第26卷 第8期 重庆理工大学学报(自然科学) 2012年8月
Vol. 26 No. 8 Journal of Chongqing University of Technology(Natural Science) Aug. 2012

基于云计算的网络安全威胁及防范

黄志宏,巫莉莉,张 波

(华南农业大学 现代教育技术中心,广州 510642)

摘 要:介绍了云计算的概念和体系结构,讨论了目前云计算面临的安全问题。通过对云安全策略和网络安全策略的研究与分析,从云端、用户端及云端和用户端互动3方面入手,设计了一个安全云计算框架,期望对云计算安全防范提供一定的参考。

关 键 词:云计算;安全策略;安全框架

中图分类号:TP393 **文献标识码**:A **文章编号**:1674-8425(2012)08-0085-06

Network Security Threats and Prevention on Cloud Computing

HUANG Zhi-hong, WU Li-li, ZHANG Bo

(Modern Education Technology Center, South China Agriculture University, Guangzhou 510642, China)

Abstract: Applications of the cloud computing are changing the way of people's work, study and life, creating a more advanced information society. The security issues accompanied by the cloud computing increasingly become the focus of people's attention. This paper focused on the network security issues on cloud computing, and through the research and analysis of the cloud security policy and network security policy designed a framework for securing cloud computing, having a certain reference value on cloud computing security.

Key words: cloud computing; security policy; security framework

云计算作为一种全新的技术带来了商业模式和工作方式的改变,给人们的工作、学习和生活提供了便利。云计算中用户数据都被存放在"云端",数据的丢失和隐私的泄露都将给用户带来重大损失,这使人们对其安全问题越来越关注。

目前,许多国际知名的IT公司,如Google、Amazon、IBM、Microsoft、Sun等都建立和提供各种云计算服务。按美国国家标准与技术研究院(NIST)的定义,云计算被划分为SPI(SaaS、PaaS、IaaS)的3层体系:① 软件即服务(SaaS),如NetSuite公司的NetSuite OneWorld(在线ERP);② 平台即服务(PaaS),如Google的Google App Engine和Microsoft的Azure Services Platform等;③ 基础设施即服务(IaaS),如Amazon的弹性计算云(EC2)和IBM的蓝云(Blue Cloud)等。2008年6月,美国知名市场研究公司Gartner在其发布的一份名为《Assessing the Security Risks of Cloud Computing》的研究报告中指出:云计算产业具有巨大市场增长前景,但是相对于其他安全产品,云计算在数据完整性、数据恢复和私密性等存在访问风

收稿日期:2012-04-25
作者简介:黄志宏(1981—),男,江苏连云港人,硕士,实验师,主要从事网络信息安全研究。

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

险，而在电子服务发现、业务兼容性和第三方审计等方面存在法律法规方面的安全评估风险[1]。在云计算的发展过程中，Google、Amazon 和微软都发生过安全事故。

本文针对云计算面临的网络安全威胁及发生过的安全事故，通过对云计算服务提供商的安全策略进行分析，将一些传统的安全防护技术引入到云计算中，构建一个安全云计算框架，为云计算安全防范提供一定的参考。

1 云计算

1.1 云计算概念

云计算(cloud computing)是网格计算(grid computing)、分布式计算(distributed computing)、并行计算(parallel computing)、效用计算(utility computing)、网络存储(network storage technologies)、虚拟化(virtualization)、负载均衡(load balance)等传统计算机技术和网络技术发展融合的产物。它旨在通过网络把多个成本相对较低的计算实体整合成一个具有强大计算能力的完美系统，并借助 SaaS、PaaS、IaaS、MSP 等先进的商业模式把这强大的计算能力分布到终端用户手中。

1.2 云计算技术体系结构

云计算技术体系结构分为 4 层：物理资源层、资源池层、管理中间件层和 SOA 构建层，如图 1 所示。物理资源层包括计算机、存储器、网络设施、数据库和软件等；资源池层是将大量相同类型的资源构成同构或接近同构的资源池，如计算资源池、数据资源池等；管理中间件负责对云计算的资源进行管理，并对众多应用任务进行调度，使资源能高效、安全地为应用提供服务；SOA 构建层将云计算能力封装成标准的 Web Services 服务，并纳入到 SOA 体系进行管理和使用，包括服务注册、查找、访问和构建服务工作流等。管理中间件和资源池层分别对应云计算 3 层服务体系中的 PaaS 层和 IaaS 层，它们是云计算技术的最关键部分。SOA 构建层则对应 SaaS 层，它的功能更多依靠外部设施提供[2]。

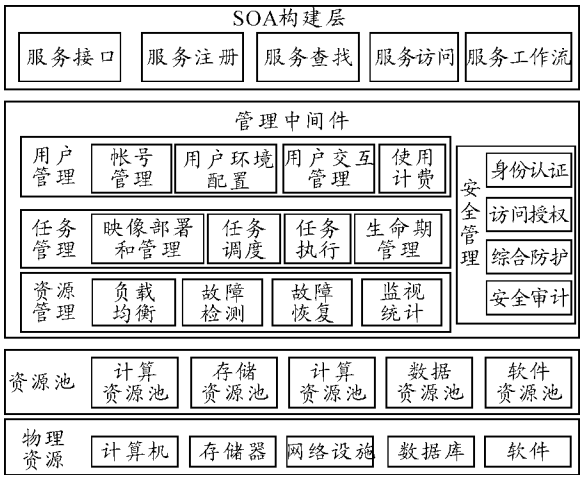

图 1 云计算技术体系结构

2 云计算面临的威胁

云计算的快速发展虽然为人们提供低成本和灵活性，但不同用户通过云服务商提供的服务访问同一个应用，将数据都存放在云端，这种集中化的管理将成为黑客攻击的重点目标，系统的巨大规模以及前所未有的开放性与复杂性，使用户面临重大的安全风险，云端的用户数据和隐私很容易泄露。IDC 公司在其 2008 年 8 月的一份调查报告中指出，云计算面临的最大挑战就是安全问题[3]。

2010 年 3 月云计算安全联盟(CSA)发布的一份由惠普承保的云计算的主要威胁 1.0 版的报告中，确定了云计算目前存在七大安全威胁[4]：

① 网络入侵，运行蠕虫病毒网络。

② 云计算供应商提供的服务和应用程序接口(API)无法得到安全保障，传输数据受到威胁。

③ 云计算供应商内部特权管理员存在监管漏洞。

④ 资源共享带来风险。由于很多虚拟服务器共享相同的配置，简单的错误配置可能造成严重的后果。

⑤ 存在数据丢失和泄漏的风险。云计算供应商是否有能力对数据进行快速恢复。

⑥ 帐户或服务劫持，即黑客通过冒用云计算供应商提供给客户的帐户，盗取该客户的信息并

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

与恶意方共享。

⑦ 模糊而不可知的威胁。云计算供应商只强调迁移至云计算后所带给企业的利益而不澄清其面临的风险。许多大公司都发生过安全事故[5]，Amazon 公司 2008 年 7 月在线计算服务的主要组件简单存储服务发生故障，导致系统宕机超过 6 h，一些网站受到影响；2009 年 12 月，亚马逊基于云计算的 EC2 服务在一个星期里发生了僵尸网络引起的内部服务故障和数据中心电源故障；Google 公司 2009 年 9 月 Gmail 服务先后发生 2 起宕机事件，导致邮件系统无法访问；2010 年 2 月 25 日，由于一个备份数据中心发生故障，导致 GoogleAppEngine 宕机，对很多谷歌客户造成影响；2009 年 10 月微软云计算服务器故障导致用户数据丢失，连同备份服务器上的用户数据也丢失了。

随着云计算的快速发展，其所面临的威胁可能会不断扩展和变化，也加深了人们对云计算安全的担忧。加强云计算的安全建设，提高安全性能，已成为云计算快速健康发展过程中不容忽视的问题。

3 云计算安全策略

当前，云计算面临的安全问题主要有数据丢失和泄漏，帐户、服务和通信劫持，共享技术漏洞，不安全的应用程序接口，云计算管理漏洞等。针对这些安全问题可以从技术防护、运营管理、法规保障[6] 3 方面入手进行防范。

3.1 技术防护

从技术层面来看，可通过安全认证、数据加密、安全传输、权限控制[7] 等手段对云进行防护。

1）安全认证。可通过使用各种强认证实现，例如一次性密码、生物识别、数字证书和 Kerberos。

2）数据加密。云计算中用户数据都被存放在“云端”，数据的丢失和隐私的泄露都将给用户带来重大损失，因此，无论是用户还是云计算服务的提供商都应该对云端数据进行加密处理。经成熟的数据加密技术（DES、RSA 或混合加密）处理后的数据，既增强了隐私性又起到被隔离的作用。

3）安全传输。数据在网络传输过程中使用 SSL、PPTP、IPSec 或 VPN 等不同的传输方式，确保数据传输的安全性和保密性。

4）权限控制。结合本地认证、USB-Key 验证以及 LDAP、Radius、POP3、Proxy 等第三方认证方式，基于角色访问控制技术 RBAC（role based access control），对云服务提供商的管理人员及客户端用户进行分级管理，通过设置不同角色并授予各种角色不同的管理和访问权限来实现权限控制。

3.2 运营管理

从运营管理方面来看，云服务商除了从合同角度对安全性进行自我约束，还可引入第三方认证，通过建立完善的企业信誉以及合约约束等手段来对自己进行约束。

从合同的角度对安全性进行约束是客户所希望的，目前已经有许多云计算服务商提出了自己的云服务水平协议，这些协议从服务质量、技术支持和知识产权等方面对服务进行了规范，也明确了服务提供者与使用者的权利和义务。而企业对自身信誉的看重，更能赢得客户的尊重。从客户角度讲，选择有实力、有信誉的服务提供商将是云计算用户的首要选择。

第三方认证是提升信任关系的有效手段，可以通过一个中立机构对信任双方进行约束。该机构可以对云服务提供商的服务进行安全认证，采用标准化的技术手段和非技术手段对服务进行检测，找出安全漏洞，对其安全级别进行评价，这样可以从第三方角度对服务的安全水平进行评比定位，为客户提供参考。IBM 大中华区云计算中心总经理朱近之表示：技术不是万能的，特别针对安全领域；用户并不是安全领域的专家，也无法判断一个云服务在技术上是否真正能够安全可靠。为此，可以采用第三方认证、建立完善的企业信誉以及采用合约约束等手段来约束服务商。

3.3 法规保障

国家应制定统一的技术标准规范和相关的法律法规，云服务提供商和用户都应承担相应的法律责任，建立互信关系。运营商在保护自己的同

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

时也需确保用户服务安全可信，数据隐私不被泄露，数据不会丢失，帮助用户规避安全风险。

4 安全云计算框架

本文针对云计算当前面临的风险和威胁，通过对云安全策略及传统网络安全策略的研究与分析，从云端、用户端及云端和用户端互动三方面入手，设计了一套安全云计算框架，如图2所示。

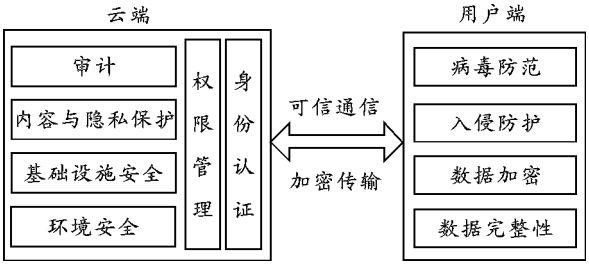

图2 安全云计算框架

4.1 云端

云端从环境安全、基础设施安全、身份认证与权限管理、内容与隐私保护(数据分类、数据保护、数据加密、数据流向)以及审计等方面入手，结合现有的各种安全技术设计了一套安全防护措施。

1) 环境安全。在云计算系统中，对于存放各种硬件设备的机房，要制定统一规范的建设标准，机房要避开各种高危(地震、磁场、闪电、火灾等)区域，安装大量的支撑设备(UPS、备用服务器等)，并安装具备相应的预报、告警、自动排除危害机制的监控系统。为防止电磁泄漏，系统内部设备应采用屏蔽、抗干扰等技术，当系统遭到危害时，能实施完善的容错措施和单点故障修复措施[8]。

2) 基础设施安全。为提高云计算系统的可靠性和可用性，需要对服务器、存储设备以及操作系统等基础设施做好安全防护工作。

① 服务器：使用电源冗余、静电防护、防电磁、短路和断路技术对用电环境进行保护；使用集群等虚拟化技术，将多台物理服务器虚拟成一台大型的逻辑服务器，可提高服务器的可用性、可扩展性、可维护性，并快速实现单点故障的恢复。

② 存储设备：使用电源冗余、静电防护、防电磁、短路和断路技术对用电环境进行保护；使用虚拟技术，将不同品牌的存储设备进行统一管理，资源进行统一调配、动态扩展；使用快照、远程镜像等技术完成存储的本地复制和异地容灾工作。

③ 操作系统：操作系统漏洞和企业自行开发的应用漏洞成为黑客重要的攻击目标。对于操作系统漏洞，随着操作系统厂商不断地提升安全性以及安全防御技术的进步，只要及时下载和安装补丁就可降低风险；对于应用漏洞，企业可以通过应用漏洞查核与分析工具、入侵检测系统、应用防火墙及安全事件审计系统进行侦测与拦阻，就可将风险降至最低。

3) 身份认证与权限管理。身份认证与权限管理是云计算面临的重大挑战。云平台存放着用户海量数据，制定良好的身份和访问管理策略，能有效保护用户隐私，减少用户损失。

① 身份认证：可通过使用一次性密码、生物识别、数字证书和 Kerberos 等各种强认证实现。例如基于用户生物信息特征的模式识别验证，用户先到云端注册，申请可信云证书，并进行注册人脸、语音等模式识别验证，注册完毕后，通过安装在本地计算机上的客户端软件绑定的计算机摄像头、话筒等生物信息特征采集装置进行人脸或语音等身份识别认证，极大地提高了用户身份认证的安全性和可靠性。

② 权限管理：一般使用基于角色访问控制技术 RBAC(role based access control)。通过设置不同角色并授予各种角色不同的管理和访问权限，实现对系统用户的分级管理。

4) 内容与隐私保护。在云计算环境中，云平台承载着大量数据的处理与储存，数据的丢失和隐私的泄露都将给用户带来重大损失。本框架基于以下几种机制实现对内容与隐私的保护：

① 数据分类：将不同类别的数据分配给 FC 或 SATA 等不同类型的存储介质，降低存储成本；根据数据所需的保护级别、性能要求、使用频率及其他的考虑因素进行分类，降低管理难度，提高运作效率和数据安全性；云服务商需提供根据预定

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

义策略自动管理迁移过程的软件，持续地将数据分配给特定介质媒体。

② 数据保护：通过布署数据防泄漏（data loss prevention，DLP）工具，不仅可以有效防止信息通过用户端外泄，而且可以确保云端敏感数据均有适当的权限管控，并通过对数据内容的管控，防止云平台运维人员无心或有意的外泄行为，降低风险。

③ 数据加密：通过 DES、RSA 等加密技术对数据进行加密处理，既可以防止云平台运维人员“监守自盗”行为，解决云端数据隔离问题，也可以防止终端设备丢失后信息发生外泄。

④ 数据流向：通过布署自动化的数据流向监控与追踪系统可及时掌握云端数据流向，记录数据操作日志。

5）审计。云审计与传统的安全审计在应用环境、解决的问题、运作模式和技术架构上都存在很大的差异。传统的安全审计是一款独立的产品，并只能面向唯一的用户执行固定的功能（信息安全审计），用户要购买整个产品才能使用。云审计则是一种服务，实现对 IaaS、PaaS 和 SaaS 各个层面的审计，解决云计算用户可信的问题[9]。由国都兴业提出的“全云审计”策略，通过在云计算环境中引入 IT 审计的理念，借助云审计有效降低了云计算面临的数据被未知的超级用户访问、数据合规性检查、数据存储位置未知、数据没有被真正隔离、数据无法恢复、司法调查困难、数据是否长期可用等风险[10]。

4.2 用户端

随着企业不断强化云端数据中心的防护能力，黑客则将攻击转向用户端，他们通常采用高持续性威胁（advanced persistent threat，APT）手法对用户端进行目标性攻击，长期埋伏于企业终端，获取企业内部敏感数据，并将终端作为攻入云端数据中心的最佳跳板。本框架的用户端从终端设备的病毒防范、入侵防护、数据加密及数据完整性验证等方面入手，结合现有的安全技术设计了一套安全防护措施。

1）病毒防范。黑客通常利用网络或者系统漏洞将木马病毒、脚本病毒、系统病毒、蠕虫病毒等各种病毒植入用户终端，针对这些病毒攻击，可以采取以下防护措施：

① 及时下载和安装系统安全漏洞补丁，避免黑客利用系统漏洞传播病毒。

② 安装具有防火墙功能的杀毒软件，及时更新杀毒软件，开启实时监控功能，每天升级病毒库，定时对系统进行病毒查杀。

③ 养成良好习惯，增强自我保护意识，不要随便打开来历不明的文件和不安全的陌生网站。

④ 定期将应用软件升级到最新版本。

⑤ 定期将重要资料进行备份和加密处理。

2）入侵防护 。为了降低终端被黑客入侵的风险，企业除了在云、端之间布署入侵检测系统、安装防火墙以外，用户还需增强自身防范意识，及时下载和安装系统安全漏洞补丁，定期升级病毒库并查杀病毒，养成良好的上网习惯。此外，用户可定期用 DOS 命令 netstat - a 或者 SuperScan 等软件对客户机开放的端口进行检测，若发现未知端口有异常连接建立或者正在监听，特别是高端端口，应立即断开网络，用检测木马的软件如 Trojan Remover 等进行检测。用进程检测软件如 360 安全卫士等监测客户机所开的进程，并和以往的进程列表作比较，留意不明进程，关闭不必要的服务。

3）数据加密。在云计算环境中，随着操作系统安全性和企业应用防护能力的提高，黑客将攻击目标转而指向用户终端。大量移动终端的出现，虽然增加了终端多样性和提高了用户自由度，但同时也增加了隐私防泄漏的难度。通过 DES、RSA 等加密技术对数据进行加密处理，即使终端被攻破或者丢失，也可有效降低隐私外泄风险。

4）数据完整性验证。由于大规模数据所导致的巨大通信代价，用户不可能将数据下载后再验证其正确性。因此，云用户需在取回很少数据的情况下，通过某种知识证明协议或概率分析手段，以高置信概率判断远端数据是否完整。典型的工作包括：面向用户单独验证的数据可检索性证明（POR）方法、公开可验证的数据持有证明

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

(PDP)方法。NEC 实验室提出的 PDI(provable data integrity)方法改进并提高了 POR 方法的处理速度以及验证对象规模,且能支持公开验证。其他典型的验证技术包括:Yun 等提出的基于新的树形结构 MAC Tree 的方案;Schwarz 等提出的基于代数签名的方法;Wang 等提出的基于 BLS 同态签名和 RS 纠错码的方法等[11]。

4.3 云端和用户端互动

为了防止云端与用户端的互动通信被第三者恶意劫持破解,通过 SSL 原理建立可信云端和用户端互动安全通道。基于可信密码学技术,通过利用加密、信息完整性校验、数字签名、身份认证交换、流量填充、路由控制、第三方公证及访问控制等安全防范机制对云、端交互数据的机密性、完整性和可用性进行防护[12]:

① 加密:即将明文信息进行隐藏,使其具有机密性。

② 信息完整性:即使用 Hash 函数对传递的信息附加一个摘要值。接收方接收到信息和摘要值后,再从接收的信息中创建一个新的 Hash 值,并将新创建的值和原来的 Hash 值进行比较。2 个值相同,则说明信息的完整性被保全。

③ 数字签名:即发送报文时,发送方用一个 Hash 函数从报文文本中生成报文摘要,然后用自己的私钥对这个摘要进行加密,这个加密后的摘要将作为报文的数字签名和报文一起发送给接收方,接收方首先用与发送方一样的 Hash 函数从接收到的原始报文中计算出报文摘要,接着再用发送方的公钥来对报文附加的数字签名进行解密,如果这 2 个摘要相同、那么接收方就能确认该数字签名是发送方的,并证明报文确实是发送方发送的。

④ 身份认证交换:即云端和用户端通过交换信息来相互证明身份。

⑤ 流量填充:即在数据流中插入一些虚假信息,从而阻止黑客进行流量分析。

⑥ 路由控制:即在数据交换双方之间改变有效路由,避免黑客在特定的路由上偷听。

⑦ 第三方公证:即选择一个双方都依赖的第三方,控制双方的通信,避免否认。

⑧ 访问控制:即通过使用密码和 PIN 等方法证明用户具有访问该信息或系统资源所拥有的权利。

5 结束语

云计算的发展前景是美好的,它的快速发展给人们的学习、工作和生活带来了便利,但同时云计算也存在大量的技术、管理与法律风险,对风险的防范措施需要不断加强。本文从技术层面设计了一个安全云计算框架,可为用户规避大量的技术风险,而法律与管理风险的防范还需要得到从国家到公司运营层面上法律法规的支持和保证。

参考文献:

[1] 郭乐深,张乃靖,尚晋刚. 云计算环境安全框架[J]. 信息网络安全,2009(7):62-64.

[2] 刘鹏. 云计算技术原理[EB/OL]. [2010-09-09]. http://www.chinacloud.cn/show.aspx?id=1929&cid=12.

[3] Dan Yachin. Cloud Computing - It Is Time For Stormy Weather[Z]. USA: [s.n.],2010.

[4] 云计算安全联盟. Top Threats to Cloud Computing V1.0[Z]. USA: [s.n.],2010.

[5] 焦迎春. 试论云计算环境下的安全建设[J]. 黑龙江科技信息,2011(3):81.

[6] 沈昌祥. 云计算安全[J]. 信息安全与通信保密,2010(12):12-15.

[7] 党卫红. 云计算的安全防护策略分析与研究[J]. 读与写杂志,2010(5):79.

[8] 薛凯,刘朝,杨树国. 云计算安全框架的研究[J]. 电脑与电信,2010(4):28-29,32.

[9] 佚名. 解析云审计与传统安全审计的区别[EB/OL]. [2011-10-24]. http://www.topoint.com.cn/html/article/2011/11/321746.html.

[10] it168. "全云审计"有效控制数据在云里面临风险[EB/OL]. [2011-10-24]. http://cio.itxinwen.com/informationize/2011/0118/219015_2.html.

[11] 冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报,2011(1):71-83.

[12] 李虹,李昊. 可信云安全的关键技术与实现[M]. 北京:人民邮电出版社,2010:331-335.

(责任编辑 刘 舸)

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net