云计算信息安全分析与实践

佟得天，刘旭东，郭涛峰，梁杰文
（中国移动通信集团广东有限公司 广州 510100）

摘 要：云计算安全性问题是当今云计算技术推广落地中遇到的最重要和最困难的问题之一。本文将从云计算安全性中的信息安全部分进行阐述，通过对云计算和云计算中信息安全的基本内容进行描述，对当前的云计算信息安全问题进行分析，给出了一些解决方案并对云计算信息安全问题的前景进行说明，最后简要论述中国移动通信集团广东有限公司（以下简称广东移动）私有云平台现阶段在云计算安全方面的实践。

关键词：云计算；信息安全；云安全
doi: 10.3969/j.issn.1000-0801.2013.02.023

Analysis and Practice of Cloud Computing Information Security

Tong Detian, Liu Xudong, Guo Taofeng, Liang Jiewen
(China Mobile Guangdong Branch Co., Ltd., Guangzhou 510100, China)

Abstract: Cloud computing security issue is one of the most important and difficult problems encountered in today's cloud computing technology to promote landing. From the cloud computing security in the information security section, the basic content of information security in cloud computing and the current cloud computing were described; information security issues were analyzed; some of the solutions and the prospects of cloud computing were given. Finally, a brief discussion of GMCC private cloud platform cloud computing security practice was presented.

Key words: cloud computing, information security, cloud security

1 引言

云计算（cloud computing）最早是2006年由Google工程师克里斯托夫·比希利亚提出的，2008年开始成为IT界最热门的技术和关键词之一，2009年各大IT厂商如IBM、微软、Google、Oracle等纷纷推出其云计算产品和服务，而各大院校、研究院、企事业单位也都参与到云计算的研究与实践中。

云计算因其资源整合高效和服务接口封闭等特性，被各行各业广泛应用于内部系统重整和外部服务应用。当前比较出名的云计算应用有Google App Engine、Amazon网络服务、IBM的“蓝云”、中国移动的“大云”等。国内的银行、电信、电力、政府行业也正在规划部署云计算服务。

站在企业的角度，是否要部署一个新技术或者新产品，最重要的一项指标是安全性，安全性不仅要考虑技术本身的安全因素，同时也要考虑连带影响，如承载在此技术平台之上的信息的安全性。尤其是那些涉及较多敏感信息，如用户数据、财务数据等保密级别较高的数据。对于云计算技术，安全性问题同样无法回避，实际上这也是目前云计算推广应用过程中所遇到的最大难题。虽然目前云计算服务提供商都在竭力淡化或避免此方面的问题，但对于消费者，这是其决定是否使用此技术或服务的关键因素。Gartner 2009年的调查结果显示，70%以上受访企业的CTO认为近期不采用云计算的首要原因在于存在数据安全性与隐私性的忧虑。而近来云计算服务不断爆出各种安全事故更加剧了人们的担忧。例如，2009年3月Google发

生大批用户文件外泄事件,美国零售商 TJX 约有 4 500 万份用户信用卡号被黑客盗取,英国政府丢失 2 500 万人的社会保障号码等资料,在线软件公司 salesforce.com 也丢失了 100万份用户的 E-mail 和电话号码,国内 CSDN 泄露用户账户数据同样引起了人们对公共信息服务安全方面的担忧。

因此,云计算安全性已经成为云计算迈向部署应用必须要解决的问题,而信息安全是云计算安全性中仍未能很好解决的问题之一[1]。无论是在公有云计算环境还是在私有云环境中,安全性问题都是需要攻克和解决的难题。

2 云计算技术概述

云计算是一套解决方案的名称,它并不是一个新兴技术,只是几种技术整合应用而推出来的概念,相关单一技术已经在多年前被提出,但由于现实环境各种各样的限制,缺乏大规模商用的契机。云计算可以看作融合了分布式计算(distributed computing)、虚拟化(virtualization)、网格计算(grid computing)、负载均衡(load balance)和并行计算(parallel computing)的产品。

云计算经过了几年的演变,从架构上可以分为如下 3 层。

- IaaS(infrastructure as a service,基础设施即服务),在基础平台设施上部署虚拟化等技术使得基础设施整合,提高利用率。
- PaaS(platform as a service,平台即服务),实现平台级的统一服务,在云计算平台级上提供企业开发/运行接口与环境,供企业实现自我服务。
- SaaS(software as a service,软件即服务),对用户提供统一的服务接口,如通过多用户架构,采用浏览器或其他客户端把服务提供出去。

这 3 层结构是自下而上构建的,IaaS 是最底层的,SaaS 是最高层的。云计算服务可以只部署 IaaS,也可以部署 IaaS+PaaS,也可以是 IaaS+PaaS+SaaS 模式。

云计算从应用角度上可以分为私有云、公共云和混合云。私有云是指部署在企业内部的云计算平台,旨在整合其公司内部 IT 资源的云计算系统;公共云泛指部署在公共计算平台中,对公众开放的云计算平台,通过收取服务费用运营云计算系统;混合云是指云计算平台既有私有云部分,也有公共云部分,是两者的融合。

云计算具有以下几个特点。

- 动态可扩展性。云计算系统能通过实时监控,把每个服务按不同的策略动态分配到合适的设备上,而只需要把基础设备在云计算系统上做登记,就可以立即纳入云计算的服务分配资源上,方便实现可扩展。
- 高可靠性和容错能力。云计算系统内部就是一个高度集群的系统,能轻松实现容灾备份功能,高可靠性和容错能力是必备的。
- 高性价比。云计算系统的一个重要功能就是能极大地提高基础平台的利用率,全部设备都能被所有服务利用。
- 服务封装。云计算系统所提供的服务,无论是使用服务还是部署服务,系统都是对外封装屏蔽的,用户不了解也不需要了解该服务具体部署在哪个设备上,由云计算系统统一动态自动予以分配。

云计算的目标是资源整合和服务化,云计算的远景是使 IT 成为普遍廉价的公共资源,如电力公司提供电力,自来水公司提供自来水,让 IT 资源和服务成为任何人能轻而易举享受到的公共资源。

3 云计算的信息安全问题

2009 年 CSA(cloud security alliance,云安全联盟)在云计算安全方面列举并分析了所面临的 7 个最大的安全威胁[2]:对云的不良使用;不安全的 API;恶意的内部人员;共享技术的问题;数据丢失或泄漏;账户或服务劫持;未知的风险。

2008 年咨询公司 Gartner 从供应商的安全能力角度出发,分析云计算面临的安全风险,发布了一份名为《云计算安全风险评估》的报告,报告中列出了云计算技术存在的 7 大风险[3]: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、持久服务。

云计算安全性的范围很广,包括技术、管理、立法、商业、企业持续服务等层面,而本文讨论的云计算信息安全问题是云计算安全性其中的一个问题。在这里不讨论云计算的可用性、持久性问题,也不涉及系统或者 IT 基础本身的安全性,因为这些安全性问题已有很多成熟的解决方案。本文主要讨论云计算所带来的新技术而产生的新的信息安全风险问题。

云计算的信息安全问题,主要是指部署在云端的数据的安全问题。作为用户,第一感觉是以前系统的所有数据都是自己掌控的,但是实施云之后,数据有很大一部分层面是对用户屏蔽了,用户自己掌控不了其中的安全性。云

计算系统俨然成为一个黑盒子,那把数据放在这个黑盒子是否安全呢?

排除本文讨论范围以外的,如可用性、内部管理、运营等问题,总结出云计算信息安全存在如下风险。

(1)应用部署安全风险

任何一个持有有效信用的人都可以注册并立即使用云平台,网络犯罪分子可以基于云平台部署各种攻击服务或各种恶意软件,攻击互联网上的任何用户,更严重的是,在云计算平台内部部署的恶意软件能直接从内部对云计算平台进行服务攻击、信息窃取等安全攻击。

(2)API 安全风险

云平台的安全性很大程度上取决于 API 的安全性。用户使用这些 API 管理和交互相关服务,这些 API 的设计必须能够防御意外和有恶意企图的行为,避免产生安全漏洞以被网络犯罪分子所利用进行攻击。

(3)虚拟化环境安全风险

在 IaaS 层均需要充分利用虚拟化和共享技术实现动态可扩展功能, 用户数据在云平台中是被动态分配的,利用这些技术并不能很安全地在多用户架构中提供强有力的隔离能力,这样就给攻击者带来了很多便利,利用不完善的访问控制、过度使用的共享技术,能把恶意程序传播到云平台的其他服务中。

(4)数据访问权限风险[4]

从云计算的整体技术架构来看,除了中央数据服务器外,用户数据存储在哪片“云”上无人知晓,精准盗取数据的难度很大,但云计算的数据访问权限存在漏洞,就很容易产生风险。当用户把数据交给云计算服务商后,服务商则拥有了该数据的访问权限,云计算平台供应商由于自身管理原因,会导致偷窥、泄漏用户的数据和程序的风险。而由于云计算提供的服务面向所有公众,允许各种各类用户进行操作,若因为某些权限漏洞,致使非法用户得到数据,也将会使数据的安全性受到致命威胁。

(5)数据存储与传输安全风险

由于云服务面向所有公众,其中不乏涉密信息,如果数据存储与传输得不到严格加密,一旦丢失,将会造成更严重的损失。另外在云计算中也无法像以前传统系统部署中通过安全域定义来实施安全边界和数据保护[5]。

4 云计算的信息安全方案

上述分析的云计算信息安全风险,是自上而下,从应用到存储来分析的, 需要对这些风险进行安全加固和规避,以提高云计算信息安全的保障。下面将从 3 个层面对云计算的信息安全风险进行安全方案的描述,分别是数据安全、应用安全、虚拟化安全[6],然后再给出当前国内外关于云计算信息安全相关解决方案的成果。

4.1 数据安全

数据安全是指保存在云服务系统上的原始数据信息的相关安全方案,包括数据传输、数据存储、数据隔离、数据加密和数据访问。

(1)数据传输

在云计算内部, 除了服务本身需要的数据传输外,还有更多因动态调整而引起的数据传输。这部分数据面临的最大威胁是直接通过明文传输, 而没有采用任何加密措施。在云计算内部的传输协议也应该能满足数据的完整性,因此应采取安全传输协议,但其当前的相关研究并不因云计算而有所改动,在这里就不再描述。

(2)数据加密[5]

为了更好地加强云计算的安全性,需在数据存储上增加数据的私密性,既能保证文件的隐私性,又能实现数据的隔离和安全存储。如亚马逊的 S3 系统会在存储数据时自动生成一个 MD5 散列, 免除了使用外部工具生成校验的繁冗,有效保证数据的完整性;如 IBM 设计出一个“理想格(ideal lattic)”的数学对象,可以对加密状态的数据进行操作。基于这些技术,企业可以根据不同的情况,选择不同的加密方式来满足不同的加密需要[7]。

(3)数据隔离

云计算中并不是所有数据都适合进行数据加密,加密数据会影响数据服务的效率。对于 PaaS 和 SaaS 应用来说,为了强调运行效率等方面的“经济性”,非法访问还是会发生的,因此需要通过实施数据隔离来解决。在云计算环境下,系统的物理安全边界将会逐步消失,转而替代的是逻辑安全边界,因此应该采用 VLAN 或者分布式虚拟交换机等技术来实现系统数据的安全隔离。

(4)数据访问

数据访问[8]的策略,也就是数据访问权限控制,可以通过安全认证的技术来解决。通过统一单点登录认证、资源认证、协同认证、不同安全域之间的认证或者多种认证方式相结合的形式,对用户身份进行严格审查,对数据进行操作前,一定要对操作者身份进行严格核查。另外在权限的合理分配方面也要做好规划和管理。而数据访问的监视

和日志审计也必不可少,特别是对敏感信息的操作,要做到可溯源。

4.2 应用安全

从云计算提供商的角度出发,描述从应用层面应当如何充分考虑来自外部的风险。

(1)IaaS 应用——虚拟化安全

IaaS 云计算提供商将用户在虚拟机上部署的所有应用都看成一个黑盒子,他们完全不会干涉所部署应用的管理工作和运维工作,仅负责提供基础资源。在 IaaS 应用中,用户应负责其应用程序的部署和管理,程序的安全性也应由用户考虑。IaaS 应用提供商利用虚拟化等技术,根据用户的需求提供基础资源,虚拟化的安全性是云服务商负责的,在 4.3 节将讨论到。

(2)PaaS 应用——API 安全、应用部署安全

PaaS 云计算提供商给用户提供在 IaaS 之上,依照平台的接口规范,部署由用户开发的平台化应用或采购现成的中间件产品。PaaS 云计算提供商关注的安全问题包括两个方面:PaaS 平台自身的安全风险和用户部署在 PaaS 平台上的应用的安全风险[9]。

PaaS 平台自身的安全风险,主要包括对外提供 API 的安全和 PaaS 应用管理的安全。对于 PaaS 的 API 安全问题,目前国际上并没有统一的标准,这对云计算 API 的安全管理带来了不确定性;而 PaaS 应用管理方面,核心的安全原则就是确保用户的数据只有用户自身才能访问和授权,实行多用户应用隔离,不能被非法访问和窃取。在这种环境下,PaaS 平台应提供平台的保密性和完整性,云服务提供商应负责监控 PaaS 平台的缺陷和漏洞,及时发布补丁更新,解决安全漏洞。

用户部署在 PaaS 平台上的应用安全风险,对于云提供商来说主要是对客户部署程序的安全审查,排除有意或无意的恶意程序甚至病毒的部署。因为用户申请要部署的程序,无论是自行开发的还是采购的,均有安全的不确定性,因此云服务提供商需要对申请部署的程序进行严格的安全审计,包括非法代码、不安全代码、存在漏洞的代码的检测,并需与用户一起对审计的结果进行分析和修正。当前这方面没有标准,因此需要各云服务商提供此安全审计要求。

(3)SaaS 应用——服务安全

SaaS 云计算提供商给用户提供的是灵活方便地使用在云计算服务端中的各种应用。SaaS 云计算提供商应必须确保提供给用户的应用程序的安全性,而用户只需对访问云端应用的终端的安全负责,如终端自身安全、客户端的访问管理等。在 SaaS 平台层,云服务提供商应重点关注所提供服务的安全性,可参考当前对软件安全性的相关考虑方案进行评估和审查。

4.3 虚拟化安全

虚拟化安全是云计算最基础部分 IaaS 的重要技术手段,对虚拟化技术的安全性进行分析,对整个云计算的安全性来说是坚实的一步。基于虚拟化技术的云计算信息安全风险主要有两个方面:虚拟化软件产品的安全和虚拟主机系统自身的安全。

(1)虚拟化软件产品安全

虚拟化软件产品[10]是直接部署在裸机之上,提供创建、启动和销毁虚拟主机的能力,对虚拟主机进行管理的一种软件。实现虚拟化的技术不止一种,可以通过不同层次的抽象来实现,如操作系统级虚拟化、半虚拟化和全虚拟化。

虚拟化软件产品保证用户的虚拟主机能在多用户环境下相互隔离,可以安全地在一台物理服务器上同时运行多个虚拟主机系统,因此云服务提供商必须建立安全控制措施,严格限制任何未经授权的用户访问虚拟化软件层,限制对虚拟化层次的访问。

另一方面,虚拟化具有动态性,即所虚拟的服务系统会根据整个云的情况进行动态调整,如把虚拟服务器进行动态切换、挂起等。虚拟化软件层必须考虑由此带来的安全风险,如切换是否完整、是否存在数据残留、是否存在数据丢失、在切换的过程中是否会被利用共享内存攻击而导致数据被窃取等,这些问题都是虚拟化软件层要解决的。

(2)虚拟主机系统安全

虚拟主机系统位于虚拟化软件产品之上,普通的物理服务器主机系统的安全原理与实践完全可以运用到虚拟主机系统上,同时也需要补充虚拟主机系统的特点。应当对虚拟主机系统的运行状态进行实时监控,对各虚拟主机系统的系统日志和防火墙日志进行分析,以此来发现存在的安全隐患。对于发现存在安全隐患的虚拟主机系统,应立即进行隔离,避免危害扩散,而对于已经不需要运行的虚拟主机,应当立即关闭。物理服务器的安全原理不再赘述。

5 广东移动私有云平台安全实践

中国移动通信集团公司已经成功地建立了“大云”云

计算平台,为了适应业务发展和技术转型的需要,广东移动分别按照 BSS、OSS、MSS 线条建立私有云计算平台。出于信息保密方面的考虑,不对云计算平台的具体方案和详细部署细节做过多叙述,仅给出一个具体的实施样例模型以进行安全方案论述。到目前为止,广东移动的私有云平台主要集中在 IaaS 层面,在进一步巩固 IaaS 建设的同时,正在着手开展 PaaS 方面的建设尝试。在云计算安全方面,如前文所述,主要集中在数据安全和应用安全两个层面。这里主要讲述在数据安全方面的实践工作。

5.1 数据和资源访问

数据访问的策略即权限控制,主要是通过安全认证和安全网关访问技术来解决。在广东移动的实践中,是通过 4A 项目的建设来统筹完成的。4A 项目实现了单点登录认证、强制用户认证,将应用资源和数据的方案控制在合理的范围内。并采用不同安全域之间的认证或者不同认证方式相结合的方式,通过动态令牌和静态口令、短信认证多种认证手段相结合的方式,对用户身份进行严格审查。特别地,对受限敏感数据进行操作或访问受限敏感网络资源前,对操作者身份进行更为严格的核查,采用按次审核的 VPN 访问方式,确保安全可靠。另外 4A 平台在权限方面进行统一合理的分配,数据或资源的访问都通过图形网管或者字符网管进行监视,并对日志和人员操作进行记录和审计,做到了可溯源。4A 平台的主要功能概念框架和访问方式的概念模型如图 1、图 2 所示。

因此,在数据和资源访问方面,广东移动将 4A 平台作为私有云的基础数据和资源访问平台,可以提供安全可靠的保障。

5.2 数据传输和隔离

广东移动在私有云平台数据传输和隔离方面主要存在如下问题。

- 不同部门对安全级别的要求不一样,管理流程不一样,需要平衡统一维护和分开管理的矛盾。

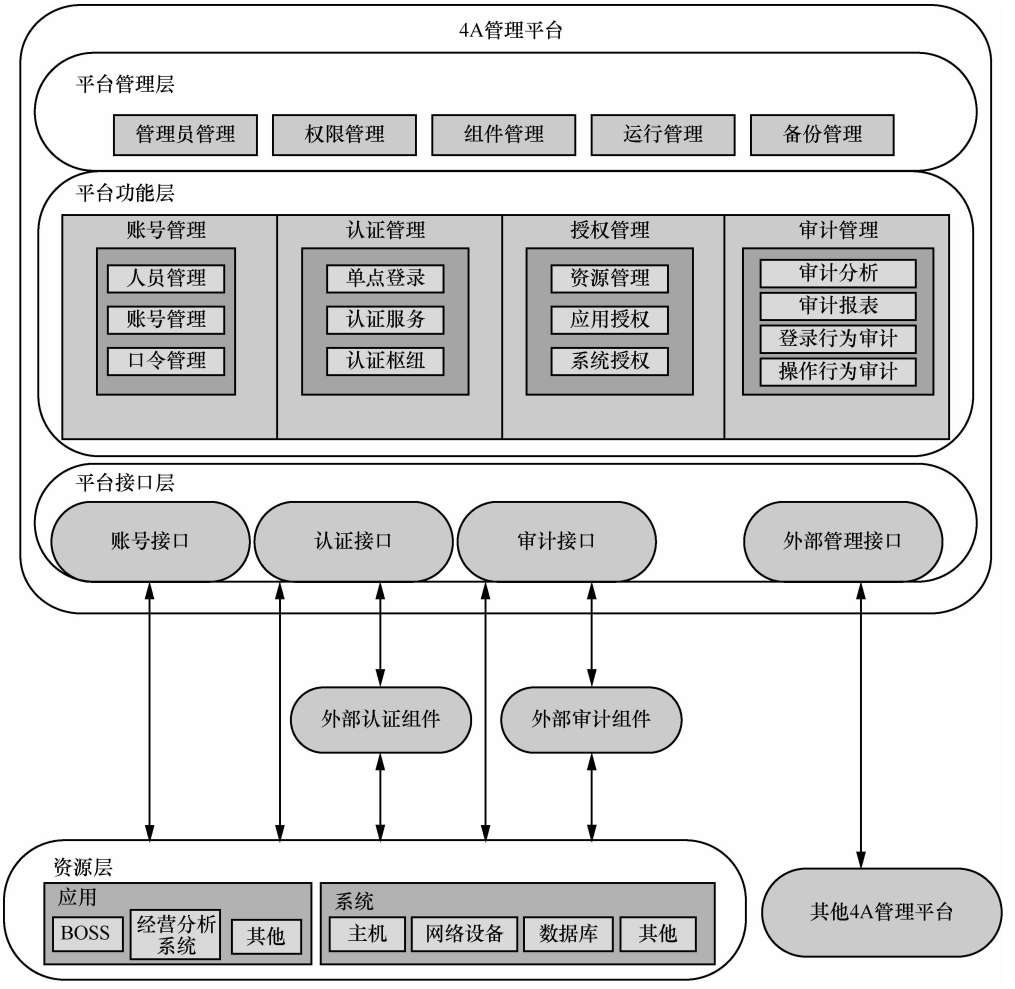


图 1 4A 系统概念框架

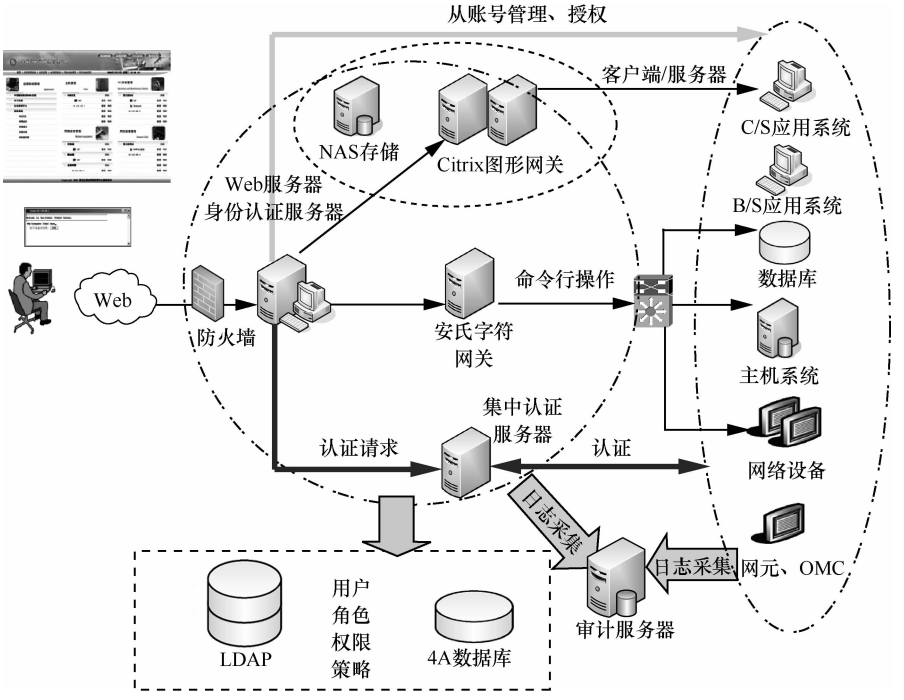


图 2　访问及控制机制

· 在虚拟化的架构下,保证安全性需做到:物理服务器内部虚拟机有流量查看与策略控制机制,虚拟机端口策略需要跟随虚拟机动态迁移,网络、服务器等安全的分工界面保持明晰,原有设计无法实现。

· 云平台业务灵活动态增减与严格安全隔离之间的矛盾。

为了解决上述问题,广东移动进行了周密的规划和详细的考虑及设计。网络上做到分层分段隔离,保证网络及信息系统间有着清晰的物理或逻辑边界。图 3 为私有云平台的网络部署逻辑。

在实践中,除了使用 IPS 安全防御系统和企业级防火墙等安全设施作为防御手段,为了保持维护和管理界面的清晰和安全性,采用了 VDC(virtual device context)技术,通过虚拟化把一台物理交换机虚拟化成多台逻辑设备技术。一台物理交换机虚拟成多台 VDC 虚拟交换机后,具有以

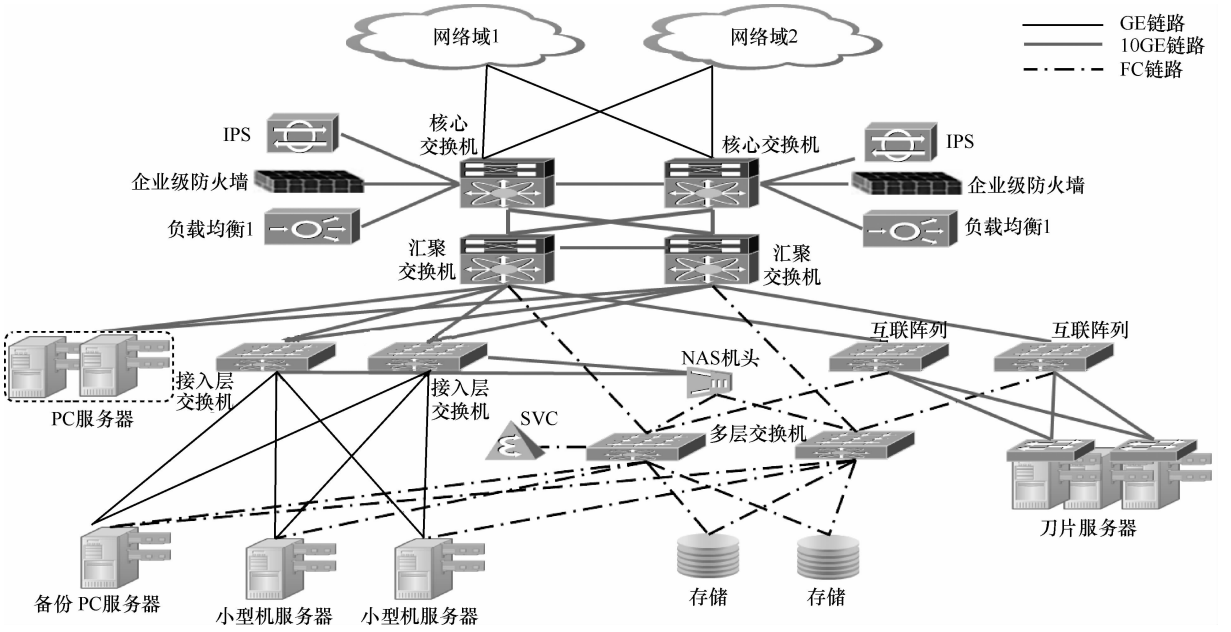
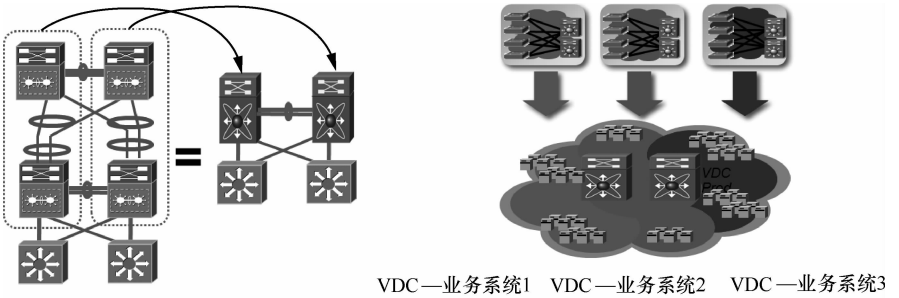


图 3　私有云平台的网络部署逻辑

下几个特点:VDC 之间完全隔离,具有独立的管理地址和配置文件;一台物理交换机最多可以虚拟成 8 台 VDC 虚拟交换机;每台 VDC 具有独立的 VLAN 空间,分别支持 4 096 个 VLAN;物理交换机上任意端口可以归属给任何 VDC 虚拟交换机。通过 VDC 的使用可以将网络按照层级进行水平分割,同时又可以按照系统维度进行垂直的安全域划分,在节省投资的同时也保证了部署的灵活性和安全性。VDC 的应用场景如图 4 所示。



(a) 场景1—网络层次水平分割　　(b) 场景2—业务层次垂直分割

图 4　VDC 的应用场景

结合虚拟化管理平台及 VPath 和 VSG 等技术,实现了多租户虚拟化安全生态系统,如图 5 所示。

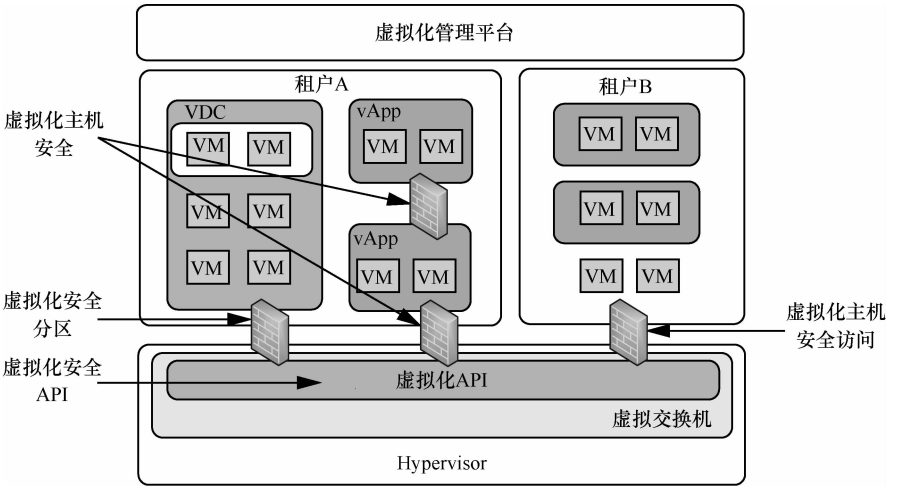


图 5　多租户虚拟化安全生态系统

综上所述,广东移动私有云计算平台在数据安全和应用安全方面的工作已经取得良好效果,逐步实现了对私有云平台内系统资源和数据的安全防护,并解决了自身云计算平台在维护和管理方面存在的难题。目前该项目已经成为行业内私有云安全的最佳实践。下一步将着手 PaaS 相关领域的信息安全研究和实施工作。

参考文献

1　尼古拉斯·卡尔. IT 不再重要. 北京: 中信出版社, 2008
2　张健. 全球云计算安全研究综述. 电信网技术, 2010(9)
3　朱源, 闻剑峰. 云计算安全浅析. 电信科学, 2010(6)
4　张健. 云计算概念和影响力分析. 电信网络技术, 2009(1)
5　郭乐深, 张乃靖, 尚晋刚. 云计算环境安全框架. 信息网络安全, 2009(7)
6　张云勇, 陈清金, 潘松柏等. 云计算安全关键技术分析. 电信科学, 2010(9)
7　张爱玉, 邱旭华, 周卫东等. 云计算与云计算安全. 中国安防, 2012(3)
8　张叶红. 数字图书馆云计算安全架构及其管理策略. 图书馆学研究, 2010(11)
9　严明. 云计算中的云安全研究. 现代商贸工业, 2009(10)
10　赵培云. 云数字图书馆安全问题浅析. 图书馆杂志, 2010(11)
11　谢四江, 冯雁. 浅析云计算与信息安全. 北京电子科技学院学报, 2008, 16(4)
12　李磊, 王金伦, 王薇等. 电信运营商发展云计算的安全问题剖析. 信息安全与通信保密, 2009(10)
13　汪来富, 沈军, 金华敏. 云计算应用安全研究. 电信科学, 2010(6)
14　黄华. 云计算安全关键技术研究. 电脑知识与技术, 2011(8)

[作者简介]

佟得天,男,现就职于中国移动通信集团广东有限公司,主要研究方向为高级网管支撑管理。

刘旭东,男,中国移动通信集团广东有限公司中级工程师,中级网管支撑主管,主要研究方向为网管支撑管理。

郭涛峰,男,中国移动通信集团广东有限公司助理工程师,中级网管支撑主管,主要研究方向为网管支撑管理。

梁杰文,现就职于中国移动通信集团广东有限公司,主要研究方向为中级网络监控与投诉管理。

(收稿日期:2013-01-10)

小流量长在线业务对 Ev-Do 网络的影响及优化

何晓明[1],贾　曼[2],刘志华[1]
(1.中国电信股份有限公司广东研究院 广州 510630;2.中国电信集团公司 北京 100032)

摘　要:分析了小流量长在线业务对 Ev-Do 网络的影响,从终端、网络、业务平台 3 个方面给出专为小流量长在线业务而优化的解决方案,并提出了加强无线运行指标预警及流量疏导等应对策略。

关键词:即时通信;物联网;小流量长在线业务;Ev-Do
doi: 10.3969/j.issn.1000-0801.2013.02.024

Influence of the Always-on Service of Little Traffic on Ev-Do Network and Optimization

He Xiaoming[1], Jia Man[2], Liu Zhihua[1]
(1. Guangdong Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China;
2. China Telecom Corporation, Beijing 100032, China)

Abstract: Influence of the always-on service of little traffic on Ev-Do network was analyzed. Optimization solutions especially for the always-on service of little traffic were given. Also, the coping strategies such as wireless operation index forecast and traffic guidance were put forward.

Key words: instant message, internet of things, always-on service of little traffic, Ev-Do

1　引言

随着 3G 网络的日益完善及广泛覆盖，移动互联网业务进入发展的快车道,智能手机已成为人们生活的基本配置。预计到 2012 年底,中国电信的 3G 手机用户数将达到 7 000 万左右,3G 智能手机用户数将占新增手机用户数的 80%以上。移动互联网在满足人们随时随地接入互联网的便捷性要求的同时,更为重要的功能是为人们提供广泛多样的社交沟通方式，如手机 QQ、手机微博等即时通信(IM) 类应用。

智能手机“永远在线(always-on)”的这种业务体验需求对 3G 网络带来了巨大的冲击。最典型的例子是 2012 年 1月 25 日发生的日本最大的移动运营商 NTT DoCoMo 大面积网络瘫痪事故,故障持续近 5 h,而这已经是 DoCoMo 在过去 6个月中出现的第 5 次网络问题。美国 AT&T、欧洲 Orange 等知名电信运营商近年来也都曾遭遇类似的网络瘫痪。

本文主要分析人们广泛使用的 IM 应用这类小流量长在线业务,对 Ev-Do 网络的影响。在对小流量长在线业务特征进行分析和现场试验的基础上,进一步梳理 Ev-Do 网络承载小流量长在线业务的实现机制,从终端、网络、业务平台各个环节提出专为小流量长在线业务而优化的解决方案。

2　小流量长在线业务特征

小流量长在线业务大体分为两类:人与人通信及机器与机器通信(M2M)。目前,国内人与人通信的小流量长在线应用软件主要以 QQ、微信、微博为代表。根据统计,校园学生中手机 QQ 和微信的渗透率达到 70%以上,而普通用户中参与 QQ 应用的用户占比也达到 30%左右;校园学生