

# 云计算环境下信息安全分析

张 慧<sup>1</sup>, 邢培振<sup>2</sup>

(1. 中州大学, 河南 郑州 450044;

2. 华北水利水电学院 水利职业学院, 河南 郑州 450000)

**摘 要:**基于互联网的云计算被认为是当今互联网发展的方向,近年来引起人们的广泛关注,如何构建安全的云计算环境成为当前计算机学科研究的热点问题之一。文中从云计算的发展现状入手,介绍了NIST推出的云计算规范、五个本质特征和云计算服务模型,分析了CSA云计算安全参考模型和Jericho Forum的云立方体模型,并从安全边界、数据安全、应用安全三个方面讨论了当前云计算环境下存在的信息安全问题,最后给出了云计算环境下保证信息安全的解决方案。

**关键词:**云计算;信息安全;模型

**中图分类号:**TP309

**文献标识码:**A

**文章编号:**1673-629X(2011)12-0164-03

## Information Security Analysis in Cloud Computing Environment

ZHANG Hui<sup>1</sup>, XING Pei-zhen<sup>2</sup>

(1. Zhongzhou University, Zhengzhou 450044, China;

2. Water Conservancy Vocational College, North China Institute of Water Conservancy  
and Hydropower Institute, Zhengzhou 450000, China)

**Abstract:** Internet-based cloud computing is considered to be the direction of development of the Internet today, has attracted much attention, how to build secure computer cloud computing environments become one of hot research subjects. In this paper, from the status quo of the development of cloud computing, first introduced the launch of the cloud NIST standard, the five essential characteristics and cloud computing services model, and then analyzed the CSA cloud computing model and the Jericho Forum security reference cube model of the cloud, and from the security boundary, data security, application security discussed the information security problem of the current cloud computing environment, given the security solutions in cloud computing environment to ensure information.

**Key words:** cloud computing; information security; model

## 0 引 言

云计算是分布式处理(Distributed Computing)、并行处理(Parallel Computing)和网络计算(Grid Computing)的发展,是透过网络将庞大的计算处理程序自动分拆成无数个较小的子程序,再交由多台服务器所组成的庞大系统经计算分析之后将处理结果回传给用户。通过云计算技术,网络服务提供者可以在数秒之内,处理数以千万计甚至亿计的信息,达到和“超级计算机”同样强大的网络服务。云计算系统的建设目标是将原来运行在PC上或单个服务器上独立的、个人化的运算转移到一个数量庞大的服务器“云”中,由这个云计算系统来负责处理用户的请求,并输出结果,它是一个以数据运算和处理为核心的系统。

文中从云计算发展现状入手,分析了云计算安全参考模型并从安全边界、数据安全、应用安全三个方面讨论了云计算环境下信息安全问题。

## 1 云计算概述

### 1.1 云计算概念

美国国家标准技术研究院(NIST)推出云计算规范之后,业界的认可度非常高,几乎可认为这是目前最权威的云计算定义。定义如下:云计算是一个模型,这个模型可以方便地按需访问一个可配置的计算资源(例如,网络、服务器、存储设备、应用程序以及服务)的公共集。这些资源可以被迅速提供并发布,同时最小化管理成本或服务提供商的干涉。

### 1.2 云计算规范核心

(1)云计算五个本质特征。

按需的自我服务、广泛的网络访问、资源池、快速的弹性能力、可度量的服务。

(2)云计算服务模型。

收稿日期:2011-04-28;修回日期:2011-08-01

基金项目:2010年郑州市科技计划(10PTGG345-5)

作者简介:张 慧(1977-),女,河南郑州人,硕士,讲师,主要从事多媒体、信息安全研究。

· 软件即服务 (SaaS)。客户所使用的服务商提供的这些应用程序运行在云基础设施上。这些应用程序可以通过各种各样的客户端设备所访问,通过瘦客户端界面像 WEB 浏览器(例如,基于 WEB 的电子邮件)。客户不管理或者控制底层的云基础架构,包括网络、服务器、操作系统、存储设备,甚至独立的应用程序机能,在可能异常的情况下,限制用户可配置的应用程序设置。

· 平台即服务 (PaaS)。客户使用云供应商支持的开发语言和工具,开发出应用程序,发布到云基础架构上。客户不管理或者控制底层的云基础架构,包括网络、服务器、操作系统或者存储设备,但是能控制发布应用程序和可能的应用程序运行环境配置。

· 架构即服务 (IaaS)。向客户提供处理、存储、网络以及其他基础计算资源,客户可以在上运行任意软件,包括操作系统和应用程序。用户不管理或者控制底层的云基础架构,但是可以控制操作系统、存储、发布应用程序,以及可能限度地控制选择的网络组件。

### (3) 云计算发布模型。

· 私有云。云基础架构被一个组织独立地操作,可能被这个组织或者第三方机构所管理,可能存在于某种条件下或者无条件存在。

· 社区云。云基础架构被几个组织所共享,并且支持一个互相分享概念的特别的社区。可能被这些组织或者第三方机构所管理,可能存在于某种条件下或者无条件存在。

· 公有云。云基础架构被做成一般公共或者一个大的工业群体所使用,被某个组织所拥有,并出售云服务。

· 混合云。云基础架构是由两个或者两个以上的云组成,这些云保持着唯一的实体但是通过标准或者特有的技术结合在一起。这些技术使得数据或者应用程序具有可移植性。

## 2 云计算安全参考模型

实际使用中的云产品,在服务模型、部署模型、资源物理位置、管理和所有者属性等方面呈现出不同的状态和消费模式,因而具有不同的安全风险特点和安全控制职责和范围。因此,需要从安全防范角度建立云计算的参考模型,实现云服务架构到安全架构之间的互联,为识别风险、控制安全和决策方案提供依据<sup>[1]</sup>。

### 2.1 CSA 的模型

CSA (cloud security alliance 云安全联盟)从服务模

型的角度提出了基于三种基本云服务的层次性及其依赖关系的安全参考模型<sup>[2]</sup>,如图 1 所示。该模型的特点在于供应商所在的级别越低,云服务用户所要承担的安全责任就越大。

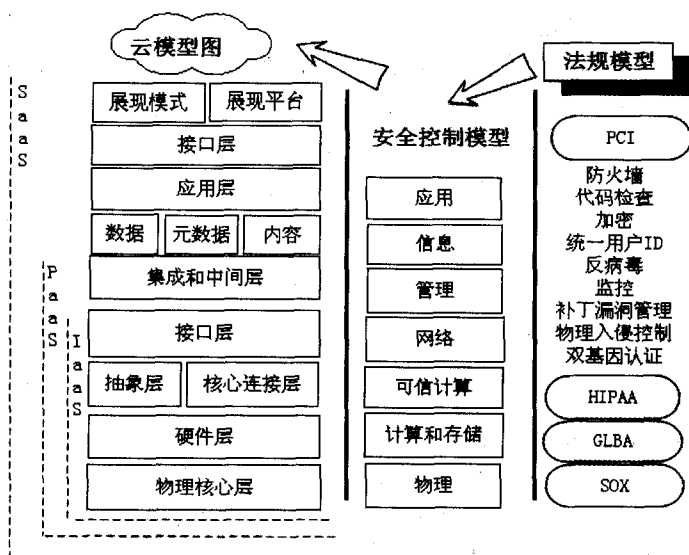


图 1 云服务安全参考模型

### 2.2 Jericho Forum 的云立方体模型

从安全协同的角度,Jericho Forum<sup>[3]</sup>从数据的物理位置(internal 和 external)、云相关技术和服务的所有关系状态(proprietary 和 open)、应用资源和服务时的边界状态(perimeterised 和 de-perimeterised)、云服务的运行和管理者(insourced 和 outsourced)4 个影响安全协同的维度上分为 16 种可能的云计算形态,用如图 2 所示的云立方体模型展示。

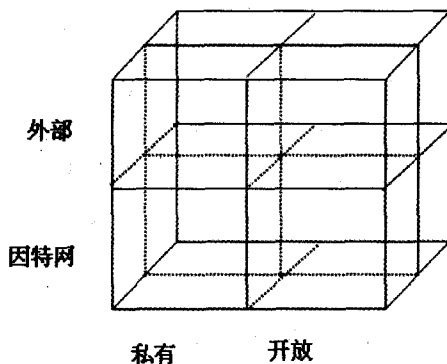


图 2 云立方体模型

云计算形态的不同使得其具有不同的协同性、灵活性及其安全风险特征。云服务用户需要根据自身的业务和安全协同需求选择云计算形态。

文中针对云计算信息安全中的数据安全和应用安全进行了重点阐述,如图 3 所示。

## 3 云计算信息安全问题

云计算由于其用户、信息资源的高度集中存在更

多的安全隐患,概括来讲,云计算主要存在以下安全问题。

### 3.1 安全边界难以定义

在传统网络中通过物理上和逻辑上的安全域定义,可以清楚地定义边界和保护设备用户,但云计算由于其用户数量庞大,数据存放分散,很难充分为用户提供安全保障。

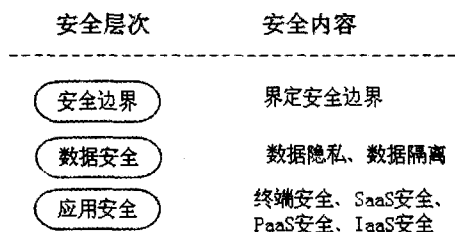


图 3 云安全内容

### 3.2 数据安全

使用云计算服务,用户并不是清楚自己的数据具体的托管服务器的位置以及具体是哪个服务器管理。基于此云用户和云服务商为避免数据丢失和窃取都非常重要,以下从数据隐私和数据隔离两个方面对云计算的安全进行阐述。

(1) 数据隐私。除了软件即服务 (software as a service, SaaS) 供应商之外,云服务供应商一般没有能力处理敏感数据(隐私数据)。数据在云服务中的存储是共享的,即没有为用户开辟独立存储区。由此数据具有潜在危险。现行的适用于局域网内的数据访问风险/利益评估方法同样也可用在云服务上<sup>[4]</sup>。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来负责维护,并且由于云计算架构的特点,这些数据可能存储在分散的地方,并且都以明文的形式存储。防火墙虽然能够对恶意的外来攻击提供一定程度的保护,但这种架构使得一些关键性的数据可能被泄露。构建私有云或者混合云来实现弹性计算和数据隐私的保护是目前一种可行的方案<sup>[5,6]</sup>。

(2) 数据隔离。目前在网络中用户基本采用数据加密方式共享数据,但在云计算环境下,如果能够将自己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。搭建于云计算平台的软件系统广泛采用 Multi-Tenancy(多租户)架构,因为所有客户数据将被共同保存在唯一一个软件系统实例内,所以需要开发额外的数据隔离机制来保证各个客户之间的数据的保密性并提供相应的灾备方案<sup>[7]</sup>。

现行的几种成熟的架构能够为系统实现数据隔离:Shared Schema Multi-Tenancy(共享表架构)、Separated Database(分离数据库架构)以及 Shared Database Separated Schema(分离表架构)<sup>[8]</sup>。不过目前云计算的数据隔离技术也仅仅是最大限度地保证用户私有数

据的安全性,绝对的安全很难做到。单租户专用数据平台能够更好地为云计算用户提供数据隔离,但其耗资巨大,并非每个用户所能承担。由此可见云计算环境下的数据隔离技术需进一步改进,以推动云计算的发展。

### 3.3 应用安全

#### (1) 终端安全。

用户终端的安全始终是网络环境下信息安全的关键点,用户终端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。

#### (2) SaaS 应用安全<sup>[9,10]</sup>。

SaaS 模式使用户使用服务商提供的在云基础设施之上的应用,对于底层的云基础设施如:网络、操作系统、存储等。因此在此模式下,服务商将提供整套服务包括基础设施的维护。服务商最大限度地为用户提

#### (3) PaaS 应用安全。

PaaS 云使用户能够在云基础设施之上创建用户和购买行为,用户同样并不管理和控制底层的基础设施,但可以控制基于基础设施之上的应用。PaaS 提供商通常会保障平台软件包安全,因此用户需要对服务提供商有一个清楚的认识,比如对服务提供商做风险评估。同时,PaaS 还面临配置不当的问题,默认配置下的安全系数几乎为零,因此,用户需要改变默认安装配置,对安全配置流程有一定的熟悉度。

#### (4) IaaS 应用安全。

用户对于 IaaS 云提供商来讲是完全不透明的,云提供商并不关注用户在云内的任何操作,因此,用户需要对自己在云内的所有安全负全责,IaaS 并不为用户提供任何安全帮助。

## 4 云安全解决方案

云计算的迅速兴起给人们带来了新的安全思考,带来了新的安全挑战。目前全球范围内各行业相关者都在努力寻求云安全解决方案。CSA 的《云计算关键领域安全指南》<sup>[2]</sup>对云计算中每一关键领域的安全控制实施均提出了建议,指导用户对云计算服务有更为深入的认识,为用户安全地使用云服务提供了指南。在指南中还提出了针对 IaaS 云、PaaS 云及 SaaS 云的解决方案。针对安全敏感问题如:业务连续性、灾难恢复、应急响应、通告和补救提出了解决方案,同时还在云治理方面提出了有效建议,涉及企业风险管理、法律和电子证据发现、身份管理等问题。《云计算关键领域

(下转第 171 页)

- 程,2006(3):70-72.
- [3] 朱若磊. 利用核心态钩挂技术防止代码注入攻击[J]. 计算机应用,2006,26(9):2134-2136.
- [4] 余俊松,张玉清,宋 杨,等. Windows 下缓冲区溢出漏洞的利用[J]. 计算机工程,2007,33(17):162-164.
- [5] 苏 朋,陈性元,唐慧林. Windows 缓冲区溢出 Exploit 代码分析研究[J]. 计算机安全,2008(1):48-52.
- [6] 王志飞. Windows 平台下缓冲区溢出的攻击及防卫[J]. 辽宁师专学报(自然科学版),2005(2):12-17.
- [7] Avijit K, Gupta P, Gupta D. TIED, LibsafePlus: Tools for runtime buffer overflow protection [C]//Proceedings of the 13th Conference on USENIX Security Symposium. Berkeley: Usenix Association,2002:191-206.
- [8] 张小斌,严望佳. 黑客分析与防范技术[M]. 北京:清华大学出版社,1999:97-104.
- [9] Rozinov K. Stackguard Protecting Against Buffer Overflows Part I - Detailed Overview [D]. [s. l.]:Polytechnic University,2003.
- [10] 大 熊. Windows 内置的病毒防护-DEP[J]. 电脑爱好者,2005(7):86-87.
- [11] 赵 磊,蒋本伦,朱玉龙. 无线局域网非授权访问控制技术[J]. 今日科苑,2008(15):108-108.
- [12] Dong Guozhu, Su Jianwen. Incremental Maintenance of Recursive Views Using Relational Calculus/SQL \* [J]. ACM SIGMOD Record,2000,29(1):44-51.
- [13] Waldspurger C A. Memory resource management in VMware ESX server [C]//In:Proceedings of 5th Symposium on Operating Systems Design and Implementation(OSDI). New York: ACM,2002:181-194.
- [14] Poon E, Fleet D J. Hybrid Monte Carlo Filtering: Edge-Based People Tracking [J]. IEEE Motion and Video Computing, 2002,5(11):151-158.
- [15] Oechslin. Making a faster cryptanalytic time-memory trade-off [C]// Proc. CRYPTO'03. [s. l.]:Springer,2003:617-630.
- [16] ORIGIN2000 服务器 SPEC 基准测试性能创世界记录[J]. 计算机辅助设计与制造,1997(7):58-58.
- [17] Craig J C, Webb J. Microsoft Visual Basic6.0 程序开发环境 [M]. 北京:博彦科技发展有限公司,2000:320-326;625-635.
- [18] 吴业福. 用 VB6 实现汉字的加密方法探讨[J]. 计算机应用研究,2001(3):143-145.
- [19] Wilander J, Kamkar M. Comparison of Publicly Available Tools for Dynamic Buffer Overflow Prevention [C]//10th Network and Distributed System Security Symposium. [s. l.]:[s. n.], 2003:149-162.
- [20] Ringenburt M, Grossman D. Preventing format-string attacks via automatic and efficient dynamic checking [C]//Proceedings of the 12th ACM Conference on Computer and Communications Security. [s. l.]:[s. n.],2005:354-363.

(上接第 166 页)

安全指南》为接触云服务提供商的企业提供有效的信息安全对策,CSA 成员仍在继续云信息安全对策的研究。

从管理角度看,随着云计算的发展,NIST、ISACA 均提倡用管理的手段控制和减小云计算安全风险。云计算服务级别协议(SLA)是云计算服务提供商和云服务用户间唯一的法律协议<sup>[11]</sup>,云服务提供商通过 SLA 获得用户信任,考虑到云计算和大型主机时代之间的相似性(对远程资源的高度依赖),云计算服务级别协议(SLA)的广泛使用势在必行<sup>[12]</sup>。

## 5 结束语

云计算是近年来的研究热点,文中分析了云计算环境下存在的信息安全问题,随着云计算的进一步发展和应用,信息安全问题势必成为云计算发展的关键技术问题,在这方面的研究还有很长的路要走。

## 参考文献:

- [1] 赵 粮,裴晓峰. 云计算环境的安全威胁和保护[J]. 中国计算机学会通讯,2010,6(5):47-50.
- [2] CSA. Security Guidance for Critical Areas of Focus in Cloud Computing V2. 1 [EB/OL]. [2010-05-10]. <http://www.cloudsecurityalliance.org/guidance/>.
- [3] Forum J. Cloud cube model: selecting cloud informations for secure collaboration [EB/OL]. [2010-05-10]. [http://WWW.opongroup.org/Jericho/eloud\\_cube-model\\_0.pdf](http://WWW.opongroup.org/Jericho/eloud_cube-model_0.pdf).
- [4] McCalline S, Jacobson V. The BSD Packet Filter: A New Architecture for User-level Packet Capture [C]//Proceedings of the 1993 Winter USENIX Technical Conference. San Diego, CA:USENIX,1993.
- [5] Miller M. 云计算[M]. 姜进磊,孙瑞志,向 勇,等译. 北京:机械工业出版社,2009.
- [6] 张为民,唐剑峰,罗治国,等. 云计算深刻改变未来[M]. 北京:科学出版社,2009.
- [7] 叶 伟. 互联网时代的软件革命-SaaS 架构设计[M]. 北京:电子工业出版社,2009.
- [8] 李德毅. 云计算:从图灵计算到网络计算[C]. 2009 云计算中国论坛. 出版地不详:出版者不详,2009.
- [9] 王 鹏,黄华峰,曹 珂. 云计算:中国未来的 IT 战略 [M]. 北京:人民邮电出版社,2010.
- [10] IBM 虚拟化与云计算小组. 虚拟化与云计算[M]. 北京:电子工业出版社,2009.
- [11] ISACA. Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives [EB/OL]. [2010-05-10]. <http://WWW.isaca.org/Template.cfm?Section=Nederlands&Template=/search/SearchDisplay.cfm>.
- [12] 张云勇,陈清金,潘松柏,等. 云计算安全关键技术分析 [J]. 电信科学,2010(9):64-69.