍之一。许多涉及云计算的安全问题有待解决,如怎样使云服务提供方和使用方之间相互信任、怎样保证云服务没有风险或低风险等。针对云计算面临的这些安全挑战,国内外研究者对一些关键技术进行了相关的研究。但从整体上来讲,关于云计算安全问题的研究刚刚起步,虽然很多组织和机构都在积极地对云计算的安全问题展开研究,但主要是 CSA、NIST 和 Google 等组织与机构所给出的对云计算安全问题的描述和关于云计算安全问题的初步解决方案。

本书全面、系统地对云安全的基本概念、云基础设施安全技术、云安全测试、云服务风险评估方法、数据安全及隐私保护技术等内容进行了深入剖析,对业界云安全实践和云安全标准进行了系统介绍,并给出若干实际例子或思路,具备很强的实践性。全书共包括 10 章,主要内容如下:

第 1 章简要阐述了云计算的产生背景、服务模型、部署模型与面临的问题,并重点探讨了云计算的虚拟化技术、编程模式、数据存储管理和资源调度等若干关键技术。

第 2 章对云计算带来的安全问题进行剖析,并给出了云计算安全的内涵和确保云安全的主流技术,让读者对云安全及其保护技术有一个初步的整体认识。

第 3 章从全局角度分析云基础设施存在的安全问题,并结合云基础设施的安全需求讨论云基础设施安全性的主要关键技术,重点讨论了虚拟化技术及其安全问题和对策。

第 4 章概要论述了云环境下数据在全生命周期中所面临的威胁、相应的安全需求以及针对这些需求可以采取的应对措施。

第 5 章分别从技术、管理和法规角度出发,对数据隐私泄露与保护数据隐私的技术手段及相关法规和管理措施进行全方位的分析。

第 6 章主要对风险概念、风险类别、风险评测方法以及云服务风险评估等方面的内容给出较详细的阐述,为读者分析云服务中可能存在的安全风险和评估云服务的安全性提供参考。

第 7 章介绍安全云应用实践,阐述若干典型云服务提供商在安全云应用中所采用的各种技术解决方案。

第 8 章主要介绍云测试的基本概念和研究现状,同时对云测试目前所面临的挑战、常用的云测试工具以及云测试的解决方案给出论述。

第 9 章围绕云计算安全标准的研究展开,介绍当前主要的云安全标准组织情况,并就它们各自在云计算安全领域的标准研究成果进行概述。

第 10 章对云安全研究的主要方向及云安全研究主流技术的现状和发展趋势进行阐述,使读者能够对当前的研究热点和技术发展动态有一个总体了解。

本书部分内容来自作者所在研究小组的研究成果,此处也参考了大量的业界研究成果和相关技术资料。本书由徐保民制订编写大纲,并负责统稿和定稿的工作。徐保民编写了第 1~7 章,李春艳编写了第 8~10 章和附录。本书的撰写得到机械工业出版社的大力支持,在此一并表示深深的谢意。

由于作者水平有限,书中难免存在不足之处,欢迎各位读者批评和指正。作者的电子邮箱为 xubaomin@gmail.com。

作 者

目 录

前言

第1章 云计算基础	1
1.1 计算模式的演变	1
1.1.1 集中式计算模式	1
1.1.2 桌面计算模式	1
1.1.3 分布式计算模式	2
1.2 理解云计算	3
1.2.1 云计算的起源	3
1.2.2 云计算的定义	4
1.2.3 云计算的类别	5
1.2.4 云计算的特点	6
1.2.5 云计算的优势	7
1.2.6 云计算的挑战与机会	7
1.2.7 云计算与网格计算的差别	8
1.2.8 云计算的发展历程	8
1.2.9 云计算国内外发展现状	10
1.3 云计算服务模型	12
1.3.1 SPI 服务模型	12
1.3.2 IaaS 模型	13
1.3.3 PaaS 模型	13
1.3.4 SaaS 模型	16
1.4 云计算部署模型	19
1.4.1 公有云	19
1.4.2 私有云	20
1.4.3 社区云	20
1.4.4 混合云	20
1.4.5 云计算部署形态	21
1.5 云计算架构	21
1.5.1 云计算参考架构	21
1.5.2 云计算实体	22
1.5.3 云计算基础框架	22
1.6 云计算应用实例	23
1.7 云计算相关技术	24
1.7.1 虚拟化	24

1.7.2 分布式编程	25
1.7.3 数据储存	26
1.7.4 资源调度	26
1.7.5 数据中心	27
1.7.6 应用编程接口	30
1.7.7 云计算安全	30
参考文献	31
第2章 云安全概述	35
2.1 概述	35
2.1.1 云带来的挑战与安全问题	35
2.1.2 引起云安全问题的缘由	36
2.1.3 云安全的内涵	38
2.1.4 云安全问题的分类	38
2.1.5 云安全的需求	41
2.1.6 云安全体系架构	43
2.1.7 云安全与传统信息安全的区别	44
2.1.8 云安全的研究现状	45
2.2 云计算面临的安全问题	48
2.2.1 数据安全问题	48
2.2.2 存储安全问题	48
2.2.3 虚拟化安全问题	48
2.2.4 隐私保护问题	49
2.2.5 云平台安全问题	49
2.2.6 云应用安全问题	49
2.3 云安全问题的深层原因	49
2.3.1 技术上的风险	50
2.3.2 策略和组织管理中的风险	51
2.3.3 法律上的风险	52
2.4 云安全关键技术	53
2.4.1 虚拟化安全	53
2.4.2 数据安全	53
2.4.3 身份认证和访问管理	53
2.4.4 加密与解密	54
2.4.5 容灾与恢复	56
2.4.6 访问控制	56
2.4.7 用户隔离	57
2.4.8 网络安全	57
2.4.9 安全审计	58
参考文献	58
第3章 云基础设施安全	60

3.1 概述	60
3.1.1 云基础设施的架构	60
3.1.2 云基础设施的安全问题	63
3.2 网络级安全	66
3.2.1 数据的保密性	66
3.2.2 认证授权和访问控制	66
3.2.3 网络的安全性和隔离性	66
3.3 虚拟化技术及其安全	67
3.3.1 虚拟化技术概述	67
3.3.2 服务器虚拟化关键技术	71
3.3.3 Xen 虚拟化	73
3.3.4 虚拟化与云计算	79
3.3.5 虚拟化的安全问题	83
3.4 云服务级安全	86
3.4.1 IaaS 云安全	87
3.4.2 PaaS 云安全	89
3.4.3 SaaS 云安全	90
3.5 应用级安全	92
3.5.1 云应用的安全	92
3.5.2 最终用户的安全	93
参考文献	93
第4章 数据安全与云存储	95
4.1 概述	95
4.1.1 数据外包的安全风险	95
4.1.2 数据外包的生命周期	96
4.2 数据安全需求	97
4.2.1 机密性	97
4.2.2 完整性	99
4.2.3 可用性	99
4.2.4 远程访问	99
4.2.5 不可依赖性	100
4.2.6 新鲜度	100
4.3 数据安全	100
4.3.1 数据安全的内涵	100
4.3.2 数据加密	100
4.3.3 数据隔离	102
4.3.4 数据访问	103
4.3.5 数据残留	103
4.4 数据威胁模型	104
4.4.1 数据安全的威胁因素	104

4.4.2 数据安全生命周期的威胁模型	107
4.5 云存储的数据安全	109
4.5.1 云存储	109
4.5.2 云存储安全	112
4.5.3 云存储 DropBox 的安全措施	115
4.5.4 安全云存储缓存系统设计	116
参考文献	118
第5章 隐私性与安全性保护	120
5.1 概述	120
5.1.1 隐私的定义	120
5.1.2 隐私的度量	122
5.1.3 隐私保护技术分类与度量	122
5.1.4 云端数据隐私问题	123
5.1.5 云端数据隐私保护现状	125
5.2 云端服务契约与隐私保护原则	126
5.2.1 云端服务契约的隐私权政策	126
5.2.2 云数据隐私保护原则	126
5.3 法律法规	128
5.3.1 国际法律法规	129
5.3.2 美国法律法规	130
5.3.3 中国法律法规	131
5.3.4 法律法规与技术	132
5.4 隐私保护技术	132
5.4.1 面向数据加密的隐私保护	132
5.4.2 面向数据失真的隐私保护	132
5.4.3 面向限制发布的隐私保护	133
5.4.4 基于同态加密的隐私保护	134
5.4.5 隐私保护技术比较	134
参考文献	134
第6章 云服务风险评估	136
6.1 概述	136
6.1.1 风险简介	136
6.1.2 信息安全风险	140
6.1.3 安全风险评估流程	144
6.2 云服务风险与措施	146
6.2.1 云服务风险概述	146
6.2.2 SaaS 风险	149
6.2.3 IaaS 风险	152
6.2.4 PaaS 风险	152
6.3 面向云服务的测试方法	153

6.3.1 性能评测	153
6.3.2 安全性评测	154
6.3.3 可用性评测	156
6.3.4 可维护性评测	157
6.3.5 可靠性评测	158
6.4 云服务风险评测示例	158
6.4.1 研究方法	158
6.4.2 风险辨识	159
6.4.3 相关性计算	161
6.4.4 评估方法	162
6.4.5 风险评估	165
6.5 SaaS 云服务评估	166
6.5.1 SaaS 风险评测现状	166
6.5.2 SaaS 风险评估指标	166
参考文献	168
第7章 云安全实践	171
7.1 OpenStack 的安全措施	171
7.1.1 OpenStack 概述	171
7.1.2 OpenStack 平台	171
7.1.3 OpenStack 的优势与劣势	174
7.1.4 OpenStack 平台的安全问题及措施	175
7.2 Azure 的安全措施	176
7.2.1 Azure 概述	176
7.2.2 身份认证与访问管理	178
7.2.3 数据安全与加密服务	178
7.3 Google Docs 的安全措施	179
7.3.1 Google 云平台概述	179
7.3.2 Google Docs	180
7.3.3 Google 文档的安全问题及措施	180
7.4 Amazon 的安全措施	181
7.4.1 概述	181
7.4.2 安全策略	184
7.5 阿里云的安全措施	186
7.5.1 概述	186
7.5.2 安全策略	186
7.6 Hadoop 的安全措施	188
7.6.1 Hadoop 概述	188
7.6.2 Hadoop 内置安全机制	190
7.6.3 第三方解决方案	191
7.7 中国电信安全云应用实践	191

7.7.1	云应用安全防护体系	191
7.7.2	云安全框架	192
7.8	基于 Hadoop 的访问控制实验	193
7.8.1	访问控制概述	193
7.8.2	Kerberos 简介	193
7.8.3	实现环境搭建	195
7.8.4	实验流程	196
	参考文献	197
第 8 章	云测试	198
8.1	概述	198
8.1.1	软件测试的关键问题	198
8.1.2	典型的软件测试方法	199
8.2	云测试	201
8.2.1	云测试的概念和类别	201
8.2.2	云测试的特点	203
8.2.3	云测试面临的挑战	203
8.2.4	云测试的研究进展	204
8.2.5	传统软件与云服务测试的异同	205
8.3	常用的云测试方法	206
8.3.1	性能测试	206
8.3.2	渗透测试	207
8.3.3	功能测试	208
8.3.4	会话劫持测试	209
8.3.5	业务逻辑测试	210
8.4	云服务质量测试	210
8.4.1	服务质量参数的选取与度量	210
8.4.2	SaaS 云服务质量测试	211
8.4.3	多租户服务质量测试	211
8.4.4	可靠性与容错性测试	212
8.5	OpenStack 平台安全测试实践	213
8.5.1	搭建环境	213
8.5.2	测试内容	216
8.5.3	选择测试方法	216
8.5.4	部署测试环境	217
8.5.5	实施测试	219
	参考文献	223
第 9 章	云计算标准	225
9.1	概述	225
9.1.1	云标准化组织	225
9.1.2	云标准化内容	226

9.2 NIST 的相关标准	227
9.2.1 《云计算参考体系架构》标准	227
9.2.2 《公有云计算中安全与隐私》草案	227
9.3 CSA 的相关标准	228
9.3.1 《云计算关键领域安全指南》白皮书	228
9.3.2 《云控制矩阵》白皮书	229
9.3.3 《身份管理与接入控制指导建议书》白皮书	229
9.3.4 《云计算安全障碍与缓和措施》白皮书	230
9.3.5 《云审计》白皮书	230
9.4 ENSIA 的相关标准	230
9.5 Gartner 的相关标准	230
9.6 ITU-T 的相关标准	231
9.7 OASIS 的相关标准	232
9.8 DMTF 的相关标准	232
9.9 OGF 的相关标准	233
9.10 OCC 的相关标准	233
9.11 CCIF 的相关标准	233
9.12 SNIA 的相关标准	233
9.13 国内云标准化进展	233
参考文献	234
第 10 章 云安全发展趋势	235
10.1 概述	235
10.2 密码技术	235
10.2.1 全同态加密	236
10.2.2 密文检索	237
10.2.3 密钥管理	238
10.3 云安全与大数据	238
10.4 可信云计算	239
10.5 云安全标准及其测评体系	240
10.6 云安全体系与技术框架	240
10.7 云安全形式化验证	240
10.8 数据完整性验证	241
10.9 数据多副本技术	241
参考文献	242
附录 常用术语中英文对照	244

第1章 云计算基础

近年来,一种新的分布式计算模式——云计算在学术界和工业界已经成为热点。被视为IT界第三次革命的云计算将带来工作方式和商业模式的根本性改变。然而,云计算到底是什么?它的产生背景是什么?它涉及哪些关键技术?它的发展前景如何?本章将通过对这些问题的阐述,帮助读者对云计算形成一个初步的认识。

1.1 计算模式的演变

利用有限的资源实现效益的最大化始终是计算机科学技术发展和追求的目标之一。例如从基于集群的计算模式发展到网格计算模式,就是一种有效利用有限资源的进步。当前如火如荼的云计算模式,则可以说是一种计算模式的升华。

要了解云计算是什么和不是什么,理解计算模式的演变过程非常重要。所谓计算模式就是指计算机完成任务的一种运行、输入/输出以及使用的方式。在计算技术的发展历史中,随着微处理器技术和计算机网络技术的不断发展,计算模式经过了集中式计算模式、桌面计算模式和分布式计算模式的变迁^[1]。

1.1.1 集中式计算模式

自1946年2月14日世界第一台名字叫“ENIAC(埃尼阿克)”的电子计算机在美国宾夕法尼亚大学诞生^[2],到20世纪70年代初,计算机设备不仅庞大和昂贵,而且异常复杂,没有经过特殊培训的人员几乎无法直接使用计算机。因此,当时只有为数不多的机构才有财力购置数量有限的计算机。这些计算机通常都是单独放在特别的房间里,并由专业人员来操作和维护。

为了节约成本,当时的计算机系统大多以一台主机为核心,用户通过终端设备与主机相连。在主机操作系统的管理下共享主机的硬件资源,包括中央处理器、内存/外存、输入/输出设备等。所有的数据存储和计算都在主机上进行,终端设备只负责接收用户的请求和显示计算结果。这就是集中式计算模式。

集中式计算模式的主要特点是可以同时为多个用户服务,主要缺点如下:

- 1) 主机负担过重,所有的计算和存储都集中在主机上。一旦主机出故障,整个系统都将瘫痪。
- 2) 系统扩展不易,当用户数量不断增加时,必须更换主机,否则系统的服务质量就要受到影响。
- 3) 系统的购置、安装及维护等费用较高,不易普及。

1.1.2 桌面计算模式

随着大规模集成电路技术的发展,计算机的小型化成为可能。20世纪70年代,少数科研

机构已开始配置供个人使用的微型计算机。但是,个人计算时代真正开始的标志是 IBM 公司在 1981 年正式推出的全球首台个人计算机 IBM PC^[3]。为了推动个人计算机的产业化发展,IBM 公司在 1982 年公开了 IBM PC 的主要技术。自此,个人计算机得以迅速发展,并由此走入寻常百姓之家。

由于许多 PC 和 workstation 已经具备了过去大型计算机的能力,可以存储大量的数据且能进行相对复杂的计算,而价格却非常便宜,因此计算模式的主流从以一台主机为核心转移到以用户桌面为核心的桌面计算模式,也称为单机计算模式或个人计算模式。

1.1.3 分布式计算模式

到 20 世纪 90 年代,随着个人计算机的蓬勃发展和局域网技术的成熟,用户通过计算机网络共享计算机资源成为可能。计算机网络的发展促使桌面计算模式迅速向分布式计算方向转移。当时,这种新出现的模式被称为 C/S 模式^[4]。其中,客户机 (Client) 是一种单用户工作站,提供与业务应用有关的表现、计算、网络连接和各类接口服务;服务器 (Server) 是一种共享型的多用户处理机,提供业务所需的计算、网络连接、数据库管理和各类接口服务。C/S 计算模式会把应用程序所要完成的任务分派到客户机和服务器上,并通过它们之间的协调共同完成。

随着 Internet 技术的发展和迅速普及,计算机之间的通信和互联超越了地域的限制,改变了人们传统的获取、交换和处理信息的方式。而万维网和浏览器的出现使得互联网从科研机构走向了大众^[5]。自 20 世纪 90 年代中期开始,一种全新的计算模式 (即 B/S 模式) 逐渐形成并发展起来^[6]。在这种模式下,用户工作界面是通过浏览器来实现的,极少部分事务逻辑在前端 (Browser) 实现,主要事务逻辑都在服务器端实现。B/S 模式简化了客户端的要求,主要计算工作都在服务器端完成,计算又一次开始向服务器端集中。

伴随着高速网络的不断涌现和计算资源的网络化,拥有个人计算机或 workstations 的广大用户,迫切需要共享分布于网络上丰富的资源,特别是计算资源。这就使得基于网络的分布式计算模式逐步成为主流的计算模式。简单地说,分布式计算就是让很多计算机同时去帮你做事情、进行计算。

由于分布式计算有着巨大的计算潜力、良好的可扩展性和灵活的体系结构,所以它对于解决大型和小型的科学计算问题都是一种非常合适的模式^[7]。从学术角度讲,分布式计算是一种把需要进行大量计算的工程数据分割成小块,由多台计算机分别计算,在上传计算结果后,将结果合并然后得出数据结论的科学。

分布式计算的最早形态出现在 20 世纪 80 年代末期的 Intel 公司。Intel 公司利用 workstations 的空闲时间为芯片设计计算数据集。随着 Internet 的迅速发展和普及,分布式计算的研究在 20 世纪 90 年代后期达到了高潮。目前分布式计算已非常流行。

分布式计算模式的演变历史开始于并行计算,主要经历了集群、网格计算和云计算三大阶段。如图 1-1 所示。从计算模式的发展趋势来看,网格计算和云计算都是随着计算规模和计算能力的日益提高,以及应用范围的扩大和用户数量的剧增而产生的,是技术和应用发展的必然趋势。云计算作为目前出现的一种最新的分布式计算模式,是由传统的多种计算模型和技术发展而来的,已成为众多企业的一种必然选择和趋势。

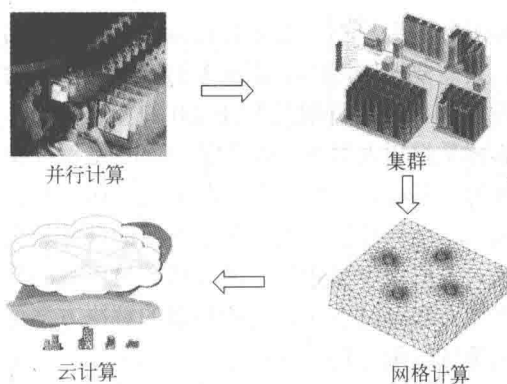


图 1-1 分布式计算模式的发展趋势

并行计算一般是指许多指令得以同时执行的计算模式。在同时执行的前提下，可以将计算过程分解成若干子过程，之后以并行方式来加以完成。并行计算可分为时间上的并行和空间上的并行。时间上的并行是指流水线技术，空间上的并行是指用多个处理器并行地执行计算。任何高性能计算都离不开并行计算技术。

集群是一种并行或分布式多处理系统，该系统是通过将一组松散集成的计算机软件和硬件连接起来作为一个整体向用户提供一组资源。在某种意义上，一个连接在一起的计算机集群对于用户和应用程序而言就像是一个单一的计算机系统。集群系统中的单个计算机通常称为节点，节点可以是连接在一起的，也可以是物理上分散而通过局域网连接到一起的。集群系统通常用来改进单个计算机的计算速度和可靠性。在一般情况下，集群系统比单个计算机（如工作站）的性能价格比要高得多。

20 世纪 90 年代初，网格计算由学术界提出，伴随互联网的兴起而迅速发展。该模式利用 Internet 把分散在不同地域的计算机组织成一台虚拟的超级计算机，每一台参与运算的计算机即为一个节点，整个计算则是由成千上万的节点构筑成一个网格，因而被称为网格计算。网格计算的焦点在于支持跨管理域计算的能力，这使它与传统的集群系统或传统的分布式计算相区别。

云计算是一种通过互联网提供弹性计算和虚拟资源服务的分布式计算模式。它是网格计算、分布式计算、并行计算、效用计算、网络存储和虚拟化等传统计算机技术和网络技术发展融合所产生一种新的商业计算模式。

1.2 理解云计算

近年来，云计算作为一个新的技术趋势已经得到了快速发展。然而，由于业界一直没有对云计算形成一个统一的定义，稀奇古怪的所谓“云计算”产品不断涌现。

1.2.1 云计算的起源

早在 20 世纪 60 年代，美国科学家 John McCarthy 就提出将计算能力作为一种公共设施提供给公众，使人们能够像使用水电那样使用计算资源。

针对此设想，通过将所有的计算资源集中起来，采用类似“效用计算”和“软件即服务”的分布式计算技术为人们提供“按需随用”的计算资源。在此背景下，用户的使用观念会发生彻底的改变，即从“购买产品”到“购买服务”的转变，因为他们直接面对的不再是复杂

的硬件和软件，而是最终的服务。用户不需要拥有看得见、摸得着的硬件设施，也不需要为机房配置专门的维护人员等，只需要把钱汇给所需服务的供应商，就会得到所需的服务。

伴随着互联网技术的发展和普及，特别是 Web 2.0 的飞速发展，各种媒体数据呈现指数增长，逐步递增的海量异构媒体数据以及数据和服务的 Web 化趋势使得传统的计算模式在进行大数据处理时，其表现有些力不从心，新的问题不断涌现。比如传统计算模型至少在如下两个方面已经不能适应新的需求：一是计算速度上受限于内核的性能和个数；二是待处理数据量受限于内存和硬盘容量。对此，人们很容易想到，能否将数量可观的计算机连接起来以获得更快的计算速度、更强大的处理能力和存储能力。这种朴素的解决方案可以追踪到分布式计算模式出现之时，只是当时的应用领域局限于科学计算。

针对上述构思的最新解决方案，是在谷歌、亚马逊等著名 IT 企业的大力推动下，为实现资源和计算能力的共享以及应对互联网上各种媒体数据高速增长的势头，所提出的一种以数据为中心的新商业计算模式——云计算^[8]。

术语“云”第一次出现是在 20 世纪 90 年代早期，主要是指大型的 ATM 网络，是对因特网的一种隐喻。而首次在学术上使用“云计算”一词的是 1997 年的 Ramnath Chellappa 教授所描述的“云计算是一个动态的计算框架，计算的边界由技术、经济、地区、信息安全需求以及基础服务供应商决定”。

然而，当下流行的“云计算”中“云”的真正发端是在 21 世纪初，是伴随着云计算鼻祖之一的 Amazon 公司于 2005 年所提出的允许小企业和私人租用其所提供的一组包括存储空间、计算能力等资源服务的称为亚马逊 EC2 的出现而出现的。

已经成为当今最流行词汇的“云计算”是由 Google 的前首席执行官 Eric Schmidt 于 2006 年 8 月 9 日在圣何塞（San Jose）举办的全球搜索引擎会议（Search Engine Strategies, SES）上首次提出的。其真正作为一个新兴的技术热门名词被 IT 业开始认可并进入产品化流程始于 2007 年左右。此后，IT 行业各大厂商和运营商纷纷制订相应的战略，新的概念、观点、产品和服务不断涌现。例如 IBM、Google、Amazon、Microsoft 和 Yahoo 等 IT 行业巨头都顺势推出各自的云计算产品和技术。同时，云计算也引起了政界和学术界的普遍关注。目前，世界各国都把云计算作为未来战略产业的重点。比如 2011 年 2 月，美国政府颁布了“联邦云计算战略”，规定“云计算优先（Cloud First）”；日本政府提出“Kasumigaseki Cloud（霞关云计算）”战略；我国“十二五”规划纲要也把云计算列为重点发展的战略性新兴产业。

总之，云计算的出现为信息技术领域带来了新的挑战，也为信息技术产业带来了新的机遇。

1.2.2 云计算的定义

云计算是一种概念性的说法，而非专指某特定的信息系统。对云计算最简单的理解，就是将计算能力提供出来作为一种服务，使企业或个人可以通过因特网取得服务。用户所需要的数据，不用存储在个人计算机上，而是放在网络的“云”上面，在任何可以使用网络的地方都可以使用。云代表了规模庞大的计算能力，由云服务供应商建造大型机房，提供各种软件和应用，让用户随时使用超级计算机的计算能力和最新应用软件，用户却不知道服务器的位置或数据的所在，就像是天上的“云”一般，虚无缥缈又抬头即见。

有人主张将 Cloud Computing 翻译为“云计算”，但也有人将它解读为“云端计算”。“云”即是我们最常使用的因特网；“端”是指使用者端或泛指用户应用网络服务来完成事情的方式。云计算的目标就是没有软件的安装，所有资源都来自云端，使用者端只需要具备连上云

端的设备和简单的接口如浏览器即可。因此云计算是一种基于因特网的计算模式，通过因特网上异构、自治的服务为个人和企业使用者提供“按需随用”的计算资源。

维基百科上给出的云计算定义：“一种基于因特网的计算新方式，通过因特网上异构、自治的服务为个人和企业使用者提供按需即取的计算。云计算的资源是动态、易扩充套件而且是虚拟化的，通过因特网提供的资源，终端使用者不需要了解云端中基础设施的细节，不必具有相应的专业知识，也无须直接进行控制，只需关注自己真正需要什么样的资源以及如何通过网络来得到相应的服务”。

但是，当谈及云计算的定义时，大多数研究者都会引用美国国家标准与技术研究院（National Institute of Standard and Technology, NIST）的定义^[9]：“云计算是一种模式，支持根据用户需求通过网络方便地访问可配置的计算资源（如网络、服务器、存储器、应用和服务）的共享池，而该池可通过最少的管理工作或服务供应商干预进行快速配置和交付。”。具体来讲，NIST 提供的云计算定义中包括了五个基本特征、三个云服务模型和四个云部署模型，如图 1-2 所示。



图 1-2 NIST 提供的云计算定义

需要指出的是，由于考虑的角度不同，业界对云计算的提法也稍有不同。IBM、Google 和 Amazon 等公司也都从自身角度出发给出了云计算的定义。尽管各自的表述方式和应用特点不同，但云计算的如下特性是可以被明确认同的：

- 1) 硬件和软件都是资源，可以是物理的，也可以是虚拟的，通过互联网以服务的方式供给用户。
- 2) 资源以分布式共享的形式存在，以单一整体的形式呈现。
- 3) 资源可以根据需要进行动态的扩展和配置。
- 4) 用户按需使用云中的资源，而不需要管理它们。

综上所述，云计算将所有的计算资源集中起来，并由软件实现自动管理，无须人为参与。这使得应用提供者无须为烦琐的细节而烦恼，能够更加专注于自己的业务，有利于创新和降低成本。

1.2.3 云计算的类别

云计算可分为云计算服务和云计算技术。前者的重点是放在提供信息服务给用户，如 Salesforce 公司所提供的在线客户关系管理 CRM 服务及 Amazon 公司所提供的在线动态虚拟主机 EC2 服务等云计算解决方案；后者的重点是放在提供高可靠性的信息基础平台，如 IBM