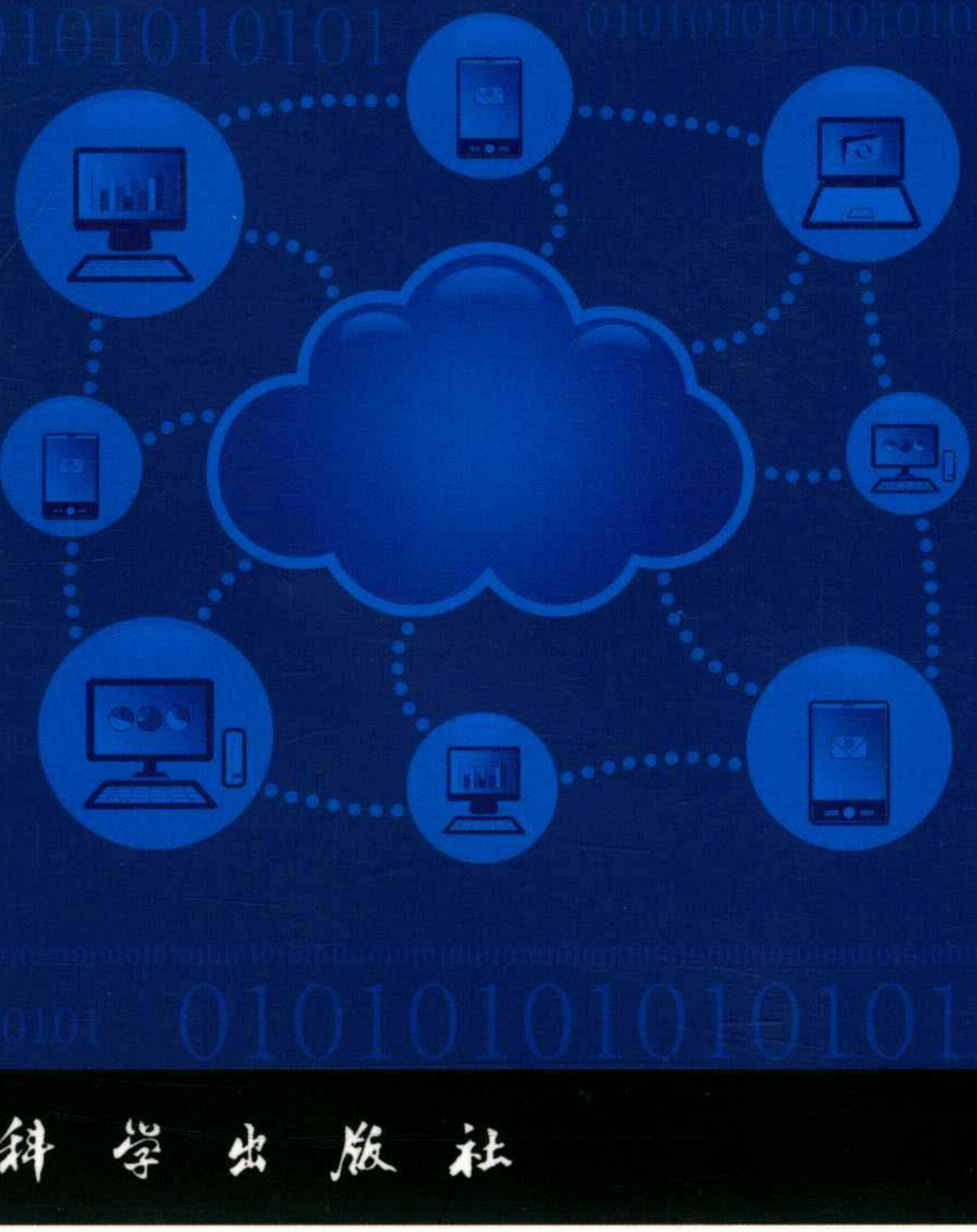
面向云计算环境的访问控制技术

王静宇　顾瑞春　著



科学出版社

面向云计算环境的访问控制技术

王静宇　顾瑞春　著

科学出版社
北京

内 容 简 介

本书以云计算环境下的安全访问控制技术研究为主线，在梳理访问控制技术研究现状的基础上，系统阐述云计算环境下与安全访问控制技术相关的模型、算法及技术等。

全书共分 12 章，主要内容包括云计算访问控制技术研究背景及面临的问题与挑战，访问控制技术相关研究现状与进展，基于信任和隐私及属性标签的访问控制，基于信任评估的属性访问控制优化技术，云环境下一种基于资源分离的 ATN 模型，云环境下基于神经网络的用户行为信任模型，云计算环境下基于 RE-CWA 的信任评估，基于 CP-ABE 的多属性授权中心的隐私保护技术，基于多 KGC 和多权重访问树的属性访问控制方案，无可信第三方 KGC 的属性加密访问控制技术，一种基于 WFPN 的云服务选择方法，基于 PBAC 和 ABE 的云数据访问控制研究。

本书可作为高等院校的信息安全、网络空间安全、计算机科学与技术等相关专业的研究生指导用书，也可供从事与云计算安全相关的科研人员和技术人员参考。

图书在版编目 (CIP) 数据

面向云计算环境的访问控制技术/王静宇，顾瑞春著. —北京：科学出版社，2017.5

ISBN 978-7-03-052177-4

Ⅰ. ①面… Ⅱ. ①王… ②顾… 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(2017)第 054675 号

责任编辑：王 哲 邢宝钦 / 责任校对：郭瑞芝

责任印制：张 倩 / 封面设计：迷底书装

科 学 出 版 社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

文林印务有限公司 印刷

科学出版社发行 各地新华书店经销

*

2017 年 5 月第 一 版 开本：720×1 000 1/16

2017 年 5 月第一次印刷 印张：13 1/4

字数：266 000

定价：79.00 元

（如有印装质量问题，我社负责调换）

前　言

云计算是一种新的应用模式，具有多租户、灵活快速和易扩展等特点，它能够显著降低运营成本和提高运营效率，已受到企业界和学术界的广泛关注。云计算的出现催生了很多新型的产业和服务，其在更有效地提高人类感知和认知社会能力的同时，也将对信息社会的发展和进步产生深远的影响。但随着云计算技术的不断发展，安全与隐私问题已经成为云计算应用的最大障碍。近年来，相关云计算调查也证明了安全与隐私问题是用户最关注的，因此，如果不能处理好云安全与隐私保护问题，那么云计算技术将无法真正大规模应用。

云计算环境下访问控制技术作为保护云服务及数据访问时的重要措施和手段，其作用至关重要。云计算环境构成复杂，如访问者要访问云资源或者云服务，其所处的环境、时间、访问时的动作及对资源的信任状况等因素对于现有的访问控制模型来说很难完全适用，因此需要不断探索研究新的访问控制技术来满足云计算环境的复杂访问控制要求。本书以云计算环境下的访问控制技术研究为主线，综合作者多年在云计算访问控制方面的研究成果，系统阐述了云计算环境下的访问控制技术的相关理论与方法，实现云资源访问者与云资源及云本身等多方之间的安全访问控制等。

全书共分 12 章。

第 1 章　引言部分介绍云计算研究工作的相关背景，提出云计算环境下访问控制技术存在的问题与挑战，并介绍本书的主要研究思路与工作。

第 2 章　介绍访问控制技术有关的国内外相关研究的工作现状与存在的问题，包括基本访问控制、属性访问控制模型、云计算环境下的访问控制技术以及基于属性加密的访问控制技术等。

第 3 章　在云计算环境各实体对细粒度安全访问、保护隐私等需求的基础上，设计面向信任和隐私的细粒度属性访问控制模型，内容包括模型架构、相关属性形式化定义、跨逻辑安全域及本地安全域访问、策略合成与评估、隐私与信任的引入和实验仿真与模型验证。

第 4 章　针对云计算环境中存在的各实体间信任问题，提出基于信任评估的属性访问控制优化技术。详细描述信任计算模块框架结构、工作流程以及信任相关概念定义等。将得到的实体总体信任度作为访问控制的关键属性之一进入下一步的访问控制决策，通过仿真实验验证其能提升属性访问控制的精准度和安全能力。

第 5 章　针对云计算环境下大量不符合条件的用户与资源拥有者进行自动信任协商，提出一种云环境下基于资源分离的自动信任协商模型。该模型在云环境下分离资源拥有者及其资源，使资源访问者不能直接与资源拥有者建立关系。

第 6 章　运用神经网络理论对信任进行建模，在相识社区的基础上，完成推荐信任的计算，并采用 RBF 神经网络的惩罚项理论解决恶意推荐问题。仿真实验模拟云环境下网格节点文件下载服务。为云环境下网格用户的行为信任研究提供新的思路。

第 7 章　主要针对用户行为信任的评估研究，对于云计算开放环境下的安全问题，本章有效分析用户的不可信行为和异常行为，结合主观和客观赋权法的权重信息，选用基于相对熵的组合赋权法，弱化单纯使用一种权重计算带来的不合理性，对用户的信任度做出客观评价。

第 8 章　针对云计算环境下用户隐私保护的问题，采用多个属性授权中心代替单一中央授权服务器，避免由单一中央授权服务器引起的安全性问题，并且设计一种交互式的密钥生成算法，利用承诺方案和零知识证明方法实现用户密钥获取过程中用户的属性以及全局身份标识不被泄露。

第 9 章　设计基于多密钥产生中心和多权重访问权限树的细粒度云数据访问控制方案，内容包括方案系统模型、方案具体实现过程描述、方案的安全性分析等。最后通过相关的仿真实验以验证方案的效率和性能。

第 10 章　设计一种优化的无可信第三方密钥产生中心的 CP-ABE 方案，内容包括方案的系统模型、安全多方计算技术、方案具体实现过程描述、方案的安全性分析以及相关的仿真实验以验证方案的效率和性能。

第 11 章　为了提高云计算环境下用户与云服务间交互的成功率和用户的满意度，提出一种基于加权模糊 Petri 网(weight fuzzy Petri net，WFPN)的云服务选择方法，并通过实验仿真结果证明方法的有效性和可行性。

第 12 章　针对云计算环境下云数据库中个人隐私数据的不合理的访问以及关乎个人敏感信息泄露的问题，提出一种基于 PBAC(purpose-based access control)和 ABE(attribute-based encryption)相结合的云数据访问控制模型。加入属性目的集合概念和属性加密技术，使访问控制方案的运算效率得到提高。

本书所提到的理论符合当前云环境的发展要求，总结关于用户信任评估和细粒度访问控制的技术，并提出高效、快捷、安全的访问控制方案，适应当前云计算访问安全的发展要求。在对传统访问控制技术研究和分析的基础上，将基于属性的访问控制理论与方法和属性基加密技术等拓展应用在云计算环境下，并对其中的关键技术问题展开讨论，以希望能够协助构建高效的云计算安全访问控制机

制，为云计算下的安全技术研究提供新思路和理论依据，有助于推动云计算技术的应用推广。

本书主要由王静宇、顾瑞春等完成，是王静宇所属的云计算安全研究团队长期以来在云访问控制技术方面的研究成果。除了王静宇、顾瑞春署名作者以外，在编写过程中得到了谭跃生老师和工程训练中心韩艳老师的大力协助，此外，还得到了邢晨烁、魏立香、范文婕、宁宁、杨利辛、蒲晨旭、娄燕贺等硕士研究生的大力协助，他们为本书做出了巨大贡献，在此表示由衷的感谢！感谢科学出版社的大力支持，对本书出版的所有相关人员的辛勤工作表示感谢！

本书的出版得到了国家自然科学基金项目(61462069、61662056)、内蒙古自然科学基金项目(2015MS0622、2016MS0609)的支持和资助。

本书体现的是作者对于云计算环境下访问控制技术的相关研究成果，由于作者水平有限，书中难免有不妥之处，敬请各位读者批评指正。

作　者

2017 年 1 月

目　　录

第1章 绪 论

1.1 引 言

云计算是基于互联网的、新兴的网络计算模式[1-5]，通过虚拟化技术、分布式并行处理技术以及在线软件服务技术等将计算、存储、网络、平台等基础设施与信息服务抽象成可运营、可管理的超级云端资源池[6-8]，动态提供给用户，其基本技术架构如图 1.1 所示。

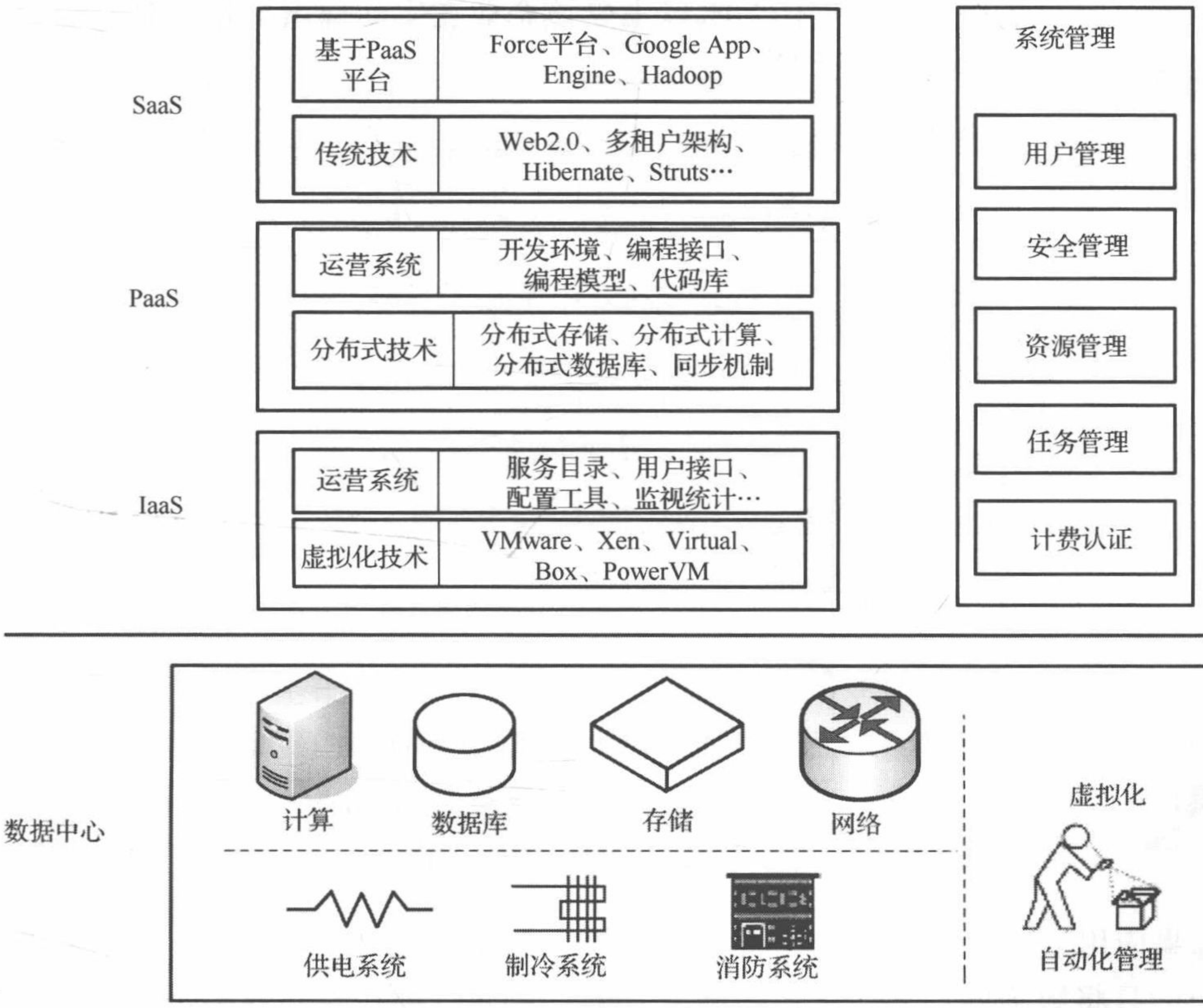


图 1.1 云计算技术基本架构

云计算通过提供超大规模的计算、存储及软件等云端资源池，为互联网用户

提供“招之即来，挥之即去”的 IT 服务[9]，包括软件即服务(software as a service，SaaS)、平台即服务(platform as a service，PaaS)、基础设施即服务 (infrastructure as a service，IaaS)等。SaaS 是面向最终用户提供在线软件服务，使用者可通过浏览器直接使用软件，无须执行安装、升级等维护工作；PaaS 是面向开发者提供开发环境、部署环境等平台级服务，开发者可基于 PaaS 平台快速开发并部署各种应用；IaaS 是将基础计算能力包括处理器、储存以及其他资源等作为一种资源向客户提供的服务。

云计算技术符合世界各国政府大力倡导和推动的低碳经济和绿色计算[10]的发展理念，已经成为互联网领域新的经济增长点，包括 Google、微软及亚马逊在内的大公司都开始研发自己的云计算基础架构及系统[11-15]。但是云计算本身在发展普及过程中也面临许多关键性问题，而首先是安全问题，并且呈现逐步上升趋势，已成为制约其发展的重要因素，2009 年 Gartner 针对云计算应用的调查结果如图 1.2 所示，这个结果表明有 70%以上受访企业在实际部署云计算时遭遇的最大挑战就是安全与隐私问题[16-18]。

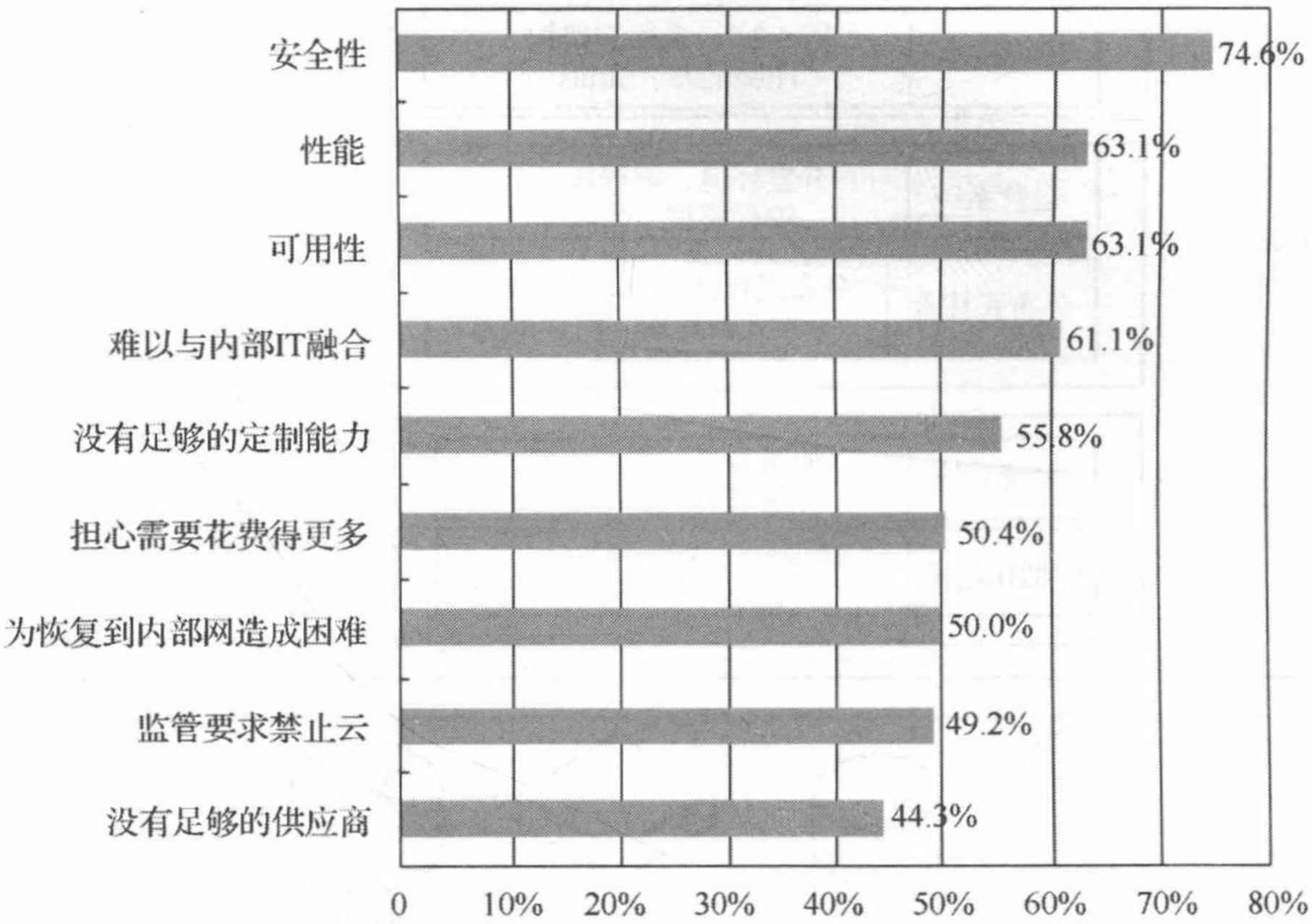


图 1.2　制约云计算应用因素的调查结果

如果应用云计算，则必然要将包含大量个人或企业的敏感信息转移到云中，即用户一旦将敏感信息存储在云端服务器中，这些数据和隐私等敏感信息便不在自己的掌控范围，数据安全问题必将引起用户的极大关注。云端服务器通常由商业云服务提供商运行操作维护，而这些云服务提供商通常属于用户外部的信任域，因此一旦敏感数据泄露，就可能造成重大经济损失或者灾难性后果等。例如，2009 年

Google 公司发生大批用户文件外泄事件和亚马逊公司所提供的云存储服务因安全问题一度被迫瘫痪等。另外，在一些实际应用系统中，数据保密性不仅只有安全及隐私问题，还可能涉及法律问题，这方面的典型是在医疗领域应用场景中，医院可能是云用户的同时自身还是内容提供商，在云服务器上发布数据，这些数据需要共享并且需要细粒度的访问控制，各用户根据自身对数据访问权限访问这些数据。例如，在医疗病例档案管理系统中，医院本身是数据拥有者，将成千上万份的各类患者医疗病历记录等存储到云服务器，这些数据需要允许数据消费者如医生、患者、研究人员等来访问各种类型的医疗记录，需要制定严格的、细粒度的访问控制策略。数据所有者一方面希望利用云计算环境所提供的丰富资源来提高效率和节省开销；另一方面也希望在云服务器上数据内容对云服务提供商来说是保密的，因此确保医疗数据机密性对云服务提供商来说是必须满足的基本要求。除了云用户自身对数据安全、访问安全的关注以外，一些有关安全事件的发生更加剧了人们对使用云计算服务的担忧。

由于云计算代表未来信息技术领域的核心竞争力，世界各国政府都大力推动本国云计算基础设施建设并开展学术研究，争取占据未来信息技术的制高点，随着各国云计算服务的大规模应用，要让个人、企业和组织等用户放心地将自己的数据交付于云服务提供商管理，就必须全面地分析并着手处理云计算所面临的各种安全问题，保护各类用户的数据安全和隐私信息。

虽然云计算作为一种信息服务模式，其安全与传统 IT 服务并无本质上的区别，但是云计算的应用模式和基础架构与传统 IT 有着很大的区别，使得云计算在安全技术应用上存在很大不同，例如，由于云计算模式下，信息应用系统高度集中、数据无边界、流动性等特点使得安全边界比较模糊，传统的安全域划分等安全机制难以保障云计算应用安全。云计算环境下的安全问题在很大程度上是由云计算本身的 5 个特征引起的[19]。

1)服务外包和基础设施公有化

在云计算环境下的应用模式采用的是服务外包模式，即数据拥有者把数据交由云端管理，这种公有化基础设施的特点使得云中的各租户无法直接控制和管理云端资源。

2)超大规模、多租户资源共享

云计算环境下，各类实体数量庞大繁杂且实体间关系非常复杂，甚至存在恶意或虚假的实体，不同用户的数据可能存放在同一云存储设备的同一物理磁盘上，云平台的这种多租户资源共享特征增加了安全访问控制的难度。

3)云计算环境的动态复杂性、多层次服务模式

对于基础设施即服务、平台即服务和软件即服务，云用户所需的具体执行环

境繁杂多样，需要动态定制和不断更新变化，导致云计算环境中各类云服务呈现多样性和动态性，难以评估其可信程度，进而使得云计算系统的安全难以保证。

4)云平台资源的高度集中性

云计算的应用模式决定了绝大多数资源都集中在几个云服务提供商平台中，也就是说，在这些云服务提供商的平台中含有海量云用户的隐私敏感信息，使得云平台变成攻击入侵或渗透的对象，安全风险不断加大。

5)云平台的开放性

云平台基本上都利用 VMware、Xen、KVM 等虚拟化管理软件构建而成，相关软件的安全漏洞频发导致系统平台安全隐患增大，另外，平台的开放性使一些存在安全漏洞的软件或恶意软件加入进来，进一步增加安全风险。

当然云计算环境的安全问题非常庞大复杂，任何单方面、单一技术手段无法真正解决云计算环境的安全问题，但从云计算大规模应用的数据拥有者角度来说，云计算的安全问题更多的是数据安全访问控制问题，现阶段有关增强云计算环境下数据安全访问控制的技术有以下几种。

(1)数据加密技术，对所有存储在云端服务器上数据进行加密存放，并保证数据的机密性、完整性和隐私，保证用户可验证和所有程序与应用系统的完整性。

(2)身份认证技术，通过提供强身份鉴别、授权和审计等来保证数据安全访问控制。

(3)可信云计算技术，基于云计算环境的复杂性，单纯使用软件很难解决所有的问题，因此可以利用硬件芯片和可信计算，在云计算环境中建立可信计算基(trusted computing base，TCB)来保护用户和云服务提供商的秘密信息，通过完整性度量、建立参与各方的身份证明和软件可信性证明来保证安全。

(4)安全增强加固技术，采用诸如改进虚拟机监控器(virtual machine monitor，VMM)代码，实现对虚拟化操作系统内核进行安全加固来保护计算或存储节点，实现对虚拟主机的保护和各虚拟主机之间的系统及数据隔离。文献[20]在虚拟机管理平台 Xen 中采用安全增强 TCB，并将这种方法用于实现可信虚拟化及提高虚拟 TPM 的安全性。

上述这些技术的应用对保证云计算环境中服务和数据的安全，推动云计算应用推广发挥了重要作用，但是在云用户通过云计算平台认证后的具体访问权限方面，还缺乏一些有效的理论模型。

在云计算环境中，云用户在访问云服务提供商的资源前，通常需要经过身份认证确认是合法用户后，才由云服务提供商进行授权，云用户对哪些资源和服务具有什么样的访问控制权限做出决定，但在实际的访问控制授权过程中，云服务提供方对某个云用户做出访问授权决定时，对这个云用户本身的具体情况并不了解，如

该云用户以前信用情况、历史访问记录、有没有过恶意攻击或其他不规范及不合理的行为等，通常都是在缺乏云用户的全部行为信息的情况下，仅根据云用户账号密码自主地做出相关访问控制授权决定的，而这将导致整个系统产生不确定性风险问题，进而可能对整个系统的安全稳定及可用性等产生很大的负面影响。

在云计算环境中，还缺乏一个权威管理中心，这个管理中心能够获得云用户、云资源等各类云主体的全部信息，使得在进行授权访问控制时，能够充分认识各类云主体，这样才能避免云服务或云资源请求者对授权者做出可能的攻击或者恶意破坏等行为。在现阶段，各类云计算环境中的资源及服务所有者都会有自己的安全规则和授权方式，并在其自身相对独立的环境中实现授权和访问。事实上，传统的访问控制机制[21]包括自主访问控制、强制访问控制和基于角色的访问控制模型等都是基于固定标识或身份的，传统访问控制模型中用户的权限多数情况下是静态不变的，适用于集中封闭式网络环境，不适用于具有开放性、共享性的云计算环境，也很难适应云计算环境中授权变化频繁的场景。开放共享的云计算环境在数据安全访问、精细访问控制和隐私保护等方面存在不足，原因如下：首先是云计算模式中传统架构的物理安全边界消失，而是以逻辑安全域的形式存在，云资源失去了物理边界处的安全防护控制，不同的服务提供者一般属于不同的安全域，交互的双方有时也经常处于不同的安全域，相互只知道对方的部分信息；其次在云计算环境中尤其是公有云环境，云用户的数量巨大，对云资源及服务的需求具有不确定性，云用户权限的授予和取消也是动态变化的，是粗粒度的管理，不能实现面向用户的精细访问控制；最后云计算属于多租户平台环境，需要对用户访问进行精确区分，以便更好地满足用户的服务需求，若要用类似基于角色的方法进行细粒度的访问控制，则需要定义大量的角色，这会给角色的分配和管理带来困难，另外，在基于角色的访问控制模型中，域间的互操作通常是利用角色映射完成的，但是在云计算环境下，不同的云服务提供者处于不同的逻辑安全域，很难建立这种角色映射关系[22]。

总的来说，最近几年云计算技术发展较快，在云计算安全研究方面也取得很多新的研究成果，如基于全同态加密技术的密文计算与检索技术、基于属性加密的访问控制技术以及可信计算技术等，但在安全云数据访问控制方面还存在很多尚未解决的问题，已有的一些安全技术在实践应用中的效果和性能还不能完全让人满意，阻碍了云计算技术的大规模应用和发展。

保护云数据安全的方法很多，本书主要侧重于通过安全访问控制技术，保护云服务不被非法访问和用户数据安全共享。研究云计算环境下安全访问控制技术，保护云实体的安全，避免由于云服务应用模式、虚拟化动态管理方式及跨安全域访问等带来的安全与隐私保护问题，对推动云计算服务的规模化应用具有重要的