

云计算在科技期刊编辑出版工作中的应用与安全问题

马 岚¹⁾ 谭 伟²⁾

收稿日期: 2012-07-02

修回日期: 2012-10-09

1) 《指挥信息系统与技术》编辑部, 210007 南京 1406 信箱 62 分箱, E-mail: matianleooffice@sohu.com

2) 中国电子科技集团公司第二十八研究所, 210007 南京 1406 信箱 79 分箱

摘 要 介绍了云计算技术在提高编辑部工作效率、扩大科技期刊影响以及避免学术不端等方面存在的优势, 比较研究了 SaaS、IaaS 和 PaaS 等不同云计算应用模式下的安全问题和用户与供应商的安全责任划分, 具体分析了不同云计算环境下科技期刊编辑部数据管理的安全问题, 并分别从政策和技术两个层面给出了科技期刊编辑应用云计算技术在数据安全防护方面的具体对策。

关键词 云计算 编辑部数据管理 安全问题

1 云计算技术在编辑部工作中的应用

2007 年末, 一个新的术语“云计算”诞生了, 其概念和内涵概括起来就是: 云计算 (Cloud Computing) 是一种新兴的商业计算模型, 它将计算任务分布在由大量计算机构成的虚拟资源池中, 使各种应用系统能够根据需要获取计算能力、存储空间和各种软件服务^[1]。在云计算环境下, 用户终端可以通过远程连接, 获取存储、计算、数据库等计算资源, 云计算环境按需部署计算资源, 用户只需要为所使用的资源付费^[2]。

在科技高速发展的今天, 新的科技期刊不断出现, 现有的科技期刊编辑部 (以下简称编辑部) 对编辑团队的划分越来越小型化, 期刊采编工作日趋智能化和集成化。在这个到处充满了“云”概念、技术和服务的现实生活中, 科技期刊编辑部为了提高工作效率, 也可借助“云端”来完成相关的数据管理工作。对于编辑部而言, 除了日常编辑事务之外, 大量的数据存储、查询和比对需求日益突显, 如果可以借助云端, 进入到相关数据资源池中搜寻需要的数据, 共享数据资源, 可以大幅降低编辑成本, 提高工作效率。

云计算技术在科技期刊编辑出版工作中的作用概括如下:

(1) 编辑部可通过云计算服务供应商按需租用云计算服务, 不再需要采购服务器和海量的存储设备, 不需要建立专门的机房设施, 也不需要设置专门的信息维护与管理人员。

(2) 编辑部可以不受服务供应商的制约, 当前市场存在

很多相互竞争的大型云计算服务供应商和灵活的商业模式, 编辑部可随时变换服务与价格更好的供应商。

(3) 编辑部可以按照服务拆分的方式租用硬件、基础软件乃至专用的编辑部期刊采编与管理系统服务, 硬件、基础软件和应用系统甚至可以由不同的云计算服务供应商提供, 进行多种服务的混合搭配, 以达到整体最优和不完全依赖于单一服务供应商的效果。

(4) 编辑可以利用云计算平台进行数据统计和信息发布, 借助于云端强大的计算能力和共享特性, 可以快速得到多种角度的统计数据图表, 并能够采用适当的方式共享给其他用户 (如读者、作者、数字期刊源等)。

针对云计算和编辑部的工作特点, 可以看出云计算技术为编辑出版工作提供以下便利:

(1) 通过“云”降低成本、提高工作效率

云端上存储的数据是海量的, 且具备较高的运行计算速度。如果利用云计算技术进行编辑部的日常工作和数据管理, 每个编辑部无须建立自己的数据库。自建数据库要花费大量的人力、物力和财力, 而且因为科技期刊的读者面相对较窄, 自建的数据库利用率很低。编辑部可以通过有针对性的查找, 找到与出版内容相似的“云端”, 与其服务提供商签订使用和约, 这样既可降低成本, 又可提高工作效率。

(2) 借助“云”宣传自己, 扩大影响

采用云计算技术的云端资源池就是很好的统计平台, 同时也是一个很好的宣传平台, 编辑部可通过向服务商提供基

础数据来宣传自己,从而扩大科技期刊的影响力,这类似于通过搜索引擎平台推广网页。通过云计算平台的推广,可提高科技期刊的知名度和影响力,最终可表现为科技期刊论文的被引频次和引用因子等专用指标参数的提高。

(3) 利用“云”的查询功能尽可能避免学术不端行为

随着科学技术的飞速发展,科技论文的数量呈级数增长,海量论文的内容难免出现重复、抄袭和剽窃等问题,严重的还会引起对著作权的侵权问题。《中华人民共和国著作权法》^[9]的颁布表明了国家从法律法规层面上已经形成了对著作权的保护意识。为了避免日后有关著作权方面的纠纷,编辑部应在接收论文投稿的同时进行相关内容的比对和查询,将论文抄袭、剽窃等学术不端行为遏制在萌芽状态。由于需要查询和比对的数据量巨大,仅靠编辑部自身的数据资源,不论在数量上还是在计算能力上,都是远远不够的。因此,编辑部可以借助云计算技术,通过网络在云端的数据资源池中有目的地进行查询和比对,在提高工作效率的同时有效避免一些不良现象。

由于云端硬件的配置和更新都是由云服务提供商提供,编辑部通过浏览器软件就可进行查询,并可同时共享云服务提供的信息、知识和服务,在有限的场地和设备条件下通过网络充分享受“云”的低成本优势,既可为编辑部缩减开支,又降低了编辑部的工作强度。

2 云计算环境下的数据安全防护

2.1 编辑部工作的安全问题分析

如上所述,云计算技术在编辑出版工作中具备较为明显的优势,但同时也存在安全隐患。传统应用环境下,不论是外购还是自主研发,编辑部都需建立自己的数据库,同时具备输入和查询等基本功能,以便管理稿件信息。在这一环境下,编辑部的数据及配套软硬件完全控制在自己手里,拥有对数据及相关资源的完全控制权利,在数据可靠性、访问控制、隐私保护、安全加密以及版本控制等各方面均具备良好的特性。

然而,在云计算环境下,用户的数据存储在云端,因而不再拥有对自己数据的完全控制能力,只能要求云服务商(Cloud Service Provider, CSP)提供有效的安全保障,用户必须信任云服务商提供下的数据安全及完整性保护。

相比于传统计算,这种新的数据访问和控制模式带来了新的安全挑战,如何避免编辑部数据库中数据被非授权用户获取、篡改和盗用,使数据库正常和安全地运行,这是云计算环境下编辑部所面临的主要问题。

2.2 不同云计算应用模式的安全责任

云计算安全问题包括三方面:(1) 云计算用户的数据和应用安全;(2) 云计算服务平台的自身安全;(3) 云计算资源的滥用。事实上,这些安全问题在传统的互联网与信息系统应用中也存在,但由于云计算业务具有高弹性、大规模、分布化的特性,使得这些安全问题变得尤为突出。

总体而言,云计算安全问题是云计算服务供应商和云计算用户的共同责任,目前两者之间的分界存在不少模糊之处,取决于采用的云计算模式。云计算有3种云服务模式:软件即服务(Software-As-A-Service, SaaS)、基础设施即服务(Infrastructure-As-A-Service, IaaS)和平台即服务(Platform-As-A-Service, PaaS)。这三类云计算服务的特点和用户云计算资源的控制能力均不相同,这使得云服务供应商和云用户各自承担的安全角色与职责也各有不同^[10]。

对于IaaS,云服务供应商主要负责为用户提供基础设施服务,如提供服务器、存储、网络和管理工具在内的虚拟数据中心,云计算基础设施的可靠性、物理安全、网络安全、信息存储安全以及系统安全是其基本职责范畴,包括虚拟机的入侵检测以及数据的完整性保护等。云计算用户则需要负责其购买的虚拟基础设施以上层面的所有安全问题,如所采用的操作系统及应用程序的安全等。

对于PaaS,云服务供应商除了为用户提供基础设施服务之处,还要负责提供一定程度上的分布式软件开发、测试与部署平台。此时,云服务供应商除了要负责底层基础设施的安全,还需要解决平台级的应用接口安全、数据可用性与计算可用性问题。云计算用户则需要负责操作系统或应用环境等平台之上的特定领域应用服务安全问题。

如果采用SaaS,云服务供应商则需更进一步保证其所提供的服务从基础设施、平台直到应用层软件的整体安全。云计算用户则需要维护与自身相关的信息安全,如身份认证的账号和密码防泄漏等。换句话说,如果因云计算用户自身泄露账号密码所造成的安全问题,不能由云服务供应商负责。

上述三类云计算服务在信息安全方面需要考虑的主要问题、对编辑部业务的影响以及供应商与用户两者之间的责任分界,具体如表1所示。

根据表1中对云计算安全问题的分析,结合小型科技期刊编辑部的自身特点,本文认为最佳的方案是采用SaaS,这样编辑部作为云计算用户,自身所需负责的安全工作较少,不需要负责平台级的安全,甚至也不需要负责应用服务安全,符合编辑部规模小、信息维护人才缺乏以及安全服务能力弱等问题。

表 1 云计算服务的信息安全问题以及供应商与用户的责任区分

安全问题	应对措施	对编辑部业务的影响	IaaS		PaaS		SaaS	
			供应商	用户	供应商	用户	供应商	用户
物理环境的安全	能够进入数据中心的人员、人员能够到达的区域以及进入数据中心以后的操作应受到监视和控制,并进行全程监控等。	涉及编辑部数据的整体物理安全性。	√	×	√	×	√	×
网络与主机安全	在网络边界应提供防火墙、入侵检测与防护系统等安全措施。	非法入侵可使数据库瘫痪,严重影响编辑部日常业务。	√	×	√	×	√	×
物理服务连续性	提供负载均衡、群集、系统高稳定性、虚拟化高可用性等技术的连续性服务和运行监控。	涉及编辑部日常业务。	√	×	√	×	√	×
身份与访问管理	应用标准化的身份验证基础架构,让身份和访问策略获得最大便携性,如实现单点登录;通过自动化流程创建和更新身份凭证配置文件和用户访问策略,可跨多种身份验证基础架构进行存储。	被授予不同权限人员可更好地保证编辑部数据安全。	×	√	√	×	√	×
信息保护	保证数据通过公众网络传输及保存在外部数据的隐私和完整性,保护运行在云平台中的应用程序内嵌入的业务逻辑、交易秘密、数字内容资产和数据隐私,保护传输中信息的完整性及验证存储后信息的可靠性。	涉及编辑部数据的完整性以及隐私保护。	×	√	√	×	√	×
平台服务连续性	平台级的安全监控、审计以及法定责任和事件响应等。	涉及日常业务中异常事故告警与及时处理。	×	√	√	×	√	×
工程安全	在服务的设计与开发时引入安全设计以及编码评估。	涉及整个日常业务。	×	√	×	√	√	×
应用安全	包括审计和日志、身份验证、授权、通信、配置管理、算法、例外管理、敏感数据、会话管理和验证等。	涉及整个日常业务。	×	√	×	√	√	×
与自身相关的信息安全	保护用户账号以及密码等信息的安全。	涉及用户在使用过程中的权限安全控制。	×	√	×	√	×	√

注:√表示要负责,×表示不需负责。

如果由于某些特殊原因不便采用 SaaS 的云计算模式,那么编辑部至少也应该采用 PaaS 的模式。这样,编辑部在云计算服务供应商提供的基础设施和平台之上,只需集中关注编辑部数据管理相关的应用服务及有关安全问题,具备一定的可行性。但是,对于小型期刊编辑部而言,考虑到应用与安全服务的复杂性,不建议采用 IaaS 的方式。

2.3 云计算安全问题分析

根据 Gartner 公司的总结^[8],云计算安全问题具体可以概括为如下 7 方面:

- (1) 特权用户访问风险: 避免管理员等特权用户的非法访问;
- (2) 法规遵守风险: 云服务供应商不能以内部规定为由拒绝外部审计;
- (3) 数据位置不确定风险: 隐私数据存储的位置不确定带来的风险;

(4) 共享存储数据风险: 多个云计算用户共享数据存储时应保证数据隔离;

(5) 数据恢复风险: 供应商必须具备数据备份与故障恢复功能;

(6) 调查支持风险: 通过数据跟踪功能支持对非法行为的取证;

(7) 长期发展风险: 服务长期性、稳定性和可持续性。

可以看出,上述问题既有政策法规方面的问题,也有技术方向的问题,因此,对云背景下编辑部数据安全防护的策略也应该分别从法规和技术两个方面进行思考。

3 云背景下编辑部数据安全防护的思考与对策

3.1 思考与总体对策

我们通过日常编辑工作,在已有工作实践基础上,对云

背景下编辑部数据安全防护问题做出了如下思考和总体策略。

(1) 应从政策层面上给出法律依据,建立准入制度,并严格审查和认真审计

云存储服务供应商的最终目的是在提供服务的同时获取最大利益,因此要求云存储服务供应商在无任何约束条件下靠自律来保障信息安全是不现实的,必须通过国家相关管理部门制定法律法规,从政策层面上强制其采用必要的安全措施,保障云服务以及云端数据的安全。

具体可通过审查认证获得相应服务资格,并坚持定期审查和复查,并在服务商运营的同时认真进行后台审计,一旦发现安全漏洞立即要求服务商整改,如果整改后依然达不到要求应取消其运营资格。

(2) 从技术层面上给出有力保障

从技术层面上制定各种安全防护措施,给出有力保障。应着重审查云存储平台的用户身份验证、访问控制、入侵防御、反病毒部署、数据迁移备份、防止内容数据泄密和网络内容与行为监控记录等措施^[8]。

(3) 从意识层面上加以强化

编辑部自身应根据相关规定强化安全保密意识^[9],具体包括:

①编辑部应谨慎选择云端服务商,并在工作中加强安全保密意识。选择那些服务好、具有完备安全防护措施的云服务提供商。一旦发现服务商在提供数据过程中存在风险和漏洞,应进行及时告警并中止合作。

②编辑部应定期更新备份数据,防止在云服务过程中由于各种原因造成服务中止以及云端消失时编辑部数据无法正常使用的现象。

3.2 技术策略

从技术角度考虑,云背景下编辑部数据安全防护应重点考虑以下6方面^[8]:

(1) 身份认证与访问授权

必须在用户身份生命周期全过程中,有效地管理用户身份和访问资源权限,包括用户注册、用户管理、用户身份标识、用户访问与权限控制以及单点登录等。

(2) 数据访问权限控制

必须建立较为完备的数据访问权限控制,并在每次数据访问时进行检验,并对用户的具体访问情况进行审计记录并保存以备查。

(3) 数据资源的私密性

用户存储在云端的数据不能被包括服务供应商在内的

人员进行非法查看或篡改,因此必须对数据进行存储隔离和存储加密。此外,数据在运行时(如加载到系统内存)也要采用虚拟机隔离或操作系统隔离等技术手段,确保不被其他人非法查看或篡改。

(4) 数据完整性

必须对数据的完整性进行检验,确保在任何时候,用户存储的数据都保持不变,不会随着时间变化而改变或被意外破坏。

(5) 数据的持久可用性

即使发生各种突发事件和灾难时,用户也可以随时获得自己的数据,可对数据进行备份、镜像以及分布式存储。

(6) 数据接口的易用性

云服务供应商应提供较完备和易用的数据接口,可允许云计算用户其接口对数据的展现内容和方式进行定制,可方便对数据进行在线或离线维护,并能够提供完备的数据分析报告。

4 结束语

科技发展推动了社会进程,以云计算为代表的新型计算模式提供了更加高效、快捷和灵活的数据存储与管理方案,可成为小型科技期刊编辑部数据管理的有效手段。但是,在这一过程中,数据安全是一个不容忽视的问题,编辑部应利用新技术和新思维来构建一个安全、可靠的数据运行环境,使科技期刊编辑工作得到良性发展。

参考文献

- 1 司品超,董超群,吴利等. 云计算概念、现状及关键技术. 2008年全国高性能计算性能学术年会论文集. 无锡:中国计算机学会高性能计算专业委员会,2008:31-36
- 2 单敏. 图书馆应用云计算的问题分析与应对措施. 漳州师范学院学报:自然科学版,2010,(2):177-180
- 3 中国编辑学会. 有关出版的法律法规选编. 北京:中国大百科全书出版社,2010:26-42
- 4 郭乐深,张乃靖,尚晋刚. 云计算环境安全框架. 信息网络安全,2009,(7):62-64
- 5 Brodtkin. Gartner: seven cloud-computing security risks. (2008-07-02) [2012-05-30]. <http://www.Networkworld.com/news/2008/070208-cloud.html>
- 6 郭凌翔. 浅谈云存储及其安全性. 福建电脑,2010,(5):86,100
- 7 马岚,杨悦. 建立健全科技期刊的保密审查制度. 中国科技期刊研究,2012,23(2),291-294
- 8 胡勇祥. 基于云计算环境下数字资源共享模式的研究. 科技创新导报,2012,(5):44