



云计算安全性探究

孙群英^{1,2}, 胡志远¹

(1. 上海贝尔股份有限公司战略部 上海 200120; 2. 复旦大学信息科学与工程学院 上海 200433)

摘要: 云安全问题从云计算技术发展之初就被普遍认为是制约其发展的核心因素。首先讨论了云计算系统中的不安全因素, 同时也对云计算技术带来的安全改善进行了分析, 对云安全性进行了深入剖析。指出云计算系统安全取决于现有安全策略的正确部署, 只要与云提供商签署适当的安全契约, 云计算系统并不比本地环境的安全风险更大。最后对于保证云计算系统安全问题, 分别从云提供商以及云用户两个角度给出了相应的安全策略建议。

关键词: 云计算; 云安全; 虚拟化; 云供应商城; 云用户域

doi: 10.3969/j.issn.1000-0801.2013.04.020

Security of Cloud Computing

Sun Qunying^{1,2}, Hu Zhiyuan¹

(1. Strategy Department, Alcatel-Lucent Shanghai Bell Co., Ltd., Shanghai 200120, China; 2. College of Information Science and Engineering, Fudan University, Shanghai 200433, China)

Abstract: Cloud security has been widely considered as the key factor restricting its development since the cloud computing technology emerged. The insecure factors of cloud computing system and the secure factors which cloud computing brings were presented and discussed. It was pointed out that cloud security depended on the validate deployment of the security policy. Cloud computing system is not less secure than native environment, as long as the right agreement is signed with cloud provider. Finally, the proposal of security policy was provided from both the cloud provider domain and the cloud user domain to ensure the security of cloud computing system.

Key words: cloud computing, cloud security, virtualization, cloud provider domain, cloud user domain

1 引言

云计算技术将大量计算资源、存储资源与软件资源连接在一起, 形成巨大规模的共享虚拟 IT 资源池, 提供无限制的、可伸缩的、易获得的 IT 资源服务, 正引领着 IT 行业向集约化、规模化与专业化的方向演进, 被普遍认为是继互联网经济繁荣的又一个重要 IT 产业增长点^[1-3]。但当前云计算技术还未成熟, 仍然面临系统集成、定制化服务、安全与隐私等方面的障碍, 其中云计算安全问题被普遍认为是制约云计算发展的首要因素^[4]。

近年来云计算安全事件不断爆发, 例如 2009 年 Google 发生大批用户文件泄露, Amazon 的 Simple Storage Service (S3) 两次中断; 2010 年 Microsoft 云计算服务 BPOS 发生数据泄露; 2011 年 Google 邮箱再次爆发大规模用户数据泄露, VMware 的 Cloud Foundry 服务在测试期间出现了服务中断事件等。另外, 2009 年 Gartner 和 Forrester Research 公司的调查结果显示, 大部分受访企业的 CTO 都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。IDC 在 2008 年的调查报告上显示, 2008-2010 年, 云计算服务面临的前三大市场挑战分别为

服务安全性、稳定性和性能表现,2009 年和 2010 年的调查同样显示,云计算安全是云计算技术发展的最大阻碍因素。但随着云计算技术的不断发展,近年来云安全方面已展开大量的部署,其担忧程度得到了缓解,虽然云安全和合规问题依然被认为是云决策的关键因素,但其风险并不比本地环境的安全风险更大,安全与否关键取决于安全策略的合理运用。根据 Forrester Research 公司 2012 年 11 月的最新研究报告显示,在澳大利亚,企业采用云计算的首要阻碍已经不再是云安全问题,取而代之的是云计算集成和隐私问题。

云计算系统的开放性更容易受到外部攻击,其数据的集中性更吸引黑客的攻击,其大规模性使得发生安全事件的影响更大。另外,虚拟化技术的大量运用也产生了新的安全问题,首先要保证虚拟化软件的安全;其次,虚拟机内部网络流量对传统安全设备不可见、多租户的环境复杂性、虚拟化环境下业务的自动化管理和开放性、用户对自己数据的控制能力减弱、合规性和遵从性等方面的改变都对安全提出了新要求^[5,6]。但值得注意的是,云计算技术也给传统安全问题带来了一定的改善,例如云计算的镜像副本机制以及动态迁移等特性,使整体系统和数据可靠性得到加强;数据的集中化安全管理能降低泄密的风险,有利于形成完备统一的安全体系,如 VDI 等。因此云计算技术本身给系统安全带来了正面的和负面的双重影响。

2 云安全挑战

传统的 IT 系统是封闭的,由各个私有部门控制;而在云环境中,数据、IT 基础设施和网络架构等均暴露在云中,网络环境复杂且不可控。另外,云计算系统大量运用虚拟化技术也带来了新的不安全因素。相对于传统 IT 系统,云计算系统挑战重重。

在网络方面,首先,传统网络安全技术的部署有赖于网络的物理拓扑边界;但在云计算环境中,多个业务系统共享同一物理基础设施,传统的物理边界被打破。如图 1 所示,虚拟化前,同一业务系统的两个结点位于同一安全域,安全策略(防火墙和 IDS/IPS)放置在安全域边界即可保证该业务系统的安全;虚拟化后,位于同一物理机的多个虚拟机可能不属于同一逻辑安全域,而位于不同物理服务器上的虚拟机可能属于同一逻辑安全域,传统的物理安全边界被打破^[7,8]。其次,传统网络中网络交换相关的安全策略均由外部网络设备进行部署;在虚拟化环境中,位于同一物理机的 VM 之间的流量通过物理机内的虚拟交换机进行交换,对于外部网络设备不可见,如何对流量进行监管以及监管的责任方的归属都成为了新的挑战。

在存储方面,传统模式下,信息保存在本地可控的环境中;云环境中,信息保存在云端,不同业务甚至竞争对手的数据都有可能保存在相同的物理设备中,必须保证数据的有效隔离。另一方面,为了保证云端的安全性和私密性,云端数据往往进行加密处理,这将导致传统的数据搜索和分析方法失效,带来了加密搜索、加密分析等技术的需求。此外,云计算的发展还处于成长期,云安全缺少相关标准,政策法规也不健全,特别地,由于云计算的数据可能存储在不同地区甚至不同国家,当出现问题时,不同地方政策法规的差异将是云计算安全的一个重大挑战。

虚拟化技术的引入也带来了很多新的安全问题。

- 虚拟机管理器(Hypervisor)是整个 VM 系统的核心,必须保证其完整性。
- 虚拟机之间共享硬件资源,不但要做好防病毒、防恶意软件和安全日志管理策略等,还需要做好安全隔离,防止同一物理机上的其他 VM 的攻击,但如果在每台 VM 上都安装防火墙、入侵检测软件等将造成资源的大量浪费。

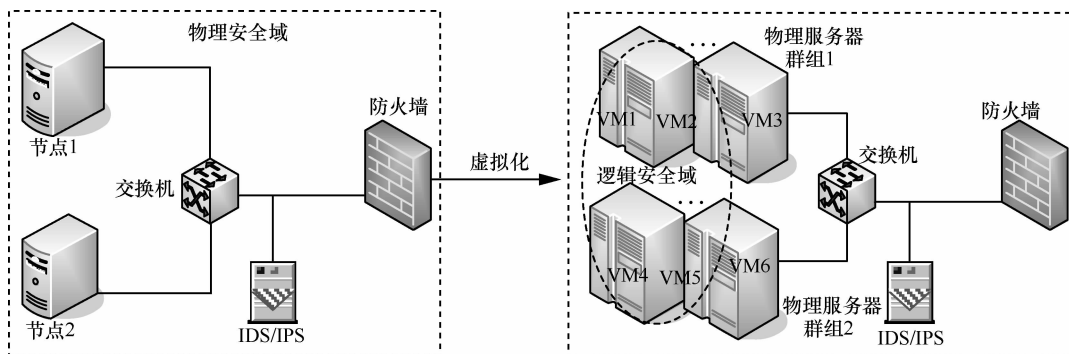


图 1 云计算系统网络拓扑



- 虚拟机迁移技术为服务器虚拟化提供了便捷的途径,但是还须保证迁移前后的安全配置环境一致以及迁移过程的安全,特别是在线迁移过程,如VMware的vMotion技术可灵活实现虚拟机的在线迁移,但其传输虚拟机内存的vMotion过程是非加密的,所以需要采取隔离措施,让所有的vMotion事件发生在专有媒介独立的网络上。

3 云安全改善

如上一节所述,云计算技术带来了众多安全挑战,使用户对自身数据的控制力减弱,但其带来的好处是用户大部分安全责任转移到云计算供应商身上。一方面,基于规模经济效益的原理,在大规模的云计算用户尤其是公有云的情况下,单位运营成本将会下降,单位安全运营的成本也会下降;更重要的是,主流的云供应商在高可靠性、安全性和冗余性上投入的成本更大,能够从系统开发之初制定安全策略方案,包括核心的云计算软件平台、相关的流程和用来控制它们的监控系统;同时,主流云供应商提供24x7h服务,会对所有操作提供持续不断的审计、监控和安全测试,响应更加专业、及时,除了确保运行的所有软件都为最新版本,还能及时发现并解决不合规事件,系统可靠性大大增强。另外,云计算技术在系统安全和数据安全方面还带来了一系列的安全改善。

在系统方面,云计算系统本质上被设计为仅执行有限的任务组,同时具有高度扩展性,要求计算硬件、网络设备、应用软件和操作系统等方面都必须实现高度标准化、自动化水平和可重复性较高,因此在引入新的设备时,出现漏打补丁或引入安全隐患(例如误开某些端口)的概率也大大降低,有益于实现安全防护。在大多数企业中,安全漏洞补丁从发布到完全安装需要几天到几周时间,而云计算系统的升级行动可实时应用到所有客户中。此外,云计算系统中,网络层、应用层和操作系统层管理层级分明,很少有人拥有超级特权的情况,避免了内部员工不当操作导致信息泄漏的问题。

在数据方面,大多数非云计算公司都是夜间备份或者重要事务备份,而主流的云供应商是实时备份并且将备份数据传输到两个或者多个全球分布的备份阵列中,并且其辅助系统方面(电力、环境控制、网络连接等)也有双重部署。另外,云计算系统中所有数据都是加密存储、加密发送的,而且个人数据淹没在大量数据中,相对于在私有云或

者非云环境中,黑客想要定位到某个特定的目标变得更加困难。

4 云安全策略

根据上两节对云计算安全的分析,云计算对系统安全带来了双重影响,从系统集成角度讲,云计算相对传统系统更加安全;从云计算技术自身讲,虚拟化技术等还存在很多安全问题需要解决。片面地认为云计算不安全或更安全都是不科学的,其安全与否最终由云计算系统的主体——云供应商和云用户决定。

4.1 云供应商域

云服务提供商作为云计算安全系统的责任主体,需要保证从系统级到应用级的安全。云供应商需要进行的系统安全考虑如图2所示,包括云物理平台安全、云中数据安全以及云平台运行安全等。

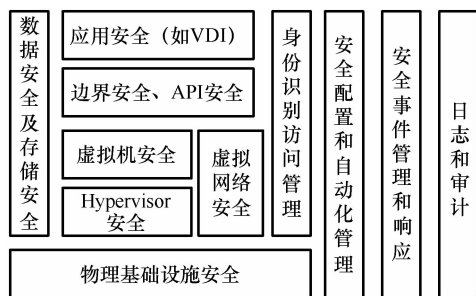


图2 云供应商域安全框架

4.1.1 云物理平台安全

云计算系统物理安全包括传统的容灾、备灾技术以及云中特有的虚拟化安全技术。如第2节所述虚拟化技术的大量运用实现资源的优化配置的同时,为云计算系统带来了众多安全挑战,包括虚拟化软件安全、虚拟机安全、虚拟机通信安全和虚拟机迁移安全等。

虚拟化软件层方面,Hypervisor作为云平台的核心,其完整性、可靠性至关重要。借助TPM(可信平台模块),在Hypervisor及各虚拟机初始化、重启之前验证其完整性,以确保其在离线时未被篡改。另外,需要对Hypervisor进行安全漏洞管理,及时对其进行补丁更新、修护,在保证Hypervisor最小化安装的同时增强安全配置,限制或禁用某些不安全的服务,以提高系统的安全性。

虚拟机安全方面,与物理设备类似,各虚拟机也需要防病毒、防恶意软件和安全日志管理策略。首先,有必要将各虚拟机进行逻辑或物理的隔离,防止物理资源共享造成

的处于同一物理机的其他虚拟机的恶意攻击。为了实现虚拟机之间的逻辑隔离,可以根据业务属性、业务安全等级、网络属性等方式对虚拟机进行分类,如将虚拟机与用户身份和/或业务逻辑标识或租户(tenant)进行关联,能在虚拟化层识别各虚拟机所从属的用户和/或业务逻辑或租户,再根据相应的访问控制策略对其进行安全保护,从而增强安全功能;还可以通过 VLAN 和不同的 IP 地址网段的方式进行逻辑隔离。对于一些运载如财务、商业机密等敏感业务逻辑的虚拟机,需要考虑采用专用的 CPU、存储、虚拟网络对其进行物理隔离。其次,可以在每台虚拟机上安装防火墙、入侵检测软件等,但这将造成资源的大量浪费。目前,业界如 VMware 的 vShield Endpoint、趋势科技的 Deep Security 等流行的做法是在一个虚拟化系统中启用一个或多个独立的具有防火墙、入侵检测等功能的安全虚拟机,为其他业务逻辑虚拟机实施安全保护,如图 3 所示,将重要的防病毒和防恶意软件功能负载卸载到安全虚拟机上,消除了防病毒代理在虚拟机中占用的空间,从而提高系统性能。

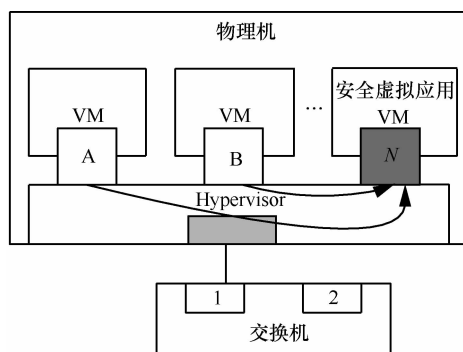


图 3 安全虚拟机

目前虚拟机之间通信的安全机制有虚拟防火墙、虚拟机间的流量分析、访问控制等。通过虚拟网络分段并在虚拟防火墙上设置安全策略以防止虚拟机之间的未授权通信。为防止虚拟机被非法访问,可结合前面讨论的虚拟机的隔离机制并通过增设相应的访问控制策略来实现。对于高安全级别的虚拟机之间的安全通信,还可以考虑建立虚拟层网络安全通道来完成。但需要注意的是,在云计算系统中,位于同一服务器内部的 VM 之间的网络流量不可见,需要考虑新的虚拟化网络流量管理方式。目前有两种模式。第一种以趋势科技等安全公司为代表,利用 VMware 等虚拟机软件公司提供的安全 API,开发安全虚拟机,能在 Hypervisor 层侦测流量交换,实现网络安全,如图 3 所示;第二种以 HP、Cisco 等网络公司为代表,已形成了两个

标准 IEEE 802.1Qbg 和 IEEE 802.1BR,该模式中将虚拟化流量引出到外部网络交换设备中,重新实现流量交换由外部网络设备进行管控,如图 4 所示。第一种模式 VM 的迁移相当于交换机的端口改变,VM 有关的网络安全策略可以自动跟随 VM 进行转移,vSphere 统一管理所有 vSwitch,相当于构成了单一大型交换机,管理简单,但服务器和上联交换机均要有网络资源管理的能力,出现问题时,可能会出现责任推诿;第二种模式可重用原有的流量管理策略,网络管理权责分明,但 Cisco 的技术需要网卡和上联交换机硬件进行升级,而 HP 的技术需要修改生成树协议。

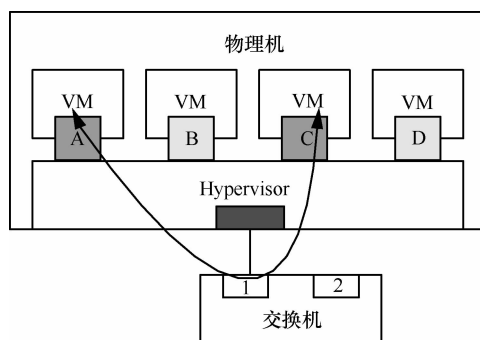


图 4 虚拟机内部流量引出模式

虚拟机迁移技术为服务器虚拟化提供了便捷的途径,但也带来了新的安全问题。一方面,如第二节所示,必须保证迁移过程的安全,特别是在线迁移过程。另一方面,还须保证迁移前后的安全配置环境一致。首先,要保证迁入端服务器的 VMM(virtual machine manager)的可靠性和完整性,这可通过可信计算、认证等技术实现;其次,虚拟机对应 VLAN ID 和 QoS 等网络层信息也应一并迁移,这在 DMTF(distributed management task force,分布式管理任务组)推出的虚拟网络白皮书已有详细的规定,可以通过网络管理中心自动跟随虚拟机迁移到新的位置^[9];再次,外置防火墙上部署的安全策略,也应进行迁移,可按照如下步骤进行。

(1)通过虚拟机管理中心 vCenter 感知虚拟机的迁移过程,提取该迁移消息中的有效信息,并通过内部维护的网络拓扑关系等技术定位到新的防火墙。

(2)对于迁出服务器对应的防火墙产品的安全策略重新标记,使迁出虚拟机的相关安全策略不再处于激活状态。

(3)对于迁入的防火墙,将虚拟机所绑定或对应的安全策略组进行配置下发,以保证该虚拟机仍然可以得到和迁移前相同的访问控制权限。



(4)最后,需保证虚拟机与服务器之间的认证、授权信息同步迁移。

4.1.2 数据安全

在传输安全方面,用户通过 Internet 访问云服务上传和下载数据时,采用的传输协议需要保证数据的机密性和完整性。

在存储方面,云计算供应商应为用户提供安全存储服务以保护其用户的敏感数据,云中存储的机密数据必须通过访问控制组合、合同责任和加密措施等进行保护。对于静态用户数据应进行加密存储,防止恶意云服务提供商、恶意的邻居租户及不良应用滥用合法用户的数据。若仅使用简单存储服务,用户可将加密文数据直接存储在云中,但是对于 PaaS 或者 SaaS 应用来说,数据加密将导致原有的数据搜索和分析算法失效,目前关于密文处理算法的研究已经有了大量成果,如同态加密、谓词加密等^[10,11],但与可商用还有较大距离。另外,在云计算系统中,数据残留更有可能会有意泄露敏感信息,因此,云服务提供商应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除,无论这些信息是存放在硬盘上还是在内存中。最后,若移动终端丢失,云服务提供商应提供隐私保护机制,通过远程锁定或远程擦除设备中的信息,保护用户的隐私。

4.1.3 身份认证安全

云计算身份管理仍需要从用户管理,认证管理,授权管理,接入管理,数据管理和供应、监测和审计 6 个方面来考虑,但云计算多租户以及物理边界被打破的特点,使得其对身份和访问管理技术有更高的要求。

对于企业级云资源用户,对身份和访问管理(IAM)有更高的要求,要求其云资源的访问控制和企业内部的访问控制措施联合,比如支持目录等。可以利用企业现有的身份授权对云计算资源进行安全授权。

(1)需要利用云 IAM 来创建和管理云服务用户和群组,为他们分配安全证书(即访问密钥、密码、多因子认证设备),或请求临时安全证书,供他们访问云服务和资源。可以管理权限以控制用户可执行的操作。

(2)可以利用云中的 IAM 创建角色和管理权限,定义允许承担该角色的实体。添加条件来控制用户和角色的云服务使用方式,如时间、来源 IP 地址,或者是否使用 SSL 等。控制承担该角色的实体或云计算资源可执行的操作,如访问特定的云计算 API 和资源。

(3)支持公司目录和云资源之间的身份联合。可以利用企业现有的身份授权对云计算资源进行安全授权,不必为这些用户创建新的身份。用户可以通过请求临时安全证书(这些证书可用于签署向云服务发送的请求)来启用身份联合。临时安全证书的组成包含短期存活的访问密钥以及与密钥关联的会话令牌。企业用户可以像往常一样使用这些访问密钥,只要在发送至云服务 API 的调用中传递相应的令牌即可。与临时安全证书关联的权限级别不会高于签发这些证书的 IAM 用户权限级别,可以在创建证书的请求中指定显式权限,从而做出进一步的限制。对于可以签发的临时安全证书的数量,并不存在限制。

目前 Amazon 公司已推出 AWS IAM 产品,为了便于开发者应用身份与访问管理,以上的身份有效管理、认证及访问授权等可以采用 API 的方式来实现,可借鉴的技术可参考 Amazon 的《AWS Identity and Access Management API Reference》。

4.2 云用户域

用户端作为云计算系统的一部分,自身也需要部署必要的安全措施或者正确利用云服务提供商提供的安全机制,保证云环境中端到端的安全,用户域安全框架如图 5 所示。首先要保证用户端设备安全,其次要保证用户访问安全。用户设备安全研究内容包括用户终端的硬件芯片安全、软件安全与浏览器安全;用户访问安全包括连接安全和存储安全。

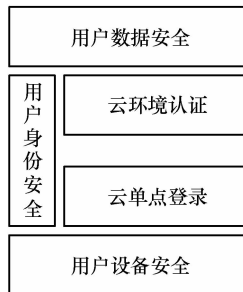


图 5 用户域安全框架

4.2.1 终端安全问题

云终端作为云计算的接入实体,安全的云终端可以更好地保证用户接入到安全的云平台中,同时也能减少云平台受到非法访问和恶意攻击的可能性,实现云环境中端到端的安全。应在云终端上部署安全软件,包括防病毒、个人防火墙以及其他类型查杀移动恶意代码的软件,同时应具有自动安全更新功能,定期完成打补丁和更新工作。此外,采用安全芯片、安全硬件/固件、安全终端软件和针对终端的安全证书等技术来提高云终端的安全性,其中安全芯片

和安全硬件/固件是从核心芯片和硬件角度确保云终端不被非法修改和添加恶意功能;安全软件则是从软件角度保证系统软件和应用软件的安全性;安全证书是确保云终端来自合法厂商,使云终端有更好的可溯源性。

4.2.2 用户访问安全方面

传统的企业或机构管理中,诸如硬件、数据、应用程序等资源都部署在企业或机构所管控的范围之内,其“信任边界”处于企业或机构的IT部门监控之下;但在云计算中,该边界有可能迁移到本企业或机构的IT控制范围之外。这种控制权的丢失,对已有的信任管理和控制模式形成了很大的挑战。

在用户连接方面,由于云虚拟机位于用户防火墙之外,很有可能遭受外来攻击,所以在连接VM之前需要先验证其完整性;在身份认证方面,传统的身份认证管理都在本地进行,而云计算中这些都在云端进行,代替了本地IT管理员的职能,但是在多数情况下,云端的身份管理并不能完全满足云客户个性化的需求,云客户仍然需要本地IT管理员保留用户的访问权限,特别是在增加新用户和取消用户时,一方面方便管理,另一方面云客户不希望在云端上管理账号、用户名等信息,所有和这些相关的操作都应该在防火墙之后进行。

最后,为了保证云计算安全,除了做好供应商域和用户域的安全外,还必须对云平台、云中信息安全以及用户设备进行管控。用户设备管控对可能危害云平台的用户行为进行预警,并对危害平台的攻击者进行定位;云中信息管控可对云中违规的内容进行搜索、检查、清除;云平台的安全管控主要针对云平台被攻击者滥用以及内部人员滥用、误用等行为进行安全监管。此外,需要相关部门制定技术标准以及法律法规来规范云计算市场,这需要政府部门、研究机构、供应商、集成商和咨询公司等各方面的共同努力。

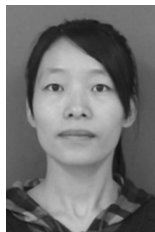
5 结束语

云计算系统本身大规模的特点使其安全影响更大,另外其广泛应用的虚拟化技术也引入了新的安全问题。但虚拟化技术安全并不是固有的技术难题,随着云计算技术的发展,最终仍能通过部署现有的安全策略进行解决。而且从系统集成角度讲,云计算自动化程度更高,人为的不当配置或误操作等安全隐患将大大减少。云计算供应商域、用户域以及监管域安全技术的逐步成熟将保证云计算系统的安全,理想情况下比传统系统更加安全。

参考文献

- 1 房晶, 吴昊, 白松林. 云计算安全研究综述. 电信科学, 2011(4): 37~42
- 2 冯登国, 张敏, 张妍等. 云计算安全研究. 软件学报, 2011,22(1): 71~83
- 3 黄瑛, 石文昌. 云基础设施安全性研究综述. 计算机科学, 2011,38(7):24~30
- 4 Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 2011,34(1):1~11
- 5 张云勇, 陈清金, 潘松柏等. 云计算安全关键技术研究. 电信科学, 2010(9):64~69
- 6 房晶, 吴昊, 白松林. 云计算的虚拟化安全问题. 电信科学, 2012(4):135~140
- 7 Sun Q, Hu Z. Security for networks virtual access of cloud computing: multimedia information networking and security (MINES). IEEE Fourth International Conference, Nanjing, China, 2-4 Nov 2012
- 8 van Cleeff A, Pieters W, Wieringa R J. Security implications of virtualization: a literature study. International Conference on Computational Science and Engineering (CSE'09), Vancouver, Canada, 29-31 Aug 2009
- 9 Virtual networking management white paper. http://www.dmtf.org/sites/default/files/standards/documents/DSP2025_1.0.0.pdf
- 10 王丽娜. 云计算环境下数据防泄漏关键技术研究. http://www.emc-china.com/rsaconference/2011/download/presentations/Day2_LiNaWang_Hackers&Threats.pdf, 2011
- 11 Van Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers. Proceedings of EUROCRYPT 2010, French Riviera, 2010:24~43

[作者简介]



孙群英,女,博士,上海贝尔股份有限公司工程师,主要研究方向为云计算安全。



胡志远,女,博士,上海贝尔股份有限公司教授级高级工程师,移动开放联盟(OMA)安全组副主席、中国移动标准化通信协会(CCSA)无线通信安全组副主席,主要研究方向为信息安全。

(收稿日期:2013-03-11)