网络与信息安全前沿技术丛书

云计算安全技术

主编 卿昱 副主编 张剑

Security in Cloud Computing

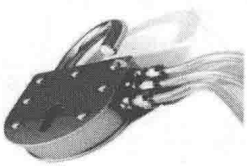
國防工業出版社
National Defense Industry Press

网络与信息安全前沿技术丛书

主　编　卿　昱
副主编　张　剑
编　著　卿　昱　张　剑　王　强　陈剑锋
　　彭凝多　陈　珂　望娅露

云计算安全技术

Security in Cloud Computing



目前，国家正在大力推进云计算的应用，加快政府、企业的新一代信息基础设施建设，云计算安全是云计算落地的关键条件之一。云计算具有弹性、按需自服务、用户多等特点，其安全防护技术较一般系统有许多不同的功能需求和特性要求。本书正是作者长期从事云计算工程实践后，总结提炼出的有关构建云计算安全体系的技术经验和实例。相信本书能够为从事云计算安全研究的科技人员和大专院校师生提供有效的指导和帮助。

国防工业出版社
National Defense Industry Press
·北京·

图书在版编目(CIP)数据

云计算安全技术 / 卿昱主编. —北京：国防工业
(网络与信息安全前沿技术丛书)
ISBN 978-7-118-08484-9

Ⅰ. ①云… Ⅱ. ①卿… 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 327023 号

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号　邮政编码 100048)
北京嘉恒彩色印刷有限责任公司
新华书店经售
*
开本 710×1000　1/16　**印张** 16½　**字数** 332 千字
2016 年 12 月第 1 版第 1 次印刷　**印数** 1—2500 册　**定价** 76.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777　　发行邮购：(010)88540776
发行传真：(010)88540755　　发行业务：(010)88540717

丛书序

网络的触角正伸向全球各个角落，高速发展的信息技术已渗透到各行各业，不仅推动了产业革命、军事革命，还深刻改变着人们的工作、学习和生活方式。然而，在人们享受信息技术带来巨大利益的同时，一次又一次网络信息安全领域发生的重大事件告诫人们，网络与信息安全已直接关系到国家安全和社会稳定，成为我们面临的新的综合性挑战，没有过硬的技术，没有一支高水平的人才队伍，就不可能在未来国际博弈中赢得主动权。

网络与信息安全是一门跨多个领域的综合性学科，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等。“道高一尺、魔高一丈”，网络与信息安全技术在博弈中快速发展，出版一套覆盖面较全、反映网络与信息安全方面新知识、新技术、新发展的丛书有着十分迫切的现实需求。

适逢此时，欣闻由我国网络与信息安全领域著名专家何德全院士任编委会主任，以国家保密通信重点实验室为核心，集聚国内信息安全界知名专家学者，潜心数年编写的“网络与信息安全前沿技术丛书”即将分期出版。丛书有如下特点：一是全面系统。丛书涵盖了密码理论与技术、网络与信息安全基础技术、信息安全防御体系，以及近年来快速发展的大数据、云计算、移动互联网、物联网等方面的安全问题。二是适应面宽。丛书既很好地阐述了相关概念、技术原理等基础性知识，又较全面介绍了相关领域前沿技术的最新发展，特别是凝聚了作者

前言

IT界近两年找不出比“云计算”、“大数据”更火的词汇了，仿佛一夜之间，所有与IT沾边的事物都改名姓“云”。当学术界争论不休，试图给“云计算”一个科学严谨定义的同时，各式各样“云计算”的产品和服务已翩翩落地。微软的Azure云平台、Google的App Engine、IBM的蓝云计算平台、亚马逊的AWS云平台等纷至沓来。在国内，阿里云、腾讯云、百度云等纷纷上马。面对云计算可能带来的巨大机遇，几乎所有的IT巨头均不惜投入巨资，积极部署云计算发展战略，剑指未来云计算巨大的产业利润。

尽管云计算前进的步伐势如破竹，但其安全问题却阻碍了云计算的发展。随着云计算的深入推进，用户对云计算安全的担忧日渐加深。调查表明，云计算安全问题目前是影响全球企业、运营商、政府向云计算过渡的最大障碍。网络巨头思科公司首席执行官John Chambers更是预言，安全将成为云计算前进路上的“噩梦”。试想一下，成千上万的用户隐私、企业商业秘密、政府敏感信息等都存储在云端之上，其势必成为全球黑客、敌对势力炙手可热的攻击目标。用户将不得不担心：

（1）云端服务器采用什么安全措施保护自己的数据？

（2）拥有特权的云端内部管理员会不会偷窥自己的数据？

（3）属于自己的数据是否脱离了限定的安全区域被其他用户非法访问？

（4）自己存储在云端的数据被分散在何处存储？那些存储的数据是否违反当地相关法律规定？

（5）云端可否保障在任何时候、任何灾难发生时不丢失自己的数据？在灾难发生后，多长时间能恢复自己的数据？

（6）如果自己的数据不幸被泄漏，云服务商怎样提供赔偿和弥补损失？

一系列传统信息系统的安全问题还没有彻底解决，云计算又给信息安全带来了更新、更严峻的安全挑战。这促使我们产生了编写《云技术安全

试读结束：需要全本请在线购买： www.ertongbook.com

技术》一书的想法。

过去的几年里，我们一直在密切关注和跟踪云计算安全技术的进展，研究如何确保企业用户在原有投资上能够获得更高安全保护的云服务，研究如何确保政府用户能够放心地将政务数据迁移到云数据中心，研究如何更有力地支撑传统应用向面向云服务架构的转型，以确保更灵活、更强大的业务能力。这些研究为本书内容的形成奠定了基础。

本书共分 11 章，各章节的具体安排如下：

第 1 章介绍云计算的基本知识，主要包括云计算定义、云服务交付模型（基础设施即服务 IaaS、平台即服务 PaaS 和软件即服务 SaaS）、云部署模型（公有云、私有云、社区云和混合云）、云计算关键技术以及典型的云计算应用案例。

第 2 章在介绍典型的云安全事件的基础上，对云计算的安全威胁进行分析，并结合云安全联盟 CSA 的《云计算安全威胁》，归纳总结云计算主要面临的安全威胁和亟待解决的安全问题，最后简单介绍云计算的安全性评估方法，对安全威胁的脆弱性暴露程度进行量化。

第 3 章介绍云计算安全体系，重点介绍广被业界接受的云安全联盟 CSA 提出的云计算安全体系，包括云计算安全技术以及实施管理、运行云计算方面的要求，其中，云安全技术研究涉及 13 个安全领域，这些安全领域从宏观上分为云的架构、云中的治理和云的运行三类。

第 4 章围绕云计算基础设施安全展开讨论，云计算引入了虚拟化技术，而虚拟化也会带来多种安全隐患，计算、存储和网络的虚拟化都具有各自需要解决的安全问题。云基础设施的安全防护应结合传统安全防护手段，通过对云计算基础设施进行全面安全加固，确保云服务的稳定性和可靠性。

第 5 章描述云应用安全，探讨云应用虚拟化和桌面虚拟化所面临的安全挑战及其相应的安全防护措施，并介绍云终端（硬件终端和软件终端）的安全风险及应对措施。

第 6 章对云数据安全展开分析，介绍确保云计算环境中数据的机密性、完整性和可用性所采取的技术，主要包括数据加密及密文计算、数据校验、数据容灾与备份、隐私保护等技术。

第 7 章围绕云计算环境中密钥管理问题展开讨论，在介绍密钥及密钥管理的基本知识的基础上，针对三种常见云服务类型，分别介绍了各种云服务类型所面临的密钥管理挑战，并提出一些解决思路。

第 8 章描述云计算环境下身份管理与访问控制，从需求、挑战、解决方案和典

型应用方面对云计算环境下的身份供应、身份认证、身份联合、访问控制等问题展开讨论。

第9章围绕安全功能服务化，着重介绍几类典型的云安全服务，包括云认证和授权服务、流量清洗服务、入侵检测服务、云杀毒服务以及安全评估服务，并在此基础上，分析和探讨了云安全服务目前存在的主要问题。

第10章探讨了云计算环境下的安全管理职责，云计算的安全管理需要根据云服务商的类型，从IaaS、PaaS和SaaS三个层面，并结合云服务商和用户两个角度，来考虑对应的安全管理职责，主要包括可用性管理，漏洞、补丁和配置管理，合规性管理，安全监测与响应等方面。

第11章主要介绍云安全标准的相关概念和国内外相关工作进展，包括NIST、ITU－T、ISO、CSA、ENISA、全国信息技术标准化技术委员会、全国信息安全标准化技术委员会、CCSA、公安部等组织机构发布和在研的多项云安全标准。

本书涉及许多新的领域和内容，虽然云计算安全方面的参考资料很有限，编写者的学术水平和研究能力也有限，但我们想尽快与读者一起，找到开启云计算安全之门的那把“钥匙”，书中难免疏漏和不足，诚望不吝赐教、斧正。

全书由中国电子科技网络信息安全有限公司组织编写；国防工业出版社王晓光编审为本书的顺利出版给予了大力支持。参与本书编写的有卿昱、张剑、王强、陈剑锋、彭凝多、陈珂、望娅露、刘汪洋、龙恺、冯成燕、郭小华、王怀胜、李姝、刘晓毅、齐伟钢、贺志生、陈天莹等。在此对大家辛勤的工作表示衷心的感谢！

编者

2016年5月

目　录

试读结束：需要全本请在线购买： www.ertongbook.com

第1章 云计算概述

当前已经进入了“云领未来”的时代，贴着“云”标签的东西满天飞，人“云”亦“云”的现象随处可见。那么，到底什么是“云”？“云”是如何运行的？“云”的架构如何描述？“云”涉及到的关键技术有哪些？“云”的优势在哪里？本章将围绕这些问题介绍云计算。

1.1 云计算定义

关于云计算的定义，迄今为止尚无统一的说法。其原因也非常明显，每个企业都希望在云计算产业链中独占先机抢夺有利地盘，因而自然都会从自身角度来对云计算进行定义和诠释。事实上，这些定义大同小异，下面列举一些比较有代表性的“云计算”定义。

（1）维基百科：云计算是一种将规模可动态扩展的虚拟化资源，以按需使用服务的方式通过互联网对外提供的计算模式，用户无需了解提供这种服务的底层基础设施，也无需去拥有和管理它们。

（2）百度百科：狭义云计算指 IT 基础设施的交付和使用模式，指通过网络以按需、易扩展的方式获得所需资源；广义云计算指服务的交付和使用模式，这种服务可以是 IT 和互联网软件，也可以是其他服务，即计算能力也可以作为一种商品通过互联网进行流通。

（3）IBM：云计算是一个虚拟化的计算机资源池，托管多种不同工作负载，能快速提供虚拟机器、物理机器从而适应资源负载的动态变化。

（4）Google：云计算是以公开标准和服务为基础，以互联网为中心，提供安全、快速、便捷的数据存储和网络计算服务。

（5）微软：云计算是“云 + 端”的混合计算模式。“云”和终端都具备很强的计算能力，因而将所有应用程序都安装在本地终端的模式不合理，从而强调“云”和终端的均衡利用，云是“软件 + 服务”的综合。

（6）Berkeley 大学：云计算是包含互联网上的应用服务以及在数据中心提供这些服务的软硬件设施。

本书采用美国国家标准与技术研究所(National Institute of Standards and Technology,NIST)对云计算的定义,具体内容如下:

云计算是一种资源利用模式,它能以简便途径和按需方式通过网络访问可配置的计算资源(网络、服务器、存储、应用和服务等),资源可以快速供给和释放,从而使得服务提供商能以最小的管理代价或仅进行少量工作就可实现资源发布。[1]

从以上云计算的定义可以看出,云计算将应用和IT资源分开,强化了协作性、敏捷性、扩展性和可用性,以及通过优化和高效计算降低了成本。简言之,云计算是将计算、存储等资源集中在资源池中,以按需服务和按量计费形式配给用户满足其需求的一种新的计算模式。云计算将计算、网络、存储、数据等资源集中在"资源池"中,并以服务的形式提供给用户,这些服务可以快速构建、准备、部署和退出,并且可迅速扩充或缩减其规模[2]。NIST定义了云计算的五个关键特征、三种服务交付模型和四种部署模型,如图1.1所示。

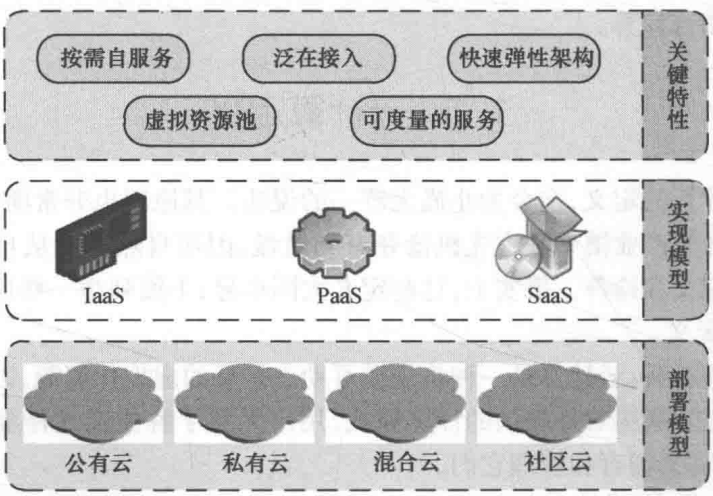


图1.1 NIST定义的云计算模型

尽管云计算内涵还在不断演变,其标准化定义也处于完善和发展之中,云计算的五个关键特征已经可以将其与传统计算模式区分开来,它们也是界定一个计算模式是否为云计算实例的关键。

(1) 按需服务:用户可以在需要时通过管理界面自己配置计算能力,而无需与服务供应商的服务人员直接或间接交互。

(2) 泛在接入:云计算的服务能力通过网络来提供,支持多种标准化网络接入手段,能够通过客户端、浏览器、移动设备等终端广泛访问。

(3) 多租户和资源池:云服务商的IT资源被汇集到资源池中,其资源主要包括计算、存储、网络。云计算根据多租户模型,按用户需求将资源池内的物理和虚拟资源动态地分配或再分配给多个租户使用,资源的放置、管理与分配策略对用户透明。

(4) 快速弹性:云计算服务能力可以快速、弹性地提供,在接到服务请求后自动地实现快速扩容、快速上线并立即投入服务。对于用户来说,可提供的服务能力近乎无限,可以随时按需购买,不用担心计算、存储能力不足导致业务瓶颈。

(5) 可度量性:云计算具备对相关 IT 资源运行状态的实时测量能力,能够自动控制并优化服务的资源使用,并产生统计报表。

云服务商构建的云计算环境一般包括用户交互接口、服务目录、系统管理(负载均衡)组件、监视统计组件、配置工具和计算/存储/网络基础资源等部分[3],如图 1.2 所示。

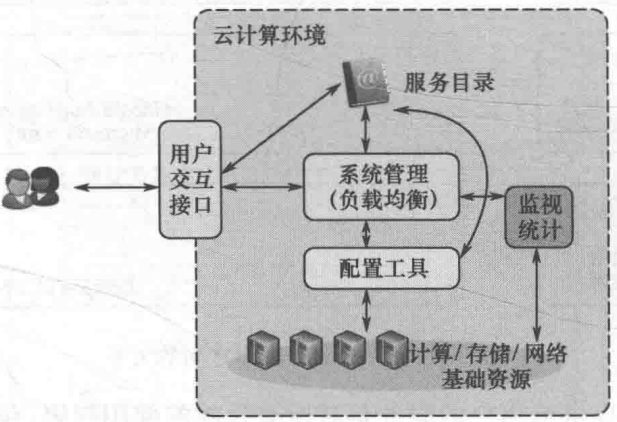


图 1.2 云计算环境的示意图

(1) 用户交互接口:对云计算环境提供的服务进行封装,提供统一、易用的访问和交互方式,如基于浏览器的业务管理界面、基于 SOA/RESTful 的自动调用接口等。

(2) 服务目录:提供云计算服务的列表,用户可以从列表中查询服务名称,查看服务说明和计费方式等,并能以便利的方式使用户重定向至服务订阅界面。

(3) 系统管理:负责云计算系统的管理维护,包括计算、存储、网络、虚拟化组件和安全策略的管理,同时提供负载均衡能力,使负载均匀分布以提高系统效率。

(4) 配置工具:根据云计算环境的运行状态,对运行参数进行动态配置,维持云计算环境的最优化运行。

(5) 监视统计:对云计算环境状态和资源使用情况的监视和统计,用于及时发现运行中产生的各种问题。

(6) 计算/存储/网络基础资源:支撑云计算环境的后台基础设施,包括计算、存储、网络等物理资源以及必要的虚拟化支撑软件等组件。[4]

1.2 云服务交付模型

基于服务交付方式可以将云计算划分为三种服务模型:基础设施即服务

(IaaS)、平台即服务(PaaS)和软件即服务(SaaS),根据每种模型的英文首字母简称为 SPI 模型。虽然业界也提出了一些其他的云计算交付模型,但 SPI 模型最被用户接受,同时也得到了 NIST 和大多数云服务商(CSP)的认可。SPI 云计算服务模型如图 1.3 所示。

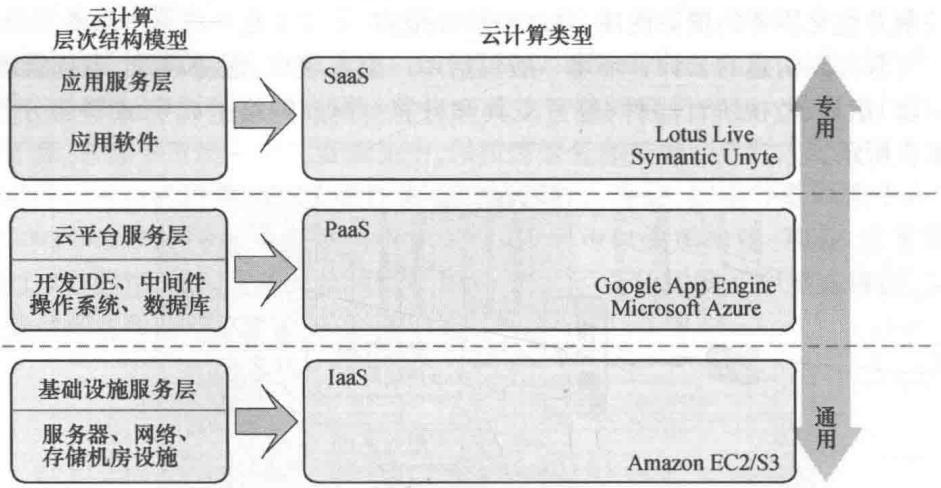


图 1.3 SPI 云服务模型之间的关系

在 IaaS 中,提供给用户的服务是对所有设施的使用权限,包括计算、存储、网络和其他资源。通过云服务商为用户分配的基础设施访问接口,用户可以选择操作系统类型、定制存储空间,并部署应用程序,还能获得网络及安全组件(如防火墙、负载均衡等)的部分管理权限。

在 PaaS 中,用户将得到能够部署可执行代码的运行环境。用户将自己开发的功能代码或购买的应用程序提交至云计算平台,并从资源池中获得相应的计算、存储和网络资源供这些程序使用。在应用程序上线、用户能够正常使用后,云服务商按照运行环境所消耗的资源、时间周期向程序开发者收取费用。使用 PaaS 的开发者可以根据预算和实际需要,选择运行应用程序的托管环境性能等级,对环境变量进行参数配置以优化应用程序的性能,而不需要管理或控制底层基础设施。

在 SaaS 中,网络、服务器、操作系统、存储等资源均由云服务商提供并进行维护,用户不需要管理或控制底层基础设施和软件运行环境,用户只需要通过客户端、浏览器、移动设备等终端就能够访问和使用云服务商所提供的软件服务,例如:Web 服务、应用程序等。

1.2.1 基础设施即服务

NIST 对 IaaS 的定义:将计算、存储、网络等基础 IT 资源以服务方式提供给用户,基于这些资源,用户可以部署和运行包括操作系统在内的各种软件,而无需管理或控制底层云基础设施,此外,用户还可以按需对 CPU、内存、磁盘、网络和安全

试读结束:需要全本请在线购买: www.ertongbook.com