

# 解读云立方体模型

黄秀丽

(国网电力科学研究院, 江苏 南京 210003)

**摘要:**作为一种新兴的技术,云计算的出现给IT界带来了很大的变革。但和所有新技术一样,云计算也将带来新的风险。面对云计算的各种风险,业务该怎样搬进什么样的云里,是所要面临的亟待解决的问题,也是文中研究的重点。首先分析了云计算带来的风险,给出了风险各要素之间的关系;接着,介绍了云立方体模型,对云立方体模型各个维度进行了详细的解读,在此基础上,介绍了COA技术;最后,结合电力系统,对电力云进行了思考,对未来的工作给出了建议。

**关键词:**云计算;云安全;云立方体模型;COA技术;解读

**中图分类号:**TP309

**文献标识码:**A

**文章编号:**1673-629X(2012)03-0245-04

## Analysis of Cloud Cube Model

HUANG Xiu-li

(State Grid Electric Power Research Institute, Nanjing 210003, China)

**Abstract:** As an emerging technology, cloud computing brings a lot of changes into the IT industry. But same as all new technologies, cloud computing will also bring new risks. Facing the risks of cloud computing, how do move into what kind of clouds is a serious problem and the research content of this paper. First analyze the risks of cloud computing and show the relationship between the various elements of risk, then present the cube model of the cloud and COA technology in detail, and finally think about state grid cloud and give recommendations for future work according to state grid.

**Key words:** cloud computing; cloud security; cloud cube model; COA technology; analysis

### 1 概述

美国国家标准与技术研究院 NIST 给云计算定义了五个关键特征、三个服务模型、四个部署模型<sup>[1]</sup>。五个关键特征为按需自服务、宽带接入、虚拟化的资源“池”、快速弹性架构、可测量的服务。三个服务模型为云软件作为服务(SaaS)、云平台作为服务(PaaS)、云基础设施作为服务(IaaS)。四个部署模型为公共云、私有云、社区云、混合云。

作为一种新兴的技术,云计算的特征、服务模型和部署模型将给IT界带来很大的变革,同时给人们的生活带来极大的便利,但和所有新技术一样,云计算也将带来新的风险。国际知名市场研究公司 Gartner 发布的《云计算安全风险评估》的研究报告称,云计算服务存在着七大潜在安全风险,即特权用户的接入、可审查性、数据位置、数据隔离、数据恢复、调查支持和长期生存性。

云计算仍是一个迅速变化的领域,要么保持在最前沿,要么就会落后。但针对云计算的各种风险,该怎

样、在哪里、搬进什么样的云里,是亟待解决的问题。面对云,需要选择符合自己需要的云形态,来确保安全,并符合相关的法律法规要求。

### 2 云立方体模型

在云中,所面临的风险与下列因素有关:信息所处的位置、所要管理的资产资源和信息类型、管理者和管理方法、控制和集成方法、合规性问题。各因素、要素关系图如表1所示。

表1 各要素关系图

	云设施管理权	云设施所有权	云设施位置	接入和使用安全性
公共	第三方	第三方	场外	不可信
私有/社区	组织	组织	场内	可信
	第三方	第三方	场外	
混合	组织和第三方	组织和第三方	场内和场外	可信与不可信

针对这些因素,Jericho论坛提出了云立方体模型<sup>[2]</sup>,将云服务模型、部署模型、资源物理位置、管理和所有者属性等图形化展示,云立方体模型如图1所示。

云立方体模型确定了四个维度(参见表2),定义了不同的云形态,描述了每个云形态的关键特征、效益

和风险。其提供了一个框架,以更详细地探索不同云形态的本质和使之安全工作涉及的一些问题。

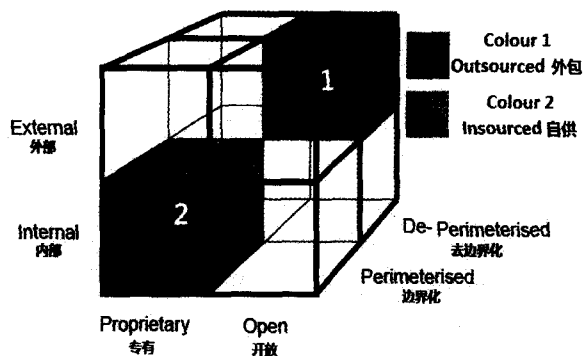


图1 云立方体模型

表2 云立方体模型维度表

序号	维度	备注
1	Dimension: Internal (I) / External (E)	维度:内部/外部
2	Dimension: Proprietary (P) / Open (O)	维度:私有/开放
3	Dimension: Perimeterised (Per) / De-perimeterised (D-p) Architectures	维度:边界化/去边界化 架构
4	Dimension4: Insourced / Outsourced	维度:自供/外包

### 3 云立方体模型解析

云立方体模型很形象地阐述了市场上现有云产品<sup>[3,4]</sup>的各种排列组合,提出了用以区分云从一种形态转换到另外一种形态的四种准则/维度,以及各种组成的供应配置方式,用以理解云计算影响安全路线的方式。本节针对云立方体的四个维度进行阐述,以解析云立方体模型。

#### 3.1 维度1:内部/外部

本维度表达的是“数据物理位置”,衡量依据是云数据是否在公司内部。如果部署在公司内则是内部维,反之是外部维。

例如,虚拟化<sup>[5]</sup>硬盘位于公司的数据中心属于内部维,亚马逊 SC3 位于“场外”属于外部维。此处注意不要做出内部比外部安全的错误假设。有时候,根据实际情况,也许有效结合两个维度一起使用能提供较安全的模型。本维度图示如图2所示。

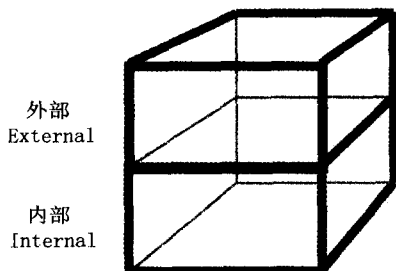


图2 维度1:内部/外部

#### 3.2 维度2:私有/开放

第二维度表达的是“技术路线”,此维度定义云技术、服务、接口等所有权,表明了云间的互操作性程度<sup>[6]</sup>,即私有系统和其它云间的“数据/应用可移植性”。

私有云是指云服务商拥有自己私有的服务手段,云中服务为私有运营,不经过大的改动,无法将“数据/应用”转移到其它云中。技术进步和创新多发生在私有领域,而私有云服务商常通过专利和商业技术秘密加以限制和保护。

开放云<sup>[7]</sup>使用开放技术,使用开放技术的云之间共享数据或相互协作时,由于使用了同样的开放技术而不受限制。一个尚未得到证实的前提是,开放云将是最有效地提高多个组织之间合作的云。本维度图示如图3所示。

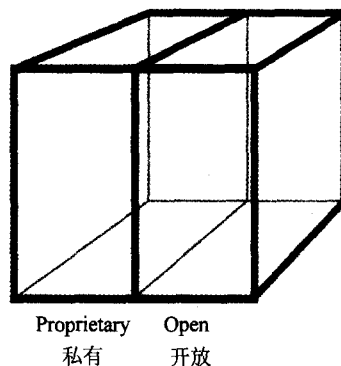


图3 维度2:私有/开放

#### 3.3 维度3:边界化/去边界化 架构

第三个维度表达的是“体系理念”,即云在公司的传统 IT 边界里面还是外面。

边界化意味着继续在以防火墙为标志的传统 IT 边界内经营,这种做法阻碍合作。边界化情况下,可以通过 VPN<sup>[8]</sup>简单地延伸组织边界到外部云域,在公司的 IP 域内运营虚拟服务器,利用目录服务来控制访问。当计算任务完成后,把边界退回到原来的传统位置。

去边界化是指传统 IT 周边的逐渐移除。假定系统边界是遵循 COA 架构<sup>[9]</sup>原则构建(例如数据通过元数据和防止数据不当使用的机制一起封装),由于 COA 系统允许安全合作,因此在去边界化环境里,公司能与第三方(业务伙伴、客户、供应商、外包方等)越过任何 COA 网络进行全球性的安全合作。

目前可以在任何体系理念-边界化或非边界化里运营四种云形态(I/P, I/O, E/P, E/O)。右上方的云形态 E/O/D-p 很可能是“最优点”,能实现最优的灵活性和合作。

基于最佳商业利益方面的考虑,私有云服务商

希望通过能增值的持续创新或限制从私有域迁移,把云用户留在立方体的左侧。从左上方云形态转移到右上方“最优点”云需要一种特殊的接口。本维度图示如图4所示。

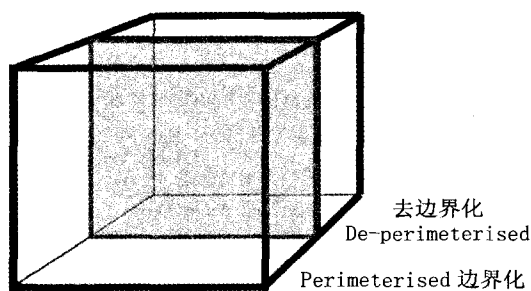


图4 维度3:边界化/去边界化

### 3.4 维度4:自供/外包

第四维度阐述的是“运维管理问题”。8个云形态 Per(I/P, I/O, E/P, E/O) 和 D-p(I/P, I/O, E/P, E/O) 里每个云形态有两种运维管理状态:自供和外包。公司自己控制运维管理属于自供维,运维管理服务外包给第三方是外包维。

这两个状态描述了运维管理权的归属,其主要是一个策略问题(即商业决定,而不是技术或架构的决定)。在云立方体模型图中用两种颜色表示(颜色1和2)第四维度,8个云形态均可以采用两种颜色中的任一颜色。

## 4 COA 技术

云立方体模型维度3中提到面向合作的 COA (Collaboration Oriented Architectures) 架构,COA 架构是为了满足公司在复杂威胁的开放环境下与众多外界合作方安全可靠地大量交互信息所设计的一个安全架构。为了达到开放式环境下的信息安全交互的目标,COA 架构中提出了信息系统需要满足的一些基本要求,并在 COA Framework<sup>[10]</sup> 中详细描述了 COA 架构的功能组件,其基本功能组件包括规则、过程、服务、属性、技术等五种。

COA 架构由 Jericho 论坛提出,为了支撑 COA 架构的设计和实施,Jericho 论坛同时提出了相应系列的技术配套文档,这些文档覆盖了设计原则、安全管理、过程管控、技术支撑等各个方面内容。

●设计规则系列文档描述了实施 COA 架构时要遵循的一些基本原则<sup>[11]</sup>,总共有 11 条:

- (1) 针对资产风险有明确恰当的防护水平和防护范围;
- (2) 安全机制必须普通、简单、可扩展、易于管理;
- (3) 基于威胁上下文;
- (4) 设备和应用必须用开放的安全协议通信;

(5) 所有设备能在非信任环境下自主配置安全策略;

(6) 所有人、流程、技术在交易中必须有公开透明的信任水平;

(7) 相互间的信任水平必须可测;

(8) 认证、授权、审计必须外部协同/交互;

(9) 接入数据由数据自身的安全属性控制;

(10) 数据隐私要求权责分离;

(11) 数据必须安全地存储、传输、使用。

●安全管理系列文档描述了身份管理、信任管理<sup>[12]</sup>、策略管理、审计和合规等四个方面的内容要求,信任管理部分涉及了内部端到端信任、组织间信任、设备间信任、商业影响等级、信息敏感分类、企业关系管理等方面内容。

●过程管控系列文档描述了个人周期管理、风险周期管理、信息周期管理<sup>[13]</sup>、企业周期管理等五个方面的内容要求,信息生命周期管理对信息声明周期进行了分析并给出了建议模型 ILM Process Model。

●技术支撑系列文档描述了 COA 架构中的关键技术,包括终端安全、内部安全通信、无线安全协议、移动终端管理安全协议、VOIP 安全协议、网络过滤、封装 & 加密<sup>[14]</sup>、数据安全等内容。

## 5 对国家电网云形态的思考

云立方体模型呈现的 16 种云形态,每一个都有不同的特点、不同程度的灵活性、不同的合作机会和不同的风险度。因此,国家电网在考虑云作为一种选择时,要根据实际应用,为不同类型业务运营选择最适合的云形态,以顺利地转型为云服务。

目前,电力系统所有业务的基础设施都部署在国家电网内部。在数据方面,国家电网在几个主要省市部署了自己的数据容灾中心。因此,在表达位置的内部/外部维上,属于内部维。

对于表达技术路线理念的私有/开放维上,考虑到将来智能电网可能需要某些特殊的电力应用需求,国家电网可以采取走私有和开放两种技术路线,通用要求采用开放技术路线,特殊要求采用私有技术路线。

目前,由于国家电网业务独立性比较强,与外界交互需求少,因此防护采用的是外围传统边界化防护,内部物理和逻辑隔离技术。但是随着 IT 技术的发展和业务需求交互的增多,去边界化架构(即新边界架构)将会逐步替代传统边界架构。电力系统作为国家重要的基础系统之一,在构建云形态时,首要考虑的关键因素是安全,因此在选择表达架构理念的边界化/去边界化维时,可根据业务的独立性和安全性需求,考虑采用边界化和去边界化结合的架构,或待新边界技术发展

成熟时仅采用去边界化架构。

国家电网所有业务的运维管理均由专设机构承担,在表达运维管理权的自供/外包维度上,属于自供。

由上可知,国家电网云形态可能会采用如下几种形态:  $I/(O \& P)/D - p/Ins$ 、 $I/O/D - p/Ins$ 、 $I/(O \& P)/(Per \& D - P)/Ins$ 、 $I/O/(Per \& D - P)/Ins$ 。

## 6 结束语

云立方体定义的云形态维度主要是商业决策因素,其中有的涉及技术因素,有的不涉及技术因素。云计算安全<sup>[15]</sup>的架构和技术问题的研究处于云立方体模型的下一层次,每种云形态都有自己的安全特点。基于云的身份、信誉、认证<sup>[16]</sup>、访问和授权、治理与合规等等,是需要进一步研究的众多相关的主题。

### 参考文献:

- [1] Mell P, Grance T. The NIST Definition of Cloud Computing [R/OL]. 2011-01. [http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145\\_cloud-definition.pdf](http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf).
- [2] Jericho. Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration [R/OL]. 2009-04. [https://www.opengroup.org/jericho/cloud\\_cube\\_model\\_v1.0.pdf](https://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf).
- [3] Buyya R, Yeo C S. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities [C]//Proc of the 2008 10th IEEE International Conf on High Performance Computing and Communications. [s.l.]: [s.n.], 2008.
- [4] Weiss A. Computing in the clouds [J]. Networker, 2007, 11(4): 16-25.
- [5] DMTF. Open Virtualization Format Specification [R/OL]. 2010-01-12. [http://www.dmtf.org/standards/published-documents/DSP0243\\_1.1.0.pdf](http://www.dmtf.org/standards/published-documents/DSP0243_1.1.0.pdf).
- [6] DMTF. Interoperable Clouds [R/OL]. 2009-11-11. [http://www.dmtf.org/about/cloud-incubator/DSP\\_ISO101\\_1.0.0.pdf](http://www.dmtf.org/about/cloud-incubator/DSP_ISO101_1.0.0.pdf).
- [7] OCM. Open Cloud Manifesto [R/OL]. 2009-04. <http://www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf>.
- [8] Pepelnjak I, Guichard J. MPLS and VPN Architectures [M]. Indianapolis, USA: Cisco Press, 2002.
- [9] Jericho. Collaboration Oriented Architectures [R/OL]. 2008-11. [http://www.opengroup.org/jericho/COA\\_v2.0.pdf](http://www.opengroup.org/jericho/COA_v2.0.pdf).
- [10] Jericho. COA Framework [R/OL]. 2008-11. [http://www.opengroup.org/jericho/COAFwk\\_v2.0.pdf](http://www.opengroup.org/jericho/COAFwk_v2.0.pdf).
- [11] Jericho. Commandments [R/OL]. 2007-05. [http://www.opengroup.org/jericho/commandments\\_v1.2.pdf](http://www.opengroup.org/jericho/commandments_v1.2.pdf).
- [12] Jericho. Trust Management-A Brief Overview [R/OL]. 2009-01. [http://www.opengroup.org/jericho/COA\\_TrustManagementOvw.pdf](http://www.opengroup.org/jericho/COA_TrustManagementOvw.pdf).
- [13] Jericho. Information Lifecycle Management [R/OL]. 2009-01. [http://www.opengroup.org/jericho/COA\\_Information\\_Lifecycle\\_Management\\_v1.0.pdf](http://www.opengroup.org/jericho/COA_Information_Lifecycle_Management_v1.0.pdf).
- [14] Jericho. Encapsulation & Encryption [R/OL]. 2009-01. [http://www.opengroup.org/jericho/EncryptionandEncapsulation\\_v1.0.pdf](http://www.opengroup.org/jericho/EncryptionandEncapsulation_v1.0.pdf).
- [15] Brunette G, Mogull R. Security Guidance for Critical Areas of Focus in Cloud Computing [R]. USA: CSA, 2009.
- [16] Burrows M, Abadi M, Needham R M. Logic of Authentication [J]. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 1989, 426: 233-271.

## 《计算机技术与发展》投稿要求

(1) 新投稿可通过 Email 发至本刊电子信箱: ctad@vip.163.com。投稿前请作者自审一遍, 论文要求主题突出、用语规范、层次清楚、结构严谨、文字精练、文理通顺、逻辑性强。

(2) 论文题目不超过 20 个汉字。

(3) 作者姓名及作者所在单位部门、城市、邮政编码(多位作者不在同一单位应分别开列)。

(4) 摘要须从目的、方法、结果、结论 4 个方面阐述, 200 字以上。

(5) 关键词 3~8 个为宜。

以上(2)-(5)项内容必须中、英文具备。

(6) 作者简介: 姓名、出生年、性别、学位、研究方向;

导师简介: 姓名、职称、研究方向。

(7) 作者在投稿时须注明是否是中国计算机学会(CCF)会员(高级会员、普通会员、学生会会员)。若是会员, 请注明会员号(凡第一作者为 CCF 会员/高级会员/学生会会员者, 将享受 85 折的版面费优惠)。

(8) 投稿时请写明详细通信地址、邮政编码、联系电话、Email 信箱等各项必备内容。收到稿件经初审通过后, 30 天内以电子邮件的方式通知作者处理意见。稿件刊登后赠送样刊 2 本。