云计算安全

陈晓峰　马建峰　李　晖　李　进　著

科学出版社

云计算安全

陈晓峰　马建峰　李　晖　李　进　著

科学出版社

北京

内 容 简 介

本书以云计算安全的基础理论和关键技术为主要内容。全书共 6 章，第 1 章是云计算基本概念介绍；第 2 章是可证明安全理论基础；第 3~6 章是全书的重点内容，介绍云安全技术的各个方面，包括可搜索加密技术、基于属性的加密技术、安全外包计算技术以及云存储安全技术。本书融前沿性、丰富性、实用性为一体，囊括云计算安全技术研究的基本核心领域，选取的内容紧扣前沿主题，有助于广大读者了解云计算安全研究的基本内容和核心技术。

本书可作为高等院校信息安全和密码学专业本科生和研究生的教材，也可供信息安全从业人员、云计算安全研究人员参考。

图书在版编目(CIP)数据

云计算安全/陈晓峰等著. —北京：科学出版社, 2016. 2

ISBN 978-7-03-047216-8

Ⅰ. ①云… Ⅱ. ①陈… 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 020448 号

责任编辑：杨向萍 李 萍 纪四稳／责任校对：张小霞

责任印制：赵 博／封面设计：迷底书装

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

中国科学院印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2016 年 2 月第 一 版 开本：720×1000 1/16

2016 年 2 月第一次印刷 印张：11 1/2

字数：232 000

定价：80.00 元

(如有印装质量问题，我社负责调换)

前　言

云计算是一种具有动态延展能力的运算方式，它可以看成分布式计算、并行处理计算、网格计算等概念的发展和应用，实现了人们长期以来“把计算作为一种基础设施”的梦想。基于云计算技术，云计算平台可以在数秒之内处理数以千万甚至亿万的信息，从而把信息资源（包括计算、存储及带宽）以服务的形式通过因特网提供给个人用户和厂商，大大减轻了资源受限用户对软件管理及硬件维护的负担，从而彻底改变了传统 IT 产业的架构和运行方式。

云计算在提供多种高效灵活的数据服务的同时，也面临着诸多挑战和一些急需解决的安全问题。目前，云计算、云存储及云安全已成为学术界和产业界共同关注的研究热点。

本书主要阐述云计算安全中的关键理论和技术。全书共 6 章，第 1 章是云计算基本概念介绍；第 2 章是可证明安全理论基础；第 3~6 章是全书的重点内容，分别介绍云计算安全关键理论和技术，包括可搜索加密技术、基于属性的加密技术、安全外包计算技术以及云存储安全技术等。

目前，国内外已有一些云计算安全的相关书籍出版。然而，已有的书籍大部分是从宏观的角度阐述云计算所面临的安全问题，侧重于云计算安全的架构和安全体系等，较少涉及基础理论和技术细节。

本书选材经过精心考虑，紧扣目前学术研究前沿领域，侧重于云计算安全的基础理论和关键技术，其中也包括作者近几年的主要研究成果。在写作过程中，既介绍研究的动机和背景，又介绍相关的理论、算法和方案，还给出了未来可能的研究方向，从而形成一个完整的体系。

本书可作为高校信息安全和密码学专业本科生和研究生的教材，也可作为云计算安全研发人员的学习和参考资料。

作者对参与本书编写的王剑锋博士、叶俊博士、黄慧博士、姜涛博士、刘亮博士、赵远杰硕士、党晓硕士、陈鹏硕士、谢星星硕士、聂海新硕士、冯岩盛硕士、邹琴硕士、朱怡潇硕士、张肖瑜硕士等一并表示感谢。另外，本书的编写得到国家自然

科学基金项目“云计算平台下数据安全的关键密码技术研究”(批准号：61272455)，教育部新世纪优秀人才支持计划基金 (批准号：NCET-13-0946) 和国家 863 计划项目“云计算平台的可信与可控技术及其支撑系统”(批准号：2015AA016007) 的资助，特此表示感谢。

由于作者水平有限，书中不妥之处在所难免，恳请读者提出宝贵意见。

作　者

2015 年 11 月 16 日

目　　录

第1章 绪 论

云计算实现了人类把计算作为一种基础设施的梦想，目前已成为学术界、产业界和政府部门共同关注的研究热点。本章主要介绍云计算的概念及其研究进展，并阐述云计算目前面临的主要安全挑战。

1.1 云 计 算

1989 年，欧洲核子研究中心研究员蒂姆 · 伯纳斯 · 李 (Tim Berners Lee) 首次提出“万维网”(World Wide Web) 的概念，这是计算机网络发展史上的一大里程碑。2004 年，蒂姆因万维网荣获第一届“千年技术奖”，成为“互联网之父”。随后，从最初的 Web 1.0 到成熟的 Web 3.0[1]，万维网的每一次跨越都给人们带来了全新的体验。最初的 Web 1.0 主要是各大网站以“单向”的方式传递信息，而用户只能通过搜索引擎搜索自己所需的信息或资源，此时的网络相当于一部“百科全书”。相对于 Web 1.0 只能实现“读”的功能，Web 2.0 则更注重交互性。此时，用户不仅是网站的浏览者，更是网站的制作者。Web 3.0 不仅继承了 Web 1.0 和 Web 2.0 的优点，同时更具智能化，能够对用户提供的信息进行有效整合，使内容特征更加明显，便于搜索。随着网络发展的日新月异，网络用户的数量也在以惊人的速度增加。国际电信联盟发布的数据显示，全球互联网用户数 2009 年为 20 亿，2014 年已突破 30 亿大关。人们在享受网络上丰富信息带来的便利的同时也在忍受着诸多问题的困扰。这些问题追根究底都是因为各种资源的受限，如计算资源、存储资源、带宽等。

2007 年，全球最大的搜索引擎服务提供商 Google 首次提出了云计算的概念，它实现了人们长期以来的“把计算作为一种基础设施”的梦想。此后，在 IBM、Google、Yahoo、Amazon 等 IT 行业巨头的大力推动之下，云计算迅速风靡全球。云计算代表了信息领域迅速向集约化、规模化与专业化道路发展的趋势，已成为产业界、学术界、政府等各界共同关注的焦点。我国政府对云计算高度重视，2011 年 7 月公布的《国家“十二五”科学和技术发展规划》中将云计算作为新

一代信息技术发展的重要方向之一，要着力实施“中国云”工程，建设国家级云计算平台，掌握云计算和高性能计算的核心技术。

1.1.1　云计算的概念

什么是云计算？通俗地讲，云计算就是以用户为中心的一种计算服务。而且，该服务就像是天上的“云”，用户可以随时根据自己的需求改变它的“规模”“形状”“配置”等。维基百科[2] 上定义云计算是“一种基于互联网的计算方式，通过这种方式，共享的软硬件资源和信息可以按需求提供给计算机和其他设备”。中国云计算专家委员会认为“云计算是通过整合、管理、调配分布在网络各处的计算资源，并以统一的界面同时向大量用户提供服务”。这些定义叙述不一，但内涵却大致相同，即将计算资源作为一种服务提供给资源受限的用户。

云计算是并行计算 (Parallel Computing)、分布式计算 (Distributed Computing) 和网格计算 (Grid Computing) 的融合和发展，然而又有所区别。

并行计算是相对于串行计算的，其基本原理是将单个复杂的任务细化成多个任务，分别交给多个不同的处理器进行处理，最后将每个小任务的结果返回，再集中处理得到最终结果。在此过程中，每个细化的任务之间相互互联，如果其中任一任务的结果出现错误，都将会影响最终的结果。分布式计算的产生就是为了处理并行计算遗留的故障 (细化的任务中某一个或者多个任务未能正确执行或者返回的结果是错误的，将会影响最终结果)，它能够通过网络将成千上万台计算机连接起来，共同完成单台计算机无法完成的巨大的计算任务。类似于并行计算，分布式计算同样是将大任务划分为多个小任务进行处理，但不同之处在于，每个小任务之间是相互独立的，上一个任务的结果未返回或者结果错误不会影响下一个任务的执行。网格计算是分布式计算的一种，强化了分布式处理计算的能力，它是通过互联网将物理位置不同的计算机连接起来组成一个“虚拟的超级计算机”，利用闲置的资源增强自身的计算能力并达到资源共享的目的。云计算是这三种计算模式的又一次升华，它不仅具备三种计算模式的特点，同时又弱化了对硬件资源的需求，将硬件资源转化成“虚拟的资源”。

1.1.2　云计算的服务构架

云计算的服务构架总共分为三个部分[3]，即基础构架即服务 (Infrastructure as a Service, IaaS)、平台即服务 (Platform as a Service, PaaS) 和软件即服务 (Software

as a Service, SaaS)。

1. 基础构架即服务

云计算的最底层。基础构架即服务 (IaaS) 拥有数以万计的服务器，可提供最基本的计算和存储资源。用户可以通过互联网访问云平台上的资源，采用“租用”的形式让 IaaS 平台上的资源为自己所用，并且无需为基础的硬件设备付出相应的原始成本。同时，它还具有自动按需分配的功能，可以根据用户计算或存储的需求自动分配相应数量的服务器，从而避免了用户为闲置的服务器付费，实现按需付费，为用户节省开支。此外，在使用资源的过程中，用户同样无需管理或控制任何云计算基础设施，但能够在此基础上调用资源。典型的例子有 Amazon EC2、Hadoop、Amazon S3 等。

2. 平台即服务

云计算的中间层。平台即服务 (PaaS) 主要向开发人员提供基于互联网的应用程序开发或测试平台。通过 PaaS 平台，开发人员可以在云端实现应用程序的设计、开发、测试、托管等一系列操作。该平台以服务的模式提供给用户，因此用户只需为自己使用的服务付费，无需为硬件或软件资源付费。除此之外，应用程序在云端上的维护十分简单，方便开发人员后续跟进。这种成本低、方便高效、应用简单的开发平台无疑会得到许多大、小型企业的青睐。典型的例子有 Google AppEngine、Microsoft Azure 等。

3. 软件即服务

云计算的最高层。软件即服务 (SaaS) 主要面向互联网终端用户，以服务的模式通过互联网将应用程序提供给终端用户。用户可以通过互联网向专门的应用程序提供商获取带有相应程序功能的服务，且无需购买应用程序，也无需将应用程序安装在自己的计算机或服务器上。由始至终用户获取的都只是应用程序的服务而不是应用程序本身，因此，用户避免了应用程序的管理和维护，同时降低了初始成本。典型的例子有 Google Docs、Salesforce CRM、Office Live Workspace 等。

这三种模式都是采用“外包”的理念，将硬件和软件的原始购置、管理维护等高成本的操作外包给云平台，用户只需为使用的服务付出相应的费用。其最终目的都是以最少的成本获取最大的服务。

1.1.3　云计算的分类

云计算的分类多种多样，按需求类型可以分为公有云 (public cloud)、私有云 (private cloud)、混合云 (hybrid cloud) 和互联云 (inter cloud) 等[4] 。

1. 公有云

公有云是运营商以营利为目的搭建的可供给第三方使用的云平台，如 Google、阿里巴巴、腾讯、亚马逊等。第三方用户可以通过互联网使用云服务，但并不拥有云服务。公有云可以通过云计算基础设施的灵活性和可扩展性提供低廉的云服务以吸引用户，降低用户的风险和成本。公有云比私有云大很多，可以根据用户的需求随时进行伸缩，改变大小，并且可以将用户基础设施风险转嫁到云服务提供商身上。

2. 私有云

私有云是相对公有云而言的，它是运营商自己运营并且使用的云平台服务，且仅供内部人员使用。私有云可以是用户使用自己的 IT 设施搭建，也可由云服务提供商搭建，既可以托管在企业数据中心防火墙内，也可托管在一个安全的主托管所内。私有云相对于公有云，它的安全性、服务质量更好，避免了多级用户访问数据造成的数据泄露等安全问题。

3. 混合云

介于公有云和私有云之间的便是混合云，它由多个云端系统组成，其中包括公有云、私有云等，这些云端相互独立但又可通过特殊的技术相互结合。混合云既具备公有云资源丰富的优点，又拥有私有云安全性高的优点，它就相当于将私有云进行扩展，在保证安全性的基础上扩充资源。如果某个企业拥有混合云，那么其便可以将企业中资源信息分为两部分：一部分是要求保密性高，且经常访问处理的资源；另一部分是闲置的资源。那么，企业可以将前一部分的资源存储在私有云上，后一部分存储在公有云中，并通过两者之间的协调互助提供云服务。

4. 互联云

互联云是一种全球性联通的“云中云”，类似于互联网“网中网”的概念，是基于现有云基础设施的一种扩展和延伸，它所提供的服务也类似于移动运营商实现漫游和长途通信的操作。由于现有的每个独立的云都没有无限的物理资源或无处

不在的地理分布，所以当一个独立的云的基础设施无法提供计算和存储资源时，或者它所在的地理位置没有基站时，互联云便能够通过互联网使得每个独立的云可以使用其他云的基础设施提供的资源 (包括计算、存储、甚至是任何类型的资源)，即通过平等互惠的协议让其他独立云的资源为自己所用。更甚者，云交换、云互传、云漫游等互联云所能实现的服务都为云服务提供者引入了新的商机。

1.1.4 移动云计算

互联网典型的终端是计算机，而云计算的发展却不仅仅局限于计算机。近几年，随着移动互联网的蓬勃发展，智能手机等移动业务迅速占领了互联网市场。然而移动终端资源受限的瓶颈 (如有限的计算能力、电池能量受限、连接受限等) 大大制约了移动业务的发展。为解决此问题，基于智能移动终端的云计算服务随之兴起，成为移动云计算的雏形。移动云计算就是指智能终端用户通过移动网络以按需、易扩展的方式获得基于云平台的服务[5](图 1.1)。移动云计算弥补了云计算的不足，实现了云服务的无时不在、无处不在的特点，并且增强了云计算服务对复杂网络的适应性。

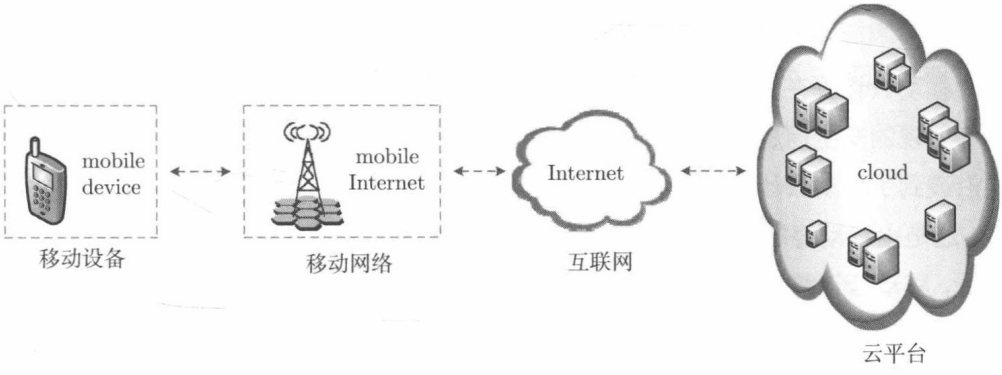

图 1.1 移动云计算

移动云计算可以看成“浓缩版”的云计算。移动终端用户通过互联网共同搭建“临时”云平台，可解决传统云计算受基础设施制约的难题，实现云平台“即用即建”的优势。在某些特定的场景下，移动云计算具有非常重要的应用前景，如某地发生地震、山洪暴发等重大自然灾害时，该地的云计算基础设施遭到了毁灭性的破坏，任何与云计算相关的应用都将无法运行。然而，移动云计算技术可以在此时发挥重要的作用，灾难现场的移动终端用户可以通过与邻近的移动用户临时搭建

一个云平台，将灾难现场的情况拍照记录并传送出去，从而可以迅速地展开救援工作。

移动云计算发展至今已经陆续出现了许多成功的案例，作为云计算的先行者，Google 公司积极开发面向移动环境的 Android 系统平台和终端，实现了传统互联网和移动互联网的信息有机整合，添加了语音搜索服务，提供了定点搜索、Google 手机地图以及 Android 的 Google 街景功能。同样，微软公司推出的“LiveMesh”，以及苹果公司推出的“MobileMe”服务等案例，表明移动云计算的飞速发展。

自移动云计算出现之后，为了让用户能够更加便捷、高效地使用云服务，云服务运营商为用户精心打造了一项智能云服务，称为“微云 (cloudlet)”[6]。通过微云用户可以方便、快捷地在智能终端和云之间进行交互。从某一层面上来说，如果我们将普通的云称为“远程云”，那么“微云”也就相当于“本地云”，即云计算在一个小领域内的应用，如家庭云、企业云、学校云等。微云介于用户和远程云之间，假如用户想用云服务来实现计算任务，那么用户首先用的是微云内的资源，当微云内的资源不足时则调用远程云的资源，如此能够实现高效便捷的服务。

移动云计算在有效地解决各种移动终端资源受限的状况的同时也带来了新的、不容忽视的安全问题。移动云计算是移动计算和云计算的结合，它们的安全威胁同样沿袭到了移动云计算。从某种程度上来讲，移动云计算比云计算更易遭受安全威胁，这是由移动终端的访问位置灵活、访问并发数大等原因造成的。从宏观的角度来看，移动云计算主要面临着以下亟待解决的安全问题。

1. 终端安全

在移动云计算模式下，移动终端是用户使用云计算服务的入口，主要包括智能手机、平板电脑、笔记本等便携式移动设备，移动终端本身的安全将会影响移动云计算的安全。例如，终端通信的安全算法、网络协议存在漏洞、终端操作系统或云应用程序存在漏洞、手机病毒等，这些都会使移动终端易受到各种安全攻击导致用户信息泄露，被攻击者跟踪、窃听、破坏等，更甚者可能导致云端服务器遭到攻击。为解决移动终端的安全问题，首先就要设计适合于移动终端、与时俱进的安全算法和协议，其次需要软硬件的共同保障，最后要增强移动用户的安全意识、养成良好

的使用习惯。

2. 信道安全

移动终端与云端服务器是通过互联网连接的，主要包括 2G/3G/4G 网络、WiFi 无线网络等。网络的复杂性、移动终端的移动性导致一系列的安全问题，主要表现为移动终端的认证问题及数据传输的安全问题。在移动终端接入认证时，攻击者可能阻碍认证或冒充云端服务器窃取用户信息。尤其是在接入未经认证的 WiFi 无线网络时，面临的安全威胁将会更大。为改善这类问题，应当增强用户身份认证或实行匿名认证、采用双向认证技术来保证用户接入时的安全。由于通信信道是公开的、不可信的，在传输时应当对数据进行加密处理，并且为增强安全级别，应使用高强度的加密算法。

3. 云端安全

云端是云计算的资源池，移动云计算的核心，主要是为用户提供云服务。云端安全问题是移动云计算安全的关键，其主要包含基础设施的安全及服务安全。云端的基础设施是移动云计算的资源地，是搭建整个云平台的基柱，无论从云端获取资源还是将资源集中存储到云端，都必须保证基础设施的安全，这样才能保证云端资源的安全。其次，要保证服务的安全。如果服务是不安全的，那么云端服务器可能会拦截移动终端与服务器之间传送的数据或是传送错误的结果到终端。因此，应当在加强数据隐私保护的同时还要增强可验证计算等安全技术。

1.2 云 存 储

云存储是云计算概念上的延伸和发展。云存储系统通过集群功能、分布式文件系统及网格计算等技术将网络中大量的存储设备联合起来协同工作，并通过一定的应用软件或应用接口，对用户提供一定类型的存储服务和访问服务。因此，云存储本质上也是一种 (基础设施) 服务。用户无需了解存储设备的物理位置、型号、容量、接口和传输协议等。

1.2.1 云存储系统结构模型

云存储系统的结构模型主要包括四个部分，即存储层、基础管理层、应用接口层及访问层。

1. 存储层

存储层是云存储最基础的部分。存储设备可以是 FC 光纤存储设备，可以是 IP 存储设备，也可以是 DAS 存储设备。云存储中的存储设备往往数量庞大且分布在不同地域，彼此之间通过广域网、互联网或者 FC 光纤通道网络连接在一起。存储设备之上是一个统一存储设备管理系统，可以实现存储设备的逻辑虚拟化管理、多链路冗余管理，以及硬件设备的状态监控和故障维护。

2. 基础管理层

基础管理层是云存储最核心的部分，也是云存储中最难以实现的部分。基础管理层通过集群、分布式文件系统和网格计算等技术，实现云存储中多个存储设备之间的协同工作，使多个存储设备可以对外提供同一种服务，并提供更大、更强、更好的数据访问性能。

3. 应用接口层

应用接口层是云存储最灵活多变的部分。不同的云存储运营单位可以根据实际业务类型，开发不同的应用服务接口，提供不同的应用服务。如视频监控应用平台、IPTV 和视频点播应用平台、网络硬盘引用平台、远程数据备份应用平台等。

4. 访问层

任何一个授权用户都可以通过标准的公用应用接口来登录云存储系统，享受云存储服务。云存储运营单位不同，云存储提供的访问类型和访问手段也不同。

1.2.2　云平台

自云计算的概念提出之后，全球各大著名的云存储服务提供商争相发展自己的云平台。目前较成熟的云平台包括 Google App Engine[7]、IBM“蓝云”计算平台[3]、亚马逊的 AWS(Amazon Web Services)[8]、微软的 Windows Azure[8] 等。

1. Google App Engine

Google 云的基础构架主要由 MapReduce (分布式计算模型)、GFS(分布式文件系统) 和 BigTable (分布式存储系统) 三个部分构成。2008 年 4 月，Google 提出了一种 Web 应用工具——Google App Engine。它是一种可以让开发者在 Google 的基础构架上免费运行自己的网络应用程序的云平台，并且不需要维护服务器。在