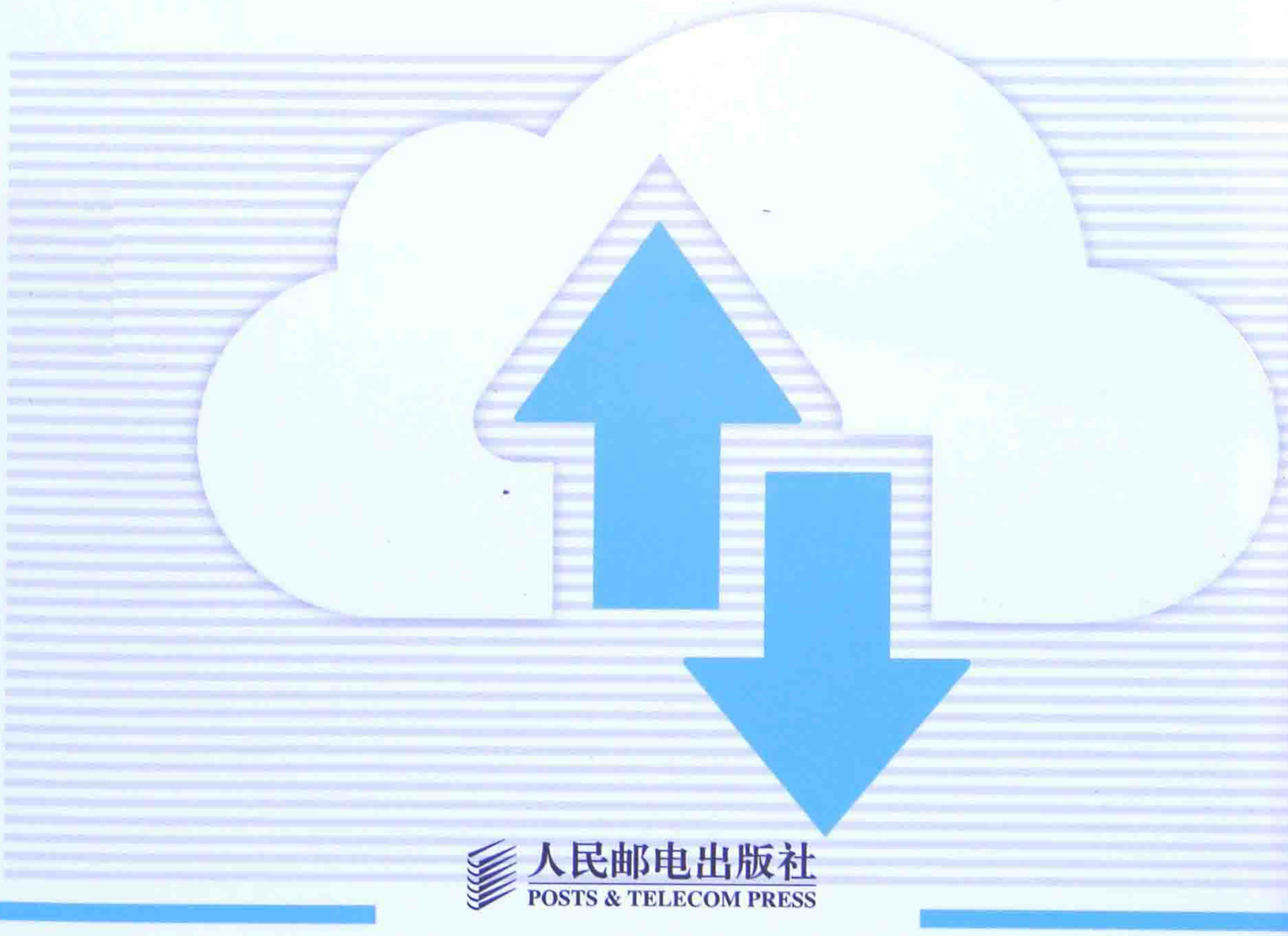
Innovative Research

中国联通研究院创新研究系列丛书

云计算安全技术与应用

张尼 刘镝 张云勇 李正 陈豪 等 编著



人民邮电出版社
POSTS & TELECOM PRESS

目 录

Contents

第1章 Chapter 1

云计算概述

自云计算（cloud computing）的概念提出以来，在市场、技术和政策等因素的驱动下，云计算以令人诧异的发展速度，逐渐走向了成熟，并将成为 ICT 行业未来发展的一个重要方向。云计算弹性调度、资源共享、服务可扩展、按需分配 4 大特性及公有云、私有云、混合云 3 大部署方式已经彻底改变了人们的生产生活。在讨论云安全之前，为了使读者更好地了解云计算本质，为更加深刻地理解云安全做好铺垫。本章介绍了云计算的基本知识。回顾云计算的发展背景，梳理云计算的定义与特征，描述云计算的部署方式与行业应用，并总结云产业带来的机遇与挑战。

1.1 云计算发展背景

21 世纪以来，云计算逐渐兴起，Amazon、Sun、IBM、Google 等公司纷纷宣布云计算计划，并在云计算的商业应用方面走在了世界前列。2008 年以来，在经济危机的刺激下，全球企业努力寻求节省成本、降低开支的良方妙计。云计算的理念和模式满足了当下 IT 服务提供者和服务使用者的主要需求。对于服务提供者，云计算满足了其对 IT 资源的高效管理需求，并利于其开拓新的业务和商业模式；

对于服务使用者，可以按需获取 IT 资源，节省开支、降低企业运行成本。

云计算从提出概念，到逐渐成熟，再到现在这样达到比较成熟的水平，依次经历了 4 个阶段：电厂模式、效用计算、网格计算（grid computing）和云计算。

1）电厂模式阶段。每当一个新的行业诞生时，发展的捷径就是利用其他行业的成功模式，而电厂模式对 IT 行业影响比较深远。电厂模式利用了规模经济的效应，不但降低了电力的价格，而且既不需要用户购买任何发电设备，也不需要用户具备任何的知识和能力去维护设备，使得用户使用电力更加方便。

2）效用计算阶段。在 1960 年左右，由于当时的计算机设备非常昂贵，以至于大多数普通的企业、机构和学校根本负担不起相关费用，一些 IT 人士萌生了共享计算机资源的想法。1961 年，人工智能之父、麻省理工大学教授约翰麦肯锡在一次会议中提出了效用计算的概念，其核心是借鉴了电厂模式，目标是将分散在各地的服务器、存储系统整合在一起，供所有用户使用，减轻独立用户对计算机设备的高额投入，使用户享受到即插即用的计算机资源，并且根据其使用量付费。但由于当时 IT 行业的发展才刚刚起步，很多关键技术还没有诞生，如互联网等，而且在计算或存储方面的需求也远远没有现在这么强烈，所以虽然想法很先进，但由于当时种种社会条件的限制，并没有实现。

3）网格计算阶段。随着计算机的普及，越来越多的计算机被人们使用，但人们对计算机 CPU 的利用率却远远达不到计算机的潜能，造成资源和能源的浪费，而互联网的出现使网格计算成为了现实。网格计算的主旨是研究如何把一个需要非常巨大的计算能力才能解决的问题分成若干小部分，再把这些部分分配给计算机网络中的若干低性能计算机来处理，最后把这些计算结果综合起来完成复杂问题的计算。但是由于在商业模式、技术和安全性方面还存在很多不足，使得其并没有在工程界和商业界取得预期的成功。

4）云计算阶段。云计算是从效用计算与网格计算发展过来的，它希望 IT 技术能够像使用电力那样方便，并且成本低廉。但是不同点在于需求方面已经有了一定规模，同时在技术方面也基本成熟。因此，云计算相比效用计算和网格计算已经具备可以发展的基础，使其更为脚踏实地。

回望云计算的发展历程，其驱动力主要来自以下 3 个方面。

1）需求驱动。随着经济、社会信息化的大发展，尤其是移动互联网和物联网应用的兴起，海量信息处理的需求激增；同时，现代应用需要满足普适化、智能化等一系列要求。因此，从客观上需要云计算技术来满足上述需求。

2）技术驱动。宽带通信与互联网技术、分布式计算、分布式数据库的快速发展，推动了虚拟化和分布式处理技术的发展，为云计算发展奠定了技术基础。

3）经济与环境保护驱动。经济危机与哥本哈根国际气候大会推动了全球产业升级、调整和节能减排时代的快速到来。由于云计算具有低成本、高效能、绿色环保等特点，因而受到各国政府的重视。

以上 3 种驱动力极大地推动了传统技术发展融合，最终演进为云计算，其涉及网格计算、分布式计算（distributed computing）、并行计算（parallel computing）、效用计算（utility computing）、网络存储技术（network storage technologies）、虚拟化（virtualization）、负载均衡（load balance）等传统技术。也就是说，云计算是传统技术发展融合的产物。

总之，云计算是 ICT 产业的一个重大变革，如同当初的电力革命和通信网的变革。100 多年前，在没有电力公用设施时，每个农场和企业都用各自的发电机单独发电，生产及维护的成本很高；电网建成后，农场和企业改为从大型的发电厂购买价格低廉、可靠性高的电力。在过去，企业或部门多采取自建电信专用网的方式。然而，随着通信技术的发展，公用电信网的通信质量和效率得到极大提

升，运营成本不断下降，新兴企业或部门转而采用公众网来实现专用网功能，原有的专用通信网也逐渐淡出电信市场。同样，当云计算服务承诺的通用访问、7×24 h 的可靠性、高安全可信性、99.999%的 SLA（service level agreement，服务等级协议）和无处不在的协作真正兑现时，今日主流的以企业或个人私有 IT 资源为中心的计算方式注定走向没落，云计算服务必将在后电信时代的 IT 产业大行其道。

然而，云计算的意义不仅限于此，其意义还在于：① 促进业务创新，云计算使得企业更专注于业务，更快、更灵活地满足和交付客户需求，为业务创新提供坚实且灵活的支撑；② 增加业务收益，云计算具有显著的网络经济特征，随着服务增加，边际成本递减，边际收益递增，总体实现收入递增。

1.2 云计算定义

由于云计算涉及技术的多个方面和产业发展的多个环节，不同的组织和企业从各自的角度给出了云计算的定义。维基百科认为：“云计算是一种将规模可动态扩展的虚拟化资源通过 Internet 提供对外按需使用服务的计算模式，用户无需了解提供这种服务的底层基础设施，也无需去拥有和控制。云形象地代表了 Internet 网络，即提供服务的基础设施。”美国国家标准技术研究所（NIST）提出的云计算的定义为：“云计算模型能以按需方式，通过网络方便地访问云系统中可配置的计算资源共享池（如网络、服务器、存储、应用程序和服务）”。同时它以最少的管理开销及最少地与供应商的交互，迅速配置、获取或释放资源。中国云计算专家委员会的专家认为：“云计算是一种新兴的商业计算模型。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、存储空间和各种软件服务。”

本书认为：“云计算”是一种新的计算方法和商业模式。通过虚拟化等技术按

照“即插即用”的方式，自助管理运算、存储等资源能力形成高效资源池，以按需分配的服务形式提供计算能力；且可通过公众通信网络整合 IT 资源和业务，向用户提供新型的业务产品和新的交付模式。

云计算作为一种技术手段和实现模式，使得计算资源成为向大众提供服务的社会基础设施，将对信息技术本身及其应用产生深远影响，软件工程方法、网络和终端设备的资源配置、获取信息和知识的方式等，无不因云计算而产生重要变化。与此同时，云计算也深刻改变着信息产业现有业态，催生了新型的产业和服务。云计算带来社会计算资源利用率的提高和计算资源获得的便利性，推动以互联网为基础的物联网迅速发展，将更加有效地提升人类感知世界、认识世界的能力，促进经济发展和社会进步。

1.3　云计算特征

云计算具备以下几种特征，包括资源共享、弹性调度、服务可扩展与按需分配。

（1）资源共享

云计算业务向云用户提供了对计算、存储、网络、软件等多种 IT 基础设施资源租用的服务，而用户不需要自己拥有和维护这些基础设施资源。

（2）弹性调度

云用户能够按需获得和调用 IT 基础设施资源，也能够按需撤销和缩减资源。云计算平台可以按云用户的需求快速部署和调度资源。

（3）服务可扩展

云计算可以根据用户的规模、使用量、需求增加云中相应的资源，使得资源的规模可以根据需要扩大，满足应用和用户规模变化的需要。

（4）按需分配

用户按需使用云中的资源，按实际的使用量付费。云计算能够兼容不同硬件厂商的产品，从而保护云业务提供商的原有投资。另外，由于云的特殊容错措施，可采用大量廉价设备来构建云，降低成本。

1.4 云计算的服务类型

云计算按服务类型大致可以分为 3 类：基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS），如图 1-1 所示。

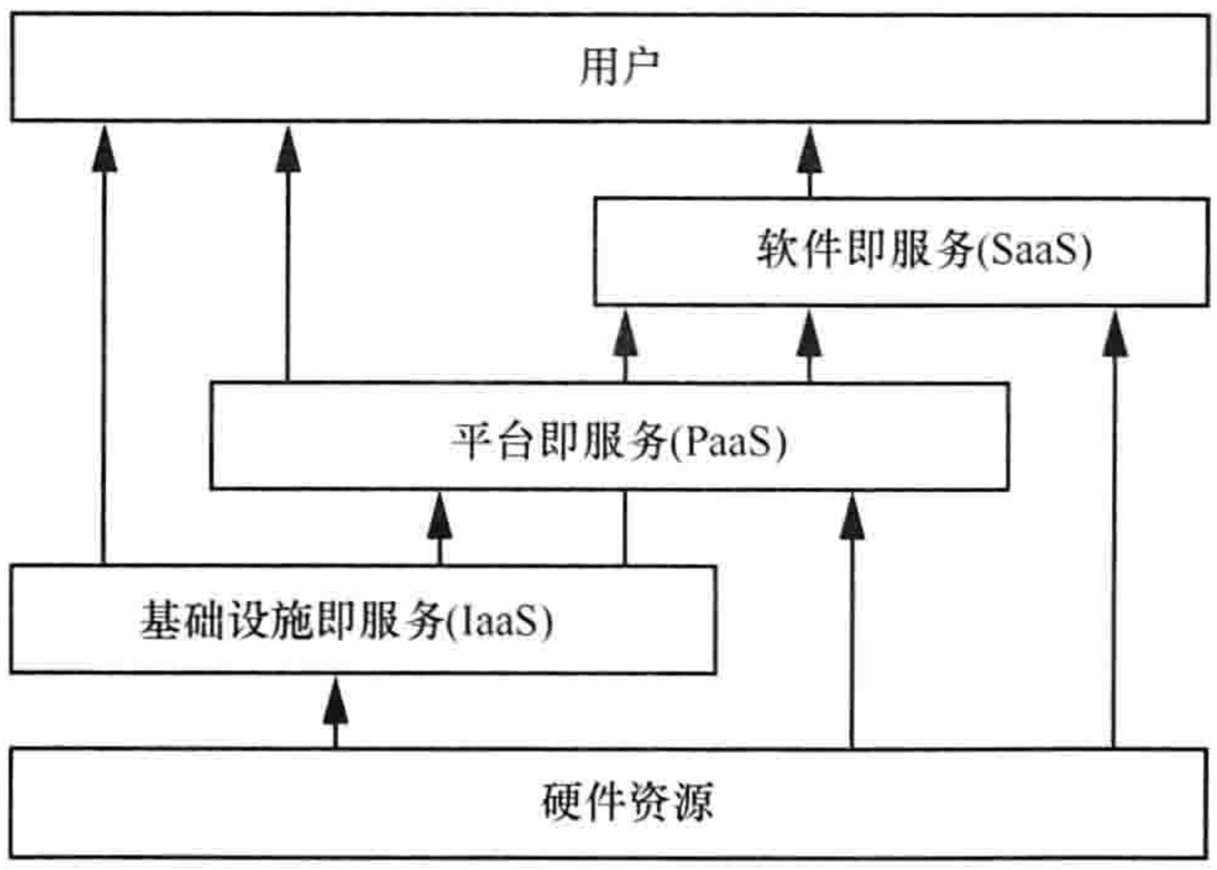


图 1-1 云计算业务模式

1）基础设施即服务位于 3 种服务类型的最底端，也是最基础的、最接近云计算基本定义的服务。云业务提供商把多台服务器组成的“云”基础设施作为服务租给用户，可以根据用户的购买量或实际使用量计费。它提供给用户计算、存储、网络及其他基础设施资源，使得用户在基础设施上配置和运行操作系统、应用软件等。用户不需要管理或者控制云的基础设施，只需要支配操作系统、存储、部署应用程序和有限地选择网络组件，例如主机防火墙等。具有代表性的公司及业务有 Amazon 的 EC2 和 Verizon 的 Terremark 等。

Amazon 有大量的 IT 资源和存储资源闲置，为了充分利用闲置的 IT 资源，Amazon 将弹性计算云对外提供效能计算和存储租用服务，包括存储空间、带宽、CPU 资源。Amazon 对存储空间、带宽按容量收费，CPU 根据运算量时长收费。例如，弹性计算云 EC2 让用户自行选择服务器配置来按需付费计算机处理任务；每个月 10 亿字节 S3 存储服务收费 15 美分。由于是按需付费，比企业自己部署 IT 硬件资源及软件资源更为便宜。因此，Amazon 成为了成功的 IaaS 服务商之一。

AT&T 提供使用量付费的公用运算服务，供企业弹性使用 IT 资源并能够随时取得所需的计算、处理和储存能力。

NTTDoCoMo 与 OpSource 合作推出了基于安全的数据中心及可靠的可扩展网络的云计算解决方案，利用公有云为用户提供虚拟化私有云，使用户在虚拟化私有环境中完成计算和应用服务，可实现在线购买，目前提供按小时计费的模式。

2）平台即服务位于 3 种服务类型的中间层，是经过云业务提供商封装的 IT 资源，通常按照用户或用户登录情况计费。它提供给用户编程语言环境，把用户创建或购得的应用程序部署在云基础设施之上，提供应用从创建到运行整个生命周期的软硬件资源环境和工具。用户不需要管理或控制包括网络、服务器、操作系统、存储等云基础设施，仅需支配部署的应用和应用程序主机环境的配置。以下是具有代表性的 PaaS 案例。

Google 的云计算平台主要采用 PaaS 商业模式，提供云计算服务按需收费。Google APP Engine 根据中央处理器租用情况收费，大约每个 CPU 核每小时收费 10~12 美元，存储方面每 10 亿字节存储空间收费 15~18 美元。

Salesforce 的 PaaS 平台 Force.com 运行在 Internet 上，采用以登录次数为基础的完全即时请求收费模式。独立软件提供商作为其平台的客户，开发出基于他们平台的多种 SaaS 应用，使其成为多元化软件服务供货商（multi-application

vendor），扩展其业务范围。

3）软件即服务位于 3 种服务类型的最顶端，它可以使用户在不使用客户端的情况下，通过 Web 浏览器享受基于网络的软件服务，并以免费或按需付费的方式向用户提供服务。SaaS 为用户提供运行在云基础设施上的应用程序。这些应用程序在各种终端设备上均能运行，通过 Web 浏览器或瘦客户端访问应用，用户不需要管理或者控制云基础设施。具有代表性的公司及业务有：阿里云软件、Saleforces、Microsoft 的邮件等。

阿里云软件向中小企业用户提供“先尝试后购买，用多少付多少，无需安装，即插即用”的软件服务，以实现低成本在线软件模式，可根据行业、区域为中小企业提供定制服务。

Salesforce.com 让客户透过云端执行商业服务，而不用购买或部署软件，并按照订户数和使用时间对企业进行收费。

微软提供公有云的 SaaS 应用服务，同时向个人消费者和企业客户提供 SaaS 云服务。例如，微软向用户提供的 Online Services 和 Windows Live 等服务均属于 SaaS 服务。

1.5 云计算部署方式

根据服务面向的对象，云计算系统的部署方式可分为 3 类：公有云、私有云和混合云，下面将逐一介绍。

（1）公有云

公有云是由云业务提供商构建并所有，部署在公司内部的安全域内，通过外部接口与外界公共互联网、移动互联网相连接，向外部用户（公众或某个很大的业界群组）提供云服务或提供对外开放能力等。公有云所有业务供外界用户使用，

用户只需为公有云提供业务资源付费即可。云用户所使用的程序、服务及相关数据都存放在公有云中，自己无需做相关投资和建设。云业务供应商负责为软件、应用程序基础架构、物理硬件基础设施的安装、管理、供给和维护。公有云的缺点是在提供业务时可能会跨越国界，触及国家或地区安全法规合规性问题，从而限制其业务正常开展。公有云代表实例如下。

亚马逊的 AWS 产品线是最具代表性且用户数量最多的公有云之一，它以提供 IaaS 服务为主，提供 S3（一种简单的存储服务）、EC2（弹性可扩展的云计算服务器）、Simple Queuing Service（一种简单的消息队列）及仍处在测试阶段的 Simple DB（简单的数据库管理）等多种云计算服务。S3 可以提供无限制的存储空间，让用户存放文档、照片、视频和其他数据。使用 EC2 服务的用户可以选择不同的服务器配置，对实际用到的计算处理量进行付费。

（2）私有云

私有云是由云业务提供商（企业或某个组织）构建并所有，部署在自身内部安全域内、专供企业内部人员或系统内分支机构使用的云架构体系，其所有服务均不提供给外部用户使用。私有云的基础设施是专为企业或组织内部为实现内部业务所设计的，由企业自身负责配置、运维、托管、管理等任务，可以提供场内服务（on-premises），也可以提供场外服务（off-premises）。

私有云的部署比较适合具备众多分支机构的大型企业或政府部门。私有云的一大特点就是具备细粒度的资源可控性、安全性。随着这些大型企业数据中心的集中化，私有云将会成为 IT 部署系统的主流模式。根据 2012 中国云安全调查结果，发现目前已有 22.8%的受访用户正在使用私有云，另有 50%的用户考虑使用私有云，两者之和达到了七成以上，私有云成为此次调查中用户最认可且安全的云模式。私有云的缺点是其持续运营成本可能会超出使用公共云的成本。私有云

代表实例如下。

私有云目前的发展趋势是集合硬件、软件和服务于一体的整体解决方案，IBM推出的“蓝云”计算平台就是其中之一，它为客户带来即买即用的云计算服务。IBM 的“蓝云”计算平台是一套软、硬件平台，将 Internet 上使用的技术扩展到企业平台上，使得数据中心使用类似于互联网的计算环境。“蓝云”大量使用了IBM 的大规模计算技术，结合 IBM 自身的软、硬件系统及服务技术，支持开放标准与开放源代码软件。

（3）混合云

根据美国国家标准技术研究所（NIST）SP 800-145 中的定义，混合云是“两个或两个以上保持各自实体独立性的不同云基础设施（私有云或公共云）形成的一个组合，该组合采用的标准或专用技术可实现数据和应用程序的可移植性。”混合云是公共云和私有云的混合。实际上，它是公有云与私有云之间的一个妥协产物，可提供各种最佳特性。例如，公有云聚集资源的灵活性和可用性，以及私有云的定制服务与内部安全性。

混合云一般由企业创建，而管理职责由企业和云服务提供商共同分担。混合云既提供公共互联网对外服务，又提供企业内部服务。当企业或机构需要同时使用公、私有云服务时，混合云是一种较为理想的方案。混合云可以为某些关键业务流程（如接收客户支付）及辅助业务流程（如员工工资单流程）提供服务。混合云的主要缺陷是很难有效创建和管理此类解决方案，公有和私有云组件之间的交互会使实际部署更为复杂。由于这是云计算中一个相对新颖的体系结构概念，在未了解清楚其架构体系之前，一般企业、机构都不太愿意采用此种云部署方式。混合云代表实例如下。

NetApp 和 Amazon Web Services（AWS）的组合即为混合云的一个典型实例。

其中，AWS 的 NetApp Private Storage 可让企业构建一个平衡专用资源和云资源的云基础设施。

1.6　云计算行业应用

近几年来，云计算的概念被越来越多的人所熟悉，云计算的应用领域也越来越广泛，云计算已成为当前信息技术领域的热门话题之一。它体现了“网络就是计算机”的思想，将大量计算资源、存储资源与软件资源链接在一起，形成巨大规模的共享虚拟 IT 资源池。基于云计算的 IT 基础设施建设模式为产业带来了节省成本、拓展应用及更加充分利用资源的全新思路，推动了 IT 产业向绿色环保和资源节约型方向发展，这符合产业发展中控制成本、节省资源、减少排放、保护环境等多方面的需求趋势。云计算也为涉及 IT 服务、互联网和移动互联网的多种应用行业开拓了全新的商业模式和建设思路，成为信息服务业发展的重要方向。

（1）政府及公共事业

政府行业将云计算技术逐步转化为实际应用，一方面是面向政府工作人员，成为政府办公、计算平台的“政务云”，另一方面是面向普通公众，成为“公共服务云”。

具体而言，“政务云”是政务信息化和业务协同的平台，可提供统一政府电子邮件、数据的存储处理、城市应急指挥、人口管理、城市减灾和风险管理、食品安全等多种政务功能。下面举一个电子政务云实例：2011 年，北京市海淀区信息办主导的海淀区电子政务网络系统信息安全工程全面启动，该项目通过采用集中部署分布式服务的 IaaS“云安全”服务模式，在海淀区电子政务网络系统中加装部署 20 台基于全程全网协同管控管理模式的 CTM 设备，以面向接入层的云安全服务的方式实现对海淀区重点政务网络中的信息事无巨细地 24 h 全过程录像，落

实全面监测和感知网络威胁和违法违规实时发现预警、安全事件事后追查的网络秩序化管理手段和措施，避免了传统上基于已知特征“被动防御”式的网络安全防御的局限性。

“公共服务云”可面向公众提供统一税收、缴费、信息发布、意见征询等涉及民生的多种服务。下面举一个“公共服务云”的实例：2012 年，北京市海淀区启动了社会组织公共服务“云平台”建设项目，并开展意见征集和需求调研工作。“公共服务云平台”通过云计算及网络技术，实现海淀区社会组织的信息展示、项目征集与管理、行业信息共享等，实现社会组织的资源整合，使社会组织中的人、财、物都得到切实合理的利用，发挥其最大的效能，真正做到资源共享服务于社会、政府服务与管理社会组织并举。

由于政府云计算中心可提供对海量数据存储、分享、挖掘、搜索、分析和服务的能力，使得数据能够作为无形资产进行统一有效的管理，通过对数据集成和融合技术，打破政府部门间的数据堡垒，实现部门间的信息共享和业务协同。“政务云”和“公共服务云”将极大地提高政府信息化水平和办公效率，并大幅节约政府 IT 建设开支，实现绿色办公。

（2）制造业：云计算发力制造业运营模式创新

面向制造业的专业服务运营商将提供基于 PaaS、SaaS 模式的软件开发和服务，为制造业企业提供包括产品、技术、平台和运维管理在内的全面支持，使制造业企业将更多的精力放在制造的业务层面上，而非 IT 基础设施的建设与运维。在 PaaS 模式下，用户首先采用云计算运营商支持的编程语言和工具编写相应的应用程序，然后放到云计算平台上运行；在 SaaS 模式下，用户既可以获得低廉的 ERP、CRM 等企业信息化解决方案及服务，又可以进行快速有效的仿真模拟。通过这种购买服务的方式，企业可以降低设计与制造成本，大幅缩短企业产品升级

换代周期，提高产品性能，提升企业信息化能力，大幅提升工业企业的自主创新效率，并推动企业核心竞争优势的提升。

（3）电信：借势发力，对内对外双重“整合”

伴随数据量和带宽增加以及移动互联的发展，要求电信运营商走向云计算，否则其运营效率和模式都不具备长期竞争力。依托云计算，国内电信企业也将借势发力，成为云计算产业的主要受益者之一，从提供的各类付费性云服务产品中得到大量收入，实现电信企业利润增长，通过对国内不同行业用户需求分析与云产品服务研发、实施，打造自主品牌的云服务体系。对内进行业务系统 IT 资源整合，提升内部 IT 资源的利用率和管理水平，降低业务的提供成本；对外通过云计算构建新兴商业模式的基础资源平台，提供公用 IT 服务，提升传统电信经济的效率，加速电信运营商平台化趋势与产业链的整合趋势，并在应用层面推动云计算的落地。

（4）金融与能源：信息化整合的“关键武器”

金融、能源企业一直是国内信息化建设的“领军性”行业用户，在未来 3 年里，中国石化、中保、农行等行业内企业信息化建设将进入“IT 资源整合集成”阶段，在此期间，需要利用“云计算”模式，搭建基于 IaaS 的物理集成平台，对各类服务器基础设施应用进行集成，形成能够高度复用与统一管理的 IT 资源池，对外提供统一硬件资源服务，同时在信息系统整合方面，需要建立基于 PaaS 系统的整合平台，实现各异构系统间的互联互通。因此，云计算模式将成为金融、能源等大型企业信息化整合的“关键武器”。

金融业的数据信息直接涉及到社会各个方面的经济利益，所以保障这些信息安全的重要性是不言而喻的。因此，云计算在金融行业中遇到的首要问题是如何保障信息的安全可靠，包括避免数据信息泄漏、非法使用、丢失及保证信息的真实可靠等。

（5）教育：云计算为教育信息化服务

目前，云计算已经在清华大学、中国科学院等单位得到了初步应用，并取得了很好的应用效果。在未来，云计算将在我国高校与科研领域得到广泛的应用普及，各大高校将根据自身研究领域与技术需求建立云计算平台，并对原来各下属研究所的服务器与存储资源加以有机整合，提供高效可复用的云计算平台，为科研与教学工作提供强大的计算机资源，进而大大提高研发工作效率。

此外，云计算在构建网络学习环境、提高网络教育效率及整合教育资源等方面发挥重要作用。通过云平台实现教育资源的开放和共享，以用户为中心，通过云计算平台强大的计算能力、快捷的数据检索、智能的数据处理、人性化的服务，有效地提高人们的学习效率。

（6）医药医疗：云计算助推新医改

医药企业与医疗单位一直是国内信息化水平较高的行业用户，在“新医改”政策推动下，医药企业与医疗单位将对自身信息化体系进行优化升级，以适应医改业务调整的要求。在此影响下，以“云信息平台”为核心的信息化集中应用模式孕育而生，逐步取代目前各系统分散为主体的应用模式，进而提高医药企业内部信息共享能力与医疗信息公共平台的整体服务能力。

（7）云计算推动农业信息化建设

通过与骨干网络等基础设施建设的配合，对农业生产的各种要素进行数字化设计、智能化控制、精准化运行、科学化管理，实现云服务与农业发展紧密结合，从而推动农业信息化的建设。农业生产方面，可以指导生产者、经营者和管理者将农产品顺利进入市场，实现农业增产、农民增收；在农民生活方面借助信息传播媒体，设计并提供针对农村、农业、农民特点和使用习惯的软件与服务，以提高农民生活质量。

1.7　云计算带来的机遇与挑战

云计算这一技术变革彻底改变了传统的 IT 产业环境，对人们的生产生活产生了深远的影响，具有极其重大的意义。云计算相关技术的部署给整个云计算产业链带来机遇的同时，也带来了众多的挑战。

1.7.1　云计算带来的机遇

云计算是一场改变 IT 格局的划时代变革。云计算庞大的市场规模超乎想象。中国云计算产业发展路径与国外云计算以市场需求驱动企业自主发展为主的情况有很大不同。由于市场结构、技术发展阶段、投资习惯等原因，未来中国的云计算发展将首先以政府采购及企业自主购买两方面同时发展，并最终带动全社会实现云计算的普及化。中国云计算产业生态系统正在加速形成和完善，云产业发展迎来空前良机。

（1）政府大力扶持，战略结构转型

云计算作为“十二五”战略性新兴产业之一，得到了政府的大力扶持。中国政府始终积极地推动云计算的发展，并将其列为未来几年 IT 发展的战略重点之一。中国政府不仅是政策制定者，而且还是大买家，对 IT 产业有着强大的影响力，并且正在利用这种影响力推动整个 ICT 产业朝云的方向发展。

目前各地方政府的云计算发展如火如荼。在电子政务建设领域，“政府云”的建设可以提高设备资源利用率，推动信息资源整合，优化服务效率。通过云平台可以提高政府信息平台的安全性，同时也提升了政府数据的公开性和管理的“透明度”，带来政府管理的创新。结合“政府云”及地方信息产业发展状况，中国已有 30 多个地方政府公布了云计算产业发展规划，相继出台了产业发展规划、行动

计划，鼓励建设示范试点工程，制定了土地、税收、资金等方面的优惠政策，以推动中国信息基础设施建设和信息化进程。

（2）提升信息服务水平，深化产业改革

云计算产业具有极大的产业带动力量，在云计算的驱动下，新的业态和新的商业模式层出不穷，各种融合式创新将不断涌现。以物联网、移动互联网为代表的新一代信息技术的交叉应用市场也在快速成长，各地“智慧城市”建设逐步落地，这些领域的深化必将推动中国整体 IT 业产值的大幅提升。

2012 年的 Gartner 调研报告显示，与其他国家的同类企业相比，中国企业的态度令人惊讶，它们很可能是采用固态硬盘（SSD）和云计算等先进存储技术的先驱。中国云计算产业有望在 2015 年占到战略性新兴产业规模的 15%以上。

（3）实现降本增效，落地节能减排

近年来，各地信息系统不断建设，各级政府、企业均投入巨资采购大量硬件设备，建设多个应用系统，但是普遍出现设备资源利用率低、重复建设严重、信息系统运维难、人工成本和能源消耗巨大等问题，提高设备资源利用率、避免重复建设、降低维护成本成为各级数据中心迫在眉睫的需求。

云计算可以提高现有设备运行效率，并减少总体拥有成本（TCO）。同时，云计算对 IT 资源的集中和整合使用可以减少设备规模，及时关闭空闲资源，有效降低能源消耗，提高资源利用率，推动国家节能减排政策的落地。

随着“云生态系统”的不断发展和完善，云计算在民生、电子政务、城市管理等多个领域信息化水平提升方面发挥越来越大的作用。通过提供海量数据存储和强大的数据处理能力，云计算能够为科技创新提供坚实基础，提高科技创新能力，并缩短产品和服务进入市场的周期，提高用户业务的敏捷性和动态性。在支撑中小企业信息化升级的同时，保障国家经济平稳较快发展。

1.7.2 云计算带来的挑战

云计算在带来很多便利和优势的同时，也带来了许多新的挑战。成功应用云计算，必须面对一系列的挑战，包括新 IT 基础设施的挑战、用户隐私的挑战、安全的挑战、数据主权的挑战及新标准的挑战。相对而言，云计算在中国起步、研发、应用、推广等环节比较晚，目前还需要解决以下几大方面的问题。

（1）云数据中心部署结构不够合理，资源利用率较低

利用云计算技术进行整合升级，提升数据中心规模，发挥集约优势成为云计算发展的重要趋势。据统计，大型数据中心的节点平均能耗仅为中小数据中心的七分之一左右。然而，在规模结构方面，中国大规模数据中心比例偏低，大型数据中心发展规模甚至不足国外某一互联网公司总量，目前还没有实现集约化、规模化建设。同时，一些地方投入巨资建成了所谓的“云清洗”系统，资源利用率却不足，使得云计算中心成了给政府贴金的“形象工程”和“卖地工程”。一些地方缺乏对云计算的系统全局认识和思考，缺乏技术研究、项目建设的经验，存在一哄而上、投资过热的情况。因此，云产业建设还需要进一步的合理规划。

（2）云服务能力亟待提高，配套资源缺乏

国内云计算服务能力与美国等发达国家相比仍有较大差距，公共云计算服务业的规模相对较小，业务较为单一，配套环境建设滞后。随着 Google、Amazon 等企业加速在全球和中国周边布局，云计算服务向境外集中的风险将进一步加大。同时暴露出国内云计算标准规范、第三方评估认证审计等配套支持环节明显不足等问题。

从平台统一角度看，目前云计算还没有形成统一的标准，服务器商众多，不同厂商的解决方案不同，各云计算平台之间不可实现互操作，从而直接影响了云

计算的大规模市场化和商业应用。

从系统管理角度看，互操作性是需要解决的首要问题。当一个云系统需要访问另一个云系统的计算资源时，必须要对云计算的接口制定合理高效的交互协议，使得不同云计算服务提供者相互合作，以便更好地发挥云计算服务的优势。

从用户体验的角度看，用户使用云计算离不开网络，稳定、高速的带宽是提供云计算服务的保障。此外，在云计算网络中完成信息的高效处理，云计算集群服务器要具备较高的性能，需要提供高性能的通信设备。

（3）信息安全法律法规和监管体系不够健全

从数据安全的角度看，虽然云计算为存储数据提供了无限的空间，也为数据的处理提供了无限的计算能力，但是用户对于托管自己加密数据的云服务提供商能否确保数据的安全这一问题还存在质疑。而且在使用云计算服务时，用户往往不清楚自己数据存放的位置，这样就会导致用户对数据安全的担心，云计算架构于互联网之上，传统安全问题依然存在，如病毒、木马的入侵、隐私信息的泄露等，新的安全问题也将浮出水面。另外，身份认证、授权与访问控制、责任认定、安全与隐私等技术问题也都还处于探索阶段。

在与云计算安全相关的数据及隐私保护、安全管理、网络犯罪治理方面，中国的云计算产业生态有较大缺失。同时，由于对安全的担心和其他顾虑，云计算服务在中国的使用率相比美国等发达国家较低。

（4）云人才缺口，缺乏成熟商业模式

据数据显示，中国云计算人才缺口达百万级，2012 年与云计算相关的职位增长超过 150%。云产业生态需要 IT 和 CT 产业融合发展，需要复合型人才梯队的培养和建设。因此，学科融合和复合型人才培养尤为重要。云计算企业的崛起，将进一步加大相关技术岗位的招聘需求，特别是那些具备软硬件知识、懂技术、

懂运营、懂市场的全能型 IT 人才，无疑将成为中国云计算发展的核心力量。

在技术浪潮和产业热情推动下，一大批厂商进入中国云计算市场，但由于目前尚未形成有效的评价、资格认证和准入机制，云计算市场上鱼龙混杂，大型、可信赖的服务提供商和行业普遍认可的成功应用实践案例匮乏，一定程度上制约了产业规模的扩张与进一步的有序发展。

在中国，云计算作为一个新兴应用，目前依旧处于发展初期，用户对技术成熟度、系统安全性、方案有效性、建设成本等方面存在较大顾虑。企业在大规模云计算系统管理、支持虚拟化的核心芯片等一些制约云产业发展的关键产品和技术方面仍亟需突破。与此同时，成熟的商业模式、统一的标准规范及合理完善的法律法规监管体系的建设需要同步加强，通过产业链的整体提升，实现中国云计算在新一轮 IT 产业浪潮中立于不败之地。

1.8　小结

云计算技术的兴起已经逐步改变了人们的生活方式，云计算不仅有效地提高网络、计算、存储等系统资源利用率，而且已经改变了现有的 ICT 商业运营模式。因此，云计算已成为 ICT 产业最热门话题之一。人们纷纷投入到云计算产业，争相研究云计算相关技术与业务模式，不断挖掘这一新兴市场的潜力。为了让读者更好地了解云计算相关背景，本章首先回顾了云计算的发展历程，根据业内对云计算的认知，提出了云计算的定义，并梳理了云计算具备的几大特征。随后从云计算的服务类型和部署方式阐述了云计算能够给用户提供的各种服务，并从多种行业应用的角度分析了云计算的出现对现有产业链所产生的影响。最后从多方面分析了云计算带来的机遇与挑战，并点出了安全方面的挑战，以引出后续的云安全话题。

参考文献：

[1] FINN A, VREDEVOORT H, LOWNDS P, FLYNN D. Microsoft Private Cloud Computing[M]. John Wiley & Sons, 2012.1-11.

[2] Cloud computing[EB/OL]. http://en.wikipedia.org/wiki/Cloud_computing.

[3] CHAVES D S A, URIARTE R B, WESTPHALL C B. Toward an architecture for monitoring private clouds[J]. IEEE Communications Magazine, 2011, 49(12), 130-137.

[4] Getting started with AWS[EB/OL]. http://docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/gsg-aws-intro.html.

[5] IBM smartcloud[EB/OL]. http://www.ibm.com/cloud-computing/us/en/.

[6] National institute of standards and technology[EB/OL]. http://www.nist.gov/ index.html.

[7] 刘鹏. 云计算(第 2 版)[M]. 北京: 电子工业出版社, 2011.

[8] BAUER E, ADAMS R. Reliability and Availability of Cloud Computing[M]. Wiley-IEEE Press, 2012.

[9] SHAIKH F B, HAIDER S. Security threats in cloud computing[A]. Internet Technology and Secured Transactions (ICITST) International Conference[C]. 2011. 214-219.

第2章 Chapter 2

理解云计算安全

如第1章所述，在云计算技术不断演进的过程中，频繁出现的安全问题已经成为制约云计算系统、云计算业务正常发展的“绊脚石”。为了消除安全隐患，云计算产业链成员纷纷投入到云安全解决方案、系列产品、软硬件的研发当中。但是，不同成员对云安全的理解、认知、定义不同，导致用户对云安全内涵理解不到位，认为云安全的范围模糊，不好界定。因此，本章对目前业内的云安全定义进行梳理，系统地归纳了云安全的两方面内涵：云自身安全与云计算安全应用。本书后续章节均以云自身安全为出发点，以保护政府、企业拥有的云平台、云系统安全为目标，开展后续云安全威胁、云安全标准、云安全技术、云安全实践的讨论。

2.1 云计算安全定义

“云安全”这一概念于2008年成为信息安全界的热点，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，被认为是网络信息安全的最新体现。云安全发展初期曾经引起不小的争议，许多人曾认为它是伪命题，现在云安全这一说法已经被广泛接受，业内安全厂商瑞星、趋势、卡巴斯基、MCAFEE、

SYMANTEC、江民科技、PANDA、金山、360 等都推出了云安全解决方案。

从另一个角度看，云安全也指通过法规政策与安全技术手段对政府、企业的云计算平台、业务应用等多层面采取预防、监控、恢复、评估等机制，以抵御来自外部网络的恶意攻击，同时防止云平台中核心资源遭到破坏、用户隐私发生泄露。

本书认为，云计算安全这个概念包括两层含义。

（1）云计算技术在安全领域的应用（云安全应用）

其含义是通过云计算特性来提升安全解决方案的服务性能，属于云计算技术的安全应用。例如，安全厂商开发了基于云的防病毒技术、挂马检测技术，这些解决方案可以对大量客户端软件的异常行为进行监测，发掘互联网木马、恶意程序的最新信息，推送到云端进行自动分析和处理，再把病毒和木马的解决方案分发至每一个客户端。

（2）安全技术在云环境下应用（云自身安全）

其含义为利用安全技术，解决云环境下的安全问题，提升云平台自身的安全，保障云计算业务的可用性、数据机密性和完整性、隐私权的保护等，这是云计算业务健康、可持续发展的基础。

就目前来看，传统安全厂商多立足于第一层内涵，利用云计算技术解决常规安全问题，而云服务提供商多关注第二层面，构建云平台的安全保障体系。

2.2 云计算安全产业链分析

云计算安全产业通过安全技术与安全管理手段保护政府、企业云平台内部数据、用户隐私、访问控制安全，同时负责抵御来自外部网络的各种恶意软件、病毒、木马的侵袭、攻击。本书认为，云计算安全整个产业链由政府、标准组织、运营商、云厂商、安全厂商、用户等产业链成员组成。

（1）政府与标准组织

国家政府部门可制定发布一系列针对云安全相关的法律法规和管理办法，同时加大对产业链各成员监管力度；各种标准组织，包括国际标准组织、国家标准组织、行业标准组织等可出台一系列关于云安全相关的技术标准，以规范整个云安全产业链及云安全市场。

（2）运营商

运营商可以开展三方面工作：第一，根据国家法律法规、国家标准、行业标准，以自身内部云安全需求为驱动，制定、发布云安全相关企业标准；第二，依据企业标准，通过同步网络现有的安全系统与云计算技术，实现运营商云系统的集中安全管控；第三，开发云计算安全业务，为内部、外部客户提供安全服务。

（3）云厂商

许多云服务提供商，如亚马逊、 IBM、 微软，可以为客户提供云计算安全、云计算服务平台能力，改善、加固现有部署解决方案，保障服务的连续性和用户数据安全性。具体方案涉及云身份验证、云安全管理、云审计、数据加密、隐私保护、虚拟化安全管理平台、虚拟防火墙等技术方案。

（4）安全厂商

传统的 IT 安全厂商如瑞星、趋势、卡巴斯基、MCAFEE、SYMANTEC、江民科技、金山、360 安全等进入云计算市场后，均推出了云安全解决方案或云安全产品。这些云安全产品可以分为基于用户侧、基于服务器侧两种类型的产品方案。第一种是基于用户侧的云安全解决方案，其思想秉承了传统安全解决方案的做法，在用户终端上部署一定的安全措施，如开发云安全客户端，以抵御来自外部的安全威胁。此类产品将用户作为监控点，通过用户主动上报或位于用户终端上的软件自动提取安全事件汇总到统一处理平台，统一平台能将分析结果反馈给

用户。第二种是基于服务器侧的云安全解决方案，一般部署于网络侧或服务器侧，其思想是在安全攻击到达用户客户端之前进行防御，预防来自于外部网络侧、服务器侧的安全威胁殃及用户终端。此类产品借助网络中的不同监控点，采用多种方式收集安全事件信息并进行加工处理，生成黑白名单或者特征库，从而在网络侧构建安全云。当普通用户访问目标信息时，首先从安全云中获取安全访问建议，从源头上阻止风险的侵入。

（5）用户

用户包括使用云安全解决方案的企业内部员工与外部普通用户。在使用已部署的云安全产品时，用户可以反馈产品的使用情况与方案的不足。云安全厂家根据用户的反馈意见，及时改进、加固现有解决方案。

从 2011 年起，各种“云”充斥着 IT 市场，云概念一度被认为是 IT 产业新一轮的革命，国内外主要 IT 企业都将云计算列为公司未来主要战略方向。然而，国内目前关于云计算、云安全的产品并不多。因此，用户很少能体验到云安全切实的服务。例如，云杀毒主要利用互联网在线存储与查杀技术，仅属于狭隘云计算范畴。而在国外市场上，云安全服务已形成了一个完整的运营系统，可以让用户看得见、摸得着。国内企业如想真正将云安全落到实处，最需要的是梳理清云安全商业服务模式，而不是盲目去开发。为了使读者更好地推进云安全产业发展，了解云安全发展态势，以下梳理了云安全产业几大趋势。

1）实现安全资源池化。云安全服务商的安全资源需支持各种类型客户安全防护需求，包括虚拟机访问控制、邮件过滤、DDoS 防护、漏洞扫描、内容过滤、防病毒、身份认证等。这些安全资源都被放到一个资源池内，再进行统一分配。

2）实现云数据的安全存储。在个人云存储服务逐渐获得用户认知后，面向企业级客户的云端存储市场正在悄然展开。据统计，2012 年中国个人云存储用户数

达到 1.07 亿，年增长率高达 371.7%。云安全服务商可借助利好势头，向用户推广云数据、云个人隐私数据保护解决方案，以保护用户隐私，政府、企业核心数据的存储。

3）安全服务网络化。云安全是基于互联网、移动互联网的服务，网络所到之处就应当是服务所在之处。因此，云安全服务可以为广大网络用户提供安全保护。

4）需部署云安全管理平台。云安全服务提供商构建云安全管理平台，对池化的安全能力进行日常的资源调度及管理，为客户提供按需可伸缩的安全服务，同时也能为客户提供自助服务及客户日常服务报表分析。

5）运营商和云安全厂商需要密切配合。随着技术不断演进，私有云与公有云的资源将被混合或者交错利用。运营商、云安全服务商通过展示自身的网络优势、用户资源优势、渠道优势等，打造聚合平台、开放平台、服务提供平台，将基础能力、开发者、应用和用户进行整合，开放自身或第三方的资源、能力、应用，并作为服务提供给用户，这些将成为必然的发展趋势。

毫无疑问，云安全产业链中的先驱者将在云计算市场发展中占据及其重要的地位，并左右企业的未来发展。目前，云安全联盟（CSA）已经开展云安全相关工作，其成员多数为与云安全产业相关的大型企业。在不到 2 年时间里，已经有超过 50 个跨国公司加入 CSA，包括 Google、HP、CISCO、Intel、MS、Oracle、Novell、AT&T、CA、McAfee、TREND、Symantec、NSFOCUS、3PAR 等。而在此之前，尚未出现具有影响力的云安全联盟组织。目前，国内云安全尚处于初级阶段，而每个厂商或者企业的技术力量都是有限的，不可能涵盖云安全产业链的所有层面。随着云计算的不断发展和演变，国内各个厂商及研究机构对于云计算、云安全将提出自己的独特见解，这些观点代表了各个领域的发展特性。通过整个产业链成员不断推动云安全的实践和创新，逐步打造完善的中国乃至亚太地区云

安全产业，发掘云安全产业中的契机，对云安全产生的发展具有极其重要意义。

2.3 云计算安全与传统安全比较

云计算与传统的计算模式相比具有开放性、分布式计算与存储、无边界、虚拟化、多租户、数据所有权与管理权分离等特点。同时，云中包含了大量软件与服务，数据量庞大，系统非常复杂。因此，传统的安全技术、管理方案难以奏效。此外，云计算系统中存放着比传统信息系统更多的海量用户数据，对攻击者来说具有更大的诱惑力，如果攻击者通过某种方式攻击云系统，将会给云服务提供商和用户带来重大损失。因此，云计算的安全性面临着比以往传统系统更为严峻的考验。为此，本节系统地梳理并比较了云计算安全与传统安全的异同点，让读者进一步了解云计算安全的特点。

云计算安全与传统安全具有以下 3 个相同点。

1）目标是相同的，保护信息、数据的安全和完整。

2）保护对象相同，保护计算、网络、存储资源的安全性。

3）部分采用技术类似，如传统的加解密技术、安全检测技术等。

在分析云计算安全与传统安全的不同点时，根据 2.1 节云计算安全的定义描述的双重内涵，将云计算安全分为云安全服务与云自身安全两个层面，分别与传统安全进行比较分析（如表 2-1 所示和表 2-2 所示）。

表 2-1 云安全应用解决方案与传统安全方案比较

比较维度	云安全应用解决方案	传统安全方案
资源占有量	占用较少资源	占用大量的计算资源
病毒样本库位置	病毒样本库位于云服务侧	病毒样本库位于本地
网络安全态势感知功能	具备网络安全态势感知功能，为用户提供更为全面的防护机制	不具备网络安全态势感知功能

表 2-2 云自身安全解决方案与传统安全解决方案的比较

比较维度	云自身安全解决方案	传统安全解决方案
虚拟化安全	涉及虚拟机安全、虚拟机管理平台安全（Hyper-v、VMware、KVM 和 Xen 安全）、虚拟网络安全等	传统安全解决方案没有系统地考虑虚拟机安全，既不能保护用户数据安全，又不能及时地发现系统中的安全漏洞与缺陷
数据安全问题	用户数据资源存储与应用部署集中化，更易遭到黑客攻击。因此，需要部署增强型数据安全解决方案	采用传统安全解决方案，如部署防病毒软件、防火墙等以保护用户数据安全
安全边界	传统安全解决方案已不适用于云环境，云系统安全边界变得愈加模糊	传统方案可以顺利地划分系统的安全域，清晰地辨别物理、逻辑安全边界
云业务模式安全	针对业务模式的改变，云服务提供商不得不考虑一些增强安全解决方案，以保护系统生命周期安全及核心数据安全	传统安全解决方案通过部署安全网关或防火墙抵御外部攻击
平台可靠性	现有方案很难快速找出云系统的故障或安全漏洞，从而修缮云系统，需要部署新型安全方案解决这一问题	在传统平台上部署应急响应机制，现有方案不能支持云平台环境，不能保证云业务的连续性
安全审计	云审计工作纷繁复杂	传统安全审计工作易于实现
云平台安全漏洞	在云环境下，可能存在新型安全漏洞	传统平台存在安全漏洞
管理安全	若安全机制部署不当，易于造成用户丢失对自己的数据控制权限	传统安全重点聚焦于物理安全、数据安全、人员安全、设备安全等方面的管控
法律问题	目前缺少云安全相关法案	政府已颁布安全相关法律法规

首先，云计算安全服务与传统业务安全方案区别如下。

（1）客户端资源占用率低

目前市面上发布的新型云计算安全方案较传统安全方案客户端的资源占用率更低，极大程度降低了客户在不同状态下的整体资源占用。

（2）病毒库置于服务器端

基于云技术的安全业务解决方案打破了传统安全方案将病毒特征库存放于本地用户终端并需不断升级更新病毒库的格局。新方案将病毒定义和特征库置于服务器侧（云端），用户仅需在本地调用引擎和特征库，即可随时访问包含成千上万样本的病毒特征库来识别对应威胁。

（3）实现云安全态势感知新功能

新型云安全业务方案可以为用户提供更为全面的防御功能，针对现有病毒不断持续快速更新、变异的特点，在执行扫描操作时，该方案可开启云安全态势感知功能，第一时间检测到恶意威胁。这样使防护模块更为有效地拦截来自不同途径的病毒、木马攻击，让用户真正体验到最为可靠、可信的安全防护。

与此同时，随着云计算安全的不断演进，在云环境下，云计算系统本身也面临着前所未有的安全挑战，这些挑战正体现了云安全的第二层含义。

（1）虚拟化安全问题

虚拟化是云计算概念相关性最紧密的一项技术，虚拟化的大规模应用引发了业内专家对云系统安全的重新思考，带来了虚拟化相关的安全问题，如虚拟机自身安全、虚拟机管理平台安全、虚拟机构成的虚拟网络安全等问题。因此，传统的基于物理安全边界的防护机制难以有效保护基于共享虚拟化环境下的用户应用及信息安全。另外，云计算系统非常庞杂，主要通过虚拟机完成计算任务，一旦虚拟机出现故障，如何快速定位故障点也是一项重大挑战。

（2）数据安全问题

云计算系统中存放着海量的用户重要数据，攻击者会千方百计地通过某种方式攻击云系统，窃取企业核心数据和用户隐私信息，将会给云计算服务提供商和用户带来重大损失。

第一，由于云环境具备用户、应用和数据资源更为集中的特点，这造成了黑客更易发动集中大规模攻击。事故一旦发生，影响范围广，后果影响严重。第二，云计算多租户的特性导致了数据在云服务中的存储空间具有共享性质，即没有专门为某个用户开辟独立存储空间，因此，存在用户数据泄露的潜在危险。第三，和传统软件相比，云计算在数据方面的最大不同是所有的数据由第三方负责维护，

并且根据云计算架构的特点，这些数据可能存储在分散的地理位置，并且都以明文的形式存储。虽然防火墙能够对恶意的外来攻击提供一定程度的保护，但仍然会造成一些关键性的数据泄露。第四，传统系统采用数据加密方式保护数据，但云计算环境下，很可能众多用户数据被共同保存在同一物理机内。因此，需要部署数据安全隔离机制，将用户自身的数据与其他用户的数据隔离开，可以更加有效地保证数据安全。

（3）云安全边界界定问题

传统系统通过在物理上和逻辑层面上划分安全域，可以清晰地定义安全边界和保护设备用户。由于云系统用户数量庞大，数据存放分散，安全边界区域模糊，传统基于物理安全边界的防护机制在云计算环境下难以奏效，很难为用户提供充分的安全保障。

（4）云业务模式带来的安全问题

云计算与传统的服务模式相比具有开放性、分布式计算与存储、无边界、虚拟性、多租户、数据的所有权和管理权分离等特点；同时，云中包含大量软件和服务，以各种标准为基础，数据量庞大，系统非常复杂，因而在技术、管理和法律等方面都面临新的安全挑战。例如，IaaS、PaaS、SaaS 业务模式均给数据安全的保护提出了更高的要求。各种业务模式在其特定的应用场景下，可能会衍生出各自特定的安全威胁。传统安全手段已经不能解决这类安全问题。需要研究针对各自业务模式下的新型安全解决方案。

（5）云计算系统可靠性问题

云计算系统非常庞大，发生故障时，如何快速地定位问题所在，是一个令人头疼的问题。过载（常见的 CPU、RAM 及 IO 被大量占用；很多用户同一天同一时间登录到客户网站造成瘫痪）、代码问题（低质量代码导致增加负载，占用大量 CPU

资源；或某些程序占用内存空间大，导致 RAM 不够；低质量 SQL 语句，缺乏索引，导致数据库崩溃）、服务器崩溃、数据库问题、带宽、硬件、CDN、数据中心问题等都可以导致云系统瘫痪，破坏系统可靠性。另外，还存在一些人为问题。例如，在进行系统更新或开发过程未经完善测试的时候，程序员、内容编辑人员、游戏开发人员甚至是内部成员可能在不经意间制造了 Bug。另外，系统扩展时，如果没有合理考虑系统架构设计，可能会导致负载均衡失衡，从而影响云系统可靠性。

（6）云安全审计问题

云计算面临着在云这一特定环境下的安全审计问题。尤其是对云安全数据的审计，包括云数据的采集、预处理、存储等方面的审计。良好的数据安全审计机制，可以较好防止企业核心数据与用户隐私数据泄露事件的发生。

（7）云平台系统安全漏洞问题

云计算服务仍由服务器搭建，各类传统主机安全威胁依然存在，且安全问题随系统规模化而被放大。若平台主机一旦发生故障，其影响范围广，后果更加严重。但是，无论为云平台系统部署何种的安全方案，云平台本身都会或多或少地存在安全漏洞，如何及时发现、修复这些安全漏洞，及时提出安全加固建议，这些问题产业链成员仍然在努力研究，以不断寻求更好的解决方案。

（8）云安全管理问题

云计算这种全新的服务模式将资源的所有权、管理权及使用权进行了分离，因此用户失去了对物理资源的直接控制，用户数据会面临与服务商协作而产生的一些安全问题，如不完整和不安全的数据删除会对用户造成损害；另外，企业和云服务提供商之间需要在安全方面达成一致，签订安全合作保密协议。用户与云服务提供商实际交互过程中，如何界定用户与云服务提供商的不同责任也是一个重要问题，以及存在一些协同和管理上的问题。例如，发生攻击时的联动，对运

营管理的模式提出安全要求，监管方面安全问题等。

（9）法律层面存在风险

法律层面主要涉及地域性的法律法规问题。云计算应用具备地域性弱，信息流动性大的特点，在信息安全监管、隐私保护等方面可能存在法律风险。特别是在我国，目前还没有出台一部针对云安全的法律法规，需要后续由政府不断推进、不断完善。

总之，不管政府、企业和用户对云计算的接纳程度如何，现实情况是云计算安全距离成熟还有很大的一段距离，需要产业链各个成员共同努力，共同推进。

2.4　小结

随着云计算这一新兴技术的不断演进，安全问题逐渐成为制约云业务发展的重要问题。针对云安全问题，业界云安全相关技术、产品、解决方案层出不穷，可谓良莠不齐。不同的厂家根据各自的应用场景对云安全理解不同，提出了不尽相同的云安全定义，而且分歧较大。本章首先提出了云计算安全的定义，深刻地剖析了云计算安全的两个层次的含义：云安全服务与云系统自身安全；然后分析了云计算安全产业链中的各个成员角色，阐述了产业链成员各自相应的功能职责，对云计算安全整体产业链的现状与未来趋势进行了点评；最后，进一步分析了云计算安全服务、云系统自身安全与传统安全之间的区别，以及面临新的安全挑战。本书第 3 章将进一步深入分析云计算面临的安全威胁与安全挑战，从而提出云计算的安全需求。

参考文献：

[1]　中国电信网络安全实验室. 云计算安全: 技术与应用[M]. 北京: 电子工业出版社, 2012.

[2] POTTER, B, MCGRAW G. Software security testing[J]. IEEE Security & Privacy, 2004, 2(5): 81-85.

[3] 潘松柏, 张云勇, 陈清金等. 云计算安全关键技术[J]. 电信科学, 2010, 26(8).

[4] 童晓渝, 张云勇, 戴元顺. 公众计算通信网架构及关键技术[J]. 通信学报, 2010, 31(8).

[5] 汪来富, 沈军, 金华敏. 云计算应用安全研究[J]. 电信科学, 2010, (6): 67-70.

[6] 冯登国, 张敏, 张妍, 徐震. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83.

第3章 Chapter 3

云安全威胁及安全需求

云计算技术在商业模式、计算模型、用户体验等方面发生了重要革新，但是其应用系统架构、用户访问行为仍然沿袭传统 IT 框架。因此，系统软硬件故障、拒绝服务攻击、病毒蠕虫、恶意代码和钓鱼网站等各类传统安全威胁仍然存在，且上述安全问题会随系统规模化而被放大。同时，云计算与传统的计算模式相比具有开放性、动态边界、虚拟性、多租户、数据的所有权和管理权分离、资源相对集中、对安全设备的性能和扩展性等方面有新的要求等特点，这使得在云计算系统在技术、管理和法律等方面面临新的安全挑战。此外，云计算系统中存放着海量用户数据，对攻击者来说具有更大的诱惑力。如果云计算系统遭受攻击，将会给云业务提供商和用户带来重大损失，云计算系统面临比以往的业务系统更为严峻的考验。

本章首先列举近年来典型云计算安全事件，之后提出云计算安全威胁及安全需求，希望通过本章的描述可以使读者对云计算安全问题有直观的认识。

3.1 云计算安全事件

（1）产品漏洞

- 2005 年 1 月，Google 的 Gmail 因发现安全漏洞，导致用户的用户名和密

码面临安全威胁。

- 2005 年 12 月和 2007 年 1 月，Google 桌面发现安全漏洞，存在远程侵入 Google 桌面的危险，整个用户电脑系统可能被控制。

（2）隐私泄露

- 2008 年 9 月 15 日，Google 文档发生意外，用户在自己的账户中发现不属于自己的文件。

- 2009 年 3 月 10 日，Google 文档误共享信息，在未经用户许可的情况下，误将用户的部分文档进行共享。那些曾经赋予共享权限的用户的文档被错误共享，且只有文本文档和演示文档遭受影响，电子表格内容未被共享。

- 2010 年 2 月 25 日，Google 推出的社交网络产品 Google Buzz 遭到 Gmail 用户的集体诉讼，用户认为其隐私受到了侵犯。该社交网络产品与 Gmail 交互，会在使用者不知情的情况下，将其经常联系的人排列在一起，并在互联网上自动传播。

- 2011 年 3 月，谷歌邮箱爆发大规模的用户数据泄露事件，约 15 万 Gmail 用户发现自己所有的邮件和聊天记录被删除，部分用户发现自己的账户被重置。

（3）黑客攻击

- 2009 年 2 月 26 日，Google 的聊天室遭黑客入侵，大部分用户都收到看似是朋友发出的信息“点击 tinyurl.com 网址，去名叫 ViddyHo 的网站”，该网站需要用户以 Gmail 登入信息登录。黑客利用有关数据入侵到用户的 Gmail 账户，被入侵的账户其后向该账户联络清单上的人发出相同信息，令病毒迅速扩散。

- 2009 年 11 月，Google 阅读器遭到洪水攻击，社交网站上张贴了大量内含有洪水攻击的 Google 阅读器链接，以引诱网友点击，一旦点击即会被植入含有洪水攻击的恶意程序，受感染计算机将成为 Koobface 僵尸网络的一员。

- 2009 年，亚马逊平台被僵尸网络恶意利用于非法活动。僵尸网络在亚马

逊的 EC2 云服务中运行着一个未授权的命令和控制中心，黑客通过入侵一个使用 EC2 云服务的网站后，在亚马逊的服务器上安装了一个命令和控制程序。

- 2011 年 4 月 19 日，索尼的 PlayStation 网络和 Qriocity 音乐服务网站遭到黑客攻击，服务中断超过一周，PlayStation 网络 7 700 万个注册账户持有人的个人信息失窃。

（4）服务故障或中断

- Google 已经历了数次服务故障。其中重大故障有：2008 年 8 月 7 日 Gmail 和 Google Apps 服务中断；2009 年 3 月 9 日 Gmail 服务中断；2009 年 5 月 14 日 Google 网络中断；2009 年 5 月 18 日 Google News 服务中断；2009 年 9 月 1 日 Gmail 服务中断；2009 年 9 月 22 日 Google News 服务中断；2009 年 9 月 24 日 Gmail 服务中断。

- 2008 年 7 月 20 日亚马逊简单存储服务宕机超过 6 h，亚马逊 S3 服务故障使 SmugMug 网站存储在 S3 服务中大量的照片和视频都无法访问。

- 2009 年 7 月 20 日，亚马逊 EC2 等 6 款云计算服务出现故障，在 12 点 31 分开始发现数据分组丢失增多，随后该问题扩展至整个美国东 1 区，在此期间，有许多用户无法访问亚马逊网站主页。此前亚马逊云计算服务曾于 2008 年 2 月、2007 年 10 月和 2009 年 6 月都出现过大范围的故障。

- 2009 年 3 月，微软的 Azure 平台宕机 22 h，凸显云计算缺陷。Azure 服务中断是由于操作系统升级时出现故障。该故障导致 Windows Azure 的部署服务减缓，大量服务器出现超时和中断。

- 2009 年 2 月 26 日从英国到南美洲巴拉圭、再到太平洋岛国萨摩亚和澳洲，全球 Gmail 用户输入账户名和密码登录邮箱，计算机上就会出现 502 服务器错误（502 server error）信息：'服务器遇到临时性错误，所以无法完成您的要求，请于 30 s 内重试。

- 2009 年 7 月 3 日，Google App Engine 曾发生故障，持续 6 h，Google App Engine 遭遇数据仓库操作延迟增加、错误率上升等故障。2010 年 2 月 25 日，Google App Engine（谷歌应用引擎）宕机，原因是一个备份数据中心发生故障。

- 2011 年 4 月 22 日，亚马逊云位于弗吉尼亚州的云计算中心宕机，导致回答服务 Quora、新闻服务 Reddit、Hootsuite 和位置跟踪服务 FourSquare 和为网络出版商提供游戏工具的 BigDoor 瘫痪，故障持续了 4 天。

- 2011 年 5 月 13 日，微软云计算交换在线（Microsoft exchange online）服务出现故障，导致用户邮件信息延迟 3~9 h 发送。2011 年 6 月，在微软发布 Office365 前一周，微软 BPOS 云托管套件服务再次中断 3 h，微软在北美的用户都受到影响。

- 2011 年 7 月 15 日，谷歌应用引擎 Java 服务出现故障，宕机超过 1 h，故障原因是基于云计算应用程序转到网络上时出现了问题。

- 2011 年 8 月 9 日，亚马逊云服务故障约 1 h，使 Netflix、Foursquare、维珍美国航空公司（Virgin America）和其他几家网站均受到影响。

3.2 云计算安全威胁

云计算面临安全威胁可分为 9 大类：数据丢失和泄露、网络攻击、不安全的接口、恶意的内部行为、云计算服务滥用或误用、管理或审查不足、共享技术存在漏洞、未知的安全风险和法律风险。下面将对这 9 类威胁进行展开论述。

3.2.1 数据丢失和泄露

对于用户而言，数据安全性和隐私保护是其最为关注的问题。所有企业都采取相应的措施保护其用户数据、运营数据的安全性，因为数据泄露将对企业造成

巨额的损失，并使企业名誉受损。从某种程度上讲，云计算的出现为这一问题增加了新的挑战。

事实上，数据丢失和泄露是云计算最大的安全威胁，云计算中关键数据的高密度聚合对攻击者而言具有极大的诱惑力。一方面，攻击者可能会在不安全的客户端上运行木马程序或控制客户端，导致用户数据从终端泄露或者被篡改；另一方面，由于云服务提供商对数据存储所采取的隔离防护措施不当或策略失效，也可能导致数据丢失或被非法用户访问、篡改。

云服务提供商作为服务的提供者，有义务保护用户数据隐私性与完整性，不能主动破坏、窃取数据，并且尽可能防范来自内部的安全威胁，可采取的安全措施包括在数据中心各区域安装监控设备，记录操作日志，与员工、合作伙伴签订保密协议等。但是，上述措施只能降低安全风险，并不能完全阻止攻击的发生，而且大多数措施是在攻击事件发生后才部署的，并不能挽回已发生攻击造成的损失。

一般说来，数据安全风险包括数据泄露、数据篡改和数据丢失，数据传输、处理、存储的各个环节。在云计算环境的传输和存储环节，用户对于自身数据的安全风险并没有实际的控制能力，数据的安全性完全依赖于云服务提供商，如果提供商对于数据安全的控制存在疏漏，就很可能导致数据泄露或丢失。现阶段可能导致安全风险有以下几种典型情况。

（1）云计算服务模式造成用户数据泄露或丢失的风险

云计算环境的不同层次都存在数据安全问题。在基础设施即服务环境中，用户可以创建私有的基础设施，加密、访问控制和监控等手段能够降低数据被泄露的风险，但由于云计算环境的架构和其他限制因素，目前数据安全监控和过滤解决方案难以部署；在平台即服务环境中，用户能够快速启动新网页、数据库和电子邮件服务器，但与基础设施即服务环境相比，用户无法确保在云中数据的安全

性，数据安全机制几乎完全依赖云服务提供商。

当用户将自身数据交给云服务提供商管理，用户即失去对数据的掌控。在云计算环境中，多个用户共享计算资源，用户无法知道资源的物理位置或者控制资源的流动。云服务提供商拥有数据的优先访问权。事实证明，由于存在内部人员失职、黑客攻击及系统故障会产生多种安全风险，云服务提供商没有充足的证据让用户确信其数据被正确地使用。例如，用户数据没有被盗卖给其竞争对手、用户使用习惯隐私没有被记录或分析、用户数据被正确存储在其指定的国家或区域、用户不需要的数据已被彻底删除等。

云计算的服务模式使得云服务提供商在对外提供服务的同时，也需要购买其他服务提供商提供的服务。因而，用户使用的云计算服务间接涉及多个服务提供商，这种复杂性进一步增加了安全风险。

此外，目前云服务提供商提供的存储服务大多互不兼容。当用户决定从一个提供商转移到另外一个提供商时会遇到迁移问题，甚至造成数据的丢失。数据未彻底删除也可能导致信息泄露的风险。

（2）由于服务器或者虚拟化软件的安全漏洞造成用户数据被入侵的风险

在典型的云计算环境中，资源以虚拟、租用的模式提供给用户，这些虚拟资源根据实际运行情况与物理资源相互绑定，而且多个虚拟资源很可能被绑定在同一物理资源中，仅靠软件区分边界。因此，如果云计算的服务器或者虚拟化软件中存在安全漏洞，那么资源可能相互越界，用户的数据很可能被其他用户访问。例如，2009 年 5 月，VMware 虚拟化软件的 Mac 版本中被指存在一个严重的安全漏洞，攻击者可以利用该漏洞通过 Windows 虚拟机在 Mac 主机上执行恶意代码。2012 年 11 月，北卡莱罗纳州大学和 RSA 公司研究者发布的报告显示了在同一台物理机上，一个虚拟机如何利用侧通道计时信息来提取出另一个虚拟机的私有密

钥。在许多案例里，攻击者甚至不需要这么复杂的操作，如果一个多租户的云计算服务数据库设计不妥当，可能就会因为一个漏洞而导致所有用户的数据遭殃。因此，如果云计算平台无法实现用户数据的有效隔离，那么云计算服务提供商就无法给用户以安全保障。

（3）数据没有进行加密导致信息泄露的风险

用户数据以静态和动态两种形式存在于云计算服务器中。静态数据一般以存储为目的，仅仅利用云计算的存储功能，不需参与运算，如文字、图片和影音文件等。动态数据一般用于索引和查询，参与运算，如数据库文件、程序文件和业务逻辑用到的文件等。

缺乏有效数据安全机制的一个主要原因是现有加密功能的制约。一般而言，对静态数据的加密是可行的，但是动态数据或者云计算的应用程序使用的数据通常都是不能加密的，因为动态数据加密后将导致无法直接对数据进行处理、索引和查询，实施上述操作都需要解密数据。

此外，云计算使用分布式架构，意味着比传统的基础设施需要更多的数据传输，在传输过程中如未采用加密机制，攻击者可以通过实施嗅探、中间人攻击、重放攻击来窃取或篡改数据。

（4）加密数据的密钥管理存在缺失导致数据泄露的风险

数据的保密性需要大量的加/解密钥，而密钥的管理是一大难题。对用户来说，如果数据的加密密钥或访问权限的丢失，将会带来严重的安全问题。加密管理信息的丢失（如加密密钥、认证代码和访问权限等）将会给用户带来损害，例如数据的丢失和不期望的信息泄漏等。

（5）用户数据存储没有进行容灾备份导致数据丢失的风险

在云计算环境中，大量用户信息、财务数据、关键业务记录等敏感数据被集

中存储并在网络中传输。在未做备份的情况下对数据删除、修改，把数据存储于不可靠的介质上，密钥的丢失导致数据无法解密，发生意外灾难但缺乏合适的备份与存档等情况，都可能带来严重的数据丢失事故。例如，2011 年 10 月，阿里云服务器磁盘错误，导致 TeamCola 公司的数据丢失； 2011 年 3 月，由于管理员操作失误，15 万谷歌用户的邮件与聊天记录丢失。

3.2.2 网络攻击

在云计算环境下，多数应用和操作都是在网络上进行。用户通过云计算操作系统将自己的数据从网络传输到云计算平台中，由云计算平台来提供服务。云计算操作系统不是部署在普通服务器的物理硬件上，而是部署在数据中心的基础设施上，其提供了集群、数据保护、动态资源规模调整、存储管理和复制、存储虚拟化工具、网络管理等一系列功能。在这种工作模式下，云计算实质上是利用大规模基础设施构建了一个网络化、虚拟化、服务化、透明化的计算环境来完成各项远程信息交互和相关虚拟化业务。因此，云计算的安全问题实质上涉及整个网络体系的安全问题，但又有其自身特点。

3.2.2.1 账户或服务流量劫持

在云计算环境中，攻击者一般通过网络钓鱼、社会工程学欺诈或利用软件漏洞来劫持无辜的用户。如果攻击者能够获得用户的某个账号、密码信息，即可窃取用户多个服务中的资料，因为用户不会为每个账户设立不一样的密码。对于云服务提供商来说，如果被劫持的密码可以登录云计算系统，那么用户的云中数据将被窃听、篡改，攻击者将向用户返回虚假信息，或重定向用户的服务到欺诈网站，并且被劫持的账号或服务可能会被利用以发起新的

攻击。同时，账户或服务劫持通常伴随着证书盗窃。窃取证书后，攻击者可以进入云计算服务的一些关键性领域，破坏其机密性、完整性和可用性。账户或服务劫持不仅对用户自身造成巨大损失，还将对云服务提供商的声誉造成严重影响。

3.2.2.2　拒绝服务攻击

拒绝服务攻击是指攻击者阻止用户正常访问云计算服务的一种攻击手段，通常是发起一些关键性操作来消耗大量的系统资源，如进程、内存、硬盘空间、网络带宽等，导致云计算服务器反应变得极为缓慢或者完全没有响应。

云计算最主要的安全威胁之一就是应用层 DDoS 攻击，这些攻击严重威胁到云计算基础设施的可用性。如果云计算服务无法使用，那么从保护访问到确保合规等安全措施都失去了价值。目前，攻击者可以通过使用非常廉价且极易获取的工具对应用层发动攻击，有时只是在应用程序中运行一小段恶意程序，程序代码甚至不足 100 byte。攻击者之所以能够攻击成功，很大原因在于企业数据中心和云服务提供商没有对这类攻击做好防御措施，防火墙和入侵预防系统等现有解决方案是企业网络分层防御策略的关键部分，但它们却被设计用于解决那些与拒绝服务攻击完全不同的安全问题。随着拒绝服务攻击的大规模流行，数据中心运营者和云服务提供商将面临巨大的安全挑战。

流量高峰期遭遇拒绝服务攻击将是一场灾难，用户无法访问目标服务器。服务中断不仅会挫伤用户对云计算服务的信心，还会导致用户考虑将关键性数据从云计算中转移以降低损失。更糟的是，由于云计算服务的收费模式通常都是按照用户消耗系统资源率来计算，因此攻击者即使没有使云计算服务完全瘫痪，也使用户因为严重的资源消耗而蒙受巨大的经济损失。

3.2.3 不安全的接口

资源和能力开放是云计算的重要业务变革之一。云服务提供商需要提供大量的网络接口和应用程序编程接口整合相关资源，向业务合作伙伴开放能力，甚至直接提供业务。例如，在云计算环境中，云服务提供商通过软件接口或应用程序编程接口让用户与云计算平台进行交互，用户通过互联网访问云计算平台上的资源。这些接口能够控制大量的虚拟机，甚至包含云服务提供商用于控制整个云计算系统的操作接口。一些第三方企业基于这些接口为用户提供增值服务，这更增加了层次化的应用程序编程接口复杂性。远程访问机制及 Web 浏览器的使用也增加了这些接口存在漏洞并被利用的可能性。亚马逊 2011 年 10 月就修补了其 EC2 服务上的一个控制接口的加密漏洞，该漏洞能被攻击者用于创建、修改和删除镜像，并能修改管理员密码等。

另外，开发过程的安全测试、运行过程的渗透测试等安全实践，不管从测试工具还是测试方法上，对于网络接口和应用程序编程接口都不够成熟，一旦后台安全功能被开放，将引入额外的安全入侵入口。

大多数的云服务提供商都在努力加强其服务的安全性，而对于用户而言未必能理解其在使用、管理和监控云计算服务过程中可能涉及的安全问题。不安全的接口设置会让企业陷入许多安全问题，影响其机密性和可用性。

3.2.4 恶意的内部行为

大多数企业都被内部恶意人员的问题所困扰，在云计算环境下，这种威胁进一步增加。在此场景下，所有 IT 设备或数据被集中管理，内部人员拥有的权限能够让其获取敏感数据甚至整个云计算服务平台的完全控制权，并且难以被发现。Verizon Business 最新一次的数据泄漏调查报告（DBIR 2013）显示，48%的数据

泄漏都是由恶意的内部人员引起的。云计算的服务模式使得有权限、有能力接触并处理用户数据的人员范围进一步扩大。这种访问范围的扩大，增加了恶意的内部员工滥用数据和服务，甚至实施犯罪的可能性。

对企业存在威胁的恶意内部人员可能是那些有进入企业网络、系统、数据库权限的在任或离任员工，第三方服务提供商或者其他业务伙伴，其任何的恶意行为都有可能导致企业系统和数据的机密性、完整性和可用性受损。如果恶意内部人员为系统管理员，他们拥有访问企业敏感信息和关键领域的权限，一旦信息被破坏或者毁灭，内部人员就可以获取关键的用户档案和数据库并且删除数据，引入病毒、蠕虫或者引入逻辑炸弹来破坏或擦除数据。因此，由云服务提供商进行安全管理的企业系统都面临着巨大的安全风险。

用户的核心数据在云计算环境中的存储，离不开管理员的操作和审核。如果云服务提供商内部的管理出现疏漏，将可能导致内部人员私自窃取用户数据，从而对用户的利益造成损害。例如，商业秘密、工程文件、财务数据、客户数据和许多其他有价值的资产可能被复制，并出售给出价最高的人或者任何地方的人，这种情况仅仅通过廉价的 USB 闪存即可做到。

另外，错误的指令也会对用户系统、服务和数据产生负面影响。例如，一个操作员或者技术人员可能会收到特殊服务的命令，或者可能是更新特定服务的命令，由于缺乏培训输入了错误的命令，以至于意外地访问了错误的用户数据库，甚至损坏整个数据库。

3.2.5　云计算服务滥用或误用

目前，出于市场的考虑，为了使更多的用户使用云计算服务，云服务提供商对登记流程的管理不是很严格，任何一个持有信用卡的用户都可以注册和使用云

计算服务，云计算服务很容易获得且租用费用低廉。因此，云计算服务很容易成为滥用或误用服务的温床。攻击者能以很低的成本租用海量的云计算和宽带资源进行分布式攻击，例如，利用云计算平台发送大量垃圾邮件、制造或托管恶意代码、大规模的破解密码、实施拒绝服务攻击、制造及管理僵尸网络等。

云计算的明显特点是可以让很小的企业使用很大数量的计算资源。对于很多企业来说，他们不能购买大规模的服务器，但可以使用成百上千个云计算服务器的资源。但是，并非所有用户都能正确良好地利用这些资源。如果攻击者想破解一个密钥，使用自己的台式机可能需要好几年，而借助云计算的强大计算能力，可能数分钟就能搞定。

此外，攻击者可以窃取合法用户的证书，能够窃听用户的活动与交易，修改数据，返回伪造信息，并把用户重定向到不合法的站点，即出现云计算中合法账户或服务被劫持的情况。这样，云计算环境即成为攻击者强大的攻击平台和有利可图的活动场所。

目前，多数企业和网络运营商部署的流量清洗系统都很难抵御来自云计算的攻击和破坏。如有报道指出，亚马逊 EC2 被用于 Zeus 僵尸网络、InfoStealer 木马、微软 Office 与 Adobe PDF 的漏洞攻击等恶意代码的托管。2011 年 4 月，攻击者利用亚马逊 EC2 服务对索尼的 Play Station Network 及 Online Entertainment 服务进行攻击，导致这些网站多次长时间下线，大量用户的私人信息被泄露。

3.2.6 管理或审查不足

3.2.6.1 身份认证管理薄弱

传统的网络安全模型中，针对网络终端用户的安全接入和访问控制已有成熟

的解决方案，但是在云计算环境下，对云端用户的安全接入和访问控制出现一些新的要求，特别是在基础设施即服务的模型中，云服务提供商需要为每个用户提供自助服务管理界面，并针对不同企业或类型的租户提供差异化的用户身份认证管理授权策略，以确保合法的用户访问正确的服务器。动态的云计算资源及访问资源的海量用户和服务，为身份基础设施服务的可扩展性、自动化和可用性需求带来挑战。同时，云服务提供商也需要在用户访问行为的日志记录和安全事件的报告分析方面提供差异化的解决方案，参与该解决方案的用户认证网关、AAA 认证授权平台在相关的多实例和多域支持方面要有更加严格的要求。薄弱的用户验证机制，或者单因素的用户密码验证都可能产生安全隐患，而云自助服务管理门户的潜在安全漏洞也将导致各种未经授权的非法访问，从而产生新的安全风险。

同样在典型的安全管理模式下，业务系统通常部署在服务提供商可监控的范围之内，服务提供商通过虚拟局域网、入侵检测系统、入侵防护系统及多因素身份认证等网络安全控制手段，对网络和系统进行安全访问。而在云计算环境下，云计算的多层服务模式使得云服务提供商的网络和系统迁移到其他服务提供商的监控范围内，这种控制权的丢失，对云服务提供商已有的信任管理和控制模式形成了巨大挑战。

此外，云服务提供商目前所支持的身份认证管理实践和标准不足，随着网络边界的持续消退，在保护用户知识产权和敏感信息及保持合规性等方面，云服务提供商面临更大的风险。

3.2.6.2　安全管理缺失

云计算服务安全管理的范围将随着服务交付模式、提供商能力和成熟度的变化而变化。用户必须在灵活性与服务提供商提供的控制这两者之间进行权衡。服

务的灵活性越强，用户在服务中实施的控制就越多，同时也带来更多额外的安全管理责任。

目前，用户主要依靠云服务提供商的安全服务来测量和管理云计算中服务的安全性和可用性。但不幸的是，云服务提供商往往对标准的支持不足，在虚拟环境中监控功能也比较弱，从而增加了云计算服务管理的难度。

对于大型用户，特别是成熟的企业用户来说，主要的安全威胁就是管理复杂系统与安全风险。当企业用传统的方式管理本地系统，其往往倾向于分解基本组织部分，如网络、防火墙、存储结构、计算服务器、灾难恢复等，并识别每部分的风险大小和类型。这种对基础设施的分析方式总体上具有很大的透明度。但是，当企业转向云计算时，分析的复杂事物和安全风险等因素的职能将交给云服务提供商，这对透明度来说具有一定的潜在影响，同时也将影响企业复杂事物和风险管理的总体策略。企业已有的系统化解决方案可能无法延伸至云服务提供商。由于大多数云服务提供商的企业级访问管理功能缺失，在服务水平协议、提供商管理功能、安全责任等领域缺乏透明度，即使企业有能力在基础设施层安装系统可使用的检测探针，但受到资源瓶颈的限制也可能无法为企业提供深入分析所必要的信息，因此企业的云计算管理功能将是个持续的挑战。

随着云计算的广泛应用，用户的网络、系统、应用程序和数据等大部分资源将移交云服务提供商控制。云计算服务交付模式将创建具有虚拟边界的计算云，以及由用户与云计算服务提供商共享责任的安全模型。这种模型在可用性、访问控制、漏洞和安全补丁及配置管理方面，给云服务提供商的运维管理带来了新的安全挑战。云服务提供商在运行维护过程中，需要对整个云计算系统的服务器、存储、网络等资源进行运维管理。在整个过程中，任何违规问题都可能对用户的应用造成损害。例如，由于配置方面的疏忽造成用户的虚拟化计算资源不足以正

常运行业务系统，或者由于网络安全的配置错误导致互联网连接不通，甚至由于提供商对公共安全风险（如拒绝服务攻击）的防护不足导致用户对外的业务交付出现故障等。

另外，云计算服务集成了互联网的内容服务、数据存储、内容分发等业务，并扩大了经营范围。但根据目前的电信分类方法，无法简单地将云计算定位为某一类电信业务，更无相应的配套安全监管要求。同时，当前云计算服务发展参差不齐，大到政府投资建设，规模达数十亿的云计算中心，小到某一智能终端厂商开发的云计算软件商店，但无论是政府还是监管机构都没有对其制定任何规则和管理要求，这给云计算系统的安全隐患预留了发展空间，一旦发生类似于亚马逊瘫痪的事件，将给企业和用户带来不可估量的损失。

3.2.6.3　调查审计困难

在云计算被广泛应用的情况下，其提供的计算、存储、带宽等资源及服务可在全球范围内获取，而非法用户提供的账户信息可能是伪造的，并可以使用盗窃的信用卡进行支付，这就给调查网络犯罪分子带来前所未有的困难。对于第三方资源提供商租用给云服务提供商的资源，溯源将更加困难。同时，不同国家和地域有关云服务提供商的法律法规不尽相同，对各种违法行为调查和溯源的取证需求各不相同，也会给违法行为的取证带来阻碍作用。另外，云计算系统中存储有大量用户的数据，在调查取证过程中，云服务提供商未必配合，其可能有权拒绝提交所托管的数据；即使配合，也将给其他用户的业务带来安全风险。例如，谷歌多次向美国政府提交维基解密志愿者的邮箱数据，这意味着 Gmail 的用户存在隐私被泄露的风险，甚至在资质审计的过程中，云服务提供商未必提供必要的信息，使得第三方机构不一定能对服务提供商进行准确客观的评估。

一般而言，虽然用户将数据控制权交给云服务提供商，但服务水平协议中不可能详细指明服务提供商对各安全问题的承诺，用户仍然会委托第三方安全服务机构对网络信息安全的相关事宜进行安全审计、安全评估及安全认证。而在云计算环境下，由于用户根本不知道其数据存放的位置，因此很难实施安全审计、评估及认证，云服务提供商也可能不会配合用户自身发起的安全审计与评估；其次，云服务提供者即使委托第三方进行相关安全审计，其结果也未必能适用于各个用户；同时，云计算环境下用户信息设施的安全审计、评估及认证方法，目前尚在研究之中。

3.2.7 共享技术存在漏洞

云计算具有资源池化的特点，云服务提供商要交付规模化的服务，就要共享基础设施、平台和应用程序，因此多租户与资源共享是其重要特征。管理程序、共享平台组件、共享应用程序等共享技术所存在的安全漏洞远比用户行为更危险，因为这种问题可能将整个系统的弱点暴露给攻击者，这些风险可能会使整个云计算系统瞬间瘫痪。组成这些基础设施的组件设计，如果没有针对多租户架构（IaaS）、重部署平台（PaaS）或多客户应用程序（SaaS）的有效隔离机制，那么所有的服务模式都将面临威胁。例如，云计算中使用的硬盘分区、CPU 缓冲等机制，以及为了保证动态的可扩展性，云计算中的计算能力、存储与网络资源在多用户间共享，这些都难以保证良好的隔离性。这种风险会导致云计算系统中非法用户的恶意行为严重影响同环境下其他用户的声誉，或者攻击者能对共享环境下其他用户的数据进行非法操作。例如，2009 年，由于发现有大量垃圾邮件发出，反垃圾邮件组织 Spamhaus 把亚马逊整个美国的 EC2 平台的 IP 地址均列入黑名单。

另外，云计算资源的虚拟池化使得传统的安全策略无法管理到每个虚拟机及虚拟网络，因而传统的基于物理安全边界的防护机制难以有效保护基于共享虚拟机环境下的用户应用及信息安全。虚拟化使得安全访问控制、认证和授权更加困难，从而使得恶意代码的传播和感染变得相对容易。攻击者可利用虚拟机管理系统自身的漏洞，入侵到宿主机或同个宿主机上的其他虚拟机。事实上，针对虚拟层 Hypervisor 的安全研究已经被广泛重视，从 2007 年开始，主流的虚拟层 Hypervisor 软件屡有漏洞被报告。当前已有攻击者演示了基于虚拟机 Hypervisor 的 rookit 攻击，即 blue pill；2009 年黑客大会上的 Cloudburst 也演示了其能利用 VMware 中显示函数的漏洞实现对宿主操作系统的攻击。

3.2.8　未知的安全风险

由于技术发展的不平衡，以及云服务提供商和用户之间的信息不对称性，使得云计算用户处于大量未知的安全风险之中。一方面，用户选择使用云服务提供商是为了解放和优化自身的资源，因此没有必要甚至没有足够的资源去全面洞察云计算中的所有细节；另一方面，云服务提供商出于商业机密和安全的考虑，并不情愿分享所有的关键信息，即使是涉及与安全直接相关的事件。在这种情形下，未知的安全风险很容易造成那些完全不可能预测而实际确实发生的安全事件。例如，在 2012 年 8 月，《连线》杂志的记者 Mat Honan 的 iCloud 账户被黑，攻击者通过苹果和亚马逊的系统，把 Honan 的 iCloud 内容全部删除，并顺便把 MacBook 存储内容也全部清空。亚马逊和苹果的系统仅从各自的系统防范来说是没有问题的，然而通过综合两个系统所泄露的信息，攻击者就控制了 Honan 的苹果账户，所以没有人在系统设计之初就能预测到这样的攻击。随着云计算应用的日益复杂，这样的安全事件还可能发生。

3.2.9 法律风险

使用云计算可能不满足某些工业标准或法律规定的要求。例如，有些法规要求特定数据不能与其他数据混杂保存在共享的服务器或数据库上；有些国家严格限制本国公民的私密数据保存于其他国家；有些银行监管部门要求客户将数据保留在本国等。从某种程度上讲，使用公有云并不能达到支付卡行业安全标准的要求。亚马逊就曾告诫客户不要提供支付卡行业标准的服务，直到2010年底才声明其某些云平台已满足支付卡行业安全标准的合规性要求。

隐私的概念在不同国家、文化和管辖范围间差别很大。隐私主要是由公众期望和法律解释所形成的。隐私的权利或义务与个人数据的收集、使用、披露、存储和销毁方面相关。总体来说，隐私是关于企业对于数据所有者所负有的责任，以及关于机构对个人信息的业务活动的透明度。隐私倡导者对云计算提出了许多顾虑，这些顾虑通常混合了安全和隐私，同时也考虑了个人信息的访问、合规性、存储、保留、销毁、审计和监测及隐私侵犯等因素。究竟谁应为安全和隐私负责，有着相互冲突的意见。在全球范围内，针对数据隐私的法律与监管规定存在很大的差异，有的地方在严格执行，而有的地方却根本不存在有关数据隐私的法律与监管规定，对于跨国公司或那些在多个管辖区域为用户提供服务的公司而言，这可以说是令人却步的挑战。在不同的国家之间，这些法律的管辖范围的确是不同的。有些法律根据机构的位置，有些根据数据中心的物理位置，而有些根据数据所有者的位置。这种相互冲突的规定，进一步加剧了在全球背景下处理个人数据的挑战。在无数的跨辖区法律斗争、国际贸易障碍和长期的政治争端背后，都存在对隐私方面的不同态度。云计算对机构面临多种全球的有时甚至相互冲突的隐私章程、法规及指导方面提出了重大挑战。

云计算的应用地域性弱、信息流动性大，信息服务或用户数据可能分布在不同地区甚至国家，在政府信息安全监管等方面可能存在法律差异和纠纷；同时，由于虚拟化等技术引起的用户间物理界限模糊很可能对司法取证带来障碍。

3.3　云计算安全需求

本节从 3 个层面介绍云计算的安全需求。

3.3.1　国家的安全需求

（1）获取信息制导权

Google 提出要通过云计算成为世界的信息（数据）中心。如果云计算服务被 Google 等国外巨头垄断，这些垄断巨头及其背后的政治势力可以借此对我国进行远程监测和控制，并通过对用户整体情况进行统计分析，获取我国舆情动向和经济运行情况等重要数据，同时还可以有针对性地向我国推送反动有害等信息，这将对我国政治、经济、文化安全构成极大的威胁。因此，大力发展具有自主产权的云计算服务，占领信息指导权，防止国情信息被利用是我国首要的安全需求。

（2）国家机密防泄漏

云用户的密码丢失或者提供商的技术漏洞都可能导致国家机密的失窃或隐私的泄露，甚至攻击者利用云计算的强大计算能力去破解网上银行密匙、国防等机密部门的防火墙，或者利用云计算服务器进行拒绝服务攻击，上述描述都可能给社会、国防安全带来极大危害。

存储在云计算中的数据可能用于世界上的任何地方，其可能成为地区或者国家关于隐私和记录保存等数据存储法律的管辖对象。因此，我国应加大国家机密

的保护力度，防止隐私数据的泄露，并严格限制信息存储位置的范围。如欧盟国家的一些隐私管理制度禁止将某些类型的个人数据传播到欧盟以外的地区，这使亚马逊和其他公司只能提供使用位于欧盟内存储设备的服务。

（3）加强信息监管

近年来，云服务提供商的基础设施逐步呈现资源全球化、规模扩大化、访问透明化的特点。信息访问的透明化给信息监管带来了很大难题。在云计算环境下中，计算、存储和网络等资源是按需分配、可动态扩展的。云计算用户利用这些资源来发布信息或运营服务，信息与载体资源之间的结合关系是动态变化的，即由云计算平台自动调度资源来提供最高效率的服务，从而增加了有害信息定位和过滤封堵的难度。例如，Amazon EC2 提供的弹性 IP（elastic IP）机制，可以支持公网 IP 地址、域名与云节点的动态绑定，使得有害内容比翻墙软件等工具更容易绕过国家信息关防系统。

同时，云计算平台作为提供协作的服务平台，其允许用户任意上传文件，并且可控制与他人共享文件，为信息的传播提供了一个开放自由的空间，这也意味着共享的服务平台极有可能成为国家与企业商业机密泄漏的新渠道。境外云计算服务节点通常提供共享访问的 SSL 加密通道，除证书发行商名字、IP、端口外无法检测任何内容，使得大量有害信息散布在其中，并且能够穿透现有的国家信息关防系统。

因此，我国应提升国家信息关防系统的性能，并通过法律手段加强对信息的监管力度。

3.3.2 云计算服务提供商的安全需求

云服务提供商应具备如下安全能力。

1）云服务提供商应具有一种机制保证用户数据的可用性。

2）云服务提供商应具有一种机制保证用户数据不被泄露、不被破坏。

3）云服务提供商应具有一种机制对不同用户的数据进行隔离。

4）云服务提供商应具有一种机制保证用户数据被彻底清除，避免因恶意恢复而泄密。

5）云服务提供商应具有一种机制对用户的数据进行查找。

6）云服务提供商应具有一种机制保证云之间的可移植与互操作性，使企业与用户方便更换云服务商。

7）云服务提供商应具有一种严密、强壮的访问控制与身份管理策略。

8）云服务提供商应具有一种加密机制对网络传输中的数据、保存在磁盘或数据库中的静态数据进行保护。

9）云服务提供商应具有一种有效的密钥管理机制，保证云服务系统中数据机密性。

10）云服务提供商应具有一种机制区分用户并识别用户的非法行为。

11）云服务提供商应具有完善的容灾和备份体系，保证云服务系统的可用性。

12）云服务提供商应具有一种机制降低存储在云中的国家及企业信息的安全风险。

13）云服务提供商应具有一种机制对云平台的脆弱性进行检测和排查。

14）云服务提供商应具有一种机制对云平台的异常行为进行监控。

15）云服务提供商应具有一种机制在不侵犯用户隐私前提下，对用户数据进行操作。

16）云服务提供商应具有一种机制确保云服务基础设施中虚拟机间的隔离加固。

3.3.3 用户的安全需求

1）数据的安全存储及用户的隐私权保护是云计算用户最重要的安全需求。由于用户的数据及相关的用户名、密码等隐私信息存储在云计算系统中，怎样确保云服务提供商安全存储数据并不随意泄露用户隐私信息，是云计算用户首要考虑的安全问题。

2）用户参与的安全管理是云计算用户的另一个安全需求。

在保证不涉及其他用户信息和数据的前提下，不干扰云服务提供商的安全服务的基础上，为用户提供相应的安全配置信息和数据运行状态信息，并在某种程度上允许用户部署实施专用安全管理软件。

3）用户需要提供的云计算服务应该是稳定、可靠和持续的。

虚拟主机能够很好地在计算能力和主存储器访问上进行共享，但是数据输入/输出（I/O）的共享上却会出现问题，不同虚拟主机之间会相互影响，从而导致数据传输速度上比较大的波动。所有的云计算服务都在互联网上，一旦数据中心发生故障，影响面是巨大的。

3.4 小结

云计算技术是一把“双刃剑”，它在改变 IT 格局的同时，也带来了新的安全问题。一系列的安全事件表明，云计算技术面临了前所未有的安全挑战，安全问题成为云计算发展的障碍。为了推动云安全的发展，云安全联盟 CSA 在 2013 年了发布《2013 云计算 9 大安全威胁》报告。根据该报告，结合多年的云安全实践，本章深度分析了云计算面临的具体的安全威胁，以期对云安全关键技术的研究和发展具有借鉴和指导意义。最后给出了云安全需求，分析了国家、企业和用户对

于云安全的迫切需要，以期能够反映推动云安全发展的急迫性。

参考文献：

[1] Security guidance for critical areas of focus in cloud security computing V3.0[EB/OL]. http://www. cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[2] Top threats to cloud computing, V1.0, cloud security alliance[EB/OL]. http://cloudsecurity alliance.org/topthreats/csathreats.v1.0.pdf.2010.

[3] 张云勇, 陈清金等. 云计算安全关键技术分析[J]. 电信科学, 2010,(9):64-69.

[4] 宋筱宁. 面向电信的云计算平台安全关键技术研究[D]. 南京邮电大学, 2012.

[5] 沈军, 樊宁. 电信 IDC 云计算应用与安全风险分析[J]. 信息安全与通信保密, 2012, (11): 95-97.

[6] 刘彦. 云计算安全风险与对策分析[J]. 硅谷, 2013,(2): 132.

[7] 佟得天, 刘旭东等. 云计算信息安全分析与实践[J]. 电信科学, 2013, (2): 135-141.

[8] 李玮. 云计算安全问题研究与探讨[J]. 电信工程技术与标准化, 2012,(4): 44-49.

第4章 Chapter 4

云安全标准

云计算标准是云计算技术发挥其价值的必要前提，云计算标准化工作是推动我国云计算技术、产业及应用发展和行业信息化建设的重要基础性工作之一。但目前业界对于云计算的认识不统一，云计算定义多达十几种，其业务的开展形式、具体技术实现框架等缺乏规范的技术指导。

在云计算发展面临的挑战中，安全和隐私被排在首位。云计算安全被认为是决定云业务落地的关键问题，实现云计算安全技术、管理及运营的标准化是云计算业务能够获得广泛接受的重要基础。目前，众多标准组织和产业联盟都将云安全标准化视为重点工作，开始着手制定云计算安全标准，以求增强云系统的互操作性和安全性，减少运营成本。例如，国际通信标准化组织 ITU-T SG17 研究组、GSMA SG 工作组等都启动了云计算标准工作，而专门成立的组织，如云计算安全联盟也在云计算安全标准化方面取得了一定的进展。本章将对国内外标准组织当前的云安全研究情况进行介绍。

4.1 ITU 云计算安全标准工作进展

ITU-T 的中文名称是国际电信联盟远程通信标准化组织（ITU-T for ITU

Telecommunication Standardization Sector），它是在国际电信联盟管理下专门制定远程通信相关国际标准的组织。该机构创建于1993年，前身是国际电报电话咨询委员会（CCITT），总部设在瑞士日内瓦。

ITU-T于2010年6月成立了云计算焦点组——FG Cloud，其主要工作是从电信角度为云计算提供支持，焦点组运行时间截止到2011年12月，后续云工作已经分散到别的研究组（SG）。云计算焦点组发布了包含《云安全》和《云计算标准制定组织综述》在内的7份技术报告。

《云安全》报告旨在确定ITU-T与相关标准化制定组织需要合作开展的云安全研究主题。确定的方法是对包括欧洲网络信息安全局（ENISA）、ITU-T等标准制定组织目前开展的云安全工作进行评价，在评价的基础上确定对云服务用户和云服务供应商的若干安全威胁和安全需求。

《云计算标准制定组织综述》报告主要是对美国国家标准与技术研究院（NIST）、分布式管理任务组（DMTF）、云安全联盟（CSA）等标准制定组织在以下7个方面开展的活动及取得的研究成果进行了综述和列表分析，包括：云生态系统、使用案例、需求和商业部署场景；功能需求和参考架构；安全、审计和隐私（包括网络和业务的连续性）；云服务和资源管理、平台及中间件；实现云的基础设施和网络；用于多个云资源分配的跨云程序、接口与服务水平协议；用户友好访问、虚拟终端和生态友好的云。报告指出，上述标准化组织都基于各自目的制定了自身的云计算标准架构，但这些架构并不相同，也没有一个组织能够覆盖云计算标准化的全貌。报告建议ITU-T应在功能架构、跨云安全和管理、服务水平协议研究等领域发挥引领作用。而ITU-T和国际标准化组织/国际电工委员会的第一联合技术委员会（ISO/IEC JTC1）则应采取互补的标准化工作，以提高效率和避免工作重叠。

另外，ITU-T SG17 安全组也涉足云安全标准的研究，Q8 云安全子组重点研究云安全。ITU-T X.1600《云计算安全框架》从宏观的角度提出了通用的云计算安全框架，并分析了云环境安全威胁与挑战。

《云计算运营安全导论》为云计算服务提供商提供了云计算安全运营指导意见，内容包括 SLA 指导意见、云计算日常安全维护技术、管理要求等。

《SaaS 应用环境安全功能需求》提供了一个通用的面向 SaaS 应用环境的安全业务功能描述，该 SaaS 应用环境独立于网络类型、操作系统、中间件、供应商特定产品与解决方案，以及任何业务或特定模型（如网络业务、Parlay X 或 REST）。该标准描述了 SaaS 架构解决方案，并以此为基础实现了电信业务云 SaaS 的安全服务能力。

4.2 CSA 云计算安全标准工作进展

为推动云计算应用安全的研究交流与协作发展，业界多家公司在 2008 年 12 月联合成立了 CSA（云安全联盟）。该联盟是一个非赢利组织，旨在提供在云计算环境下最佳的安全方案，推广云计算应用安全的最佳实践，并为用户提供云计算方面的安全指引。自成立后，CSA 迅速获得了业界的广泛认可。现在，CSA 和 ISACA（国际信息系统审计协会）、OWASP（开放式 Web 应用程序安全项目）等业界组织建立了合作关系，很多国际领袖公司成为其企业成员。目前其企业成员中涵盖了思科、戴尔、Novell、VMware、RSA、Google、HP、Intel、微软、Oracle、AT&T、CA、McAfee、TREND、Symantec、NSFOCUS、3PAR 等国际领先的电信运营商、IT 和网络设备厂商、网络安全厂商、云计算提供商。

云计算安全联盟确定了云计算安全的 15 个焦点领域，每个领域都给出了具体建议，并从中选取较为重要的若干领域着手标准的制定，在制定过程中，广泛咨

询 IT 人员的反馈意见，获取关于需求方案说明书的建议。云计算安全联盟确定的 15 个云计算安全焦点领域分别是：信息生命周期管理、政府和企业风险管理、法规和审计、普通立法、eDiscovery、加密和密钥管理、认证和访问管理、虚拟化、应用安全、便携性和互用性、数据中心、操作管理事故响应、通知和修复、传统安全影响（商业连续性、灾难恢复、物理安全）、体系结构。

CSA 目前已经发布一系列云安全方面的资料，包括云安全指南，云安全首要威胁、云计算风险控制矩阵等。

CSA 在 2011 年 11 月 14 日发布的《云计算安全指南》v3.0 版本，着重总结了云计算的技术架构模型、安全控制模型以及相关合规模型之间的映射关系，从云计算用户角度阐述了可能存在的商业隐患、安全威胁及推荐采取的安全措施。同时还讨论了当企业部署云计算系统时面临的安全风险并且给出相应的安全建议。云安全指南指出，云安全应覆盖其完整的生命周期，并完成最佳实践及分析工具。在云安全完整的生命周期中，理想的云安全状态至少应该包括安全治理、识别、访问控制、数据保护及审核，最终实现安全即服务。除此之外，还分别从云治理和云运行的角度提出了 13 个部署云计算系统时需面对的安全“痛点”：即治理和企业风险管理、法律与电子证据发现、合规与审计、信息生命周期管理、可移植性和互操作性、业务连续性和灾难恢复、数据中心运行、应急响应、通告和补救、应用安全、加密和密钥管理、身份和访问管理、虚拟化等，如图 4-1 所示。

4.3　GSMA 云计算安全标准工作进展

2012 年 1 月举行的 GSMA SG（安全组）82 次全会上，中国联通成功牵头立项《云业务安全框架》，并获得编辑席位，同年 9 月 SG84 次全会上，中国联通顺

利完成此项目并向 SG 提交云业务安全框架终稿。本标准项目属于云计算及信息安全领域，是中国联通首次在国际标准组织牵头安全立项，为国内运营商首次在国际标准组织中牵头云计算立项，亦为首个获得 GSMA 永久文档编号的云计算及安全领域标准。

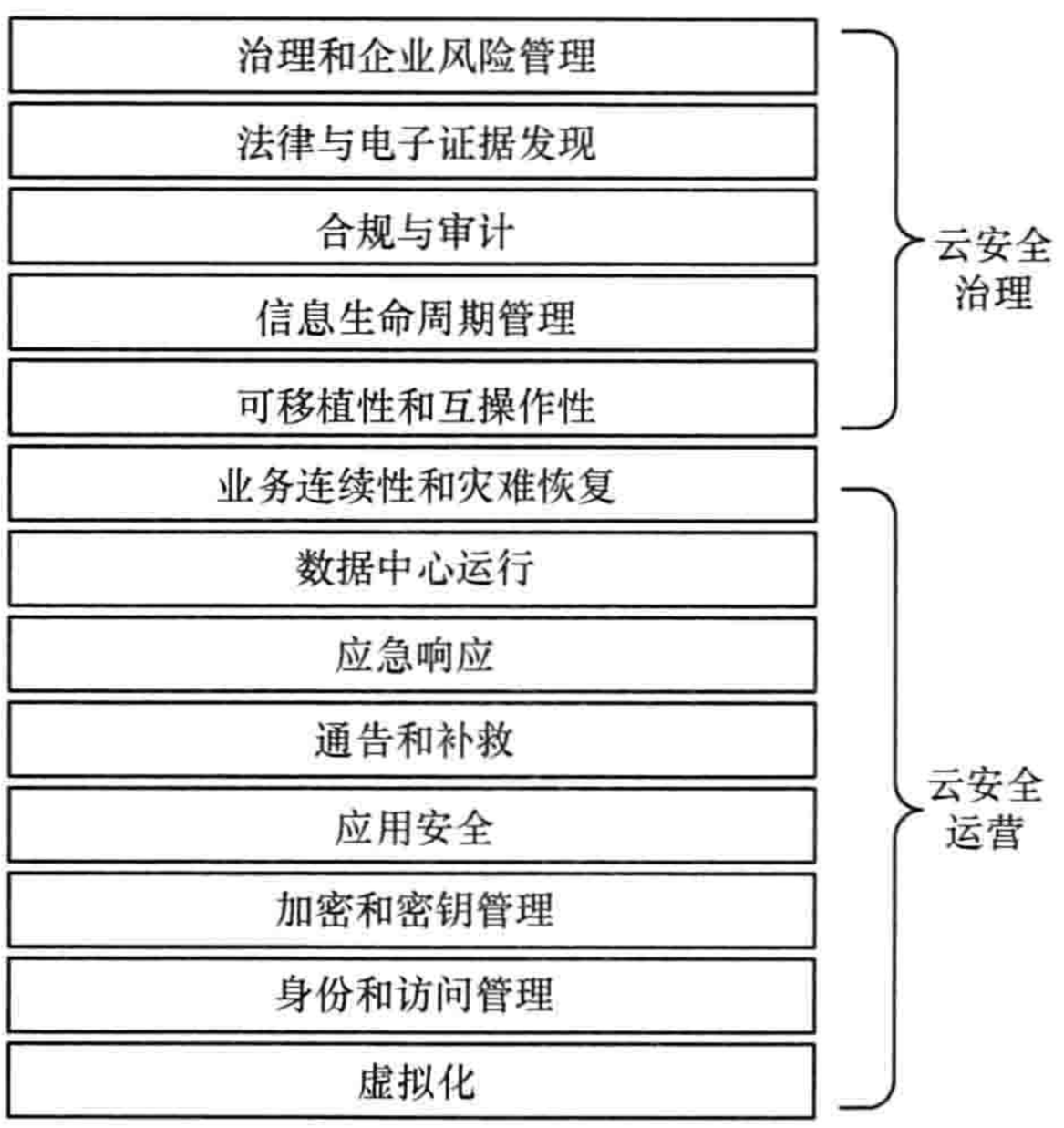


图 4-1　云安全治理与运营模型

此标准从运营商需求出发，从技术、运营、服务 3 个角度诠释了云业务安全，并提出基于移动环境下云业务安全框架及技术要求，这与其他国际标准组织 ITU、IETF、CSA、Oasis 的云计算工作不同，为中国乃至世界上的云计算安全服务标准化工作发展提供了重要的支持，该标准指导并构建了符合运营商云计算安全需求的技术内涵，有效提升了云基础设备及云业务平台的安全服务水平，降低了云计算系统安全威胁、提高了云服务连续性、保障了用户的信息安全，从而保障云业务的安全运营，树立起安全可信、稳定可靠、具有行业特征的云服务品牌。

4.4 OASIS 云计算安全标准工作进展

OASIS（organization for the advancement of structured information standards）是一个推进电子商务标准发展、融合与采纳的非盈利性国际化组织。

2010 年 5 月 19 日，OASIS 的国际标准组织成立了一个新的小组，致力于解决由云计算身份管理带来的严重的安全挑战。新成立的 OASIS 云身份（IDCloud）技术委员会将确定现有身份管理标准的差距，并研究当前标准实现互操作性所需的框架。委员会成员将根据收集的用例进行风险和威胁分析，并为缓解脆弱性提供指导。IDCloud 技术委员会将与包括云安全联盟和 ITU - T 在内的其他相关标准组织保持密切的联系。

OASIS 输出的云安全相关文稿有：

- Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare Version v1.0, November 2009；
- Cross - Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version v1.0, November 2009；
- SAML Security Assertion Markup Language V2.0, 2005-03；
- XACML eXtensible Access Control Markup Language V2.0, 2005-02；
- WS-Security policy V1.2, 2007-07；
- WS-Trust WS-Trust V1.3, 2009-02。

4.5 NIST 云计算安全标准工作进展

NIST（national institute of standards and technology）是属于美国商业部的技术

管理部门，其前身是 1901 年建立的联邦政府的第一个物理科学实验室。

NIST 主要为美国联邦政府服务，NIST 制定的云计算定义主要聚焦于云构架、安全和部署策略。NIST 的云计算标准化工作包括如下几方面。

（1）SAJAAC（标准加速，以大跨步推进云计算的采纳）

计划建立一个 Portal 和 Lab 团队，征求并公布建议的标准、最佳实践、互通建议、use case、可下载执行的云计算系统等，并根据 use case 和规范，对这些系统实现进行测试，发布测试结果和评价。目前，已经收集到 9 个实现系统，并期待更多。

（2）FedRAMP（联邦风险与授权管理程序）

美国联邦政府 CIO 办公室下面的项目，定义联邦的认证、鉴定、授权过程，NIST 是其中的技术顾问。

（3）NASA 的 Nebula 云计算项目：承诺将来开源。

输出文稿：

1）cloud-def-v15.doc, NIST definition of Cloud Computing Definition V15, 2009-10。

2）Effectively and Securely Using the Cloud Computing Paradigm Presentation V26, 2009-10。

NIST 云计算安全标准定位于为美国联邦政府安全高效的使用云计算提供标准支撑服务。迄今为止，NIST 成立了 5 个云计算工作组，出版了多份研究成果，由其提出的云计算定义、3 种服务模式、4 种部署模型、5 大基础特征被认为是描述云计算的基础性参照。NIST 云计算工作组包括：云计算参考架构和分类工作组、促进云计算应用的标准推进工作组、云计算安全工作组、云计算标准路线图工作组、云计算业务用例工作组。

云计算安全工作组是 NIST 为政府部门安全使用云计算所组建的必不可少的工作组，其成立之初的目标有 3 个。

1）从所有利益相关方（包括美国联邦政府和企业）中收集云计算服务中关于安全方面的担心。

2）分析/ 区分优先级妨碍美国联邦政府采用云服务所面临的障碍。

3）分析缓解这些障碍所有可能的使用方法。

随后调整增加了第 4 个目标：定义补充 NISTSP 500-293 中描述的参考体系架构和分类安全参考体系架构。

工作组目前主要的成果有：云计算安全障碍和缓解措施列表、草案《美国联邦政府使用云计算的安全需求》、《云计算安全体系架构》等。NIST 在云计算领域相关出版物如下：

- SP800-125《完全虚拟化技术安全指南》，2011-1；
- SP800-144《公有云中的安全和隐私指南》，2011-12；
- SP800-145《云计算定义》，2011-9；
- SP800-146《云计算梗概和建议》，2012-5；
- SP500-291《云计算标准路线图》，2011-8；
- SP500-292《云计算参考体系架构》，2011-9；
- SP500-293《美国政府云计算技术路线图》，2011-11。

4.6　CCSA 云计算安全标准工作进展

自 2011 年以来，中国通信标准化协会网络与信息安全工作组（CCSA TC8）承担了大量的云安全标准化工作。

“电信业务云安全需求和框架研究”项目，其研究范围为电信业务云环境的安

全需求和安全框架。需求研究包括电信业务云环境的通用安全需求和特殊安全需求。安全框架集成多种安全功能，以便在电信领域高效灵活地提供多业务云环境下的差异化安全保护。

“云计算应用与安全技术要求”项目，从云服务提供商的角度出发，对云计算安全运营需求和云计算安全运营框架进行研究，规范云计算安全运营技术要求，为云服务提供商开展安全运营提供指导和依据。

TC8 WG4 下设的云安全子组于 2011 年 9 月成立，其迅速成为国内云安全标准化工作研究基地，目前该子组承担的标准化项目如下。

1）“云存储服务安全技术及框架研究”项目，主要研究云存储服务安全技术与框架，并详细分析框架中的应用层、数据层、系统管理层和存储设备层上的服务安全关键技术。主要适用于各云存储安全平台的构建，对如何确保应用安全、数据安全，如何提高可信平台进行了详细研究。

2）“公共云计算基础设施即服务（IaaS）安全技术要求”项目，研究制定了公共云计算 IaaS 服务安全体系架构，分别从虚拟化安全、数据安全、平台安全、运营管理安全等方面规范公共云计算 IaaS 服务安全技术要求，指导 IaaS 平台及应用的安全建设。

3）“公共云计算安全即服务体系架构”项目，主要研究公共云计算安全即服务的定义和特征、应用模型及技术实现要求等内容，为云服务提供商开展公共云计算安全（即服务）提供指导和依据。

4）“云计算安全需求、风险与威胁体系”项目，从用户及业务角度梳理云计算的安全需求；从不同云类型（公有云、私有云及混合云）、具体云计算业务及网络场景、云计算各个层面（IaaS/PaaS/SaaS），全面梳理云计算平台/系统面临的安全风险和威胁；对安全风险及威胁进行分级，根据危害性大小和发生的难易程度

分等级。

5）“云的可信技术研究”项目，其研究内容包括：可信云体系架构研究，包括云对租户、租户对云及租户间的信任关系建立，攻克相关安全技术不完善或性能较低的问题；云计算环境的可信模型；用户隐私保护、数据隐私保护；云可信第三方审计；云运行环境可信等关键技术及其实现方案。

6）“公有云中隐私保护措施”项目，研究范围是云计算中公有云部署模型，专门针对云端隐私保护安全框架提供指导性建议，制定主要技术，其内容包括：隐私保护机制中的身份和访问管理、隐私保护机制中存储数据隐私保护、公有云中保护云隐私的云审计策略及隐私保护机制中立法及相关的法律制度。

7）“公有云安全基线研究”项目，主要技术内容包括云服务的架构安全、业务平台安全、基础设施安全、运维安全、管理安全、物理环境安全等方面的基线安全要求，涉及接入控制、身份认证和授权、信息保护措施、攻击防范、配置管理、安全审计、应急响应、风险评估等多个方面的安全控制点。

8）“基于云计算的互联网数据中心安全指南”项目，描述了基于云计算的互联网数据中心的安全威胁，提出了云计算数据中心安全体系架构，并规范了实现云计算数据中心的安全要求。此标准适用于基于云计算互联网数据中心的安全规划、设计和实现。

4.7 小结

国内外各标准组织与云安全相关的标准情况如表 4-1 所示，国际标准组织的云安全工作相对分散，这与其关注范围有关。总体来看，目前 NIST 在云计算、云安全定义及参考架构方面获得了普遍认可，而 ITU-T 则在云计算与电信网络结合、功能需求和参考架构方面较为深入，CSA 分别在计算虚拟化、云存储、云安

全方面输出的标准、规范、技术报告较为成熟，受到业界的广泛关注，而 Oasis、CCSA 等传统标准组织在云计算标准制定工作上也各有侧重。

表 4-1　各标准组云安全工作

标准组织	项目或议题	研究角度
ITU	云安全框架、云安全运营指导意见等 3 项标准	通信产业云安全建议
CSA	云安全指南、云安全威胁等近 10 项白皮书	ICT 产业界角度提供云安全实践
GSMA	云服务安全框架	移动运营商的云业务系统安全需求及实践
OASIS	围绕云环境下身份管理制定系列规范	云安全技术
NIST	云安全定义、云计算隐私等十余项出版物	云构架、安全和部署策略
CCSA	云计算应用与安全技术要求等几十项规范或研究课题	覆盖云安全技术、管理、运营的各个层面

值得注意的是，在国际标准组织的云安全工作半数为我国通信企事业单位（中国电信、中国联通、工信部电信研究院、中兴通讯公司等）牵头，这表明我国云安全国际标准化工作已处于领先地位。我国的通信标准化协会中云安全工作非常全面，尤其是 TC8 WG4 云计算子组成立之后，研究逐渐形成体系，随着云计算安全的需求、威胁、架构等问题的逐步明确，CCSA 云计算安全标准化工作可能会在未来取得较大进展，对国内的云计算落地起到重要的指导作用。

参考文献：

[1] MELL P. GRANCE T. The NIST definition of cloud computing[EB/OL]. http://csrc.nist.gov/groups/SNS/cloud-computing.

[2] ITU-T SG17:security[EB/OL]. http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx.

[3] Security guidance for critical areas of focus in cloud security computing V3.0[EB/OL]. http://www. cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[4] Top threats to cloud computing, V1.0, cloud security alliance, 2010[EB/OL]. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[5] Cloud computing security[EB/OL]. http://en.wikipedia.org/wiki/Cloud_comput ing_security.

[6] GSMA[EB/OL]. http://www. infocentre2.gsma.com.

[7] CCSA[EB/OL]. http://www.ccsa.org.cn.

第5章 Chapter 5

云安全关键技术

云计算已成为 ICT 产业发展的热点，云计算本质上是传统电信 IDC 增值业务的延伸和扩展，通过互联网对用户提供 IT 基础资源（包括计算、存储、网络、软件等）的按需租用，能够降低用户的 IT 运维成本，使得用户可以专注于自身业务。

云计算的发展带来了移动互联网网络资源、业务资源、用户资源在应用模式上的重大变化。多租户、资源共享、数据存储的非本地化、承载业务类型的多元化及网络带宽的快速增长不仅需要进一步强化传统的安全问题，同时也为移动互联网应用引入了新的安全问题。

因此，在云计算快速推进、广泛普及的同时，有必要重点对云安全技术进行系统研究，在云中引入更强大的安全措施；否则，云服务不仅无法控制，而且还将对国家、企业、用户带来严重的安全威胁。

5.1 云安全架构体系概述

在系统论述云计算安全技术之前，首先需要建立一个合理、完备的安全架构体系。在云安全构架的指导下，可以有效地部署各种云安全关键技术，以满足云

业务提供商、运营商、安全厂商、用户构成的云生态系统的安全需求，从容应对云环境下各种安全威胁。

根据之前章节对云安全的理解与认知，提出一个通用的云安全架构，在此基础上统领、组织本章后续的云关键技术，如图 5-1 所示。云安全架构分为用户域、云服务域、监管域共 3 个域。用户域涉及用户侧安全技术，包括云终端设备安全与云终端身份管理技术。云服务域涉及云服务侧安全技术，主要从 IaaS、NaaS（network security as a service，网络安全即服务）、PaaS、SaaS 4 个业务层级考虑安全关键技术的部署，由于云数据安全比较特殊，它贯穿了整个云服务域，需要从云服务域整体角度考虑予以论述。同时，本架构还构建了统一的云监管域，部署云监管相关安全技术，监控用户域与云服务域的运行情况。

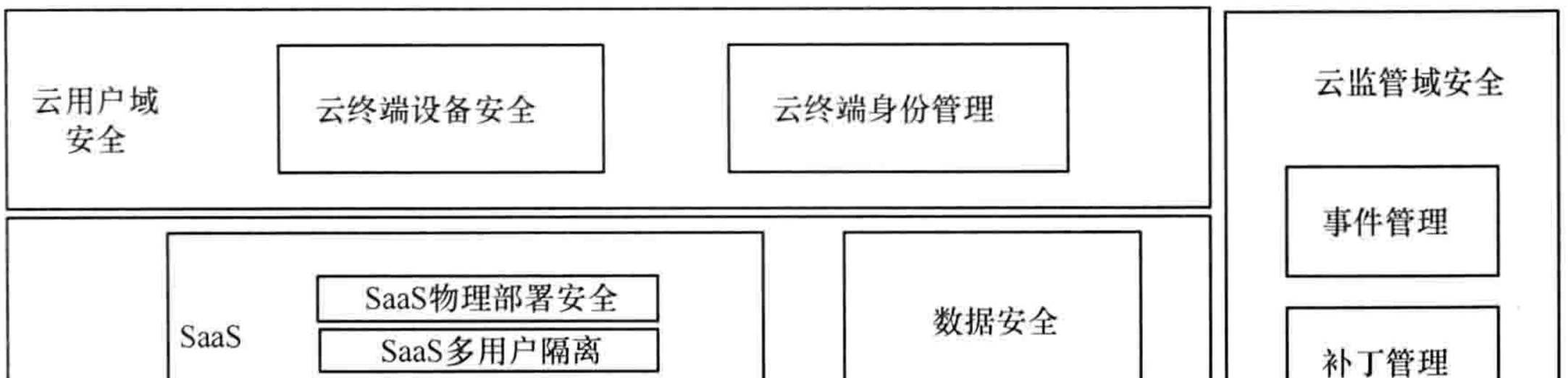


图 5-1　云安全架构

5.2 云服务域安全

本节描述的云服务域从 SaaS、PaaS、NaaS、IaaS 这 4 个层面展开讨论。由于云服务域中的数据安全比较特殊，所有层面均可涉及到数据安全。因此，本节将云数据安全单独作为一个子节进行论述。

5.2.1 IaaS 安全

云业务提供商利用虚拟化相关技术构建虚拟化服务器，可以大幅度提高物理服务器的运算效率与利用率。而虚拟化作为 IaaS 层面的核心技术，其安全问题不容忽视。本节 IaaS 安全从虚拟机自身安全与虚拟化软件（虚拟化管理平台）安全两个方面展开论述。

5.2.1.1 虚拟机安全

咨询公司 Gartner 预测，2014 年全球将有超过半数的服务器使用虚拟技术，如果不能解决虚拟机的安全问题，那么云计算基础设施层面临严重的安全风险。那么，虚拟机可能面临的典型安全问题如下。

1）虚拟机逃逸问题。虚拟化技术可以实现各种资源的按需、快速分配。在某些情况下甚至不需重启虚拟机即可分配硬件资源。随着虚拟化技术的普及，虚拟机的安全问题随之而来。看似独立运行的多个虚拟机，很可能位于同一物理主机上。传统物理机条件下，物理机上所有运行的程序可以彼此“看”到对方，如果具备足够的权限，它们可以相互进行通信。但在虚拟机环境下，由于虚拟化软件存在漏洞，导致虚拟机中运行的程序绕过底层进入宿主机中，这种现象被称为虚拟机逃逸。理论上讲，虚拟机逃逸是指攻击者突破虚拟机管理器（Hypervisor），获得宿主机操作

系统管理权限，并控制宿主机上运行的其他虚拟机。产生此问题的原因有：一是Hypervisor本身存在漏洞；二是虚拟机用户发起恶意攻击。若出现虚拟机逃逸的情况攻击者既可攻击同一宿主机上的其他虚拟机，也可控制所有虚拟机对外发起攻击。虚拟机逃逸的后果会使整个安全虚拟化模型完全崩溃，攻击者获取宿主机的绝对控制权。因此，虚拟机逃逸通常认为是虚拟机面临的最严重威胁。

2）虚拟机嗅探问题。虚拟机之间的嗅探对传统安全机制提出了新挑战。由于同一物理服务器上虚拟机之间不需要经过物理防火墙与交换机设备相互访问，使得攻击者可以利用简单的数据分组探测器，很轻松地读取虚拟机网络上所有的明文传输信息。然而，传统安全设备尚不能提供防虚拟机嗅探的安全防护手段。

针对上述安全威胁，下面将介绍4种虚拟机防护机制。

（1）虚拟机自身安全

为保证虚拟机自身的安全，一般采用的方法是在每台虚拟机上安装防火墙、入侵检测软件等，但这将造成资源的大量浪费。目前，业界流行的做法是在一个虚拟化系统中启用一个或多个独立的具有防火墙、入侵检测等安全功能的虚拟机，为其他业务逻辑虚拟机进行安全保护。以VMware vShield Endpoint为代表，该产品将重要的防病毒和防恶意软件功能部署到一个安全虚拟机上，节省了防病毒代理在虚拟机中占用的资源，从而提高系统性能。

虚拟机防护的另一种做法是在Hypervisor中部署虚拟防火墙，该方案将在下一节中详述。

在虚拟服务器环境中，几个虚拟机共享主机服务器上有限的物理硬件资源。如果其中的任何一个虚拟机过度消耗硬件资源，其他虚拟机则不能正常运行。为避免攻击者对单个虚拟服务器发动DDoS攻击，虚拟化系统需要对虚拟机进行全面的监控，并对单个虚拟机消耗的内存和CPU时间进行限制，避免任何一个虚拟

机过度消耗物理硬件的资源。

此外，可以采用虚拟化在线管理系统对虚拟机进行管理，对物理服务器及 Hypervisor 的运维操作应遵循运维相关流程，采用实时审计技术予以监控，并建立和完善各虚拟机的安全日志、系统日志和防火墙日志。虚拟机销毁及迁移以后，需要及时消除原有物理服务器上的磁盘和内存数据，使虚拟机无法恢复。对不需要运行的具有安全隐患的虚拟机要及时关闭。

（2）虚拟机隔离技术

物理资源共享使得虚拟机很容易遭受同一物理机的其他虚拟机的恶意攻击，因此有必要将各虚拟机进行逻辑或物理隔离。虚拟机的隔离程度依赖于虚拟化技术，在没有进行特殊配置的情况下，虚拟机之间并不允许相互通信。虚拟机之间的有效隔离，可以保证未授权的虚拟机不能访问其他虚拟机的资源，出现安全问题的虚拟机也不会影响其他虚拟机及虚拟机系统的正常运行。

为了实现虚拟机之间的隔离，可以根据业务属性、业务安全等级、网络属性等方式对虚拟机进行分类，目前流行的安全策略有 TCP 五元组（源 IP 地址、目的 IP 地址、源端口、目的端口、协议）、安全组（资源池、文件夹、容器）等；也可以从更小的颗粒度对虚拟机进行隔离，如将虚拟机与用户身份、业务逻辑标识或租户进行关联，能在虚拟化层识别各虚拟机所从属的用户、业务逻辑或租户，再根据相应的访问控制策略对其进行安全保护，从而增强安全功能；还可以通过 VLAN 的不同 IP 网段的方式进行隔离。对于一些运载如财务、商业机密等敏感业务逻辑的虚拟机，可以使用专用 CPU、存储、虚拟网络对其进行物理隔离。

（3）虚拟机迁移技术

为了实现资源的复用和性能的隔离，虚拟化技术将各种应用实例封装在不同的虚拟机中，从而运行在共享的物理硬件服务器上。但当这些服务器因为某种故

障瘫痪时，运行在服务器上面的虚拟机将一同遭殃。另外，在资源聚合过程中，如果没有合适有效的负载分配与调度算法，很容易导致服务器负载不均衡，使得部分服务器负载超过处理能力，而部分服务器负载远远低于处理能力。由此可能带来系统不稳定、服务质量降低等一系列问题。

采用虚拟机迁移技术不仅可以在某些服务器故障瘫痪时，将业务自动切换到网络其他相同环境的虚拟服务器中，以达到业务连续性的目的；而且可以实现负载均衡，从而提升系统整体性能。同时，迁移技术使得用户可以用一台服务器同时替代以往的多台服务器，从而节省了用户大量的机房空间及管理资金、维护费用和升级费用。迁移的优势在于简化系统维护管理，提高系统负载均衡，增强系统错误容忍度和优化系统电源管理。目前流行的虚拟化管理平台如 VMware、Xen、HyperV、KVM 都提供了各自的迁移组件。

可靠的虚拟机迁移技术是解决虚拟机安全问题的关键。因为可靠的虚拟机迁移安全机制能有效地保证虚拟机成功迁移。一方面，必须保证迁移过程的安全，特别是在线的迁移过程，如 VMware 的 vMotion 技术可灵活实现虚拟机的在线迁移，但其传输虚拟机内存的 vMotion 过程是非加密的，所以需要采取隔离措施，让所有 vMotion 事件发生在专有媒介独立的网络中。另一方面，还需保证迁移前后的安全配置环境一致。首先在虚拟机迁移之前，为确保虚拟机迁移目的平台的安全性和可靠性，可以先对虚拟平台进行远程认证和一致性检测等措施，从而确保虚拟机成功迁移和安全运行。其次，虚拟机对应的 VLAN ID 和 QoS 等网络层信息应一并迁移，外置防火墙上部署的安全策略也应进行迁移，具体可按照如下步骤进行。

第一，通过管理中心感知虚拟机的迁移过程，提取该迁移消息中的有效信息，并通过内部维护的网络拓扑关系等技术定位到新的防火墙。

第二，对于迁出服务器对应的防火墙产品的安全策略重新标记，使迁出虚拟机的相关安全策略不再处于激活状态。

第三，对于迁入的防火墙，将虚拟机所绑定或对应的安全策略组进行配置下发，以保证该虚拟机仍然可以得到和迁移前相同的访问控制权限。

最后，需保证虚拟机与服务器之间的认证、授权信息同步迁移。

（4）虚拟机补丁管理

虚拟化服务器与物理服务器一样需要补丁管理和日常维护。对虚拟机进行补丁修复，可以有效降低系统的安全风险。但是，随着虚拟机增长速度的加快，补丁修复问题也在成倍上升。虚拟机和物理机打补丁的区别是在于数量。例如，一个企业采用 3 种虚拟化环境（两个网络内部，一个隔离区），大约有 150 台虚拟机，这样的布置使得管理程序额外增加了功能用于补丁管理，而且当服务器成倍增长时，也给技术工程师增加补丁服务器数量带来一定压力。因此，虚拟化系统需要支持虚拟机补丁的批量升级和自动化升级，并加强对休眠虚拟机安全系统状态的监控。

补丁管理是系统化的工作，其实施的好坏直接影响组织的总体安全水平，而在整个实施过程中需要协调多方面的资源以及所有 IT 用户的关注和支持。其流程如图 5-2 所示。

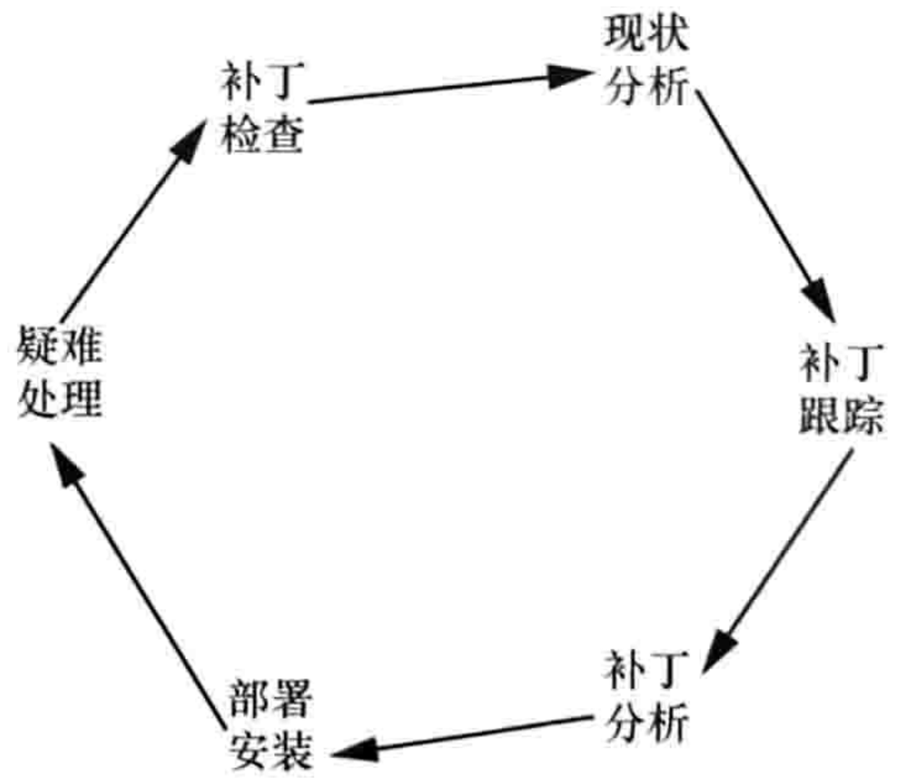


图 5-2　补丁管理

1）现状分析

补丁管理首先需要分析IT环境和信息资产重要登记，以便有针对性地跟踪组织所需要的补丁和应对措施。

IT环境：与系统管理员和网络管理员讨论确定组织的安全策略，当前使用的操作系统类型和版本、应用软件类型和版本、网络设备类型和版本以及相应的补丁版本等。

信息资产重要登记：了解组织的应用状况，掌握目前组织的重要信息资产，根据业务流程的重要程度，确定资产的价值度，然后根据软件版本、补救措施、业务空闲时间等确定打补丁的紧急程度和时间。

2）补丁跟踪

根据组织的IT环境跟踪对应软件的补丁，补丁的来源主要分为3类：软件厂商、安全机构和安全厂商。

3）补丁分析

分析漏洞影响：根据漏洞的威胁成因和严重性进行分析，制定相应的计划。

确定补丁的严重等级：根据厂商的安全公告和安全补丁信息，确定符合组织的补丁严重等级，制定补丁修补计划，包括修补时间和修补方式。

测试补丁：根据组织的实际应用环境进行补丁测试，判断该补丁在组织环境下的兼容状况。补丁测试需要遵从测试的广泛性和针对性，即在组织的实际情况下进行充分测试。测试环境需要包含组织的各种应用，尤其是关键应用，以判断补丁对关键应用的影响。测试补丁需要从安全可靠的地址获取补丁软件。如果在测试过程中发现问题，需要做详细的分析，判断发生问题的原因，并做及时的处理；如果不能解决则需要记录下发生该问题的环境，并进行重复验证；如果证实是该环境和补丁发生冲突，则反馈给厂商。

4）部署安装

补丁测试后，如果没有问题，需要根据紧急程度制定补丁分发计划，通常根据组织的环境分批安装，原则上资产价值大、威胁等级高的系统优先安装。确定顺序后，提交变更，相关人员进行补丁安装。

提交变更后，组织评审小组（包括安全专家、系统管理员等）对变更的必要性、风险和补丁推行计划等问题进行评审。评审通过后，由系统管理员和业务代表根据各系统业务的实际情况协商变更时间，确定变更计划。确定变更计划后，每个系统管理员各自提交变更请求进行系统变更，同时记录变更过程中提交的问题。

5）疑难处理

在补丁安装过程中，由于系统的多样性和复杂性，经常会发生很多问题。相关人员应时刻记录这些问题，并进行技术分析，以便尽快解决。对于能解决的问题，应尽快进行总结并编写 FAQ，以便在组织内部解决相同的问题。对于不能解决的问题可以分为两种情况。

① 不能安装补丁：此时需要确定临时的解决办法消除漏洞威胁，或者暂时接受当前的风险。

② 安装补丁后系统或应用不能正常运行：此时需要启用应急方案，采用备份系统或者卸载补丁。

同时，将这些不能解决的问题提交给厂商。

6）补丁检查

为了确定补丁的安装情况，需要对安装的系统进行检查。既可以通过工具进行全网检查，也可以通过漏洞扫描工具进行检查，通过编写的脚本进行检查或者人工抽查。

5.2.1.2　虚拟化软件安全

虚拟化软件层直接部署于裸机之上，提供能够创建、运行和销毁虚拟服务器的能力。主机层的虚拟化能通过任何虚拟化模式完成，包括操作系统级虚拟化、半虚拟化或基于硬件的虚拟化。其中，Hypervisor 作为该层的核心，应重点确保其安全性。

Hypervisor 是一种在虚拟环境中的元操作系统，其可以访问服务器上包括磁盘和内存在内的所有物理设备。Hypervisor 不但协调硬件资源的访问，同时也在各个虚拟机之间施加防护。当服务器启动并执行 Hypervisor 时，会加载所有虚拟机客户端的操作系统并分配给每台虚拟机适量的内存、CPU、网络和磁盘。Hypervisor 实现了操作系统和应用程序与硬件层之间的隔离，这样就可以有效地减轻软件对硬件设备及驱动的依赖性。Hypervisor 可以允许操作系统和应用程序工作负载在更广泛的硬件资源之上。Hypervisor 支持多操作系统和工作负载，每个单独的虚拟机或虚拟机实例都能够同时运行在同一个系统上，并共享计算资源。同时，每个虚拟机可以在不同平台之间迁移，实现无缝的工作负载迁移和备份能力。

目前，市场上有多种 X86 管理程序（Hypervisor）架构，其中 3 个最主要的架构如图 5-3 所示。

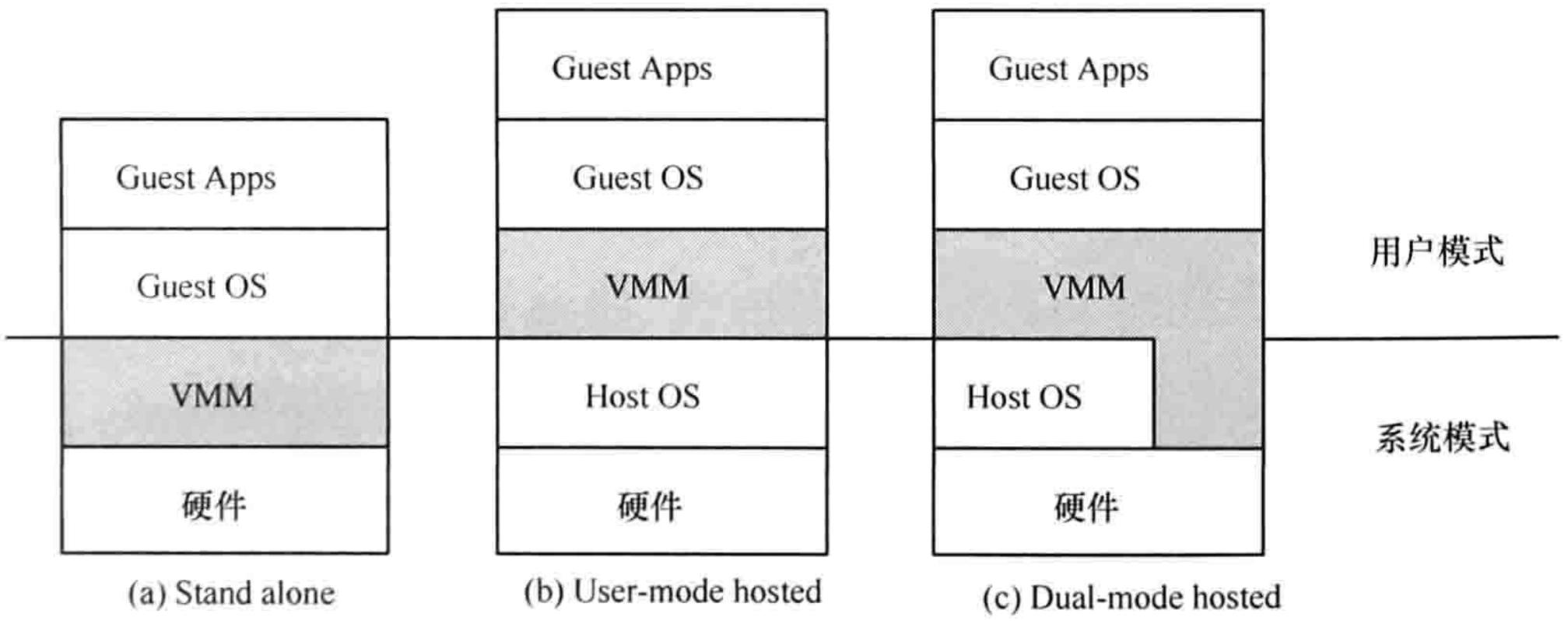


图 5-3　Hypervisor 架构类别

虚拟机直接运行在系统硬件上，创建硬件全仿真实例，被称为裸机型。

虚拟机运行在传统操作系统上，同样创建的是硬件全仿真实例，被称为托管（宿主）型。

虚拟机运行在传统操作系统上，创建一个独立的虚拟化实例（容器），指向底层托管操作系统，被称为操作系统虚拟化。

其中，裸机型的 Hypervisor 最为常见，直接安装在硬件计算资源上，操作系统安装并运行在 Hypervisor 之上。

正是由于可以控制在服务器上运行的虚拟机，Hypervisor 自然成为攻击的首要目标。保护 Hypervisor 的安全远比想象中更复杂，虚拟机可以通过几种不同的方式向 Hypervisor 发出请求，这些方式通常涉及 API 的调用，因此 API 往往是恶意代码的首要攻击对象，所以所有的 Hypervisor 必须重点确保 API 的安全，并且确保虚拟机只会发出经过认证和授权的请求，同时对 Hypervisor 提供的 HTTP、Telnet、SSH 等管理接口的访问进行严格控制，关闭不需要的功能，禁用明文方式的 Telnet 接口，并将 Hypervisor 接口严格限定为管理虚拟机所需的 API，关闭无关的协议端口。此外，恶意用户利用 Hyprevisor 的漏洞，也可以对虚拟机系统进行攻击。由于 Hypervisor 在虚拟机系统中的关键作用，一旦其遭受攻击，将严重影响虚拟机系统的安全运行，造成数据丢失和信息泄漏。

针对上述安全威胁，本节介绍 3 种虚拟化软件保护机制。

（1）虚拟防火墙

虚拟防火墙是完全运行于虚拟环境下的防火墙，它如同一台虚拟机，一般运行在 Hypervisor 中，对虚拟机网络中的数据分组进行过滤和监控。虚拟防火墙可以是主机 Hypervisor 中的一个内核进程，也可以是一个带有安全功能的虚拟交换机。

在 Hypervisor 中，虚拟机不直接与物理网络相连，通常只连接到一个虚拟交

换机上，再由该虚拟交换机与物理网络适配器连接。在这种类型的架构中，每个虚拟机共享物理网络适配器和虚拟交换机，这使得两台虚拟机之间可以直接通信，数据分组不通过物理网络，也不被硬件防火墙所监控。克服这种缺陷的最好方法就是创建虚拟防火墙，或者在所有的虚拟机上安装软件防火墙，以利用虚拟防火墙确保 Hypervisor 的安全。

（2）访问控制

访问控制是实现既定安全策略的系统安全技术，它通过某种途径显示管理所有资源的访问请求。根据安全策略要求，访问控制对每个资源请求做出许可或限制访问的判断，可以有效防止非法用户访问系统资源，以及合法用户非法使用资源等情况的发生。在 Hypervisor 中设置访问控制机制，可以有效管理虚拟机对物理资源的访问，控制虚拟机之间的通信。

虚拟化软件通常安装在服务器上。如果虚拟主机能够使用主机操作系统，那么该主机操作系统中不能包含任何多余的角色、功能或者应用。主机操作系统只能运行虚拟化软件和重要的基础组件（如杀毒软件或备份代理）。同时避免将操作系统加入到生产环境中，可以在专用活动目录中创建一个专门的管理域管理虚拟主机。该类型的域允许使用域成员的管理产品，而不用担心主机服务器被盗后曝光生产域。

目前，很多组织在虚拟机中部署了 vIDS/vIPS。vIDS/vIPS 可以通过分析网络数据或采集系统数据对虚拟机进行安全控制，其具有以下作用。

- 监视分析用户及系统活动；
- 进行系统配置和弱点审计；
- 识别反映已知进攻的活动模式并向相关人士报警；
- 进行异常行为模式的统计分析；

- 评估重要系统和数据文件的完整性；
- 进行操作系统的审计跟踪管理，并识别用户违反安全策略行为。

（3）漏洞扫描

针对虚拟化软件的漏洞扫描是加强虚拟化安全的一个重要手段，虚拟化软件的漏洞扫描主要包括以下几个方面的内容。

- Hypervisor 的安全漏洞扫描和安全配置管理；
- 虚拟化环境中多个不同版本的 Guest OS 系统的安全漏洞扫描，如虚拟机承载的 Windows（XP/2000/2003/Win7）系统、Linux（Ubuntu/Redhat）系统等；
- 虚拟化环境中第三方应用软件的安全漏洞扫描；
- 云计算环境下的远程漏洞扫描。

虚拟化软件的漏洞扫描系统逻辑结构如图 5-4 所示。

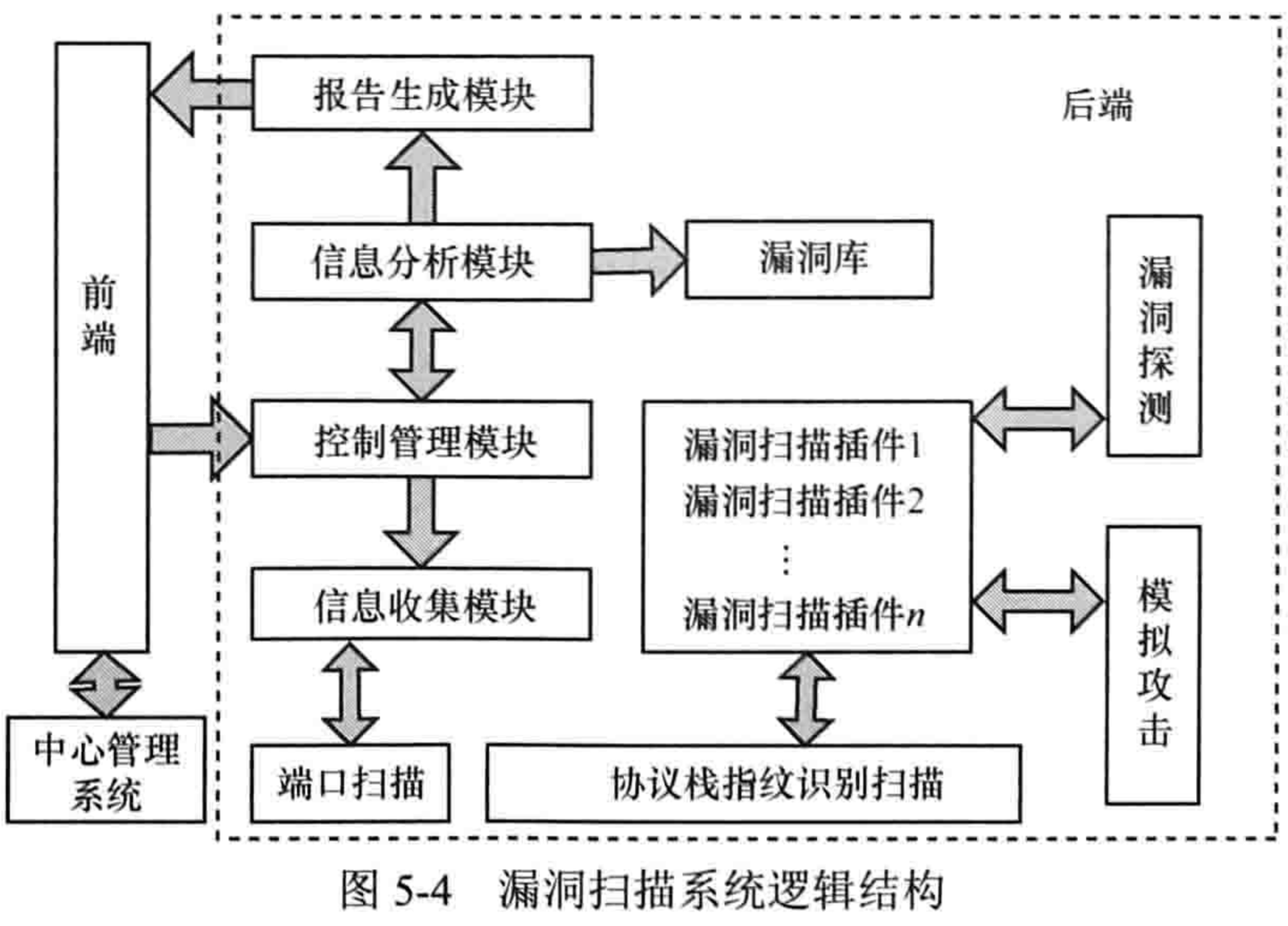


图 5-4　漏洞扫描系统逻辑结构

前端主要实现信息的传递通信。前端一方面将中心管理系统传递的用户请求和控制信息及时传至后端相应模块，另一方面又将扫描结果反馈至中心管理系统，双方通信主要通过调用 Socket API 来实现。

后端主要收集目标系统的基本信息，依据收集的信息调用相应的漏洞扫描插件完成漏洞扫描，并生成包括目标的弱点、漏洞危险级别及漏洞修补方法在内的漏洞扫描报告。后端的构成包含以下几个模块：控制管理模块、信息收集模块、信息分析模块、报告生成模块、漏洞库、漏洞扫描插件库等。

- 控制管理模块是后端的核心，主要功能有：接收前端传递的扫描请求，并从信息收集模块接收信息；调用漏洞扫描插件进行外部扫描和模拟入侵，将所有返回信息递交分析模块；分析模块与漏洞库信息进行比对，并将比对结果交至报告生成模块，由报告生成模块交至前端。

- 信息收集模块主要利用端口扫描与协议栈指纹识别等扫描技术从目标主机搜集相关信息，这些信息包括目标主机的开放端口和服务信息，以及其使用的操作系统类型和版本控制信息等；或者从主机内部利用系统管理员身份收集主机的安装及配置信息，包括安装的软件、补丁版本、文件属性设置等。

- 信息分析模块主要用于将收集的信息与漏洞库中的信息进行对比分析。

- 报告生成模块主要将信息分析结果以明确的方式进行显示，方便管理员查看。

- 漏洞库用于存放已知的安全漏洞数据，这些数据一般由各软件公司公布的漏洞信息和其他安全测试人员发现的漏洞信息组成。漏洞库中的数据以规格化存储，以便对其进行查询、增添、删除和修改等方面的管理及匹配原则的制定。

- 漏洞扫描插件库中的插件是信息收集或模拟攻击的脚本。每个插件封装成一个或多个漏洞的测试手段，用于对被测试的系统进行漏洞探测和模拟入侵。

另外，启用 Hypervisor 的内存安全强化策略，将虚拟化内核、应用程序及可执行组件存储在无法预测的随机内存地址中，可以使恶意代码很难通过内存漏洞利用系统漏洞。同时开启 Hypervisor 的内核模块完整性检查功能，以利用数字签

名确保由虚拟化环境加载的模块、驱动程序及应用程序的完整性和真实性。

5.2.2 NaaS 安全

在云环境中，云业务提供商在考虑诸多新特性所带来的安全挑战的同时，也不能忽视传统网络的安全问题。因此，云业务提供商需向用户提供网络安全即服务，系统地考虑 NaaS 安全技术。首先，云环境下，特别是公有云环境下，外部用户访问云系统需要部署统一的接入认证机制，以保证云系统的访问控制安全。其次，在某些场景下，特别是在私有云场景下，用户的接入物理位置与被访问的云系统位置可能相隔千里，为了保障用户在访问过程中实现端到端的安全，需要部署网络传输安全机制。最后，为了使云服务提供商更好地实时监控物理网络流量，防止异常流量攻击的发生，网络流量监控机制也需考虑。因此，在 NaaS 安全部分，本书将重点介绍上述三方面的内容。

5.2.2.1 统一接入机制

统一接入机制，即云用户身份管理及访问机制，指用户可以根据被统一分配的不同级别身份角色来访问云平台资源所涉及的流程、技术和策略。正确使用身份管理能够提高云系统的运营效率，还能满足云计算安全相关法规、隐私和数据保护等方面的安全需求。

统一接入机制包含以下几个功能。

（1）身份的有效管理

统一接入机制支持用户账号生命周期管理：用户身份管理要遵循账号的生命周期管理，该用户可以是外部用户、系统、管理人员。生命周期管理必须包括账号注册、角色权限分配、角色权限变更、账号删除全过程的管控。账号注册、变

更等均需有相应的审批过程。可以通过建立用户组，对用户进行集中的身份管理，为集中访问控制、集中授权、集中审计提供便利。

（2）密码及认证管理

- 该机制需建立统一的认证系统，提高访问认证的安全性，并对不同级别用户的密码进行系统管理，可根据云计算系统的安全策略来统一设定相应的密码策略，如密码长度、密码复杂度等。同时，云系统需支持密码同步服务和密码重置服务。

- 云系统支持主流认证方式，如 LADP、数字证书认证、令牌卡认证、硬件信息绑定认证、生物特征认证、多因素认证等，可按需撤销这些信任凭证。以上部分具体细节，如生物特征认证、多因素认证等关键技术将在 5.3 节云终端域详细讨论。

- 系统支持不同应用系统的单点登录，并可设置单点登录的最长会话时间、最长空闲时间、最长高速缓存时间等。

- 云系统支持对不同类型和等级的系统、服务、端口采用相应等级的一种或多种组合认证方式，以满足安全等级与成本、易用性的平衡要求。

- 云系统支持提供用户访问日志记录，记录用户登录信息，包括系统标识、登录用户、登录时间、登录 IP、登录终端等标识。

（3）访问授权

- 系统支持根据身份标识及访问策略（如角色或访问控制列表）访问系统资源。

- 用户账号访问授权精确到自然人，用户通过账号进行标识，每个用户一个账号，每个账号只属于一个人。

- 系统支持集中控制用户访问：根据用户、用户组、用户级别进行集中授

权和分级授权，控制用户可以执行的操作。

- 云系统支持访问策略制定：针对不同用户，对资源的访问权限进行策略制定；针对指定的资源定义相应的访问控制列表，并需要反映到虚拟化层，如虚拟机的 IP 地址和端口号、访问时间等。可借鉴的技术有 RBAC、ACL 等。

（4）审计

云服务提供商提供的云系统根据已定义的访问策略在企业或机构内对用户访问资源合规性进行及时的监控、审计。例如，支持用户账号权限的集中审计：用户账号集中审计能发现、阻止私设账号或账号逾期未收回，利用已经作废或假冒的账号进行登录尝试，试图利用合法账号访问未经授权的资源等非法行为。

（5）身份与访问管理 API

身份管理的功能要支持 API 的方式来实现，部署 API 安全受控机制，由云系统安全管理员操作云系统安全监控设备监控系统 API 访问受控行为，预防、阻止黑客操控恶意应用进行非法 API 攻击。

5.2.2.2 云环境下网络传输安全机制

云计算分布式的特性决定用户的物理位置与云系统资源所处的物理位置可能相隔较远，且通过公网或专网相连，而用户访问所获取的数据往往是企业的核心数据或者用户个人敏感数据，为了保证用户远距离访问云系统资源过程的安全性，需要部署云环境下的网络传输保护机制，典型技术如虚拟专用网络 VPN 机制。

VPN 指的是在公用网络上建立专用网络的技术。整个 VPN 网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台，如 Internet、ATM（异步传输模式）、frame relay（帧中继）等之上的逻辑网络，用户数据在逻辑链路中传输。

VPN 具备以下特性。

- 成本低。投资小，只需购买相关的 VPN 设备，并向本地 ISP 购买一定带宽的接入服务。
- 高可用性。通过购买 ISP 的宽带接入服务，部分维护责任迁移至 ISP。如果公网中的一个 VPN 节点不可用，可以使用公网的另外一个节点代替。
- 高安全性。通过加密技术使数据分组在公网上安全地传输，实现端到端的安全性。
- 高可扩展性。可从公网动态申请网络资源，进行 VPN 的动态扩展和维护，有利于保护投资，降低网络投资成本。

由于 VPN 在不安全的 Internet 中实现通信机制，需支持采用安全机制实现 VPN 的安全通信，如隧道技术、加解密认证技术、密钥交换技术等。

（1）IPsec

IPsec（IP security，IP 网络层安全标准）支持 IPv4 和 IPv6，可以“无缝”地为 IP 层引入安全特性，并为数据源提供身份验证、完整性检查及机密性保证机制。IPsec 为一组协议，包括安全协议及相关安全参数的密钥管理协议部分。它为数据源提供身份验证、完整性检查及机密性保证机制。

IPsec 在两个端点之间建立 SA（security association，安全联盟）进行数据的安全传输。SA 定义了数据保护中使用的协议和算法，以及 SA 有效时间等属性。IPsec 在转发加密数据时产生新的 AH、ESP 或（AH 与 ESP）附加报头，且被加密，附加报头和加密用户数据被封装在一个新的 IP 数据分组中；传输方式中，只是传输层（如 TCP、UDP、ICMP）数据被用来计算附加报头，附加报头和被加密的传输层数据被放置在原来 IP 报头的后面。

IPSec 提供了两个主机之间、两个安全网关之间或主机和安全网关之间的数

据保护。在两个端点之间可以建立多个 SA，并结合访问控制列表，使 IPsec 可以对不同的数据流实施不同的保护策略。由于 SA 是单向的，通常两个端点之间存在 4 个 SA，其中每个端点有两个 SA：一个用于数据分组发送，另一个用于接收。

（2）GRE

GRE（generic routing eucapsuluation），即通用路由封装协议，主要用于源路由和目的路由之间所形成的隧道。GRE 隧道通常是点到点的，即隧道只有一个源地址和一个目的地址。随着技术的进步，现在也有通过使用下一跳路由协议 NHRP 实现点到多点的 GRE 隧道。

在 VPN 的技术体系中，普通主机网络的每个点都可利用其地址及路由所形成的物理连接，配置成一个或多个隧道。在 GRE 隧道技术中入口地址使用普通主机网络的地址空间，而在隧道中流动的原始报文使用 VPN 的地址空间，这样就要求隧道的起点和终点作为 VPN 与普通主机网络之间的交界点。这种方法的好处是使 VPN 的路由信息从普通主机网络的路由信息中隔离出来，从而多个 VPN 可以重复利用同一个地址空间而没有冲突。

（3）加解密认证技术

为了保证数据在 VPN 传输过程中的安全性，不被非法用户窃取或篡改，一般都在 VPN 隧道的起点进行加密，在隧道终点再对其进行解密。

现在的 VPN 大都采用单钥的 DES 和 3DES 作为加解密和主要技术，而以公钥和单钥的混合加密体制（即加解密采用单钥密码，而密钥传送采用双钥密码）来进行网络上的密钥交换和管理，不但可以提高传输速度，还具有良好的保密功能。

认证技术可以防范来自第三方的主动攻击。用户和设备双方在交换数据之前，先核对彼此的数字证书，如果准备无误，双方再开始交换数据。用户身份认证最

常用的技术是口令认证，而网络设备之间的认证则需要依赖由 CA 所颁发的电子证书。目前主要的认证方式有：简单口令，如质询手验证协议 CHAP 和密码身份验证协议 PAP 等；动态口令，如动态令牌和 X.509 数字证书等。

（4）密钥交换技术

IKE 是指 IPSec 定义的密钥交换技术。它沿用了 ISAKMP 的基础、OAKLEY 的模式及 SKEME 的共享和密钥更新技术，从而定义出了自己独一无二的验证加密生成技术和共享策略协商技术。IKE 协议依靠对称密码体制、非对称密码体制和散列函数，提供了诸多的交换模式和相关的选项。

IKE 定义了通信双方进行身份认证、协商加密算法及生成共享的会话密钥方法。IKE 的精髓在于不在不安全网络直接传送密钥，而是通过一系列安全的数据交换，通信双方最终计算出共享密钥。

（5）访问控制技术

VPN 的基本功能是对用户实现访问控制。由 VPN 服务的提供者与最终网络信息资源的提供者，共同来协商确定不同用户对特定资源的访问权限，以此实现基于用户的细粒度访问控制，以实现对信息资源最大程度的保护。

访问控制策略可以细分为选择性访问控制和强制性访问控制。选择性访问控制是基于主体或主体所在组的身份，一般被内置于操作系统当中，而强制性访问控制则是基于被访问信息的敏感性。

5.2.2.3 云环境下网络流量监控

为避免网络攻击对云系统的危害，需要在网络行为分析的基础上，根据特定的安全策略对网络流量进行审计。审计的方法可以包括：关键字、关键协议、关键数据来源等。本节主要讨论物理网络的流量监控，关于虚拟机网络监控可参见

本章 5.2.1 小节 IaaS 安全。

网络流量审计主要使用深度包检测技术（DPI, deep packet inspection）和深度流检测技术（DFI, deep flow inspection）技术。

（1）DPI 技术

DPI 技术是一种基于应用层的流量检测和控制技术，可通过分光等方式检测网络数据流出入。当 IP 数据分组、TCP 或 UDP 数据流通过基于 DPI 系统时，该系统通过深入读取 IP 分组载荷的内容来对 OSI 7 层协议中的应用层信息进行重组，从而得到整个应用程序的内容。通过 DPI 技术分析 IP 报文中 4～7 层数据，识别业务类型、用户访问目标地址、用户接入方式、终端类型、位置等信息。

（2）DFI 技术

在网络行为分析过程中，DFI 技术可以作为 DPI 技术的补充。DFI 与 DPI 进行应用层的载荷匹配不同，采用的是一种基于流量行为的应用识别技术，即不同的应用类型体现在会话连接或数据流上的状态各有不同，并以此为特征量对流量进行识别。

5.2.3 PaaS 安全

PaaS 是把分布式软件的开发、测试和部署环境当作服务，通过互联网提供给用户。PaaS 可以构建在 IaaS 的虚拟化资源池上，也可以直接构建在数据中心的物理基础设施之上。PaaS 为用户提供了包括中间件、数据库、操作系统、开发环境等在内的软件栈，允许用户通过网络来进行应用的远程开发、配置、部署，并最终在服务商提供的数据中心内运行。PaaS 层面安全，需要关注以下几个方面。

5.2.3.1 PaaS 平台安全

PaaS 提供给用户的能力是通过在云基础设施之上部署用户创建的应用而实现的，这些应用通过使用云服务商支持的编程语言或工具进行开发，用户可以控制部署的应用及应用主机的环境配置，不需要管理或控制底层的云基础设施，包括网络、服务器、操作系统或存储等。

云服务提供商为保护 PaaS 层面的安全，首先需要考虑保护 PaaS 平台本身的安全。具体措施为：对 PaaS 平台所使用的应用、组件或 Web 服务进行风险评估，及时发现应用、组件或 Web 服务存在的安全漏洞，并及时部署补丁修复方案，以保证平台运行引擎的安全。同时，尽可能要求增加信息透明度以利于风险评估和安全管理，防止被黑客的攻击。

5.2.3.2 PaaS 接口安全

对于 PaaS 服务而言，它使客户能够将自己创建的某类应用程序部署到服务器端运行，并且允许客户端对应用程序及其计算环境配置通过各类接口进行控制。PaaS 接口范围包括提供代码库、编程模型、编程接口、开发环境等。代码库封装平台的基本功能如存储、计算、数据库等，供用户开发应用程序时使用，编程模型决定了用户基于云平台开发的应用程序类型，它取决于平台选择的分布式计算模型。

由于来自客户端的代码可能是恶意程序，如果 PaaS 平台暴露过多的可用接口，会给攻击者带来可乘之机。例如，用户通过接口提交一段恶意代码，这段恶意代码可能抢占 CPU 时间、内存空间和其他资源，也可能会攻击其他用户，甚至可能会攻击提供运行环境的底层平台。因此，PaaS 层平台的接口安全问题值得重点关注。

云平台接口安全是指如何保证用户可以安全地访问各种业务应用，同时避免

来自网络的攻击造成破坏。当用户或者第三方应用欲访问云平台中受保护资源时，需先与云平台认证服务器进行交互，利用自身携带的 access key 及相应的 access key ID 通过 API endpoint 进行认证授权。若认证成功，则可访问云平台中的受保护资源，或者云平台返回处理后的数据。同时，为防止来自网络的攻击，可以在云平台网元设备 API endpoint 处部署防止 DDoS 关键安全技术；为云平台设备 API endpoint 提供 SSL 保护机制，防止中间人攻击篡改、删除用户隐私数据。SSL 是大多数云安全应用的基础，目前众多黑客社区都在研究 SSL，PaaS 提供商应采取一定的技术手段来缓解 SSL 攻击。用户必须要确保有一个变更管理项目，在应用提供商指导下进行正确应用配置或打配置补丁，及时确保 SSL 补丁和变更程序能够迅速发挥作用。开发人员需要熟悉云平台的 API、部署和管理执行的安全控制软件模块。同时，必须熟悉平台特定的安全特性，这些特性被封装成安全对象和 Web 服务，通过调用这些安全对象和 Web 服务实现在应用内配置认证和授权管理。

5.2.3.3 PaaS 应用安全

PaaS 应用安全是指保护用户部署在 PaaS 平台上应用的安全。在多租户 PaaS 的服务模式中，最核心的安全原则就是多租户应用隔离。例如，云服务提供商需要在多租户模式下提供“沙盒”架构，平台运行引擎的“沙盒”特性可以集中维护部署在 PaaS 平台上应用的保密性和完整性，并监控新的程序缺陷和漏洞，以避免这些缺陷和漏洞被用来攻击 PaaS 平台和打破“沙盒”架构。同时，云用户应确保自己的数据只能由自己的企业用户和应用程序访问。

5.2.3.4 非关系型数据库安全

随着云计算的发展，云服务提供商除了考虑部署传统的关系型数据安全机制，

同时还需要重点考虑如何保障非关系型（NoSQL）数据库的安全。非关系型数据库存储了大量的视频、音频、图片等数据，可以快速处理海量数据，具有高并发性、高可扩展性等优势。由于 NoSQL 数据库具有分布式的特点，可以拥有多个服务节点。考虑 NoSQL 数据库的安全，需要从两方面考虑。

一方面，需要考虑数据库内部存储及服务节点之间的安全。主要考虑数据库内部的服务间访问、交互及数据库数据存储的安全问题，包括内部服务的访问控制、数据文件存储的保密性、完整性及内部服务的可用性等。

另一方面，需要考虑数据库客户端与服务端之间的安全。主要考虑客户端到服务端之间的访问及交互过程中涉及的安全问题，包括外部用户的访问控制、访问数据的加密传输、数据传输的完整性以及数据可用性等方面，访问控制通常比较重要，它又包括用户身份认证与授权两个方面。关于用户身份认证关键技术内容，可参见 5.3.2 小节云终端身份管理中谈到的用户身份关键技术。

谈及 NoSQL 数据库部署具体安全措施，以 HBase 数据库为例（HBase 是 NoSQL 数据库中安全特性最丰富的产品），可以进行安全策略部署，包括 Kerberos 认证机制、Coprocessor 机制、ACL 访问控制机制等。同时，对 NoSQL 数据库进行安全评估，可以从数据库的保密性、完整性、可用性三方面进行评估打分，使内部管理员了解目前 NonSQL 数据库的安全态势。

5.2.4 SaaS 安全

SaaS 其概念和用法刊登在 2001 年 2 月美国软件与信息产业协会发布的白皮书（《战略背景：软件即服务》）中。起初，Salesforce 公司将 SaaS 应用于客户关系管理行业。当时 SaaS 将应用软件统一部署在服务器上，用户根据自身的实际需求，通过互联网向其定购所需的应用软件服务，并按照定购服务的多少和时间的

长短向其支付费用。

在国内，八百客于 2006 年先后推出了全球首个中文 SaaS 在线企业管理软件平台和中文应用软件协同开发平台。目前国内主流的 SaaS 服务提供商有：八百客、天天进账网、中企开源、CSIP、阿里软件、友商网、伟库网、金算盘、CDP、百会创造者和奥斯在线等。

SaaS 模式与传统软件模式的架构存在显著的不同。传统软件模式是孤立的单用户模式，即顾客购买软件应用程序并安装在服务器上，服务器只是运行特定的应用程序，并且只对特定的最终用户组提供服务。SaaS 模式是多重租赁的架构模式，即在物理上很多不同的用户共同分享硬件基础设施，但在逻辑上每个用户独享所属的服务。多用户结构设计最大化了用户间的资源分享，但仍可以安全区分每个用户所拥有的数据。例如，一个公司的用户通过 SaaS 的客户关系管理（CRM）应用程序访问用户信息，这个用户所使用的应用程序实例能够同时为几十或者上百个不同公司的用户提供服务，而这些用户对于其他用户是完全未知的。

SaaS 模式的主要优点如下。

- 典型的 SaaS 部署通常不需要任何硬件就能在现有的互联网框架下运行，有时为了使 SaaS 应用程序运行更加稳定，只需更改防火墙的规则和配置。
- SaaS 的应用程序交付模式很典型地运用了以网络作为基础设施的一对多的交付方式。终端用户可以通过网络浏览器接入 SaaS 应用程序，甚至有些 SaaS 提供商提供其接口用以支持他们应用程序的独有特性。
- SaaS 模式使得用户可以把应用程序的管理运营外包给第三方（软件提供商或服务提供商），这样可以降低应用程序软件的软件许可、服务器及其他基础设施的开销，其中也包括内部应用程序运维人员的费用。
- SaaS 模式使得软件提供商得以控制和限制软件的使用，遏制软件的复制

和分发，促进其对软件所有衍生版本的控制。SaaS 的集中控制常常可以使得软件提供商或者代理商通过多个业务建立持续的收入，却不需要在用户的每个设备上都预装软件。

SaaS 安全主要包括 3 个方面，分别是物理部署安全、多用户隔离及业务的授权访问。

5.2.4.1　SaaS 物理部署安全

在 SaaS 模式下，用户的数据和资料等都保存在 SaaS 服务器端，服务器端一旦崩溃或存储数据的服务器遭到黑客攻击，这些数据的安全就会受到威胁。所以，物理部署的安全是保证 SaaS 安全的基本需要。

物理部署安全包括管理和技术两方面。管理方面的安全主要是服务器机房的环境安全，包括气体灭火、恒温恒湿、联网电子锁防盗、24 h 专人和录像监控、网络设备带宽冗余、口令进入机房等。技术方面服务器数据存储需要加密，网络传输需要采用安全的通信协议。服务器和防火墙的负载平衡、数据库集群和网络储存备份在近几年也成为必须采用的技术。

5.2.4.2　SaaS 多用户隔离

对于 SaaS 服务而言，解决 SaaS 底层架构的安全问题关键在于，在多用户共享应用的情况下如何解决用户之间的隔离问题。

解决用户之间的隔离问题可以在云架构的不同层次实现，即物理层隔离、平台层隔离和应用层隔离。

（1）物理层隔离

这种方法为每个用户配置单独的物理资源，以实现在物理上的隔离。用户不用

去担心服务器的地理位置和性能，不同的用户可以申请分配到属于自己的不同的服务器，那么用户之间数据就不会发生冲突，同时也达到了隔离的目的。这种方法是最容易实现，安全性较好，但也是硬件成本最高的，能够支持的用户数量也最少。

（2）平台层隔离

平台层处于物理层和应用层之间，主要是封装物理层提供的服务，使用户能够更加方便地使用底层服务。要在这一层上实现隔离，需要平台层能够响应不同用户的不同需求，把属于不同用户的数据按照映射的方式反馈给不同的用户，这样就能够达到隔离的目的。这种方式平台层会消耗较多的资源，实现数据和用户请求的映射，但硬件成本比物理层隔离方案低，能够支持的用户数量也比物理层隔离方案多。

（3）应用层隔离

应用层隔离主要包括应用隔离沙箱和共享应用实例方式。前者采用沙箱隔离应用，每个沙箱形成一个应用池，池中应用与其他池中的应用相互隔离，每个池都有一系列后台进程来处理应用请求。这种方式能够通过设定池中进程数目达到控制系统最大资源利用率的目的。

后者要求应用本身需要支持多用户，用户之间是隔离的，但是成千上万的用户可能使用同一个应用实例，用户可以用配置的方式对应用进行定制。这种方式具有较高的资源利用率和配置灵活性。

5.2.4.3 SaaS 业务授权访问

在传统的业务授权方式中，业务提供商负责整个业务提供过程中的全部工作，包括业务逻辑信息管理、业务资源存储、业务资源提供等。当用户向业务提供商申请某种业务时，业务提供商首先根据用户的用户名和密码等信息对用户进行身份认证，然后根据用户的权限信息对用户申请的业务进行访问控制，最后根据用

户的访问控制信息和业务逻辑信息调度业务资源，为用户提供业务。

而在云计算环境下，传统的业务授权方式具有明显的缺点。首先，业务提供商向用户提供业务的效率低。因为业务提供商需要从云服务提供商获取业务资源后，再向用户提供业务。其次，业务提供商的服务负载高。因为业务提供商需要首先调度业务资源，然后才能向用户提供资源。当用户数量庞大，业务提供商调度和提供资源的负载就会很高，这就需要增加业务提供商的资源投资，从而失去业务提供商利用云计算实现降低资源投资的意义。最后，用户访问业务资源的方式有限。因为用户只有通过业务提供商，才能获取相应的资源。

为了解决上述问题，云计算环境下的业务提供方式可以采用用户通过业务提供商颁发的凭证直接访问云计算服务提供商的方式使用户获取业务资源，而且这种方式还保护了业务提供商的用户信息。根据用户获取凭证内容的不同，用户有两种获取资源的方法。

1）用户从业务提供商获取的访问凭证包括业务资源信息、业务逻辑信息和访问控制信息等。用户可以通过此凭证直接访问云服务提供商，云服务提供商根据此凭证直接向用户提供业务资源。

2）用户从业务提供商获取的访问凭证包括业务资源信息，但不包括业务逻辑信息和访问控制信息。当用户通过此凭证直接访问云计算服务提供商时，云计算服务提供商需要首先根据此凭证向业务提供商获取业务逻辑信息和访问控制信息，然后根据业务逻辑信息和访问控制信息向用户提供业务资源。具体步骤如下。

- 用户向业务提供商申请资源信息，业务资源信息可为各类业务资源的 ID 等。
- 业务提供商根据用户申请，向用户提供相关资源信息。
- 用户向云计算服务提供商发送业务资源信息，请求访问业务资源。

- 云计算服务提供商确认用户请求中是否携带该资源的访问控制凭证。在没有凭证时，云计算服务提供商根据请求中携带的资源信息获取相应的业务提供商信息，并向该业务提供商发送资源访问控制请求，其中资源访问控制请求中携带用户的标识信息和业务资源信息。

- 业务提供商根据用户的标识信息对用户进行身份认证和访问控制，颁发该业务资源的访问控制信息给云计算服务提供商；资源访问控制信息包括业务资源授权信息。

- 云计算服务提供商对接收的资源访问控制信息进行认证，并向认证通过的用户提供相应的业务资源。

针对上述两类不同的方法，第一类方法的用户从业务提供商获取的凭证中包括权限信息，从而减少了云计算服务提供商获取权限的过程，因此访问业务的效率相对较高。而第二类方法的用户可以更灵活地使用业务，用户可以利用授权凭证随时随地使用业务。因为用户获取的凭证信息相对简单，存放、传输等要求低，并且云计算服务提供商向业务提供商获取用户的权限信息，减少了权限信息的传输环节，降低了权限信息被窃取的风险。

5.2.5 数据安全

传统 IT 系统中，数据的所有权和管理权是统一的，都属于用户本身。而在云计算环境下，最大的不同是用户需要把数据交给云服务提供商，造成数据所有权与管理权的分离。用户拥有数据的所有权，但是数据的管理权不再仅属于用户自己，云服务提供商可以管理和维护本属于用户的私有数据。

传统 IT 系统向云计算系统过渡时，传统的数据保护机制将遭到云计算架构的挑战，云数据在存储、使用及删除过程中都可能产生新的安全需求。云数据安

全的需求主要有如下几点。

- 云数据安全需要新的机制保证数据机密性；
- 云计算环境的用户数据共享底层架构，混合存储，需要有效的隔离机制；
- 云数据的冗余存储需要保证数据备份的一致性；
- 用户保存在云端的无用数据需要可靠删除。

云计算模式下，大量企业及用户数据集中在云中存储，如果缺乏安全保障，用户数据可能会被泄露或篡改，尤其是企业用户的数据，可能包含很多商业机密，用户数据可能包含敏感信息，如果泄露出去将给企业及用户造成重大损失，也必将影响云服务提供商的信誉，不利于云计算的发展和应用。

5.2.5.1　云数据加密

云计算环境中的存储数据可以分为两类：静态数据和动态数据。静态数据是指用户的文档、报表、资料等不参与计算的用户数据；动态数据是指需要动态验证或参与计算的用户数据。本节将从数据加密算法、密钥管理方案及安全基础设施三方面阐述静态数据加密机制。

静态数据的使用场景一般先进行加密，然后存储在云端。然而这种“先加密再存储”的方法可以有效地处理静态数据，并不适用于需要参与运算的动态数据，因为动态数据需要在 CPU 和内存中以明文形式存在。目前对动态数据的保护还没有成熟的方案，本节后续介绍的同态加密机制可以为读者提供参考。

（1）静态数据加密机制

1）数据加密算法

可选择的数据加密算法有两种：对称加密和非对称加密。对称加密算法是它本身的逆反函数，即加密和解密使用同一个密钥，解密时使用与加密同样的算法

即可得到明文。常见的对称加密算法有 DES、AES、IDEA、RC4、RC5、RC6 等。非对称加密算法使用两个不同的密钥，一个公共密钥和一个私有密钥。在实际应用中，用户管理私有密钥的安全；而公钥则需要发布出去。用公钥加密的信息只有私钥才能解密，反之亦然。常见的非对称加密算法有 RSA 以及基于离散对数的 ElGamal 算法、Rabin 算法等。

两种加密技术的优缺点如下：对称加密的速度比非对称加密快很多，但缺点是通信双方在通信前需要建立一个安全信道来交换密钥；而非对称加密无需事先交换密钥就可实现保密通信，且密钥分配协议及密钥管理相对简单，但实现速度较慢。

2）密钥管理方案

对于静态数据加密（如长期的档案存储），一些用户加密他们自己的数据然后发送密文给云服务提供商。这些用户控制并保存密钥，在需要的情况下解密数据。因此云服务提供商必须对用户的密钥进行保护。在存储、传输和备份过程中都必须保护密钥的安全，较差的密钥管理方案可能对加密的数据产生严重威胁。

密钥管理方案主要包括密钥粒度的选择、密钥管理体系及密钥分发机制。

密钥是数据加密不可或缺的部分，密钥数量的多少与密钥的粒度直接相关。密钥粒度较大时，方便用户管理，但不适合于用户密钥的更新。密钥粒度小时，可实现细粒度的访问控制，安全性更高，但产生的密钥数量大难于管理。

适合云存储的密钥管理办法主要是分层密钥管理，这种密钥管理体系就是将密钥以分层的方式存放，上层密钥用来加/解密下层密钥，只需将顶层密钥分发给用户，其他层密钥均可直接存放于云存储中。考虑到安全性，大多数云存储系统采用中等或细粒度的密钥，因此密钥数量多，而采用分层密钥管理时，用户或可信第三方只需保管少数密钥就可对大量密钥加以管理，效率更高。

可选择的密钥分发机制有：客户端方式、云存储密文分发方式和第三方机构分发方式。根据应用场景的不同，选择适合的密钥分发方式。

上述 3 种方式各有优缺点。客户端方式是用户自行管理密钥，安全程度高，但一旦用户下线，其提供的共享资源将无法被访问，因此该方式更适合私有云存储；云存储通过密文方式分发，充分发挥云存储的存储资源优势，可以随时提供数据共享，但密钥冗余量大，造成大量存储资源浪费；采用第三方机构分发，既安全又可随时共享数据，但对应用场景的要求高，适用范围小，更适于某种特定的应用。

建议云存储采用 2-3 层的分层管理密钥管理方式，并使用 PKI 体系中的公私钥算法为用户分发顶层密钥，分发方式采用客户端方式。

3）安全基础设施

为了保证数据的机密性，云服务提供商除了需要提供可靠的密钥管理方案外，还需向用户提供如下安全基础设施：CA 认证中心、签名服务器、安全网关、加密文件系统、硬件 USB Key 做强认证。

① 签名服务

CA 中心为每个用户签发证书（保存在 USB Key 内），同时管理用户证书。用户获取证书后即可通过签名服务进行强认证完成身份验证，杜绝用户因密码泄露导致身份被仿冒，进而防止敏感数据泄露。

签名服务可以访问 CA 认证体系中的加密机实现签名、验证签名功能。加密机可以提供高强度的 RSA 公私钥算法支持，也能提供各种对称算法支持，如 AES、3DES 算法。

② 安全网关

安全网关是安全操作的屏障，它与 USB Key 配合对所有登录用户进行强认

证，将非法用户拒之门外。远程客户端可以与安全网关建立安全的传输通道，把用户的私有数据安全地传送到云计算环境中。

安全网关主要功能包括：用户身份认证、安全文件传输、密码服务和安全审计。

③ 远程终端

用户远程终端采用 USB Key 作为用户身份识别。当用户要使用云资源时，首先在安全网关上认证。

终端要实现安全传输客户端功能，集成 FTP 等文件传输协议，并支持断点续传功能。

④ 加密文件系统

加密文件系统组件在指定的云计算应用节点通过与用户进行密钥交换得到文件加密密钥，采用这个密钥完成数据加解密，将解密数据用于计算，运算完成后将加密结果数据保存到本地磁盘或者远程文件服务器。用户数据无论是在 Internet 传输，还是在机群内部传输均是高强度加密的密文，能有效防止泄密的发生。

软件实现的文件加密算法在 I/O 轻负载时可以满足要求，但是 I/O 操作频繁，软件算法会成为性能瓶颈。因此，加密文件系统将支持访问硬件加密卡提供的密码算法服务，完成加解密运算。

每个用户可以有自己的加密目录，如果在共享文件服务器上，各个用户的加密信息是私有隔离的。也可以把文件设置成多个用户共享，有权限的用户都可以打开加密过的文件进行访问。

（2）动态数据加密机制

同态加密是基于数学难题的计算复杂性理论的密码学技术。这种技术可实现在加密的数据中进行诸如检索、比较等操作，得出正确的结果，而在整

个处理过程中无需对数据进行解密，因此这种加密机制比较适用于动态数据的场景。

同态加密的原理是对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。设加密操作为 E，明文为 m，加密得 e，即 e = E(m)，m = E'(e)。已知针对明文有操作 f，针对 E 可构造 F，使得 F(e)= E(f(m))，这样 E 就是一个针对 f 的同态加密算法。

同态加密技术是密码学领域的一个重要课题，目前尚没有真正可用于实际的全同态加密算法，现有的多数同态加密算法要么是只对加法同态（如 Paillier 算法），要么是只对乘法同态（如 RSA 算法），或者同时对加法和简单的标量乘法同态（如 IHC 算法和 MRS 算法）。少数的几种算法同时对加法和乘法同态（如 Rivest 加密方案），但是由于严重的安全问题，也未能应用于实际。2009 年 9 月，IBM 研究员 Craig Gentry 在 STOC 上发表论文，提出一种基于理想格（ideal lattice）的全同态加密算法，成为一种能够实现全同态加密所有属性的解决方案。虽然该方案由于同步工作效率有待改进而未能投入实际应用，但是它已经实现了全同态加密领域的重大突破。

5.2.5.2　云数据隔离

云计算采用多租户模式实现了可扩展性、可用性、可管理性并提升了系统运行效率，但其代价是用户数据的混合存储。虽然云计算应用在设计之初已采用诸如“数据标记”等技术以防非法访问其他用户数据，但由于应用程序漏洞，非法访问事件时有发生，典型案例如谷歌文件非法共享。虽然一些云服务提供商使用额外手段，诸如第三方应用程序的安全验证工具以加强应用程序安全，但从本质

上讲，在多租户环境下无法做到数据物理隔离，因此到目前为止还没有安全机制能确保用户数据绝对安全。

在这种多租户环境中，可采用 3 种已经比较成熟的架构实现云数据隔离，即共享表架构、分离数据库架构和分离表架构。

（1）共享表架构

共享表架构即所有的用户共享相同的数据库实例和相同的数据库表，但可以通过用户 ID 等字段来区分数据的从属关系。

由于共享表架构最大化地利用了单个数据库实例的存储能力，所以这种架构的硬件成本非常低廉。但对于程序开发者来说，却增加了额外的复杂度，因为多个用户数据共同存储在相同的数据库表内，这需要额外的业务逻辑来隔离每个用户的数据。此外，这种架构的灾备成本也会很高，因为这不仅需要专门编写数据备份的程序，而且在恢复数据时，需要对数据库表进行大量的删除和插入操作，一旦数据库表包含大量其他客户的数据，势必对系统性能和其他客户的体验带来巨大影响。

（2）分离数据库架构

分离数据库架构即每个用户独享各自的数据库实例。

相对于共享表架构而言，由于每个用户拥有单独的数据库实例，所以这种架构可以非常高效便捷地实现数据的分离和灾备，但硬件成本将非常高昂。

（3）分离表架构

分离表架构即所有用户共享相同的数据库实例，但每个用户独享由一系列数据库表组成的 Schema。

相对于共享表架构和分离数据库架构而言，分离表架构是一种折中的方案，在这种架构下，实现数据的分离和灾备比共享表架构容易，而硬件成本比分离数

据库架构低廉。

这 3 种架构根据软件系统客户如何使用数据库实例和数据库表进行划分。如果所有的软件系统客户共享使用相同的数据库实例和相同的数据库表（可以通过类似于租户 ID 字段来区分数据的从属）则为共享表架构；如果每个软件系统客户单独拥有自己的数据库实例则为分离数据库架构；如果软件系统客户共享相同的数据实例，但是每个客户单独拥有自己的由一系列数据库表组成的表结构，则为分离表架构。

3 种架构的优缺点比较如表 5-1 所示。

表 5-1　3 种架构优缺点比较

架构	优点	缺点
共享表架构	最大化地利用了单个数据库实例的存储能力，硬件成本低廉	多个客户的数据共存于相同的数据库表内，需要额外的业务逻辑来隔离各个客户的数据，实现灾难备份的成本也非常高
分离数据库架构	每个客户拥有单独的数据库实例，这种架构可以非常高效便捷地实现数据安全性和灾难备份	硬件成本非常高昂
分离表架构	折中的多租户方案，实现数据分离和灾难备份相对共享表架构更加容易一些，硬件成本也较分离数据库架构低	实现数据分离和灾难备份相对分离数据库架构更加困难一些，硬件成本也较共享表架构高

上述 3 种架构都有其优缺点，所以在设计云系统时，系统架构师需要进行全面的分析和考量，综合各方面的因素以选择合适的多租户架构。有一些选择方法可供参考，例如，系统服务的客户数量越多，则越适合使用共享表的架构；对数据隔离性和安全性要求越高，则越适合使用分离数据库的架构。而在超大型的云系统中，一般都会采用复合型的多租户架构，以平衡系统成本和性能，这其中 Salesforce.com 便是一个典型的案例。Salesforce.com 最初搭建于共享表架构，但是随着新客户的不断签入，单纯的共享表架构已经很难满足日益增长的性能要求，Salesforce.com 逐步开始在不同的物理区域搭建分布式系统。在全局上，

Salesforce.com 以类似于分离数据库的架构运行，在单个区域内，系统则仍然按照共享表架构运行。

5.2.5.3 云数据备份

数据冗余技术可以有效提升云计算系统安全性与可靠性。数据冗余技术简单来说就是将同一份数据产生多个备份，并将备份存储在不同位置的服务器上。云数据备份会发生副本数据和主版本数据不一致的情况，如主节点发生故障，主节点失效之后数据丢失，更新操作未能及时触发，那么副本和主版本就会发生数据不一致。

解决办法是通过基于版本号的备份策略实现云数据备份一致性，在数据更新之后，按照版本号排序的方法来保证数据备份的一致性。也就是说，为数据的每个版本设定一个版本号，当数据在某个服务器上崩溃时，通过多个版本的版本号来判定更新操作在几个服务器版本中的先后顺序，从而明确是否需要处理版本之间的冲突。举个例子，数据 X 存在 A、B 两台服务器上，在某一台服务器上，数据 X 发生了两次更新，分别产生两个版本：X1（A，版本号 1）和 X2（A，版本号 2），则只需备份版本号较大的版本即可。如果数据 X 在 A 上更新为 X1（A，版本号 1），在 B 上更新为 X2（B，版本号 1），则这两个版本是没有冲突的，存储系统应该调整 X1 及 X2 数据更新结果，保存最新版本 X3（A，B，版本号 1）。

5.2.5.4 云数据清除

用户将数据存放到云存储中，但这些数据是具有保存期的。通常，企业或者个人用户在存储某一数据到达一定的时间之后，会选择在云存储中删除该数据。但是，云存储中数据的实际管理者是云存储服务提供商，用户只能向云存储发送

一个“删除”的指令，而无法保证云存储是否真的将该数据彻底从其存储设备中删除。云存储的服务提供商完全可以留下该数据的一个或者多个复制，却告知用户该数据已删除。在这种情况下，如果用户的加密密钥又意外地泄露或者被窃取，那么该数据的隐私内容就会被云存储服务商获知。

对于这个问题，首先需要依靠具有法律约束的服务等级协议（SLA）来保障用户的隐私安全。SLA 是服务提供商和用户双方经协商而确定的关于服务质量等级的协议或合同，而制定该协议或合同是为了使服务提供商和用户对服务、优先权和责任等达成共识。服务提供商在该协议中应详细描述对用户数据的加密保护、使用的存储服务器及备份的数目，一旦用户的隐私数据泄漏，可以利用服务等级协议向法院上诉，从而保护用户的自身利益。

对于企业级别的机密数据，云计算运营商应当采用磁盘擦写、数据销毁算法及物理销毁等方法来对机密数据进行彻底清除。

同时，云存储提供商还应该构建相应的密钥管理中心，负责管理用来加密数据的控制密钥。根据用户的请求，密钥管理中心保存，返回或者删除控制密钥，从而使得用户能够更加安全可靠地使用云存储服务。

5.3　云终端域安全

云终端是指云用户使用的终端设备，包括服务器、桌面电脑、笔记本电脑、平板电脑、手机等。云终端是云计算的接入实体，也是云用户和云计算平台之间联系的纽带。云终端安全是云计算安全的重要环节，也是网络环境下信息安全的关键点。安全的云终端能够更好地保证云用户安全地接入云计算平台，同时减少了云计算平台受到非法访问和恶意攻击的可能性。目前，终端用户大量使用应用商店及互联网下载应用程序，其中很多应用都难以避免地存在安全漏

洞，这些漏洞加大了云终端用户被攻击的安全风险，进而危害云计算生态环境的安全。因此，云服务提供商应该采取必要的措施保护云终端的安全，从而在云计算环境下实现端到端的安全。本节将从云终端设备安全与云终端身份管理两方面展开论述。

5.3.1 云终端设备安全

首先，云终端设备在硬件方面需要采用安全芯片、安全硬件/固件、安全终端软件和终端安全证书等技术来提高云终端的安全性，并确保云终端设备不被非法修改和添加恶意功能，同时保证云终端设备的可溯源性。

其次，合理部署安全软件是保障云计算环境下信息安全的第一道屏障，云终端设备在软件方面需要部署安全软件，包括防病毒、个人防火墙，以及其他类型查杀移动恶意代码的软件，以保证系统软件和应用软件的安全性，同时安全软件需要具有自动安全更新功能，能够定期完成补丁的修复与更新。

5.3.2 云终端身份管理

在动态和开放的云计算系统中，云终端可以通过多种方式访问云计算资源，身份管理不仅可以用来保护身份，而且还可以用来促进认证和授权过程。而认证和授权在多租户的环境下可以保证云计算服务的安全访问。通过整合认证和授权服务，可以防止由于攻击和漏洞暴露而造成的身份泄漏和盗窃。身份保护用于防止身份假冒，授权用于防止云计算资源（如网络、设备、存储系统和信息等）的未授权访问。

随着身份管理技术的发展，融合生物识别技术的强用户认证和基于 Web 应用的单点登录被应用于云终端。基于用户的生物特征身份认证比传统输入用户名和

密码的方式更加安全。用户可以利用手机上配备的生物特征采集设备（如摄像头、MIC、指纹扫描器等）输入自身具有唯一性的生物特征（如人脸图像、掌纹图像、指纹或声音等）进行用户登录。而多因素认证则将生物认证、一次性验证码（OTP，one time password）与密码技术相结合，提供给用户更加安全的用户登录服务。为了让读者进一步了解强认证背景知识，下面介绍各种典型的强认证技术。

（1）单点登录

单点登录是一种流行的用户身份认证解决方案，旨在于提高用户登录效率，为网站减少网络负担，提高管理员工作效率。单点登录的实现，首先需要多家网站建立网站身份联盟，在身份联盟内部，所有网站互相信任。由身份联盟特定的身份管理提供商（IDP）提供统一的用户名、密码管理。普通用户只需登录一次，即可访问联盟内其他信任的成员网站，而不需要重复登录。单点登录方式可以方便用户在较短的时间内登录不同的网站，不需要记忆大量不同的用户名与密码。一些典型的单点登录技术方案例有基于 SAML 语言的单点登录方案。

在移动互联网领域，Orange 与 T mobile 共同引领 Open ID Connect 业务的发展与部署，两家运营商共同推进 N-API fast track 项目。该业务主要应用于用户单点登录访问运营商门户网站上的在线业务与第三方 SP 在线业务。斯里兰卡 Dialog 公司开展了 Dialog connect 业务，为用户提供一种第三方网站应用的单点登录方案，即输入一次用户名、密码，便可在第三方网站进行在线支付业务。

（2）多因素认证方案

利用两种或以上物理媒介进行用户的身份认证，以便加强用户身份确认过程的真实性和准确性。例如，在电脑上进行某些关键操作，如支付确认、注册确认等，需要网站系统发送的一次性验证码OTP至移动终端，然后将该OTP输入网页，从而确保该关键操作人的身份真实性。

斯里兰卡 Dialog 公司为保证 Connect 单点登录业务在用户身份认证的真实性与安全性，采用 SMS-OTP 方案。当用户使用账号登录时，已注册的移动终端会接收到一次性密码，然后输入至电脑 Web 页面中，实现 Connect 用户登录。

（3）生物认证方案

为了解决用户身份认证过程的安全问题，目前业界已经提出了一种利用生物特征识别技术用于识别人类真实身份。用户可以利用自身的生物特征，如指纹、声纹、人脸、虹膜等，无需记忆密码，只需用户通过采集设备输入自身的生物特征样本登录一次就可以访问网站所有相互信任的应用子模块。

采用生物特征识别技术用于用户身份登录可以克服传统密码认证手段存在的缺点。

- 采用用户的生物特征作为用户的唯一身份标识取代传统密码进行登录，由于生物特征属于人体的自然属性，因此无需用户记忆。
- 由于生物特征属于与生俱来的自然属性，所以不涉及记录到纸张上失窃的情况，安全性大大提升。
- 相对于传统密码登录，生物特征更难以被复制、分发、伪造、破坏，以及被攻击者破解。
- 生物特征属于私人的自然属性，因此不可能出现一个账号被共享的情况，避免法律纠纷。

2011 年 5 月，Orange 销售内置生物指纹识别器的智能终端为保障消费者个人信息安全，特别是可以满足一些特殊岗位工作人员的需求。

根据云环境下的实际情况，下面介绍一种基于生物密钥的移动终端单点登录技术方案（如图 5-5 所示），该方案可以减少云服务提供商内部的网络负担，提高云平台管理员的工作效率，提高云用户登录效率，加强内部员工云用户认证安全。

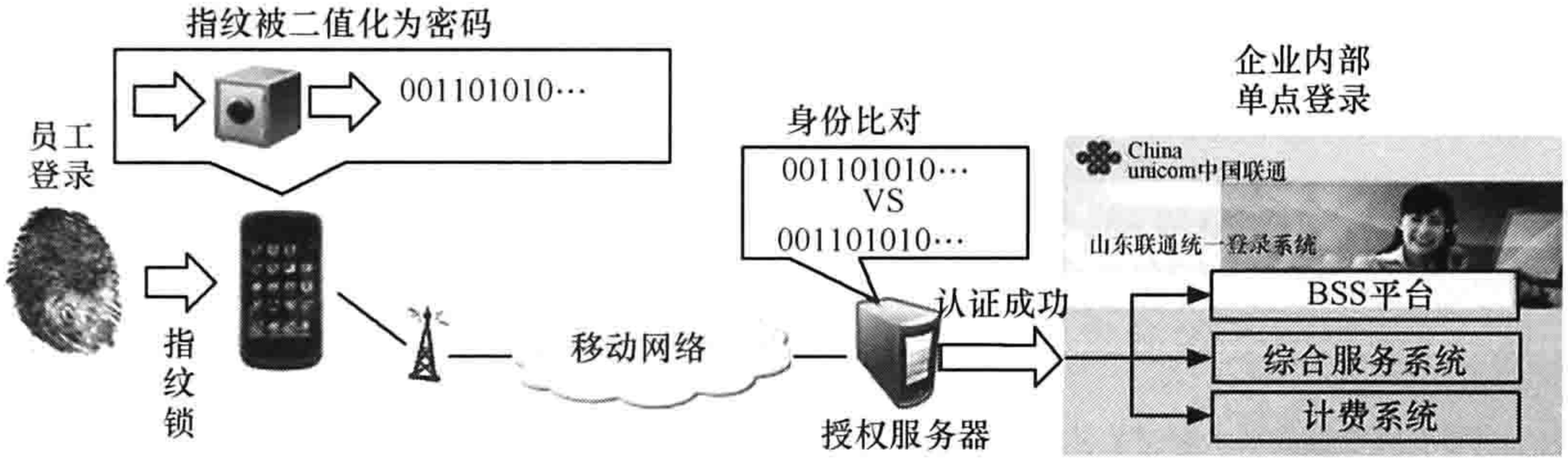


图 5-5 基于生物密钥的单点登录安全加固解决方案

该方案大体分为两部分：用户注册与用户单点登录认证部分。

1）用户注册流程：如果一个移动用户需要登录云服务提供商的某个网站并访问某项授权服务，第一次登录不可避免地需要注册新用户。注册流程如图 5-6 所示。

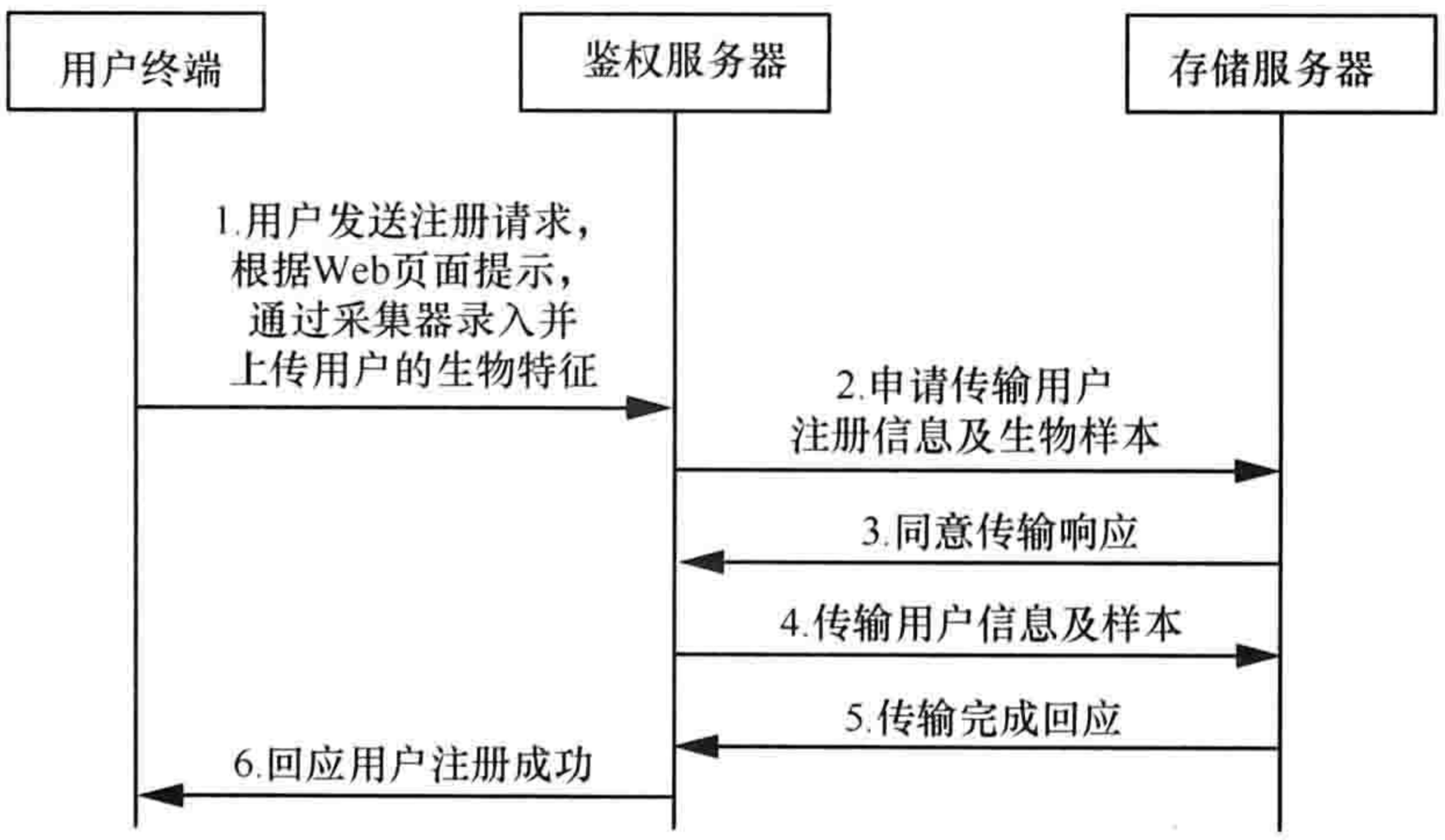


图 5-6 用户注册流程

本方案针对移动云环境下的特性，开发生物密钥技术作为云网络单点登录的用户身份认证手段，图 5-6 中的生物特征特指适合移动云环境下的人体生物特征，如指纹等。其中，采集器根据不同类型的特征可以设置相应的生物特征采集器，如指纹识别采集设备、Webcam 等。鉴权服务器与存储服务器均位于云平台内。

终端用户注册流程如下。

① 用户从移动终端发起申请用户注册的会话后，用户可以填写用户信息、采集、上传若干用于训练的注册生物样本。

② 当鉴权服务器接收到生物样本信息后，对用户信息存储服务器发起会话，提出将用户信息、生物样本信息传输到存储服务器的申请。

③ 存储服务器回应鉴权服务器同意传输的申请。

④ 鉴权服务器传输用户信息及生物样本到存储服务器侧。

⑤ 存储服务器回应鉴权服务器传输完成。

⑥ 鉴权服务器回应用户注册成功，整个用户注册部分完成。

2）用户 SSO 认证部分流程，如图 5-7 所示。票据服务器、应用服务器与鉴权服务器相同，均位于云平台内。

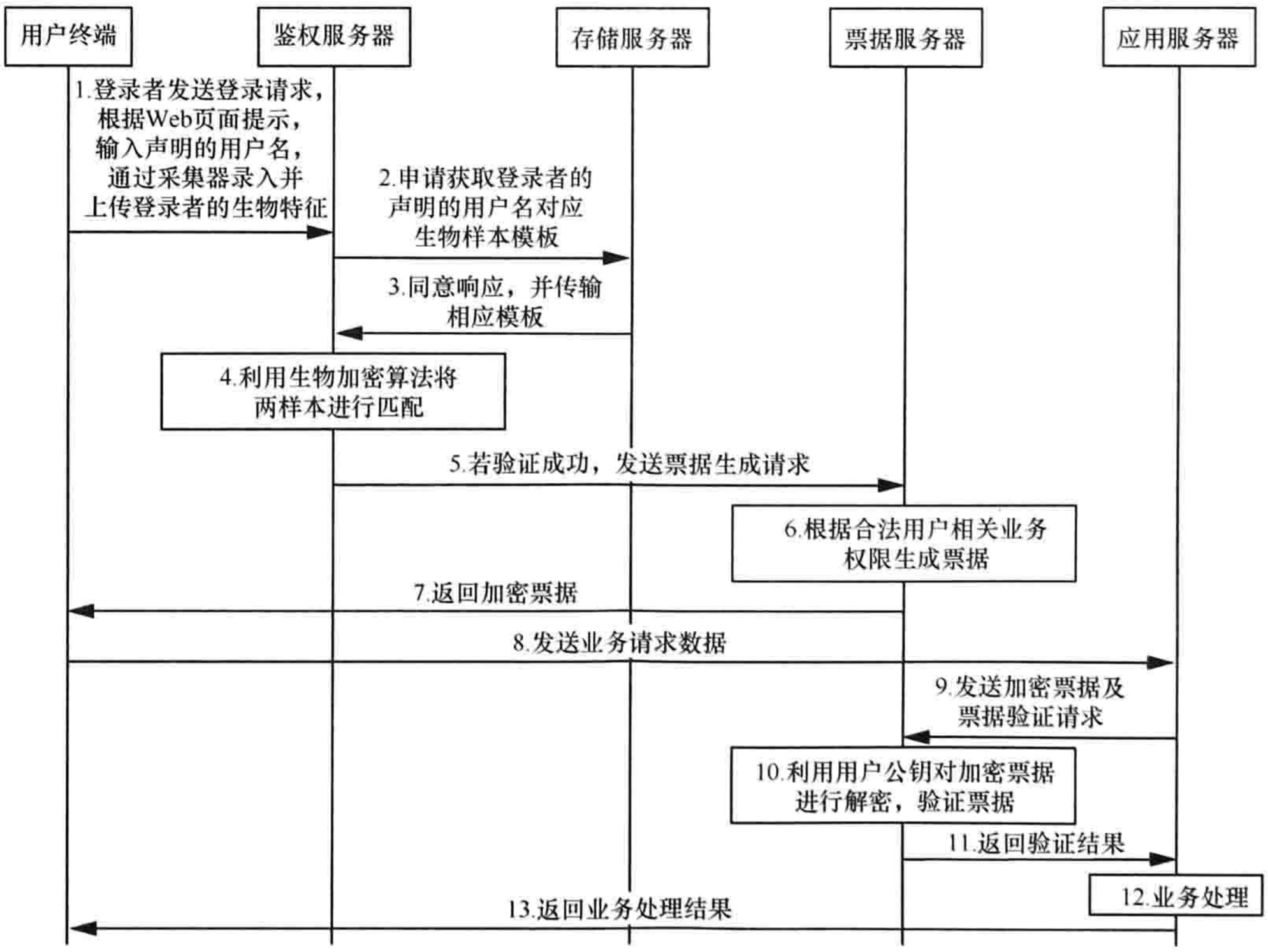


图 5-7　用户 SSO 认证及处理业务的流程

① 终端登录者发送登录请求，通过登录者声明的用户名，同时利用终端附带的采集器上传登录者生物样本到鉴权服务器。

② 鉴权服务器发送获取被声明的用户名与该用户的生物样本的申请至存储服务器。

③ 存储服务器做出响应，将声明用户名及生物样本模板发送至鉴权服务器。

④ 鉴权服务器利用生物密钥技术对模板与待测样本进行匹配，若结果匹配说明登录者的身份与其声明身份一致，则身份验证成功；否则，身份验证失败。

其中，生物密钥技术用于身份验证的具体方案如下。

a. 鉴权服务器对登录者提供的样本与若干个用户注册样本进行生物特征提取，每个生物样本都会得到一个对应的特征向量，该特征向量为生物样本的关键点或感兴趣点的坐标集合 $V=\{(x_1,y_1),(x_2,y_2),(x_3,y_3),\cdots,(x_n,y_n)\}$，即由一系列二元组组成的向量。由于本方案针对移动云环境，因此，以指纹作为生物特征是最佳的选择，通过移动智能终端上自带的指纹采集传感器来采集登录用户指纹图像，并以指纹图像的关键点、感兴趣点坐标作为特征向量。此处，需要鉴权服务器建立鉴别攻击者或恶意软件尝试重复登录的安全机制。如果攻击者或者恶意软件连续登录 6 次不成功，则禁止该账号当日的登录行为。

b. 将用户若干注册样本对应的每对坐标二元组按顺序分为两组集合 A、B，分别存储关键点、感兴趣点的横坐标与纵坐标。利用拉格朗日插值方法拟合出一个多项式曲线解析式，有 $p(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n$，并将该式的系数 $A=\{a_0,a_1,\cdots a_n\}$ 作为用户密钥 S。

c. 将用户密钥离散化为传统密钥的形式，即二值化字符串：首先，对 S 中系数 A 按大小排序然后取出中值 a_m，则离散化后的系数 A' 有：$A'=\left\{\left\lfloor\frac{a_i}{a_m}\right\rfloor \middle| i=0,1,2,\cdots,n\right\}$，其中，$\lfloor\ \rfloor$ 代表下取整运算。这样，系数 A' 被转化为二值化后的字符串，即为密钥 S。

d. 对登录者的生物样本采取与注册时生物样本相同的特征提取方法，然后获取关键点或感兴趣点的坐标集合 $U=\{(x_1',y_1'),(x_2',y_2'),(x_3',y_3'),\cdots,(x_n',y_n')\}$，然后根据第二、三步获取登录者密钥 S_{test}。若 S_{test} 与 S 的值完全一致，说明登录者的身份与声明身份一致，登录成功；否则，登录失败，鉴权服务器发送登录失败消息至用户终端。

e. 若验证成功，发送票据生成请求至票据服务器侧；若失败，返回用户终端认证失败的消息。

f. 票据服务器根据该用户的相关信息生成包含用户业务权限的票据，用户信息可从存储服务器获取。

g. 票据服务器发送加密票据至客户终端。

h. 用户发送业务请求数据的请求，发送用户终端私钥加密的票据。

i. 应用服务器向票据服务器发送用户的加密票据，并发送票据验证请求。

j. 票据服务器调用用户公钥对加密票据解密，读取该用户的业务权限及有效时长。

k. 票据服务器将以上用户验证信息发送至应用服务器。

l. 若验证成功，应用服务器进行相关业务处理。

m. 应用服务器返回业务处理结果至用户终端。

5.4　云监管域安全

由于不法分子可以利用云平台的能力来进行危害国家、社会、个人安全的行为，云平台上的信息发布和传播具有不同于以往的特点，也给信息监管带来了巨大挑战。为了监控云用户域与云服务域安全，需要在云监管域构建云安全管理平台。一般来说，云安全管理平台需满足以下需求。

（1）运行监控和管理

一是通过简便的方法监控流量大小、带宽、CPU 利用率、服务器运行状态、自动发现软件、存储空间、多服务器部署及托管应用程序的出错率等；二是实现资源配置管理，为用户提供数据库、虚拟服务器检测、VPN 的弹性和动态管理、软件配置、负荷管理、软件审计、补丁管理、运行时配置管理、通知及报警。

（2）恶意行为监控

云计算安全管理平台能够判断用户的非恰当使用、滥用和恶意使用云计算服务的场景，阻止这些现象的发生，并且识别出这些异常用户。例如，阻止恶意用户使用云计算系统发起洪水攻击、发送垃圾邮件、非法暴力破解密码等。

为了满足以上需求，本节所述的云安全管理平台从安全事件管理、补丁管理、灾难恢复、云安全评估、云安全审计、虚拟化安全协调 6 个方面开展讨论。

5.4.1　事件管理

为提高云计算应用风险预防、业务连续运行能力，云计算服务提供商针对可能影响业务的突发事件进行管理。云安全管理平台具备的事件管理机制包括事件监控、预警和响应。

监控：用来捕捉云服务的安全状态、预测异常情况和提供警告。

预警：针对预先可被部分探知的风险，制定完整的预警应对措施，将损失降低到可接受的程度。

响应：制定应急事件响应流程。响应流程应包括风险上报、风险评估、风险决策、风险告知、风险警备、数据恢复、应用接管、预警总结。

为了解云计算服务是否在整个基础设施中如期的运行，需要进行持续的监控用来捕捉云服务的安全状态，预测异常情况和提供警告。例如，监控虚拟化平台和虚拟机的实时性能。事件管理机制可以在安全事件发生前后，判断问题所在，并做出及时的响应。

5.4.2 补丁管理

为减少安全漏洞，云安全管理平台可以规范、监管安全补丁的管理工作。安全补丁管理过程应至少包括：补丁分析、补丁测试、部署安装、补丁检查 4 个环节。安全补丁管理流程可以由安全事件触发，也可以按周期触发。

5.4.3 灾难恢复

云安全管理平台需要具备灾难恢复能力，当遇到灾难时，如系统瘫痪、数据丢失，应尽快恢复到安全状态保证系统正常运转。这个机制可以保证云服务的持续性，保证云服务不会中断。

5.4.4 云安全评估

云安全管理平台的云安全评估机制包括安全风险评估方法、安全风险测评规范体系、安全风险辅助评测工具等。

安全风险评估方法为云计算安全的风险评估提供技术手段和方法支撑。安全

风险评估关键技术的研究，包括工具漏洞扫描技术、远程渗透测试技术、网络架构分析技术、IDS 采样分析技术等。

安全风险测评规范为云计算安全风险测评提供测评指标和方案规范。安全风险测评规范的具体内容包含风险评估框架及流程、风险评估实施、信息系统生命周期各阶段的风险评估、风险评估的工作形式等。

安全风险辅助评测工具为云计算应用模式下移动互联网安全风险测评提供评测工具和管理平台。风险辅助评测工具的开发主要包含云计算应用模式下移动互联网风险评估模块的开发和云计算应用模式下移动互联网安全测评模块的开发。

5.4.5　云安全审计

云安全管理平台可以建立完善的日志记录及审核机制，通过对操作、维护等各类日志进行统一、完整的审计分析，提高对违规事件的事后审查能力。

（1）审计数据采集

审计数据来源于网络系统层面以及业务层面，其中网络系统层面主要采集虚拟机、虚拟机管理系统、网络设备、安全设备、数据库等的日志信息、告警信息等；业务应用层面主要包括账号权限变更数据、账号登录行为数据、账号登录后各种操作记录等。审计数据应完整记录用户访问过程，包括登录用户的发起点、登录时间、退出时间、登录方式等；同时完整记录租户和管理用户所执行的每一个涉及资源配置或数据变化的行为。审计数据采集需将所有系统时钟时间保持同步，以真实记录系统访问及操作情况。

审计数据需备份到专用服务器或安全介质内，并至少保存半年或更长的时间。

（2）审计数据分析

云业务提供商为审计数据部署安全事件关联分析功能，灵活定制关联分析规

则、条件等。

1）网络及系统层面：制定基于规则、基于统计、基于资产的关联分析规则。

2）业务及应用层面：制定基于时序关联规则、基于账号与重要操作行为的关联规则、基于账号与权限关联规则，以及基于业务操作与系统日志的关联规则。

（3）审计结果

云系统可以对审计数据进行实时监控和实时呈现，呈现方式包括 E-mail、弹出窗口、Syslog、SNMP Trap、工单报警、电话通知等。

5.4.6 安全协调

云环境中，虚拟化作为云计算的一大特征，相关虚拟资源的快速提供和弹性扩展使得安全管理变得非常困难。当前已有的安全方案，如 VPN 的弹性和动态管理，云基础设施自动的安全监控，还不能完全解决虚拟机的安全管理。因此，云安全管理平台需要部署更加完善的虚拟化安全协调机制来协调整个云计算系统中多个层面虚拟化安全管理、协调功能。典型的虚拟化安全协调机制，如云安全管理平台借助虚拟机监控器保护云计算应用的隐私性，从而在操作系统与其他应用不可信的情况下保证虚拟机中应用的隐私数据不会被恶意泄露。

5.5 小结

云计算作为新的互联网服务模式，在带来了诸多好处的同时也面临着巨大的安全挑战。在云环境下，弹性资源分配、多租户、虚拟化、数据的所有者与管理者分离等特性需要新的安全策略与安全机制，而云服务商在开展这些工作之前，首要的是设计完善安全架构体系。

因此，本章提出一种通用的云安全架构，在此基础上按照云服务域、云终端

域、云监管域的逻辑展开云安全关键技术的论述。其中，云服务域重点介绍了 IaaS、PaaS、NaaS、SaaS、数据安全技术，云终端域主要讨论了终端的设备安全与身份管理相关技术，云监管域安全主要从事件管理、补丁更新、灾难恢复、云安全评估、云安全审计等方面进行了讨论。

参考文献：

[1] REWAGAD P, PAWAR Y. Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing[A]. IEEE Communication Systems and Network Technologies[C]. 2013. 437-439.

[2] MOHAMED E M, EL-ETRIBY S, ABDUL-KADER H S. Randomness testing of modern encryption techniques in cloud environment[A]. IEEE Informatics and Systems[C]. 2012.1-6.

[3] MUDZINGWA D, AGRAWAL R. A study of methodologies used in intrusion detection and prevention systems (IDPS)[A]. IEEE Southeastcon[C]. 2012.1-6.

[4] SANCHEZ R, ALMENARES F, ARIAS P, *et al*. Enhancing privacy and dynamic federation in IdM for consumer cloud computing[J]. IEEE Transactions on Consumer Electronics, 2012, 58(1): 95-103.

[5] SUZUKI A, OIKAWA S. Implementing a simple trap and emulate VMM for the ARM architecture[A]. IEEE Conference on Embedded and Real-Time Computing Systems and Applications[C]. 2011.371-379.

[6] KAI H, KULKARENI S, HU Y. Cloud security with virtualized defense and reputation-based trust mangeament[A]. IEEE Dependable, Autonomic and Secure Computing[C]. 2009.717-722.

[7] CHRISTIAN C, ALEXANDER S, IDIT K. Trusting the cloud[J]. Newsletter ACM SIGACT News, 2009, 40(2):81-86.

[8] YAMUNADEVI L, ARUNA P, SUDHA D D, *et al*. Security in virtual machine live migration for KVM[A]. 2011 International Conference on Process Automation, Control and Computing (PACC)[C]. 2011.1-6.

[9] KAUFMAN L M. Data security in the world of cloud computing[J]. Security & Privacy, IEEE, 2009, 7(14): 61-64.

[10] 蔡平. 基于 Hadoop 的 NoSQL 数据库安全研究[D]. 上海: 上海交通大学, 2013.

第6章 Chapter 6

云计算平台安全运营

在传统 IT 领域中，有一种得到普遍认可的观点，即资产所有者对服务器、存储设备、网络设施、应用程序、数据等拥有绝对的控制权，这种思维方式在云计算中并不存在。因此云平台安全运营是与云安全技术同等重要的话题，本章将详细介绍云平台安全运营所必须具备的要素。

6.1 云计算运营需求概述

从技术角度来看，云计算系统和传统 IT 系统类似，包括终端、网络设备、服务器（集群）应用系统及支撑系统等部分，传统 IT 系统中各个层次面临的安全问题（如系统的物理安全、主机、网络等基础设施安全，应用、服务安全等）在云计算环境中仍然存在。

从业务模式角度看，云计算对比传统 IT 系统的优势在于其规模经济，重用思想带来的成本效益。为了支撑这种成本效益，云服务商提供的服务必须足够灵活，最大限度地满足用户的需求。

但是，将安全机制集成到云服务方案中常会降低这些方案的灵活性。与传统 IT 系统相比，灵活性降低体现在，同样的安全机制部署在云计算环境中无法获得

同等的效果。其主要原因在于基础设施的抽象化、缺乏可视化和缺乏集成多种熟悉的安全控制手段的能力，这一点在网络层面尤为明显，这些差异需要引起云服务商重视。

云安全架构的一个关键特点是云服务提供商提供云化层级越低（IaaS<PaaS<SaaS），云用户自己所要承担的安全能力和管理职责就越多。

为描述方便，需要了解云服务的服务等级协议（SLA，service-level agreement）安全要求。SLA 是云服务提供商和用户之间签订的服务保障承诺，是用户对云服务提供商产生信任的基础，云服务供应商和云用户之间的关系必须通过 SLA 来描述，云服务提供商整体安全运营工作将围绕 SLA 指标要求展开。

如果要向用户承诺 SLA，则意味着在合同里需要对服务本身和提供商的服务水平、安全、管控、合规性及责任期望等有明确要求。目前存在两种类型的 SLA：可协商 SLA 和不可协商 SLA。如果采用不可协商的 SLA，则管理员需要根据协议负责这一部分。当缺少 SLA 时，系统管理人员需要控制云的所有方面。

云服务提供商首先必须保障云计算业务系统自身的安全性、可用性，然后，在满足国家安全监管、法律法规需求的基础上，保障云计算业务系统平台的运营安全，云平台的安全运营具体内容包括如下内容：

- 云平台物理安全；
- 云平台访问控制；
- 云平台数据库及配置；
- 人员管理；
- 云安全监控：通过安全监测、安全预警、安全响应等，实现云计算应用系统的动态安全管理；

- 云安全审计：满足用户及云服务提供商的安全审计要求；
- 云服务迁移、备份与恢复；
- 云安全评估。

本章后续将对上述内容进行具体描述。

6.2　云平台安全运营管理

6.2.1　云平台物理安全

物理安全是系统防御的第一道防线，用于保证用户对实物资产的合法访问，防御物理窃取档案资料、商业秘密，防御工业间谍活动和欺诈。

6.2.1.1　环境安全

环境条件，如湿度，温度等，会对云计算平台系统的可靠运行产生影响，必须保护环境安全，减少环境风险及降低对信息未经授权的物理访问风险。

云服务提供商的设施需要通过实施控制来保护人员和资产，以保护运维环境免遭危害。这些防护设备包括但不限于温度和湿度控制器、烟雾探测器和自动灭火系统。

云数据中心应根据公布的内部标准，当地的法规或法律，配备支持特定环境的设备，包括不间断电源。要求机房内配备互为热备份的 UPS 电源，UPS 在无外电供应情况下供电不少于 60 min。UPS 电源应符合 GB7620-2009 的标准。同时应遵循电源种类、电压变化范围、电源插头类型、耗电量及接地电阻等相关技术要求。

6.2.1.2　设备的位置和保护

云计算设备需要放置在一个物理上安全的位置，以尽量减少不必要的访问。

安保人员应考虑在附近发生灾难的潜在影响。例如，邻近建筑物发生火灾、从屋顶或地面层发生的漏水或街上的爆炸等。

6.2.1.3 设备维护

为了确保设备持续的可用性和完整性，需要对设备定期进行维护，包括：按照供应商推荐的维修间隔和规范维护设备，仅允许授权的维修人员进行设备的维修和服务，在实际维护过程中，对所有疑似故障或实际故障进行记录。当云系统设备运往异地时，需采取相应的保护措施，如使用安全的封装，保存在安全可靠的场所，有清晰完整的运输和追踪计划。保证在此过程中操作的可追溯性。

6.2.1.4 网络设备要求

交换设备应配置多台，网络设备与网络链路应有冗余备份。网络设备在单台故障时能够自动、及时地恢复。

网络系统应支持访问控制、安全检测等一系列安全功能，应提供完整的网络监控、报警和故障处理功能。

核心主机设备应采用双机热备、互备或者多机负载分担，单台主机故障时其他主机能够承担全部业务。双机做高可用（HA，high availability）时应能快速实现故障切换，不影响在线业务。服务器设备电源、风扇等也应采用冗余配置。

6.2.2 云平台访问控制

6.2.2.1 网络安全访问控制

用户与云平台之间应进行路由控制，建立安全的访问路径，并增加适当的网络安全配置策略。

平台管理人员应根据各系统的工作职能、重要性和所涉及信息的重要程度等

因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

应避免将重要网段部署在网络边界处或直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；重要业务网段的边界应当部署防火墙、IPS 或用 ACL 等手段进行技术隔离。

可采用如下措施加强云平台网络控制：

1）限制管理终端对网络设备的访问；

2）设置安全访问控制，过滤掉已知蠕虫常用端口；

3）关闭未使用的端口，如路由器的 AUX 口；

4）关闭网络设备不必要服务，如 FTP、TFTP 服务等；

5）避免在远程维护过程中出现用户账户和设备配置信息泄露，如采用安全的 SSH 登录远程维护设备；

6）修改 BANNER 提示，避免默认 BANNER 信息泄露系统平台及其他信息；

7）禁止管理、维护终端同时连接内网与互联网；采取必要的技术手段，防止终端的违规外联。

6.2.2.2　边界防护

对系统间边界进行清晰界定和防护，在系统内部进行区域划分和防护，加强边界访问控制机制，增加访问控制配置，并使用防火墙等访问控制设备对高安全等级区域进行边界防护。

6.2.2.3　防火墙安全访问控制

在防火墙上配置对常见病毒和攻击端口的 ACL 过滤控制策略，防止发生病毒或蠕虫扩散，影响核心设备正常工作。

6.2.3 云平台数据库及配置安全

数据库应支持 C2 或以上级安全标准、多级安全控制，支持数据库存储加密、数据传输通道加密及相应冗余控制。

操作系统软件应能够根据任务情况合理分配系统资源，当系统负荷过大时不会因为资源耗尽而发生宕机。

软件系统应具有容错能力，在单个进程的处理过程中出现错误时不影响整机的运行。软件系统支持在线升级功能，在不关机不中断业务的情况下实现自动或者手动升级。

应用系统应具备自动或手动恢复措施，以便在发生错误时能够快速地恢复正常运行。

所有软件应是已经投入商用的最新稳定版本。

6.2.4 人员管理

人员管理的一个重要原则是云平台管理、操作人员操作权限的最小化，降低干扰系统运行、危及云服务的风险。

角色和职责是云计算环境的一部分，通过角色和职责、人、流程及技术集成一起，形成了支撑租户安全的统一基础。

职责分离（SOD）指要求两名以上具备不同职责的人员来完成某项操作，职责分离的优点是可以降低内部人员权限误用或滥用风险。

6.2.5 云安全监控

云安全监控的目的是确保云平台的可用性。云安全监控包括如下内容。

- 日志监控：通过监控系统的输出日志，监控相关事件。

- 性能监控：对网络、系统、应用等内容提供可用性、用户体验和安全性方面的监控服务。保障云计算用户的业务稳定安全运行，当平台发生故障时，及时向管理人员报警。

- 恶意行为监控：恶意用户企图越权访问资源，某些租户对受限资源（如 CPU、内存、SAN 存储）的使用超过了公平分配的资源限制，或者在共享基础设施的其他应用中存在恶意行为，都将对其他租户产生影响。

监控不同服务类型的云应用，有如下考虑。

- 对于基于 IaaS 的应用，相比于部署在非共享环境中的应用，监控该类应用几乎是“正常的”，客户需要监控共享基础设施的事件或恶意租户对应用的无授权访问尝试。

- 监控基于 PaaS 的应用需要额外的工作。除了平台提供商提供能够监控已部署应用的监控方案外，还有两个方案可供选择：编写另外的应用逻辑来执行平台内的监控任务，或把日志发送到一个远程监控系统，该系统可以是内部监控系统，也可以是一个第三方监控服务。

- 由于 SaaS 应用提供最少的灵活性，监控这类应用的安全性是最困难的，云中应用监控要考虑的是：虽然提供商（或第三方云监控服务）搭建了一个监控系统来监控客户的应用，但这些监控系统正监控着几百甚至几千个用户。因此，如果用户有条件，运行只监控自己应用的自主监控系统通常会比云提供商的系统响应更快，效果更好。

6.2.6　云安全审计

云安全审计通常包括日志收集、数据库审计、网络审计等。云服务提供商需

要部署网络和数据审计措施，对网页内容、邮件内容等敏感信息进行审计；建立完善的日志记录及审核机制，通过对操作、维护等各类日志进行统一、完整的审计分析，提高对违规事件的事后审查能力。

（1）审计数据采集

审计数据来源于网络系统层面以及业务层面，其中网络系统层面主要采集虚拟机、虚拟机管理系统、网络设备、安全设备、数据库等的日志信息、告警信息等；业务应用层面主要采集账号权限变更数据、账号登录行为数据、账号登录后各种操作记录等。审计数据应完整记录用户访问过程，包括登录用户的发起点、登录时间、退出时间、登录方式等；同时应完整记录租户和管理用户所执行的每一个涉及资源配置或数据变化的行为。审计数据采集应将所有系统的时钟保持同步，以真实记录系统访问及操作情况。

审计数据应备份到专用服务器或安全介质内，并至少保存半年或更长的时间。

（2）审计数据分析

审计数据应支持安全事件关联分析功能，能灵活定制关联分析规则、条件等。

1）网络系统层面：应支持基于规则、基于统计、基于资产的关联分析；

2）业务应用层面：应支持基于时序关联规则、基于账号与重要操作行为的关联、基于账号与权限关联，以及基于业务操作与系统日志的关联。

（3）审计结果

应支持对审计数据进行实时监控和实时呈现，呈现方式包括 E-mail、弹出窗口、Syslog、SNMP Trap、工单报警、电话通知等。

6.2.7 云服务迁移、备份与恢复

信息安全的三要素是保密性、完整性和可用性。业务连续性对应着可用性。

云平台应具备灾难恢复能力，当遇到系统瘫痪、数据丢失等灾难时，应尽快恢复到可用状态，保证云服务的连续性，云服务不会中断。

向云服务提供商的过渡将包括对供应商合约承诺的正常运行时间进行评估。然而仅通过服务水平协议可能还无法满足客户，应充分考虑典型业务中断造成的潜在影响。服务连续性维护应作为维持业务运营的关键保障。

对于 IT 而言，云存储可用来完成备份与灾难恢复。云备份与灾难恢复的目标是降低基础架构、应用及总体业务流程的成本，云备份与灾难恢复应该具备可靠、廉价易管理等特点。

6.2.8　云安全评估

除了面临传统的安全威胁之外，云计算平台还会遭遇特有的安全风险，在这种背景下，需要参照相关标准，对云服务提供商的业务连续性、灾难恢复和传统的安全环境进行有针对性的评估。例如，保障云计算平台基础设施的物理安全，这需要按照各种指标进行彻底的评估，这一点对云和非云平台的安全要求是相似的。

对于云服务，应明确安全评估机制、评估范围、评估方式、评估组织等要素，定期对业务平台进行安全评估，可以采取第三方进行安全评估与审核（对安全评估发现的安全隐患进行风险控制、加固、转移及接收标准的相关策略）。

云安全测评包括安全风险评估方法、安全风险测评规范体系、安全风险辅助评测工具等。

- 安全风险评估方法为云计算安全的风险评估提供技术手段和方法支撑。安全风险评估关键技术的研究，包括工具漏洞扫描技术、远程渗透测试技术、网络架构分析技术、IDS 采样分析技术等。
- 安全风险测评规范为云计算安全风险测评提供测评指标和方案规范。安

全风险测评规范的具体内容包含：风险评估框架及流程、风险评估实施、信息系统生命周期各阶段的风险评估、风险评估的工作形式等。

- 安全风险辅助评测工具为云计算模式下安全风险测评提供评测工具和管理平台。风险辅助评测工具的开发主要包含云计算模式下风险评估模块的开发和云计算模式下安全测评模块的开发。

6.3 小结

云平台安全运营是与云安全技术同等重要的话题，云服务提供商首先必须保障云计算业务系统自身的安全性、可用性，然后，在满足国家安全监管、法律法规需求的基础上，保障云计算业务系统平台的运营安全。本章从云计算运营者的角度出发，阐述云计算平台的安全运营需求和安全运营框架，可为云服务提供者安全、可靠地运营云服务提供指导和依据。

参考文献：

[1] 中国电信网络安全实验室. 云计算安全: 技术与应用[M]. 北京: 电子工业出版社, 2012.

[2] ZHANG N, LI D, ZHANG Y Y. A research on cloud computer security[A]. ITA 2013[C]. 2013.

[3] Security guidance for critical areas of focus in cloud security computing V3.0[EB/OL]. http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[4] TIM M, SUBER K, SHAHED L. 刘戈舟, 杨泽明, 刘宝旭. 云计算与隐私[M]. 北京: 机械工业出版社, 2011.

第7章 Chapter 7

云安全实践

IDC 市场调研机构的数据显示，云计算服务在 2013 年达到整体 IT 消费的 10%，年收益高达 442 亿美元，5 年内年平均增长为 26%，这是传统 IT 行业增长速度的 6 倍。而 Frost & Sullivan 等市场研究机构近年来对全球市场的云计算调查数据显示，超过半数的企业用户对云计算的安全性担忧。毫无疑问，云计算的蓬勃发展，已经使云安全上升至产业的高度。针对目前备受关注的云安全问题，本章将介绍政府部门、国内外知名厂商和电信运营商在云安全方面的实践工作。

7.1 政府部门云安全实践

目前，政府部门已经运用电子化手段开展国家管理工作，政府网站为政府与公众之间搭建了有效的信息交换平台。但由于政府网站主要采用传统 Web 架构，因此容易遭受网络攻击。近几年来，信息泄露、网络钓鱼、病毒入侵、木马、恶意软件、垃圾短信等安全事件频繁发生，严重影响政府网站信息业务的正常运转。因此，政府部门急需部署有效的安全手段保障政府网站安全、有效、稳定地运行，以实现对政府网站的全面监控（外网、互联网出口、重要信息系统），并及时发现各类 Web 威胁、漏洞等问题。

随着云计算的诞生与发展，安全服务行业也随之发生改变。国内安全厂商以上述云计算技术和用户需求为契机，向政府部门提供云安全解决方案或云安全服务。云安全解决方案能够实现各种信息安全监测数据的实时收集、关联和分析，再通过专业化支撑平台和先进监测工具及时发现、识别安全事件，及时掌握安全状态，了解最新的网络攻击、病毒传播和异常行为等信息，为全方位预警、应急响应和事件调查提供强有力的支撑。

在云安全实践中，安全厂商服务方式也将发生改变，这体现在从原来的项目实施阶段的一次性服务转向整个运营阶段的全程动态服务，服务广度逐渐增加。例如，对云业务系统的信息安全评估服务、信息安全规划服务、信息安全方案实施服务、信息安全运维保障服务等。

除了依靠与厂商合作的方式外，政府部门还应积极推进监管政策及法律法规的制定与实施，这些监管政策和法律法规从宏观层面制约、指导所有具体业务，以实现对云服务的安全监管。

7.2 云服务提供商的安全实践

7.2.1 谷歌

2011 年，谷歌发布了关于云安全的白皮书“Security Whitepaper: Google Apps Messaging and Collaboration Products”，用户通过白皮书可以详细地了解谷歌采取的安全措施、政策及涉及谷歌应用程序套件的相关技术，因此用户可以放心地使用谷歌开发的应用产品。白皮书可以向当前客户与潜在客户提供强大而广泛的安全基础知识。书中核心内容表明谷歌剖析了云服务技术中存在的安全问题及自身的安全管理。同时，书中还多方位地提到云服务的安全策略，包括谷歌的组织安

全、资产分类与控制、物理与环境安全、操作安全、访问控制、系统开发与维护、灾难恢复与业务连续性等。同时，谷歌也对数据的存储、访问和传输等多个层次进行控制表示关注。

7.2.2　IBM

目前 IBM 企业信息安全架构主要分为 3 个层次：安全治理风险管理及合规管理、安全运维以及基础安全服务和架构。基础安全服务和架构是依托安全治理风险管理及合规管理而构建，安全运维是对信息安全全生命周期进行管理，而基础安全服务和架构则是企业安全建设技术需求和功能的实现者。

IBM 同时开展了三项云咨询服务，这些服务为需要建设云系统的中小企业提供帮助，或通过服务让现有的云系统更安全、更高效。这三项服务包括：

1）提供云计算安全战略路线图，为那些没有构建 IT 系统建设的新公司提前了解云技术，树立安全目标和指导企业如何发展出一套完整的云基础架构；

2）可以评估正在运行云服务但尚未通过安全测试的公司；

3）提供专门针对云应用程序的安全服务。

7.2.3　微软

微软公布了适用于其云服务上的安全政策——《保障微软的云基础设施》，其高度概括了微软在保护其基础设施与用户数据、应用程序方面采取的措施。微软可以依据风险评估、纵深防御、周期循环的风险再评估来制定适当的新对策来保证这些措施的安全实施。与此同时，微软还充分地遵守监测有关数据保密性和完整性的法律法规。此外，微软将国际标准化组织（ISO）和报表审计准则（SAS）的 70 个认证作为衡量云安全是否健全的标准。

微软推出的基于云计算的操作系统 Windows Azure 具有简单、可靠、强有力的特点，使客户能够专心于开发商机而不必分心于操作障碍。Windows Azure 为开发人员提供按需的计算和存储，通过 Microsoft 数据中心在互联网上托管、扩充和管理服务。Windows Azure 也具有保护数据和服务的安全性，而且数据完全由客户自主控制。中国地区 Windows Azure 服务存储的所有数据都将被加密，并且只有客户才有密钥。同时，由于微软与开源社区的协作，所以 Windows Azure 支持大量开源应用程序、框架和语言，并且数量仍在不断增加。

7.2.4 惠普

惠普于 2009 年 3 月推出 Cloud Assure 服务，有效地扩展了惠普的 SaaS 合作伙伴计划，其经销商可以为客户提供更多基于云的服务。HP Cloud Assure 包括了惠普应用安全中心、惠普性能中心与惠普业务连续性中心，惠普技术人员可以为用户提供安全扫描、执行性能测试和部署可用性监测服务。对于安全扫描而言，Cloud Assure 通过自动化渗透测试确定潜在漏洞，这样可以帮助客户精确了解云服务中的安全风险，防止供应商和消费者的数据遭到非授权访问。对于执行性能测试，Cloud Assure 服务能够满足最终用户对带宽和连接的需求，并密切跟踪最终用户体验。同时，部署可用性检测服务可隔离最终用户环境和业务流程中潜在的问题，确定造成问题的根本原因，并对性能问题进行分析。这样不仅能够对应用有了透彻的了解，延长服务正常使用时间，而且提高了应用的性能。

7.2.5 苹果

苹果公司曾推出 Mobileme 的云计算同步服务。它的基本功能是同步 Mac、iPhone、PC 之间的数据。此外，Mobileme 中称作 Find My iPhone 的应用为用户

提供手机物理丢失或被盗后的安全锁定服务。如果用户不慎丢失了自己的 iPhone 或 iPad 设备，用户可以通过该应用进入自己的 Mobileme 账户，进而确定 iPhone 或 iPad 的位置，为遗失的设备远程设置密码锁定，向任何看到这款设备的人显示一条信息，或者远程注销设备以保护隐私数据。

另外，苹果公司云服务 iCloud 可以为用户提供存放照片、文档、电子书、应用软件、日历、电子邮件、通讯录等内容的服务，并以无线的方式将上述内容推送到 iPhone、iPod、iPad、iPod touch 等设备。iCloud 还提供个人位置服务，可以随时让朋友、家人获悉用户的个人位置。

7.2.6 VMware

vCloud Networking and Security 是 VMware 提供的软件定义网络连接和安全解决方案，它可以提高运营效率、发挥敏捷性优势，并且能够根据业务需要迅速扩展。它的优势在于可以在单一解决方案中提供包括虚拟防火墙、VPN、负载平衡和 VXLAN 扩展网络等多项服务。借助该产品的管理功能并结合 VMware 其他产品，可降低数据中心运营的成本和复杂性，提高虚拟数据中心和私有云部署的运营效率和敏捷性。

7.3 运营商云安全实践

7.3.1 中国移动

“大云”平台是中国移动自主研发的核心基础产品组件，目前已形成包括 IaaS、分析型 PaaS 及云管理系统在内的 4 大类 13 项产品。IaaS 产品主要包括弹性计算系统、分布式对象存储系统、弹性块存储系统、文件中间件等。分析型 PaaS

产品主要包括并行数据挖掘系统、搜索引擎系统、结构化海量数据管理系统、商务智能平台等。

中国移动为大云系统部署了诸如 Web 应用防火墙等安全产品，并对整个系统进行安全管理监控。

中国移动还提出了端到端的云安全解决方案，主要包含 4 个方面：一是虚拟化安全，如虚拟机监控、虚拟机隔离、镜像的安全存储、虚拟机安全迁移；二是运行安全，如静态代码分析、对内外攻击防护、程序运行安全；三是接口安全，如避免政策规避、避免恶意接口调用、接口调用认证；四是数据安全，如数据加密、安全访问、内容安全、数据备份和消亡。

此外，中国移动还开展了可信云体系架构的研究工作，具体内容包括云对租户、租户对云及租户间的信任关系建立，攻克相关安全技术不完善或性能较低的问题，建立云计算环境的可信模型、用户隐私保护、数据隐私保护、云可信第三方审计等。

7.3.2 中国电信

中国电信的天翼云计算体系框架分为资源云、能力云和应用云 3 个层面。资源云包括云主机、云存储等；能力云把通信能力和互联网应用能力相结合，通过标准化接口，开放短彩信、定位、视频监控、统一通信等能力；应用云则基于中国电信云计算资源和智能云网络，将能力开放与行业应用相结合，面向公众及政企推出云存储、云邮箱、云桌面、销售管家、物流 E 通等应用。

在云安全的实践方面，中国电信建立了基于云计算架构的大容量 DDoS 攻击防御业务平台，该业务平台基于云计算架构进行构建，采用“全网统一调度、并行处理、就源清洗”的处理机制，在资源的统计复用基础上极大地提高了防御能力。

中国电信还提出了商密云技术体系，该体系采用国家商用密码技术和产品，构建基于云计算技术架构特性的商密云技术体系，为用户提供身份管理、安全认证服务、商密云存储服务；并与运营商运营支撑平台接驳，交互数据，满足云计算应用的安全防护及 SLA 服务指标需求，保障电信级云计算应用平台及业务运营安全。

7.3.3　中国联通

沃云平台是由中国联通公司自主研制的通用性云计算平台，该平台提供全面的云计算服务，包含计算、存储、网络等 IaaS 资源服务以及数据库即服务、中间件即服务、存储即服务等 PaaS 能力服务，同时实现 IaaS 与 PaaS 云平台综合管理。

在安全实践方面，沃云系统除了现有边界部署传统网络安全防御设备，应用层用户身份认证等安全措施以外，还构建了符合联通沃云运营需求的云安全架构模型。框架分别从用户侧安全、云数据安全、云基础设施安全及监管域安全 4 个角度来诠释云平台整体安全的架构与关键技术，并以此搭建了沃云安全管理测试平台。该平台全面监控虚拟化网络通信，包括虚拟化平台内外通信以及虚拟机间通信，集中监控虚拟化环境的威胁，实现统一配置、集中管控。

7.3.4　中华电信

台湾最大的电信运营商中华电信为确保云服务的安全可靠性，推出“多合一云测试解决方案 Spirent Avalanche Virtual”和“4~7 层应用性能测试解决方案 Spirent Avalance”。其中，Spirent Avalanche Virtual 是可提供在云中重现真实用户流量所需的客户端和服务器仿真能力的测试解决方案。同时可提供测量部署在云中应用的性能所需要的经验数据。后者可以验证云计算中心的安全性。其安全性

测试扩展到云服务的多个方面，如可以通过仿真云计算环境中的攻击来测试虚拟防火墙，同时可以测试部署在云中的虚拟化网络基础设施和应用。

7.3.5 Verizon

Verizon 为云安全联盟 CSA 的主要成员，在云安全方面起步较早。

Verizon 推出了一揽子主机托管解决方案，可以为主机托管用户提供物理安全、网络安全、流量清洗等安全服务。Verizon 于 2011 年宣布已经完成对 CloudSwitch 公司的收购。CloudSwitch 公司作为一家软件供应商，帮助企业将应用从企业数据中心移入云环境，为用户提供加密通道，保证用户安全地使用云计算应用。

另外，Verizon 还与 Novell 合作推出一项基于 Novell 技术的产品，为客户运行云应用提供安全保障。该产品为按需身份和访问管理服务，用户可对 Web 访问应用、网络服务、身份联盟和 Web 一次登录进行管理，无需额外的硬件、软件或者专门的 IT 资源。该服务的内建审计特性还可帮助客户减轻与系统和数据访问相关的合规报告负担。

7.3.6 AT&T

美国运营商 AT&T 为其 IDC 用户提供了一项云安全增值服务。这项服务其实是在 E-mail 的安全网关上提供了一种类似软件即服务的安全服务，可以管理 E-mail 和信息的安全，并确保信息完整、安全地进入企业网络。该服务还可监控外发 E-mail，用以避免企业间的数据通信流失。AT&T 的 IDC 用户均可以购买这项模块化的邮件安全服务。

对 AT&T 来说，这个增值服务不需要进行额外的硬件投资，不用购买邮件安

全网关，也不需要占用机房的资源，如设备、网络带宽、电源、机房空间等，却实现了其 IDC 业务的差异化，丰富了用户体验。

7.4 小结

随着云计算的不断发展和演变，从政府、云服务商到电信运营商，产业链中各个成员对于云安全都有自己的需求和独特见解，这些观点都代表了它们在各自领域对云安全所做的贡献。以电信运营商为例，云安全有两方面的应用：一是采用云计算技术新建、整合已有的安全系统设施，实现全网统一的安全调度和统计复用，提升全网的安全防护能力；二是基于云安全基础设施，开发面向客户的云安全服务产品，将云安全从运营商延展到为客户服务。

相信通过本章的介绍，读者可以对云计算产业链中各成员的安全实践活动有所了解。

参考文献：

[1] 云时代下的政府安全运营服务[EB/OL]. http://tech.hexun.com/2010-09-26/ 124999042. html.

[2] 云计算应对云安全挑战，政府监管需先行[EB/OL]. http://sec.chinabyte.com/400/12654900. shtml.

[3] KAI H, KULKARENI S, HU Y. Cloud security with virtualized defense and reputation- based trust mangeament[A]. IEEE Dependable, Autonomic and Secure Computing[C]. 2009.717-722.

[4] KOCHUT A, DENG Y, HEAD M R, *et al*. Evolution of the IBM cloud: enabling an enterprise cloud services ecosystem[J]. IEEE IBM Journal of Research and Development, 2011, 55(6):1-13.

[5] ROLOFF E, BIRCK F, DIENER M, *et al*. Evaluating high performance computing on the

windows azure platform[A]. IEEE Conference on Cloud Computing[C]. 2012.803-810.

[6] HP cloud assure[EB/OL]. http://www8.hp.com/us/en/software-solutions/cloud-management.html#. UkglfNK mi q8.

[7] Apple mobile me[EB/OL]. http://www.apple.com/cn/support/mobileme/.

[8] VMware vCloud networking and security[EB/OL]. http://www.vmware.com/files/pdf/products/vcns/VMware-vCloud-Networking-and-Security-Datasheet.pdf.

[9] 中国移动大云[EB/OL]. http://labs.chinamobile.com/cloud/.

[10] 中国电信天翼云[EB/OL]. http://www.ctyun.cn/.

[11] 中国联通沃云[EB/OL]. http:// www.wocloud.com.cn/.

第8章 Chapter 8

云安全发展趋势

云计算发展并未达到业界的预期，一方面需要云计算管理及技术的进一步成熟，另一方面用户对云的认知、认可也有一个时间过程，短期内可能体会不到云计算优势，且很有可能被云计算概念的多样性迷惑，或因云计算的不成熟而顾虑重重。由上可见，云计算的应用与推广任重道远。

国内的云服务商应清醒地认识到，当前我国的云计算产业与国外相比仍存在差距：据 Gartner 等国外咨询机构统计，在全球云计算的市场中，美国云服务市场的规模占到全球的 60%，欧洲占到 24.7%，我国目前只占到 3%。因此，云计算服务提供商，需要脚踏实地从某一具体的云服务领域开展自主研发工作，做出真正满足用户需求的产品。同时，云服务商还必须考虑我国的特殊需求，这些需求表现在信息服务方面，既要考虑国内用户的喜好，又要考虑我国对信息安全的具体要求。毫无疑问，在上述两种需求中，云计算安全问题都是关键因素。

基于以上考虑，本章将总结云安全引发的变革，并对云安全的发展趋势进行展望。

8.1 云安全变革

云计算既带来了信息安全的挑战，同时也促进了信息安全的变革。这种变革主要体现在 3 个方面，即技术理念的变革、产业发展的变革和安全战略的变革。

技术理念的变革，指的是云计算创造了新的机遇，同时也带来了新的风险。云计算的发展带来了网络资源、业务资源、用户资源在应用模式上的重大变化。多租户、资源共享、数据存储的非本地化、承载业务类型的多元化及网络带宽的快速增长不仅需要进一步强化传统的安全问题，同时也为互联网应用引入了新的安全问题。如何在便利与安全方面取得平衡，这需要从技术理念上进行变革。

产业发展的变革，指的是信息安全由产品研发向服务化进行转变。应积极推动信息安全产品和技术转型，从产品研发转向基础设施、服务的研究，从而通过标准化服务解决用户所面临的各种各样的安全问题。

安全战略的变革，指的是市场监管引导的重点发生了转移。如过去更重视骨干网络基础设施的安全保障工作，而在云计算时代，则将更加重视对网络空间大规模攻击的防范，新建立的基础设施也要采取相应的技术保障手段。虽然云计算推进了信息安全的变革，但这种变革并非意味着对原有技术体系的颠覆。

除了在信息安全的技术理念、产业和安全战略方面进行变革，还应该从法律层面、行政层面及行业自律的层面，对云计算的安全进行监管。应进一步健全隐私保护、数据安全的相关法律；政府可以从政策层面对云计算进行界定，并通过通信质量、安全等测试，对云服务提供商进行资格认证；此外，还可以借助行业协会的力量，在商业层面和市场竞争的层面采取一些有约束性的举措，从而维护行业的正常秩序。

随着云计算慢慢普及和标准化，会形成良性的市场竞争机制，由若干运营商

共同提供云服务。如果某一家运营商所提供的云服务性能不佳、稳定性不强，用户将转而购买其他运营商的服务。在这种情况下，安全问题与云计算运营方的关系密切，安全问题不解决，很可能就运营不下去，因此云服务提供商会非常重视安全问题，进而推动和催进云服务稳定性的提高及云计算安全难题的解决。

8.2　云安全展望

前面章节系统地介绍了云计算安全的基本定义、内涵、面临的安全威胁、云计算服务安全体系架构，云计算安全技术、标准现状、平台安全运营、产业应用现状等内容，在此基础上，对云安全前景有如下展望。

（1）云安全市场将进一步规范化

云安全这一名称已经被严重滥用，业内安全厂商的跟风现象严重，信息产业市场上存在着很多的云计算安全解决方案和产品，但与真正的云安全服务相差甚远，用户在使用各式各样的“云安全”产品时拥有“非常不同”的体验，无法得到用户的认知，这种情况无助于云计算的推广与应用，在此种需求下，云安全市场将会逐渐细分并加速规范化进程。

（2）CCSA 在云安全标准化方面将起到关键作用

随着云计算的不断发展和演变，国内外各标准组织、厂商及研究机构对于云计算、云安全都形成自己的独特见解，这些观点都代表了各个领域的发展特性。同时每个企业的技术力量都是有限的，不可能涵盖云安全产业链的所有层面，全球云安全标准工作人员存在大量空白，有较大的突破空间。

近年来，我国国内企业已在中国通信标准化协会（CCSA）中开展多项云计算安全研究工作，并积极向全球云计算标准化组织中推广。TC8 WG4 云计算子组成立之后，我国的云安全工作逐渐形成体系。可以预见的是，CCSA 在云安全领

域的作用将更加突出，并将加大云安全标准在国内的领导、整合力度，进一步加强其在国际标准组织的影响力。

（3）云安全产业将进一步成熟

随着云计算的普及，云计算技术被越来越多的企业和公司接受，这些公司已经通过使用云应用程序提高了工作效率，降低了公司成本，更多的公司都在寻找增加使用云的机会。但是，由于云计算在推广的过程中出现了一些安全问题，即使是顶级的云服务供应商，诸如亚马逊、谷歌和微软等，也时常会出现故障，服务的恢复并不是简单的过程，实施服务升级可能导致大规模的数据损坏。安全威胁仍然是云计算落地的最大阻碍。

对于用户而言，云计算的优势明显大于其缺点，经济利益要大于潜在风险。因此，用户会首先对应用及数据进行风险评估、细分等级，用户不会考虑将高敏感度数据或应用放到云服务中，但会将安全敏感度不高的数据或应用逐渐迁移到云中进行试点，并逐步推广到其他领域。

在此种背景下，服务可用性、系统安全可靠性应该是云服务商提供首要考虑的问题，同时拥有成熟、完整云安全解决方案的厂商或云服务提供商将在云计算市场中获益，并进一步促进云安全产业的发展。另一方面，用户对云服务提供商SLA水平将提出更高的要求，并要求在正式签署的合同中体现云安全相关的条例，在此过程中，用户将完成安全管理理念上的转变，即IT安全并非依靠云安全厂商和云安全产品就能完全解决。

上述整个过程都会使云安全产业不断成熟与前进。

（4）电信运营商会更加重视云计算安全

从国家安全的角度出发，如果政府部门、企事业单位、个人用户将数据存储在海外云服务商的网络中，那么我国的信息命脉将随时可能被外国政府所控制。

因此，云安全需要充分考虑全球 ICT 巨头对本国 ICT 业及信息安全带来的风险。毫无疑问，政府应保证本土企业在云安全中的核心地位，大力扶植进行云安全研究的企业快速健康的发展，突破关键技术，制造拥有自主知识产权的产品。

电信运营商在“云安全”领域具有较大的优势。

首先，云计算安全对网络带宽的大量需求只有电信运营商有能力解决。

其次，3G 及后 3G 技术的商用，让移动宽带迅速崛起，与有线宽带结合，运营商和应用提供商可以为用户带来自由、无缝的体验。

再次，运营商能够充分利用基础设施、用户、信息数据，为产业提供从服务层到通道层的全面服务。

最后，运营商有巨大的 IT 系统和业务体系，为满足自身的需求，会建立庞大的云计算平台。

运营商如忽略云平台的安全问题，很可能面临运营危机。因此，运营商将重视安全问题，并基于自身优势提供更多的云安全服务。最终，它将促进发展和改善云服务和云计算安全问题的解决。

此外，政府应该通过相关政策充分鼓励电信运营商在移动互联网云计算方面的研发投入，鼓励国内企业和运营商合作，并进行商业化运行。

（5）传统的安全机制将进一步增强，以满足云安全要求

云计算的特性对传统安全机制提出了更高的要求，例如，云中用户数据同态加密技术、面向云环境的增强身份管理技术、面向云环境的终端隐私管理技术等。这些技术是对传统的数据加密技术、身份管理技术、隐私管理技术的增强。在此驱动下，产业界、学术界将进一步加大研发力度，对传统的安全技术进行拓展，从而增强在融合了移动互联网、大数据、物联网、云计算环境下的安全保障能力和水平。

（6）云资源滥用可能成为产业界下一个热点

云计算模式逐步得到企业和用户的认知和认可。由于其低成本、低门槛、资源动态弹性分配等特点，越来越多用户对云计算模式和应用更加的认可，越来越多的开发者对于云计算资源及服务能力有更多创意。而不法分子也同样可以滥用云平台的能力来进行危害社会安全的行为，云计算平台上的信息发布和传播具有不同于以往的特点，给信息监管带来了巨大挑战。如何克服云服务滥用的缺点是下一个热点问题。

8.3 云安全建议

总之，实现高水平云计算安全仍然需要经历长期而艰难的努力，为促进云服务健康发展，我们对于云计算及云安全有如下建议。

1）要加强云计算发展环境的建设，开展以云计算为中心的自主研发工作，创造一个有利于云计算应用、云计算产业健康发展的氛围。

2）要坚持以服务带动产业的发展，以应用牵引技术的创新，以云计算技术为核心，优先发展公有云服务，通过大规模的公共服务，带动上下游企业和服务企业的技术创新和产业发展能力，从而形成良性的云计算生态环境。同时，在服务企业战略转型和业务变革的过程中，创造更大的价值。

3）从国家和政府的层面，要加强云计算层面规划的统筹监管，制定中国云计算发展规划，合理布局云计算数据中心等基础设施。

4）积极推进移动互联网、物联网、宽带、大数据技术的发展，要把上述技术作为云计算的基础性、先导性、促进性的工作加以推动，使云计算能够尽快普遍地部署，普惠整个社会进步和全区域的发展。

5）建立和完善云计算服务及安全管理的法律法规，从国家的层面加强基础设

施安全、数据安全、个人隐私保护、数据跨境流动等方面的法律法规环境的建设，建立和健全合理的行业自律和管理制度，以保障我国云服务健康有序发展和保护用户的合法权益。

6）应修订重要行业关于采购 IT 服务的法律法规，对重要行业采购云服务做出明确规定。例如，规定政府、军事国防、金融、医疗卫生等拥有个人或敏感信息的单位只能使用国内云服务商的服务，且数据必须存储在本国境内等。

7）提升云计算标准的重要性，提高我国在云计算领域以及国内外标准组织中的话语权和对产业的影响力。

8）加强关键技术人才的培养和引进，提供必要的学习交流机会，尽快形成我国云计算研发骨干队伍。

缩略语

AAA	Authentication，Authorization，Accounting	认证、授权、计账
ACL	Access Control List	访问控制列表
AES	Advanced Encryption Standard	高级加密标准
AH	Authentication Header	认证头
API	Application Programming Interface	应用程序编程接口
ATM	Asynchronous Transfer Mode	异步传输模式
CA	Certificate Authority	证书的签发机构
CCITT	International Telegraph and Telephone Consultative Committee	国际电报电话咨询委员会
CCSA	China Communications Standards Association	中国通信标准化协会
CDN	Content Delivery Network	内容分发网络

CHAP	Challenge Handshake Authentication Protocol	点对点询问握手认证协议
CPU	Central Processing Unit	中央处理器
CRM	Customer Relationship Management	客户关系管理
CSA	Cloud Security Alliance	云安全联盟
CT	Communication Technology	通信技术
DDoS	Distributed Denial of Service	分布式拒绝服务攻击
DES	Data Encryption Standard	数据加密标准
DFI	Deep Flow Inspection	深度流检测
DPI	Deep Packet Inspection	深度分组检测
EC2	Elastic Compute Cloud	弹性计算云
ENISA	European Network and Information Security Agency	欧洲网络信息安全局
ERP	Enterprise Resource Planning	企业资源计划
ESP	Extended Stack Pointer	堆栈指针
GSMA	Global System for Mobile Communications Association	GSM 协会
HTTP	Hypertext Transfer Protocol	超文本传送协议
IaaS	Infrastructure as a Service	基础设施即服务

ICMP	Internet Control Message Protocol	Internet 控制报文协议
ICT	Information Communication Technology	信息通信技术
IDC	Internet Data Centre	互联网数据中心
IKE	Internet Key Exchange	Internet 密钥交换协议
IPS	Intrusion Prevention System	入侵防御系统
IPsec	Internet Protocol Security	Internet 协议安全性
ISACA	Information Systems Audit and Control Association	国际信息系统审计协会
ISAKMP	Internet Security Association Key Management Protocol	Internet 安全联盟密钥管理协议
ISO	International Organization for Standardization	国际标准化组织
ISP	Internet Service Provider	互联网服务提供商
IT	Information Technology	信息技术
ITU	International Telecommunications Union	国际电信联盟
ITU-T	International Telecommunication Union Telecommunication Standardization Sector	国际电信联盟远程通信标准化组织
I/O	Input/Output	输入输出端口
GRE	Generic Routing Encapsulation	通用路由封装协议

LADP	Lightweight Directory Access Protocol	轻量目录访问协议
NaaS	Network Security as a Service	网络安全即服务
NIST	National Institute of Standards and Technology	美国国家标准技术研究所
OASIS	Organization for the Advancement of Structured Information Standards	结构化信息标准促进组织
OS	Operating System	操作系统
OTP	One Time Password	一次性验证码
PaaS	Platform as a Service	平台即服务
PAP	Password Authentication Protocol	密码认证协议
PKI	Public Key Infrastructure	公钥基础设施
QoS	Quality of Service	服务质量
RAM	Random Access Memory	随机存储器
RBAC	Role-Based Access Control	基于角色的访问控制
REST	Representational State Transfer	表述性状态转移
SA	Security Association	安全联盟
SAML	Security Assertion Markup Language	安全断言标记语言
SaaS	Software as a Service	软件即服务
SAS	Statement on Auditing Standard	报表审计准则

SSH	Secure Shell	安全外壳协议
SSL	Secure Sockets Layer	安全套接层
SSO	Single Sign On	单点登录
SLA	Service Level Agreement	服务等级协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SP	Service Provider	服务提供商
SQL	Structured Query Language	结构化查询语言
TCO	Total Cost of Ownership	总体拥有成本
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议
UPS	Uninterruptible Power System	不间断电源
VIDS	Virtual Intrusion Detection Systems	虚拟化入侵检测系统
VIPS	Virtual Intrusion Prevention System	虚拟化入侵防御系统
VLAN	Virtual Local Area Network	虚拟局域网
VMM	Virtual Machine Manager	虚拟机管理程序
VPN	Virtual Private Network	虚拟专用网络