JIYU ANQUAN XIEYI DE
YUNJISUAN PINGTAI SHUJU ANQUAN JI
YINSI BAOHU YANJIU

基于安全协议的云计算平台数据安全及隐私保护研究

陈建辉 著

电子科技大学出版社
University of Electronic Science and Technology of China Press

JIYU ANQUAN XIEYI DE
YUNJISUAN PINGTAI SHUJU ANQUAN JI
YINSI BAOHU YANJIU

基于安全协议的云计算平台数据安全及隐私保护研究

陈建辉 著

电子科技大学出版社
University of Electronic Science and Technology of China Press

图书在版编目(CIP)数据

基于安全协议的云计算平台数据安全及隐私保护研究 / 陈建辉著. -- 成都 : 电子科技大学出版社, 2018.8
ISBN 978-7-5647-6541-5

Ⅰ. ①基… Ⅱ. ①陈… Ⅲ. ①计算机网络—安全技术—研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 164595 号

基于安全协议的云计算平台数据安全及隐私保护研究
陈建辉 著

策划编辑 谭炜麟
责任编辑 谭炜麟

出版发行 电子科技大学出版社
成都市一环路东一段 159 号电子信息产业大厦九楼
邮编 610051
主 页 www.uestcp.com.cn
服务电话 028-83203399
邮购电话 028-83201495

印 刷 河南承创印务有限公司
成品尺寸 145mm×210mm
印 张 6
字 数 167 千字
版 次 2018 年 8 月第一版
印 次 2018 年 8 月第一次印刷
书 号 ISBN 978-7-5647-6541-5
定 价 30.00 元

序　言

天下大势，分久必合，合久必分，计算机网络发展也遵循此发展规律。

计算机初诞生时，都是以大型主机为中心集中进行计算，为共享使用当时较为昂贵的主机资源，不同用户通过分布在不同地理位置的终端与主机联机使用主机计算及软件资源，为第一代集中式“主机－终端”（Host－Terminal）网络计算模式；20 世纪 80 年代个人计算机快速兴起，第一代“主机－终端”网络计算模式中的终端逐步被个人计算机代替，第二代“客户端－服务器”（Client－Server）网络计算模式成为主流，网络计算资源从中心主机逐步转移到了分散的个人计算机上，为第二代分散式网络计算模式；90 年代之后，随着互联网的快速发展，对客户端要求更低、使用更便捷的第三代网络计算模式“浏览器－服务器”（Browser－Server）迅速普及，“浏览器－服务器”模式再次将计算资源和信息资源集中在 Web 服务器端，为典型的集中式网络计算模式；2010 年之后，互联网逐步进入了新的发展阶段，伴随手机、平板电脑、手环、智能家居等智能设备的逐步普及，在移动互联、物联网、大数据等技术的推动下，“云计算”（Cloud Computing）逐步成为第四代网络计算模式，云计算模式是对“浏览器－服务器”模式中集中特性的进一步加强，将计算资源、存储资源、带宽资源、软件资源、数据资源都逐步集中在统一的云平台上，用户通过各类智能终端使用云平台提供的资源及服务。需要指出的是，在集中式“云计算”网络模式逐渐成为主流的当前，以区块链为代表的去中心化网络技术也在迅速发展，分散式个人中心化网络计算模式正在渐进发展。

从第一代到第四代网络计算模式，网络设备数量、用户规模和应用领域呈现数量级增加趋势，网络主流计算平台也经历了大型机、个人计

算机、智能终端设备的计算平台变革，但有一个始终延续不断的主题是“安全”。安全始终是网络和信息安全领域发展面对的焦点问题，更是当今云计算产业发展面对的关键挑战。

从人类社会发展的历程来看，安全是人类生存和发展过程中始终关注、不可忽视的重大命题。人类在不断发展过程中面临着来自人类内部的自我挑战和来自宇宙的外部挑战。随着技术发展和人类对自身及宇宙认识的不断深入，人们发现安全隐患会越来越多，造成的后果也会越来越严重，但同时人类对自身的防护能力也越来越强。世上没有绝对的安全，更没有永恒的安全。我们不能为防范安全问题因噎废食，更不能对安全隐患漠不关心、疏忽大意。

本书针对云计算安全这一主题，首先对云计算技术及云计算安全进行概述，其次对应用安全协议解决拒绝服务攻击问题、云计算环境下的数据安全和隐私保护问题进行探讨与研究，最后针对云计算数据安全给出了几个基本的云计算数据安全模型。

本书得到了航空经济发展河南省协同创新中心、河南省航空物流大数据工程研究中心、多模信息感知河南省工程实验室、郑州航空工业管理学院计算机学院的大力支持，同时受到了河南省基础与前沿技术研究计划项目“云计算环境下数据安全与隐私保护研究”（132300410443）、教育部人文社会科学研究项目“电子商务中的隐私冲突及其协调机制研究”（15YJCZH234）等基金项目的支持，李坤对本书亦有贡献，同时书中引用了大量国内外学者研究成果与公开资料，在此一并表示感谢。需要特别感谢的是我的家人，书稿撰写过程中他们始终给予了我充分的鼓励和足够的支持，谨以此书献给他们！

由于作者水平有限，书中难免存在不足和缺点，敬请各位专家学者批评指正。

陈建辉

2018 年 5 月 20 日

目　录

第1章　云计算基础

20世纪60年代，以大型机为核心的“主机－终端”（Host－Terminal）计算模式成为第一代网络计算模式，20世纪80年代，随着个人计算机的兴起，第二代网络计算模式“客户端－服务器”（Client－Server）逐步成为主流，20世纪90年代，随着互联网的快速发展，第三代网络计算模式“浏览器－服务器”（Browser－Server）迅速普及，2010年之后，互联网逐步进入了新的发展阶段，“云计算”（Cloud Computing）逐步成为第四代网络计算模式。

1.1　概　述

1.1.1　起　源

云计算（Cloud Computing）最早诞生于亚马逊等大型互联网公司处理海量数据的实践，分布式计算（Distributed Computing）、并行计算（Parallel Computing）、效用计算（Utility Computing）、网络存储（Network Storage Technologies）、虚拟化（Virtualization）、负载均衡（Load Balance）、热备份冗余（Hot Backup Redundancy）等，是传统计算机和网络技术发展融合的产物。

2006年3月，亚马逊推出弹性计算云（Elastic Compute Cloud；EC2）服务。2006年8月9日，埃里克·施密特（Eric Schmidt）在搜索引擎大会（SES San Jose，2006）首次提出“云计算”的概念。

1.1.2 定 义

云计算是基于互联网相关服务的增加、使用和交付模式，通过互联网来提供动态易扩展且经常是虚拟化的资源。由于云计算尚处于起步阶段，主要是应用场景的变化和实现技术的发展，所以云计算并没有一个统一的定义。

云计算研究学者刘鹏教授在其著作《云计算》(第三版)中对云计算做了长、短两种定义。长的定义是："云计算是一种商业计算模型，它将计算任务分布在大量计算机构成的资源池上，使各种应用系统能够根据需要获取计算力、存储空间和信息服务。"短的定义是："云计算是通过网络按需提高可动态伸缩的廉价计算机服务。"

目前另外一个被广泛熟知的是美国国家标准与技术研究院(National Institute of Standards and Technology，NIST)2009 年关于云计算的定义："云计算是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问，进入可配置的计算资源共享池(资源包括网络、服务器、存储、应用软件、服务等)，这些资源能够被快速提供，只需投入很少的管理工作，或与服务供应商进行很少的交互。"

1.1.3 特 点

云计算技术一般具有以下特点：

(1)超大规模。云计算平台面向大量用户提供服务，要求具有相当的规模。Amazon、IBM、微软、阿里等大型 IT 企业云计算平台均拥有几十万台甚至上百万台服务器。国内外大型银行、证券、石油等非 IT 企业建立的内部私有云一般也拥有成千上万台服务器。

(2)虚拟化。云计算平台将大量存储、计算资源虚拟化为统一管理

的资源池，并根据用户需求分配不同单位虚拟资源给用户使用。云计算技术支持用户在任意位置、使用各种终端获取网络应用服务。用户所请求的资源来自云计算平台，应用在云计算平台上运行，但用户无须了解应用运行的具体设备及位置。

(3)高可靠性。云计算平台采用数据中心建设技术，除了高可靠性物理设备和保障管理措施外，数据中心内部和不同数据中心之间采用容错备份、容灾备份等措施来保障服务的高可靠性，提供比本地计算机更高的可靠性。

(4)通用性。云计算平台针对不同用户需求，提供从基础硬件设施、系统软件平台到应用软件服务等不同层次的云计算服务，满足不同用户的不同的应用需求。

(5)弹性化。对于云计算平台本身而言，其规模可以随着发展动态伸缩，满足规模增长的需要。对于用户而言，可以根据自身资源需求量随时按需租用适量资源，不但可以大大缩短购买和建设周期，同时根据需求动态租用资源，既不会造成资源过多的浪费，也不会因资源不足而不能满足业务需求。

(6)成本低廉。大型 IT 企业建立的公共云计算平台具有良好的规模效益，大规模集中式自动化管理的云计算平台构建模式下，不但使用户企业无须负担日益高昂的数据中心建设管理成本，而且云计算平台的集中性、通用性使资源的利用率较之传统系统有大幅度的提升，建设周期和成本仅为原来的几十分之一。

云计算平台和技术的快速发展给社会、企业和个人带来了极大的便利，但也不可避免地存在数据和隐私泄露风险增大的情况，需要进一步研究解决。

1.2　云计算模型

除了云计算的概念定义外，美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）所定义的云计算模型也得到了业界的广泛认可，模型示意如图 1.1 所示，主要包括了云计算的五个基本特征、三种云计算服务模式以及四种云计算部署方式。

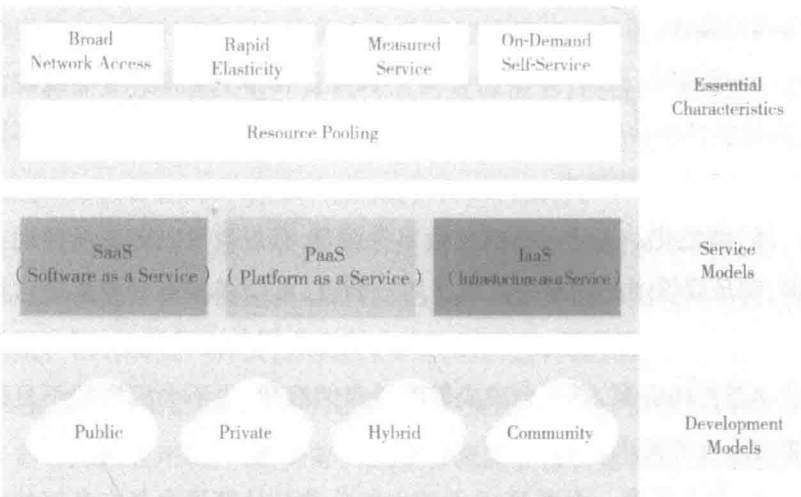

图 1.1　NIST 云计算模型

1.2.1　云计算基本特征

如果具备以下特征，就可以把它看作云计算。如果缺少其中任何一个，则很可能不是云计算。

（1）独立划分的资源池。资源池是最根本的特性，所有的云计算提供商都会把资源集中起来，然后抽象到一个池中，以特定的策略分配给不同的用户使用。

资源服务者以多租户的模式为用户提供服务，根据消费者的需求

动态分配或重分配不同的物理和虚拟资源。就像使用本地独立资源一样，用户通常并不控制或了解这些资源池的确切位置，但能够在较高的抽象层面指定资源的位置（例如国家、地区或数据中心层面）。资源的例子包括存储、计算、内存和网络带宽等。

（2）快速弹性服务。云计算平台提供弹性供给或释放资源的能力，用户可以根据需要快速地增加或缩小资源规模，有时也可以自动完成。对于消费者来说，感觉资源是无限的，能够随时使用任何数量资源。

快速弹性服务是仅次于资源池的第二重要特征，一方面能够保证云计算服务平台及时响应用户的资源需求，另一方面也可以提高有大量用户使用的云计算平台的资源使用效率。

（3）可计量服务。云系统通过在某种程度上适当抽象级别（例如，存储、处理、带宽和活跃用户账户）的度量能力自动控制和优化资源的使用。资源使用可以被监控、控制和报告，服务提供者和使用者都透明地使用服务。

可计量服务确保用户只使用他们所分配的东西，如果有必要的话，还可以对他们收取费用。这就是“效用计算”这个术语的由来，因为资源可以像水和电一样被消耗，客户只需要支付他们所使用的东西。可计量服务是云计算服务商业化应用的基础。

（4）广泛的网络访问。基于网络和标准访问机制提供服务，用户可以使用异构的瘦或胖客户端（如移动电话、平板电脑、笔记本电脑和工作站）。

云计算平台应具有较好的通用性，不对访问终端的硬件和操作系统进行限制。

（5）按需自助服务。消费者可以单方面获取计算能力，如服务器时间和网络存储等，无须与每个服务提供者进行人工交互就可以根据需要自动完成。

按需自助服务将服务流程自动化，避免人工介入，最大限度地缩短了响应时间，提高了服务效率。

1.2.2 云计算服务模式

美国国家标准与技术研究院(NIST)制定了一套广泛采用的术语用于描述云计算的各方面内容。NIST 针对云计算服务定义了三大服务模式，称为 S-P-I 模式：软件即服务(software as a service，SaaS)，即将整个商业应用作为一项服务来提供；平台即服务(platform as a service，PaaS)，允许在云平台上进行快速应用开发；基础设施即服务(infrastructure as a service，IaaS)，即将计算资源(CPU)、储存资源和带宽作为一项服务来提供。

(1)SaaS。SaaS 模式下，云服务商向用户提供的是运行在云基础设施之上的应用软件。用户不需要购买、开发软件，可利用不同设备上的客户端(如 WEB 浏览器)或程序接口通过网络访问和使用云服务商提供的应用软件。用户通常不能管理或控制支撑应用软件运行的低层资源，如网络、服务器、操作系统、存储等，但可对应用软件进行有限的配置管理。

SaaS 模式将运行在云平台上的软件进行封装，并提供应用程序访问的接口，满足特定的需求。比如全球按需 CRM 解决方案的领导者 Salesforce，创建于 1999 年 3 月，可提供随需应用的客户关系管理平台。Salesforce 允许客户与独立软件供应商定制并整合其产品，同时建立他们各自所需的应用软件。

Salesforce.com 提供按需定制的软件服务，用户每个月需要支付类似租金的费用来使用网站上的各种服务，这些服务涉及客户关系管理的各个方面，从普通的联系人管理、产品目录到订单管理、机会管理、销售管理等。所有的记录和数据都储存在 Salesforce.com 上面，用户随时

可以根据需要增加新的功能或者去除一些不必要的功能，真正地实时按需使用。对于用户而言，还可以避免购买硬件、开发软件等前期投资以及复杂的后台管理问题。

另外，比如在线地图、在线文字处理软件及网盘等各类应用。这类应用的特点都是有较大的数据计算或者存储要求，而用户端设备的计算和存储能力性能较弱。因此用户端使用“云”端的访问接口将计算的任务放在“云”端进行，而用户端仅使用网络获得计算的结果。并且用户可以根据自己的需求来按次数或者流量使用此类服务，而不必一次性购置所有的软件及数据资源。

(2) PaaS。PaaS 模式下，云服务商向用户提供的是运行在云计算基础设施之上的软件开发和运行平台，如标准语言与工具、数据访问、通用接口等。用户可利用该平台开发和部署自己的软件。用户通常不能管理或控制支撑平台运行所需的低层资源，如网络、服务器、操作系统、存储等，但可对应用的运行环境进行配置，控制自己部署的应用。

PaaS 实际上是指将软件研发的平台作为一种服务，它是基于特定平台的服务，该平台提供的是比应用软件具有更强通用性的、支持各类应用的虚拟化的软件运行平台。基本的软件平台包括操作系统、数据库、网络服务管理及中间件等。通常这个平台附带有开发环境，供“云计算”的使用者直接在平台上进行开发，并在该平台上运行应用。应用的开发者仅按照平台的使用说明和编程接口使用该平台即可，而不用关注平台所存在的环境。

以国外某 G 公司为例其 PaaS 向用户提供了 Python 开发语言，并提供该公司的云计算 API 接口，用户可以直接使用其强大的基础设施和软硬件环境，按照用户应用所耗费的网络流量和其他物理资源来收费。

(3) IaaS。在 IaaS 模式下，云服务商向用户提供虚拟计算、存储、网络等资源，提供访问云计算基础设施的服务接口，用户通过互联网可以

获得完善的基础设施服务。客户可在这些资源上部署或运行操作系统、中间件、数据库和应用软件等。用户通常不能管理或控制云计算基础设施,但能控制自己部署的操作系统、存储和应用,也能部分控制使用的网络组件,如主机防火墙。

IaaS 处于三大服务模式的最底层,通过特定的虚拟化软件将服务器的计算资源、存储资源和网络的传输能力等基础资源进行封装,然后通过统一的访问接口向用户提供这种资源的访问。用户可以根据自己的实际需求定制并购买相应资源的使用权。

当前,Amazon、微软、阿里、华为等众多 IT 公司提供这种云计算服务。用户根据自己的应用定制所需要的资源的数量,例如 CPU 的处理性能、内存的大小、硬盘的大小、带宽的大小等,用户可以在云平台上运行需要的操作系统、软件和服务平台,如同使用一台真实的计算机,通过这种方式用户可以高度定制化自己的应用。IaaS 将虚拟资源进行相互隔离,不同的用户彼此之间互不影响。

云计算三种交付模式的关系如表 1.1 所示。

表 1.1　云计算三种交付模式

<table>
<tr><td colspan="3">应用 SaaS</td></tr>
<tr><td colspan="3">平台 PaaS</td></tr>
<tr><td colspan="3">基础设施 IaaS</td></tr>
<tr><td colspan="3">虚拟管理层</td></tr>
<tr><td>物理服务器</td><td>物理存储</td><td>物理带宽</td></tr>
</table>

从技术角度来看,PaaS 连接 IaaS 和 SaaS,是对底部 IaaS 的再次包装,进而提供更好的运行平台来支持各种 SaaS 应用。IaaS、PaaS 和 SaaS 这三种模式都是采用了 IT 外包的方式,以减轻企业负担,降低管理、维护服务器硬件、网络硬件、基础架构软件和应用软件的人力成本。

1.2.3　云计算部署方式

NIST 定义了云计算的四种部署方式：私有云、公有云、社区云和混合云。

(1)私有云。云计算平台仅提供给某个特定的用户使用。私有云的云计算基础设施可由云服务商拥有、管理和运营，这种私有云称为外部私有云或外包私有云；也可由用户自己建设、管理和运营，这种私有云称为内部私有云或自有私有云。

私有云的部署比较适合于有众多分支机构的大型企业或政府部门。相对于公共云，私有云部署在企业内部，因此其数据安全性、系统可用性都可由自己控制。但其缺点是投资较大，尤其是一次性的建设投资较大。

(2)公有云。公有云的云计算基础设施由云服务商拥有、管理和运营，为外部客户提供服务，云计算平台的用户范围没有限制。典型的公有云包括亚马逊 AWS、微软 Azure、阿里云、腾讯云等。

对于使用者而言，其所应用的程序、服务及相关数据都存放在公共云的提供者处，自己无须做相应的投资和建设。存在的问题是，由于数据不存储在自己的数据中心，其安全性存在一定的风险。同时，公共云的可用性不受使用者控制，这方面也存在一定的不确定性。

(3)社区云。云计算平台限定为特定的用户群体使用，群体中的用户具有共同的属性(如职能、安全需求、策略等)。社区云的云计算基础设施可由云服务商拥有、管理和运营，这种社区云称外部社区云；也可以由群体中的部分用户自己建设、管理和运营，这种社区云称为内部社区云。

(4)混合云。上述两种或两种以上部署方式的组合称为混合云。相比较而言，混合云的部署方式对提供者的要求较高。

目前公有云发展迅速，一些中小企业也已经把自己原来的业务迁移到公有云上，不再扩容自己原来的 IT 基础设施。一些新公司则一开始便租用公有云计算服务，不用担心 IT 基础设施的建设问题。出于数据安全保密等诸多因素的考虑，大型企业较多建设私有云或混合云。社区云则适用于具有合作或联盟关系的机构企业，比如某城市的智能交通云平台或教育云平台等。

1.3 云计算架构

云计算技术大规模商业应用的引领者如亚马逊，该公司为支撑自身业务建立了庞大的 IT 基础设施，推出云计算服务的初衷只是为充分利用内部 IT 资源。与电子商务业务起家的亚马逊主要提供基础设施服务不同，微软是在看到云计算的发展趋势后携带原有操作系统和开发平台优势进入云计算领域提供平台服务，国内云计算的代表者阿里云的发展历程则与亚马逊类似。

1.3.1 某 G 公司云计算架构

该公司较早使用了云计算，也是云计算技术的行业引领者。其众多应用就是建立在其“云”上的，例如该公司搜索引擎就是建立在“云”上。其采用较为廉价的个人计算机硬件而非专业服务器硬件构建服务器集群来搭建数据中心。数据中心往往建立在电费较低、冷却成本低、地广人稀的位置，这样整体的运营成本能够大幅度降低，而且便于管理。当前该公司的“云”拥有超过千万的服务器，而且服务器的数量还在不断地增加。利用云的强大计算存储能力，该公司向很多用户提供了 SaaS 的云计算服务，用户在一些处理能力很弱的终端（比如手机、平板电脑）能便捷使用以上提供的服务。