云计算安全关键技术分析

张云勇,陈清金,潘松柏,魏进武
(中国联通研究院　北京 100048)

摘 要　云计算以一种新兴的共享基础架构的方法,提供“资源池”化的由网络、信息和存储等组成的服务、应用、信息和基础设施等的使用。云计算的按需自服务、宽带接入、虚拟化资源池、快速弹性架构、可测量的服务和多租户等特点,直接影响到了云计算环境的安全威胁和相关的安全保护策略。云计算具备了众多的好处,从规模经济到应用可用性,其绝对能给应用环境带来一些积极的因素。如今,在广大云计算提供商和支持者的推崇下,众多企业用户已开始跃跃欲试。然而,云计算也带来了一些新的安全问题,由于众多用户共享 IT 基础架构,安全的重要性非同小可。本文分析了云计算特定的安全需求和解决方案以及国内外的研究和产品现状。

关键词　云计算;虚拟化;安全;可信

1　云计算安全问题

根据 IDC 在 2009 年年底发布的一项调查报告显示,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。该三大挑战排名同 IDC 于 2008 年进行的云计算服务调查结论完全一致。2009 年 11 月,Forrester Research 公司的调查结果显示,有 51%的中小型企业认为安全性和隐私问题是他们尚未使用云服务的最主要原因。由此可见,安全性是客户选择云计算时的首要考虑因素。

云计算由于其用户、信息资源的高度集中,带来的安全事件后果与风险也较传统应用高出很多。在 2009 年,Google、Microsoft、Amazon 等公司的云计算服务均出现了重大故障,导致成千上万客户的信息服务受到影响,进一步加剧了业界对云计算应用安全的担忧。

总体来说,云计算技术主要面临以下安全问题。

(1)虚拟化安全问题

利用虚拟化带来的可扩展有利于加强在基础设施、平台、软件层面提供多租户云服务的能力,然而虚拟化技术也会带来以下安全问题:

- 如果主机受到破坏,那么主要的主机所管理的客户端服务器有可能被攻克;
- 如果虚拟网络受到破坏,那么客户端也会受到损害;
- 需要保障客户端共享和主机共享的安全,因为这些共享有可能被不法之徒利用其漏洞;
- 如果主机有问题,那么所有的虚拟机都会产生问题。

(2)数据集中后的安全问题

用户的数据存储、处理、网络传输等都与云计算系统有关。如果发生关键或隐私信息丢失、窃取,对用户来说无疑是致命的。如何保证云服务提供商内部的安全管理和访问控制机制符合客户的安全需求;如何实施有效的安全审计,对数据操作进行安全监控;如何避免云计算环境中多用户共存带来的潜在风险都成为云计算环境所面临的安全挑战。

(3)云平台可用性问题

用户的数据和业务应用处于云计算系统中,其业务流

程将依赖于云计算服务提供商所提供的服务,这对服务商的云平台服务连续性、SLA 和 IT 流程、安全策略、事件处理和分析等提出了挑战。另外,当发生系统故障时,如何保证用户数据的快速恢复也成为一个重要问题。

(4)云平台遭受攻击的问题

云计算平台由于其用户、信息资源的高度集中,容易成为黑客攻击的目标,由于拒绝服务攻击造成的后果和破坏性将会明显超过传统的企业网应用环境。

(5)法律风险

云计算应用地域性弱、信息流动性大,信息服务或用户数据可能分布在不同地区甚至不同国家,在政府信息安全监管等方面可能存在法律差异与纠纷;同时由于虚拟化等技术引起的用户间物理界限模糊而可能导致的司法取证问题也不容忽视。

2 云计算安全参考模型

从 IT 网络和安全专业人士的视角出发, 可以用统一分类的一组公用的、简洁的词汇来描述云计算对安全架构的影响,在这个统一分类的方法中,云服务和架构可以被解构,也可以被映射到某个包括安全、可操作控制、风险评估和管理框架等诸多要素的补偿模型中去,进而符合合规性标准。

云计算模型之间的关系和依赖性对于理解云计算的安全非常关键,IaaS (基础设施即服务) 是所有云服务的基础,PaaS(平台即服务)一般建立在 IaaS 之上,而 SaaS(软件即服务)一般又建立在 PaaS 之上,它们之间的关系如图 1 所示。

IaaS 涵盖了从机房设备到硬件平台等所有的基础设施资源层面。PaaS 位于 IaaS 之上,增加了一个层面用以与应用开发、中间件能力以及数据库、消息和队列等功能集成。PaaS 允许开发者在平台之上开发应用,开发的编程语言和工具由 PaaS 支持提供。SaaS 位于底层的 IaaS 和 PaaS 之上,能够提供独立的运行环境,用以交付完整的用户体验,包括内容、展现、应用和管理能力。

云安全架构的一个关键特点是云服务提供商所在的等级越低,云服务用户自己所要承担的安全能力和管理职责就越多。下面对云计算安全领域中的数据安全、应用安全和虚拟化安全等问题(见表 1)的应对策略和技术进行重点阐述。

表 1 云安全内容矩阵

云安全层次	云安全内容
数据安全	数据传输、数据隔离、数据残留
应用安全	终端用户安全、SaaS 安全、PaaS 安全、IaaS 安全
虚拟化安全	虚拟化软件、虚拟服务器

3 云计算安全关键技术

3.1 数据安全

云用户和云服务提供商应避免数据丢失和被窃,无论使用哪种云计算的服务模式(SaaS/PaaS/IaaS),数据安全都变得越来越重要。以下针对数据传输安全、数据隔离和数据残留等方面展开讨论。

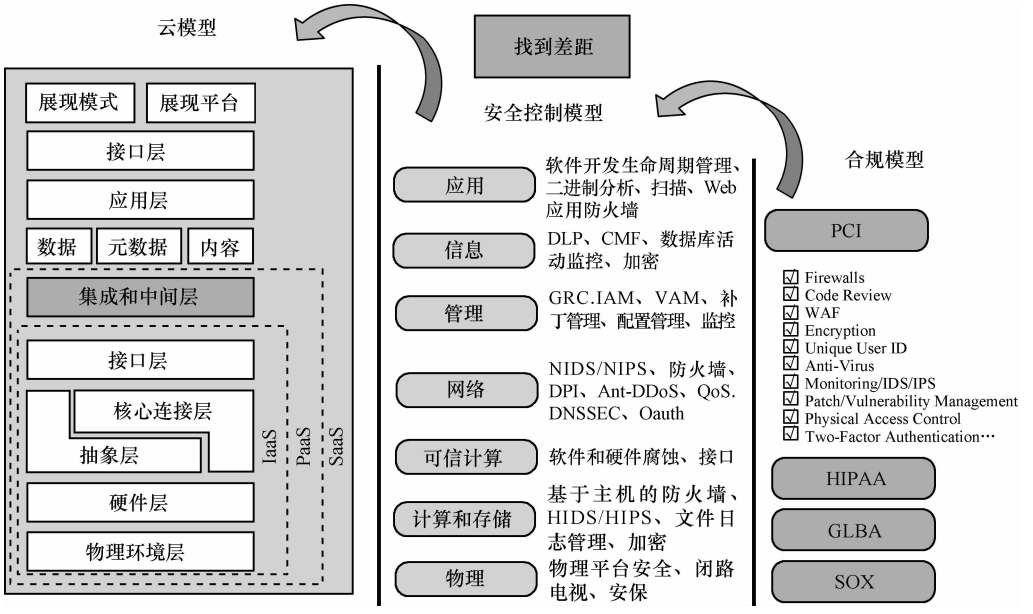

图 1 云计算安全参考模型

(1)数据传输安全

在使用公共云时,对于传输中的数据最大的威胁是不采用加密算法。通过 Internet 传输数据,采用的传输协议也要能保证数据的完整性。如果采用加密数据和使用非安全传输协议的方法也可以达到保密的目的,但无法保证数据的完整性。

(2)数据隔离

加密磁盘上的数据或生产数据库中的数据很重要(静止的数据),这可以用来防止恶意的云服务提供商、恶意的邻居"租户"及某些类型应用的滥用。但是静止数据加密比较复杂,如果仅使用简单存储服务进行长期的档案存储,用户加密他们自己的数据后发送密文到云数据存储商那里是可行的。但是对于 PaaS 或者 SaaS 应用来说,数据是不能被加密,因为加密过的数据会妨碍索引和搜索。到目前为止还没有可商用的算法实现数据全加密。

PaaS 和 SaaS 应用为了实现可扩展、可用性、管理以及运行效率等方面的"经济性",基本都采用多租户模式,因此被云计算应用所用的数据会和其他用户的数据混合存储(如 Google 的 BigTable)。虽然云计算应用在设计之初已采用诸如"数据标记"等技术以防非法访问混合数据,但是通过应用程序的漏洞,非法访问还是会发生,最著名的案例就是 2009 年 3 月发生的谷歌文件非法共享。虽然有些云服务提供商请第三方审查应用程序或应用第三方应用程序的安全验证工具加强应用程序安全,但出于经济性考虑,无法实现单租户专用数据平台,因此惟一可行的选择就是不要把任何重要的或者敏感的数据放到公共云中。

(3)数据残留

数据残留是数据在被以某种形式擦除后所残留的物理表现,存储介质被擦除后可能留有一些物理特性使数据能够被重建。在云计算环境中,数据残留更有可能会无意泄露敏感信息,因此云服务提供商应能向云用户保证其鉴别信息所在的存储空间被释放或再分配给其他云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。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云用户前得到完全清除。

3.2 应用安全

由于云环境的灵活性、开放性以及公众可用性等特性,给应用安全带来了很多挑战。提供商在云主机上部署的 Web 应用程序应当充分考虑来自互联网的威胁。

(1)终端用户安全

对于使用云服务的用户,应该保证自己计算机的安全。在用户的终端上部署安全软件,包括反恶意软件、防病毒、个人防火墙以及 IPS 类型的软件。目前,浏览器已经普遍成为云服务应用的客户端,但不幸的是所有的互联网浏览器毫无例外地存在软件漏洞,这些软件漏洞加大了终端用户被攻击的风险,从而影响云计算应用的安全。因此云用户应该采取必要措施保护浏览器免受攻击,在云环境中实现端到端的安全。云用户应使用自动更新功能,定期完成浏览器打补丁和更新工作。

随着虚拟化技术的广泛应用,许多用户现在喜欢在桌面或笔记本电脑上使用虚拟机来区分工作(公事与私事)。有人使用 VMware Player 来运行多重系统(比如使用 Linux 作为基本系统),通常这些虚拟机甚至都没有达到补丁级别。这些系统被暴露在网络上更容易被黑客利用成为流氓虚拟机。对于企业客户,应该从制度上规定连接云计算应用的 PC 机禁止安装虚拟机,并且对 PC 机进行定期检查。

(2)SaaS 应用安全

SaaS 应用提供给用户的能力是使用服务商运行在云基础设施之上的应用,用户使用各种客户端设备通过浏览器来访问应用。用户并不管理或控制底层的云基础设施,如网络、服务器、操作系统、存储甚至其中单个的应用能力,除非是某些有限用户的特殊应用配置项。SaaS 模式决定了提供商管理和维护整套应用,因此 SaaS 提供商应最大限度地确保提供给客户的应用程序和组件的安全,客户通常只需负责操作层的安全功能,包括用户和访问管理,所以选择 SaaS 提供商特别需要慎重,目前对于提供商评估通常的做法是根据保密协议,要求提供商提供有关安全实践的信息。该信息应包括设计、架构、开发、黑盒与白盒应用程序安全测试和发布管理。有些客户甚至请第三方安全厂商进行渗透测试(黑盒安全测试),以获得更为详实的安全信息,不过渗透测试通常费用很高而且也不是所有提供商都同意这种测试。

还有一点需要特别注意的是,SaaS 提供商提供的身份验证和访问控制功能,通常情况下这是客户管理信息风险惟一的安全控制措施。大多数服务包括谷歌都会提供基于 Web 的管理用户界面。最终用户可以分派读取和写入权限给其他用户。然而这个特权管理功能可能不先进,细粒度访问可能会有弱点,也可能不符合组织的访问控制标准。

用户应该尽量了解云特定访问控制机制，并采取必要步骤，保护在云中的数据；应实施最小化特权访问管理，以消除威胁云应用安全的内部因素。

所有有安全需求的云应用都需要用户登录，有许多安全机制可提高访问安全性，比如说通行证或智能卡，而最为常用的方法是可重用的用户名和密码。如果使用强度最小的密码（如需要的长度和字符集过短）和不做密码管理（过期，历史）很容导致密码失效，而这恰恰是攻击者获得信息的首选方法，从而容易被猜到密码。因此云服务提供商应能够提供高强度密码；定期修改密码，时间长度必须基于数据的敏感程度；不能使用旧密码等可选功能。

在目前的 SaaS 应用中，提供商将客户数据（结构化和非结构化数据）混合存储是普遍的做法，通过惟一的客户标识符，在应用中的逻辑执行层可以实现客户数据逻辑上的隔离，但是当云服务提供商的应用升级时，可能会造成这种隔离在应用层执行过程中变得脆弱。因此，客户应了解 SaaS 提供商使用的虚拟数据存储架构和预防机制，以保证多租户在一个虚拟环境所需要的隔离。SaaS 提供商应在整个软件生命开发周期加强在软件安全性上的措施。

（3）PaaS 应用安全

PaaS 云提供给用户的能力是在云基础设施之上部署用户创建或采购的应用，这些应用使用服务商支持的编程语言或工具开发，用户并不管理或控制底层的云基础设施，包括网络、服务器、操作系统或存储等，但是可以控制部署的应用以及应用主机的某个环境配置。PaaS 应用安全包含两个层次：PaaS 平台自身的安全；客户部署在 PaaS 平台上应用的安全。

SSL 是大多数云安全应用的基础，目前众多黑客社区都在研究 SSL，相信 SSL 在不久的将来将成为一个主要的病毒传播媒介。PaaS 提供商必须明白当前的形势，并采取可能的办法来缓解 SSL 攻击，避免应用被暴露在默认攻击之下。用户必须要确保自己有一个变更管理项目，在应用提供商指导下进行正确应用配置或打配置补丁，及时确保 SSL 补丁和变更程序能够迅速发挥作用。

PaaS 提供商通常都会负责平台软件包括运行引擎的安全，如果 PaaS 应用使用了第三方应用、组件或 Web 服务，那么第三方应用提供商则需要负责这些服务的安全。因此用户需要了解自己的应用到底依赖于哪个服务，在采用第三方应用、组件或 Web 服务的情况下用户应对第三方应用提供商做风险评估。目前，云服务提供商借口平台的安全使用信息会被黑客利用而拒绝共享，尽管如此，客户应尽可能地要求云服务提供商增加信息透明度以利于风险评估和安全管理。

在多租户 PaaS 的服务模式中，最核心的安全原则就是多租户应用隔离。云用户应确保自己的数据只能有自己的企业用户和应用程序访问。提供商维护 PaaS 平台运行引擎的安全，在多租户模式下必须提供“沙盒”架构，平台运行引擎的“沙盒”特性可以集中维护客户部署在 PaaS 平台上应用的保密性和完整性。云服务提供商负责监控新的程序缺陷和漏洞，以避免这些缺陷和漏洞被用来攻击 PaaS 平台和打破“沙盒”架构。

云用户部署的应用安全需要 PaaS 应用开发商配合，开发人员需要熟悉平台的 API、部署和管理执行的安全控制软件模块。开发人员必须熟悉平台特定的安全特性，这些特性被封装成安全对象和 Web 服务。开发人员通过调用这些安全对象和 Web 服务实现在应用内配置认证和授权管理。对于 PaaS 的 API 设计，目前没有标准可用，这对云计算的安全管理和云计算应用可移植性带来了难以估量的后果。

PaaS 应用还面临着配置不当的威胁，在云基础架构中运行应用时，应用在默认配置下安全运行的概率几乎为零。因此，用户最需要做的事就是改变应用的默认安装配置，需要熟悉应用的安全配置流程。

（4）IaaS 应用安全

IaaS 云提供商（例如亚马逊 EC2、GoGrid 等）将客户在虚拟机上部署的应用看作是一个黑盒子，IaaS 提供商完全不知道客户应用的管理和运维。客户的应用程序和运行引擎，无论运行在何种平台上，都由客户部署和管理，因此客户负有云主机之上应用安全的全部责任，客户不应期望 IaaS 提供商的应用安全帮助。

3.3 虚拟化安全

基于虚拟化技术的云计算引入的风险主要有两个方面：一个是虚拟化软件的安全；另一个使用虚拟化技术的虚拟服务器的安全。

（1）虚拟化软件安全

该软件层直接部署于裸机之上，提供能够创建、运行和销毁虚拟服务器的能力。实现虚拟化的方法不止一种，实际上，有几种方法都可以通过不同层次的抽象来实现相同的结果，如操作系统级虚拟化、全虚拟化或半虚拟化。在 IaaS 云平台中，云主机的客户不必访问此软件层，它完全应该由云服务提供商来管理。

由于虚拟化软件层是保证客户的虚拟机在多租户环境下相互隔离的重要层次,可以使客户在一台计算机上安全地同时运行多个操作系统,所以必须严格限制任何未经授权的用户访问虚拟化软件层。云服务提供商应建立必要的安全控制措施,限制对于 Hypervisor 和其他形式的虚拟化层次的物理和逻辑访问控制。

虚拟化层的完整性和可用性对于保证基于虚拟化技术构建的公有云的完整性和可用性是最重要,也是最关键的。一个有漏洞的虚拟化软件会暴露所有的业务域给恶意的入侵者。

(2)虚拟服务器安全

虚拟服务器位于虚拟化软件之上,对于物理服务器的安全原理与实践也可以被运用到虚拟服务器上,当然也需要兼顾虚拟服务器的特点。下面将从物理机选择、虚拟服务器安全和日常管理三方面对虚拟服务器安全进行阐述。

应选择具有 TPM 安全模块的物理服务器,TPM 安全模块可以在虚拟服务器启动时检测用户密码,如果发现密码及用户名的 Hash 序列不对,就不允许启动此虚拟服务器。因此,对于新建的用户来说,选择这些功能的物理服务器来作为虚拟机应用是很有必要的。如果有可能,应使用新的带有多核的处理器,并支持虚拟技术的 CPU,这就能保证 CPU 之间的物理隔离,会减少许多安全问题。

安装虚拟服务器时,应为每台虚拟服务器分配一个独立的硬盘分区,以便将各虚拟服务器之间从逻辑上隔离开来。虚拟服务器系统还应安装基于主机的防火墙、杀毒软件、IPS(IDS)以及日志记录和恢复软件,以便将它们相互隔离,并与其他安全防范措施一起构成多层次防范体系。

对于每台虚拟服务器应通过 VLAN 和不同的 IP 网段的方式进行逻辑隔离。对需要相互通信的虚拟服务器之间的网络连接应当通过 VPN 的方式来进行,以保护它们之间网络传输的安全。实施相应的备份策略,包括它们的配置文件、虚拟机文件及其中的重要数据都要进行备份,备份也必须按一个具体的备份计划来进行,应当包括完整、增量或差量备份方式。

在防火墙中,尽量对每台虚拟服务器做相应的安全设置,进一步对它们进行保护和隔离。将服务器的安全策略加入到系统的安全策略当中,并按物理服务器安全策略的方式来对等。

从运维的角度来看,对于虚拟服务器系统,应当像对一台物理服务器一样地对它进行系统安全加固,包括系统补丁、应用程序补丁、所允许运行的服务、开放的端口等。同时严格控制物理主机上运行虚拟服务的数量,禁止在物理主机上运行其他网络服务。如果虚拟服务器需要与主机进行连接或共享文件,应当使用 VPN 方式进行,以防止由于某台虚拟服务器被攻破后影响物理主机。文件共享也应当使用加密的网络文件系统方式进行。需要特别注意主机的安全防范工作,消除影响主机稳定和安全性的因素,防止间谍软件、木马、病毒和黑客的攻击,因为一旦物理主机受到侵害,所有在其中运行的虚拟服务器都将面临安全威胁,或者直接停止运行。

对虚拟服务器的运行状态进行严密的监控,实时监控各虚拟机当中的系统日志和防火墙日志,以此来发现存在的安全隐患。对不需要运行的虚拟机应当立即关闭。

4 云计算安全现状

云计算应用安全研究目前还处于起步阶段,业界尚未形成相关标准,目前主要的研究组织主要包括 CSA(cloud security alliance,云安全联盟)、CAM (common assurance metric – beyond the cloud)等相关论坛。

为推动云计算应用安全的研究交流与协作发展,业界多家公司在 2008 年 12 月联合成立了 CSA,该组织是一个非赢利组织,旨在推广云计算应用安全的最佳实践,并为用户提供云计算方面的安全指引。CSA 在 2009 年 12 月 17 日发布的《云计算安全指南》,着重总结了云计算的技术架构模型、安全控制模型以及相关合规模型之间的映射关系,从云计算用户角度阐述了可能存在的商业隐患、安全威胁以及推荐采取的安全措施。目前已经有越来越多的 IT 企业、安全厂商和电信运营商加入到该组织。

另外,欧洲网络信息安全局(ENISA)和 CSA 联合发起了 CAM 项目。CAM 项目的研发目标是开发一个客观、可量化的测量标准,供客户评估和比较云计算服务提供商安全运行的水平,CAM 计划于 2010 年底提出内容架构,并推向全球。

许多云服务提供商,如 Amazon、IBM、Microsoft 等纷纷提出并部署了相应的云计算安全解决方案,主要通过采用身份认证、安全审查、数据加密、系统冗余等技术及管理手段来提高云计算业务平台的健壮性、服务连续性和用户数据的安全性。另外,在电信运营商中 Verizon 也已经推出了云安全特色服务。

在 IT 杀毒产业中,云安全的概念提出后,其发展迅

速,瑞星、趋势、卡巴斯基、MCAFEE、SYMANTEC、江民科技、PANDA、金山、360 安全卫士、卡卡上网安全助手等都推出了云安全解决方案。瑞星基于云安全策略开发的 2009 新品,每天拦截数百万次木马攻击,其中 1 月 8 日更是达到了 765 万余次。趋势科技云安全已经在全球建立了 5 大数据中心,几万部在线服务器。据悉,云安全可以支持平均每天 55 亿条点击查询,每天收集分析 2.5 亿个样本,资料库第一次命中率就可以达到 99%。借助云安全,趋势科技现在每天阻断的病毒感染最高达 1 000 万次。

从上可知,目前的云安全产品主要来自于传统的 IT 杀毒软件厂商,其产品也主要集中在应用的安全领域,要实现云安全指南中定义的关键领域的安全保障,还需要云平台提供商,系统集成商,云服务提供商,杀毒软件厂商等的共同努力。

参考文献

1 Sanjay Ghemawat, Howard Gobioff, Shun-Tak Leung. The google file system. http://labs.google.com/papers/gfs-sosp2003.pdf

2 Mike Burrows. The chubby lock service for loosely-coupled distributed systems. http://labs.google.com/papers/chubby-osdi06.pdf

3 Michael Armbrust, Armando Fox, Rean Griffith, et al. Above the clouds: a berkeley wiew of cloud computing.Communication Magazine, 2009

4 IBM 虚拟化与云计算小组. 虚拟化与云计算. 北京:电子工业出版社,2009

5 MichaelMiller 著. 姜进磊,孙瑞志,向勇等译. 云计算. 北京:机械工业出版社,2009

6 叶伟等. 互联网时代的软件革命—SaaS 架构设计. 北京:电子工业出版社,2009

7 刘黎明. 云计算—第三次 IT 产业变革,http://labs.chinamobile.com/mblog/74856_1794

8 尼古拉斯·卡尔. IT 不再重要. 北京:中信出版社,2008

9 李德毅. 云计算:从图灵计算到网络计算. 2009 云计算中国论坛,2009

10 范承工. 抢云市场先机, 迎产业洗牌, http://storage.it168.com/a2009/0526/577/ 000000577295. shtml,2009

11 陈全,邓倩妮.云计算及其关键技术.计算机应用, 2009(9)

12 叶伟等. 互联网时代的软件革命—SaaS 架构设计. 北京:电子工业出版社,2009

13 电信运营商将主导企业云计算市场,http://labs.chinamobile.com/mblog/57950_11090

14 中电信抢滩云计算在上海开建“信息银行”. http://www.ezcom.cn/Article/16813

15 中国电信推能力开放平台, http://www.cww.net.cn/news/html/2009/12/3/ 2009123 158512299.html

16 尹爱昊. 通过业务开放提升网络价值, http://www.cww.net.cn/tech/html/2009/6/25/20096 25134607610.html

17 张为民,唐剑峰,罗治国等.云计算深刻改变未来. 北京:科学出版社, 2009

18 王鹏.走近云计算. 北京:人民邮电出版社,2009

19 Peter Fingar,王灵俊. 云计算:21 世纪的商业平台. 北京:电子工业出版社, 2009

20 王鹏. 云计算的关键技术与应用实例. 北京:人民邮电出版社,2010

21 刘鹏. 云计算. 北京:电子工业出版社, 2010

22 王鹏,黄华峰,曹珂. 云计算:中国未来的 IT 战略. 北京:人民邮电出版社, 2010

Key Security Technologies on Cloud Computing

Zhang Yunyong, Chen Qingjin, Pan Songbai, Wei Jinwu

(China Unicom Research Institute, Beijing 100048, China)

Abstract Cloud computing is a new method sharing infrastructure which provides the usage of service, application, information and infrastructure composed of “resource pool” computing, network, information and storage. The features of cloud computing directly impact the security threats of its environment and relative security policies, which include the self-service on demand, broadband access, visualization resource pool, quick elastic architecture, measurable services and multi-tenant. Cloud computing could definitely introduce positive effect because it has multiple benefits from scale economy to application availability. Nowadays, more and more enterprise users are ready to be involved in the cloud circle with the support of cloud computing providers and advocates. However, cloud computing also brings some new security issues. The security problem is very important since a large number of users share the IT infrastructure. In this paper, the specific cloud computing security requirement and solution are analyzed. The current status of international and domestic research and products are presented.

Key words cloud computing, visualization, security, credibility

(收稿日期:2010-08-17)