[文章编号] 1004-325X(2010)01-0050-03

云计算时代的数字图书馆信息安全思考

Thinking about the Information Security of the Digital Library in Cloud Computing Era

王长全 （山东大学威海分校商学院 山东 威海 264209）
艾 雾 （山东大学威海分校图书馆 山东 威海 264209）

[摘 要] 云计算时代数字图书馆的信息安全问题，一方面来自云服务提供商提供的安全保障，另一方面来自图书馆的信息安全需求。针对数字图书馆可能面临的安全存储、访问控制、权限管理、数据保密及知识产权等信息安全问题，云计算时代的数字图书馆应采用最新的技术手段、统一身份认证、严格控制访问权限、加快信息安全基础设施建设、制定相关标准及政策法规，以保障图书馆的合法权利和数据安全。

[关键词] 云计算 图书馆 信息安全
[中图分类号] G250.76 [文献标识码] B

[Abstract] In Cloud Computing era, information security problems of the digital library come from the security provided by the cloud service providers, on the other hand, come from the information security demand of the digital library. To solve information security problems that the digital library may face , such as the data storage, access control, jurisdiction management, data security and intellectual property, digital libraries should adopt the latest technological means, unify the identity authentication, control the authority of visiting strictly, accelerate the infrastructure construction of the information security, make relevant standards, policies and regulations, in order to guarantee the lawful right and data security of the library.

[Key words] Cloud Computing; Library; Information security

1 引 言

作为一种新兴的、备受赞誉的技术，云计算技术一经推出就得到了业界人士的推崇。图书馆历来是信息技术应用的重镇，“云”时代也不例外。从数据库商提供网络版全文数据库到图书馆自动化管理系统托管平台的出现，再到Web2.0技术在图书馆的应用，这一切图书馆技术发展均可视为云计算相关技术或服务在图书馆的应用。2009年4月，OCLC（Online Computer Library Center，联机计算机图书馆中心）正式宣布即将推出基于WorldCat书目数据的“Web协作型图书馆管理服务”[1]，不仅此项服务被公认为是一项云计算服务，而且此举预示着云计算开始在图书馆领域广泛应用。未来的云计算技术将给图书馆工作带来深刻的变革，例如，云计算时代的数字图书馆将不必再购买和安装本地自动化管理系统，而是采用网络服务的形式由供应商直接提供便利的软件服务；通过Web云接入，可以实现超大规模的计算和存储服务及无处不在的访问，从而克服目前数字图书馆服务器访问限制的瓶颈；将分布式存储的数据库和一站式检索界面结合起来，进行数字资源的整合、组织、关联、导航，甚至是可视化服务，以实现不同“云”之间的互操作及全方位的网络扩展服务，等等[2]。云计算技术的应用无疑会使图书馆的服务方式与服务内容产生巨大变革，但同时也会给数字图书馆的信息安全带来新的挑战。

2 云计算时代数字图书馆的信息安全问题

在云计算模式中，虽然数据集中存储，数据中心的管理者对数据进行统一管理、分配资源、均衡负载、部署软件、控制安全以及进行可靠的安全实时监测，从而使用户的数据安全得到最大限度的保证，但是，所有的东西都高高挂在“云”端而不是握在自己手里，必定存在着相当大的风险。在云计算环境下，无论对于云服务提供商还是使用云服务的图书馆而言，安全问题都是第一重要问题，也是云计算应用中亟需解决的问题。

2.1 云服务提供商需要提供的安全保障

2.1.1 如何保证用户数据的安全性与可用性？

虽然“云”从技术上使用了数据多副本容错、计算节点同构可互换等措施来保障服务的高可靠性，但从相关报道披露的2008年10个最糟糕的Web2.0网络故障事件来看，其中有多项与云计算应用有关，如亚马逊S3的服务中断、Google Apps（在线办公应用软件）的服务中断、Gmail邮

箱爆发全球性故障、微软的云计算平台 Azure 停止运行 22 小时等。这些故障事件让那些还处在“云雾”中的多数业内人士和用户对于云计算的安全性和可用性再度产生了忧虑和怀疑[3]。

2.1.2 如何为用户提供标准、规范、风险共担的服务？

如果我们仔细研究一下亚马逊的云服务合同，不难发现其中很多条款是不合理的。比如第 7.2 条款中规定:“我们对于任何未经授权的访问或使用造成的破坏、删除、销毁或弄丢任何你的内容或应用的程序不负有责任。”[4]在该合同中，服务提供商并不承诺对任何数据泄密事件及数据被破坏行为承担法律责任或义务。可见，由于目前缺乏云计算架构的安全模型和标准，云计算服务提供商有可能规避大部分安全风险问题，而将风险转嫁给用户。

2.1.3 如何得到用户的信任？

信任问题是云计算发展过程中的一大障碍。华中科技大学教授金海认为，“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。”[5]

2.2 云计算时代数字图书馆的信息安全需求

按照“云”的理念，如果云计算得以实现的话，那么未来图书馆将不需要维护自己的服务器，也不需要在本地硬盘上保存数据，用户只需要有终端设备就可以通过互联网查询和使用各种信息资料。但是云计算的复杂性、用户的动态性、数据的变化性都有可能使数字图书馆的各种资源和数据的安全性、保密性、可用性、完整性等变得不确定，甚至造成无法估量的损失，所以在享受云计算便捷服务的同时，图书馆对于数据资源的安全管理又提出了新的需求。

2.2.1 数据安全存储

图书馆对云计算最大的担心在于数据的安全性，无论是书目数据、读者数据、流通数据还是电子书刊、特色馆藏数据库等资源一旦丢失，后果将不堪设想。云计算环境下，图书馆的数据、程序都不在本馆机器上。如何保证数据不会意外丢失、毁损以及不会被非法收集、处理、利用？怎么保证明天这个“云”还存在？明天还能否正常访问本馆数据？数据能否绝对安全？等等，都将成为图书馆对于云计算提出的最基本的要求。

2.2.2 访问控制管理

访问控制的目的是保证各图书馆数据资源不被非法访问和使用。云计算环境对于黑客极具吸引力，因为“云”本身不但集中存储了各种资源，对于恶意软件的隐藏也提供了便利的条件。再加上云环境的高度复杂性不可避免地会给黑客留下一些机会，使其可以通过寻找云环境内的安全漏洞来窃取用户资料或破坏所存储的信息（包括图书馆的各种数据），因此必须采取有效手段予以防范。

2.2.3 用户权限管理

用户权限，即合法用户可以进行的具体操作。用户登录到云环境下的数字图书馆后可进行浏览、检索、下载、创建、更新(修改和删除)等操作，但并不是每个用户都可以进行所有的操作，不同的用户将具有不同的权限。在云环境下，图书馆数据的创建、更新及整合等事宜，如读者数据的更新、馆藏书目数据的维护、随时需要提交的馆藏信息与订购信息等，仍由图书馆负责。这就要求云计算环境能够对普通用户、图书馆管理者和云计算服务商进行合理的权限划分与管理，以保障数据安全。

2.2.4 数据保密需求

图书馆的读者数据、借阅数据、财经数据等交给云计算服务商后，具有保密控制权的并不是图书馆，而是云计算服务商。而在云环境下，要求保密的这类信息随着信息服务的多元化将有可能出现在整个信息服务的收集、传输、处理、利用、存储和传播的各个环节，这将严重威胁图书馆的信息安全。虽然每一家云计算服务提供商都强调使用加密技术来保护用户数据，但也仅限于数据在网络上的加密传输，数据在处理、存储和传播时的安全问题仍然没有解决。

2.2.5 知识产权保护

数字图书馆的知识产权问题在云时代不仅依然存在，并且还有新变化。图书馆购买云计算服务后，将自己的数据交给“云”，由云计算企业托管这些数据。理论上说，用户应该完全拥有被托管数据的知识产权。但是在现实中，云计算企业深知“数据核心”原理，因而他们会千方百计利用这些数据，并以数据整合、数据挖掘、知识服务的名义使其对用户数据的利用合法化。近年来，OCLC 利用 WorldCat 中集成的馆藏数据开发出了一些新产品，如每季的高校图书馆与科研图书馆推荐书目、作品的读者对象等。其 Web 级服务，也就是云计算图书馆集成系统，一旦上线，将会集成大量图书馆的本地读者信息及借阅数据。这些数据与书目信息不同，本是由成员馆所唯一拥有的，但如果云提供商加以开发而成产品，其知识产权的界定将成为新的问题[6]。

3 云计算时代的数字图书馆信息安全策略

针对上述云计算的安全风险及云环境下数字图书馆的安全需求，图书馆应当充分了解目前最新的技术发展状况，未雨绸缪，在构建“图书馆云”的过程中重点考虑以下几方面的安全策略。

3.1 采用最新的技术手段,保障图书馆数据的存储安全。

云环境下为了保证图书馆数据的万无一失，对于服务商和图书馆来说，都应该采取更为安全有效的技术手段。一方面，服务商应采用目前最为先进的虚拟化海量存储技术来管理和存储数据资源。海量存储技术中最经常的是使用镜像和校验技术进行容错，需要在两套不同的设备中维护相同的数据，一旦主设备损坏，可立即切换到镜像设备进行访问。虚拟化海量存储技术是采用数据副本的方式进行容错，它不需要冗余设备，通过对每个虚拟盘创建多个

副本来提高数据的可用性和访问性能。这种方法不需要维护规模庞大的映射表，即使磁盘被损坏，也不会影响正常的读写访问，更适合在云环境下的海量存储网络系统中实现[7]。另一方面，图书馆也应自行对各种馆藏数据资源进行及时、全面的备份及长期、可靠的保存。

3.2 统一身份认证，实现有效的访问控制。

统一认证是实现图书馆服务安全的前提，其中用户的身份认证对云环境下的数据安全起到了至关重要的作用，只有通过认证的授权用户才能访问“云”中的相应资源[8]。由于云计算环境具有异构性、动态性、跨组织性等特点，不可能要求用户在使用每一个云资源之前都进行身份认证，因此云环境下的数字图书馆可采用单点登录的统一身份认证方式。被授权的图书馆用户只需主动进行一次身份认证后便可以访问其他被授权的资源，而不再需要进行其他的身份认证过程。这样能够极大地提高用户的访问效率，同时也满足了数字图书馆开放的特性。

3.3 严格控制访问权限，保障图书馆的服务安全。

云环境下的数字图书馆可以根据用户信息需求的不同，将用户从低到高划分为若干个层级，并严格控制用户对资源的访问权限[9]。目前较为成熟的权限管理与控制技术是PMI（Privilege Management Infrastructure，特权管理基础设施），它是基于属性证书（Attribute Certificate，简称AC）的授权管理平台，它以PKI（Public Key infrastructure，公钥基础设施）体系为基础，向所有用户提供与应用相关的授权服务，并在用户请求服务时进行权限验证，成为用户和服务提供者间的安全通信基础。图书馆通过PMI进行授权管理，使普通用户登录进入“云”后只能根据事先指派的角色进行数据查询，使承担图书馆数据维护工作的用户登录系统后能够按照管理员的角色分派相应的操作权限。云认证平台对认证信息通过用户权限确认后，将相关信息通过应用服务的认证接口发送给具体的应用服务进行验证，验证成功后，该用户即可调用该应用服务完成具体的数据维护工作。

通过单点登录的统一身份认证与PMI权限控制技术，图书馆能够根据不同用户的层级对应设置不同的资源层级访问权限，使二者形成匹配，从而严格控制用户对资源的访问；同时还能将云计算资源从物理上和逻辑上分成多层进行管理和控制，以有效地保证数据与服务的安全。

3.4 加快信息安全基础设施建设，满足图书馆数据的保密需求。

目前，信息安全基础设施的核心是公钥基础设施（PKI），它是提供公钥加密和数字签名服务的系统或平台，由公开密钥密码技术、数字证书、证书发放机构和关于公开密钥的安全策略等共同组成。PKI的建设和完善使云环境下的图书馆可以在多种应用环境下方便地使用加密和数字签名技术，从而使放到“云”中的数据在存储和传输过程中不能被非授权者偷看，不能被非法篡改，也不能被否认，从而保证了数据的机密性、完整性和有效性，为图书馆建立起一个安全的网络运行环境。

3.5 制定相关标准及政策法规，保障图书馆的合法权利和数据安全。

尽管云计算领域已经在关注标准和协议问题，但图书馆界对于云计算的应用还应该有自己的行业标准。图书馆的行业管理者应该组织关于应用云计算所需的标准和相关协议的研究，并形成行业的应用规范。同时，由于数据安全和保密问题更多涉及的是政策层面的问题，云计算企业的管理政策、企业信誉，甚至国家政策，都可能对云计算数据的安全造成极大的影响，所以需要整个产业链中的各个利益相关者（包括图书馆）在发展过程中不断磨合、谈判和研究，以促成相关管理章程或政策法规制度的出台，从而对知识产权保护、责任追究及各方权益提供有力保障。另外，还应加强对云计算“管理服务提供商”(Management Service Provider，简称MSP)的研究，即研究MSP的开放性、共享性、标准化、安全性能、保密级别、企业的诚信与可持续发展性，研究MSP评价方法与测评指标体系，以便形成图书馆行业对于云计算应用的有效管理，保障图书馆的基本利益和数据安全。

4 结 语

云计算将极大地改进数字图书馆的服务方式与服务功能，同时也将给图书馆带来挑战。其中，安全问题是其能否成功的核心问题。合理和完整的图书馆云计算安全框架必须充分考虑图书馆、用户、云计算提供商、第三方审计等各方利益及其相关性，合理配置安全属性，以便解决这个复杂的巨大系统的安全问题。

参考文献：

[1] OCLC Announces Strategy to Move Library Management Services Web Scale[EB/OL].(2009-04-23)[2009-07-25].http://www.oclc.org/news/releases/200927.htm.

[2] 周 舒,张岚岚. 云计算改善数字图书馆用户体验初探[J].图书馆学研究, 2009(4):28-30.

[3] 孙永杰.云计算风起，落地要过安全关[J].西部论丛, 2008(9):66-68.

[4] 王健红.关注云计算安全设计[N].计算机世界,2009-07-06(47).

[5] 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.

[6] 胡小菁,范并思.云计算给图书馆管理带来挑战[J].大学图书馆学报, 2009(4):7-12.

[7] 王 迪,薛 巍,舒继武,等.海量存储网络中的虚拟盘副本容错技术[J].计算机研究与发展, 2006 (10):1849-1854.

[8] 刘高嵩,张传昌.网格环境下统一身份认证的研究[J].网络安全技术与应用, 2008(10):19-21.

[9] 赵海霞,刘万国，洛凤军. 数字图书馆安全的用户分级研究[J]. 图书馆学研究, 2008(11):50-52.

[**作者简介**]

王长全 男，1970年生，副教授，研究方向：信息系统与信息安全。

艾 雾 女，1970年生，副研究馆员，研究方向：图书编目。

[收稿日期：2009-09-09]