云计算中的信任机制研究

何 颖,徐 军,侯雅婷
(南京航空航天大学 计算机科学与技术学院,江苏 南京 211100)

摘 要:云计算作为继网格计算、对等计算以及服务计算之后的一种新型计算模式,其异构、虚拟、松散等特性导致了有别于传统计算模式的新的安全问题。为此,从云计算的特点出发,综合回顾并分析了云计算作为新型计算模式所引发的比传统分布式计算更加复杂的安全问题。从边界访问控制、租户间信任、服务质量、虚拟化安全等方面讨论了信任机制与云计算安全的关系,并就如何对云计算环境中的信任进行有效评估问题进行了讨论分析。结合云计算环境下的安全需求,讨论分析了将信任机制引入到云计算环境中的理论依据和可行性,深入剖析了信任机制在云计算背景中不同技术层面的应用。针对当前云计算研究工作中的不足,提出了云计算环境中关于信任机制研究的下一步方向。

关键词:云计算;云计算安全;信任机制;声望
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2017)10-0101-05
doi:10.3969/j.issn.1673-629X.2017.10.022

Research on Trust Mechanism in Cloud Computing

HE Ying,XU Jun,HOU Ya-ting
(College of Computer Science and Technology,Nanjing University of Aeronautics and Astronautics,Nanjing 211100,China)

Abstract:Cloud computing has been considered as a new type of computation model after grid computing,peer-to-peer computing and service computing,and its heterogeneous,virtual and loose characteristics leads to new security problems different from the traditional computing model. Therefore,starting from the characteristics of cloud computing,the more complex security problems in contrast with the traditional distribution computing caused by cloud computing as a new type of computation model are synthetically reviewed and analyzed. The relationship between trust mechanism and security of cloud computing is discussed involving border access control,trust among tenants,service quality and virtualization security etc as well as that of effective evaluation on the trust mechanism in the environment of cloud computation. According to the security requirements of cloud computing environment,the theoretical basis and feasibility for introduction of confidence mechanism into cloud computing environment is discussed and analyzed and the applications of trust mechanism in various technical layers in the context of cloud computing is analyzed in depth. In allusion to deficiencies in the present investigations on cloud computing,the research orientation of trust mechanism in environment of cloud computing is also proposed.

Key words:cloud computing;cloud computing security;trust mechanism;reputation

0 引 言

云计算是一种虚拟化与并行分布式计算发展融合的全新计算模式。云计算依靠低成本、超大规模、虚拟化、高可扩展性等独特优势引发了 IT 产业界的技术革命。然而云计算发展的重要阻碍是日渐增加的安全问题[1]。

云计算环境中存在的安全问题主要包括云系统自身的安全、数据存储安全以及应用安全[2-3]。首先,云计算的高度自治性、独立性和动态性等特性,使得云计算中普遍存在数据安全性与隐私性的忧虑[4]。其次,云计算面向服务的可扩展计算模式,导致了服务的可信度降低。再次,随着云计算用户和云计算服务内容的多元化增长,用户需求和提供商的服务模式出现了明显的信任危机[5]。

随着安全风险的增加,管理问题的明显化,社会各界对安全机制和管理方法的研究越来越重视。当前有关云计算的安全问题的研究主要集中在数据隐私与完整性[6]、虚拟资源的安全、身份认证[7]、用户资源和资

收稿日期:2016-10-07 **修回日期**:2017-01-18 **网络出版时间**:2017-07-11
基金项目:中央高校基本科研业务费(NZ2013306);南京市医学科技发展一般性课题(YKK1571)
作者简介:何 颖(1992-),女,硕士研究生,研究方向为社交网络与信任机制。

源处理的安全[8]、访问控制[9]等方面。

在云计算模式下,结构松散耦合和计算动态造成其安全管理的复杂性,导致传统的安全解决方案已不能完全解决云计算环境中新涌现出的安全问题[10]。当前已有方案的不足主要表现在对边界访问控制、实体可信、云服务质量评价、虚拟化安全等方面。但其松散架构也为信任评估这一弹性机制引入云计算提供了广阔空间,信任机制可以有效解决边界模糊的访问控制,评价标准不统一的云服务质量评价,以及云计算环境中交互实体安全等安全问题。

针对云计算中的安全问题,讨论并提出了包含信任管理的云计算安全框架;剖析了云计算不同层次的安全问题,强调了引入信任机制的必要性;描述了信任在云计算安全领域的具体应用,并对比分析了各信任模型的优缺点;指出了当前研究工作的不足,并阐述了今后一段时间信任在云计算各技术领域的研究热点及其发展趋势。

1 云安全问题

云计算系统除了面临传统的信息安全问题外,由于其自身的新特性,引发了一些新的安全问题。在复杂的网络环境中,安全威胁的表现形式可能不尽相同,但通常来讲,网络安全的主要目的是确保对象的信息安全,防止恶意主体的攻击、窃听、非法访问等手段,建立一套完整的保护机制。

1.1 安全问题总结

云计算实质上是为达到海量计算资源的共享,创新性提出的基础架构分布式设计。云计算模式在信息处理、信息存储和信息共享等方面具有显著优势,云计算可以动态地创建应用服务和数据资源,而这些服务与资源都是高度虚拟化的。从服务概念出发,将云计算的核心应用分为 3 个层次[11]:软件即服务(SaaS)、平台即服务(PaaS)、基础设施即服务(IaaS)。不同层次所面临的安全问题不同。根据文献[12-14],可概括出云计算各层常见的安全问题,如图 1 所示。

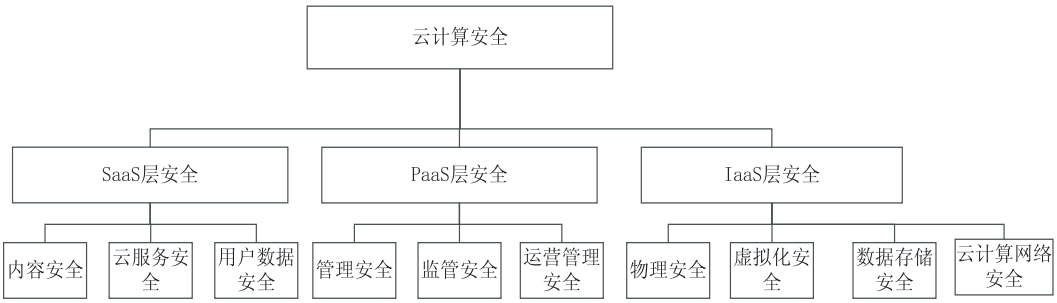

图 1 云计算安全问题

云计算的首要安全需求就是数据安全与隐私保护。需求的目标是针对客户,在云计算中,如果云服务商监守自盗,就会对用户数据进行搜集分析,并将其用于不正当商业用途,恶意泄露或出卖用户隐私[15]。现阶段,云计算没有可靠的第三方机构统一管理,故各个计算站点都是依靠点对点建立信任关系。同时,交互节点的可信保障机制也是首要需求,即服务请求者或服务提供者需通过信任机制,确保对方的可信度,才能完成服务请求或提供,包括客户与服务商之间的信任、服务商之间的信任等。从技术层面针对各层服务详细总结了云计算面临的具体安全问题。

1.2 云计算安全框架

文献[16]提出了建立包含安全服务体系、安全标准体系和测评体系的云计算安全体系。在此基础上,根据云计算中用户的安全目标和安全管理中运用的安全机制,提出了包含用户接入层、核心业务层、服务管理层以及虚拟资源层的云计算安全框架,如图 2 所示。

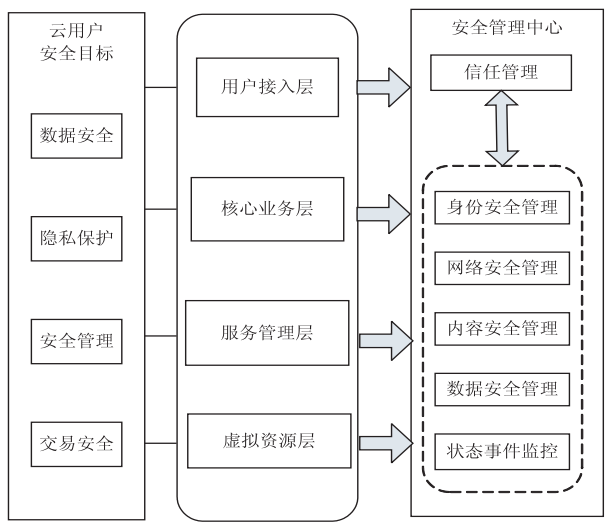

图 2 云计算安全框架

云计算环境中用户实体的主要安全目标可以概括为数据安全、隐私保护、安全管理和交易安全。实现上述目标的主要手段在于信任管理、身份安全管理、网络安全管理、内容安全管理、数据安全管理、状态事件监控。其中,信任管理作为一种弹性管理手段,通常在各个管理层面都有相应研究和应用,主要包含:用户接入层中的用户身份安全管理中的可信访问控制和对于非授权用户的身份认证;核心业务层中的多租户共享运营模式和多层服务模式;服务管理层的可信服务推荐

和组合服务评价;虚拟资源层的虚拟机可信和可信计算。文献[17]对云计算的安全问题做了详细总结,包括基础设施安全、数据安全、通信安全、访问控制。

2　云计算的信任问题

云计算既存在传统的安全问题,也有自身特性带来的新问题,为了利用信任机制解决安全问题,需要了解在云计算中的各种安全隐患和攻击行为。

2.1　边界访问控制问题

在开放的云环境中,由于用户身份的不确定性,服务资源的虚拟性和计算的动态性,造成了云计算用户接入层安全管理的复杂性。

传统的访问控制技术是一种基于身份的授权技术,在管理范围内设置安全身份授权,即用户的身份是可以确定的。如在公司内部,计算机、网络、路由器等 IT 设备和设施形成了一个可被企业信息系统管理员完全控制的网络,通常称作“可控信任域”。其所有服务资源都处于企业的完全控制之下,是值得信任的,可以根据人力资源中的职务关系对员工给予相应的访问控制权限。对服务资源进行访问的用户可以被分为授权用户和非授权用户,通信协议中包含加密、认证、协商等过程,然后根据 ACL 表中确定的身份信息分配相应的权限,而在服务器组内部也有一系列针对服务器安全防护的身份认证和访问控制等安全策略。

随着分布式计算的发展,面向服务架构的特点对访问控制提出了新的挑战。与传统的分布式系统相比,面向服务架构的分布式系统中,不管是提出请求的客户,还是提供服务资源的服务商,具有高度动态的特性[18],主要表现在:

(1)身份可匿:对象无法事前知道其准确真实的身份;

(2)缺乏扩展性:对新的访问条件和新增限制,不能灵活处理;

(3)针对不同的管理域,没有统一认定的策略或者信任机制进行管理;

(4)缺乏权威机构的管理。

在传统的 RBAC 模型中,授权对象和操作的变化都对应着相应的权限分配,而这种模式没办法适应高度动态的云计算模式。

2.2　用户与服务提供商之间的信任问题

由于在云计算这种分布式环境中,没有能保障云服务可靠性的官方性质的集中认证与授权中心,导致网络中服务和服务提供者的品质参差不齐,无法保证服务提供者一直提供真实、高质量的内容和服务。因此,有必要鉴别云服务和云服务提供者的品质。

云计算多层服务和资源的虚拟化,导致用户对服务提供商是否可信持怀疑态度;云计算的高度开放性使得用户的可信度变得更难计算,用户的自由加入或离开给信任管理带来了重大挑战;多组合问题和多层服务问题也导致用户实体之间,服务提供商之间存在可信问题。

2.3　云服务质量

在云计算中,服务提供者向消费用户提供了基于核心业务层的 3 种服务,即 IaaS、PaaS、SaaS。对比传统服务下采用的产品被动防御安全策略,在云计算服务环境下是不可靠的。根据服务资源的不确定性、分布性、开放性、动态性等特点,需要研究对应的信任机制,建立可信度计算模型,对实体之间的信任度进行评估,以保证云服务的安全。

2.4　虚拟化安全问题

虚拟化技术是云计算最核心的技术,它基于使用软硬件分时服务、模拟与仿真执行等技术,达到在单个计算机物理设备上模拟出多个相互隔离的硬件执行环境的目的。

云计算环境相比之前的技术,大量运用计算能力虚拟化、网络虚拟化、存储虚拟化等虚拟化技术,这些技术完成共用底层基础设施(infrastructure)的抽象,提供统一的可编程接口,映射彼此隔离且具有不同拓扑的虚拟网络到共用的基础设施,为用户提供差异化服务。

使用虚拟化技术后主要产生两方面的问题[19]:一是虚拟化技术引入后产生了一些特定的安全风险,怎样解决虚拟化方面的安全是云计算与传统安全的一个重大区别;二是云计算代表着一种计算使用方式的转变,在终端、网络和服务端的安全需求均发生了相应变化,传统的安全保护手段已经不适应云计算的需求。针对虚拟机操作系统内核级的攻击可以突破系统边界,造成比传统系统环境更大的危害。

3　云计算中的信任技术及其应用

信任管理可以为云计算中交互的实体建立信任的桥梁,下面将从云计算中运用的关键技术出发,着重分析访问控制中有关信任的安全策略,信任在解决云计算内外统一协作的安全问题、实体身份认证、隐私保护、服务质量、虚拟计算等方面的应用。

3.1　基于信任的访问控制

访问控制是解决信息泄露问题的核心技术,它完成用户的权限分配,然后根据不同的权限,允许合法用户访问权限内受保护的资源,拒绝非授权用户的访问,有效保护了受限信息的传播,用户的合法权限和私人信息不被泄露。目前最流行的访问控制模型有自主访问控制模型(Discretionary Access Control, DAC)、强制

访问控制模型(Mandatory Access Control,MAC)和基于角色的访问控制模型(Role-Based Access Control,RBAC)。

信任管理的凭证具有更高的表现性,此类凭证可以与授予权限的持有用户的各种属性完全绑定,还能绑定在完全可编程的“能力”。这样的凭证可加强信任管理的表现性,对安全策略、凭证或者信任关系给予统一管理,对分布式系统的访问控制或者授权方式提供通用、可靠的方法。运用信任管理能很好地解决图 3 中的访问控制问题。

假设用户 U_1 能正常访问云 C_1 的服务,云 C_1 对用户 U_1,U_2,U_3 有不同的访问策略,独立云 C_1,C_2,C_3 之间也有相应的服务访问策略。当用户 U_1 需要访问云 C_2 或 C_3 的服务时,由于 C_2 和 C_3 没有针对用户 U_1 的访问策略,将导致 U_1 无法访问云 C_2 和 C_3 的服务。在引入信任机制后,若云 C_1 与 U_1 有信任关系,云 C_1 与云 C_2 也有信任关系,则当用户 U_1 请求访问云 C_2 时,云 C_2 可以根据云 C_1 对用户 U_1 的信任度结合自身对云 C_1 的信任度,综合自身相关策略,给予用户 U_1 相应的访问权限。可见,信任机制确实为上述系列问题提供了较好的解决方案。

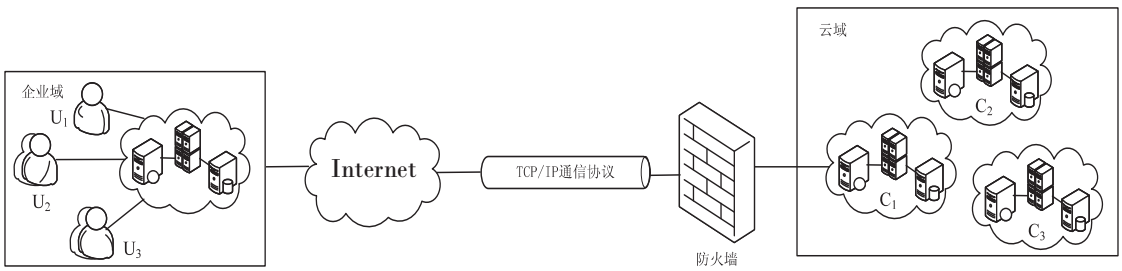

图 3 云计算网络架构模型

3.2 交互实体信任评估

在云计算中,数据拥有者、数据用户和云服务提供商分别处于不同的安全域。数据拥有者失去了对数据存储与访问的物理控制权和直接控制权,租户需要对服务商的可信度进行评估。同样,为避免恶意用户滥用资源,通过非法手段窃取其他租户或云平台的隐私数据,或者利用云平台提供的资源进而攻击云平台中的其他用户或云平台本身,用户的可信度因为云平台的高度开放性,在对用户的加入或离开基本没有限制的情况下,面临重大的挑战。为避免上述情况的发生,有必要对云计算环境中的用户进行监测。

3.3 基于信任的服务质量评估

云计算环境下云服务的可信度评价是一个涉及众多云服务用户的复杂的群体演化过程,在各种主客观因素影响下得到的评价结果具有显著的不确定性。云计算的应用面向不同的服务场景,所以根据消费者的不同,评价存在片面性、倾向性甚至是个人偏见性。因此,可行计算和信任机制的研究与建立需要避免这些问题,评估与推荐需要尽量客观准确。云计算和服务计算中引入了动态按需服务的方式,将 SLA 作为服务双方关于服务内容、质量等方面的约定,有效改变了 QoS 与可信性的计算方法和策略,服务交互双方的服务级别可以通过协商来确定。但是服务协商过程增加了可信计算的复杂性,使得提供信任保障的可信策略更具挑战性。当前云计算可信服务推荐研究中对于抗恶意攻击的研究还较少,也很少有考虑系统容错和组合服务中服务调度的效率问题,均只考虑了单一的云服务推荐,同时,也没有考虑时间效应。

3.4 虚拟计算可信

可信保证体系是虚拟计算环境的基础组件。虚拟计算环境下的信任管理具有不确定性和动态性,因此,虚拟计算环境下的可信保证体系应具备主观性、基于证据以及上下文相关性的特性。针对虚拟计算环境下虚拟共同体的服务选取以及自主元素的可信度计算的安全问题,在云计算中不同租户的数据与计算可能在相同的物理设备上完成,在虚拟机上用户可以运行多个操作系统和各种应用程序,物理资源的共享使恶意租户通过底层硬件环境对其他租户的虚拟机发起攻击成为可能。此外,虚拟机的外包使用模式下,如何向用户证明虚拟机中的执行内容可信也成为一个需要解决的问题。云计算中的应用服务没有固定的安全边界。特别是针对由多租户共享的运营模式,对资源的可控性进一步减弱,资源可能交叉地被多个租户租用,根本无法统一规划安全边界,建立防护措施,可以通过使用访问控制与信任机制相结合的安全策略。而多层服务模式使云计算内外服务协商难以统一的问题,同样可以通过信任对云间进行服务协商来解决。虚拟计算可信关系可以结合证据理论和上下文相关性来建立。

4 结束语

针对云计算访问控制中有关信任的安全策略,信任在解决云计算内外统一协作的安全问题,围绕信任在实体身份认证和虚拟计算等方面的应用进行了广泛深入的总结回顾,并介绍了最新的研究成果。同时,围

绕云计算中存在的典型安全问题,结合信任机制的现有研究成果进行了深入剖析。综上,当前云计算中信任机制的研究在理论及实现方面还存在如下问题:

(1)当前云计算中信任机制的主要研究在于信任评估区分恶意节点的精确度,对恶意攻击(合谋)的抵抗能力(健壮或鲁棒性)等,但是缺乏风险机制和统一的信任模型的性能评价标准。

(2)在已有研究中,信任模型性能的评价大多采用模拟实验的办法进行功能评价,而没有在云平台进行实际性能的评测。

(3)云计算中对于组合服务和工作流调度的信任没有明确的评价指标,对其可信度的评估还不够完善。

可以发现,云计算环境下多种安全需求和应用模式对信任机制提出的新挑战,提炼信任机制在新的情况下所出现的科学问题,并对其进行研究,具有更加迫切的意义。同时,也应结合其他学科的知识,研究动态信任关系的新模型。云计算场景中访问控制表(ACL)与身份认证的模糊性,为信任机制的引入提供了弹性空间,可以据此认为运用信任机制与 ACL 灵活适配的认证模式将是今后的研究热点。

参考文献:

[1] Nemati H. Optimizing information security and advancing privacy assurance: new technologies[M]. [s. l.]: IGI Publishing,2012.

[2] Tianfield H. Security issues in cloud computing[C]//IEEE international conference on systems, man, and cybernetics. [s. l.]: IEEE,2012:1082-1089.

[3] Zissis D, Lekkas D. Addressing cloud computing security issues[J]. Future Generation Computer Systems,2012,28(3):583-592.

[4] Pearson S, Shen Y, Mowbray M. A privacy manager for cloud computing[C]//IEEE international conference on cloud computing. Berlin: Springer,2009:90-106.

[5] Wang S, Liu Z, Sun Q, et al. Towards an accurate evaluation of quality of cloud service in service-oriented cloud computing [J]. Journal of Intelligent Manufacturing,2014,25(2):283-291.

[6] 肖人毅. 云计算中数据隐私保护研究进展[J]. 通信学报,2014,35(12):168-177.

[7] Yang J H, Lin P Y. An ID-based user authentication scheme for cloud computing[C]//Tenth international conference on intelligent information hiding and multimedia signal processing. [s. l.]: IEEE,2014:98-101.

[8] Wang C, Wang Q, Ren K, et al. Privacy-preserving public auditing for data storage security in cloud computing[C]//INFOCOM. [s. l.]: IEEE,2010:1-9.

[9] Lin G, Bie Y, Lei M. Trust based access control policy in multi-domain of cloud computing[J]. Journal of Computers,2013,8(5):1357-1365.

[10] Almorsy M, Grundy J, Müller I. An analysis of the cloud computing security problem[C]//Proceedings of APSEC 2010 cloud workshop. Sydney, Australia: [s. n.],2010.

[11] Mell P, Grance T. The NIST definition of cloud computing[J]. Communications of the ACM,2010,53(6):50.

[12] Ali M, Khan S U, Vasilakos A V. Security in cloud computing: opportunities and challenges[J]. Information Sciences,2015,305:357-383.

[13] Hashizume K, Rosado D G, Fernández-Medina E, et al. An analysis of security issues for cloud computing[J]. Journal of Internet Services and Applications,2013,4(1):1.

[14] Zhou M, Zhang R, Xie W, et al. Security and privacy in cloud computing: a survey[C]//Sixth international conference on semantics knowledge and grid. [s. l.]: IEEE,2010:105-112.

[15] 张　凯,潘晓中. 云计算下基于用户行为信任的访问控制模型[J]. 计算机应用,2014,34(4):1051-1054.

[16] 冯登国,张　敏,张　妍,等. 云计算安全研究[J]. 软件学报,2011,22(1):71-83.

[17] Zapata B C, Alemán J L F, Toval A. Security in cloud computing: a mapping study[J]. Computer Science & Information Systems,2015,12(1):161-184.

[18] 许　峰,赖海光,黄　皓,等. 面向服务的角色访问控制技术研究[J]. 计算机学报,2005,28(4):686-693.

[19] 易　涛. 云计算虚拟化安全技术研究[J]. 信息安全与通信保密,2012(5):63-65.