



# 中小企业云服务解决方案及关键技术实现研究

刘国萍, 郑燕冰

(中国电信股份有限公司北京研究院 北京 100035)

**摘要:** 云服务模式契合了中小企业信息化发展的需求。然而, 如何将平台服务、宽带网络、多样化终端有机结合提供一体化服务, 在国内外仍处于探索和试点阶段。在分析中小企业信息化需求的基础上, 提出了基于“云—管—端”架构的中小企业云服务解决方案, 给出了方案总体架构、技术体系架构及产品服务架构设计; 并从技术角度阐述了企业资源池构建、虚拟化应用部署及云服务安全保障等关键实现, 最后给出了方案实践部署架构及发展现状。

**关键词:** 云计算; 中小企业云服务; 云管端架构; 企业资源池; 虚拟化应用部署; 云服务安全

**doi:** 10.3969/j.issn.1000-0801.2013.09.007

## Research of Cloud Computing-Based Solution and Key Technical Implementation for Medium-Sized and Small Enterprises

Liu Guoping, Zheng Yanbing

(Beijing Research Institute of China Telecom Co., Ltd., Beijing 100035, China)

**Abstract:** It was still in the stage of exploration and experiment at home and abroad on how to unify the platform service, broadband network and diverse terminals to provide the integrated services although the cloud service mode accorded with the need of the medium-sized and small enterprises on the information development. A solution based on the cloud, pipeline and terminal architecture was proposed on the basis of the requirement analysis for the medium-sized and small enterprises. The overall framework, the technical architecture and the product hierarchy were put forward. The key implementation for the enterprise resource pool, virtualized application deployment and the cloud service security were discussed from the technical view and the practicing deployment architecture and its state of the art were provided.

**Key words:** cloud computing, cloud service for medium-sized and small enterprises, cloud and pipeline and terminal architecture, enterprise resource pool, virtualized application deployment, cloud service security

### 1 中小企业云服务需求

全球最大的会计师事务所普华永道在《2011 年中国企业长期激励调研报告》中的统计数据表明, 国内数量庞大的中小企业平均生命周期仅为 2.5 年。对于这样一类未来发展不确定因素大、发展需求强烈而又缺乏信息化管理手段等的客户群体, 其对信息化的需求不同于一般大型企业

或政府机构, 其具有如下特征:

- 水电式服务——节省资金、少投入, 使用了才付费;
- 即开型服务——快速部署、省时间, 即申请即开通;
- 顾问式服务——维护简单、易管理, 专业代维代管;
- 在线式服务——使用方便、高可用, 可随时随地访问。

云计算具有按服务提供、按用量计费、集中管理、一直



在线等特点,天然契合中小企业信息化需求,极大地降低其软硬件投入成本及信息化进入门槛,提高其信息化发展水平,助力其企业发展,是中小企业信息化服务提供的理想模式。微软《2011年中小企业云服务采用研究报告》称,39%的中小企业希望在3年内购买一项以上的云服务。

## 2 中小企业云服务解决方案

### 2.1 中小企业云服务总体架构

针对国内中小企业信息化的需求特征,从目标用户IT基础设施“云化”入手,基于“云—管—端”体系架构设计了一套集宽带、应用和服务一体化交付的一揽子解决方案——中小企业云服务解决方案。解决方案总体架构如图1所示,总体架构中涵盖了从用户侧网络接入到云端基础设施和云端应用3个层面。

中小企业云服务解决方案旨在面向产业园区、商务楼宇和具有一定行业群特征的中小企业客户群以及面向农

村/城镇两低两高(低收入和操作技能、高信息和娱乐需求)弱势群体客户群,借助于电信运营商为主导的创新型云服务模式,提供安全可靠的集宽带、IT资源、应用及服务一体化的云计算服务,解决中小企业IT基础设施部署门槛高、初期投资大、维护难等现实问题。

“省钱省时省力,助力企业成长”是中小企业云服务设计的核心宗旨,方案优势集中体现在以下3个方面。

(1) 企业用户侧基础设施的一揽子提供、建设和维护服务

基于中国电信宽带接入,在企业侧根据具体需求部署网关、瘦PC终端、电话机、传真机、打印机、本地存储、翼机通POS机等组网和办公设备,搭建完整的办公网络环境,中国电信亦可提供维护服务。

(2) 桌面虚拟化、应用虚拟化、电信能力的深度嵌入  
企业所需业务应用由中国电信侧云平台提供和加载。通用云应用包括:云桌面、云办公/IT、云存储、云安全等;特定应用通过云平台进行加载,如IT开发应用、物流行业应

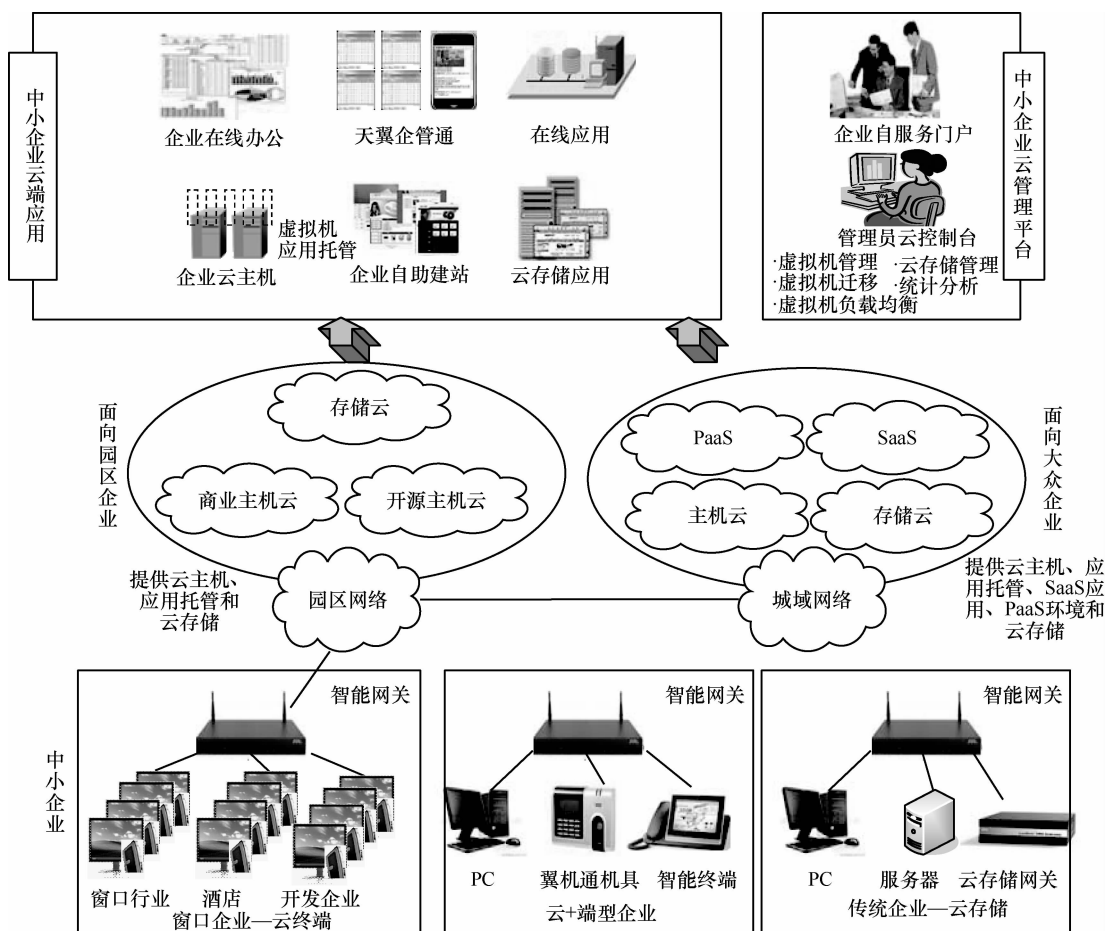


图1 中小企业云服务解决方案总体架构

用、营业和销售应用等;一方面将中国电信自身业务应用能力和所加载的企业应用结合,另一方面延伸到瘦 PC、智能终端、手机等终端。

### (3) 以用户为中心的商业模式设计

以用户为中心设计多种商业模式,比如中国电信负责集采瘦 PC、网关、打印机、POS 机等设备,客户可按月租用,也可一次性购买,中国电信负责维护,收取宽带接入、资源使用、维护服务等费用。

## 2.2 中小企业云服务系统架构

中小企业云服务解决方案从系统设计角度包括服务平台、宽带网络及各类终端,平台是应用与服务的承载实体,网络是服务传输通道,终端是服务与应用的展现实体。从逻辑层次上划分,整个系统由物理资源层、虚拟化环境(包括虚拟化平台、虚拟化资源接口层)、云平台能力层、云服务层、云门户、云服务运营和管理以及云安全体系组成。中小企业云服务系统架构如图 2 所示,系统架构主要从技术角度描述系统实现的逻辑分层。

云门户包括用户门户和电信管理门户,用户门户面向园区管委会办公人员、企业用户等提供业务申请、使用查询等自助服务接入;电信管理门户面向园区管委会技术人员和电信管理人员,提供业务运营和管理、平台管理、虚拟资源管理以及安全管理的统一服务接入。

云服务层提供应用服务和信息服务。应用服务包括虚拟主机、办公云桌面、云存储等云服务和 SaaS 托管应用,信息服务建立 BI 应用开发环境,从应用服务中抽取数据进行挖掘和分析,提供业务决策和支持能力。

云平台能力层封装电信能力和互联网 IT 能力,对托

管的 SaaS 应用提供面向服务的多租户运行环境,完成服务的定位、注册、编排和依赖性检查、监视、安全访问、审计和日志等服务管理功能。

虚拟化资源层通过对虚拟化平台、并行计算环境统一管理调度,对计算、存储等物理资源进行池化,抽象成可管理、可调度的逻辑资源,屏蔽异构云平台(包括 Microsoft Hyper-V、VMware、XenServer、KVM 等)调用接口,向上提供一致化的访问。

云终端系统包括瘦终端、聚类行业云终端、电视云终端、智能手机、PC 等。

此外,作为云宽带运营的辅助系统,还需要提供云服务运营和管理框架和云安全体系作为支撑。

云服务运营和管理包括服务运营、服务管理、平台管理和虚拟资源管理。服务运营是指服务的订购和加载,实现云服务的开通;服务管理是指服务的 SLA 管理、计量管理、服务监控以及统计分析等功能;平台管理包括多租户运行环境管理(SaaS 应用提供环境)、BI 应用开发环境管理和门户管理;虚拟资源管理包括对异构云平台的统一管理,实现对虚拟资源的统一分配、调度、性能监控、使用统计等管理以及对云宽带网络服务的管理(主要包括多租户 VPN 网关、防火墙、负载均衡、路由器、交换机、虚拟交换机的管理等)。

云安全管理包括用户安全、应用和服务安全,用户安全是指登录账号管理和密码管理,为用户使用云服务提供 SSO 环境;应用和服务安全是指提供应用/服务访问安全、访问审计以及应用/服务之间的联邦认证功能,支持 OAuth 和 OpenID 认证授权机制。

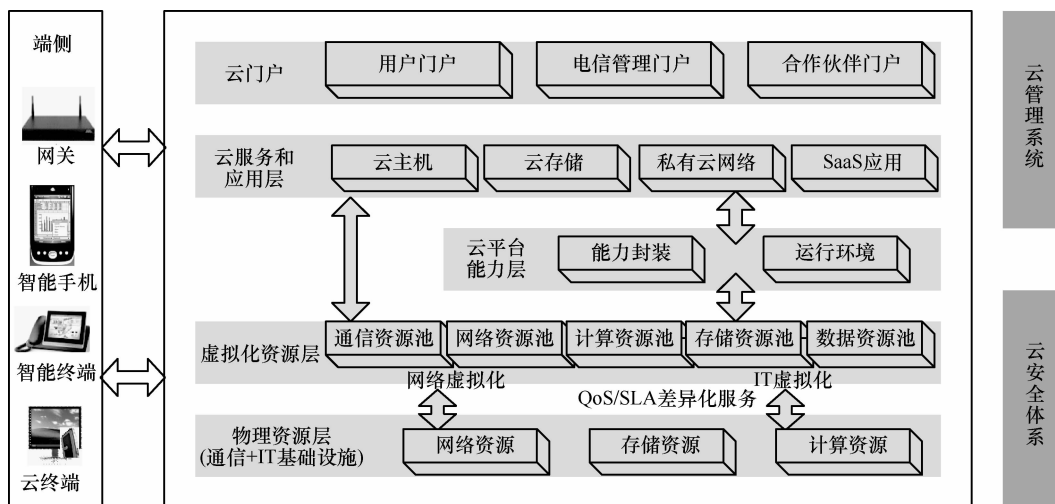


图 2 中小企业云服务系统架构



### 2.3 中小企业云服务服务体系

根据中小企业云服务解决方案的设计宗旨及系统架构的设计能力,中小企业云服务可提供涵盖高中低端客户群的端到端一体化产品服务体系,如图3所示。在图3中提供的服务体系包括IT资源(如云主机、云存储)、企业私有云应用(如云办公)、SaaS应用(如云财务)和定制化解决方案(如云呼叫中心)。

中小企业云服务产品服务体系涵盖企业云宽带及网络虚拟化、服务器和存储资源虚拟化、企业级云应用/云主机/智能建站/云桌面等。对于低端客户群体(包括农村弱势群体),设计以低成本、普及型的云宽带业务产品切入市场,提供其低操作门槛的云宽带及云终端接入服务,带动农村宽带业务的发展,填平社会数字鸿沟;对于中高端客户,以高质量、差异化的云宽带产品切入市场,提供基于企业私有云的跨终端协同体验与应用,如企业私有云网络、云办公、云通信等,增强客户满意度和黏性;对于聚类商业客户,以快部署、易使用的云宽带产品切入市场,提供基于云服务模式的应用软件管理服务,如云呼叫中心、云财务、云开发等产品,降低企业创业发展门槛,助其快速成长。

中小企业云服务产品体系设计以降低中小企业信息化使用门槛为宗旨,以宽带接入业务发展和宽带价值填充为诉求点,以定制差异化终端、引入差异化服务内容为手段,最终实现从电信与客户双赢策略。

## 3 中小企业云服务关键技术实现

中小企业云服务解决方案的技术实现关键要解决3类技术问题:第1类是企业级资源池构建,即在统一资源池的基础上如何构建安全、高效的企业级企业资源池;第2类是基于虚拟化资源池的应用部署技术,即如何规划将SaaS应用或企业托管式应用部署于虚拟化资源池上;第3类是整个中小企业云服务的安全保障,是中小企业云服务应用推广的关键。

### 3.1 企业级资源池构建

企业级资源池是中小企业云服务产品服务体系的基础服务内容,为企业级应用提供IT承载实体,是构建弹性、灵活、安全的中小企业云服务的核心设施。

企业级资源池构建主要考虑多租户管理、安全隔离及网络互通等问题,其中多租户管理依赖资源管理系统实现,因此从资源池构建本身需要考虑安全隔离和网络互通两个因素。目前主流的虚拟化技术(如Microsoft Hyper-V、VMware、XenServer、KVM等)通常提供了对CPU、内存、网络接口、文件系统等系统级的安全与隔离,因此,对于服务提供商而言,在构建企业资源池时需要重点考虑的问题主要是网络安全隔离与互通,即需要对提供企业的资源池进行整体网络规划并提供自动化网络配置能力。

目前企业资源池的组网技术主要有两大类标准,分别是服务器厂商主推的IEEE 802.1Qbg标准和Cisco主推的

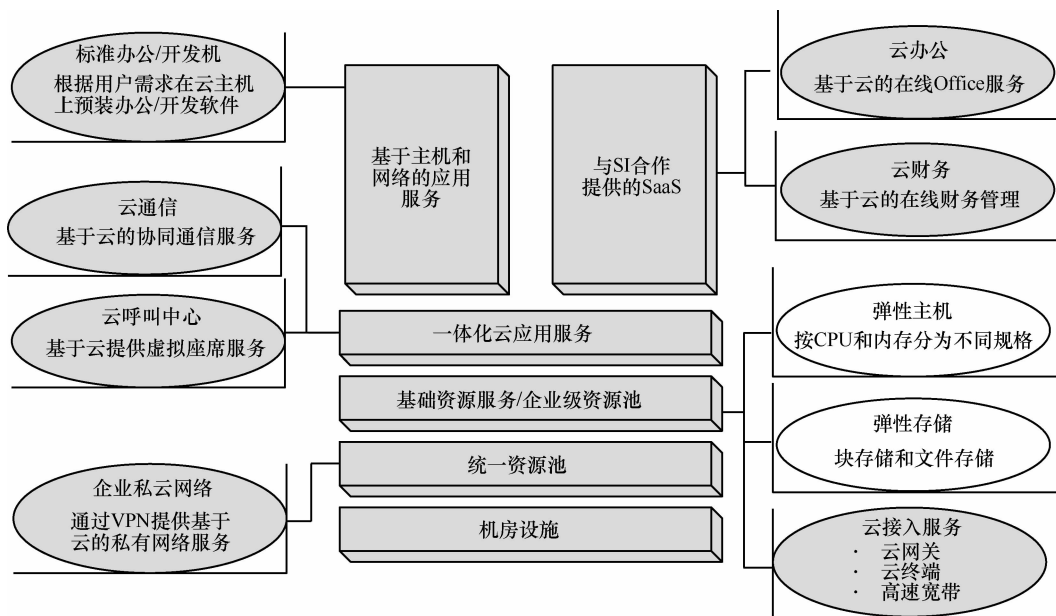


图3 中小企业云服务产品服务体系

IEEE 802.1Qbh、IEEE 802.1BR、VN-Tag 标准。表 1 是这两大类标准技术的简要对比。从技术方案的效果来看,依托 IEEE 802.1Qbg 的解决方案主要解决虚拟机的网络接入问题,可以完全兼容现有的 IP 网络设备;而依托 IEEE 802.1Qbh、IEEE 802.1BR、VN-Tag 等标准的解决方案则是一整套的网络虚拟化解决方案,但是对虚拟化软件、网卡等都有特殊要求,因而这些标准除 IEEE 802.1BR 外都已废止或转为个别厂商私有应用。

大规模数据中心的建设可以考虑基于 IEEE 802.1Qbg 标准的 VEB、VEPA 方式来扩大虚拟机内部网络;而一般的企业资源池建设多采用多通道(multi-channel)的方式,以适用各种虚拟化软件以及简化虚拟化软件设置。

基于 IEEE 802.1Qbg 标准的多通道方式,实现了中小企业云服务企业级资源池的网络自动化配置能力,实现功能框架如图 4 所示。图 4 中采用了两种方案实现网络设备的自动化配置:调用综合网管平台接口和直接调用单个网络设备的接口。后者实现复杂度低,非常适合小型、异构的企业级网络资源的配置和管理。

通过网络自动化配置技术实现,达到了屏蔽不同厂商设备差异性的目的,并简化了北向接口的复杂度,为提供大规模企业级资源池及应用服务奠定了良好的技术基础。

3.2 应用虚拟化部署

中小企业云宽带服务平台的统一资源池不仅可以作为企业级资源池直接出租给客户使用,也可以作为平台上的 SaaS 应用或企业托管式应用的 IT 承载实体,基于虚拟化资源池的应用部署可以为其提供更高的可用性、更大的灵活性及更好的管理性,这对于成本敏感且业务上线要求快的中小企业尤为重要。

应用虚拟化部署设计的关键流程如图 5 所示。该流程中的核心步骤是先确定可以虚拟化的服务器场范围及服务器角色,并利用容量规划理论来规划物理环境,然后使用获得的物理工作负荷要求作为虚拟环境规划的输入并

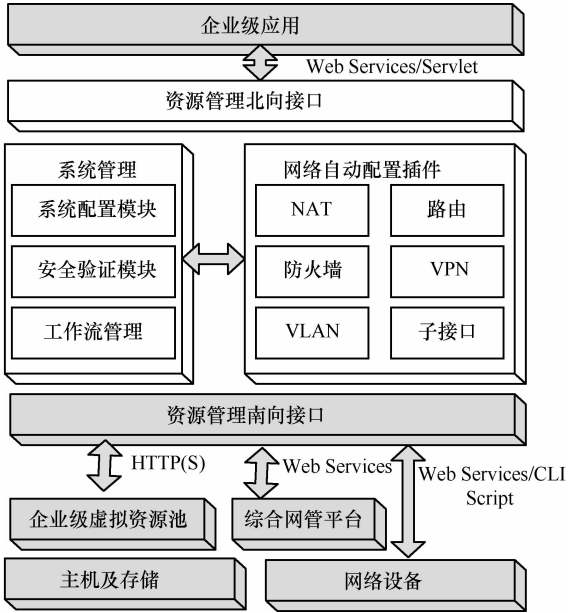


图 4 中小企业云服务企业级资源池自动化配置实现  
进行虚拟化环境与物理环境映射,最后设计虚拟化部署体系架构及其他高可用方案并进行测试与调优。

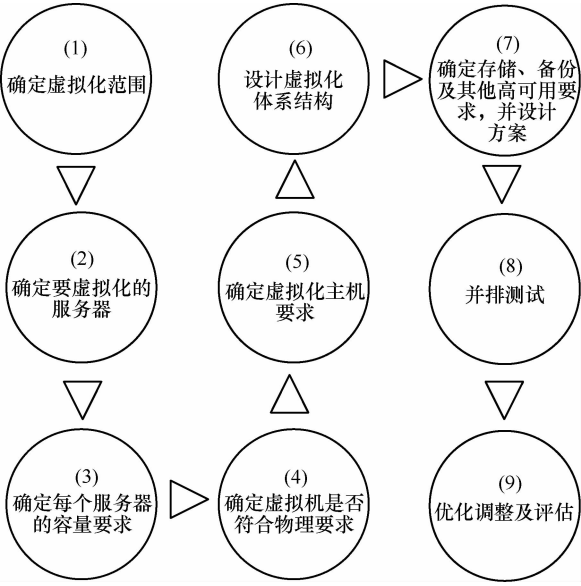


图 5 应用虚拟化部署流程

表 1 主流企业资源池构建技术对比

|      | IEEE 802.1Qbg             |                                                         |                        | IEEE 802.1Qbh             | IEEE 802.1BR | VN-Tag |
|------|---------------------------|---------------------------------------------------------|------------------------|---------------------------|--------------|--------|
|      | VEB                       | VEPA                                                    | 多通道                    |                           |              |        |
| 提出方  | HP(H3C)/IBM 等服务器厂商        |                                                         |                        | Cisco                     | Cisco        | Cisco  |
| 模式本质 | · vSwitch;<br>· 网络功能进入服务器 | · 简化的 vSwitch,要求网络支持基于端口的 hairpin 转发;<br>· 服务器内支持部分网络功能 | · 通道;<br>· 网络功能只在服务器外部 | · 通道;<br>· 部分网络功能键回复到服务器内 |              |        |
| 性质   | 标准                        |                                                         |                        | 标准                        | 标准           | 私有     |
| 标准进展 | 文稿完成,框架确定/标准流程审议          |                                                         |                        | 废除                        | 标准讨论         | 私有应用   |



对于已经获得应用在物理环境下的容量需求且部署规模明确时,应用虚拟化部署的核心步骤是虚拟化服务器资源需求与物理主机的资源映射模型。对于基于微软 Hyper-V 虚拟化技术的服务器场,虚拟化服务器资源需求(已获得的物理环境下的容量需求)与物理主机资源需求间的参考映射模型如下:

物理主机总处理资源需求(逻辑 CPU 颗数) $= (\sum_{i=1}^n \text{虚拟服务器 } i \text{ CPU 核心数} \times \text{CPU 速率(MHz)} \times \text{CPU 利用率}) / 0.85 + 1$  (1)

物理主机总内存资源需求 $= \sum_{i=1}^n \text{虚拟服务器 } i \text{ (总内存量(MB)} \times \text{内存利用率(\%))} + 32 \text{ MB} + 2 \text{ GB}$  (2)

物理主机总网络 I/O 资源需求 $= \sum_{i=1}^n \text{虚拟服务器 } i \sum_{j=1}^n \text{虚拟网卡 } j \text{ (平均每秒收到字节数} + \text{平均每秒发送字节数)} / 0.85$  (3)

物理主机总磁盘 I/O 资源需求 $= (\sum_{i=1}^n \text{虚拟服务器 } i \text{ (平均每秒磁盘读字节数} + \text{平均每秒磁盘写字节数)}) / 0.85$  (4)

上述模型中,0.85 是主机虚拟化有效因子,式(1)中“1”是主机虚拟化 CPU 损耗,式(2)中“2 GB”是主机虚拟化内存损耗,“32 MB”是多虚拟化内存损耗补差。此模型是对虚拟机配置及使用情况做大量调测后给出的参考模型,在不同的使用场景下可进行相应的参数调整。

### 3.3 云服务安全保障

云服务的数据安全、用户隐私保护已成为用户使用云服务最为担心的问题之一。中小企业云服务是面向中小企业提供的云服务,同样,其服务安全也将成为其能否在中小企业中广泛应用的重要因素之一。

中小企业云服务除了解决传统的信息系统所具有的安全问题,如系统防护、数据加密、用户访问控制等问题外,还需要解决由于集中服务模式以及虚拟化技术引入可能引发的安全问题,如防 DoS 攻击、虚拟机隔离、多租户数据隔离、残留数据擦除以及多 SaaS 应用统一身份认证等问题。

要解决云服务可能存在的安全问题、消除用户对云服务使用的安全担忧,安全技术实施是基础。中小企业云服务是一种公有云服务模式,从服务模式上涉及 IaaS、PaaS、SaaS 三大类服务。根据这三大类服务的服务模式及服务内容不同,相应地每一类服务所侧重的

安全防护技术手段及应用遵循的合规模型也有所不同,图 6 是中小企业云服务安全体系架构模型及合规模型。与传统 IT 系统安全相比,中小企业云服务在网络安全、资源安全、数据安全及多租户 SaaS 应用安全等层面充分考虑了云服务模式所引发的安全风险,并充分利用虚拟化防火墙、可信计算、数据加密、身份认证等技术实施来为中小企业客户提供服务安全保障。

中小企业云服务服务安全不仅需要从技术层面加以保障,还需要从提升用户安全认知、强化服务运营管理等多个层面进行保障。在提升用户安全认知方面,应加强用户对不同重要性数据迁移的认知,并在服务合同中强化用户自身的服务账号保密意识;在服务管理方面,严格设定关键系统的分级分权管理权限并辅之以相应规章制度,同时加强对合作供应商的资格审查与保密教育。

## 4 中小企业云服务实践

为进一步验证方案可行性并加速应用落地,项目前期在中国电信股份有限公司北京研究院实验室和陕西电信数据中心机房搭建了原型验证系统及试商用系统。图 7 是中小企业云服务试点部署架构,资源节点部署在北京和陕西两地以方便不同地域用户对资源的访问,而管理节点仅在北京部署,节省了系统投入成本。

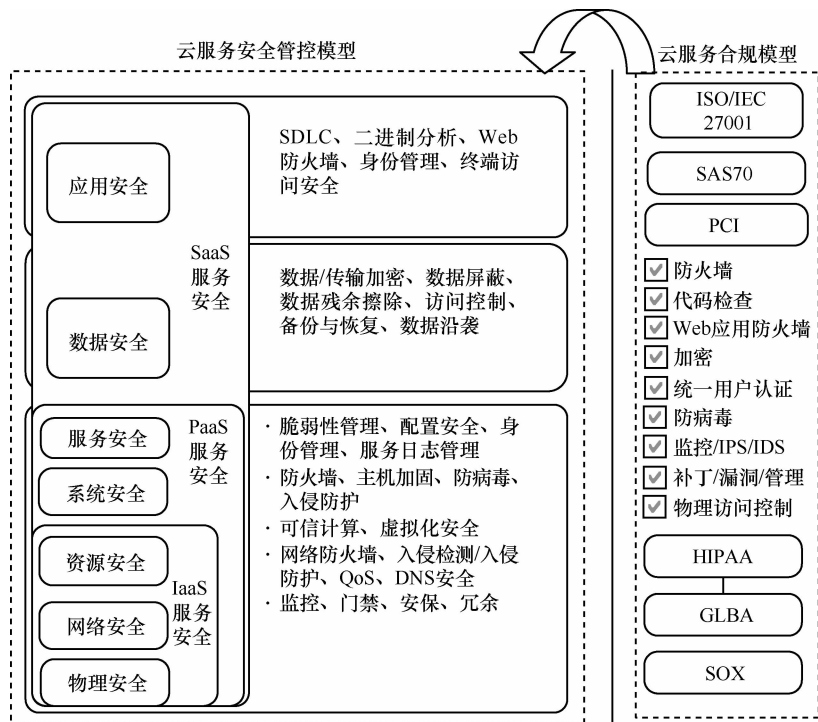


图 6 中小企业云服务安全体系架构及合规模型

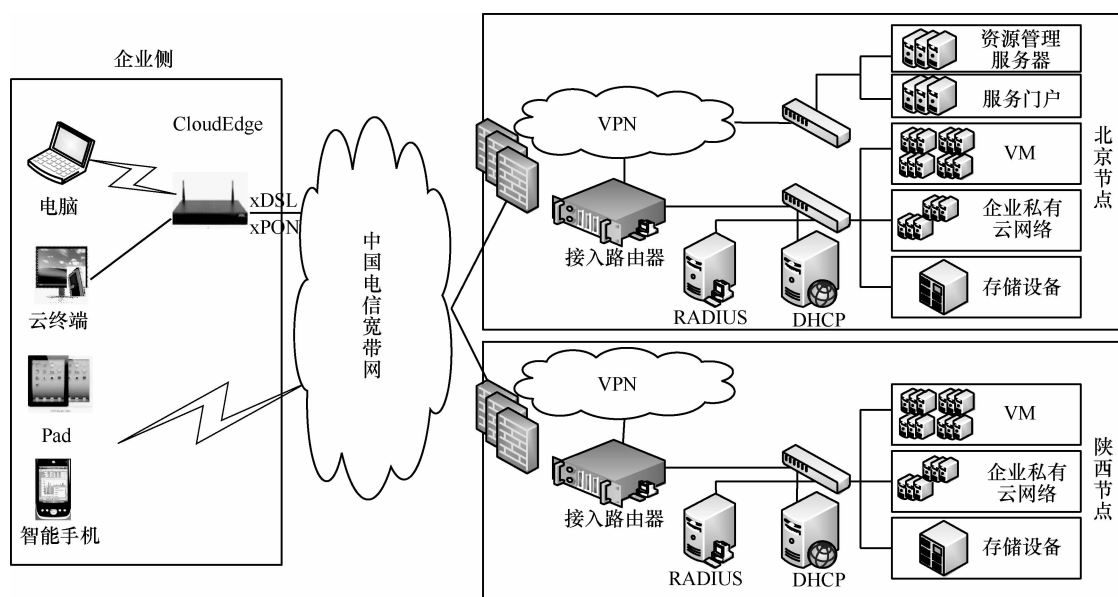


图7 中小企业云服务试点部署架构

在图7中,服务器资源、存储资源和网络设备采用分布式架构部署于北京和陕西两地,并基于开源和商用虚拟化技术构建了共享式资源池;管理和节点集中部署于北京,对陕西和北京两地的资源节点进行集中管理和统一调度;云平台的接入路由器等网络设备支持虚拟化技术;中小企业和园区客户通过有线/无线宽带接入云平台访问资源基础服务和应用服务。

在共享资源池构建及云服务管理平台实现的基础上,正在引入国内外主流SI(如微软、用友等)应用及服务能力;此外,已实现部分电信自有应用的云化验证迁移,如基于云呼叫中心实现陕西省10000号客服系统和现有OA系统的迁移。目前,中小企业云服务系列产品用户数已达到5000个。

## 5 结束语

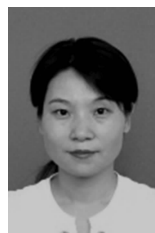
中国电信积极探索和实践中小企业云服务,通过构建基于“云—管—端”架构的中小企业云服务,解决了中小企业IT基础设施部署门槛高、初期投资大、维护困难的现实问题,实现了企业内部资源与云侧资源的无缝结合,有助于构建运营商“云—管—端”结合的云服务体系,增强运营商在中小企业云计算领域的竞争优势,推动国内中小企业云计算产业联盟的发展。

## 参考文献

- 1 Velte T, Velte A, Elsenpeter R. Cloud Computing: a Practical Approach. McGraw-Hill Osborne Media, 2009

- 2 Amazon elastic cloud computing cloud. <http://aws.amazon.com/ec2>, 2013
- 3 ITU-T Cloud-o-0081. Requirements and Framework Architecture of Cloud Infrastructure, 2012
- 4 Wood T, Shenoy P, Gerber A. The case for enterprise-ready virtual private clouds. Proceedings of the Conference on Hot Topics in Cloud Computing (HotCloud), San Diego, CA, June 2009
- 5 Bollapragada V, Khalid M, Wainner S. IPSec VPN Design. Cisco Press, 2005
- 6 ISO/IEC 27000. Information Technology-Security Techniques-Information Security Management System-Overview and Vocabulary, 2009
- 7 CSA. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 2009
- 8 NIST Special Publication 800-145. The NIST Definition of Cloud Computing (Draft) Recommendations, 2011

## [作者简介]



刘国萍,女,博士,中国电信股份有限公司北京研究院高级工程师、产品研发工程师,主要研究方向为中小企业云服务模式及信息应用安全研究。

郑燕冰,男,中国电信股份有限公司北京研究院工程师、产品研发工程师,主要研究方向为中小企业(SME)信息化应用及平台系统体系架构设计开发。

(收稿日期:2013-06-04)