HZ BOOKS
华章教育

教育部-阿里云产学合作协同育人项目成果

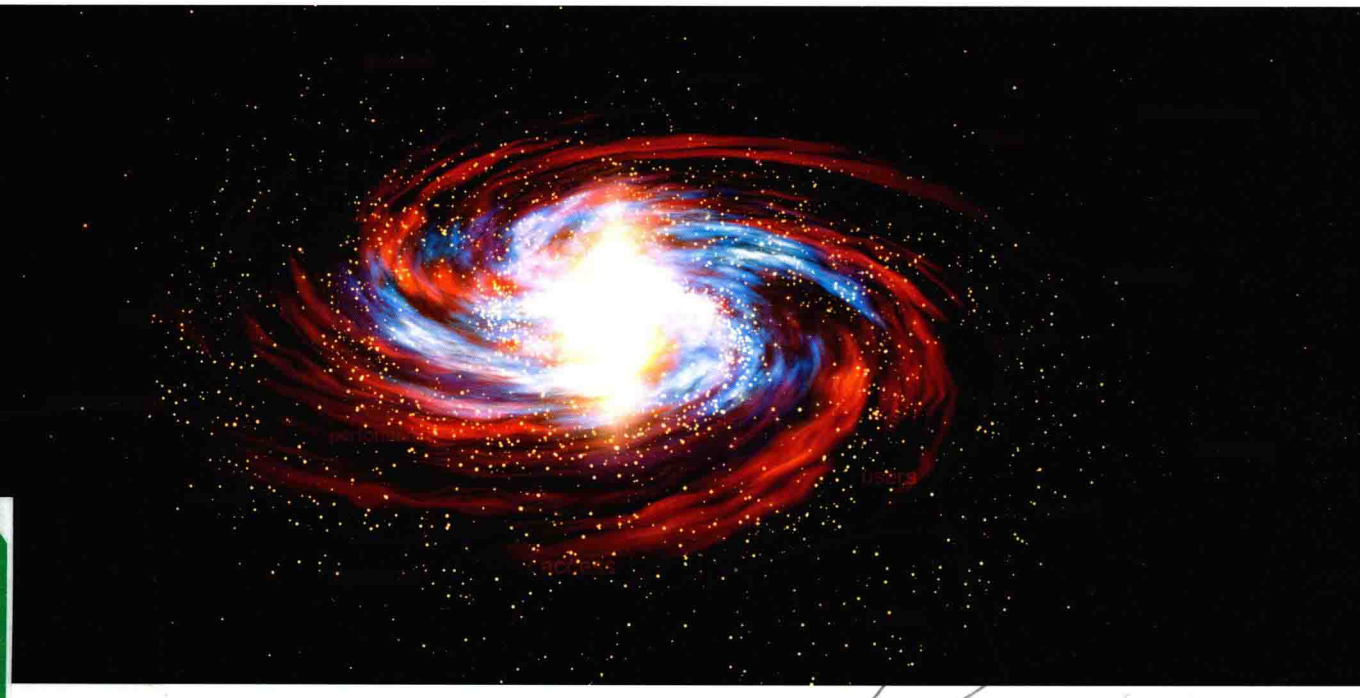
计算机类专业
系统能力培养
系列教材

云计算方向

云安全原理与实践

CLOUD SECURITY PRINCIPLE AND PRACTICE

陈兴蜀 葛龙 主编
罗永刚 曾雪梅 王海舟 王文贤 编著



- 全面、系统地介绍云安全的概念、原理、技术、运维、标准、法律法规
- 学术研究与产业界工程实践紧密联系，理论与实用性有机融合

机械工业出版社
China Machine Press

教育部-阿里云产学合作协同育人项目成果

计算机类专业
系统能力培养
系列教材

云计算方向

云安全原理与实践

CLOUD SECURITY PRINCIPLE AND PRACTICE

陈兴蜀 葛龙 主编

罗永刚 曾雪梅 王海舟 王文贤 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

云安全原理与实践 / 陈兴蜀，葛龙主编 . —北京：机械工业出版社，2017.7
（计算机类专业系统能力培养系列教材）

ISBN 978-7-111-57468-2

I. 云… II. ①陈… ②葛… III. 计算机网络 – 安全技术 – 教材 IV. TP393.08

中国版本图书馆 CIP 数据核字（2017）第 159613 号

本书系统地介绍了云安全的基本概念、原理和技术，主要内容包括云计算的安全风险分析、虚拟化安全、身份管理与访问控制、云数据安全、云运维安全、云服务的安全使用、云安全解决方案以及云计算相关的标准、法规等，并通过产业案例使读者掌握云安全的相关实践技术，从产业发展角度理解云安全的技术发展和趋势。

本书适合作为高等院校信息安全、计算机、电子工程及相关专业云安全课程的教材，也适合作为从事云安全工作的技术人员和研究人员的参考书。

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：朱　劼　　责任校对：李秋荣
印　　刷：北京诚信伟业印刷有限公司　　版　　次：2017 年 8 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：16.5
书　　号：ISBN 978-7-111-57468-2　　定　　价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

FOREWORD

丛书序言

——计算机专业学生系统能力培养和系统课程设置的研究

未来的5～10年是中国实现工业化与信息化融合，利用信息技术与装备提高资源利用率、改造传统产业、优化经济结构、提高技术创新能力与现代管理水平的关键时期，而实现这一目标，对于高效利用计算系统的其他传统专业的专业人员需要了解和掌握计算思维，对于负责研发多种计算系统的计算机专业的专业人员则需要具备系统级的设计、实现和应用能力。

1. 计算技术发展特点分析

进入本世纪以来，计算技术正在发生重要发展和变化，在20世纪个人机普及和Internet快速发展基础上，计算技术从初期的科学计算与信息处理进入了以移动互联、物物相联、云计算与大数据计算为主要特征的新型网络时代，在这一发展过程中，计算技术也呈现出以下新的系统形态和技术特征。

（1）四类新型计算系统

1）嵌入式计算系统 在移动互联网、物联网、智能家电、三网融合等行业技术与产业发展中，嵌入式计算系统有着举足重轻和广泛的作用。例如，移动互联网中的移动智能终端、物联网中的汇聚节点、“三网融合”后的电视机顶盒等是复杂而新型的嵌入式计算系统；除此之外，新一代武器装备，工业化与信息化融合战略实施所推动的工业智能装备，其核心也是嵌入式计算系统。因此，嵌入式计算将成为新型计算系统的主要形态之一。在当今网络时代，嵌入式计算系统也日益呈现网络化的开放特点。

2）移动计算系统 在移动互联网、物联网、智能家电以及新型装备中，均以移动通信网络为基础，在此基础上，移动计算成为关键技术。移动计算技术将使计算机或其他信息智能终端设备在无线环境下实现数据传输及资源共享，其核心技术涉及支持高性能、低功耗、无线连接和轻松移动的移动处理机及其软件技术。

3）并行计算系统 随着半导体工艺技术的飞速进步和体系结构的不断发展，多核/众核处理机硬件日趋普及，使得昔日高端的并行计算呈现出普适化的发展趋势；多核技术就是在

处理器上拥有两个或更多一样功能的处理器核心，即将数个物理处理器核心整合在一个内核中，数个处理器核心在共享芯片组存储界面的同时，可以完全独立地完成各自操作，从而能在平衡功耗的基础上极大地提高 CPU 性能；其对计算系统微体系结构、系统软件与编程环境均有很大影响；同时，云计算也是建立在廉价服务器组成的大规模集群并行计算基础之上。因此，并行计算将成为各类计算系统的基础技术。

4）基于服务的计算系统 无论是云计算还是其他现代网络化应用软件系统，均以服务计算为核心技术。服务计算是指面向服务的体系结构（SOA）和面向服务的计算（SOC）技术，它是标识分布式系统和软件集成领域技术进步的一个里程碑。服务作为一种自治、开放以及与平台无关的网络化构件可使分布式应用具有更好的复用性、灵活性和可增长性。基于服务组织计算资源所具有的松耦合特征使得遵从 SOA 的企业 IT 架构不仅可以有效保护企业投资、促进遗留系统的复用，而且可以支持企业随需应变的敏捷性和先进的软件外包管理模式。Web 服务技术是当前 SOA 的主流实现方式，其已经形成了规范的服务定义、服务组合以及服务访问。

（2）“四化”主要特征

1）网络化 在当今网络时代，各类计算系统无不呈现出网络化发展趋势，除了云计算系统、企业服务计算系统、移动计算系统之外，嵌入式计算系统也在物联时代通过网络化成为开放式系统。即，当今的计算系统必然与网络相关，尽管各种有线网络、无线网络所具有的通信方式、通信能力与通信品质有较大区别，但均使得与其相联的计算系统能力得以充分延伸，更能满足应用需求。网络化对计算系统的开放适应能力、协同工作能力等也提出了更高的要求。

2）多媒体化 无论是传统 Internet 应用服务，还是新兴的移动互联网服务业务，多媒体化是其面向人类、实现服务的主要形态特征之一。多媒体技术是利用计算机对文本、图形、图像、声音、动画、视频等多种信息进行综合处理、建立逻辑关系和人机交互作用的新技术。多媒体技术使计算机可以处理人类生活中最直接、最普遍的信息，从而使得计算机应用领域及功能得到了极大的扩展，使计算机系统的人机交互界面和手段更加友好和方便。多媒体具有计算机综合处理多种媒体信息的集成性、实时性与交互性特点。

3）大数据化 随着物联网、移动互联网、社会化网络的快速发展，半结构化及非结构化的数据呈几何倍增长。数据来源的渠道也逐渐增多，不仅包括了本地的文档、音视频，还包括网络内容和社交媒体；不仅包括 Internet 数据，更包括感知物理世界的数据。从各种类型的数据中快速获得有价值信息的能力，称为大数据技术。大数据具有体量巨大、类型繁多、

价值密度低、处理速度快等特点。大数据时代的来临，给各行各业的数据处理与业务发展带来重要变革，也对计算系统的新型计算模型、大规模并行处理、分布式数据存储、高效的数据处理机制等提出了新的挑战。

4）智能化 无论是计算系统的结构动态重构，还是软件系统的能力动态演化；无论是传统 Internet 的搜索服务，还是新兴移动互联的位置服务；无论是智能交通应用，还是智能电网应用，无不显现出鲜明的智能化特征。智能化将影响计算系统的体系结构、软件形态、处理算法以及应用界面等。例如，相对于功能手机的智能手机是一种安装了开放式操作系统的手机，可以随意安装和卸载应用软件，具备无线接入互联网、多任务和复制粘贴以及良好用户体验等能力；相对于传统搜索引擎的智能搜索引擎是结合了人工智能技术的新一代搜索引擎，不仅具有传统的快速检索、相关度排序等功能，更具有用户角色登记、用户兴趣自动识别、内容的语义理解、智能信息化过滤和推送等功能，其追求的目标是根据用户的请求从可以获得的网络资源中检索出对用户最有价值的信息。

2. 系统能力的主要内涵及培养需求

（1）主要内涵

计算机专业学生的系统能力的核心是掌握计算系统内部各软件 / 硬件部分的关联关系与逻辑层次；了解计算系统呈现的外部特性以及与人和物理世界的交互模式；在掌握基本系统原理的基础上，进一步掌握设计、实现计算机硬件、系统软件以及应用系统的综合能力。

（2）培养需求

要适应“四类计算系统，四化主要特征”的计算技术发展特点，计算机专业人才培养必须“与时俱进”，体现计算技术与信息产业发展对学生系统能力培养的需求。在教育思想上要突现系统观教育理念，在教学内容中体现新型计算系统原理，在实践环节上展现计算系统平台技术。

要深刻理解系统化专业教育思想对计算机专业高等教育过程所带来的影响。系统化教育和系统能力培养要采取系统科学的方法，将计算对象看成一个整体，追求系统的整体优化；要夯实系统理论基础，使学生能够构建出准确描述真实系统的模型，进而能够用于预测系统行为；要强化系统实践，培养学生能够有效地构造正确系统的能力。

从系统观出发，计算机专业的教学应该注意教学生怎样从系统的层面上思考（设计过程、工具、用户和物理环境的交互），讲透原理（基本原则、架构、协议、编译以及仿真等），强化系统性的实践教学培养过程和内容，激发学生的辩证思考能力，帮助他们理解和掌控数字世界。

3. 计算机专业系统能力培养课程体系设置总体思路

为了更好地培养适应新技术发展的、具有系统设计和系统应用能力的计算机专门人才，

我们需要建立新的计算机专业本科教学课程体系，特别是设立有关系统级综合性课程，并重新规划计算机系统核心课程的内容，使这些核心课程之间的内容联系更紧密、衔接更顺畅。

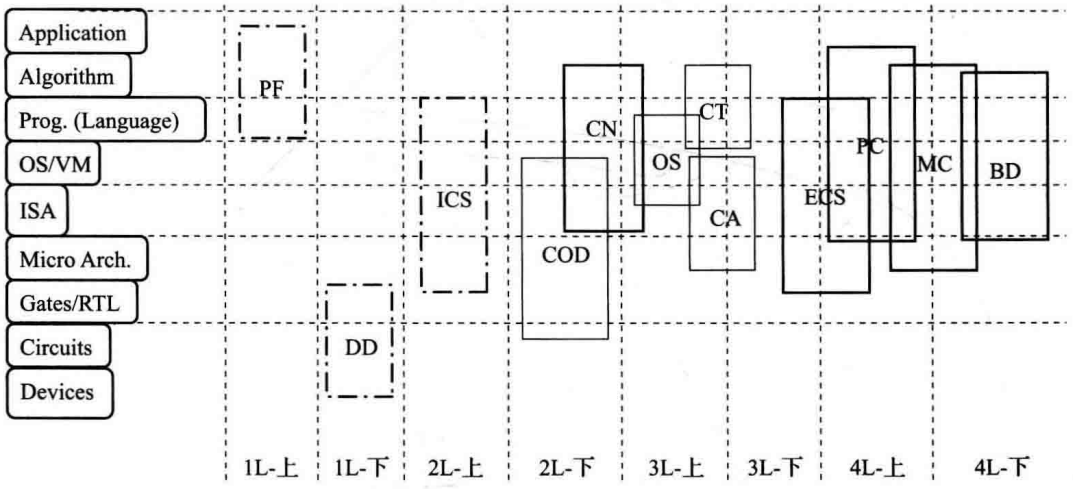
我们建议把课程分成三个层次：计算机系统基础课程、重组内容的核心课程、侧重不同计算系统的若干相关平台应用课程。

第一层次核心课程包括："程序设计基础（PF）""数字逻辑电路（DD）"和"计算机系统基础（ICS）"。

第二层次核心课程包括："计算机组成与设计（COD）""操作系统（OS）""编译技术（CT）"和"计算机系统结构（CA）"。

第三层次核心课程包括："嵌入式计算系统（ECS）""计算机网络（CN）""移动计算（MC）""并行计算（PC）"和"大数据并行处理技术（BD）"。

基于这三个层次的课程体系中相关课程设置方案如下图所示。



图中左边部分是计算机系统的各个抽象层，右边的矩形表示课程，其上下两条边的位置标示了课程内容在系统抽象层中的涵盖范围，矩形的左右两条边的位置标示了课程大约在哪个年级开设。点划线、细实线和粗实线分别表示第一、第二和第三层次核心课程。

从图中可以看出，该课程体系的基本思路是：先讲顶层比较抽象的编程方面的内容；再讲底层有关系统的具体实现基础内容；然后再从两头到中间，把顶层程序设计的内容和底层电路的内容按照程序员视角全部串起来；在此基础上，再按序分别介绍计算机系统硬件、操作系统和编译器的实现细节。至此的所有课程内容主要介绍单处理器系统的相关内容，而计算机体系结构主要介绍各不同并行粒度的体系结构及其相关的操作系统实现技术和编译器实现技术。第三层次的课程没有先后顺序，而且都可以是选修课，课程内容应体现第一和第二

层次课程内容的螺旋式上升趋势，也即第三层次课程内容涉及的系统抽象层与第一和第二层次课程涉及的系统抽象层是重叠的，但内容并不是简单重复，应该讲授在特定计算系统中的相应教学内容。例如，对于“嵌入式计算系统（ECS）”课程，虽然它所涉及的系统抽象层与“计算机系统基础（ICS）”课程涉及的系统抽象层完全一样，但是，这两门课程的教学内容基本上不重叠。前者着重介绍与嵌入式计算系统相关的指令集体系结构设计、操作系统实现和底层硬件设计等内容，而后者着重介绍如何从程序员的角度来理解计算机系统设计与实现中涉及的基础内容。

与传统课程体系设置相比，最大的不同在于新的课程体系中有一门涉及计算机系统各个抽象层面的能够贯穿整个计算机系统设计和实现的基础课程：“计算机系统基础（ICS）”。该课程讲解如何从程序员角度来理解计算机系统，可以使程序员进一步明确程序设计语言中的语句、数据和程序是如何在计算机系统中实现和运行的，让程序员了解不同的程序设计方法为什么会有不同的性能等。

此外，新的课程体系中，强调课程之间的衔接和连贯，主要体现在以下几个方面。

1）“计算机系统基础”课程可以把“程序设计基础”和“数字逻辑电路”之间存在于计算机系统抽象层中的“中间间隔”填补上去并很好地衔接起来，这样，到 2L- 上结束的时候，学生就可以通过这三门课程清晰地建立单处理器计算机系统的整机概念，构造出完整的计算机系统的基本框架，而具体的计算机系统各个部分的实现细节再通过后续相关课程来细化充实。

2）“数字逻辑电路”“计算机组成与设计”“嵌入式计算系统”中的实验内容之间能够很好地衔接，可以规划一套承上启下的基于 FPGA 开发板的综合实验平台，让学生在一个统一的实验平台上从门电路开始设计基本功能部件，然后再以功能部件为基础设计 CPU、存储器和外围接口，最终将 CPU、存储器和 I/O 接口通过总线互连为一个完整的计算机硬件系统。

3）“计算机系统基础”“计算机组成与设计”“操作系统”和“编译技术”之间能够很好地衔接。新课程体系中“计算机系统基础”和“计算机组成与设计”两门课程对原来的“计算机系统概论”和“计算机组成原理”的内容进行了重新调整和统筹规划，这两门课程的内容是相互密切关联的。对于“计算机系统基础”与“操作系统”“编译技术”的关系，因为“计算机系统基础”以 Intel x86 为模型机进行讲解，所以它为“操作系统”（特别是 Linux 内核分析）提供了很好的体系结构基础。同时，在“计算机系统基础”课程中为了清楚地解释程序中的文件访问和设备访问等问题，会从程序员角度简单引入一些操作系统中的相关基础知识。此外，在“计算机系统基础”课程中，会讲解高级语言程序如何进行转换、链接以生成可执行代码的问题；“计算机组成与设计”中的流水线处理等也与编译优化相关，而且

“计算机组成与设计”以MIPS为模型机进行讲解，而MIPS模拟器可以为“编译技术”的实验提供可验证实验环境，因而“计算机系统基础”和“计算机组成与设计”两门课程都与“编译技术”有密切的关联。“计算机系统基础”“计算机组成与设计”“操作系统”和“编译技术”这四门课程构成了一组计算机系统能力培养最基本的核心课程。

从“计算机系统基础”课程的内容和教学目标以及开设时间来看，位于较高抽象层的先行课（如程序设计基础和数据结构等课程）可以按照原来的内容和方式开设和教学，而作为新的“计算机系统基础”和“计算机组成与设计”先导课的“数字逻辑电路”，则需要对传统的教学内容，特别是实验内容和实验手段方面进行修改和完善。

有了“计算机系统基础”和“计算机组成与设计”课程的基础，作为后续课程的操作系统、编译原理等将更容易被学生从计算机系统整体的角度理解，课程内容方面不需要大的改动，但是操作系统和编译器的实验要以先行课程实现的计算机硬件系统为基础，这样才能形成一致的、完整的计算机系统整体概念。

本研究还对12门课程的规划思路、主要教学内容及实验内容进行了研究和阐述，具体内容详见公开发表的研究报告。

4. 关于本研究项目及本系列教材

机械工业出版社华章公司在较早的时间就引进出版了MIT、UC-Berkeley、CMU等国际知名院校有关计算机系统课程的多种教材，并推动和组织了计算机系统能力培养相关的研究，对国内计算机系统能力培养起到了积极的促进作用。

本项研究是教育部2013 ~ 2017年计算机类专业教学指导委员会“计算机类专业系统能力培养研究”项目之一，研究组成员由国防科技大学王志英、北京航空航天大学马殿富、西北工业大学周兴社、南开大学吴功宜、武汉大学何炎祥、南京大学袁春风、北京大学陈向群、中国科技大学安虹、天津大学张刚、机械工业出版社华章公司温莉芳等组成，研究报告分别发表于中国计算机学会《中国计算机科学技术发展报告》及《计算机教育》杂志。

本系列教材编委会在上述研究的基础上对本套教材的出版工作经过了精心策划，选择了对系统观教育和系统能力培养有研究和实践的教师作为作者，以系统观为核心编写了本系列教材。我们相信本系列教材的出版和使用，将对提高国内高校计算机类专业学生的系统能力和整体水平起到积极的促进作用。

“计算机类专业系统能力培养系列教材”编委会

2014年5月

本书编委会

主编　陈兴蜀（四川大学）

　　葛　龙（四川大学）

编委　（按拼音顺序排列）

董斌雁（阿里云公司）　　李　俊（阿里云公司）

李兰柱（阿里云公司）　　李妹芳（阿里云公司）

罗永刚（四川大学）　　苏建东（阿里云公司）

王海舟（四川大学）　　王文贤（四川大学）

王晓斐（阿里云公司）　　邬　怡（阿里云公司）

肖　力（阿里云公司）　　杨　宁（阿里云公司）

曾雪梅（四川大学）

特别感谢

肖　力（阿里云公司）

李妹芳（阿里云公司）

PREFACE

序

当前，一场科技革命浪潮正席卷全球，这一次，IT 技术是主角之一。云计算、大数据、人工智能、物联网，这些新技术正加速走向应用。很快，它们将渗透至我们生产、生活中的每个角落，并将深刻改变我们的世界。

在这些新技术当中，云计算作为基础设施，将全面支撑各类新技术、新应用。我认为：云计算，特别是公共云，将成为这场科技革命的承载平台，全面支撑各类技术创新、应用创新和模式创新。

作为一种普惠的公共计算资源与服务，云计算与传统 IT 计算资源相比有以下几个方面的优势：一是硬件的集约化；二是人才的集约化；三是安全的集约化；四是服务的普惠化。

公共云计算的快速发展将带动云计算产业进入一个新的阶段，我们可以称之为“云计算 2.0 时代”，云计算对行业演进发展的支撑作用将更加凸显。

云计算是“数据在线”的主要承载。“在线”是我们这个时代最重要的本能，它让互联网变成了最具渗透力的基础设施，数据变成了最具共享性的生产资料，计算变成了随时随地的公共服务。云计算不仅承载数据本身，同时也承载数据应用所需的计算资源。

云计算是“智能”与“智慧”的重要支撑。智慧有两大支撑，即网络与大数据。包括互联网、移动互联网、物联网在内的各种网络，负责搜集和共享数据；大数据作为“原材料”，是各类智慧应用的基础。云计算是支撑网络和大数据的平台，所以，几乎所有智慧应用都离不开云计算。

云计算是企业享受平等 IT 应用与创新环境的有力保障。当前，企业创新，特别是小微企业和创业企业的创新面临 IT 技术和 IT 成本方面的壁垒。云计算的出现打破了这一壁垒，IT 成为唾手可得的基础性资源，企业无须把重点放在 IT 支撑与实现上，可以更加聚焦于擅长的领域进行创新，这对提升全行业的信息化水平以及激发创新创业热情将起到至关重要的作用。

除了发挥基础设施平台的支撑作用外，2.0 时代的云计算，特别是公共云计算对产业的影响将从量变到质变。我认为，公共云将全面重塑整个 ICT 生态，向下定义数据中心、IT 设备，甚至是 CPU 等核心器件，向上定义软件与应用，横向承载数据与安全，纵向支撑人工智能的技术演进与应用创新。

对我国来说，发展云计算产业的战略意义重大。我认为，云计算已不仅仅是“IT 基础设施”，它将像电网、移动通信网、互联网、交通网络一样，成为“国家基础设施”，全面服务国家多项重大战略的实施与落地。

云计算是网络强国建设的重要基石。发展云计算产业，有利于我国实现 IT 全产业链的自主可控，提高信息安全保障水平，并推动大数据、人工智能的发展。

云计算是提升国家治理能力的重要工具。随着大数据、人工智能、物联网等技术应用到智慧城市、智慧政务建设中，国家及各城市的治理水平和服务能力大幅提升，这背后，云计算平台功不可没。

云计算将全面推动国家产业转型升级。云计算将支撑“中国制造 2025”“互联网 +”战略，全面推动“两化”深度融合。同时，云计算也为创新创业提供了优质土壤，在“双创”领域，云计算已真正成为基础设施。

在 DT 时代，我认为计算及计算的能力是衡量一个国家科技实力和创新能力的重要标准。只有掌握计算能力，才具备全面支撑创新的基础，才有能力挖掘数据的价值，才能在重塑 ICT 生态过程中掌握主导权。

接下来的几年，云计算将成为全球科技和产业竞争的焦点。目前，我国的云计算产业具备和发达国家抗衡的能力，而我们对数据的认知、驾驭能力及对资源的利用开发和人力也是与发达国家等同的。因此，我们正处在一个“黄金窗口期”。

我一直认为，支撑技术进步和产业发展的最主要力量是人才，未来世界各国在云计算、大数据、AI 等领域的竞争，在某种程度上会转变为人才之争。因此，加强专业人才培养将是推动云计算、大数据产业发展的重要抓手。

由于是新兴产业，我国云计算、大数据领域的人才相对短缺。作为中国最大的云计算服务企业，阿里云希望能在云计算、大数据领域的人才培养方面做出努力，将我们在云计算、大数据领域的实践经验贡献到高校的教育中，为高校的课程建设提供支持。

与传统 IT 基础技术理论相比，云计算和大数据更偏向应用，而这方面恰恰是阿里云的优势。因此，我们与高校合作，优势互补，将计算机科学的理论和阿里云的产业实践融合起来，让大家从实战的角度认识、掌握云计算和大数据。

我们希望通过这套教材，把阿里云一些经过检验的经验与成果分享给全社会，让众多计算机相关专业学生、技术开发者及所有对云计算、大数据感兴趣的企业和个人，可以与我们一起推动中国云计算、大数据产业的健康快速发展！

胡晓明

阿里云总裁

PREFACE

前　言

近几年，云计算（Cloud Computing）迅速发展，从美国的亚马逊到我国的阿里云，国内外的云计算服务提供商提供了类型繁多、性价比高的IT服务模式，新的服务类型还在不断推出，并在各行各业得到了广泛应用。云计算是信息技术发展过程中的一次巨大变革，众多国家政府以及大型IT企业都制定了云计算发展战略规划，以引领或适应技术变革的趋势。

在云计算发展的同时，其安全问题也日益凸显。CSA（Cloud Security Alliance，云安全联盟）在2016年2月发布了《2016年12大顶级云计算安全威胁》，指出了包括数据泄露、系统漏洞、拒绝服务、共享技术等在内的12项云安全威胁，云计算的安全问题逐渐成为制约其快速应用和发展的重要因素。

为了让读者全面了解云计算中的安全问题，本书从云计算的基本概念入手，由浅入深地分析了云计算中面临的安全威胁、云计算服务应具备的安全能力、如何安全地使用云计算服务，以及云安全的相关标准等。本书强调云计算的技术特点，系统介绍了云计算服务过程中提供方、使用方所关注的安全问题，并将理论与实践紧密结合。在本书撰写过程中，四川大学网络空间安全研究院与阿里云深度合作，共同探讨教材的大纲、内容，并同时面向研究生和高年级本科生授课，探索高校课程和教材建设的创新合作模式。本书是学术研究成果与企业实践的结合，关键技术章节配有基于阿里云平台的实验，“理论＋实践”的模式使得读者能够更好地理解教材所阐述的关键知识点，通过动手实践让读者加深对理论知识的理解。

本书分为四个部分，包含11章，各个部分的内容组织安排如下：

第一部分（包括第1章和第2章）主要介绍云计算相关的基础知识。其中，第1章概述云计算的发展历程以及基本概念，并对云服务中的角色和责任进行了划分和界定，为读者后续的深入学习奠定基础。第2章从技术、管理以及法律法规三个方面分析了云计算的安全风险，并给出了进行云计算安全设计时需要考虑的原则。

第二部分（包括第3~8章）剖析云计算服务的安全能力、运维安全以及云安全技术的发展。其中，第3章讨论主机虚拟化带来的安全问题，详细分析其面临的虚拟机信息窃取、虚拟机逃逸、Rootkit攻击等安全威胁及其对应的安全解决方案。第4章阐释网络虚拟化的安全问题，分析IaaS环境下网络安全域的划分与构建，并介绍阿里云的VPC，最后提出两种针对虚拟网络的安全服务接入机制。第5章介绍云计算下的身份认证、授权管理以及操作审计。第6章根据云数据安全的生命周期，分析数据从创建到销毁各个阶段面临的安全问题以及对应的关键保护技术。第7章介绍云运维的基本内容，分析其相对于传统运维的区别以及应注意的问题。第8章结合下一代网络应该考虑的技术，介绍零信任模型、MSSP、APT攻击防御、大数据安全分析等内容。

第三部分（包括第9章和第10章）介绍如何安全地使用云计算服务。其中，第9章针对云用户控制权弱化的问题，区分了云计算服务的角色并进行了责任划分，然后从用户的角度介绍云计算服务的使用过程。第10章结合不同应用场景介绍云安全解决方案。

第四部分（包括第11章）介绍当前云计算服务的安全标准和管理机制。第11章阐释国内外云计算服务的安全管理、云安全标准以及管理规范。

本书的层次结构清晰，内容循序渐进，可作为高等院校信息安全、计算机及其他信息学科云安全相关课程的教材，也可以作为广大云计算运维人员、云计算安全开发人员以及对云安全感兴趣的读者的参考书籍。作为教材时，可参考第3章到第5章的最佳实践进行课程实验，包括第3章云计算平台中的虚拟化主机安全管理，第4章VPC的相关实验，第5章身份管理、权限管理以及操作审计的实践等。本书为读者提供云安全问题的系统知识，并借助阿里云的实践使读者深入理解关键技术，提升读者对云安全理论的掌握和应用能力。

本书由陈兴蜀主持编写，第1~2章和第11章由陈兴蜀编写，第3章、第6章由曾雪梅编写，第4~5章和第8章由葛龙编写，第7章由罗永刚编写，第9章由王海舟编写，第10章由王文贤编写。本书在写作的过程中得到了四川大学网络空间安全研究院师生的大力支持，王毅桐、金鑫、邵国林、杨露、陈广瑞、苑中梁、车奔、陈佳昕、赵成、陈蒙蒙、赵丹丹、王煜骢、王伟、王小艳、滑强、李敏毓、马晨曦等进行了大量的工作，没有他（她）们的支持与帮助，很难完成本书编写工作。

本书是教育部－阿里云产学合作专业综合改革项目的规划教材，同时获得四川大学研究生课程建设项目的支持。

感谢阿里云团队对本书编写给予的大力支持，李妹芳、苏建东、杨宁、李俊、李兰柱、董斌雁、安忍、王晓斐、邬怡、杨宁、肖力等阿里云的专家为本书的编写提供了大量帮助，尤其

在讨论书稿内容、提出重要建议、申请阿里云平台资源、提供参考资料等方面给予了重要支持。

同时还要感谢机械工业出版社华章分社朱劼编辑和出版团队的辛勤工作。

本书仅代表作者及研究团队对于云计算安全的观点，由于水平有限，书中难免存在不准确或不足之处，恳请读者批评指正，以便后续改进和完善。

编者

2017 年 5 月

CONTENTS

目　录