计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
49(Suppl.): 186－191, 2012

云计算应用及其安全问题研究

刘 玮[1,2,3] 王丽宏[3]

[1](中国科学院计算技术研究所 北京 100190)

[2](中国科学院大学 北京 100049)

[3](国家计算机网络应急技术处理协调中心 北京 100029)

(liuwei@isc.org.cn)

A View of Cloud Computing Applications and Security Issues

Liu Wei[1,2,3] and Wang Lihong[3]

[1](*Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100190)

[2](*University of Chinese Academy of Sciences, Beijing* 100049)

[3](*National Computer network Emergency Response technical Team/Coordination Center of China, Beijing* 100029)

Abstract With the rapid evolution process of global information, following the distributed computing, parallel computing and grid computing, cloud computing has become a new Internet service model, and received widespread concern from industry, academia and government. In this paper, we study the concept of cloud computing and the status of development. Then, we propose its typical characteristics from the point of service model. Next, we discusse the probable cloud computing security problems. Finally, we advance the public cloud management services system, which can be used by the cloud computing providers to strengthen their security means, and by the consumers to choose proper cloud computing applications, and also for the establishment of third party cloud computing security assessment, monitoring and management platform. Thus the system plays a role of promoting the safety and orderly development of cloud computing industry.

Key words cloud computing; security; service standard system

摘 要 随着全球信息化进程的不断演进,云计算成为继分布式计算、并行计算、网格计算之后的一种新的互联网服务模式,受到业界和政府的广泛关注.我们从云计算的概念定义和发展现状出发,从服务模式的角度分析提出了云计算服务的典型特征,深入分析了云计算服务可能存在的安全问题,进而提出了公有云管理服务规范体系.该规范体系可以作为企业加强安全防护手段、用户按需选择云计算服务,以及建立第三方云计算安全评估、监测和管理平台的参考和依据,从而起到促进云计算产业安全、有序发展的作用.

关键词 云计算;安全问题;服务规范体系

中图法分类号 TP393

“云计算”这一概念由 IBM 公司于 2007 年 10 月提出.因动态部署、按需使用、弹性增长等特点,云计算迅速成为继分布式计算、并行计算、网格计算之后的一种新的互联网服务模式,受到业界和政府的广泛关注.在这种服务模式下,用户不需要一次性购置系统软件、服务器等大量软硬件设备,只需通过互联网将计算、存储等任务提交给云计算提供商,云计算提供商利用分布式计算机群完成任务后,再通过

收稿日期:2012-08-13

基金项目:国家自然科学基金项目(61170230);国家“八六三”高技术研究发展计划基金项目(2012AA011002)

互联网将结果反馈给用户.云计算通过互联网对用户提供IT基础资源(包括计算、存储、网络、软件等)的按需租用,能够降低用户的IT运维成本,使得用户可以专注于自身业务.

云计算经历了从概念到实践、从技术重组到模式创新的长足发展,各类云计算应用如雨后春笋般涌现.由Google、IBM、亚马逊、微软等IT巨头引领的云计算风潮愈演愈烈,纷纷发布了云计算产品和服务,如亚马逊(Amazon)的云计算服务AWS(Amazon Web Services)、Google推出的Google App Engine、IBM的Blue Cloud(蓝云)计算平台、微软的云计算平台Azure.国内有世纪互联提供的类似亚马逊EC2的云计算服务"云快线CloudEx",中国移动研究院的"大云(BigCloud)"计划,无锡市政府和IBM联合建立的太湖云计算中心等.

由于从事云计算研究的人员具有不同背景、云计算技术存在多样化、企业和机构对云计算及其前景的解析角度不同等原因,云计算一直处于"一个概念、多种表述"的状况,但这些并没有阻碍云计算市场的发展.

Gartner、IDC等咨询机构均一致看好云计算产业,认为其具有较大的市场发展空间.Gartner预测[1]到2012年,80%的财富1 000强企业将使用云计算服务.到2013年云计算服务市场规模将增长至1 501亿美元.IDC预测[2]2012年云计算市场规模可达420亿美元.目前企业引入云计算有逐年成长趋势,预计到2012年,将有8.5%的公司部署这一服务,而云计算占IT总支出的增长率达到27%,而传统IT支出的增长率为5%.

云计算作为新的互联网服务模式,在带来了诸多好处的同时也带来了新的安全问题.据国际权威咨询集团IDC的调查分析表明:用户将安全作为对云计算的主要顾虑,大约有75%的受访者担心安全问题[3].

1　云计算概念和相关定义

1.1　云计算概念

尽管目前还没有公认的云计算定义可以给人们带来统一的认识,不过可以从维基百科、云计算服务商、学术研究机构和IT专业人士的观点中获得对云计算更全面更深入的理解[4-16].综合目前工业界和研究界对云计算的各种定义,云计算的概念如下:

"云计算"这一术语泛指云计算服务、支撑云计算服务运营的云计算平台和云计算相关的技术.

云计算服务(或"云计算业务")是一种通过互联网对用户提供IT资源(包括计算、存储、网络、软件等)按需租用的服务.提供这样服务的供应商称为云计算服务商.

云计算平台是指支撑云计算服务的基础设施(包括数据中心、硬件、软件、运维支持等),它将大规模的服务器、存储设备、网络带宽甚至软件资源聚合形成共享资源池,通过先进的虚拟化技术和资源按需分配与调度等技术提供给网络用户"弹性"的IT服务能力."弹性"意味着用户可以根据业务规模快速获得所需的IT资源,同时"弹性"也意味着云计算平台可以作为一种强大的运算系统,来实现海量数据存储和处理等任务.

云计算技术是指保障云计算平台高效运行的核心技术,涉及架构、运维、硬件和软件等多方面,例如数据中心节能降耗技术[17]、海量存储技术[18]、服务器虚拟化技术[19]、资源管理与调度技术[20-21]、并行处理技术[22]、多用户共享隔离与安全技术[23]等.

美国国家标准与技术研究院制订的《云计算工作定义》[12]归纳了云计算的3种交付模式:软件即服务(software as a service,SaaS)、平台即服务(platform as a service,PaaS)、基础设施即服务(infrastructure as a service,IaaS).对于云计算的部署模式,美国国家标准与技术研究院归纳出私有云、团体云、公共云和混合云4种模式.本文针对目前主要的公共云服务,研究其可能存在的安全问题.

2　云计算典型特征和主要云计算服务

2.1　计算的典型特征

NIST定义了云服务展现出的5个关键特征,代表了它与传统计算方法的关系和区别:即按需自服务、宽带接入、虚拟化的资源"池"、快速弹性架构、可测量的服务[12].

云计算安全联盟(cloud security alliance,CSA)认为,在NIST定义的上述关键特征之外,认为多租户(multi-tenancy)是云的一个重要特征[24].

国内学者更多的从能效、系统架构、功能特性角度来定义云计算.陈康、郑纬民[25]认为,云计算是能够提供动态资源池、虚拟化和高可用性的下一代计算平台.现有的云计算实现使用的技术体现了以下3个方面的特征:硬件基础设施架构在大规模的廉价服务器集群之上;应用程序与底层服务协作开发,

最大限度地利用资源;通过多个廉价服务器之间的冗余,使用软件获得高可用性.

云计算服务的开展依赖于传统的分布式系统、网络存储等技术,归根结底是服务模式的创新.通过对现有的公认的云计算实例分析,以及学术界和工业界的普遍看法,云计算服务的典型特征分析应从其服务模式或用户使用模式入手,具体包括以下5个方面:

1) 基础资源租用.云计算服务提供对计算、存储、网络、软件等多种IT基础设施资源租用的服务.云计算服务的用户不需要自己拥有和维护这些资源.

2) 按需弹性使用.云计算服务的用户能够按需获得和使用资源,也能够按需撤销和缩减资源.云计算平台可以按用户的需求快速部署和提供资源.云计算服务的付费服务应该按资源的使用量计费.

3) 透明资源访问.云计算服务的用户不需要了解所使用资源的物理位置和配置等信息.

4) 自助业务部署.云计算服务的用户利用服务提供商提供的接口,通过网络将自己的数据和应用程序部署于云计算平台的后端数据中心,而无需服务商的人工配合.

5) 开放公众服务.云计算服务用户所部署的数据和应用可以通过互联网发布给其他用户共享使用,即提供公众服务.

2.2 主要云计算服务

云计算自2007年开始受到IT业的重视,国外各大IT企业先后投入巨资研发并运营云计算服务,国内部分企业也开始商业化运营的尝试.根据上一节提出的云计算典型特征,结合商用云计算服务,本文拟定了云计算服务范围,如表1所示.

云主机服务:是IaaS模式的一种,提供弹性的主机租用服务,一般由IDC企业或电信运营商提供.如世纪互联旗下的云快线公司提供的CloudEx服务,阿里巴巴和万网联合研发的类似Amazon EC2的IaaS服务"阿里云".

云存储服务:是IaaS模式的一种,提供按需分配的网络存储服务,即"网盘".主要提供商有华为的数据银行、新浪微盘、金山快盘和T盘等.云存储服务一般提供1G以上的网络硬盘空间,收费用户可以获得更多的空间和存储功能升级(例如文件总数、单个文件大小限制等).

平台即服务:即PaaS模式,提供Web应用开发和托管平台.新浪的Sina App Engine是国内PaaS平台,与新浪微博结合,为微博用户提供服务.

软件即服务:即SaaS模式,面向中小企业提供在线的OA,ERP,CRM等软件租用.典型服务包括用友伟库、八百客和国外著名的在线办公厂商ZOHO在中国运营的百会等.

表1 云计算服务范围表

服务类型	描述	例子
云主机租用	提供弹性和按需部署的主机租用和计算能力服务,所提供主机用于开展各类互联网信息服务	Amazon EC2 世纪互联 CloudEx 阿里巴巴 阿里云
云存储	提供在线的可按需扩展的存储服务,存储内容可以分享和传播	Amazon S3 华为 DBank 新浪微盘 金山快盘/T盘
应用平台服务	提供公共的应用开发和托管平台,所提供应用开发接口可用于开展各类互联网信息服务	Google App Engine Windows Azure Force.com 新浪 App Engine
在线软件租用服务	提供在线的软件租用服务,软件运行于远端数据中心,用户将数据的存储和处理均托管于远端数据中心	Saleforce.com 用友伟库 百会 Baihui.com 八百客 800app.com

接下来本文将结合云计算服务分析其可能带来的安全问题.

3 云计算安全问题分析

3.1 云主机服务安全问题分析

云主机服务面向网站等提供可动态分配和按需计费的主机租用服务,并为用户提供了自助管理界面,让用户可以随时添加或删除新的服务器,其一般过程为:选择机房位置、启动操作系统镜像、选择云主机的硬件配置、选择计费模式,最后是安全与备案选项,选择服务器用途,提供备案号.

完成购买后大约20 min后即获得完整权限的独立的云计算主机(Windows或Linux).云主机服务提供了非常方便和快速的自助服务,使得用户可以比以往容易获得主机资源,而按需付费的机制使得用户可以低成本的获得计算资源.同时,其可能存在的安全问题如下:

1) 对云计算用户的身份缺乏实名认证.用户注册时所需要填写的包括真实姓名、身份证和电话等,但这些信息的真实性可能未经审核.如果用户使用伪造的身份证,并且在申请云主机资源后发布不良信息,或者从事网络攻击活动,将难以追溯真实身份.

2) 对云计算用户获得的默认计算资源权限缺乏控制. 用户只需要向账户中充值即可获得动态申请云主机的功能,用户申请的云主机可以用于做任何互联网业务. 虽然安全与备案选项中列出了用户如果需要开办网站需提供备案号,在实际中,系统一般默认情况下,没有对用户新获取的主机采取端口限制,即默认用户可使用云主机开放任何信息服务(如 Web 网站、代理等).

3) 云计算主机仍存在漏洞和被攻击风险. 一般云主机租用服务都为云主机提供了免费的杀毒和木马清除软件. 但是,是否选择安装取决于用户,并且这些防护大多仅针对 Windows 主机,云主机面临和互联网上主机一样被攻击的风险.

3.2　PaaS 服务安全问题分析

开发者可以通过 PaaS 服务商定制过的编程环境进行 Web 应用开发和托管,并且可以使用其提供的公用服务,包括下载、存储、内存缓存、数据库、任务队列等. PaaS 平台通常提供一个受限的托管环境,对用户最终的应用进行安全限制. 用户通过页面注册即可下载应用开发 SDK,编写和上传应用. 其可能存在的安全问题分析如下:

1) 对用户身份的审核. 由于 PaaS 服务提供了信息发布和服务的平台,需要对开发者身份进行真实性审核.

2) 对信息发布服务缺乏备案等审核措施. 由于 PaaS 服务提供了信息托管和发布功能,并且易于与 SNS、微博等第三方应用平台对接,通过 API 方式供其他用户使用,但 PaaS 服务中的大部分应用没有申请独立备案.

3) 平台漏洞可能导致未授权的访问. 由于 PaaS 平台提供了受限的应用开发环境,其编程环境存在的漏洞可能会导致用户应用未经授权访问底层资源和其他用户的应用信息. 潜在的公用服务层 Bug 可能导致非法访问和资源滥用.

3.3　云存储服务安全问题分析

微盘一般默认给用户提供超过 1 GB 的空间,有的微盘还同时提供网页和桌面客户端方便用户同步电脑和"云"中存储的文件,利用微盘发布信息的自由性是其主要安全问题. 目前,微盘的用户身份几乎不需要验证,分享和发布到其他平台的方式也日趋简单便捷,这使得微盘信息的传播速度快、波及面广,可能面临网络恶意程序、垃圾或不良信息大量传播的安全问题.

3.4　SaaS 服务安全问题分析

SaaS 服务可能存在的安全问题主要包括以下两方面:

1) 服务宕机和数据丢失风险. 由于企业的关键数据和日常事务均租用 SaaS 平台,因此服务的可靠性、企业数据的可靠性是面临的主要问题.

2) 企业秘密泄漏风险. 底层基础设施、公有的服务平台、应用软件本身对 SaaS 用户都是透明的,SaaS 运营企业的信誉、品牌和公信力需要受到第三方检测和监督.

3.5　云计算安全问题

云计算的资源高度集中化使得传统的网络安全问题更加严峻,同时其虚拟化、多租户和动态性也引入了新的安全问题. 经过上述分析,云计算的安全问题主要涉及 3 个层面:

1) 云计算服务用户的数据和应用. 用户数据和应用托管在云计算平台面临着安全与隐私的双重风险,主要包括多租户环境下的来自云计算服务商和其他用户的未授权访问、数据访问控制、隐私保护、内容安全管理、用户认证和身份管理问题.

2) 云计算服务平台自身. 随着云计算服务的业务规模扩大和用户增多,云计算平台本身易成为黑客攻击的目标. 虚拟化计算和存储方式的技术架构使得云平台本身的安全性尤为突出,但目前尚未建立云计算安全风险评估体系以及第三方的云平台安全评估机制.

3) 云计算平台提供服务的滥用. 云计算所提供的可弹性扩展的资源有可能被当作恶意的网络攻击工具,或被当作垃圾和不良信息的传播渠道,但目前尚没有针对云计算服务水平和合法性的监督管理机制.

4　公有云安全管理服务规范体系设计

云计算的共享化、规模化特征使得传统网络安全、数据安全和内容安全问题的危害程度得到放大. 同时,云计算的资源动态供应、虚拟化等技术特征给用户带来便利的同时也给实现安全事件的可审计性带来负担. 针对第 3 节分析的云计算安全问题,云计算安全应从云安全技术体系、云安全标准及评测体系两个方面考虑,云安全技术体系主要以数据安全和隐私保护为主要目标,重点解决虚拟化应用、多租户共享带来的安全问题;云安全标准及评测体系主要以建立云安全指导标准及其评测体系为目标,重点解决安全目标验证、安全服务等级评测问题.

基于上述分析,本文提出了公有云安全管理服务规范体系,如图 1 所示:

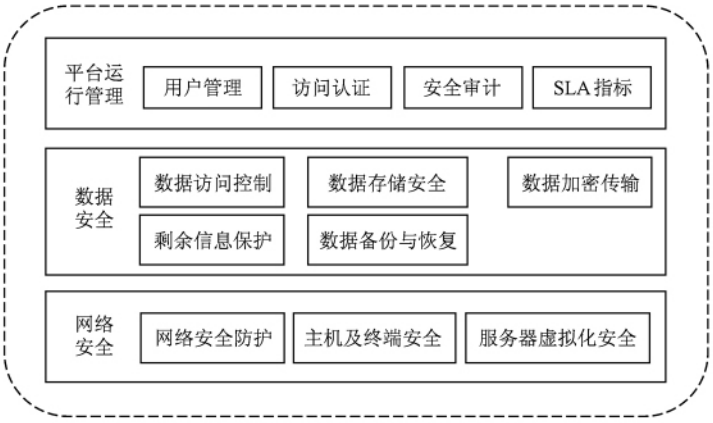

图1 公有云安全管理服务规范体系

根据公有云安全管理服务规范体系建立第三方云安全管理服务平台,提供云计算资源网络安全评估与监测服务、云计算数据传输与安全管理服务和云计算服务主体认证和质量监测服务,实现网络安全、数据安全、平台运行的3层安全评估、监测和管理功能.

4.1 云计算资源网络安全评估与监测服务

云计算资源网络安全评估与监测服务对运行云计算服务的数据中心基础设施以及提供给用户的云计算资源和接口样本(如云计算虚拟机、PaaS平台的编程接口)进行网络安全评测.具体包括:

网络安全防护:包括防火墙、DDoS检测、漏洞扫描、入侵检测设备等.

主机及终端安全:对于IaaS类服务,包括虚拟机镜像的安全性、用户自定义镜像、虚拟机到物理机的渗透漏洞测试等;对于PaaS类服务,对所提供的PaaS服务接口进行安全权限渗透和压力测试等.

该项服务可以通过API接口的方式向云计算服务商提供公用的网络安全监测服务.

4.2 云计算数据传输与安全管理服务

云计算数据传输与安全管理服务对云计算服务商提供的数据加密和防护措施进行评估,具体包括:数据存储的灾备、通信行为的私密性保护,所使用的密钥级别和加密算法等.

数据访问控制:虚拟环境下的逻辑边界安全访问控制策略设置,虚拟机、虚拟机组间的数据访问控制.

数据传输安全:是否支持采用数据加密、VPN等技术,以保障通信行为的私密性.

数据存储安全:是否支持加密存储服务.

剩余信息保护:数据删除后和存储资源重新分配前是否进行了彻底的数据擦除.

数据备份与恢复:是否支持数据完整和增量备份,是否支持映像恢复及数据恢复.

4.3 云计算服务主体认证和质量监测服务

云计算服务主体认证和质量监测服务对平台运行情况和服务质量进行评估,具体包括:是否实现平台用户帐号、访问控制、授权、审计功能的集中管理;是否建立统一、集中的认证和授权系统进行访问认证;是否建立安全审计系统,具备违规溯源的事后审查能力,以及是否符合SLA服务水平规范等.

在云计算服务主体认证服务方面,对云计算服务涉及的主体(云计算服务提供商、云计算用户)提供公共的认证服务.针对云计算用户身份核实的身份认证服务:即针对云计算用户个人或企业的身份真实性、企业资质审核的公共服务.该服务可以API接口方式提供给云计算服务商,具体方式包括:身份信息审核、移动电话审核、企业执照审核等;针对服务提供商的资质认定:即针对云计算服务商的资质进行评估,对符合资质的服务提供商发放业务牌照.

在技术标准评测方面,根据云计算服务类型,按照公用的技术标准以及供应商所提供的技术标准进行评测,以确认云计算服务商所提供的服务是否符合用户期望的SLA.

5 结束语

本文围绕云计算应用的现状及其安全问题开展研究,首先分析了目前较普遍的云计算概念和相关定义,提出了云计算区别于其他互联网应用模式的5个典型特征,即基础资源租用、按需弹性使用、透明资源访问、自助业务部署和开放公众服务.根据云计算典型特征,对云计算服务进行了分类分析,进而对其可能带来的安全问题进行了分析,最后针对这些安全问题提出了公有云安全管理服务规范体系,

该规范体系从网络安全、数据安全、平台运行管理3个层次,指出了云计算安全管理的对象和目标.公有云安全管理服务规范体系可以作为企业加强安全防护手段、用户按需选择云计算服务,以及建立第三方云计算安全评估、监测和管理平台的参考和依据,从而起到促进云计算产业安全、有序发展的作用.

参 考 文 献

[1] Christy Pettey. Gartner Says Worldwide Cloud Services Revenue Will Grow 21.3 Percent in 2009. 2009 (2009-03-26) [2012-03-18]. http://www.gartner.com/it/page.jsp?id=920712

[2] IDC: 2013年云计算市场规模可达442亿美元. 2009 (2009-10-12) [2012-03-18]. http://www.cio360.net/index.php?m=content&c=index&a=show&catid=86&id=41080

[3] CNET科技资讯网. 云计算平台只是提供云服务的第一步. 2009 (2009-04-03) [2012-03-18]. http://www.cnetnews.com.cn/2009/0403/1361303.shtml

[4] Cloud computing. [2012-03-18]. http://en.wikipedia.org/wiki/Cloud_computing

[5] 云计算. [2012-03-18]. http://baike.baidu.com/view/1316082.htm

[6] Greg Boss, Padma Malladi, Dennis Quan, et al. IBM云计算白皮书. 2007 (2007-10-08) [2012-03-15]. http://www.ibm.com/developerworks/websphere/zones/hipods/

[7] IBM云计算中心&HiPODS. "智慧的地球"——IBM云计算2.0. 2009 (2009-06-30) [2012-03-18]. http://storage.it168.com/a2009/0630/598/000000598296.shtml

[8] 李开复. 云中漫步——迎接云计算时代的到来. 2008 (2008-05) [2012-03-18]. http://www.googlechinablog.com/2008/05/blog-post_09.html

[9] 张亚勤. 未来计算在"云-端". 2008 (2008-09-04) [2012-03-18]. http://blog.sina.com.cn/s/blog_596ccc870100aps1.html

[10] 亚马逊:云计算是分层次以及类别的. 2008 (2009-06-07) [2012-03-18]. http://www.enet.com.cn/article/2009/0605/A20090605482905.shtml

[11] Sun公司. Sun的云计算架构介绍白皮书第1版. 2009 (2009-06) [2012-03-18]. http://wenku.baidu.com/view/7780d217866fb84ae45c8df0.html

[12] Michael Armbrust, Armando Fox, Rean Griffith, et al. Above the clouds: A Berkeley view of cloud computing, EECS-2009-28. UC. Berkeley. 2009 [2012-03-18]. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

[13] Chris Rose. A break in the cloud?: The reality of cloud computing // Proc of 2009 EABR & TLC Conf. Prague, Czech Republic, 2009: 1-5

[14] 钱德沛. 云计算和网格计算差别何在. 2008 (2008-10-16) [2012-03-18]. http://server.51cto.com/Visits-93098.htm

[15] Foster I, Zhao Y, Raicu I, et al. Cloud computing and grid computing 360-degree compared //Proc of the Grid Computing Environments Workshop. 2008: 1-10

[16] Luis M Vaquero, Luis Rodero-Merino, Juan Caceres, et al. A break in the clouds: Towards a cloud definition. ACM SIGCOMM Computer Communication Review, 2009, 39(1): 50-55

[17] Cheng D. PaaS-onomics: A CIO's guide to using Platform-as-a-Service to lower costs of application initiatives while improving the business value of IT. Santa Clara, CA: LongJump, 2008

[18] Chang F, Dean J, Ghemawat S, et al. Bigtable: A distributed storage system for structured data // Proc of the 7th USENIX Symp on Operating Systems Design and Implementation (OSDI'06). Berkeley, CA: USENIX, 2006

[19] Susanta Nanda, Tzi-cker Chiueh. A survey of virtualization technologies. 2005 [2012-03-21]. http://www.ittc.ku.edu/~kulkarni/teaching/archieve/EECS800-Spring-2008/survey_virtualization_technologies.pdf

[20] Zaharia M, Konwinski A, Joseph A D, et al. Improving mapreduce performance in heterogeneous environments//Proc of the 8th USENIX Symp on Operating Systems Design and Implementation. Berkeley, CA: USENIX, 2008

[21] Hindman B, Konwinski A, Zaharia M, et al. A common substrate for cluster computing //Workshop on Hot Topics in Cloud Computing (HotCloud). Berkeley, CA: USENIX, 2009: No.19

[22] Jaliya Ekanayake, Geoffrey Fox. High performance parallel computing with clouds and cloud technologies. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin: Spinger, 2010

[23] HP Labs. Cloud and Security. 2011 [2012-04-12]. http://www.hpl.hp.com/research/cloud_and_security.html

[24] 云安全联盟(CSA). 云计算关键领域安全指南. 2009 (2009-12-01) [2012-03-25]. https://cloudsecurityalliance.org/guidance/csaguide-cn.v2.1.pdf

[25] 陈康,郑纬民. 云计算:系统实例与研究现状. 软件学报, 2009, 20(5): 1337-1348

刘　玮　女,1984年生,博士研究生,主要研究方向为网络信息安全、智能信息处理.

王丽宏　女,1967年生,教授,博士生导师,主要研究方向为网络信息安全、计算机体系结构.