doi :10.3969/j.issn.1671-1122.2011.06.014

云计算环境下信息安全分级防护研究

董建锋[1]，裴立军[2]，王兰英[3]

（1.62301 部队自动化站，北京 100071；2. 二炮后勤部司令部，北京 100085；3. 二炮网管中心，北京 100085）

摘　要：文章通过对云计算带来的信息安全问题的分析，建立了云计算安全体系结构模型，进而提出按照等级防护的思路破解云计算安全防御难题的应对办法。

关键词：云计算；信息安全；等级防护

中图分类号：TP393.08　**文献标识码：**A　**文章编号：**1671-1122（2011）06-0038-03

Cloud Computing Environment of Information Security Level of Protection

DONG Jian-feng[1], PEI Li-jun[2], WANG Lan-ying[3]

(1.62301 *Force Automation Station, Beijing 100071, China;*
2. *ErPao Logistics Department Headquarters, Beijing* 100085*, China;*
3. *ErPao Network Management Center, Beijing* 100085*, China*)

Abstract: Through the cloud caused by the analysis of information security issues, the establishment of the security architecture of cloud computing model, puts forward the idea of protection in accordance with the level of security and defense challenges cloud break responses.

Key words: cloud computing; information security; level protection

0 引言

云计算是继计算机、网络出现之后的又一次信息领域的革新，通过跨地域、跨国界的整合，将计算资源以服务的形式提供给用户，将用户从复杂的底层硬件、软件与网络协议中解放出来，具有超强的计算能力和低成本、规模化等特性，只需少量投入就能得到所需要服务，已经成为下一代互联网的发展趋势。

目前，各国都加大了对云计算研究的投入力度，力争在技术、标准、服务和用户资源上获得控制权。就我国而言，云计算更合乎中国经济向服务型和高科技型转变的趋势，三网融合、政府和医疗信息化，以及大量快速成长的电子商务应用，给予了中国云计算强大的市场驱动力，可以说云计算的时代已经到来。另一方面，发达国家经过多年的技术研究和资源重组，正在逐步形成行业垄断；云计算安全事件频发，其稳定性、安全性、完整性等都是亟待解决的问题；加上公共平台的开放和不可控特性，云计算在给我国带来机遇的同时，也面临着信息安全的巨大挑战。

1 云计算技术面临的安全问题

云计算是信息技术领域的一次重大变革，IBM 创始人托马斯·沃森曾经预言：全世界只需要 5 台计算机。云计算的出现似乎让我们看到这个美好梦想实现的可能性。但随着云计算在各领域内的快速发展，安全事件也频繁发生：2007 至 2008 年间，亚马逊云计算平台出现了大范围的故障；2009 年，微软 Azure 云计算平台彻底崩溃，大量用户数据丢失；2009 年，谷歌公司“不小心”泄露了客户私人信息等等。这些陆续出现的一系列安全问题以及诸多潜在威胁，给人们对云计算的美好愿景敲响了警钟。“把资源和数据放到云端，安全是个问题”——已经成为人们谈到云计算时最为担忧的。

1.1 传统的安全边界消失

基于边界的安全隔离与访问控制是传统安全防护的重要原则，很大程度上依赖于各区域之间明显清晰的区域边界，强调的

收稿时间：2011-05-10

作者简介：董建锋（1976-）：男，山西，工程师，主要研究方向：信息安全；裴立军（1977-），男，工程师，主要研究方向：信息技术；王兰英 (1962.11-)，女，河北，高级工程师，硕士，主要研究方向：网络管理。

是针对不同的安全区域设置有差异化的安全防护策略；在云计算环境下，基础网络架构统一化，存储和计算资源高度整合，传统的安全设备部署边界正逐步消失，云计算环境下的安全部署需要寻找新的模式[1]。

1.2 虚拟化服务的安全问题

“计算机科学中的任何问题都可以通过增加一层映射而解决”[2]，按照这种思路，当前计算机系统的许多问题可以通过计算机系统的虚拟化而解决。同时，虚拟化作为云计算中心的关键技术，基于存储资源和服务器资源的高度整合，其自身的可扩展性能够极大地拓展基础设施和软件平台层面提供云服务的能力。在这种情况下，如何应对云计算中心基础网络架构、数据存储和应用服务的虚拟化交付，对安全设备的设计构建和安装部署提出了更高的技术要求，也成为云计算环境下信息安全建设所关注的重点。

1.3 数据集中后的安全问题

一是传统的网络中各种应用服务的标准流量和突发流量有迹可循，流量模型设计相对较为规范、简单，对安全设备的处理能力没有太高的要求。而在云计算环境下，同类型存储或者应用服务器的规模增长迅猛，动辄以万为单位进行扩展，并且不能分而治之，必须依托统一架构的基础网络来承载。与传统网络环境相比，这就对安全设备本身的性能指标提出了更高的要求。二是用户的数据存储、处理、网络传输等都与云计算系统有关。如何避免多用户共存带来的潜在风险；如何保证云服务的身份鉴别、认证管理和访问控制等安全机制符合用户的需求，并能够实施有效的安全审计，这些都成为云计算环境所面临的安全挑战[1, 2]。

1.4 稳定性和可靠性问题

一是云计算环境下，用户的数据和业务应用流程等均依赖于云计算所提供的虚拟化服务，这必然对云计算服务的稳定性、安全策略部署、容灾恢复能力和事件处理审计等提出了更高更进一步的需求。二是用户、信息资源的高度集中，相对传统的网络平台更加容易成为网络攻击的目标，因各类恶意代码、黑客程序、病毒木马等攻击造成的破坏程度将会呈指数级上升。

2 云计算给国家安全带来的风险[3]

可以看出，云计算在提供便利服务的同时，也带来了多种多样的信息安全风险，以上列出的仅是云计算技术本身的风险，就云计算服务体系来说，其最重要、最核心的风险是：国家安全风险和产业经济信息失控风险。

2.1 云计算对国家信息安全的威胁

以美国为代表的发达国家，为占领云计算这一制高点，保持在标准、技术和信息资源等方面的绝对优势，纷纷投入大量人力、物力，逐步推进符合自身利益的云计算战略，企图通过对云计算技术、标准和平台的垄断，进而达到控制全球信息资源的目的。试想，如果未来国家的数据和资源都高度集中在云端的话，一旦被窃取整合、处理分析，将势必对我们的国家信息安全造成严重威胁。

2.2 云计算对产业信息安全的威胁

近期，工业和信息化部、科技部等五部委联合发布了《关于加快推进信息化与工业化深度融合的若干意见》，其中明确指出要创新信息化与工业化深度融合推进机制。目前在研发、设计、采购、生产到营销这一价值链上，工业化和信息化的结合比以往任何时候都要紧密。其中，多数大中型企业选择的软件平台，都是由技术和服务水平上实力雄厚的跨国公司所提供的。同时，在云计算环境下，为满足用户对信息资源的访问和应用服务的需求，企业的管理信息系统将依托大型服务器集群，统一架构在虚拟化资源池中，形成所谓的“企业级云计算”。在这个大平台上，企业内部的商业机密必然会存在随时暴露的隐患，极大地威胁了企业的生存发展，进而影响了我国整体的产业信息安全。

因此，美国提出并主导的云计算服务体系虽然在应用上非常有价值，但是对于全球其他国家来说，这就是美国国家战略的一个部分，如果忽略了对这一点的深刻认识，不能从战略的高度去着手解决云计算带来的安全问题，中国的国家信息安全和信息产业发展必将会被美国所挟持。

3 实施等级防护应对云计算发展过程中的安全风险

早在 1994 年，国务院颁布了《中华人民共和国计算机信息系统安全保护条例》，之后又出台了一系列的意见、细则和办法。作为计算机信息系统重要发展方向之一的云计算系统，按照“分区分域、纵深防御”的原则，实行信息安全等级保护，建立健全云计算安全防御体系，是从整体上、根本上解决其安全问题的有效办法，已经成为关系到国家信息安全与信息产业发展的战略工程。

3.1 安全区域边界划分

云计算的安全体系结构总体上应该包括应用层安全、主机安全和网络安全，但具体的划分方式见仁见智，本文根据云计算需要解决的安全问题，将云计算安全防御体系等级防护结构划分为：基础网络级、虚拟化服务级和数据存储级三级防护模型，如图 1。并对照此结构模型的区域边界，确立了各自相应的防护内容，如表 1。

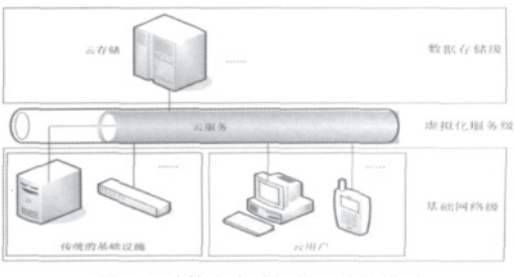

图1 云计算安全防御体系结构模型

表1 等级防护区域与安全防护内容对应表

等级防护区域划分	安全防护主要内容
基础网络级	保障各类计算资源基于统一基础架构的网络接入和运行平台的安全。
虚拟化服务级	保障整合、处理各种虚拟化资源，提供“按需服务”的承载平台的安全。
数据存储级	保障云计算海量数据存储、传输并实现数据安全隔离的支撑平台的安全。

3.2 安全机制

3.2.1 建立纵深防御机制，确保基础网络安全

一是要建立集中统一的云计算安全服务中心。在云计算环境下，物理的安全边界逐步消失，云计算平台的用户只能依靠基于逻辑的划分来实现隔离，而不再是以往基于单个或者按照类型来进行划分，更不能只实施简单的流量汇聚或部署孤立的安全防护系统来保障整个平台的安全。因此必须将安全服务的部署应用由基于各子系统的安全防护，转变为基于整个云计算架构网络的安全防护，提供集中统一的安全服务，从而适应这种逻辑隔离模型的要求。二是通过 VPN 和数据加密等技术，构建安全的逻辑边界。利用搭建好的技术安全通道，将提出安全服务需求的用户数据流，交付至安全服务中心分析处理，当服务完成后再按原有的转发路径返回至用户端，保障用户数据的网络传输安全。三是完善云计算平台的容灾备份机制，包括重要系统、数据的异地容灾备份。总之，建立云计算系统的纵深安全防御机制，就是要覆盖整个云计算服务的后台、网络和前端，从而提高整个云计算平台的安全性、可靠性，保障云计算服务的稳定性和连续性。

3.2.2 构建可靠的虚拟化环境，确保云计算服务安全

“按需服务”是云计算平台的终极目标，而只有借助虚拟化技术，才有可能根据用户的需求，来提供个性化的应用服务和合理的资源分配。也就是说，无论是基础的网络架构，还是存储和服务器资源，都必须要支持虚拟化，才能提供给用户端到端的云计算服务。因此，秉承安全即服务的理念，在云计算数据中心内部，一是应采用 VLAN 和分布式虚拟交换机等技术，通过虚拟化实例间的逻辑划分，实现不同用户系统、网络和数据的安全隔离；二是应采用虚拟防火墙和虚拟设备管理软件为虚拟机环境部署安全防护策略，并对云计算系统的运行状态和进出的数据流量实施实时监控，及时发现并修复虚拟网络和系统异常；三是应采用防恶意软件，建立补丁和版本管理机制，防范因虚拟化带来的潜在安全隐患，确保虚拟化环境与物理网络环境一样安全、可靠。

3.2.3 综合应用多种技术手段，确保数据安全

数据的存储安全，确保用户信息的可用性、隐私性和完整性，是云计算安全的核心内容，无论是数据的加密、隐藏，还是数据资源的灾难备份等方面，都是围绕着数据安全展开的。因此，在云计算环境下，一是应采用数据加密技术，建立密钥管理与分发机制，实现用户信息和数据的安全存储与安全隔离，防止用户间的非法越权访问；二是应实施严格的身份监控、登录认证、权限控制和用户访问审计，实现用户信息和数据的高效维护与安全管理；三是应完善和建立数据备份恢复机制和残余信息保护措施，保证当用户数据发生异常时能够及时的进行恢复；保证当存储资源被重新分配给新用户时，提前做好可靠的数据擦除，防止原用户数据被非法恢复。

3.3 安全防护手段

一个完整的云计算安全模型，应该是以身份认证（身份鉴别）为基础、以数据安全（数据加密）和授权管理（访问控制）为核心，以监控审计（安全审计）为辅助的安全防御体系，结合本文提出的云计算安全体系等级防护结构模型，应将各类安全防护手段落实到各个等级区域边界中，从而保证各级安全目标的实现，如表 2 所示。

表2 云计算安全等级防护体系与安全防护手段对照表

等级防护	主要技术手段
基础网络级	主机身份鉴别
	VPN 和数据加密
	安全隔离
	访问控制
	安全审计
	入侵防范
	恶意代码防范
	终端准入控制
	终端安全加固
	容灾备份
虚拟化服务级	VLAN 隔离
	分布式虚拟交换
	流量监控
	虚拟防火墙
	身份认证
	访问控制
	安全审计
	版本和补丁管理控制
	资源控制
数据存储级	身份认证
	数据加密
	数据擦除
	备份与恢复

4 结束语

作为下一代互联网技术的一项重大变革，云计算给予中国一个新的发展机遇，如果错过了这次机会，中国将失去信息技术领域的话语权和实现跨越式发展的主动权。而在发展云计算的同时，必须认识到云计算给信息安全带来的巨大威胁。安全是云计算服务首要前提，是云计算可持续发展的基础，面对诸多挑战，没有回避的空间，只能积极参与到云计算安全平台的建设研发当中，通过大力推广具有自主技术的云产品，实行严格的信息安全等级保护，进而构建中国自己的云计算安全防御体系，最终使云计算的安全性难题得到破解。相信随着整个云计算产业链的不懈努力，中国的云计算应用及服务必将朝着可信、可靠、可持续的方向健康发展。（责编 杨晨）

参考文献：

[1] 比特网 . 云计算环境下安全模型与传统安全模型的差异 [EB/OL].http://datacenter.chinabyte.com/195/11459195.shtml, 2010-08-03/2011-05-09.

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

[3] 王燕等 . 云计算时代对我国信息安全的思考 [J]. 现代管理科学，2011，(02)：29.