ISEC
国家信息安全工程技术研究中心

云计算和云计算信息安全

国家信息安全工程技术研究中心 • 文仲慧

ISEC

一、云计算发展概述

二、云计算定义分析

三、云计算信息安全

四、云计算信息安全解决方案（略）

一、云计算发展概述

云计算概念和实践的出现不是偶然的，而是有着深刻的技术背景、现实的社会背景、浓厚的商业背景和隐含的政治背景。

（1）深刻的技术背景

CPU等硬件技术的快速发展，并行计算、分布计算、网格计算、效用计算、虚拟计算等计算技术的快速发展，宽带网络、无线网络等网络技术的快速发展，这些都是云计算得以发展的深刻技术背景。简言之，云计算发展的技术背景不是某一类技术的发展，而是多类技术共同发展形成的综合技术背景，这些多类技术发展到一定阶段，一定会形成一种融合与整合的需求，由此，云计算应运而生、水到渠成了。

(2) 现实的社会背景

社会信息化、网络化的发展已成为不争的历史事实，计算速度、存储容量按照摩尔定律不断发展，也已形成社会共识。但是，符合摩尔定律不断发展的不仅仅是计算速度和存储容量，网络扩展速度和信息系统扩展速度，至少在目前也完全符合摩尔定律。

这种全社会对信息化的大量、迫切需求，必然会提出一个重要问题：每个人或每个单位是否都要自己购买各类设备、自己铺设物理网络、自己建设信息系统、自己组建开发队伍、自己养活运维人员，等等？另一方面，即使资金充裕的个人或单位，可以在信息化建设方面完全自给自足，那么其计算资源（包括存储、计算、网络等）是否发挥了最大效益、是否存在大量闲置？再一方面，大量重复建设也给全社会造成了极大浪费和环境污染。

从绿色环保、资源共享、资源出售、减少开支等等方面看，都需要一种新的商业模式，每个人或每个单位仅仅购买他所需要的信息化方面的服务，或者更简单地讲，每个人、每个单位应该能够像购买水、购买电那样购买到他所需要的服务。云计算正好完全迎合了这种社会需求。

（3）浓厚的商业背景

云计算创造了一种新的商业模式！最早发现和提出云计算这种特点的是对铜香具有特殊嗅觉的商家。为了追求利益最大化和最快化，国际上相当一批风险投资公司迅速行动起来，匆匆挤身到云计算这个技术色彩十分浓厚的高科技领域，为云计算的发展提供了重要的资金支持。商家们知道，谁先抢占了这个阵地，谁就可能大捞一把。于是乎，商家们又使出了惯用伎俩，开始对云计算大肆进行包装和抄作。不管怎样，商家们至少极大地推进了云计算的发展，将云计算发展的时间表缩短了至少十年。

（4）隐含的政治背景

信息是国家重要的战略资源，信息技术和信息的开发应用已经渗透到国家政治、经济、军事和社会生活的各个方面，成为生产力的重要因素。互联网的发展，已经给中国人一个惨痛的教训，所有的域名服务器无一例外都在国外，中国人不得不受制于人、受限于人、受控于人。云计算目前尚处于发展初期， 可是美国国家标准和技术研究院(NIST)已经提出了云计算定义的第15个版本，这反映出美国人在这一领域的政治敏感性。云计算这种隐含的政治背景，至少引起了像中国这样的大国的警觉，同时，也有利地推动和促进了云计算概念和产业的发展。

二、云计算定义分析

随着云计算理论研究和应用发展的深入，各种云计算概念不断翻新，其中不乏鱼目混珠、良莠不齐之说，一些似是非是、似像非像的说法不一而足。因此，有必要从一个统一的概念上规范云计算的定义。这个统一的概念，既是美国国家标准和技术研究院(NIST)信息计算实验室(ITL)对云计算所做的定义。NIST没有从科研角度阐述云计算概念，也没有支持某些公司或集团的云计算定义，而是综合大多数云计算定义和解释，归纳出云计算的定义的。

2009年10月7日，该组织发表对云计算所做定义的第15版。这个定义如下：

云计算的定义

作者：　彼得·梅尔、提姆·格兰斯

第15版，2009年10月7日发布

美国国家技术与标准研究院　信息技术实验室

注1 ：云计算仍是一个不断发展的词汇。它的定义、应用场景、基本技术、问题、风险和收益，将在公众和企业参与的激烈辩论中不断发展。这些定义、属性和特征都将随着时间而演变和改变。

注2 ：云计算行业代表一个由众多商业模式、企业、市场定位构成的一个庞大的生态系统。这一定义试图涵盖各种云计算观点。

云计算定义：

云计算是一种能便捷、按需、由网络接入到一个可定制的计算资源共享池的模式。计算资源包括网络、服务器、存储、应用、服务等。最小限度的管理工作或最小限度的服务提供商的交互行为可以迅速地提供和释放这些资源。这种云模式提高了可用性，它由五个主要特点、三个服务模式和四个部署模式组成。

五个主要特点：

（1）按需自助服务。使用者可以单方面获得诸如服务器时间和网络存储之类的计算能力，计算能力可按需自动部署而无需使用者与服务提供商进行人工交互。

（2）通过网络获取。计算能力可以通过网络接入以标准方式访问而获得。这种标准方式通过异构的瘦客户端或胖客户端平台（例如移动电话，笔记本电脑，PDA等）得到推广使用。

（3）计算资源池化。提供商的资源被池化，不同的物理资源和虚拟资源可根据客户需求动态分配和再分配，以便以多用户租用模式被多个使用者使用。使用者一般无法控制或知道资源的确切地理位置，但在更高一级的抽象概念上（如国家、州或者数据中心）可以指定资源的位置。这些资源包括存储、处理器、内存、网络带宽和虚拟机。

(4)能力快速伸缩。计算能力可以迅速和弹性地部署，在某些情况下可以自动部署，以便快速扩展和快速释放。对使用者来说，可以获取的计算能力看似无限，可在任意时间购买任意数量的计算资源。

（5）度量优化服务。云系统通过在某种抽象意义上均衡度量计算资源而使得计算资源与服务类别相适应（例如存储、处理、带宽以及现有使用者帐号），实现自动控制和优化资源使用。资源的使用情况可被监视，控制和报告，而对服务提供商和使用者来说这些都是透明的。

三个服务模式：

（1）云软件服务（SaaS）。云软件服务是各种客户端设备使用供应商运行在云基础设施上的应用程序，通过诸如网页浏览器这样的瘦客户端接口接入，例如：web-mail。使用者不管理或控制底层云基础设施、网络、服务器、操作系统、存储器，甚至个人应用功能，但是有限制的用户定制应用配置设置可能除外。

(2)云平台服务（PaaS）。云平台服务是使用者应用供应商提供的程序语言和工具，例如：Java、.Net、python，创建自己的应用程序，并将这些程序部署到云基础设施上去。使用者不管理或控制底层云基础设施、网络、服务器、操作系统、存储器，甚至个人应用功能，但使用者可以控制已部署的应用程序，也可以控制应用程序所托管的环境配置。

（3）云基础设施服务（IaaS）。云基础设施服务是使用者利用供应商出租的处理能力、存储、网络和其它基本的计算资源，部署和运行任意软件，包括操作系统和应用程序。使用者不管理或控制底层云基础设施，但可以控制操作系统、储存、部署的应用程序，也可能有限度地控制可选的网络组件，例如：防火墙、负载均衡器等。

四个部署模式：

（1）私有云。云基础设施由一个组织单独操作，该基础设施可能由该组织或第三方管理，其存在可设定前提，也可不设定前提。

（2）社区云。云基础设施由一些组织共享，支持一个分享共同关注点的社区（例如，任务，安全要求，政策和遵守的考虑）。该基础设施可能由这些组织或第三方管理，其存在可设定前提，也可不设定前提。

（3）公共云。云基础设施由一个销售云计算服务的组织所拥有，服务对象是一般公众或大规模产业群。

（4）混合云。云基础设施是由两种或两种以上的云（私有云、社区云或公共云）组成，每种云仍然保持独立，但可用标准的或专有的技术将它们组合起来，具有数据和应用程序的可移植性（例如，可以通过平衡云间的负载用来处理突发负载）。

注：云软件通过以无国界、松耦合、模块化、语义协同性为聚焦进行服务，充分利用了云概念的优势。

应该说，NIST对云计算的定义还是比较清晰和严谨的。经查阅NIST早期云计算定义的版本，最新版本与早先版本定义最主要的差别在于弱化了云计算的商业特点，而强化了云计算的技术特点。

通过上述定义可以看出，理论上讲，云计算可以整合的物理计算单元包括巨型机、小型机、服务器、个人电脑，甚至单版机、单片机等等所有具有CPU的物理设备；云计算可以整合的网络包括所有现有的网络，以及将来可能出现的网络；云计算最适合那些需要大规模存储资源、或者需要大规模计算资源、或着需要在存储和计算资源之间进行动态平衡、或者需要大规模占用网络带宽资源的计算任务。

三、云计算信息安全

在传统计算模式下，使用者对数据的存储和计算拥有完全的控制权；而在云计算模式下，使用者的数据与计算，以及物理计算单元的管理完全依赖于服务提供商，使用者仅仅保留对虚拟机的控制。因此，从使用者的角度看，保证存储数据和计算结果的安全性、私密性显得尤为重要。

传统的信息安全问题，在云计算中仍然存在，而云计算的特点又提出了新的信息安全问题。

●云上数据存储、隔离、冗余、销毁等等特点提出的新的数据安全问题。

云计算重要特点和优点之一，是云可以提供几乎无限的存储能力，需要大规模存储的计算任务可以充分利用这一特点和优点。但是，在云上，数据完全可能是异地分布存储的，完全可能是不同系统的数据存储在同一个物理介质上，完全可能出于数据恢复的考虑而将异地分布存储的数据进行异地分布冗余备份，完全可能在异地分布存储的数据被销毁后出现数据是否真的被彻底销毁了的疑问。

云上这种数据存储、隔离、冗余、销毁等等新特点提出了云上数据安全的新需求。因此，应该研究在云计算环境中，实现异地存储数据的保密性、完整性、可用性等问题，应该研究如何利用冗余机制在系统故障或崩溃的情况下提高系统可用性的问题，应该研究云中数据恢复、数据安全隔离等问题。

●云上分布计算特点提出的新的计算安全问题。

云计算重要特点和优点之一，是云可以提供几乎无限的计算能力，需要大规模计算的计算任务可以充分利用这一特点和优点。但是，在云上，计算一般是分布异地进行的，敏感计算任务存在保密问题；其次，由于在云上计算过程具有不透明性， 因此， 云上计算的可控性问题也需要研究；再次，由于在云上计算一般是分布异地进行的，且计算过程具有不透明性，因此，计算结果的真实性，或者说计算结果的可证明性也需要研究。综上，需要针对以上问题，研究云上安全的计算算法。

●云计算快速伸缩特点提出的新的综合安全问题。

云计算的重要特点和优点之一，是云计算具有快速伸缩特点，即云可以根据使用者的要求，在存储、计算、网络等等计算资源方面进行动态平衡和调整，当云上的存储资源较多时，可以给使用者调整出更多的存储资源；当云上的计算资源较多时，可以给使用者调整出更多的计算资源。这对于那些需要时间——空间折中计算的任务是十分必要的，也是十分有利的。但是，这种时间——空间的动态平衡和调整，对存储安全和计算安全提出了更高、更难的要求。

云计算新的信息安全问题还包括：

●云计算安全信任体系（身份认证、访问控制、取证）问题，具体包括：云与用户的双向身份认证，基于用户属性及访问权限的细粒度访问控制策略，云计算中隐私定义、隐私建模和隐私保护级别分类，在云环境中对信息安全事件进行追踪、计算机取证以及责任认定等。

●云计算监管监控（网络行为监管监控、内容监管监控）问题，具体包括：云环境中业务监测、威胁监测、环境监测、服务质量监测、数据分布监测等；对云计算中可能出现的异常网络行为、或不合法内容存储与传播等能进行及时监控，针对第三方的隐私保护技术等。

总之，云计算信息安全是一个新的研究和实践领域，至少在以下四个方面有必要进行深入研究：

一是云计算的特点分析；

二是云计算的信息安全风险分析；

三是云计算的信息安全模型与框架；

四是云计算的关键技术（如上述的关键技术）。

四、云计算信息安全解决方案

谢谢各位！