

云计算:从云安全到可信云

吴吉义^{1,2} 沈千里¹ 章剑林¹ 沈忠华¹ 平玲娣²

¹(杭州师范大学电子商务与信息安全重点实验室 杭州 310036)

²(浙江大学计算机科学与技术学院 杭州 310027)

(Dr_PMP@yahoo.com.cn)

Cloud Computing: Cloud Security to Trusted Cloud

Wu Jiyi^{1,2}, Shen Qianli¹, Zhang Jianlin¹, Shen Zhonghua¹, and Ping Lingdi²

¹(Key Laboratory of E-Business and Information Security, Hangzhou Normal University, Hangzhou 310036)

²(School of Computer Science and Technology, Zhejiang University, Hangzhou 310027)

Abstract Cloud computing, with exciting market prospects, has a number of potential risks and safety issues to the cloud services users. After an objective analysis of the security challenge and problem, in current cloud computing development, the latest research progress in the field of cloud security were summarized. Finally, the important research directions in the field were pointed out. It's will be a new trend for the cloud computing and trusted computing technology to integrate.

Key words cloud computing; cloud security; trusted cloud; survey

摘要 虽然云计算产业具有激动人心的市场前景,但对于使用云服务的用户而言,云计算存在着多方面的潜在风险和各種安全问题.在客观分析了当前云计算领域发展中面临的安全挑战问题基础上,总结了云安全领域的最新研究进展,最后还指出了云安全领域的主要研究方向.云计算与可信计算技术的融合研究将成为云安全领域的重要趋势.

关键词 云计算;云安全;可信云;综述

中图法分类号 TP309

云计算是以虚拟化技术为基础,以网络为载体提供基础架构、平台、软件等服务为形式,整合大规模可扩展的计算、存储、数据、应用等分布式计算资源进行协同工作的超级计算模式^[1].在云计算模式下,用户不再需要购买复杂的硬件和软件,而只需要支付相应的费用给“云计算”服务提供商,通过网络就可以方便地获取所需要的计算、存储等资源.对于该定义需要特别说明的是,云计算的一个重要价值是软硬件需求的按需扩展能力^[2],完全脱离“本地”计算、数据资源的云计算只是一种比较理想的状态,考虑到私有云、遗留系统、可靠性、安全性等因素,云

计算具有整合资源按需扩展方面的特殊意义.

根据国际数据公司(IDC)的预测,全球云计算的市场规模将从2008年的160亿美元增加到2012年的420亿美元^[3],占总投入比例也将由4.2%上升到8.5%.此外,根据预测,2012年云计算的投入将占IT年度投入增长的25%,而到2013年则会占30%以上.全球最具权威的IT研究与顾问公司甘特纳(Gartner)的数据分析则认为2009年云计算市场收入增加20%以上,超过560亿美元;而投资机构美林集团(Merrill Lynch)则认为云计算在2011年将会有1600亿美元的市场.每个公司基于不同

收稿日期:2010-12-10

基金项目:国家自然科学基金项目(61070153);浙江省教育厅科研计划基金项目(20071371);浙江省自然科学基金项目(Y1080831)

的云计算定义和理解,这也解释了市场规模和估价的差异.云计算技术的出现使得人们可以直接通过网络应用获取软件和计算能力,这一新的模式将会给传统的 IT 产业带来一场巨大的变革,云计算正在成为一种发展趋势.

虽然云计算产业具有巨大的市场增长前景,但对于使用云服务的用户而言,云计算存在着多方面的潜在风险和各种安全问题.在客观分析了当前云计算领域发展中面临的安全挑战问题基础上,总结了云安全领域的最新研究进展,最后指出了云安全领域的主要研究方向.云计算与可信计算技术的融合研究将成为云安全领域的重要方向.

1 安全问题成为领域发展的最大挑战

近两年来,云服务提供商频频出现各种不安全的事件.2008 年 2 月 15 日 Amazon 出现了网络服务宕机事件,使得几千个依赖亚马逊的 EC2 云计算和 S3 云存储的网站受到影响,其中包括 Twitter, SmugMug, 37Signals 和 AdaptiveBlue 等.2009 年 2 月 24 日,谷歌 Gmail 邮箱爆发全球性故障,服务中断时间长达 4 h.此次故障是由于位于欧洲的数据中心例行性维护,导致欧洲另一个数据中心过载,连锁效应扩及其他数据中心,最终致使全球性断线.2009 年 3 月 7 日,Google 发生了大批用户文件外泄事件.2009 年 3 月 15 日,微软的云计算平台 Azure 停止运行约 22 h,微软至今没有给出详细的故障原因.2009 年 6 月 11 日,Amazon 的 EC2 中断了几个

小时,原因是雷击损坏了公司数据中心的电力设备,造成一些 AWS 客户服务中断.2009 年 7 月 19 日,亚马逊云计算服务网络服务再次中断.

云计算在极大地方便用户和企业廉价使用存储资源、软件资源、计算资源的同时,面临的最大挑战或者说存在的问题来自安全方面.文献[4]总结的云计算十大问题与机会,如表 1 所示.其中服务可用性(availability of service)、数据防丢失(data lock-in)、数据保密性和可审计性(data confidentiality and auditability)、数据传输瓶颈(data transfer bottlenecks)、性能不可预知性(performance unpredictability)、大规模分布式系统中的漏洞(bugs in large-scale distributed systems)、声誉共享(reputation fate sharing)等都与保密性和可靠性相关.文献[1]也提出云计算必须妥善解决安全(security)、数据和应用的互操作(data and application interoperability)、数据和应用可移植性(data and application portability)、治理和管理(governance and management)、计量和监测(metering and monitoring)5 项挑战,否则将影响其实现承诺.国内“计世资讯(CCW Research)”发布的《2009 中国云计算发展状况白皮书》^[5]也指出“云计算技术的稳定性、可靠性和安全性如何”是当前国内用户对云计算的主要顾虑之一.惠普的云计算专家 Goldsack 等人^[6]也认为:云计算基础设施服务必须具备隐私性和安全性、服务质量和性能保证、灵活性、向上和向下的可伸缩裁剪性以及故障恢复能力等一些特定属性,才能够满足企业级的要求.

表 1 云计算发展的十大问题与机会

No.	问题(obstacle)	机会(opportunity)
1	服务可用性(availability of service)	选用多个云提供商;利用弹性来防范分布式拒绝服务(DDoS)攻击
2	数据防丢失(data lock-in)	标准化的 API;使用兼容的软硬件以进行波动计算(surge computing)
3	数据保密性和可审计性 (data confidentiality and auditability)	采用加密,VLANs 和防火墙技术;针对跨地域数据存储的法律调整
4	数据传输瓶颈(data transfer bottlenecks)	快速硬盘;数据备份/存档;更低的广域网路由成本;更高带宽的 LAN 交换机
5	性能不可预知性(performance unpredictability)	改进虚拟机支持;闪存;支持 HPC 应用的虚拟机组调度
6	存储可扩展性(scalable storage)	研发可扩展存储系统
7	大规模分布式系统中的漏洞 (bugs in large-scale distributed systems)	研发基于分布式虚拟机的调试工具
8	快速扩展(scaling quickly)	研发基于机器学习的自动扩展技术;使用快照实现低成本资源保护
9	声誉共享(reputation fate sharing)	提供类似 Email 的声誉保护(reputation-guarding)服务
10	软件许可(software licensing)	付费使用(pay-for-use)模式许可;批量销售

2 云安全领域的研究进展

由于整个云计算领域的研究刚刚起步,有关云安全(cloud security)的研究还非常少,云安全的基本概念或界定也还比较模糊混乱. RSA^[7], Gartner^[8], CSA^[9], SUN^[10], IBM^[11]等组织在云计算领域的最新研究对云安全管理与技术的发展具有积极意义. RSA 在其云计算安全白皮书中,列举了在供应商管理、技术标准、数据可迁移性、数据机密与隐私、访问控制、符合性、以及安全服务水平等方面的安全度量指标,并总结了基础设施(infrastructure)、身份(identity)、信息(information)等 3 大类云计算安全要素. RSA 实验室(RSA Laboratories)的 Bowers 等人^[7]还提出了一种高可靠性、完整性云存储模型 HAIL,并进行了安全性和效率方面的实验.

2008 年 7 月,国际研究机构甘特纳(Gartner)发布的一份名为“Telework in the Cloud: Security Risks and Remedies”的报告^[8],也列举了云计算存在的特权用户的接入、可审查性、数据位置、数据隔离、数据恢复、调查支持、长期生存性等 7 大风险. 报告认为,云计算需要进行安全风险评估的领域包括数据完整性、数据恢复及隐私等. 此外,还需对电子检索、可监管性及审计问题进行法律方面的评价.

2008 年 10 月,IBM 发布的《新兴安全性技术趋势展望》白皮书^[11]概括了预计在接下来 2~5 年内将会影响安全性环境的九个重要的趋势和技术,其中排在第一位的趋势为“保护虚拟化环境的安全”. 具体包括对云计算环境中以下 3 方面问题的解决:①各组织(云服务提供商)应该准备好强有力的单独管理功能,通过可在多个虚拟化平台间应用的分离策略,可以从其余用户中分离出专用于某个用户的应用、数据和基础设施;②应该像保护物理环境那样有力地保护和管理虚拟环境的完整性. 应该将网络监控和入侵防御等传统的安全性功能应用到虚拟环境中;③由于虚拟化资源是作为数据图像存储的,所以有可能遭到污染. 各组织应该建立图像管理功能,以保护并维护包括功能强大的变更和批处理管理程序等在内的资源定义.

2009 年 4 月,在美国旧金山的 RSA 大会上正式成立的云安全联盟(CSA)发布的一份名为“云计算关键领域安全指南(security guidance for critical areas of focus in cloud computing)”的报告^[9]提出了便携性与互用性(portability and interoperability),数据中心操作管理(data center operations),法规与审计

(compliance and audit),事件响应、告知与修复(incident response, notification, and remediation),应用安全(application security),加密与密钥管理(encryption and key management),身份认证与访问控制(identity and access management)等 15 个需要解决的领域(domain)安全问题. 全面概括了云计算用户和提供商必须解决的问题,涵盖了和云计算相关的法律、技术和管理等各方面问题.

云安全(cloud security)是一个综合的概念和问题,研究的是云计算过程涉及的环境(environment)、流程(process)、技术(technique)、管理(management)、服务(service)等各个层面的安全问题. 如果单纯从某一个层面如技术角度去定义,无疑是偏面的,不能从根本上揭示问题本质. 云安全领域研究工作的努力目标是达成安全云(secure cloud)或安全云计算(secure cloud computing),虽然这事实上是一个没有终点的方向.

目前,云服务商在信息安全的工作还非常有限. 一般只是对存储数据进行加密,使用 SSL, SSH 等安全协议保证数据传输安全和用户安全访问. 但是当用户数据在后端服务器的内存(RAM)中计算处理时,则必须是以明文的形式才能进行处理的,这为利用操作系统漏洞攻击载入内存中的数据提供了可能. 如何对内存数据进行保护和隔离将是云计算的重要安全需求之一.

文献[12]提出了如图 1 所示的安全云(secured cloud),其中公共云中用户的数据与其他组织的数据充分隔离存储,通过采用安全独立的云区域(secured & isolated cloud area)提供虚拟机资源保证高度隔离,最重要的是数据进行了由专家设计并测试的加密处理. 云服务商与组织内部的通信通过加密的 VPN 专用通道,符合用户组织安全策略设计的日志管理和资源安全管理措施. 此外,还包括可移植性(portability)、带管理的访问(administrative access)、安全性测试(testing)、透明度(transparency)、规范(compliance)等方面的要求.

数字化身份管理(digital identity management services)是云计算平台根据用户身份属性(identity properties)和历史记录(interaction histories)进行服务访问控制的重要措施,文献[13]一种基于身份特征、AgZKPK (aggregate zero knowledge proofs of knowledge)加密协议和语义匹配技术的解决方法.

文献中 EMC 毛文波等人^[14]有关云计算安全的

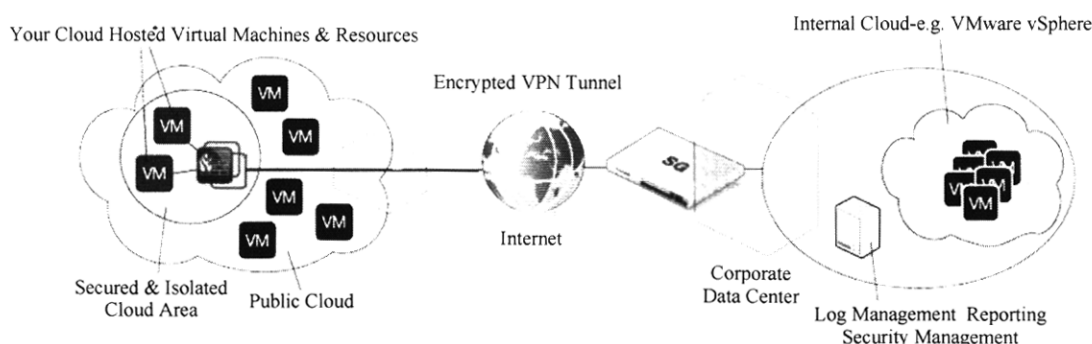


图1 安全的云

最新研究,是根据图2所示的面向服务的云计算架构从云计算前端(客户端、用户端)到后端(服务器端、数据中心)逐层进行分解展开的,非常有参考价值。

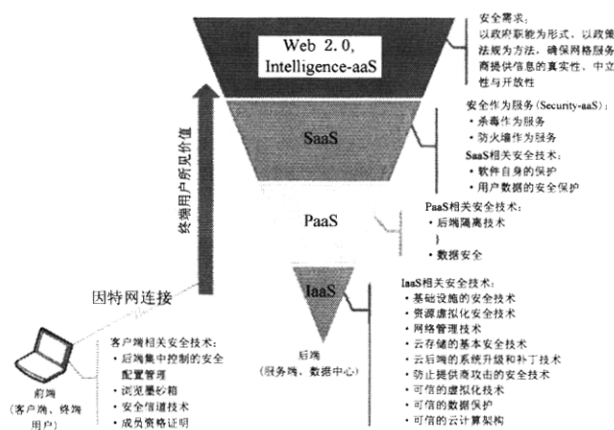


图2 面向服务的云计算架构及相关安全技术

Santos 等人^[15]设计提出了可信云计算平台(trusted cloud computing platform, TCCP), 包括一系列信任结点(N)、信任协调者(TC)、非信任云管理者(CM)和外部信任实体(ETE)等, 如图3所示。其中 TC 由一个特定的外部信任实体(ETE)维护。TCCP 通过提供黑盒(closed box)运行环境来保证客户虚拟机的安全, 同时还允许用户对安全性进行测试与验证。

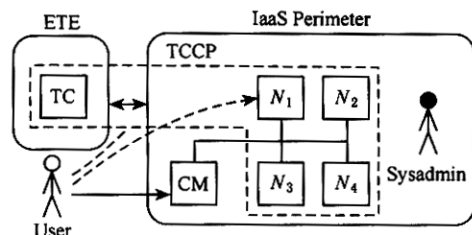


图3 可信云计算平台 TCCP

在国内,陈海波、臧斌宇等人^[16]从云计算平台的安全性、可维护性、可用性、可信性等方面进行了

“云计算平台可信性增强技术”的研究,很大程度上具有“开拓性”的意义。与华中科技大学(Huazhong University of Science and Technology)的金海教授等人^[17-18]在著作中提到的“安全可信的虚拟计算系统”的观点接近,文献[19]对虚拟化技术如何提升系统安全性进行了分析,提出虚拟化至少在3个方面对安全性提升具有不可估量的影响:①可以轻松隔离和屏蔽不稳定或具有安全隐患的应用程序;②可以支持提供高效的灾难恢复方案和健全有力的犯罪分析;③虚拟化还能提供更为廉价的人侵检测工具。

复旦大学(Fudan University)、武汉大学(Wuhan University)、华中科技大学(Huazhong University of Science and Technology)、清华大学(Tsinghua University)和 EMC 还联合启动了“道里”研究项目^[20],专门致力于云计算环境下关于信任和可靠度保证的全球研究协作,结合可信计算技术和硬件虚拟化技术实现用户可验证的安全应用隔离和行为规范,加强对云计算和云存储服务中的用户数字财产的保护。可信计算技术通过增强体系结构的安全来提高计算平台的安全性。从当前本领域研究的发展形式分析,云计算与可信计算技术的融合以更好解决云服务中的安全问题将成为一个重要方向。

3 结束语

云计算宣告了以设备为中心计算时代的终结,取而代之的是以互联为中心的计算模式。但是并非只停留在空中,靠哗众取宠来赢得赞誉。云计算使用户可以把计算处理工作的一部分甚至全部外包出去,信息部门不需要为公司服务器的维护配置专业技术人员,而是通过互联网来访问计算基础设施。一家大型云计算服务提供商能迅速满足各种客户对更多计算功能的需求,那些没有大型数据中心的中小

型企业也能够利用云计算服务提供商的强大处理功能,有效地降低 IT 成本。作为一项有望大幅降低成本的新兴技术,云计算正日益受到众多企业的认可。

从学术研究的角度,云安全领域亟待需要解决的问题包括:如何对存储数据、传输数据进行加密的问题;云计算中新加密算法的研究与算法更新换代问题;云服务应用程序组件间的身份验证问题;云计算平台安全性评估标准与应用;如何对有权访问异域云服务的用户以及访问方式进行管理;云服务应用程序接口的安全与访问控制问题;服务云计算需要的新一代网络安全技术;研究建立完善的云计算服务质量(QoS)体系;云计算与可信计算技术的融合研究。

云计算模式下,所有的业务处理都将在服务器端完成,服务器一旦出现问题,就将导致用户应用无法正常运行,数据无法访问。虽然解决云故障的时间一般并不长,然而足以作为一个对云计算的警示。毕竟云服务的规模都十分庞大,在出现问题之后,很容易导致网民对于云计算模式的怀疑,动摇用户对云服务的信心。由此可见,如果云计算的可靠性和安全性的软肋不能很好解决的话,云计算的普及仍有很长一段路要走。

参 考 文 献

- [1] 吴吉义,平玲娣,潘雪增,等.云计算:从概念到平台.电信科学,2009,(12):23-30
- [2] Open Cloud Manifesto. [2010-11-11]. <http://www.opencloudmanifesto.org>
- [3] Leavitt N. Is Cloud computing really ready for prime time? IEEE Computer, 2009, (1): 15-20
- [4] Armbrust M, Fox A, Griffith R, et al. Above the Clouds: A berkeley view of cloud computing. 2009 [2010-11-11]. <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>
- [5] CCW Research. 2009 中国云计算发展状况白皮书. 2010 [2010-11-11]. <http://www.tsinghuausa.org/W0509web/id0509/yun.pdf>
- [6] Goldsack P, et al. Cells-as-a-Service——一项云计算基础设施服务. 中国计算机学会通讯(CCFC), 2009, 5(6): 26-31
- [7] Bowers K D, Juels A, Oprea A. HAIL: A high-availability and integrity layer for cloud storage //Proc of the 16th ACM Conf on Computer and Communications Security. New York: ACM, 2009. <http://www.sigsac.org/ccs/CCS2009/>
- [8] Gartner. Teleworking in the cloud: Security risks and remedies. 2010 [2010-11-11]. http://www.gartner.com/resources/167600/167661/teleworking_in_the_cloud_sec_167661.pdf
- [9] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing, 2010 [2010-11-11]. <http://www.cloudsecurityalliance.org/guidance/csaguide.pdf>
- [10] SUN. 云计算架构介绍白皮书. 1 版. 2010 [2010-11-11]. http://developers.sun.com.cn/blog/functionalca/resource/sun_353cloud_computing_chinese.pdf
- [11] IBM. 新兴安全性技术趋势展望, 2010 [2010-11-11]. <http://www-935.ibm.com/services/cn/gts/pdf/ibm-tendency.pdf>
- [12] Clavister. Security in the cloud clavister white paper. 2010 [2010-11-11]. http://www.clavister.com/pdf/clavister-whp-security_in_the_cloud.pdf
- [13] Elisa Bertino, Federica Paci, Rodolfo Ferrini. Privacy-preserving digital identity management for cloud computing. Bulletin of the IEEE Computer Society Technical Committee on Data Engineering, 2009, 32(1): 21-27
- [14] 毛文波. 云计算安全, 2010 [2010-11-11]. <http://blog.pconline.com.cn/article/334526.html>
- [15] Santos N, Krishna P, Gummadi Rodrigo Rodrigues. Towards Trusted Cloud Computing. 2010 [2010-11-11]. http://www.mpi-sws.org/~gummadi/papers/trusted_cloud.pdf
- [16] 陈海波. 云计算平台可信性增强技术的研究. 上海: 复旦大学, 2010
- [17] 金海. 计算系统虚拟化: 原理与应用. 北京: 清华大学出版社, 2008
- [18] 石磊, 邹德清, 金海. Xen 虚拟化技术. 武汉: 华中科技大学出版社, 2009
- [19] 安全性: 虚拟化优势的另类解读, 2007 [2010-11-11]. <http://publish.it168.com/2007/0321/20070321007101.shtml>
- [20] Daoli, Daoli Trusted Cloud Infrastructure, 2009 [2010-11-11]. <http://www.daoliproject.org>

吴吉义 男,1979 年生,博士研究生,高级工程师,中国计算机学会高级会员、服务计算专委会、协同计算专委会。主要研究方向为云存储技术、电子服务。

沈千里 男,1978 年生,讲师,中国计算机学会会员。主要研究方向为云存储技术、电子服务。

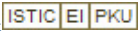
章剑林 男,1966 年生,教授,中国计算机学会会员。主要研究方向为分布式计算、电子服务。

沈忠华 男,1973 年生,副教授,硕士生导师,中国计算机学会高级会员。主要研究方向为密码学、电子服务安全。

平玲娣 女,1946 年生,教授,博士生导师。主要研究方向为新一代互联网络、网络信息安全。

作者: 吴吉义, 沈千里, 章剑林, 沈忠华, 平玲娣, Wu Jiyi, Shen Qianli, Zhang Jianlin, Shen Zhonghua, Ping Lingdi

作者单位: 吴吉义, Wu Jiyi (杭州师范大学电子商务与信息安全重点实验室 杭州 310036; 浙江大学计算机科学与技术学院 杭州 310027), 沈千里, 章剑林, 沈忠华, Shen Qianli, Zhang Jianlin, Shen Zhonghua (杭州师范大学电子商务与信息安全重点实验室 杭州 310036), 平玲娣, Ping Lingdi (浙江大学计算机科学与技术学院 杭州 310027)

刊名: 计算机研究与发展 

英文刊名: Journal of Computer Research and Development

年, 卷(期): 2011, 48(z1)

参考文献(20条)

1. 吴吉义;平玲娣;潘雪增 云计算:从概念到平台[期刊论文]-电信科学 2009(12)
2. Cloud Security Alliance Security guidance for critical areas of focus in cloud computing 2010
3. IBM 新兴安全性技术趋势展望 2010
4. SUN 云计算架构介绍白皮书. 1版 2010
5. Gartner Teleworking in the cloud: Security risks and remedies 2010
6. Bowers K D;Juels A;Oprea A HAIL:A high-availability and integrity layer for cloud storage 2009
7. Goldsack P Cells-as-a-Service-一项云计算基础设施服务 2009(06)
8. CCW Research 2009中国云计算发展状况白皮书 2010
9. Armbrust M;Fox A;Griffith R Above the Clouds:A berkeley view of cloud computing 2010
10. Leavitt N Is Cloud computing really ready for prime time[外文期刊] 2009(01)
11. Daoli Daoli Trusted Cloud Infrastructure 2010
12. Open Cloud Manifesto 2010
13. 安全性:虚拟化优势的另类解读 2010
14. 石磊;邹德清;金海 Xen虚拟化技术 2009
15. 金海 计算系统虚拟化:原理与应用 2008
16. 陈海波 云计算平台可信性增强技术的研究 2010
17. Santos N;Krishna P Gummadi Rodrigo Rodrigues. Towards Trusted Cloud Computing 2010
18. 毛文波 云计算安全 2010
19. Elisa Bertino;Federica Paci;Rodolfo Ferrini Privacypreserving digital identity management for cloud computing 2009(01)
20. Clavister Security in the cloud clavister white paper 2010

本文读者也读过(4条)

1. 曾文英, 赵跃龙, 尚敏, Zeng Wenying, Zhao Yuelong, Shang Min 云计算及云存储生态系统研究[期刊论文]-计算机研究与发展 2011, 48(z1)
2. 王意洁, 孙伟东, 周松, 裴晓强, 李小勇, WANG Yi-Jie, SUN Wei-Dong, ZHOU Song, PEI Xiao-Qiang, LI Xiao-Yong 云计算环境下的分布存储关键技术[期刊论文]-软件学报2012, 23(4)
3. 刘正伟, 文中领, 张海涛, Liu Zhengwei, Wen Zhongling, Zhang Haitao 云计算和云数据管理技术[期刊论文]-计算机研究与发展2012, 49(z1)
4. 杨健, 汪海航, 王剑, 俞定国, YANG Jian, WANG Hai-hang, WANG Jian, YU Ding-guo 云计算安全问题研究综述[期刊论文]-小型微型计算机系统2012, 33(3)