

云计算及安全分析

陈丹伟,黄秀丽,任勋益

(南京邮电大学 计算机学院,江苏 南京 210003)

摘 要:云计算是个新兴的名词,目前对它的定义和内涵还没有公认的界定,许多研究团体对它的研究都处于起始阶段,对云计算体系结构及其安全分析的研究也很少。云计算是一种计算模式,意味着面向服务的体系架构。文中首先对云计算的定义、特征进行了阐述;接着,提出了云计算体系架构,并对其进行了详细阐述;最后,介绍了云计算所面临的安全问题,在此基础上对云计算安全性进行了详细分析,针对云计算所面临的各种问题,给出了相应的安全机制。

关键词:云计算;体系结构;云计算安全;安全架构

中图分类号:TP301.6

文献标识码:A

文章编号:1673-629X(2010)02-0099-04

Analysis of Cloud Computing and Cloud Security

CHEN Dan-wei, HUANG Xiu-li, REN Xun-yi

(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Cloud computing is an emerging conception, and there is little consensus on how to define and understand it. Most research communities have recently embarked, and there are little researches on cloud computing architecture and its security. Cloud computing is a kind of computing paradigm and means service-oriented architecture. Define cloud and its characteristics firstly, and then give cloud computing architecture in detail, lastly introduce the security issues of cloud computing and give corresponding security mechanism against these security issues.

Key words: cloud computing; architecture; cloud computing security; security architecture

0 引言

当几个月前 Google 提出云计算的概念的时候,Amazon 说自己做的事情就是云计算,IBM, Intel, Sun 都声称自己在云计算领域有深刻的计划。于是,作为一个新的概念,云计算走入人们的视野,并日益引起人们的关注。

云计算的产生有其潜在的背景,随着 Internet 网络应用技术和普及,尤其是 Web2.0 的发展导致网络用户和网络数据量高速增长,对数据的处理能力提出了更高的要求。此外,网络资源的需求和利用出现失衡状态,某些应用需要大量的网络资源,而大量的网络资源没有得到充分利用。因此,资源的整合和优化是网络发展的必然趋势,云计算应运而生。

目前,对云计算的理论研究滞后于实践应用,理论研究尚处于初级阶段,而初步的云计算产品已在市场进入应用。

1 云计算体系架构

1.1 云计算的概念

云计算是个新兴的名词,目前对它的定义和内涵还没有公认的界定。在众多的云计算定义中,采用如下的定义^[1]：“云计算是一种由规模经济驱动的大规模分布式计算模式,通过这种计算模式,实现抽象的、虚拟的、可动态扩展、可管理的计算,存储,平台和服务等资源池由互联网按需提供给外部用户。”

从上述定义可以得出云计算的含义,云计算具有如下的显著特征:

(1) 大规模:云计算是一种分布式计算模式,而且是有规模经济驱动的计算模式,因此,大规模是云计算的首要特征,只有大规模的云计算才能实现云计算各种服务优势,尤其是服务的能力和服务的规模经济。

(2) 虚拟化: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,这些服务通过虚拟化技术实现。用户在任意位置、使用各种终端从云中获取应用服务,而无需了解它的具体实现和具体位置。

(3) 可靠性:云计算的发展依赖于云服务市场,而云服务的发展依赖于云服务的可靠性,因此,云计算必

收稿日期:2009-05-25;修回日期:2009-08-13

基金项目:国家十一五科技支撑计划项目(2007BAK34B06)

作者简介:陈丹伟(1971-),男,副教授,硕士研究生导师,研究方向为信息安全。

须采取措施来保障服务的高可靠性,可靠性是云计算必不可少的特性。

(4) 可扩展性:“云”的规模可以动态扩展,满足应用和用户规模增长的需要。同时,云服务也支持用户应用在云中的可扩展性。

(5) 动态配置:云服务可以按需定制,按需供应。

(6) 经济性:云计算依靠规模经济,规模经济带来的是低成本优势,经济性是云计算的重要特征。

1.2 云计算体系架构

在对云计算进行剖析后,可以把云计算体系架构^[2,3]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。

云计算体系架构的五层结构表格如表 1 所示,其中有五层服务,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。此外,表中同时列出了五层服务的典型市场产品。

表 1 云计算体系架构

架构层次	服务形式	功能(by web)	典型市场产品
应用层	SaaS by web services	本层在开发平台上开发各种应用程序,提供各种分布式应用服务	Google Apps Sales force CRM System
开发平台层	PaaS by web services	本层在资源架构层之上构建开发平台,提供各种分布式开发服务	Google App Engine Sales force Apex System
资源架构层	IaaS by web services	本层在内核层之上构建计算资源架构,提供分布式计算服务	Amazon EC2 Enomism Elastic Cloud
	Cloud DaaS by web services	本层在内核层之上构建存储资源架构,提供分布式存储服务	Amazon S3 EMC Storage Managed Service
	CaaS by web services	本层在内核层之上构建通信资源架构,提供基于局域网或 Internet 的分布式通信服务	Microsoft CSF
核心层	KaaS by web services	本层在物理资源层之上实现基本的分布式资源管理,通过各种抽象服务提供分布式应用的部署环境	Globus Condor
物理层	HaaS by web services	本层是构成云骨干的地理分布的局部资源,提供各种局部资源支持	IBM-Morgan Stanley's Computing Sublease IBM's Kitty hawk Project

下面按照层次结构,分别对层次作用进行介绍:

1) 物理层:是指地理位置不同的分布在各地的局部资源,提供局部资源支持。局部资源可以是计算资源、存储资源、传感器、服务器、网络等各种本地资源。物理层是云计算的底层基础设施。物理层提供者负责运行、管理、维护和升级物理资源,提供 HaaS 服务给有巨大 IT 需求的大型企业。

2) 核心层:是指对分布式资源的基本管理功能,通过抽象服务提供分布式应用的部署环境。核心层功能可以通过 OS kernel、超级监督者、虚拟机监视器或集

群中间件实现抽象服务。提供 KaaS 给分布式应用的部署者。

3) 资源架构层:是指在核心层之上部署的分布式应用,提供基本的分布式资源服务。本层提供的基本分布式资源服务包括 IaaS, DaaS, CaaS。其中, IaaS 是分布式计算服务,提供灵活、高效、高强度的计算服务, IaaS 主要通过虚拟技术实现。DaaS 是分布式存储服务,提供可靠、安全、大容量、便捷的数据存储服务。CaaS 是网络通信服务,提供可靠、安全的网络通信服务。

4) 开发平台层:是指通过 API 为应用程序开发者提供各种云计算编程环境,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。

5) 应用层:是指通过开发平台提供的开发环境和市场需求,开发出来的各种应用程序。应用程序提供者负责软件的开发、测试、运行、维护、升级,为用户提供安全、可靠的服务。

2 云计算安全机制

2.1 云计算面临的安全问题

美国知名市场研究公司 Gartner 日前发布的一份名为《云计算安全风险评估》的研究报告称,虽然云计算(cloud-computing)产业具有巨大市场增长前景,但对于使用这项服务的企业用户来说,他们应该意识到,云计算服务存在着七大潜在安全风险,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:

1) 特权用户的接入: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访问方面的具体信息。

2) 可审查性:云计算服务商愿意而且有能力做到遵从相关法律法规。

3) 数据位置:云计算服务商给出合同承诺,遵守相关数据管理法律法规,提供数据存储地点信息的查询服务。

4) 数据隔离:云计算服务商按照不同数据,提供数据隔离存储服务。

5) 数据恢复:云计算服务商有能力对数据进行快速全面恢复。

6) 调查支持:云计算服务商以合同承诺来支持特定的几种调查。

7) 长期生存性:云计算服务商提供长期发展风险

的安全措施,譬如用户如何拿回自己的数据,以及拿回的数据如何被导入到替代的应用程序中。

2.2 云计算的安全机制

在云计算安全要求诸条款中,一些条款需要技术性安全机制的支持来实现,一些条款需要非技术性安全机制来实现,而有些条款则要依靠两种技术结合起来实现。这里的技术性安全机制包括了认证、授权、审计、加密等传统的安全技术,而非技术性安全机制是指相关的安全法律法规。

目前,云计算尚没有一个被广泛接受的安全体系结构。有很多学者和组织对安全 Web Services 体系结构做了有益的探索,并提出了一些方案与产品,各自有不同的特点。结合论文已提出的云计算体系架构,将安全要求的实现落实到各个服务层次上,提出如表 2 所示的云安全体系架构:

表 2 云安全体系架构

服务层次	安全问题	技术性安全机制		非技术性安全机制
		本体安全机制	服务安全机制	
SaaS	软件漏洞、版权问题	软件补丁、软件版本升级		
	平台构建漏洞、平台可靠			
PaaS	性、平台可用性、平台完整性	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		
	数据机密性、数据可靠性、	数据加密、数据隔离、数据	WS-Security	
DaaS	数据完整性、数据一致性、	摘要、数据校验、数据备份、灾难恢复	WS-Reliability	
	数据可用性		WS-Trust	
			WS-Authorization	规章制度
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		法律法规
			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、分布式抽象技术和管理方案改进		等服务安全机制
HaaS	硬件故障、电源故障、非法访问、电磁泄露、环境安全、病毒攻击、本地网络入侵	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		

下面按照层次结构,分别对各个层次的本体安全问题和安全机制进行介绍:

1)HaaS:物理层资源主要指本地资源,所以 HaaS 层面临的安全问题主要是本地安全问题。本地的硬件资源面对的安全问题和传统的硬件安全问题一样,除了物理设备本身的问题如硬件故障和电源故障之外,还包括设备的位置安全、物理访问、物理环境安全和地域因素。本地的软件资源面临的问题和传统的软件安全问题一样,包括病毒攻击、本地网入侵等安全问题。针对物理层面临的诸多问题,可以利用传统的安全机制来进行安全防范,这些机制包括故障处理、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。

2)KaaS:核心层在物理层之上提供抽象的分布式资源管理,通过各种抽象技术提供分布式应用的部署环境,所以面临的安全问题,包括分布式资源管理软件

漏洞、分布式抽象技术缺陷、分布式资源管理方案漏洞,而解决方案为分布式管理软件补丁、分布式管理软件升级、分布式抽象技术、分布式资源管理方案改进。

3)CaaS:网络通信服务层^[4-6]的目的是提供可靠、安全的网络通信服务。所以面临的问题包括工作流管理漏洞、通信机密性、通信可靠性、通信可用性和网络安全,可以采用的安全机制包括工作流完善、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。

4)DaaS:数据存储层的目的是提供可靠、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,包括数据机密性、数据可靠性、数据完整性、数据一致性、数据可用性,相应的安全机制有数据加密、数据隔离、数据摘要、数据校验、数据备份、灾难恢复。

5)IaaS:计算层主要提供灵活、高效、高强度的计算服务,所面临的问题包括计算性能不可靠,即并行计算中由资源竞争导致的性能干扰。IaaS 主要通过虚拟技术实现,在虚拟环境中常采用并行计算间性能隔离机制来解决并行计算间的干扰问题^[7]。

6)PaaS:开发平台以 API 方式提供各种编程环境,面临的安全问题包括平台构建漏洞、平台可靠性、平台可用性、平台完整性,相应的解决方案有平台升级和 Parley-X 保护。

7)SaaS:软件层面面临的主要问题和传统的软件安全面临的安全问题相同,主要包括软件漏洞、版权问题。而解决方案采用软件补丁、软件版本升级。其中版权问题属非技术性安全机制。

云意味着一种面向服务的架构体系^[8],通过隐藏底层细节,向客户提供透明服务。XaaS^[2]是一种新的服务提供模式,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,云服务是一种 Web Services^[9],在提供服务的过程中面临 Web Services 的各种安全问题,而云服务安全机制需要借鉴 Web Services 的各种安全机制^[10],主要包括 WS-Security^[11],WS-Reliability,WS-Trust,WS-Authorization,WS-Secure Conversation 等。

非技术性对策主要包括:法律、管理、教育培训等方面。在一系列非技术对策中,法律以其权威性、强制性为后盾,是一种非常有效的非技术性保障。安全需要一系列的法律法规。这些法律法规对于服务保护起到了极大的防范和保护作用。这是法律法规也是保护服务安全、确保其发展的法律法规依据。安全不仅是一个技术问题,同时也是一个管理问题。正如很多制

制造业“安全生产,重在管理”制度一样,服务的安全包含了太多的内容,各方面的防范重点和所采取的技术手段也不尽相同,要想最大程度保障服务的安全,需要从内部管理真正去加强^[12]。

3 结束语

在阐述云计算定义和内涵的基础上,研究探讨了云计算体系架构的层次结构,并分析了其安全问题。云意味着一种面向服务的架构体系,通过隐藏底层细节,向客户提供透明服务。因此,基于客户的使用和服务交互安全考虑,下一步工作就是在已提出云安全体系架构的基础上,对基于 Web Services 的云服务安全方案进行深入的研究。

参考文献:

- [1] Foster I, Zhao Yong. Cloud Computing and Grid Computing 360 - Degree Compared[M]//2008 Grid Computing Environments Workshop, IEEE. Austin, Texas: [s. n.], 2008.
- [2] Aymerich F M, Fenu G, Surcis S. An Approach to a Cloud Computing Network[C]//2008 First International Conference on Applications of Digital Information and Web Technologies, IEEE. Czech Republic: Technical University of Ostrava, 2008: 113 - 118.
- [3] Youseff L, Butrico M, Silva D D. Toward a Unified Ontology of Cloud Computing[M]//2008 Grid Computing Environments Workshop, IEEE. Austin, Texas: [s. n.], 2008.
- [4] Johnston W, Metzger J, O'Connor M, et al. Network Commu-

nication as a Service - Oriented Capability[M]//High Performance Computing and Grids in Action. [s. l.]: IOS Press, 2008: 1 - 35.

- [5] Hanemann A, Boote J W, Boyd E L, et al. Perfsonar: A service - oriented architecture for multi - domain network monitoring [M]//ICSOC, ser. Lecture Notes in Computer Science, B. B. et al. [s. l.]: Springer, 2005: 241 - 254.
- [6] Hofstadter J. Communications as a Service[EB/OL]. 2007 - 11. <http://msdn.microsoft.com/en-us/library/bb896003.aspx>.
- [7] Koh Y, Knauerhase R C, Brett P, et al. An analysis of performance interference effects in virtual environments[C]//ISPASS. [s. l.]: IEEE Computer Society, 2007: 200 - 209.
- [8] Buyya R, Yeo C S, Venugopal S. Market - Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities[C]//Proc. of 10th IEEE Conference on HPCC'08, IEEE. Dalian, China: [s. n.], 2008: 5 - 13.
- [9] Steel C, Nagappan R, Lai R. 安全模式[M]. 北京:机械工业出版社, 2006: 159 - 162.
- [10] IBM, Microsoft. Security in a Web Services World: A Proposed Architecture and Roadmap[EB/OL]. 2002 - 04 - 07. <http://msdn2.microsoft.com/en-us/library/ms977312.aspx>.
- [11] OASIS Standard. Web Services Security: SOAP Message Security 1.1 (WS - Security 2004)[EB/OL]. 2006 - 02 - 01. <http://docs.oasis-open.org/wss/v1.1/>.
- [12] 赛迪网. Web 服务安全“三层门”[EB/OL]. 2006 - 07 - 25. media.ccidnet.com/art/2651/20060725/651665-1.html.

(上接第 98 页)

参考文献:

- [1] Leonard J J, Durrant - Whyte H F. Mobile robot localization by tracking geometric beacons[J]. IEEE Transactions on Robotics and Automation, 1991, 7(1): 376 - 382.
- [2] Bailey T, Whyte H D. Simultaneous Localization and Mapping Part II: State of Art[J]. Robotics and Automation Magazine, 2006, 13(10): 100 - 112.
- [3] Whyte H D, Bailey T. Simultaneous Localization and Mapping Part I: The Essential Algorithms[J]. Robotics and Automation Magazine, 2006, 13(4): 99 - 110.
- [4] Chatila R, Laumond J. Position referencing and consistent world modeling for mobile robots[J]. Robotics and Automation, 1985, 2(1): 138 - 145.
- [5] Dissanayake G. A Solution to the Simultaneous localization and map building(SLAM) problem[J]. IEEE Transactions on Robotics and Automation, 2001, 17(3): 229 - 241.
- [6] Thrun S, Fox D, Burgard W. Robust Monte Carlo localization for mobile robots[J]. Artificial Intelligence, 2001, 128(5): 99 - 141.
- [7] Murphy K. Bayesian map learning in dynamic environments[J]. Advances in Neural Information Processing Systems (NIPS), 1999, 12: 1015 - 1021.
- [8] Doucet A, Freitas N, Murphy K. Rao - blackwellised particle filtering for dynamic bayesian networks[C]//In Proceedings of the Sixteenth Conference on Uncertainty in Artificial Intelligence. Stanford: Morgan Kaufmann Publishers, 2000: 176 - 183.
- [9] Montemerlo M, Thrun S, Koller D, et al. FastSLAM: A factored solution to the simultaneous localization and mapping Problem[C]//In Proceedings of the AAAI National Conference on Artificial Intelligence. Canada: AAAI Press, 2002: 593 - 598.
- [10] Thrun S, Fox D, Burgard W. Probabilistic Robotics[M]. London, England: The MIT Press, 2005.
- [11] Murphy K. Dynamic Bayesian Networks: Representation, Inference and Learning[D]. Berkeley: University of California, 2002.