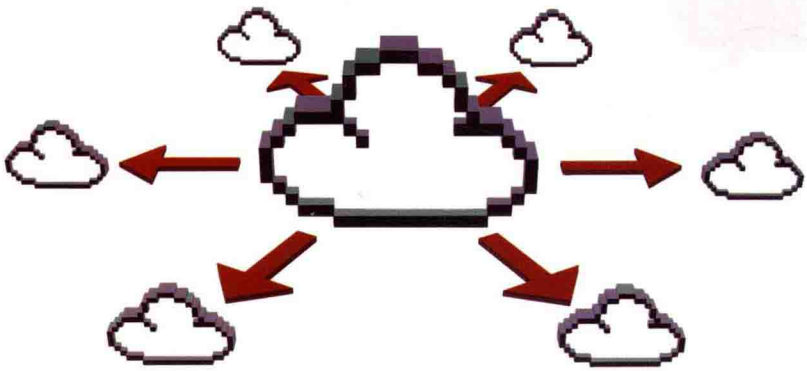
云计算环境下基于行为信任的访问控制安全技术研究

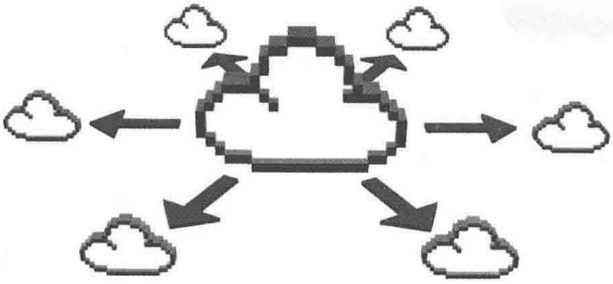
林果园◎著



中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

云计算环境下基于行为信任的访问控制安全技术研究

林果园◎著



人民邮电出版社
北京

图书在版编目（CIP）数据

云计算环境下基于行为信任的访问控制安全技术研究/林果园著. -- 北京 : 人民邮电出版社, 2016.12
ISBN 978-7-115-43782-2

Ⅰ. ①云… Ⅱ. ①林… Ⅲ. ①互联网络－安全技术－研究 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2016)第270367号

内 容 提 要

本书在分析云计算及其安全特点的基础上，探讨通过基于行为的访问控制来动态调节主体的访问范围，实现 BLP 和 Biba 模型有机结合，利用交互虚拟机和行为的可信性来保障系统的动态可信，结合用户与服务端两种信任评估算法，将信任管理与 RBAC 模型结合，实施基于相互信任度的域内和跨域访问控制策略，并提出相关模型。

本书可作为高等院校计算机相关专业和其他信息类专业研究生的参考书，也可以供相关领域的科技工作者参考。

◆ 著　　林果园
责任编辑　邢建春
执行编辑　秦　菲
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100078　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京天宇星印刷厂印刷

◆ 开本：880×1230　1/32
印张：4.5　　2016 年 12 月第 1 版
字数：120 千字　　2016 年 12 月北京第 1 次印刷

定价：39.00 元

读者服务热线：(010) 81055410　印装质量热线：(010) 81055316
反盗版热线：(010) 81055315

前 言

云计算作为一种新型的计算模式，能够为用户提供强大的虚拟化、可扩展性的网络服务资源，但同时也面临着严峻的安全挑战。访问控制技术是保障云计算安全的重要措施，然而直接将传统的访问控制模型应用到云计算环境并不能有效地解决云计算开放环境所面临的不确定性及脆弱性问题。在云计算环境中，只有同时确保云计算环境内部与外部的可信性，才能够有效保证云用户与云服务端交互过程中双方的安全性。因此，本书重点研究云用户与云服务端之间的安全访问控制模型以及相互信任关系，并在此基础上实施云计算环境中基于行为互信任的动态角色访问控制。主要研究内容有以下 6 个方面。

（1）将 BLP 模型与 Biba 模型通过访问控制有机结合，各取其优点，提出了一种保护云端服务器中数据的保密性和完整性的云计算访问控制安全模型，即 CCACSM 模型。该模型主要继承了 BLP 模型的简单安全属性和*属性公理，以此加强数据的保密性；并且结合 Biba 模型的严格完整性策略来保证数据的完整性。

（2）针对现有云计算系统虚拟机间信任链传递方案的不足，结合横向和纵向信任传递的研究，提出了一种复合动态信任链模型。通过度量交互方和当前行为的可信性来保证虚拟机的完整运行。通过对交互虚拟机的完整性度量，实现纵向的信任链传递，来保障信息流入的虚拟机是可信的；在虚拟机之间通过基于行为的度量方式，实现横向的信任传递，保障虚拟机信息源本身的完整性，确保输出可信。

（3）提出了一个基于信任证据—信任属性—信任值三级结构的用户行为信任层次模型。在该模型中，首先搜集用户的历史行为信息作为原始信任证据；然后对原始信任证据进行划分，按照其属性特征将其划分到不同的行为信任属性集中；最后根据用户的各个行为信任属性及权重计算出用户行为信任评估值。

（4）设计了一个基于蚁群优化算法的云服务端信任评估模型。云计算中服务节点的信任评估应充分考虑用户对云服务端的信任随着交互次数以及时间的变化关系，该模型利用蚁群优化算法引入信任信息素作为判断服务节点的信任依据，在云计算环境中建立了一种动态且随时间和交互事件变化的节点行为信任模型，从而计算云服务节点的信任度，为用户推荐更加可信的云服务节点。

（5）提出了一种云计算环境下基于行为互信任的动态角色访问控制方法（MTBAC）。本书分别从模型的定义、框架结构、算法流程以及多域授权决策机制等方面对 MTBAC 进行了详尽的定义与介绍。MTBAC 充分结合 RBAC 模型的优势，并综合考虑云计算环境动态性、多域性的特点，在用户与云服务端相互信任的基础上，实施云计算本地域和跨域的动态角色访问控制策略。

（6）设计两组仿真实验对 MTBAC 的性能进行比较和分析。通过与其他访问控制方法对比，验证基于信任的访问控制方法在云计算环境中的有效性和适用性；通过云计算用户与云服务端双向信任与单向信任的对比实验，分析基于双向信任的访问控制的相对优势。

本书的组织结构如下。

第 1 章：绪论。介绍本书的研究背景及意义，并讨论国内外对云计算及其安全、信任模型、访问控制的研究现状，并指出信任管理与访问控制相结合形成的基于信任的访问控制模型在云计算环境中应用的研究现状及意义。

第 2 章：信任模型及访问控制方法。介绍信任模型的相关概念并分析比较几种典型的信任模型及其优缺点；给出访问控制策略定义以及典型访问控制模型的优缺点分析，为后续的研究工作奠定了

理论基础。

第 3 章：基于行为的云计算访问控制安全模型 CCACSM。以 BLP（Bell-LaPadula）模型和 Biba 模型为参考，通过基于行为的访问控制技术来动态调节主体的访问范围，实现 BLP 模型和 Biba 模型的有机结合，提出了 CCACSM 模型。该模型不仅能保护云端服务器中数据的完整性和保密性，而且使云计算环境具有相当的灵活性和实用性。最后给出了该模型的组成部分、安全公理和实现过程。

第 4 章：云计算中虚拟机间复合动态信任链模型 MDTCM。分析云环境下虚拟机同驻威胁，提出 4 种安全要素。为了保障安全要素，提出了一种复合的动态信任链传递模型。通过度量交互虚拟机和当前行为的可信性来保障系统的动态可信。在虚拟机监视器中设计了一个信任链构建模块，通过动态监控，达到控制信息流的目的。

第 5 章：云用户行为信任模型。提出云计算用户行为信任层次分解模型，从用户行为信任证据的获取、规范化处理、信任属性的划分以及信任度的计算等方面展开用户行为信任的分析与研究。

第 6 章：云服务端信任评估模型。结合蚁群优化算法，在云服务端行为信任评估中引入信任信息素的概念，并根据节点的历史交互行为和服务质量等因素，预测云服务节点未来的服务行为是否可信。

第 7 章：云计算环境下基于相互信任的访问控制方法。结合第 5 章的云用户行为信任模型和第 6 章的云服务端信任评估模型，提出基于用户与云服务端相互信任的访问控制方法 MTBAC，给出了互信机制的定义与形式化描述，并提出了基于相互信任度的访问控制算法和多域授权决策机制。

第 8 章：模拟实验及性能分析。通过两组模拟实验分别验证信任模型应用于云计算系统的优势以及 MTBAC 的性能与效率。

参加本书部分文字编撰和相关实验工作的还有贺珊、别玉玉、朱洁、唐乾，这里对他们的辛苦工作表示感谢。

云计算环境是一个发展迅速的计算平台，很多方面还在不断完善和变化。由于能力和水平所限，虽然竭尽全力，但仍然难免存在错误和疏漏，希望各位专家、读者批评指正。

作者

2016 年 10 月 10 日于徐州

目 录

第1章 绪　论

1.1 研究背景及意义

云计算作为一种新兴的计算模式，由分布式计算、并行计算、网络存储、虚拟化等技术相互融合发展而来，体现了“网络就是计算机”的基本思想。云计算将网络中的大规模资源集中并连接在一起，形成虚拟化的计算资源池（也称作“云”），为用户提供规模庞大的云服务[1,2]。云计算技术的运用代表超级计算能力，可以像商品一样在“市场”上流通，只不过这里的“市场”特指网络，即Internet。鉴于云计算的一系列优势，近年来，云计算在计算机网络与信息技术领域的发展如火如荼，其应用前景也极其诱人，无论是大型 IT 公司（如谷歌、亚马逊），还是小型信息科技公司，无不把云计算纳入企业的未来发展战略。著名的信息技术研究和分析公司Gartner 在分析报告中指出，云计算将取代现有的虚拟化技术，成为最重要的技术趋势。

目前云计算的发展也面临着很大的挑战。尽管云计算的诸多优势已得到业界认可，但要将企业的机密信息及重要业务存入云

计算平台，还需要很大的勇气，云安全问题是首先需要考虑的问题。如果云计算安全问题不能得到妥善解决，云计算将很难得到用户的认可，云计算技术及业务的进一步发展将举步维艰。最初的云计算应用范围较窄，开放性不强，因此最初的设计者对安全问题的考虑不够充分、全面，仅依靠防火墙、访问控制等基本的安全防护措施，大部分云安全问题就可得到有效的解决。但随着云计算的发展壮大，云计算资源越来越多地被暴露在因特网之下，受到攻击的次数和规模呈指数递增，因此其安全模式由传统的封闭式安全访问控制逐渐转变成动态、开放的安全控制策略。云计算中数据的安全、用户隐私保护等所构成的安全问题，直接关系到云计算的进一步发展。云安全事件的频繁发生使其稳定性、安全性、完整性、可信性等都成为亟待解决的问题。面对这些问题，传统的企业内部数据保护策略已经不再适用。如何保证云用户行为以及云服务端的安全可信性，是云计算迫切需要解决的核心问题之一。

云计算以其超大规模、虚拟化、高可靠性的独特优势引发了计算机网络变革，然而频繁出现的云安全问题却给云计算的前景蒙上了一层阴影。“云”中集结了网络中的大规模计算资源、软件资源及存储资源，然而要实现资源的安全共享，访问控制问题必须得到有效解决。对于每个用户来说，在对方身份未知的情况下要求进行协同，存在很大的风险性，因为该用户可能是一个善意的用户，也可能是一个恶意的用户。因此，在云计算环境下制定安全可靠的访问控制策略就变得格外重要。早期的访问控制技术不仅能够防止非授权用户的入侵，保证合法用户的正常访问，而且可以解决由合法用户的误操作所引起的安全问题。但传统的访

问控制是一种集中且封闭式的基于身份的访问授权技术，仅能够解决单个域中的安全问题。云计算既然是通过网络中的虚拟资源池提供服务，各资源主体往往不属于同一安全管理域，同时云计算的网络覆盖范围极广，因此云计算具有跨域性、动态性等。而传统的基于身份的访问控制技术显然已经无法满足云计算的安全需求。当前最有效的方法就是在传统访问控制的基础上进行改进与拓展，进而适应云计算的安全新需求。如何将传统的访问控制技术扩展更新以适应新的安全需求，解决云计算平台下的安全问题是当前研究的一大热点，也是云计算环境下访问控制技术的重要内容。

目前，云计算中的访问控制技术主要是IAM（Identity and Access Management）技术，但 IAM 技术并未考虑云计算的多域性特点，不能很理想地解决云计算中跨域访问控制与授权问题。实施云计算环境下的跨域访问控制、信任问题是云计算安全访问控制的核心。1996 年，Blaze 将人类社会中人与人之间的“信任”关系应用到计算机领域，提出要对“信任”进行管理，这为解决云计算环境中的安全问题提供了一条新思路，即在信任管理的基础上，把信任机制引入到访问控制技术中，给出信任的定义与计算方法，并将这种拓展的访问控制模型植入云计算平台进行研究。由于信任的动态性，信任计算是一大难点。

建立云用户与云服务端之间的相互信任关系是云计算安全问题得以解决的关键因素。因此，本书主要研究云计算环境中的相互信任关系以及在此基础上进行的动态访问控制策略，进而解决云计算安全的基础性问题。在云环境下进行基于相互信任的访问控制的研

究具有重要的应用前景和理论价值，构建安全可靠的访问控制方法与高效灵活的访问控制机制，对提高云计算环境的系统安全性，控制用户对云计算平台的安全访问，都具有十分重要的意义。

1.2 国内外研究现状

1.2.1 云计算及其安全

广义的云计算是指“服务”的使用和交付模式，包括软件即服务（SaaS，Software as a Service）、平台即服务（PaaS，Platform as a Service）和基础设施即服务（IaaS，Infrastructure as a Service）3 种使用交付模式。狭义的云计算是指 IT 基础设施的使用和交付模式，指通过互联网获得所需的云计算资源与服务，包括云计算平台、软硬件及互联网、IT 服务，提供云计算资源与服务的网络统称为“云”。“云”中的资源在使用者看来是可以无限扩展的，并且可以随时获取、按需使用、随时扩展、按使用付费。云计算服务的特征如图 1-1 所示[3]。

云计算平台就是链接了超大规模的网络资源与服务的“云”，这种“云”网络无论是超级计算能力还是提供服务的能力都十分强大，利用虚拟化技术，每一个链接到云计算平台的服务器功能都得到极大的扩展，可以共同完成超级计算以及大规模存储等任务。云计算的系统架构模型[4]如图 1-2 所示，其体系结构主要包括为用户提供接口的云用户端，云用户端会为用户展示云计算平台所能提供的服务目录，还包括完成服务器集群虚拟化部署的部署工具，以及完成云服务及资源管理的管理系统和资源监控系统等。

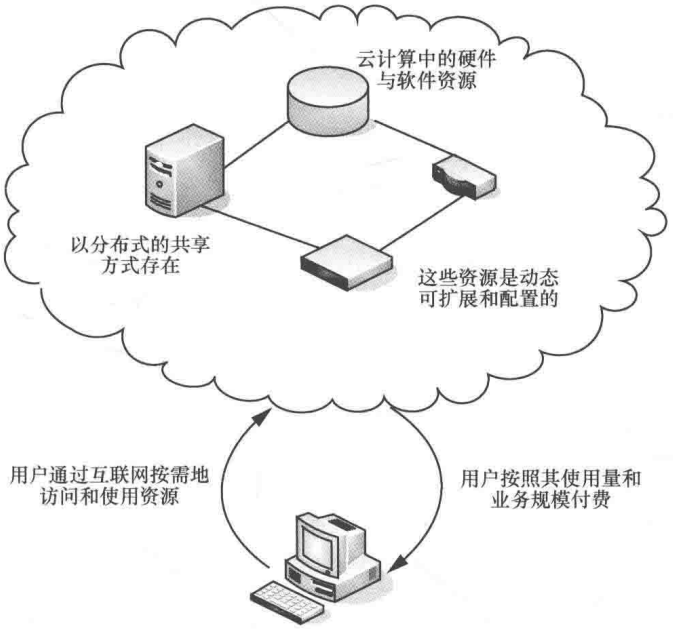


图 1-1 云计算的特征

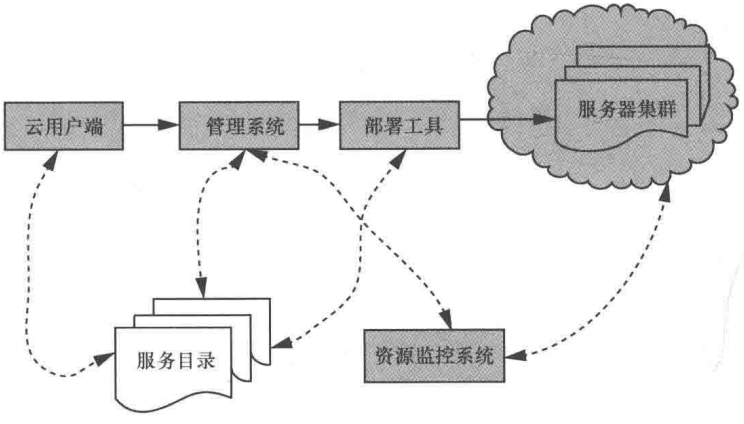


图 1-2 云计算系统架构模型

云计算是一种新型的计算模式，通过互联网以服务的形式为用户提供动态、可伸缩的虚拟化计算资源，为 IT 的发展带来新的转机。

云计算不仅具备高性能的服务、无限的存储容量，而且还具有兼容性强、扩展性好、维护成本低的特点，因此云计算竞争优势显著，市场前景广阔[5]。尽管如此，随着安全问题的暴露，云安全成为制约云计算发展的重大挑战。

云计算通过互联网提供服务，因此，互联网的开放性和不确定性必然导致云计算面临一系列安全问题。Patterson 在伯克利云计算白皮书中总结出了云计算将会面临的十大安全挑战，其中，数据的安全性、服务的可用性、性能的不可预知性、大规模分布式系统的安全漏洞以及声誉危机等，都与云计算的保密性和可靠性相关[6]。基于对云平台和云数据中心安全性的考虑，很多企业和用户对是否采用云计算仍然存在顾虑和担忧。

国内外在云计算安全部署方面已有很多成功的案例，如 Amazon 的弹性计算云（EC2）提供多层次的安全机制，保证 EC2 上的数据不会被未授权的用户非法截获，同时在确保用户使用灵活性的基础上适当进行相关的安全部署。另外，Google Apps 采用对网络的安全进入设置限制的方法进行安全防护。但由于云计算架构规模庞大，一旦发生故障将会损失惨重，同时还会“树大招风”成为诸多攻击者的攻击目标。

目前解决云计算安全问题的关键在于针对特定的安全风险建立可行的云安全框架，并运用该框架结合关键安全技术展开研究。信任机制的引入给云计算的安全可信性带来了转机。针对云平台的可信性，Hyukho 等[5]通过分析云平台中节点的历史记录信息，建立信任模型，通过信任计算对节点的性能和可信度进行排序，从而找到最优节点。当用户发送云服务请求时，云平台使用当前最优节点为