HZ BOOKS
华章IT

·网络空间安全技术丛书·

可信云计算基础设施关键技术

张焕国 赵波 王骞 等著

机械工业出版社
China Machine Press

可信云计算基础设施关键技术

TRUSTED CLOUD COMPUTING INFRASTRUCTURE

张焕国 赵波 王骞 等著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

可信云计算基础设施关键技术 / 张焕国等著 . —北京：机械工业出版社，2018.10
（网络空间安全技术丛书）

ISBN 978-7-111-61179-0

I. 可… II. 张… III. 云计算 – 研究 IV. TP393.027

中国版本图书馆 CIP 数据核字（2018）第 240812 号

本书比较全面地介绍了可信云计算基础设施与环境的构建理论和关键技术。内容包括：云计算与可信计算基础、可信计算环境构建技术、面向云计算的可信平台模块、面向云计算的可信软件环境、可信云服务器技术、可信云计算网络技术、可信云计算数据安全技术、软件定义的弹性云安全、云环境下安全外包计算。

本书内容丰富、新颖实用，可作为从事信息安全、云计算、大数据、计算机、通信、电子信息等领域的科技人员的技术参考书，也可用作信息类专业的教师、研究生和高年级本科生的教学参考书。

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：余　洁　　责任校对：殷　虹
印　　刷：北京诚信伟业印刷有限公司　　版　　次：2019 年 1 月第 1 版第 1 次
开　　本：186mm × 240mm　1/16　　印　　张：19.75
书　　号：ISBN 978-7-111-61179-0　　定　　价：79.00 元

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

前　言

随着信息技术与产业的高速发展和广泛应用，人类社会进入了信息化时代。网络空间是信息时代人们赖以生存的信息环境，是所有信息系统的集合。

因为网络空间既是人的生存环境，也是信息的生存环境，所以网络空间安全是人和信息对网络空间的基本要求。又因为网络空间是所有信息系统的集合，是复杂的巨系统，所以网络空间的信息安全问题更加突出。

没有网络安全，就没有国家安全。没有信息化，就没有现代化。核心技术是国之重器。因此，我们必须下定决心，加速推动信息领域核心技术突破，把我国建设成网络强国，确保我国的网络空间安全。

云计算是一种以互联网络为基础的面向服务的计算，按需服务，计量收费，为用户提供丰富的服务。

云计算的服务总体上可分为三层：基础设施即服务（IaaS），用户可以租用云计算的硬件服务器等基础设施；平台即服务（PaaS），用户可以租用云计算的软件开发平台，开发自己的个性化定制软件；软件即服务（SaaS），用户可以租用云计算的应用软件。云计算旨在使计算像水、电、油一样，成为公共基础资源。用户只需要向云计算管理机构购置服务，而不需要自己购置硬件基础设施、软件开发平台和应用软件。这显然是极为方便的，而且极大地降低了用户的成本。

但是，面向服务的计算在工作模式上必然是资源共享，而资源的共享将引发诸多信息安全问题。例如：基础设施和平台安全问题，云计算有几乎无限的计算资源（基础设施、平台和软件），但是用户不知道这些资源是否可信；服务安全问题，云计算有几乎无处不在的服务，但是用户不知道这些服务是否可信；数据安全问题，云计算有几乎无限的存储空间，但是用户不能感知自己数据的存在，不知道自己的数据存储在哪里，更不能控制自己的数据。于是，用户就不信任云计算，不信任自然就不会应用。用户对云计算不信任也就成了影响云计算广泛应用的主要原因。

大数据处理与云计算是一对“双胞胎”。一方面，云计算具有几乎无限的存储和计算能力；另一方面，大数据需要巨大的存储空间和强大的计算能力。因此，大数据必然存储于云计算的存储系统并依靠云计算系统进行处理。只有这样结合，才是最合理、最节省的方案。由此可见，云计算和大数据的开发应用与安全可信是相互联系的。于是，云计算的安全问题就会影响到大数据的安全；反过来，大数据的安全问题也会影响到云计算的安全。

可信计算是一种旨在增强计算机系统可信性的综合性信息安全技术。而且，可信计算特别

适合用于提高信息系统的基础设施和平台的可信性。因此，采用可信计算技术增强云计算和大数据系统的可信性成为一种必然的选择。

为了确保云计算的安全可信，人们提出了可信云计算的概念。所谓可信云计算，是指将可信计算技术融入云计算环境中，构建可信云安全架构，向用户提供可信的云服务。

中国在可信计算领域起步很早、成果可喜并有很多创新，整体水平居于国际前列。早在2003年，武汉瑞达公司就与武汉大学合作开发出我国第一款嵌入式安全模块（ESM）和第一款可信计算机（SQY14嵌入密码型计算机），并得到实际应用。2012～2018年，华为、浪潮、大唐高鸿等公司与武汉大学合作研制出自己的可信云服务器，并实现了产业化。

为了研究、掌握云计算安全的基础理论与关键技术，国家科学技术部发布了“云计算安全理论与方法研究”的973项目（项目号：2014CB340600）。华中科技大学、武汉大学和中国科学院信息工程研究所共同承担了这个项目。武汉大学具体承担了“可信云系统安全架构基础理论与方法研究”子课题（项目号：2014CB340601）。除了973项目的支持外，武汉大学的研究还得到国家863项目、国家自然科学基金重点项目、国家自然科学基金面上和青年项目、企业合作项目的支持。

经过近5年的研究，武汉大学的项目组在可信云系统安全架构基础理论与方法方面取得了一些创新性成果，并基于这些成果编写了本书。

本书比较全面地介绍了可信云计算基础设施与环境的构建理论和关键技术。本书的第1章由张立强撰写，第2章由张焕国撰写，第3章由赵波、严飞撰写，第4章由余发江撰写，第5章由王鹃、余发江撰写，第6章由余发江撰写，第7章由王鹃撰写，第8章由王张宜撰写，第9章由王鹃撰写，第10章由王骞、王志波撰写。

作者相信，本书的出版和发行将会增进可信计算、云计算安全、大数据安全等领域的学术和技术交流，促进这些领域的理论研究和技术进步。

作者感谢国家科学技术部、国家自然科学基金委员会和合作企业的支持！没有作者承担的973项目、863项目、国家自然科学基金重点项目、国家自然科学基金面上和青年项目、企业合作项目的支持，就不会有这些研究成果，更不会有本书的出版和发行。

作者感谢973项目组内华中科技大学和中国科学院信息工程研究所的所有老师和同学！他们给了我们许多指导和帮助。大家组成了一个团结愉快的小组，共同完成了这个项目的研究。

作者感谢中国可信云计算社区的所有朋友！本书中的许多内容都曾经在社区的活动中进行过交流，并得到朋友们的指导和帮助。

作者要特别感谢华为、浪潮、大唐高鸿等公司的合作！正是这些合作，使得书中一些技术得以落地、实现产业化，为国家做出了实际贡献，同时也用实践检验了这些技术的可行性和有效性。

最后作者感谢本书的所有读者！

由于作者的专业水平有限，加上撰写时间很紧，书中错误在所难免，敬请读者指正。我们在此先致感谢之意。

张焕国

于武汉大学珞珈山

目　录

第1章

云计算概论

1.1 云计算的概念

2006年8月9日，时任Google首席执行官的埃里克·施密特（Eric Schmidt）在搜索引擎战略大会（SES San Jose 2006）上首次提出云计算（Cloud Computing）的概念。云计算的实际研究开发源于2007年Google工程师克里斯托弗·比希利亚（Christophe Bisciglia）所做的“Google 101”项目。

经过近十年的发展，云计算已经从概念走进了现实生活，对人们的工作、生活、娱乐以及各行各业产生了深远的影响。云计算通过整合、管理、调配分布在网络各处的计算资源，以统一的界面通过互联网络同时向大量用户提供服务。从本质上来说，云计算是一种以互联网络为基础、面向服务的分布式并行计算模式。

相对于其他计算模式而言，云计算具有按需服务、资源池、普适网络连接、超大规模、弹性伸缩等特点。云计算服务提供商将计算资源、存储资源、网络资源等汇聚成资源池，云计算用户以租用服务的方式，通过互联网络接入资源池中，按照需求动态地调配服务资源和享受服务，并通过计时、计次等方式支付服务费用。云服务提供商拥有海量的计算、存储或网络资源，能够支持不同规模、不同类型的各类用户对资源的使用。

典型的云计算服务交付模型为SPI模型，即从上到下依次为软件即服务（Software as a Service，SaaS）、平台即服务（Platform as a Service，PaaS）和基础设施即服务（Infrastructure as a Service，IaaS）。软件即服务是指将应用软件通过Web作为服务提供给用户使用，典型的应用包括企业关系管理系统、财务管理系统、办公软件等，典型的服务提供商包括Google Doc、Salesforce、金蝶等。平台即服务是指将支持软件开发、运行、调试、维护等服务的平台通过Web作为服务提供给用户使用，典型的应用包括软件开发平台、软件调试平台、软件运行环境及容器等，典型的服务提供商包括Microsoft Azure、Google App Engine、Force.com、Sina App Engine等。基础设施即服务是将计算、存储、网络等基础设施通过Web作为服务提供给用户使用，典型的应用包括IT基础设施、虚拟计算资源、虚拟存储资源等，典型的服务提供商包括

Amazon EC2、Amazon S3、OpenStack、阿里云等。

典型的云计算部署模型包括公有云、私有云、混合云和社区云。公有云即面向大众或大型组织提供云基础设施，云基础设施归云服务提供商所有。私有云是单独为某个机构建立的云基础设施，它可以由机构自己管理，也可以由第三方管理；既可以部署在机构内部，也可以部署在机构外部。社区云是由几个机构共享的云基础设施，用于支持具有共同关注点的特定社区。混合云是两种以上云（私有云、社区云和公有云）的结合，每个云都作为一个单独实体，通过标准或专有技术绑定在一起。

1.1.1　基础设施即服务

基础设施即服务（IaaS）的本质是使得用户无须关心计算中心的地理位置，将计算中心的任务分隔开来，即以服务的形式交付计算机基础设施。作为最底层和最基础的服务，IaaS 将基础设施（计算资源和存储）作为服务能力出租，代表了一种以标准化服务方式在互联网上提供基本存储和计算能力的手段。IaaS 为用户提供一个虚拟机镜像，该镜像在一个或多个虚拟服务器上调用。IaaS 作为服务计算的最原始形式，主要提供对物理基础设施的访问。

NIST 的 IaaS 定义如下："为客户提供了一种供应处理器、存储、网络和其他基础计算资源的能力，客户能够在所提供的计算资源上部署和运行任何软件，包括操作系统和应用程序。客户不对底层云基础设施进行管理和控制，但是对操作系统、存储、部署的应用程序具有控制能力，可能对某些网络组件（如防火墙等）具有有限的控制能力。"

一般来说，企业在计算系统基础设施方面的投入占据了企业的大部分开销。专用硬件和软件的购买和租赁、雇佣内部技术人员和购买技术咨询的费用成为企业的主要开支。采用 IaaS 模型（通常还附带 SaaS 或 PaaS 模型）能够提供一定的灵活性，能够快速地随需应变，这种能力是传统 IT 基础设施在获取、实现以及维护方面所无法企及的。

1.1.2　平台即服务

平台即服务（PaaS）的本质是使得用户无须关心计算平台的操作系统以及软件环境配置与管理，于 IaaS 之外提供更高封装的服务。PaaS 可描述为一个完整的虚拟平台，它包括一个或多个服务器（在一组物理服务器上虚拟而成）、操作系统以及特定的应用程序（如支撑基于 Web 的应用程序的Apache 和 MySQL）。PaaS 与 IaaS 的不同之处在于，它不像 IaaS 只提供虚拟硬件，也提供软件栈。例如，除了虚拟服务器和存储外，PaaS 还提供特定的操作系统和应用程序集（通常是作为一个虚拟机或文件，如 VMware 的 .vmdk 格式），以及对必需服务（如 MySQL 数据库或其他专用本地资源）的访问。

NIST 的 PaaS 定义如下："为客户提供了一种在云基础设施上部署客户所创建的应用程序的能力，以及在云基础设施上部署客户所获取的、使用提供商支持的编程语言和工具所创建的应用程序的能力。客户无须管理和控制底层的云基础设施，包括网络、服务器、操作系统和存储，不过需要对已部署的应用程序进行控制，并且对应用程序所在的环境进行配置。"

PaaS 厂商为应用程序开发者提供如下服务：

- 虚拟开发环境。
- 应用程序标准，通常建立在开发者的需求上。
- 为虚拟开发环境所配置的工具集。
- 为公共应用程序开发者提供的现成的发布渠道。

PaaS 模型为应用程序设计者和发布者提供了一个低成本的途径，支持完整的 Web 应用软件开发生命周期（Software Development Life Cycle，SDLC），从而减少了使用硬件和软件资源的需求。PaaS 解决方案可以是一个完整的端对端应用开发、测试和部署方案，也可以是一个较小的、更加专业化的、聚焦在某个特定领域（如内容管理）的方案。

一个软件开发平台要想成为真正的 PaaS 解决方案，需要具备以下几个基本要素：

- 应该对应用程序的使用情况进行基线监控，用于促进平台流程改进。
- 应该提供与其他云资源的无缝集成，如 Web 数据库与其他 Web 基础设施组件和服务。
- 应该支持动态多租户，通过云可以比较容易地在整个软件开发生命周期中实现开发者、客户端以及用户之间的协作。
- 必须把安全性、隐私性和可靠性作为基本服务进行维护。
- 必须是基于浏览器的。

为软件的销售和分发创建一个现成渠道是 PaaS 模型的优势之一。小型开发团队和刚起步的开发者可以通过 PaaS 提供商来访问一些无法获取的开发资源。

PaaS 厂商可以提供各种类型的商品，既可以是相对完善的，包括一个完整的应用程序运行、开发、测试和部署环境，也可以是综合服务的，包括可扩展性、维护和版本控制等。

1.1.3 软件即服务

软件即服务（SaaS）解决方案即通过 Web 交付应用软件。SaaS 提供商通常利用某个许可收费模型，按照客户需求来部署软件。SaaS 提供商可以将应用程序部署到自己的服务器中，也可以使用其他厂商的硬件设备。

应用程序的许可既可以直接发放给一个组织、一个用户或一组用户，也可以通过第三方来管理用户和组织间的多个许可，如应用程序服务提供商（ASP）。用户通过任何事先约定或授权的 Internet 设备来访问应用程序，通常都是利用 Web 浏览器。一个完整的 SaaS 服务应该是将一个功能齐全的应用套件作为服务按需提供，在云上作为一个应用程序实例运行，为多个组织用户和个人用户提供服务。

NIST 的 SaaS 定义如下："为客户提供一种使用运行在云基础设施上的、由服务提供商所提供的应用程序的能力。这些应用（如 Web 电子邮件）可以在各种客户端设备上通过一个瘦客户端接口（如 Web 浏览器）进行访问。用户无须管理和控制底层的云基础设施，包括网络、服务器、操作系统、存储，以及个别应用程序的性能，一些较为有限的、用户相关的、应用程序配置设定除外。"

与传统购买（通常是指购置费用或许可费用）并安装软件的方式不同，SaaS 用户通过运营费用模式（按使用付费或认购协议）租赁软件的使用权。按使用付费的模式也称为按需许可模

式，是指某些通过 SaaS 模型交付的应用程序，其收费模式采用计次使用或计时使用的方式，而不是传统许可中那种预支付费用的方式。

1.2　云计算的技术特点

1.2.1　面向服务

云计算除了将资源以服务的方式提供，逐渐形成集中化、规模化的软件复用之外，还有另外一个重要的方面就是提供用户按需即取这些服务的手段，即帮助用户实现服务的发现、聚合和验证，进而完成满足用户需求的过程。在互联网环境下，软件作为服务将会成为连接各种网络资源、数据资源、计算资源的核心，成为数据和数据交换的基础。快捷、高效地利用软件服务资源，可构造具有竞争力的服务和应用。软件服务强调以用户为中心，使得用户以更自然的交互方式表达需求，得到个性化服务。云计算中按需即取的关键问题为实现用户主导、面向领域的跨系统、跨媒体、即时定制的服务或者服务的柔性组合。服务及其组合能够形成不同粒度的模块为终端用户提供个性化服务。

1.2.2　弹性伸缩与自动调配

可伸缩性是以更大的规模来完成目前的任务，如延展一个 Web 应用的规模在于让更多的人使用它。纵向的可伸缩性是指在同一个逻辑单元内增加资源来提高处理能力。这样的例子包括在现有服务器上增加 CPU，或者在现有的 RAID/SAN 存储中增加硬盘来提高存储量。横向的可伸缩性是指增加更多逻辑单元的资源，并令它们像一个单元一样工作。纵向伸展相对比较容易做到，但会随着规模增长而成本越来越昂贵。大多数集群方案、分布式文件系统、负载均衡都是在提高横向的可伸缩性。

云计算中心可以根据需求的变化，对计算资源自动进行分配和管理，实现高度“弹性”的缩放和优化使用，而在这个过程中，用户却不必关心具体的操作流程。云计算中心的规模可以动态伸缩，以满足服务和用户规模变化的需要。并且，随着用户或服务自身需求的变化，云计算中心也可以自动地提供相应的资源扩展或资源释放功能。同时，云计算中心还可通过网络对松散耦合的各种应用组件进行分布式部署、组合和使用，并按不同的需求提供服务。另外，在访问请求和数据处理多元化方面，云计算中心还可以支撑各不相同的多种业务应用的同时运行和资源共享。

可以预见，未来用以支撑特定或综合服务的云计算中心都将是一个包含为数较多且承担不同角色和任务的节点的大型网络。云计算中心是网络中的节点，但是同类云计算中心之间可能会形成一个虚拟的、联邦的平台，该平台对于用户而言是透明的。传统的方式是在系统构建初期通过手工部署的方式建立每个节点的角色职能，节点的角色一旦确定便很难更改，这就造成当节点故障来临的时候，周边节点不能动态地顶替其功能，造成系统的部分瘫痪，如果一些关键节点出现故障，甚至可能出现全网停服的现象。这种静态系统的管理难度很大，更严重的是随着系统运营规模的扩大，将最终形成一个难以管理的复杂网络环境，给运营和维护带来巨大

的困难。整合了动态负载均衡及资源调配机制的云计算中心可以很好地解决大规模系统的有效管理问题。它能够实时地侦测全网各个节点的运行状态，收集重要节点和区域网络的负载信息。基于这些信息，系统就可以动态地调整和均衡全网范围内不同区域资源的负载。当某些节点失效或网络发生小面积故障时，系统会从全网中按照设定的某种策略寻找负载较低的其他节点，把失效节点的工作内容转移过来。当故障恢复时，计算能力又将重新转移回去。当业务变化或某些紧急情况发生时，整个系统的资源需要重新部署，系统将制订调整计划，通过分发新的策略重新规划系统中每个节点的角色和工作内容，并在统一的时间点完成各个节点的新角色切换。通过这种机制，使得云计算中心的问题检测和自动响应控制行动成为可能。同时，它还可以降低现有问题的扩散并防止问题的再次发生。

1.2.3 虚拟化技术

虚拟化的概念早在20世纪60年代就已经提出并应用在大型主机上。随着一些软件公司如VMware、Xen、Microsoft等推出不同的虚拟化软件，虚拟化涉及的应用领域与层次不断扩展，应用范围也在大幅增加。虚拟化技术包括指令级虚拟化、硬件抽象层虚拟化、操作系统级虚拟化、编程语言级虚拟化、程序库级虚拟化以及桌面虚拟化等。指令级虚拟化通过纯软件方式将虚拟执行环境中的指令翻译成主机所采用的指令进行执行，如Boschs模拟器可以在PowerPC平台上模仿x86机器。硬件抽象层虚拟化是在同一个硬件指令集上模拟多个计算机，提高物理计算平台的效率。要想实现这个目的，必须实现具有特权级别的管理软件，如虚拟机管理器（VMM）或虚拟机监控器Hypervisor，作为硬件之上的微内核系统，对CPU、内存等关键部件进行管理，同时对上层的操作系统提供调用接口。VMM具有多种实现方式：一种是独立的VMM，如VMware公司的ESX Server，需要为底层硬件开发驱动；另一种是借助主机操作系统的VMM，如VMware公司的Workstation，可以利用主机操作系统的驱动程序。操作系统级虚拟化是在同一个操作系统环境下提供多个操作环境，并且保证多个操作环境之间的隔离。如，Docker容器利用了Linux的LXC机制，通过CGroups和namespace确保每个容器在CPU、内存、网络等资源方面具有一定的独立性。编程语言级虚拟化是指为应用程序创建虚拟执行环境，并提供自定义的指令集，确保程序能够跨平台执行，如Java虚拟机（JVM）可以执行Java字节码，支持加载、算术、类型转换、对象创建、栈操作、异常处理等指令。程序库级虚拟化是指通过翻译和模拟程序库，实现不同应用程序二进制接口（ABI）和不同应用程序编程接口（API）的仿真，如WINE通过在UNIX系统上实现Windows API/ABI的虚拟层可以实现在UNIX系统上运行Windows程序。桌面虚拟化是指通过浏览器等轻量级交互界面实现对传统操作系统界面的模拟，使得终端无须运行主机操作系统就能进行日常的办公，如Google的Chrome浏览器。

1.3 云计算的安全需求

1.3.1 基础设施与平台的安全

IaaS服务是将计算、存储、网络等基础设施通过Internet方式提供给用户使用。虚拟化技术

是 IaaS 的重要组成部分。

由于虚拟机监控器对下实现对硬件资源的管理，对上提供对多个虚拟机实例的管理，因此，虚拟机监控器容易成为系统中的攻击目标。由于虚拟机监控器相对于操作系统而言复杂性和代码量要小很多，因此可以通过静态分析或动态分析确保虚拟机监控器代码的安全性与可靠性，在系统启动过程中可以通过验证虚拟机监控器的完整性确保其没有被篡改。下面以 KVM 为例介绍 VMM 的安全性。KVM 是利用 x86 CPU 的虚拟化技术与 Linux 内核实现的完全虚拟化解决方案。在 KVM 体系结构中，Linux 内核作为虚拟机监控器，KVM 虚拟机作为 Linux 中的一个进程。KVM 包括两个组件：一个是运行在内核模式的设备驱动程序，用来管理 CPU 提供的虚拟化硬件；另一个是运行在用户模式的 Qemu 模拟器，用来模拟 PC 硬件执行 I/O。KVM 体系结构中的多个虚拟机相当于多个 Linux 进程，通过 Linux 系统的多进程调度与隔离机制提供保护。一方面，KVM 并没有为虚拟机提供单独的安全机制，而是充分利用 Linux 的安全机制；另一方面，KVM 充分利用硬件提供的虚拟化技术进行安全防护。例如，Intel 的 VT-d 技术通过加入 DMA 和中断重映射支持 I/O 虚拟化，通过创建 DMA 保护域实现不同虚拟机之间的物理内存和 I/O 设备的隔离。

虚拟机实例是通过虚拟机监控器创建出来的、运行在虚拟执行环境中的系统。虚拟机实例往往是通过虚拟机镜像创建出来的，任务执行完毕之后被资源回收。结合虚拟机实例的生命周期来说，虚拟机实例所面临的安全风险包括以下几种：镜像不安全、启动不安全、执行过程中不安全、销毁不安全。为了确保虚拟机镜像安全，首先要确保虚拟机镜像来源可靠。可以通过镜像的完整性校验确保虚拟机镜像没有被篡改、没有被添加恶意程序与软件，并且不存在尚未打补丁的安全漏洞；还可以通过虚拟机镜像加密、签名等机制确保镜像的安全性。虚拟机实例启动时，可以通过对关键部件完整性校验确保启动过程中部件没有被篡改和破坏。虚拟机实例启动后，可以通过在虚拟机实例中部署防病毒软件和入侵检测软件、在内核中部署强制访问控制机制等对虚拟机实例进行安全性增强，通过部署安全审计模块等对执行过程中的安全事件进行扫描，确保虚拟机实例自身的安全。在虚拟机实例回收过程中，确保虚拟机实例中的数据已经被完全清除，不存在敏感数据和用户相关文件，符合虚拟机退役安全策略。

通过虚拟化技术，可以在一个物理服务器上运行多个虚拟机实例，这些虚拟机实例之间通过虚拟网络进行通信。虚拟网络是指将传统的局域网技术内嵌到单台服务器中，包括网卡虚拟化、虚拟网络、网络虚拟化等关键技术。网卡虚拟化通过软件模拟的方式将一个物理网卡共享给多个虚拟机实例，包括基于软件的网卡虚拟化方法和基于硬件的网卡虚拟化方法。虚拟网卡可以有单独的 MAC 地址和 IP 地址，所有虚拟机实例利用虚拟网卡和虚拟交换机通过物理网卡连接至物理交换机。虚拟网络是由虚拟链路组成的网络，虚拟网络节点之间的连接并不使用物理线缆连接，而是依靠特定的虚拟链路相连，典型的虚拟网络包括层叠网络、虚拟专用网络以及虚拟二层延伸网络。层叠网络是在现有网络的基础上搭建另外一种网络，允许对没有 IP 地址标识的目的主机路由信息，如分布式散列表可以路由信息到特定的节点。虚拟专用网络通过公用的网络架构来传送内联网的信息，利用已加密的隧道协议来达到保密、终端认证、信息准确性等安全效果，可以在不安全的网络上传送可靠的、安全的信息。虚拟二层延伸网络实现通过

三层网络连接的两个二层网络的互通，如 MPLS L2VPN 技术、Cisco OTV 以及 H3C EVI 技术都是借助隧道的方式，将二层数据报文封装在三层报文中并跨越中间的三层网络，实现两地二层数据的互通。网络虚拟化改变了传统网络架构的控制模式，如软件定义网络（SDN）将网络分为控制平面和数据平面，网络的管理权限交给了控制平面的控制器软件，通过 OpenFlow 传输通道统一下达命令给数据层设备。数据平面设备仅依靠控制平面的命令转发数据包。由于 SDN 的开放性，第三方也可以开发相应的应用并置于控制层内，使得网络资源的调配更加灵活。SDN 有三种主流实现方式，分别是 OpenFlow 组织主导的开源软件、Cisco 主导的应用中心基础设施以及 VMware 主导的 NSX。相对于物理网络安全而言，虚拟网络由于采用了软件方式，更加容易被攻击，因此，虚拟网络的安全需要在传统物理网络安全的机制上进一步确保软件实现的安全。

由于云计算服务外包的方式，用户丧失了对自身数据的物理可见性与可控性，因此对自身数据的安全性担忧尤为突出，已经成为阻碍云计算发展的重要原因。除了传统的数据机密性、完整性、可用性等安全需求外，数据可提取性证明、数据持有性证明、数据存在性证明、数据删除证明等针对数据的可控、可见的特殊需求也成为云计算数据安全性中的重要组成部分。数据的机密性往往通过数据加密的方式予以保障，然而，如果让用户在客户端进行加密，然后将加密数据上传到云上，虽然可以确保数据的机密性，但是数据的查找、删除、更新等操作变得极为困难，现有的同态加密算法尚不能完全支持用户需求。用户将数据放置在云端，需要不定期地检测自身数据的完整性和可用性，因此基于完整性验证的挑战 - 应答协议成为重要基础，包括数据可提取性证明、数据持有性证明、数据存在性证明等机制均是通过数学方法在不完全提取用户数据的情况下向用户证明自身数据的安全可靠。数据中心往往会对用户数据进行多副本存储，确保数据的可靠性与可用性。另外，用户还需要云服务提供商证明当其希望删除云中数据时，云中所有的数据均得到安全消除，这也需要相应的安全机制予以保证。

1.3.2 软件的安全

云中软件的安全性包括 VMM、虚拟机实例以及虚拟机中应用软件的安全性。

- **VMM 的安全性**。在以虚拟化为支撑技术的云平台中，VMM 在物理机上拥有最高权限，对 VM 的安全监控等其他安全服务都是通过 VMM 来完成，其安全性非常关键。保护 VMM 的完整性不被破坏是 VMM 安全的基础要求。
- **VM 镜像的安全性**。对于虚拟机镜像中是否包含恶意软件、盗版软件等，需进行安全检测。
- **VM 安全监控与执行验证**。在云计算中，VM 运行于服务方，除了用户授权的程序外在 VM 上是否还运行有其他程序、用户的具体操作在 VM 上是否得到了正确执行，这些都存在疑问。为保障用户 VM 的安全运行，云平台需具有对单个 VM 进行监控的能力，能对 VM 的执行过程进行验证。
- **云端软件的运行隔离与侧信道攻击防护**。在云计算中，不同用户的 VM、云端应用可能运行在同一个物理机器上，共享同一个物理 CPU 和内存，这为攻击者进行侧信道攻击带来了便利。云平台需对云端软件的运行进行安全隔离，提供侧信道攻击的防护机制。

- **云平台应用软件安全**。各类云应用自身的安全性直接关乎云计算产业的发展，首先需要预防应用本身固有的安全漏洞，同时设计针对云计算特点的安全与隐私保护机制，提高应用安全性。
- **云平台软件安全审计**。在云计算中，为了获得用户信任、满足各种合规性要求和明确安全事故责任，服务商需提供必要的支持，以能对云平台软件的运行进行安全审计。安全审计必须提供满足审计事件的所有证据以及证据的可信度说明，且不应泄露其他用户的信息。
- **云平台软件安全恢复**。整体恢复难以保持业务的连续性，不太适用于云计算服务。云平台需针对进程、软件、系统等不同层次，提供相应的软件安全恢复机制。

第2章

可信计算概论

本章主要介绍可信计算的概念和发展、可信计算的关键技术，以及笔者对可信计算、信息安全和计算机安全的一些思考和新认识。

2.1 网络空间安全的概念

人类社会在经历了机械化、电气化之后，进入了一个崭新的信息化时代。在信息化时代，人们生活和工作在由物理世界、人类社会和信息空间（Cyberspace）组成的三元世界中[1-2]。

早在1982年，加拿大作家威廉·吉布森在其短篇科幻小说《燃烧的铬》中创造了“Cyberspace”一词，意指由计算机创建的虚拟信息空间。Cyberspace在这里强调计算机爱好者在游戏机前体验到“交感幻觉”，体现了Cyberspace不仅是信息的聚合体，还包含了信息对人类思想和认知的影响。此后，随着信息技术的快速发展和网络的广泛运用，Cyberspace这一概念不断演化。

2008年，美国第54号总统令对Cyberspace进行了定义：Cyberspace是信息环境中的一个全球域，由独立且互相依存的IT基础设施和网络组成，包括互联网、电信网、计算机系统，以及嵌入式处理器和控制器。

除了美国之外，还有许多国家也对Cyberspace进行了定义和解释，但与美国的说法大同小异、各有侧重。

目前，国内外对Cyberspace还没有统一的定义。笔者认为：Cyberspace是信息时代人类赖以生存的信息环境，是所有信息系统的集合。它以计算机和网络系统实现的信息化为特征[1-2]。

因此，把Cyberspace翻译成“信息空间”或“网络空间”比较好。其中信息空间突出了“信息”这一核心内涵，网络空间突出了“网络互联”这一重要特征。在本书中我们主要采用网络空间这一名称。

众所周知，人身安全是人对其生存环境的基本要求，即要确保人身免受其生存环境的危害。因此，哪里有人，哪里就存在人身安全问题，人身安全是人的影子。同样，信息安全是信息对其生存环境的基本要求，即要确保信息免受其生存环境的危害。因此，哪里有信息，哪里