云计算安全研究综述*

房　晶,吴　昊,白松林

(北京交通大学轨道交通控制与安全国家重点实验室　北京 100044)

摘 要　随着云计算的发展,云计算的安全问题越来越受到关注。本文将全面分析云计算中与安全有关的各类问题及其解决方案。文中首先介绍了云计算的体系架构,接着比较了云计算安全和传统安全的区别,重点介绍了云计算的安全技术,最后从云计算的标准组织和产品的角度阐述了现阶段云计算安全的重点研究领域和成果。

关键词　云计算;云计算安全;用户认证与授权;数据安全;虚拟化安全;安全组织

1　引言

在云计算环境中,用户不再拥有基础设施的硬件资源,软件都运行在云中,业务数据也存储在云中,因此云计算安全关系到云计算这种革命性的计算模式是否能够被业界接受。本文将对云计算所面临的诸多安全问题进行深入探讨。

2　云计算体系架构

业界许多大公司都投身云计算,推出了自己的云计算平台或服务,如 Google 的网络程序开发平台 Google App Engine、IBM 的“蓝云”计划、亚马逊的弹性计算云以及微软的基于云计算的操作系统 Windows Azure 平台等。各公司的云计算采用的技术和细节不尽相同,但采用的架构可以抽象为图 1[1]。云端用户通过管理系统和部署工具接入服务集群中,即云中,通过云完成海量计算和存储业务。

* 国家自然科学基金资助项目(No.60830001),轨道交通控制与安全国家重点实验室重点项目(No.RCS2008ZZ007)

3　传统安全和云计算安全的比较

从图 1 的云计算体系架构可以看出,云计算的运营和传统 IT 网络是不同的。由于云计算最初是在企业内部网络运行的,并不对外开放,在设计之初没有太多考虑安全性问题,从而导致了现在云计算安全的一系列问题。

首先,传统的 IT 系统是封闭的,存在于企业内部,对外暴露的只是网页服务器、邮件服务器等少数接口,因此只需要在出口设置防火墙、访问控制等安全措施,就可以解决大部分安全问题。但在云环境下,云暴露在公开的网络中,任何一个节点及它们的网络都可能受到攻击,因此安全模式需要从“拒敌于国门之外”改变为“全民皆兵,处处作战”。

其次,相对于传统的计算模式将信息保存在自己可控制的环境中,在云计算环境下,信息保存在云中,数据拥有和管理分离,怎样做好数据的隔离和保密将是一个很大的问题。

再次,在云环境下,用户的服务系统更新和升级大多数是由用户在远程执行的,而不是采取传统(在本地按版本更新)的方式,每一次升级都可能带来潜在的安全问题

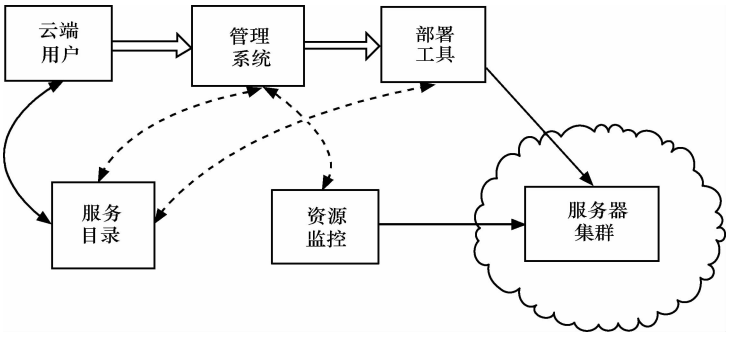

图 1　云计算体系结构框架

和对原有安全策略的挑战[2]。

另外,云计算环境相比之前的技术,大量运用虚拟化技术,怎样解决虚拟化方面的安全又是云计算安全与传统安全的又一重大区别。

除了技术方面,还有一个比较重大的问题,传统的安全技术已经出现多年,标准、法律、法规都相对成熟,而现在的云计算安全缺少标准,而且政策法规也不健全,再加上云计算自身的特点,数据可以存储在世界的任何一个角落,当出现问题时,国家政策的不同也是云计算安全的一个重大挑战。

4　云计算安全技术研究

在讨论云计算的安全问题前,需要先简单谈一下云计算对企业用户带来的安全益处。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用云的情况下,单位运营成本将会下降,单位安全运营的成本也会下降。安全运营包括网络监控、操作系统应用程序的补丁部署、软件和硬件系统配置的加固、权限管理等。就用户本身而言,云计算的一大好处就是在降低单位运营成本的同时,许多安全责任也随之转移到云计算供应商身上,不需要用户操心。从这个角度讲,云计算和近年来的企业外包模式相似。不过云计算供应商在高可靠性、安全性和冗余性上投入的成本更大。当然由于云计算独特的模式,它所产生的安全问题也是很多的,从上到下可以归结为如图 2 所示的几个方面的安全问题。从上到下依次采用用户认证与授权,数据隔离、加密及保护,网络隔离,灾备管理措施。由于云计算中多处用到虚拟化技术及其思想,故在其安全层次归结图中并没有列出,但下文会有介绍。

4.1　用户认证与授权

在一个典型的组织中,应用在组织的外围部署了信任边界,信任边界主要是静态的,并由 IT 部门监测和控制。在传统模型中,信任边界包括网络、系统和应用程序,这些托管在 IT 部门管理的私有数据中心中,并且通过 VPN、IDS、IPS 等进行网络安全控制。而在云计算中,组织的信任边界将变成动态的,并且超出 IT 的控制,而组织的网络、系统和应用的边界将进入服务提供商的域中。通常是一些大型服务提供商,它可能从事电子商务、提供链式管理、外包和团体及伙伴的协作等。这些失去的控制将挑战既定的信任治理和控制模型,如果管理不当会防止一个组织内采用云服务。为了弥补网络控制丢失且加强风险保证,解决身份和访问安全问题,需要采用身份认证与授权的安全手段。

用户认证与授权旨在授权合法用户进入系统和访问数据,同时保护这些资产免受非授权用户的访问。传统的认证技术有安全口令 S/K、令牌口令、数字签名、单点登录认证、资源认证等,可使用 Kerberos、DCE 和 Secureshell 等目前比较成熟的分布式安全技术。云计算的用户认证与授权措施需要具备如下的能力。

(1)身份管理:在用户身份生命周期中,有效管理用户身份和访问资源的权限是非常关键的。

· 用户生命周期管理,包括用户自注册、自管理和自动化的用户 ID 部署服务。

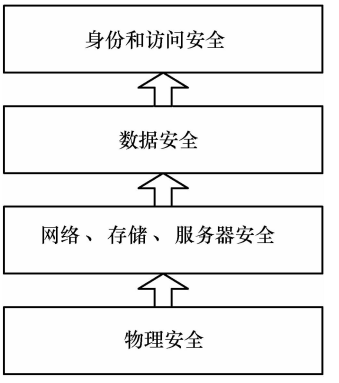

图 2　云计算安全层次归结

· 用户身份控制,包括访问和权限控制、单点登录和审计。

(2)访问授权:访问授权应该在用户生命周期内提供及时的访问,从而加强安全和保护 IT 资源。一般情况下,访问管理应该提供以下功能(在云系统中,可参考 Bel1.1aPadula 模型和 Biba 模型设计适用于云系统的访问机制)。

· 为多个服务和用户提供集中的访问控制,确保安全策略的执行是一致的。

· 根据 IT 需求和业务目标,提供基于策略的安全基础架构自动化。

· 在任意的 Web 服务应用系统间建立共享认证和属性信息的身份联邦。

(3)管理分布式环境下的用户,包括能够为用户配置一个或多个角色。

(4)多因素认证,通过 USBkey、用户指纹、用户口令等多种方式对用户身份进行认证,并进行多级精细化的授权。

(5)提供执行口令和个人信息变更的 Web 自助接口。

(6)基于 LDAP 的统一身份认证完成将分散的用户和权限资源进行统一、集中的管理,实现用户单点登录就可以访问多个系统。

现在已知的身份和访问安全解决方案有 3 种:欧洲隐私和身份管理、IE7 的 Windows CardSpace、OpenID。这里重点介绍一下 OpenID。OpenID 是一个分散的认证协议,可以帮助用户管理多个数字身份,更好地对分享他们的 PII (personally identifiable information)进行控制。一个用户必须记住一个用户名和密码——一个 OpenID,用这个登录到网络中,和可信第三方进行交换,指定一个特定的 OpenID 用于认证。而用户事先向 OpenID 供应商注册了一个 OpenID。它被称为“钓鱼天堂”,因为它对钓鱼攻击是敏感的。

4.2 数据安全

云计算的安全问题及其技术手段[3]见表 1。作为云计算的用户,关心的是自己数据的安全性,这包括数据的私密性、完整性和可用性等,主要体现在以下方面。

4.2.1 数据隔离

数据隔离是我们比较关心的一个问题。云计算的一个核心技术是虚拟化,这意味着不同用户的数据可能存放在一个共享的物理存储中。

云计算系统对于客户数据的存放可采用两种方式实现:提供统一共享的存储设备或者单独的存储设备。前者需要存储自身的安全措施,比如存储映射等功能可以确保数据的隔离性,它基于共享存储的方式,能够节约存储空间并且统一管理,可以节省管理相关的费用;而后者不但有存储自身的措施,而且从物理层面隔离保护了客户的重要数据,优点是能有效保护用户数据,缺点是存储无法有效利用。数据隔离如图 3 所示。

表 1 云计算的安全问题及其技术手段

安全性要求	对其他用户	对服务提供商
数据访问的权限控制	权限控制程序	权限控制程序
数据存储的私密性	存储隔离	存储加密、文件系统加固
数据运行时的私密性	虚拟机隔离、操作系统隔离	操作系统隔离
数据在网络上传输的私密及安全性	传输层加密,如 HTTPS、SSL、VPN 等网络隔离	网络加密
数据完整性	数据检验	
数据持久可用性	数据备份、数据镜像、分布式存储	
数据访问速度	高速网络、数据缓存、CDN	

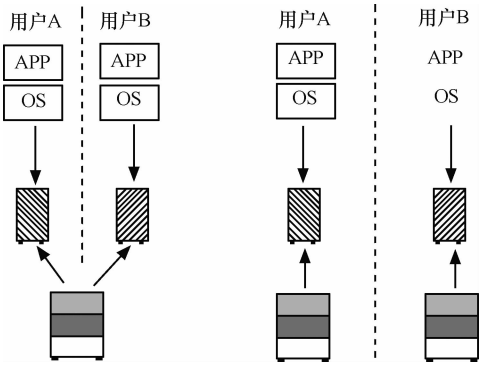

图 3 数据隔离

可以利用沙箱(Sandbox)隔离完成数据隔离。沙箱是一种程序的隔离运行机制,其目的是限制不可信进程的权限。沙箱技术经常被用于执行未经测试或不可信的客户程序。为了避免不可信程序可能破坏其他程序的运行,沙箱技术为不可信客户程序提供虚拟化的磁盘、内存以及网络资源,而这种虚拟化手段对客户程序是透明的。由于沙箱里的资源被虚拟化(或被间接化),所以沙箱里的不可信程序的恶意行为往往会被限制在沙箱中。

4.2.2 数据加密

数据加密的目的是防止他人拿到数据的原始文件后进行数据的窃取。在云计算环境中,数据的隔离机制可以防止其他用户对数据的访问,因此,数据加密的目的主要是防止“内鬼”,即避免服务提供者对数据进行窃取。数据

加密在云计算中的具体应用形式为:数据在用户侧使用密钥进行加密,然后上传至云计算环境中,使用时再实时解密,避免将解密后的数据存放在任何物理介质上。

数据加密有很多种成熟的算法,比如对称加密、公钥加密、iSCSI 加密等,这里不予赘述。

在云计算环境中,与数据加密配合使用的方法还有数据切分,就是把数据在客户端打散,经过加密后分散在几个不同的云服务上面, 这样对于任何一个服务提供商来说,都无法获取到完整的数据,即使通过暴力破解也无法取得数据内容。

4.2.3 数据保护

云计算平台的数据保护安全措施能对客户所有的数据和信息——结构化、非结构化和半结构化的数据,提供全面的保护功能。对存放于完全不同的存储格式中的数据进行发现、归类、保护和监控,并提供对关键的知识产权和敏感的企业信息的保护。

对于存储在云计算平台中的数据,可采取快照、备份和容灾等重要保护手段确保客户重要数据的安全,即便受到黑客、病毒等逻辑层面的攻击或者地震、火灾等物理层面的灾害,也都可以有效保护客户数据。

对于数据备份,可通过现有的企业级备份软件或者存储备份功能实现,可按照用户设定的备份策略对其文件和数据库进行自动备份及恢复,包括在线和离线备份。

4.2.4 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用户前得到完全清除,无论这些信息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用户前得到完全清除。SNIA(storage network industry association)标准组织有关于这方面的研究, 例如有学者提出要多次擦除,一般 7 次擦除数据就不能恢复, 从而不会造成数据泄漏,还有人提出仅对加密的密钥进行擦除,即使数据有残留也不能进行恢复等方法。

4.3 网络隔离

针对网络、存储和服务器安全问题,采用网络隔离技术。网络隔离提供数据传输的安全性,这种机制在网络银行、电子支付等金融领域已经运用得比较广泛。基础架构云可通过多张网络保证网络的安全性和隔离性。

(1)VLAN

主要用在数据中心内部,用于隔离不同的应用和客户程序,确保一个客户无法获取其他用户的网络数据,但是网络的管理员可以看到所有的网络数据。因此,这种方法只有隔离性,没有保证私密性。

(2)VPN

又称虚拟专用网络,是将多台分布的计算机用一个私有的经过加密的网络连接起来,形成一个私有的网络。采用这种方法可以彻底保证用户数据的传输安全,即使是云计算后台的网络管理员也无法窃取数据。

(3)HTTPS/SSL

这是一种常见的传输安全技术,主要用在浏览器和服务器之间的通信上,比较适合点对点的安全保障。

4.4 灾备管理

遇到机房失火、地震等极端情况造成的数据丢失和业务停止,云计算平台应该可以切换到其他备用站点以继续提供服务。

对于一个云计算服务的用户,可以选择多个云计算服务提供商,选择不同地点的数据中心提供服务,这样即使服务停止甚至服务提供商倒闭,用户也可以保留自己的数据,并继续运行自己的业务。

4.5 虚拟化安全

如图 4 所示,从云计算平台的角度来看,最基本的单元是虚拟机, 虚拟机安全是云计算平台安全的最基本要求。虚拟化安全是云计算需要考虑的特有安全威胁之一。虚拟化技术是将底层的硬件,包括服务器、存储与网络设备全面虚拟化,在虚拟化技术上,通过建立一个随需而选的资源共享、分配、管控平台,可根据上层数据和业务型态的不同需求,搭配出各种互相隔离的应用,形成一个服务导向的、可伸缩的 IT 基础架构,为用户提供出租 IT 基础设施资源形式的云计算服务。

虚拟化安全包括虚拟机间信息流控制、虚拟机监控、虚拟机可信平台、虚拟机隔离、虚拟网络接入控制等。综合起来可以归结为两个方面: 一个是虚拟化软件的安全;另一个是客户端或虚拟服务器的安全[4]。

(1)虚拟化软件安全

该软件层直接部署于裸机上,能够提供创建、运行和销毁虚拟服务器等功能, 如操作系统级虚拟化(Solaris

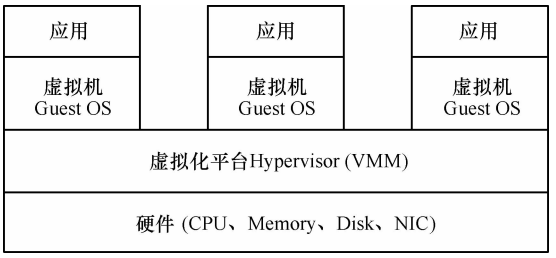

图 4　虚拟化角度的云计算平台

containers、BSD jails、Linux-VServer)、半虚拟化(硬件和 Xen、VMware 的结合) 或基于硬件的虚拟化(Xen、VMware、Microsoft Hyper-V)。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。在 IaaS 服务中,用户不能接入虚拟化软件层,该层由云服务提供商操作和管理。

(2)虚拟服务器的安全

虚拟服务器或客户端面临许多主机安全威胁,包括接入和管理主机的密钥被盗、攻击未打补丁、在脆弱的服务标准端口侦听、劫持未采取合适安全措施的账户等,需要采取以下措施。

- 选择具有 TPM(可信计算平台)安全模块的虚拟服务器。
- 安装时为每台虚拟服务器分配一个独立的硬盘分区,以便进行逻辑隔离。
- 每台虚拟服务器应通过 VLAN 和不同 IP 网段的方式进行逻辑隔离,对需要通信的虚拟服务器间通过 VPN 进行网络连接。
- 进行有计划的备份,包括完整、增量或差量备份方式。

5　云计算的安全组织及标准

(1)Cloud Security Alliance(云计算安全联盟,CSA)

CSA 是在 2009 年的 RSA 大会上宣布成立的,其成立的目的是为了在云计算环境下提供最佳的安全方案。CSA 确定了云计算安全的 15 个焦点领域, 并对每个领域给出了具体建议,15 个焦点领域分别是信息生命周期管理、政府和企业风险管理、法规和审计、普通立法、eDiscovery、加密和密钥管理、认证和访问管理、虚拟化、应用安全、便携性和互用性、数据中心、操作管理事故响应、通知和修复、传统安全影响(商业连续性、灾难恢复、物理安全)、体系结构[5]。目前,CSA 已经发布了两个版本的《云计算关键领域安全指南》,为云计算安全提供了重要的参考。

(2)Open Cloud Manifesto(开放云计算宣言)

"开放云计算宣言"已经正式发布,主要内容包括:什么是云计算和云计算的优势、云计算面临的挑战和障碍、开放云的目标和原则。其中,第一条原则就是,云计算提供者必须合作,确定能通过公开合作和适度采用标准,解决采用云计算可能遭遇的挑战,包括安全性、整合性、便携性、互通性、管理、测量与检测等方面。

(3)Distributed Management Task Force(分布式管理任务组,DMTF)

该组织的主要工作将集中在研究促进企业内私有云和其他私有云、公共云和混合云的操作性的方法通过开放云资源管理标准提高平台间的互操作性。2010 年 7 月,该组织下的云计算工作组 CMWG 起草了开放云标准孵化器(OCSI)、开发云资源管理协议、封包格式和安全管理协议,发布了云互操作性和管理云架构的白皮书。

(4)Common Assurance Metric-beyond the cloud(CAM 项目)

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。

另外, 云计算中与安全管理相关的标准是 ITIL (information technology infrastructure library)和 ISO/IEC27001 和 ISO/IEC27002。

6　云计算安全公司及其产品

(1)趋势科技推出云安全 3.0 应对云计算的 3 大威胁

2010 年 7 月 22 日,趋势科技推出基于趋势科技云安全技术核心的全新云安全 3.0 解决方案,成为全球保护云计算安全的首家网络安全厂商。从借助云实现更高等级的安全,到保护云自身的安全,趋势科技云安全 3.0 为云环境下企业至关重要的信息平台与数据资产两个核心要素提供安全防护:一方面用"云的防护盾"技术保障云平台本身的高可用性,使得各种企业数据中心、应用系统或者云环境免受病毒、攻击、系统漏洞等威胁侵害;另一方面,通过"云中保险箱"技术保护用户存放于云端的隐私和关键数据不被非法窃取和利用。

(2)Altor Networks 虚拟化产品

Altor Networks 公司于 2007 年成立, 主要专注虚拟安全领域。2008 年,Altor 使用 VMware 的应用程序接口(API)来开发虚拟安全分析器, 以检测虚拟交换机流量——在虚

拟层上的网络层流量。该公司还开发了虚拟网络防火墙,该防火墙基于虚拟机管理器,可认证有状态的虚拟防火墙检查所有通过虚拟机的包,组织所有未经批准的连接和允许数据包进行更深层次的检查,该防火墙还能监控虚拟机间的网络流量。现在该公司已经被 Juniper Networks 收购。

(3)McAfee 公司

McAfee 公司发布了一个基于云的电子邮件网关 McAfee SaaS Email Security & Archiving Suite,能完成实时监控和分析传入的邮件流量,同时可以隐藏关键的邮件传输网关。

(4)Panda Security 公司

Panda Security 提供基于云的反恶意软件的服务,发布了熊猫云反病毒和熊猫云保护。其中,熊猫云保护依赖于 Panda Collective Intelligence(综合智能)技术,为中小型企业提供完全托管的安全服务,并且提供了终端和电子邮件离线保护的功能。

(5)Kaavo 公司

该公司的代表产品是基础设施及中间件按需软件(IMOD),Kaavo 解决了管理和保护云上应用数据这两个难点。他们的目标是为云提供一种一键式简单的自助界面,同时使其具有传输安全、基于角色访问控制、自动系统监控等功能,以及以应用为中心,可让系统在线部署的配置能力。另外,Kaavo 支持亚马逊 EC2、Eucalyptus、IBM 和 Rackspace 云。

(6)Navajo System 公司

该公司的代表产品是虚拟专用 SaaS(VPS),数据存放时加密,返回用户时自动解密,而且密钥由用户自己控制,这样使得数据库和身份盗窃变得无用,而且即使数据被偷走也难以辨认。对许多企业来说,隐私和管理上的担忧是公共云服务部署的一个阻碍。Navajo 试图用他们独创的 SaaS 应用数据安全解决方案改变这一现状。

7 结束语

随着云计算技术的快速发展和更广泛应用,云计算将会面临更多的安全风险。虽然有几个标准组织在研究云计算安全,但是目前业界对云计算安全的解决并没有统一的标准和解决方法。不少公司推出云计算安全的产品,但是创新力度明显不够,而且通常只能解决一小方面的问题。云计算安全的研究目前大多数是存在于企业,要解决云计算安全的诸多问题,少不了学术界的参与,未来需要企业和学术界共同解决云计算的安全问题,推动云计算的发展。

参考文献

1 王鹏.走进云计算.北京:人民邮电出版社,2009

2 《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

3 朱近之.智慧的云计算.北京:电子工业出版社,2010

4 Tim M,Subra K,Shahed L. Cloud security and privacy. USA:O'Reilly & Associates,2009

5 Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v2.1,http://cloudsecurityalliance.org/csaguide.pdf

[作者简介] 房晶,北京交通大学硕士研究生,主要研究方向为云计算安全;吴昊,副教授,主要研究方向为无线宽带通信、移动通信、扩频通信;白松林,北京交通大学硕士研究生,主要研究方向为存储安全。

Review of Cloud Computing Security

Fang Jing, Wu Hao, Bai Songlin

(State Key Laboratory of Rail Traffic Control and Safety of Beijing Jiaotong University, Beijing 100044, China)

Abstract With the development of cloud computing, the security issues of cloud computing are being more and more focused. In this paper, some types of security-related problems and their solutions of cloud computing are being comprehensively analyzed. Firstly, this paper describes the architecture of cloud computing and then compares the difference of cloud computing security and the traditional security, focusing on the technology of cloud computing security, and finally elaborate the key research areas and results of current cloud computing security from the perspective of cloud computing standard organizations and products.

Key words cloud computing, cloud computing security, user authentication and authorization, data security, virtualization security, safety organization

(收稿日期:2011-02-18)