云计算数字图书馆的安全防护*

□ 李留英 / 南京政治学院上海分院军事信息管理系 上海 200433

摘要：云计算数字图书馆为用户带来新的服务模式和内容，但给信息安全带来新的问题。文章分析了云计算数字图书馆的特点及安全隐患、云安全的优势和核心技术，探讨了云安全在云计算数字图书馆的应用。

关键词：云计算，数字图书馆，云安全
DOI：10.3772/j.issn.1673—2286.2011.02.012

随着互联网技术的发展，云计算正逐渐得到广泛应用，也使数字图书馆在经历了互联网时代、Web 1.0时代、Web 2.0时代后，进入云计算时代。云计算技术为数字图书馆带来全新的服务模式和服务内容，但也给信息安全防护带来新的问题。

1 云计算数字图书馆

1.1 云计算的发展

云计算（Cloud Computing）是分布式处理（Distributed Computing）、并行处理（Parallel Computing）和网格计算（Grid Computing）的发展，是这些技术的商业实现。云计算是一种新兴的基础架构方法，通过网络将无数设备连接在一起，提供各种IT服务。它使得超级计算能力通过互联网自由流通，用户只需通过互联网来购买或租赁计算能力，以节省成本。云计算的出现，将使用户从以桌面为核心的使用习惯，转向以网络为核心的存储与服务。它是一种以互联网为中心的计算方式，已在商业领域获得较为成功的应用。

云计算发展至今，已形成以谷歌、雅虎、微软、IBM和亚马逊5大公司的高度集成、扩张发展态势，并逐渐形成垄断全球计算和存储服务市场的局面。云计算正获得越来越多的关注，越来越多的企业以不同的产品和形式进入云计算领域[1]。

中国在云计算方面起步较晚。2008年3月中国移动启动“Big Cloud”计划。2008年12月30日，阿里巴巴宣布在南京建立云计算中心。2010年1月22日，由中国电子学会发起的中国云计算技术与产业联盟（China Cloud Computing Technology and Industry Alliance，CCCTIA）在北京正式成立。

1.2 云计算数字图书馆的发展

经过十多年的数字化发展，数字图书馆建设已经取得骄人的成绩。当前绝大部分图书馆的信息服务架构于IT之上，IT不仅决定了图书馆信息服务的能力，而且也影响着图书馆的组织结构、运行成本和服务模式。

云计算提供的网络服务模式将会对图书馆带来全新的管理和服务。它可以合理地利用云系统的强大硬件设施，实现各大高校和企业的数字图书馆之间信息共享，使数字图书馆的商业成本大大降低，效率大幅

* 本文系国家社科基金青年项目“网络信息资源内容安全主动监控体系研究与实现”（项目编号：07CTQ004）的研究成果之一。

提高。对用户来说，通过云服务可以随时获得相关的数字图书馆的信息，无需考虑地域差异，节省了资源在网络中的延迟时间。

云计算在图书馆的应用，目前主要集中在平台层和软件层，而基础设施层是图书馆界面临的最大挑战。由于云计算服务能从基础设施层解决许多长期困扰图书馆网络信息管理和服务中存在的问题，因此将会有越来越多的图书馆通过云计算来提升图书馆网络信息管理与服务的水平，实现可靠的网络存储和更大的网络效应，降低管理与服务的成本[2]。

云计算已成为数字图书馆发展的重要问题。2008年10月，Jason Griffy在《图书馆杂志》旗下的NetConnect杂志发文提出“云图书馆员”（Cloud Librarians）的新概念。2009年初，Michael Stephens预测云计算是图书馆界十大技术趋势之首。2009年4月23日，世界最大联机图书馆服务供应商OCLC宣布推出基于WorldCat书目数据的“Web级协作型图书馆管理服务”，被公认为是一项云计算服务，标志着云计算在图书馆领域广泛应用的开始。2009年5月，英国Talis公司的Richard Wallis、Google的France Haugen等人提出“云计算图书馆”（Cloud Computing Library）的新概念。Google数字图书馆计划表明数字图书馆与云计算已经联姻。2009年7月14日，美国国会图书馆开始DuraCloud计划，以使用云技术永久访问数字内容。

目前，国外许多图书馆组织与协会也开始探讨图书馆的云计算使用。如2009年7月12至14日，由华中科技大学图书馆、美国约翰-霍普金斯大学图书馆、中国图书馆学会等联合举办了“2009第六届数字环境下图书馆前沿问题研讨会”，会议专门谈论了云计算对图书馆的影响等问题。

我国的数字图书馆经过十多年建设，已取得较好的应用，并构建了三大公共服务体系，其中中国高等教育文献保障系统（China Academic Library Information System，CALIS）为中国的高等教育实现良好的服务[3]，是一个开放式的中国高等教育数字图书馆，是中国经济和社会发展的重要基础设施。目前，CALIS技术中心开发的支持分布式云服务的CALIS数字图书馆云平台框架（CALIS Easy Cloud Platform）已初步完成，为CALIS三期项目建设和新一代数字图书馆系统的开发和实施奠定了全新的技术基础。CALIS云平台包括如下四个部分：（1）CALIS数字图书馆公共服务平台：构建CALIS云服务中心；（2）CALIS数字图书馆SaaS（Software as a Service）服务平台：为图书馆提供SaaS服务；（3）数字图书馆本地服务平台：包括本地应用基础平台和本地应用系统；（4）CALIS云联邦服务平台：将不同的图书馆本地服务、CALIS公共服务以及第三方公共服务集成。

2 云计算数字图书馆的安全威胁

目前，多数的数字图书馆采用分布计算方式，各种数据集中保存在服务器上。一旦服务器出现故障或面临恶意攻击，图书馆服务器上的各类信息资源将会遭到破坏或丢失，将使数字图书馆无法为用户提供信息服务，甚至无法恢复数据，从而给数字图书馆造成不可挽回的后果。

采用云计算技术，可以确保数字图书馆资源存储的可靠性，避免了因服务器出错而导致的资源丢失现象，同时也保证了在不理想的网络安全环境下一旦发生信息丢失后，数字图书馆可以继续为用户提供服务。

但是，云计算本身也存在一定的风险。在云计算模式下，所有的业务处理都由云端的服务器完成，服务器一旦出现问题，将导致所有用户的应用无法运行，数据无法访问。未来的云计算安全威胁多种多样，云计算数据中心将成为黑客攻击的首选目标，其所面临的安全隐患防不胜防。如果云计算的可靠性和安全性无法解决，云计算的普及将会遇到很多难题。

美国高德纳咨询公司Gartner发布的《云计算安全风险评估》[4]称，云计算服务存在着七大潜在安全风险，分别是：特权用户的接入、可审查性、数据位置、数据隔离、数据恢复、调查支持和长期生存性。

根据云计算的特点和数字图书馆的现状，云计算数字图书馆主要面临如下安全威胁[5]：

（1）大量的网络和应用系统漏洞。云计算服务推动了互联网的发展，与传统的操作系统、数据库、C/S应用系统的安全漏洞相比，云服务的多客户、虚拟化、业务逻辑复杂、用户参与等特点为数字图书馆带来巨大的安全挑战甚至灾难。

（2）拒绝服务攻击。拒绝服务攻击和分布式拒绝服务攻击是目前最常用的攻击方式。在云计算模式下，将有更多的图书馆业务迁移到云服务中心，一旦黑客依赖网络实施拒绝服务攻击，对数字图书馆数据中心造成的后果和破坏程度将远远超过传统的局域网。

（3）信息泄露。在云计算环境下，许多数字图

书馆建设者将数据和业务存储在云服务提供商的IT系统中。为保障云服务商内部自身的安全管理和职责分离，应确保云服务商能够提供数据的专人或专职维护，实现数据隐私的保密，并签订保密协议。即可运用法律手段来维护数字图书信息的安全保密工作，并倡导国家成立专门的机构来监督云中的资源。

3 云计算的安全

3.1 云计算为信息安全带来的优势

云计算的强大计算与同步调度能力，可以极大地提升信息安全公司对新威胁的响应速度，为此各大安全厂商纷纷在安全领域引入云计算。云计算将为信息安全的发展带来如下好处[6]：

（1）数据集中存储，可减少数据泄露，实现可靠的安全监测。由于传统模式很容易导致数据泄露，数据集中存储更容易实现安全监测。通过建立多个数据中心，数据中心的管理者可以对数据进行统一管理，负责资源分配、负载均衡、软件部署、安全控制，通过安全实时监测，降低使用者成本。

（2）事件快速反应。用户可利用云计算服务商提供的取证服务器实现快速取证准备，缩短取证时间，降低服务器出错概率，使取证更有针对性，通过执行加密校验和散列（hash）隐藏取证痕迹，缩短存取受保护数据时间。

（3）密码可靠性测试。利用云计算可减少密码破解时间，并能保证密码强度的可靠性。

（4）日志。云存储可以帮助用户记录想要的标准日志，而且没有日期限制，只需按次数收费，并可以根据日志探测计算机的动态信息，实现实时监测。

（5）提升安全软件的性能，云计算整体提升了安全产品性能，尤其杀毒软件的性能得到很大提高。

（6）可靠的构造。利用云计算的虚拟化技术及工具，定义用户自己的安全状态，利用离线安装补丁减少漏洞，用更低的成本和更少的时间检测安全状况。

（7）安全性测试。通过云计算的共享应用程序服务，可以节省大量的安全性测试费用。

3.2 云安全

目前，各大安全厂商纷纷采用云计算技术，提升其对病毒样本的收集能力，减少威胁的响应时间，中国的安全厂商提出了云安全（Cloud Security）的概念和云安全体系。

云安全是由云计算派生出来的一个应用，是云计算在安全领域的分支，为网络安全防护打开了一条创新之路。云安全融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，传送到服务器端进行自动分析和处理，再将病毒和木马解决方案分发到每一个客户端。云安全可以让用户以最低限度的存储和计算资源，获得最完善的安全防护，最大化节省网络资源，为用户节省成本。

云安全的概念最早由趋势科技公司提出，并得到了众多安全厂商的跟随与认可。趋势、卡巴斯基、McAfee、Symantec、江民科技、Panda、金山、360安全卫士等都推出了云安全解决方案，将查杀能力从传统的客户端向服务器端（云安全系统）转移。云安全已经成为信息安全界的热门话题。

随着恶意程序及木马的泛滥，传统的特征库判别法已无法有效地处理日益增多的恶意程序。运用云安全技术后，病毒识别和查杀不再依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析以及处理，整个互联网形成一个巨大的杀毒软件。参与者越多，每个参与者就越安全，整个互联网就更安全。

安全厂商实施云安全必须拥有庞大的数据中心和大量的服务器。2010年3月15日，瑞星公司启用亚洲最大的云安全数据中心。它采用5000多台企业级专业服务器，为10亿用户提供高质量的安全检测、云安全信息交互及互联网威胁处理服务，使用户享受更快的病毒响应、更高质量的病毒库、更快的升级速度。

4 云计算数字图书馆的云安全防护

4.1 典型的云安全系统

目前，各大厂商借助云安全技术，推出了各自的云安全系统，实现全方位的安全防护[8]。

趋势科技是较早提出云安全概念的公司之一。2008年趋势科技推出了云安全1.0。它采用一些云安全技术对全球网址、邮件服务器和文件进行信誉评估，

对整个互联网进行恶意代码搜集，从网关上阻止Web威胁。2009年7月24日，趋势科技推出了云安全2.0技术，它采用云安全技术实现从网关到终端Web威胁的整体防护。2010年，趋势科技提出面向云计算安全服务的云计算3.0的概念，即从来自云计算的防护（Security From Cloud Computing）过渡到给云计算提供防护（Security For Cloud Computing），扩展了对云安全自身的保护。云安全3.0技术将数据中心虚拟化安全防护作为重点，为虚拟设备防护和网络代理设备的防护提供了有效保证。

瑞星云安全系统将用户和瑞星技术平台通过互联网紧密相连，让每一台电脑变成一个木马监测站，组成一个庞大的木马/恶意软件监测、查杀网络。随着瑞星云安全系统逐渐成熟完善，并通过与搜狐、巨人、淘宝、支付宝等公司深入合作，瑞星构建了一个立体化、智能化的网络安全综合平台。

虽然瑞星和趋势科技的云安全的技术路线不同，但具有相同的目标：终端越来越瘦，云端病毒库和杀毒能力越来越强。趋势科技已经实现了终端的零病毒码存储；瑞星通过对云安全系统数据的分析，对杀毒软件最大限度地优化，使其查杀能力更强，消耗资源更少。

随着云计算的广泛应用，传统的安全防护方法已无法满足基于云计算数字图书馆的安全要求，必须因时制宜建立以云安全体系为核心的信息安全防护体系。

4.2 云计算数字图书的安全部署

数字图书馆作为云计算的服务提供者（Library as a Service），可以开发数字图书馆云服务平台，利用构建的私有云和公共云，提供多种数字图书馆服务，使用户获得透明的服务。

针对日益严峻的安全形势，可以借助CALIS数字图书馆云服务平台，建立全国的数字图书馆云安全管理中心；借助数字图书馆的本地服务平台以及云服务联邦平台，建立各地区以及省级中心图书馆云安全中心；直接利用瑞星公司或其他安全公司的云安全产品系列，并和其他相关安全产品，形成一个立体的安全防护体系。

通过这种方式，用户无需在客户端保存大量的病毒库信息，只需和数字图书馆的云服务器进行短暂连接就可以判定文件的安全性，大大减轻了客户端系统的负担，保证了客户端的流畅，也提高了杀毒防毒能力；同时与其他安全产品，如防火墙、入侵检测等联动，构建一个完整的快速的防护体系，从而使云计算数字图书馆的安全风险降到最低。

参考文献

[1] 欧阳璟. 云计算趋势一览[J]. 程序员2008年精华本,2008(1):282-286.
[2] 李永先,栾旭伦,李森森. 云计算技术在图书馆中的应用探讨[J]. 江西图书馆学刊,2009(1):105-106.
[3] 王文清,陈凌. CALIS数字图书馆云服务平台模型[J]. 大学图书馆学报,2009,27(4):13-18.
[4] WANG Chenxi, PENN J, HERALD A. How Secure Is Your Cloud? Forrester Research For Security & Risk Professionals[R/OL]. [2009-08-03]. http://www.forrester.com/Research/Document/Excerpt/0,7211,45778,00.html.
[5] 赵粮,裘晓峰. 云计算环境的安全威胁和保护[J]. 中国计算机学会通讯,2010,6(5):47-50.
[6] 中国云计算网.云计算为安全带来的七大好处[EB/OL]. [2010-03-20]. http://www.cncloudcomputing.com/jinghua/98.html.
[7] 张洋. 云安全的七大技术核心[EB/OL]. [2008-09-27]. http://netsecurity.51cto.com/art/200809/90956.htm.
[8] 六大安全厂商“云安全”详解[EB/OL]. [2009-07-28]. http://articles.e-works.net.cn/Security/Article69617.htm.

作者简介

李留英（1972-），南京政治学院上海分院信息管理系副教授，硕士生导师，研究方向：信息安全、信息处理。E-mail: lly003@vip.sina.com

Security Protection of Cloud Computing Digital Library

Li Liuying / Department of Military Information Management, Shanghai Branch of Nanjing Political College, Shanghai, 200433

Abstract: Although Cloud Computing Digital Library brings new service scheme and content for users, it faces new security problems. The paper analyzes the characteristics and security hazards of Cloud Computing Digital Library, advantages and key techniques of cloud security, and proposes the application of cloud security in Cloud Computing digital library.

Keywords: Cloud Computing, Digital Library, Cloud Security

（收稿日期：2010-10-19）