

Security Analysis and Discussion of Cloud Computing

LIU Zhi-fang¹, ZHANG Xue-hong²

1. Information Technology Center, Tangshan Normal University, Tangshan, China

2. Department of Computer Science, Tangshan Normal University, Tangshan, China

E-mail: 1. lzf@tstc.edu.cn, 2. zxh@tstc.edu.cn

Abstract: Cloud computing is a new term, but has become a hot issue now, which is grid computing、distributed computing、parallel computing、utility computing、Network Storage Technologies、virtualization、load balancing, and other traditional computer technology and network technology integration products. Through the network to multiple computing entities into one powerful computing capability of the perfect system, and the distribution of computing power to provide a different end-user, enjoy on-demand "cloud" of the powerful computing capabilities. Cloud computing is a service-oriented architecture, cloud computing security issues is an important issue in its development. The paper first gives the definition of cloud computing, Described the characteristics of cloud computing; for cloud computing security risks and security needs was also discussed. Then, according to the architecture of cloud computing has security problems faced by each layer, made the appropriate security mechanisms.

Keywords: Cloud computing; Architecture; Security model; Information security

云计算的安全问题分析与探讨

刘志芳¹, 张学红²

1. 唐山师范学院信息技术中心, 唐山, 中国, 063000

2. 唐山师范学院计算机科学系, 唐山, 中国, 063000

E-mail: 1. lzf@tstc.edu.cn, 2. zxh@tstc.edu.cn

【摘要】云计算是个新兴的名词,但已成为当今一个热点问题,是网络计算、分布式计算、并行计算、效用计算、网络存储、虚拟化、负载均衡等传统计算机技术和网络技术发展融合的产物。通过网络把多个计算实体整合成一个具有强大计算能力的系统,并把强大的计算能力分布提供个各终端用户,按需享受“云”的强大计算处理能力。云计算是一种面向服务的体系架构,在云计算中安全问题是其发展中的一个重要问题。文中首先对给出云计算的定义,对云计算的特征进行了阐述;针对云计算的安全风险和安全需求做了探讨。接着,根据云计算的体系架构分析了各层所面临的安全问题,提出了相应的安全机制。

【关键词】云计算; 体系架构; 安全模型; 信息安全

1. 引言

IBM 公司于 2007 年底宣布了云计算计划以来,“云计算”、“云安全”迅速成为当今 IT 界最热门得话题,国内外各大研究机构和厂商都相继发布了云计划,推出了与其相关的安全产品。“云”落大地,标志着 IT 行业步入“云时代”。那么“云”是什么?我们要怎样面对“云”呢?

2. 关于云计算

2.1 云计算定义

IBM 的技术白皮书“Cloud Computing”中对云计算的定义^[1]:“云计算一词用来同时描述一个系统平台或者一种类型的应用程序,一个云计算的平台按需进行动态地部署、配置、重新配置以及取消服务等。

云计算是一个新兴的商业计算模型,它把计算作为一种服务,利用高速互联网的传输能力,将数据的处理过程从单个终端移到网络上的计算机集群中。集群中的计算机都是很普通的工业标准服务器,他们由一个大型的数据处理中心统一管理,数据中心按客户的需求分配计算资源,达到与超级计算机同样的效果。

“云”，一方面是对那些网状分布的计算机的比喻，另一方面也描述了数据的计算过程被隐匿起来，由服务器按你的需要，从大云中“雕刻”出你所需要的那一朵。在这个过程中，用户不必知道具体的实现技术，只要购买相应的服务就可以像电能一样使用。

2.2 云计算的特点^[2]

首先云计算是分布式模式，物理节点和服务都是分布在“云”中，构成云计算的大规模特征，另外在“云”中存储着海量的数据和无数的软件和服务应用，他们构筑于各种标准和协议之上。

第二是虚拟化，这是云计算最强调的特点。每一个应用部署的环境和物理平台是没有关系的。云计算把各层次功能封装为抽象实体，对用户提各层次的云服务，达到对应用进行扩展、进行迁移、进行备份。这些服务通过虚拟化技术通过虚拟平台进行管理和实现。

第三是动态可扩展。可以随时往“云”中添加计算机，网络中任何一台机器都可以按需要更换和升级。对用户和服务来说也可以随时扩展，这就意味着，“云”几乎就像生物一样能长生不老，具有无限的生机。

3. 云计算基本模型

在图 1 中的基本模型中^[3]，用户通过用户接口从云计算服务目录中选择一项自己需要的服务，请求被送给系统管理单元，并查找提高服务所需要的资源，然后调用 Provisioning Tool 从“云”中提取出所需的资源，雕刻出一朵特定的“云朵”来提供服务^[4]。其中 Monitoring and metering 为可选单元，监视“云”的使用情况，保存资源与特定用户的归属关系，Servers “云”里面是由服务器互连构成的大网，由系统管理工具进行管理，可进行并行计算，通过虚拟技术实现最大化资源的利用并提供服务给用户。

4. 云计算安全机制

4.1 云计算面临的安全问题

美国 Gartner 公司 2008 年发布了一份《云计算安全风险评估》研究报告^[5]，列举了云计算服务存在的七大潜在安全风险，即特权用户的接入、可审查性、数据位置、数据隔离、数据恢复、调查支持和长期生存性。针对《云计算安全风险评估》中提出的七大风险，可得出云计算用户的安全需求^[6]：

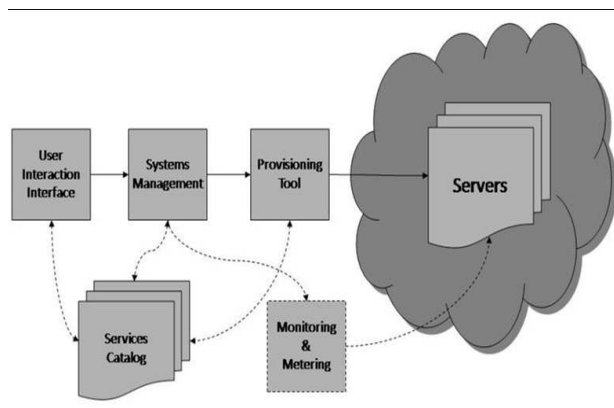


Figure 1. Cloud computing basic model

图 1. 云计算基本模型

1) 特权用户的接入：

需要在公司外部处理信息时因缺少内部的各种安全控制措施，会给数据带来安全风险，这样就需要了解云计算服务商提供和监管，享有特权的管理员方面的具体信息，以及控制数据访问方面的具体信息。

2) 可审查性：

在“云”中用户对自己数据的完整性和安全性负有最终责任，在传统模式下服务提供商需要通过外部审计和安全认证。但在云计算模式下，一些提供商却拒绝接受这样的审查，素以用户需要了解云计算服务商是否愿意并且有能力做到遵从相关法律法规。

3) 数据位置：

用户在使用云计算服务时，并不清楚自己的数据储存在什么地方，是否存储在一些专门管辖的特殊位置，不清楚服务商是否遵循了当地的隐私协议，所以应要求云计算服务商给出合同承诺，并遵守当地相关数据管理法律法规，能够提供数据存储地点信息的查询服务。

4) 数据隔离：

在云计算的体系中，所有用户的数据都共享在“云”中，一般情况下我们可以通过加密的方式来保障数据的安全，但显然不能满足对数据的高安全要求，那么用户应当了解云中的加密服务是否是由专家设计，并通过了安全测试，如果加密系统失效的话，计算提供商是否可以将数据作相应的隔离处理，能否按照不同数据提供隔离存储服务和数据加密失效锁定服务。

5) 数据恢复：

虽然用户不知道数据存储的具体位置，云计算提供商也应有义务告知用户在发生灾难时，用户的数据

和服务将会面临怎样的问题，那些任何没有经过备份的数据和应用程序都将可能丢失和瘫痪，用户需要了解服务提供商是否有能力快速恢复数据，以及需要多长时间，能否对数据进行全面恢复。

6) 调查支持:

在云计算环境下，和传统模式下的那些调查不恰当的应用或是非法的活动将难以实现。在云计算环境下，用户的数据可能会存放在一起或者数据共享，而且有可能会在多个数据中心之间转移。如果服务提供商没有这方面监管措施，那么在有违法行为发生时，将难以进行调查取证。这就需要云计算服务商以合同承诺来支持特定的几种调查并有能力采取相应的技术措施。

7) 长期生存性:

云计算具有长期发展风险。用户需要确认如果服务商在发生破产或被收购这类问题时，自己的数据是否会受到影响，用户需要了解在出现问题时如何拿回自己的数据，以及拿回的数据是否能够被导入到新的云中或替代的应用程序中。

4.2 云计算的安全体系架构

目前，一些学者和组织对云计算安全体系结构做了很多的探索和研究，提出了一些方案，生产了相应的产品，他们各自具有不同的特点。云计算体系划分为五个层次：物理层、核心层、资源架构层、开发平台层、应用层^[7]。如表 1 所示，

在五层体系架构中对应了五种服务，每层服务中均可以将 Web Services 的 UI 接口提供给用户，所有服务具有可靠、安全、可扩展、按需服务、经济等特点。下面按照层次结构，分别对各个层次的主体安全问题和主体安全机制进行介绍。

1) HaaS (Hardware as a Service): 物理层资源主要指构成云骨干的地理分布的局部本地资源，可以是计算资源，存储资源，传感器，服务器，网络等。在这一层面面临主要是本地安全问题，包括硬件故障、电源故障、位置安全、物理访问、环境安全和地域因素。软件资源面临病毒攻击、本地网入侵等安全问题。这层是云计算的最底层，可以提供服务给有巨大 IT 需求的企业，目前产品主要有 IBM- Morgan Stanley' s Computing Sublease 和 IBM' s Kitty hawk Project。针对这一层面面临的问题，可以采用传统的安全机制，包括故障处理、备用电源、设备访问控制、电磁干扰、环境保护、杀毒软件和防火墙等措施。

Table 1. Cloud security architecture

表 1. 云安全体系架构

架构层次	服务层次	安全问题	技术性安全机制		非技术性安全机制
			主体安全机制	服务安全机制	
应用层	SaaS	软件漏洞、版权问题	软件补丁、软件版本升级		
开发平台层	PaaS	平台构建漏洞、可靠性、可用性、完整性	平台升级、Parley- X 保护		
	IaaS	计算服务性能不可靠	并行计算间性能隔离	WS-Security	
	DaaS	数据机密性、可靠性、完整性、一致性、可用性	数据加密、数据隔离、数据摘要、数据校验、数据备份、灾难恢复	WS-Reliability WS-Trust WS-Authorization	规章制度 法律法规
资源架构层	CaaS	工作流管理漏洞、通信安全、网络安全	工作流完善、通信安全方案、网络安全方案	WS-Secure Conversation	
	KaaS	软件漏洞、分布式抽象技术缺陷、分布式管理漏洞	软件补丁及升级、分布式抽象技术和方案改进	等服务安全机制	
核心层	HaaS	硬件故障、非法访问、环境安全、病毒攻击、网络入侵	故障处理、备用电源、设备访问控制、电磁干扰、环境保护、杀毒软件、防火墙		
物理层					

2) KaaS (kernel as a service): 核心层提供抽象的分布式资源管理功能。在这一层中通过各种抽象技术提供了分布式应用的部署环境，提供 OS kernel、集群中间件等事项服务。主要产品有 Globus 、Condor 等。这层中要面临分布式资源管理软件漏洞、分布式抽象技术缺陷、分布式资源管理漏洞等安全问题。解决方案为要对其进行软硬件升级，改进分布式抽象技术，改进分布式资源管理方案。

3) CaaS (Communicate as a service): 网络通信服务层，提供可靠、安全的网络通信服务。典型的应用有 Microsoft CSF。这层中主要面临工作流管理漏洞、通信机密性、通信可靠性、通信可用性和网络安全等问题。可以采用工作流完善、通信加密、通信时延和带宽控制、通信安全协议和网络入侵检测等措施进行防范。

4) DaaS (Data as a Service): 数据存储层，提供分布式的可靠、安全、大容量、便捷的数据存储服务。

它所面临的主要安全问题是数据安全,数据的机密性、可靠性、完整性、一致性、可用性。典型应用有 Amazon S3、EMC Storage Managed Service。我们可以采用对数据进行加密、数据隔离、数据摘要、数据校验、数据备份、灾难恢复等措施。

5) IaaS (Infrastructure or Integration as a Service): 计算层主要提供灵活、高效、高强度的分布式计算服务,主要产品有 Amazon EC2 和 Enomalism Elastic Cloud。面临的问题是计算性能的不可靠,其原因是在并行计算中的资源竞争导致的性能干扰引起。在虚拟环境中常采用并行计算间性能隔离机制来解决这个问题。

6) PaaS (Platform as a Service): 开发平台层,提供分布式开发服务。以 API 方式提供各种编程环境,同时也为程序开发者提供扩展、负载均衡、授权、email、用户界面等多样服务支持。PaaS 加速了应用服务部署,支持应用服务扩展。如 Google App Engine 和 Salesforce Apex System。主要安全问题包括平台的构建漏洞、可靠性、可用性、完整性。采取的措施是对平台进行升级,对平台进行 Parley-X 保护。

7) SaaS (Software or Storage as a Service): 软件层提供分布式应用服务。为用户提供开发、测试、运行、维护、升级等安全可靠的服务,如 Google Apps、Salesforce CRM System。主要问题是软件漏洞、版权问题。而解决方案是采用软件补丁、软件版本升级。其中的版权问题属非技术性安全机制。

云是面向服务的架构体系,在云中底层细节被隐藏起来,只向客户提供透明服务。在云计算体系结构中的 XaaS (“X as a service”、“anything as a service”或 “everything as a service”)是 “一切皆服务”,是一种新的服务提供模式^[8]。其最主要的含义是将提供的功能以服务的方式提供出来,然后根据类似于 SLA(Service Level Agreement) 的方式为其客户提供相应的服务。因此,云服务也是一种 Web Services,在提供服务的过程中也要面临 Web Services 的各种安全问题。那么

云服务安全机制也就可以借鉴 Web Services 的各种安全机制,如 WS-Security, WS-Reliability, WS-Trust, WS-Authorization, WS-Secure Conversation 等来实现。

在云计算体系架构中非技术性对策中主要包括法律法规、管理制度、教育培训等方面。需要一系列的故障制度和正式文件对服务进行防范和保护。安全不仅是一个技术问题,也是一个管理问题。另外还要对使用者和维护者或运营者进行培训和学习,确保其能够正确使用云计算服务。

5. 结束语

现在已步入云计算的时代,云计算通过将中间件组件化、虚拟化使复杂的问题可以简单快速的解决。但云计算的广泛使用还需要一段时间,仍然有一些问题需要解决,比如云计算的协议标准不统一,不同服务商不能完全整合,数据和服务迁移问题,人们对于云的认识程度和认可度不够,相应硬件环境和软件环境的建设,相关法律法规的制定和完善,亟待解决的安全问题等等。但随着信息技术的发展,这些问题会相继得到解决,相信云最终会落于我们寻常百姓身边。

References (参考文献)

- [1] cloud computing, <http://baike.baidu.com/view/1316082.htm>
- [2] <http://www.cloudcomputing-china.cn/Article/jh/200805/1.html>
- [3] Huaweismantec, cloud computing, huawei, Electronic Documents, Huawei technologies Co., Ltd, P7.
- [4] cloud computing, <http://www.huaweismantec.com/en/>.
- [5] IT Experts Net, Cloud computing security risk assessment, <http://security.ctocio.com.cn/securitycomment/175/8204675.shtml>
- [6] Ge hui, Information Security of Cloud Computing[J], Silicon valley, 2009(2), P42-43.
- 葛慧, 云计算的信息安全[J], 硅谷, 2009(2), P42-43.
- [7] Chen Danwei, Huang Xiuli, REN Xunyi, Analysis of Cloud Computing and Cloud Security[J], computer technology and development, 2009(2), p99-102.
- 陈丹伟, 黄秀丽, 任勋益, 云计算及安全分析[J], 计算机技术与发展, 2009(2), p99-102.
- [8] What is XaaS (anything as a service)?, http://www.whatis.com.cn/word_5533.htm.