情报科学
第31卷 第1期 2013年1月

近四年来我国云安全问题研究进展

王　婷,黄国彬

(北京师范大学 管理学院,　北京 100875)

摘　要:运用科学计量学方法对2008年至2011年间有关云安全的期刊论文进行了统计,分别从文献数量、期刊分布、作者、研究主题等方面对我国云安全的研究现状进行了分析总结,结果显示,我国学术界对于云安全的研究主要集中在云安全定义、数据存储、数据传输等10个方面。文章归纳了现存的云安全风险及应对策略,并提出了优化云安全研究的建议 加强基础理论研究、注重创新思维、注重实证研究、加大政府应对策略的研究力度、重视对国外云安全的研究,为进一步研究云安全提供参考。

关键词:云安全 ;云计算 ;研究进展 ;科学计量学
中图分类号 :TP309　　文献标识码 :A　　文章编号 :1007-7634 (2013) 01-153-08

Research Progress of Cloud Security From 2008 to 2011 in China

WANG Ting, HUANG Guo-bin

(School of Management, Beijing Normal University, Beijing 100875 *, China)*

Abstract: The paper applied the scientometrics method to make a statistical analysis of the study of the cloud computing security study in China from 2008 to 2011.It analyzed the current research of cloud computing security study in China from the number of articles, the types of journals, the authors and the themes.The results show academic circles focused on ten subjects: cloud computing security definition, data storage, data transmission, etc. This paper summed up its existing problems and coping strategies, made recommendations to optimize cloud computing security study: strengthening basic theoretical study, emphasizing innovation, emphasizing empirical study, strengthening the research of the government 's coping strategies and attaching importance to cloud computing security study abroad. Those recommendations provide references for the further study.

Keywords: cloud security; cloud computing; research progress; scientometrics

2003年美国国家科学基金会投资830万美元支持的‘网格虚拟化和云计算VGrADS’项目正式启动了云计算的研发序幕,经过近十年的快速发展,云计算已经广泛地应用于医学、教育、金融、通信、企业内部管理等各大领域,并带来了巨大的经济效益和社会效益,但是随着云计算的普及,其安全问题也逐渐显现出来,并在一定程度上阻碍了云计算的进一步发展。在IDC(互联网数据中心)的一次关于‘用户认为云计算模式的调整和问题是什么’的调查中,安全性以74.6%位居榜首,可见,安全问题已经成为‘云计算’时代最需要破解的难题[1]。目前学术界正对此进行深入研究,笔者试图对现有的云

收稿日期 :2011-11-22
基金项目 :国家社科基金项目(11CTQ004)
作者简介 :王　婷(1986-),女,山西人,硕士研究生,主要从事数字图书馆、信息法学研究.

安全研究进行梳理和统计分析，以期对我国云安全研究的现状清楚地了解，为进一步研究云安全提供参考。

1 云安全文献统计分析

1.1 论文数量统计分析

笔者以CNKI(《中国期刊全文数据库》)为检索工具，使用‘题名=云计算 or 云服务 or 云安全 or 关键词=云计算 or 云服务 or 云安全 and 主题=信息安全’组合检索式，对2008年-2011年(截至2011年10月18日)四年来有关云安全方面的期刊论文进行了统计分析，共命中123篇，经认真筛选，选取了最相关的103篇论文。结果见表1。

表1 2008-2011年我国云安全研究论文年代表

年份	论文数(篇)	百分比(%)
2008	4	3.9
2009	15	14.7
2010	45	43.7
2011	39	37.9

从表1可以看出，我国云安全研究论文量呈上升趋势，这与我国云计算的进程有着密切联系，近几年，各种类型的云服务如电子邮件、网络硬盘、在线交易等越来越多的出现在人们的视野，其采用的分布式计算和虚拟化技术带给用户的便利、低廉等是无所能及的，然而相应的安全性问题也随之进入了用户的视角，如2008年亚马逊公司S3服务断网6小时，2009年Google Gmail云计算平台故障，微软的Azure云计算平台彻底崩溃等等，这些云安全问题给用户、企业、甚至国家带来巨大的损失，随着云计算应用的深入.云安全问题的重要性也在不断上升，其在一定程度上阻碍了云计算发展的进程，因而引起更多人的关注。

1.2 论文期刊分布统计分析

本文所统计的103篇论文分别发表在76种期刊上，其中仅刊载1篇的期刊有64种，占期刊总数的84.2%；刊载2篇的期刊有7种，占期刊总数的9.2%；刊载3篇及以上的有5种，占期刊总数的6.6%。载文量在2篇及以上的期刊有《信息安全与通信保密》、《信息网络安全》、《电脑知识与技术》等。详见表2。

从表2可以看出，云安全相关论文主要集中在计算机类期刊，其中前三位分别是《信息安全与通信保密》、《电脑知识与技术》、《信息网络安全》，载文量分别为7、6、6，分别占该研究领域总载文量的6.8%、5.8%、5.8%。其他相关领域的期刊虽然载文量较少，但并不表示该领域不重视云安全问题，以图书情报类期刊为例，载有云安全相关论文的期刊有《情报杂志》、《现代情报》、《情报科学》、《情报资料工作》、《图书馆学研究》、《四川图书馆学报》、《科技情报开发与经济》、《图书馆建设》，其载文量分别为1、1、1、1、1、1、1、2，这可在一定程度表明图书情报界的学者已经开始关注云计算带来的安全问题。

表2 载文量在2篇及以上的期刊统计

名次	期刊名	载文量(篇)
1	信息安全与通信保密	7
2	电脑知识与技术	6
3	信息网络安全	6
4	科技信息	3
5	中国金融电脑	3
6	电脑与电信	2
7	计算机安全	2
8	软件世界	2
9	图书馆建设	2
10	网络与信息	2
11	现代商贸工业	2
12	信息安全与技术	2

1.3 论文作者数量、机构统计分析

1.3.1 论文作者数量统计分析

本文统计了近四年来云安全研究论文的作者有104名，通过对论文作者发文量的统计分析，可以从中发现我国云安全研究领域的主要作者，详见表3。

表3 作者发文量统计

发文量(篇)	作者数(名)	所占比例(%)	作者
9	2	1.9	马晓亭；陈臣
3	11	10.6	张亚红、郑利华、邹国霞、艾铜青、段红、黄华、罗锋盈、宁家骏、杨新民、王燕、王煦
2	16	15.4	白洁、冯登国、韩永刚、兰天静、李遵富、罗忠、孙啸轩、应志鹏、吴珍、张冬青、张瑞平、陈雅娟、王小猛、胡庆平、赵玉科、周文豪
1	75	72.1	略

从表3可以得出，发文量在3篇及以上的有13位学者，仅占作者总数的12.5%。这说明我国云安全领域的核心作者仍未形成。

1.3.2 论文作者机构统计分析

通过对103篇文章作者机构类型的统计分析，发现有49篇论文的作者机构是高校院系，占全部论文的47.6%；有21篇论文的作者机构是科研机构，占全部论文的20.4%；有9篇论文的作者机构是图

书馆，占全部论文的8.7%；有11篇论文的作者机构是企业，占全部论文的10.7%(详见表4)。当前研究情况下，高校学者比科研机构研究人员更为关注云安全的问题。

表4　发文作者的机构分布情况

序号	机构类型	发文量(篇)	所占比例(%)
1	高校院系	49	47.6
2	科研机构	21	20.4
3	图书馆	9	8.7
4	企业	11	10.7
5	其他	21	20.4

1.4　论文主题统计分析

通过对检索到的103篇有关云安全研究方面论文的简单的阅读与整理，统计到10个集中的研究主题。通过分析可将这10个研究主题大致归为三类，云安全定义、云计算带来的安全问题及应对策略。我国学者对于云安全问题的研究主要集中在数据存储方面、数据传输方面、数据访问方面、服务方面、监管方面、法律法规方面，对于应对策略主要是从用户、云服务提供商、政府方面进行研究。各研究主题的论文数量分布详见表5。

表5　主要研究主题分布

序号	研究主题	论文数(篇)	所占比例(%)
1	云安全定义	13	12.6
2	数据存储	23	22.3
3	数据传输	13	12.6
4	数据访问	13	12.6
5	服务安全	5	4.9
6	服务监管	14	13.6
7	法律法规	11	10.8
8	用户应对策略	13	12.6
9	提供商应对策略	8	7.8
10	政府应对策略	5	4.9

2　云安全研究主题及研究内容

2.1　云安全的定义

云计算的出现使得人们可以随时随地通过网络获取各种软件服务和超大的计算能力，然而在其为用户提供廉价、便利、可靠的服务的同时也引起了一连串的质疑，如存储在云端的数据是否安全？会不会丢失?丢失之后能否快速完整的恢复?云服务提供商提供的服务是否可靠等，这些问题在一定程度上使得云计算的发展陷入了困境。在这一背景下，中国企业首次提出了“云安全”这一概念。2010年中国云计算调查中，对IT168旗下ITPUB、IXPUB和ChinaUnix三大社区论坛所广泛覆盖的中国IT专业技术应用人群进行了云安全认知调查，调查结果是65.1%的用户认为云安全是利用云计算技术提升企业信息安全；62.9%的用户认为云安全是将安全作为一种服务向用户提供，如云杀毒；54%的用户认为云安全是要解决云计算本身的安全性问题[2]。那么，到底什么是‘云安全’呢，目前学术界尚未达成一致的说法，大多数研究者认同一个观点，即云安全是网络时代的最新体现，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常检测，获取互联网中木马、恶意程序的最新信息，推送到Server端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端[3]。这样整个互联网就像一个庞大的杀毒软件，而且用户越多，每个用户就越安全，整个网络也就越安全。张亚红、郑利华、邹国霞用一句话总结了‘云安全’，他们认为云安全其实就是从传统的单机杀毒模式，转换成网络化的主动防毒模式[4]。瑞星安全工程师王占涛称[5]，在瑞星看来，整个网络就是一个云，而整个网络的安全，也就是云的安全。然而菲菲认为[6]，广义的云安全应该包括：用云计算保护用户安全；保护云操作系统的安全；解决‘云’的安全问题；在云里提供安全服务。

研究者在对‘云安全’概念的探讨中出现了争议，即‘云安全’到底是一种技术还是一种理念呢？对于此问题各个学者的看法不一。兰天静认为[7]，云安全不仅是一种全新的技术，而且也是一种全新的理念，使病毒防御从被动查杀转为主动防御，大大提高了病毒查杀能力和效率。趋势科技和绿盟则指出‘云安全’是一项新的技术，是一项革命性的技术颠覆[5]。韩立华、韩立宁、张亮等认为‘云安全’并不是一种安全技术，而是一种将安全互联网化的理念[8]。覃俊，黄力平也认同这个观点，同时，他们指出有必要区分‘安全云’和‘云安全’的概念。“云安全’只是一种理念，在业界有相当一部分资深人士认为‘云安全’原理上甚至只是分布拒绝式服务攻击或僵尸网络攻击的反其道而行之。而‘安全云’的概念和范围则要比‘云安全’要广得多，技术深度也不可同日而语；‘安全云’是完整的云计算环境中的信息安全体系，不仅是理念，还包括了各种管理标准、技术架构[9]。

笔者认为，从广义来讲，云安全就是云计算带来的安全问题，涉及数据安全、服务安全、政府监管、法律法规等多个方面。

有错误，本来就有主动防御的

2.2 当前有关云安全的主要研究角度

通过对检索到的有关云计算产生的安全问题的相关论文的阅读与分析，笔者总结出云安全问题主要集中在数据存储、数据传输、数据访问、服务安全、服务监管、法律法规等。

2.2.1 数据存储方面

我国学术界主要从数据存储、数据传输和数据访问三方面来研究数据安全问题。在数据存储方面，用户一旦把数据传输给云服务商，从本质上讲，就已不能完全控制对这些数据的自主处理。这就使得研究者不得不深思，把数据存储在“云”端会不会引起法律争议，数据会不会丢失、泄露，能否彻底地删除，丢失的数据能否快速完整地恢复，数据能不能进行有效的隔离等一系列的问题。

张亚红、郑利华、邹国霞非常重视数据存储安全，他们认为数据存储方面相应的安全机制有数据加密、数据隔离、数据校验、数据备份、灾难恢复[9]。马晓亭，陈臣则认为[10]，数据存储安全还应该包括数据删除及数据存储位置。这两种观点囊括了大多数研究者讨论的数据存储安全问题。刘猛[11]、郝文江[12]、叶加龙[13]、张公让[13]、文伟平[14]等研究者具体阐述了数据存储位置安全问题。在云计算模式下，用户一旦将数据存储在虚拟的数据中心，也就是“云”端，就已经不是事实上的数据拥有者和数据处理者，云服务提供商拥有甚至超过用户的权限，一旦这些权限失控，就会影响到用户的个人数据隐私。那罡指出[15]，数据能否彻底删除也会影响用户的个人数据隐私，由于服务商都会帮助备份，一张放到互联网上的图片被删掉之后还是可以被查到，隐私得不到很好的保证。

另外，在云计算模式下，用户的个人数据随机分布在不同物理位置的各个虚拟数据中心，此时，数据隐私保护面临不同法律体系争议。陈芸芸举了一个很好的例子[16]：当一家企业在英国处理数据后，将这些数据存储在爱尔兰的一个服务器上，但通过法国（因为在法国有分公司）来发送，在这种情况下，哪个国家的法律适用于争议的解决尚不明确。冯登国[17]、刘猛[11]葛慧[18]等阐述了数据隔离安全问题，在云计算模式下，用户的数据都存储于共享环境中，如果不能对用户数据进行有效的隔离，用户就不清楚自己的“邻居”到底是谁，有什么企图，会不会对自己造成伤害等，那么云服务提供商也就无法说服用户相信自己的数据是安全的。另外，如果发生重大事故时云服务商不能对用户的数据进行及时的恢复，云服务提供商也就无法使得用户相信自己的数据是安全的。

2.2.2 数据传输方面

在云服务中，数据传输高度依赖于网络设备，由于网络信息以二进制代码为载体，传输过程中，首先要将各种图文信息通过计算机设备转换为数字代码，然后通过传导线路进行传输，最后要通过计算机设备将数字代码还原成人们可以识别的图文信息，其中任何一个技术环节的缺失都会给用户数据带来安全风险。

几乎所有这一主题的研究者都认为黑客、病毒等是威胁“云计算”时代网络信息安全的致命因素。孙铁[19]、刘波[20]、刘楷华[21]、谢四江[22]、冯雁[22]、金志敏[23]等都在这个方面做了具体阐述，其中学者周昕的观点较有代表性，他指出早期的黑客侵入他人计算机的目的一般只是出于开玩笑或炫耀技术，而现代的黑客则更多地利用计算机网络的漏洞牟取不当经济利益或实现某种政治目的。周昕还概括了在“云计算”环境下，黑客侵犯网络隐私权的特征：侵权形式的多样化；客体的扩大化和数据化；侵权对象性质的双重化；侵权行为手段的智能化和隐蔽化；侵权后果的严重化和复杂化。他还指出在“云计算”时代，计算机病毒对网络信息获取的威胁十分巨大，一旦用户准备上传到“云计算”服务器的信息来源或传递中的信息感染上病毒，就会形成“多米诺骨牌效应”，不仅破坏“云计算”服务器的内部数据结构和硬件设备，导致信息无法被正常读取和运算，还会迅速扩散到与“云计算”系统相联接的其他用户的计算机系统，造成无可估量的损失[24]。

在数据传输安全方面，除了黑客、病毒等带来的安全风险，硬件系统也有可能造成信息失密，如计算机内的信息可能通过电磁波形式泄漏出去，外部网络通信线路也可能被截获、监听等。另外，刘波强调[20]，虽然数据传输的过程中处于加密状态，但是云服务商可能获取加密解密的密钥，给用户的数据安全带来风险。

2.2.3 数据访问方面

在数据访问方面，学术界主要讨论了身份管理、访问控制、用户权限等问题。在云计算模式下，一些云服务商可能以用户未知的方式越权访问用户数据，同时由于“云”端的数据处于共享环境，如果缺乏用户访问控制和信息操作权限的有效管理，也会导致用户的数据被非法访问。关于这一主题

的研究，张亚红、郑利华、邹国霞的观点较有代表性，他们不仅指出企业可以根据信息密级程度以及用户对信息需求的不同，将信息和用户从低到高划分为若干个等级，并严格控制用户对信息的访问权限，而且还概括了用户身份认证的重要性，并提出企业应该结合单点登录的统一身份认证和权限控制技术，严格控制用户对信息资源的访问，使得数据和服务安全得到有效的保证[4]。薛凯、刘朝、杨树国列出了传统的认证技术，如安全口令S/k、令牌口令、数字签名、单点登录认证，资源认证等[25]。张瑞平、陈雅娟、王小猛等重点强调了动态密码认证和短信验证认证，并指出动态密码认证其实是利用静态密码和短信密码的结合而实现，即在登录网络时输入用户自定义的账号和静态密码之后，同时通过短信下发6位短信密码，信息填写正确才能登录。短信验证认证是指身份认证系统以短信形式发送随机的六位密码到客户的手机上，客户在登录或者交易认证时候输入此动态密码，从而确保系统身份认证的安全[26]。

2.2.4 服务安全方面

云计算与传统计算模式的安全风险一样，服务安全性问题仍有待解决，不同的是，在云计算模式下用户对服务提供者的依赖性更高。云服务安全与否决定了云服务被用户接受的可能性，这引起了很多研究者的重视。经过笔者的整理与分析，归纳出围绕这一主题开展研究的主要学者有蒋建春[14]、文伟平[14]、宁家骏[27]、刘猛[11]等。这些研究者主要讨论了服务的可靠性、服务的延续性及服务协议的合法性问题。刘猛认为[11]，由于云计算的服务是通过各种软件模块以及Web Services来集成实现，因此一旦这些软件出现安全事件，将会产生巨大的影响。

云计算是一种基于Internet的计算模式，因此云计算服务对网络的依赖程度非常强。而停电、地震等突发性事件或软件故障、硬件老化、人为操作失误等都有可能造成网络故障。一旦发生网络故障，将会造成云计算服务中断。此外，云计算服务商破产或被他人收购，也会造成服务中断或不稳定。此外，服务安全方面还包括服务协议的合法性，蒋建春、文伟平提到[14]，在云计算的形式下，一些恶意的服务者所提供的服务内容不一定能够满足服务协议。

2.2.5 服务监管方面

近年来，随着云安全事件的不断出现，云计算服务的监管问题也逐渐显现出来，成为制约云计算应用和发展的一个重要问题，因此有效的监管机制至关重要。在监管方面我国学者研究的主要是第三方认证问题，第三方认证是采用一个中立机构来对双方进行约束，中立机构必须具备很好的公信力，而且不会被任何一方所左右，在安全领域有着丰富的经验和技术能力[20]。艾铜青强调了第三方监管的重要性，他指出政府应该通过立法及监督的方式从另一角度保证该云计算商业模式稳定正常运行[28]。与艾铜青观点相似，魏毅峰、张亮指出[29]，政府应该建立第三方监管机构，确保云计算环境安全稳定运行。华中科技大学教授金海也强调了第三方监管的重要性，金教授认为[30]，云计算要普及并不容易，人们会信赖地把自己的钱放到银行里，因为银行是国有的，银行背后有政府的法律保证，但云计算运营厂商数据中心的数据安全却没有任何有公信力的第三方在制度上的保证，因此用户不敢把数据放进运营商的数据中心里。郝文江[12]、葛慧[18]提出了同样的问题，即传统服务提供商需要通过外部审计和安全认证，但并不是所有的云计算提供商都会接受这样的审计服务，一旦一些服务商拒绝接受审计，使用云计算的用户对自己数据的完整性和安全性就会负有最终的责任。刘楷华、李雄进一步研究指出[21]，即便云计算提供商接受审计服务，他们提供给认证机构的数据也不一定是实时有效的。冯登国指出[31]，实现云计算监控管理必须解决以下几个问题：(1) 实现基于云计算的安全攻击的快速识别、预警与防护。(2) 实现云计算内容监控。(3) 识别并防止基于云计算的密码类犯罪活动。

2.2.6 法律法规方面

云计算的法律法规问题主要包括两个方面，即信息安全技术标准和信息安全立法。在云计算时代，信息安全技术标准能够为信息安全提供技术保障，而信息安全立法能够为信息安全提供法律保障，目前我国缺乏相关的云计算技术标准和立法，这就给云计算产业的发展带来了瓶颈，极大地阻碍了云计算的长期发展。夏良，冯元总结出[32]，云计算缺乏安全标准会导致数据的保密性、完整性和可用性最终由云计算的消费者自行承担。汪兆成从三个方面阐述了云计算相关的法律法规不完善，首先，当信息储存在云中时，并没有明确的法律规定服务方或政府不能查看这些信息。其次，当前云计算服务供应商在服务协议中尽可能地规避了大部分风险问题。最后，在云计算中，数据存储常常分

布在不同的国家或地区[33]。王长全[34]、艾雾[34]、谌洪惠[35]、刘波[20]、艾铜青[28]等多位研究者均从不同角度阐述了我国云计算的法律法规问题，笔者认为周昕的观点较有代表性，他指出现行立法的弊端主要表现为：我国现行立法中尚未对网络信息安全的概念做出明确界定，立法缺乏系统性和权威性；现行绝大多数相关立法的法律位阶低，信息安全监管手段单一，缺乏有效的事后监管机制和长效监管机制；现行立法内容重复较多，对信息技术发展趋势估计不足；现行立法对信息安全主管部门的职权界定模糊。他还提出了四大建议：应尽快制定出台《信息安全法》，并将其作为网络信息安全法律体系的基本法；立法应体现出一致性原则；应建立起各职能部门之间的协作互动机制；进一步健全和完善信息安全标准立法[24]。

2.3 云安全应对策略

笔者通过对检索到的26篇关于云安全应对策略的相关论文的阅读与分析，整理出解决云安全问题需要多管齐下，需要政府、云服务提供商、云用户三方的共同努力。

在政府方面，云安全不仅是一个技术问题，而且还涉及到一个国家的军事、经济、政治等多方面的安全。因此，仅仅通过发展技术来解决云安全问题是远远不够的，只有充分发挥我国政府的职能作用，加快制定云安全相关立法，完善云安全管理，及时制订国家级的战略规划，协调全国范围内的云计算，才能实现云计算的更好更快的发展。经笔者的仔细阅读与分析发现，我国学者关于这一主题的研究较少，在笔者检索到的103篇云安全相关论文中，研究政府应对策略的论文只占了4.9%，而云计算的发展要以政府和市场为主导，政府是不可忽视的力量。王燕，王煦指出[36]，美国在维护信息安全方面的一系列举动，再次提示我国要加强国家层面的信息安全统一领导和协调，加大信息安全，数据安全立法方面的工作，尽快填补目前的法律空白。

在云服务提供商方面，如果云计算服务提供商没有采取足够的措施解决其服务的安全问题，整个云计算系统暴露给黑客的漏洞就会更多。那么云服务提供商如何才能最大程度地确保其服务安全？杜经纬总结了四点[37]，国家对云计算服务提供商进行规范和监督；采用必要的强制措施；云计算厂商采用必要的安全措施；云计算厂商采用分权分级管理。叶加龙，张公让也认为应该从这四个方面进行提高[13]。张亚红，郑利华，邹国霞认为云服务提供商还应该采用主动防御技术保证信息安全，一方面保护存储在云中心的数据安全，另一方面在用户即将访问有害网页或病毒程序前提醒用户[4]。朱芳芳[38]和叶夏菁[39]的观点相似，都认为云服务提供商应该从安全云计算五步走、建立相应的数据安全措施、了解安全漏洞管理、维护取证日志和网络日志这四个方面提高，其中安全云计算五步走是指：了解云计算特有的松散结构对传送到它上面的数据安全有何影响；确保云提供商能够提供有关其安全架构的详细信息并愿意接受安全审计；确保内部安全技术和实践；了解法律、法规对传送到云中的数据有何影响；关注可能影响到数据安全的云技术和实践的变化。

在云用户方面，云计算服务自产生以来，已经拥有了众多用户，但是随着云计算服务的发展，各种安全事件层出不穷，严重影响了用户对云计算业务和相关应用的接受程度。那么用户应该如何选择比较安全的云计算服务提供商来获取云服务？夏良，冯元认为[32]，云用户应该选择信誉良好的云服务，尽量使用付费存储，仔细阅读隐私声明。刘猛认为[11]，用户还应该注意使用过滤器，加强用户口令管理，使用加密技术，保护API密钥。魏毅峰，张亮指出[29]，用户还应该考虑商业模式，在设法确定哪些云服务提供商值得信任时，应当考虑它们打算如何盈利。杜经纬[37]、叶加龙[13]、认为增强用户的安全防范意识也很重要，对存储在云里的数据，要经常备份。

3 当前云安全研究存在的不足与建议

3.1 当前研究存在的不足

3.1.1 云安全概念界定模糊

通过对检索到的103篇论文的阅读与思考，笔者发现只有13篇论文总结了云安全的定义，而这13篇中有6篇都是在重复某一种观点，只是换种方式表达而已。在剩余的7篇论文中，对‘云安全’的概念出现了两种主要的分歧，一种认为‘云安全’是云杀毒安全；一种认为‘云安全’不仅包括云杀毒安全，还包括用户安全、服务安全、各种管理标准、法律法规等，即云计算带来的安全问题。目前，支持第一种观点的研究者较多。

3.1.2 云安全研究内容重复

笔者对我国云安全研究论文的统计分析结果表明，我国云安全研究呈现递增的态势，但通过对检索到的103篇论文主要内容进行对比分析，笔者发现很多论文陷入了低水平重复的误区，许多作者的观点只是在转述某种观点，换种说法或者调整一下文章结构而已，缺乏新意，研究性较弱。如关于云计算带来的安全问题的相关论文中大多数作者所阐述的几乎都是数据存储、数据丢失、数据隔离、数据传输、服务可靠性可延续性、法律法规等方面的问题，只是换种说法，换个例子而已。

3.1.3 云安全实证研究缺乏

通过对检索到的103篇论文的仔细阅读与思考，从中发现我国对云安全的研究侧重于理论研究，对云安全的实证分析很少，而研究成果缺乏实证数据的支撑，其理论指导意义和实际应用价值必然大打折扣。比如云计算带来的安全问题这一方面，如果缺乏实证分析，其研究结果显然苍白无力。

3.1.4 有关政府应对策略的研究力度不够

笔者通过对检索文献的阅读与统计分析，发现有关政府应对策略研究的论文只有5篇，在这些研究成果中，一些学者提出的解决措施对解决实际问题的意义不是很大，有些学者虽然提出了对现实具有一定指导意义的应对策略，但其研究结论仅仅建立在理论推演的基础上，缺乏必要的原型系统验证或实例佐证。

3.1.5 对国外云安全的研究很少

就目前来看，国内很少有人对国外，尤其是对发达国家的云安全进行研究。在笔者检索到的103篇论文中，仅有4篇论文关于国外云安全研究的介绍，这个数据表明目前国内云安全研究学者对国外同领域研究成果的重视和利用程度有待提高。

3.2 研究建议

针对目前我国云安全研究中存在的问题，笔者认为可以从以下五个方面推进我国云安全的深入研究。

3.2.1 加强对云安全的基础理论研究

清晰界定云安全概念，确定云安全的内涵和外延，逐步构筑相对完整的云安全基础理论体系。

3.2.2 注重创新思维的运用

在云安全的研究中应该注重创新思维，根据有关理论调研或实证研究，发表具有研究性的观点，而不是转述别人的看法或汇总别人的观点，同时应该尽量细化主题内容并进行深入研究。

3.2.3 注重实证研究

没有调查就没有发言权，云安全的研究应该重视理论联系实际，尽可能开展实证研究，为今后的云安全研究提供可验证的依据。

3.2.4 加大政府应对策略的研究力度

我国云计算的发展是以政府和市场为主导，政府的力量不容忽视，如数据安全、数据保护、服务安全等更多地涉及政府层面。因此，加强这方面的研究将有利于为政府更好的发挥引导作用提供理论依据。

3.2.5 重视对国外云安全的研究

在云安全研究中要积极借鉴国外的研究成果，跟踪世界云安全的研究动向，注重云安全的前沿和热点问题的研究，提高我国云安全研究的整体水平。

4 结　语

在云服务环境下，无论是云计算服务提供商还是云用户，安全问题都是第一大问题，我们应该理性地看待云计算，既要看到云计算带给社会的种种便利，又不能忽视云安全问题。通过分析总结我国云安全研究的现状，笔者认为各个领域如医学、教育、金融等已经开始重视云安全的研究，但仅仅停留在云安全问题的理论研究层面，学术界应该深入研究云安全原型系统及基于原型系统的实证式研究。

参考文献

1 孙威民.全球大型互联网和云计算服务提供商安全漏洞[EB/OL].http://it.shm.com.cn/network/185879/781081174777.shtml,2011-04-01.
2 2010技术回顾:云安全将成为复合型技术[EB/OL].http://www.chinacloud.cn/show.aspx?id=5406&cid=14,2010-12-26.
3 方　杰.浅谈云安全[J].信息系统工程,2009,(8):58-61.
4 张亚红,郑利华,邹国霞.云计算环境下的信息安全探讨[J].网络安全技术与应用,2010,(10):76-77.
5 吴　珍.漫步云端—探秘云安全[J].信息安全与通信保密,2008,(11):16-17.
6 菲　菲.云安全新概念:解读云安全2.0技术[J].电脑知识与术,2009,(10):56-58.
7 兰天静.基于‘云’端的网络安全研究[J].信息与电脑,2011,(4):25.

8 韩立华,韩李宁,张 亮,等.信息安全保障模式变革浅析[J].中国西部科技,2010,9(5):35-37.
9 覃 俊,黄力平.云计算时代的新闻传媒行业信息安全实践[J].电脑知识与技术,2011,7(22):5315-5317.
10 马晓亭,陈 臣.数字图书馆云计算安全分析及管理策略研究[J].情报科学,2011,29,(8): 1186-1191.
11 刘 猛.探析云计算中的信息安全[J].电脑编程技巧与维护,2010,(24):133-134.
12 郝文江.云计算与信息安全[J].城市与减灾,2010,(4):12-15.
13 叶加龙,张公让.云计算与信息安全[J].价值工程,2011,(1):184-185.
14 蒋建春,文伟平.“云”计算环境的信息安全问题[J].信息网络安全,2009,(6):61-63.
15 那 罡.保卫云端[N].中国计算机报, 2011-01-03(35).
16 陈芸芸.欧洲云计算的法律迷宫[J].信息化建设,2011,(5):26-28.
17 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.
18 葛 慧.云计算的信息安全[J].硅谷,2009,(1):42-43.
19 孙 铁.云环境下开展等级保护工作的思考[J].信息网络安全,2011,(6):11-13.
20 刘 波.云计算的安全风险评估及其应对措施探讨[J].移动通信,2011,(9):34-37.
21 刘楷华,李 雄.云计算的安全模型和策略分析[J].电脑知识与技术,2011,7 (8):1750-1751.
22 谢四江,冯 燕.浅析云计算与信息安全[J].北京电子科技学院学报,2008,16 (4):1-3.
23 金志敏.基于云计算下的高校图书馆数据安全策略的探讨[J].计算机安全,2011 ,(6):96-99.
24 周 昕.“云计算”时代的法律意义及网络信息安全法律对策研究[J].重庆邮电大学学报,2011,23(4):39-47.
25 薛 凯,刘 朝,杨树国.云计算安全框架的研究[J].电脑与电信,2010,(4):28-32.
26 张瑞平,陈雅娟,王小猛,等.一种基于云计算的新型移动增值业务测试平台设计与实现[J].移动通信,2010,(22):75-80.
27 宁家骏. 以发展眼光看待云计算安全[J].信息安全与技术,2010,(9):3-5.
28 艾铜青.云计算技术及安全[J].电脑知识与技术,2011,6(17):4608-4609.
29 魏毅峰,张 亮.浅析云计算环境下的信息安全[J]. 郧阳师范高等专科学校学报,2010,30(3):39-41.
30 杨 怡,赖迎春.云计算环境下的安全问题浅析[J].电脑知识与技术,2009,(16):4154-4156.
31 冯登国.开启云计算安全时代[J].信息网络安全,2011,(3) :1-2.
32 夏 良,冯 元.云计算中的信息安全对策研究[J].电脑知识与技术,2009,5(26):7368-7382.
33 汪兆成.基于云计算模式的信息安全风险评估研究[J].信息网络安全,2011,(9):56-59.
34 王长全,艾 雾.云计算时代的数字图书馆信息安全思考[J]. 图书馆建设,2010,(1):50-52.
35 谌洪惠.云计算的安全挑战[J]. 电脑知识与技术,2011,7(24):5848-5849.
36 王 燕,王 煦.云计算时代对我国信息安全的思考[J].现代管理科学,2011,(2):85-87.
37 杜经纬.云计算时代对信息安全的影响及对策分析[J].信息安全与技术,2011,(5):13-18.
38 朱芳芳.云安全实现措施的研究[J].商品与质量,2010,(6):180.
39 叶夏菁.基于数字化校园的云安全方案[J].现代计算机(专业版),2011,(7):78-80.

(实习编辑 赵红颖)

(上接第141页)

http://www.htsc.com.cn/aboutht/stepIntoHT/htgk.html,2012-05-01.
23 李毅中.最近几年中国出现实体经济空心化问题(2012中国网财经全国两会大型专题.专家视点) [EB/OL].http://finance.china.com.cn/special/lianghui2012/20120306/573649.shtml,2012-03-06.
24 储一昀.交叉持股问题的文献综述及研究展望[J].上海立信会计学院学报,2007,21(6):25-32.
25 巨潮资讯网(中国证监会指定信息披露网站).上市公司资讯[EB/OL].http://www.cninfo.com.cn/information/lclist.html,2012-05-01.
26 孙华平.2011年中期上市公司交叉持股情况一览[N].证券时报,2011-8-17(C7).
27 Borgatti, S.P., Everett, M.G. and Freeman, L.C. Ucinet for Windows: Software for Social Network Analysis[EB/OL].http://www.analytictech.com/ucinet/,2012-05-01.

(实习编辑 赵红颖)