云服务中的数字学术信息资源安全风险防范*

周知，吕美娇
（武汉大学信息资源研究中心，武汉 430072）

摘要：随着大数据时代到来，数字学术资源的存储与服务越来越依托于云技术开展，云服务成为数字学术信息服务的主要架构，在数字图书馆等知识服务机构中的应用日益广泛。但由于技术环境、用户调用关系的改变，云服务中的数字学术信息资源安全问题趋向复杂化，对此本文提出一种面向关键环节的云服务数字学术资源安全防范框架。

关键词：云服务；数字学术信息资源；风险防范
中图分类号：G203
DOI：10.3772/j.issn.1673-2286.2017.07.003

大数据时代数字学术信息资源增长迅速、类型复杂，同时随着用户访问调度频繁、任务需求内容复杂，传统的本地存储与服务架构已无法满足用户需求[1]。面对这种情况，国内外各类知识机构信息服务工作，倾向选择基于云技术开展，如联机计算机图书馆中心（OCLC）的在线编目联合目录服务、中国高等教育文献保障系统（CALIS）的数字图书馆云平台构建、国家科技图书文献中心（NSTL）的多馆共享云服务体系构建等。然而，云服务在提升用户服务水平，提高资源管理效率的同时，也带来新环境下的安全风险问题，包括个人隐私泄露、知识产权侵害、分布式攻击等[2]。

知识服务机构利用云服务虽可以给用户提供便利服务，为资源带来高效管理，但也面临更加复杂的安全问题。因此，以科学的视角看待云服务中数字学术信息资源安全问题，从管理和技术等角度提出防范体系十分重要，但目前鲜有研究对该问题提出有针对性的管控策略。鉴于此，本文在充分分析云服务中数字学术信息资源风险发生机制与关联机制的基础上，提出面向关键环节的安全风险防范体系，为实践工作开展提供参考。

1 云服务中的数字学术信息资源风险机制

云服务中的数字学术信息资源面临各种潜在风险，制定相关的防范措施需分析风险发生机制与影响机制，根据其发生条件、环节与特征，进行针对性管控。

1.1 数字学术信息资源风险发生机制

我国对云服务风险分析的相关标准有待完善，《中华人民共和国国家标准信息安全技术、信息安全风险评估规范》（GB/T 20984—2007）是我国关于信息安全方面的国家标准，该标准通常用于信息系统的风险管理、评估等活动[3]。云服务本身是一种信息系统，可以利用国家标准对其进行风险发生机制分析。云服务中的数字学术信息资源风险发生机制，如图1所示。

（1）云服务中数字学术资源资产要素。资产是组织的核心，不同类型资产的价值类型不同（包括硬件资产、软件资产和数据资产），云服务中数字学术信息资源是云系统中最重要的资产（包括数据库、科研论文、科研数据等）。资产由于各方面原因容易被破坏、窃取和利用，因此确保数据资产的安全需耗费一定成本，云服务中的数字学术信息资源的风险识别也应以数据资产为主。

（2）云服务中数字学术资源威胁要素。威胁来自云服务系统的内部和外部，增加风险发生的可能性，并

* 本研究得到国家社会科学基金重大项目“云环境下国家数字学术资源信息安全保障体系研究”（编号：14ZDB168）资助。

有可能演化为安全事件。按照威胁的危害程度，可设置不同的对抗级别，根据其发生作用的环节进行有针对性的管控部署，并结合定性与定量方法，识别出最重要的威胁。

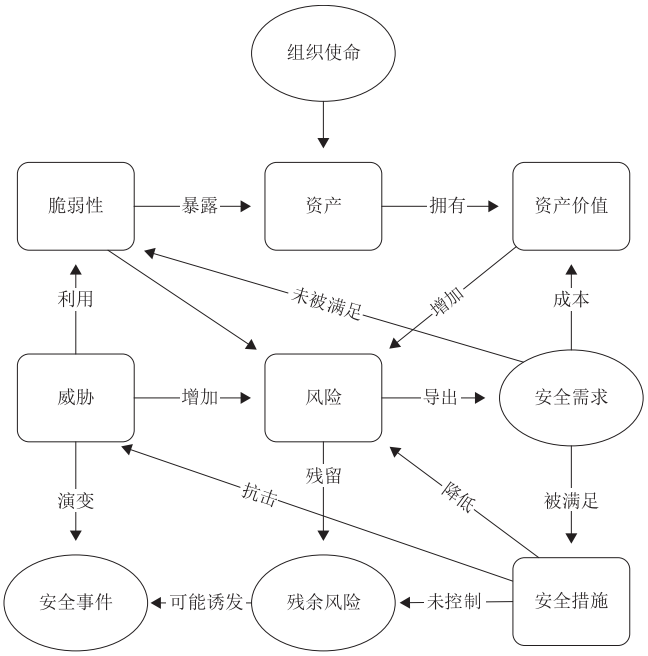

图 1 云服务中的数字学术信息资源风险发生机制

（3）云服务中数字学术资源脆弱性要素。脆弱性暴露云服务中数据资产的价值，增加了风险的可能性，成为威胁发生的重要途径。因此，脆弱性是风险识别与管控的重要因素，将脆弱性加固可切断风险链条，对脆弱性的分析可从云服务系统的安全需求或威胁的角度入手。

1.2 数字学术信息资源风险关联机制

确定云服务中的学术信息资源安全风险发生机制，明确防范措施应以数据资产、软件资产和硬件资产为核心，进行风险关联机制分析。本文借鉴系统动力学思想，将系统中资产的风险以因果关系进行关联机制表示（见图2）。

（1）云服务中的硬件风险关联机制。给硬件资产造成直接破坏的威胁有7项，包括保养不当、偷盗、内部员工蓄意破坏、存储介质故障、硬件操作失误、硬件维护失误、网络部件技术故障。

风险的连带关系包括：工作人员缺乏资产维护意

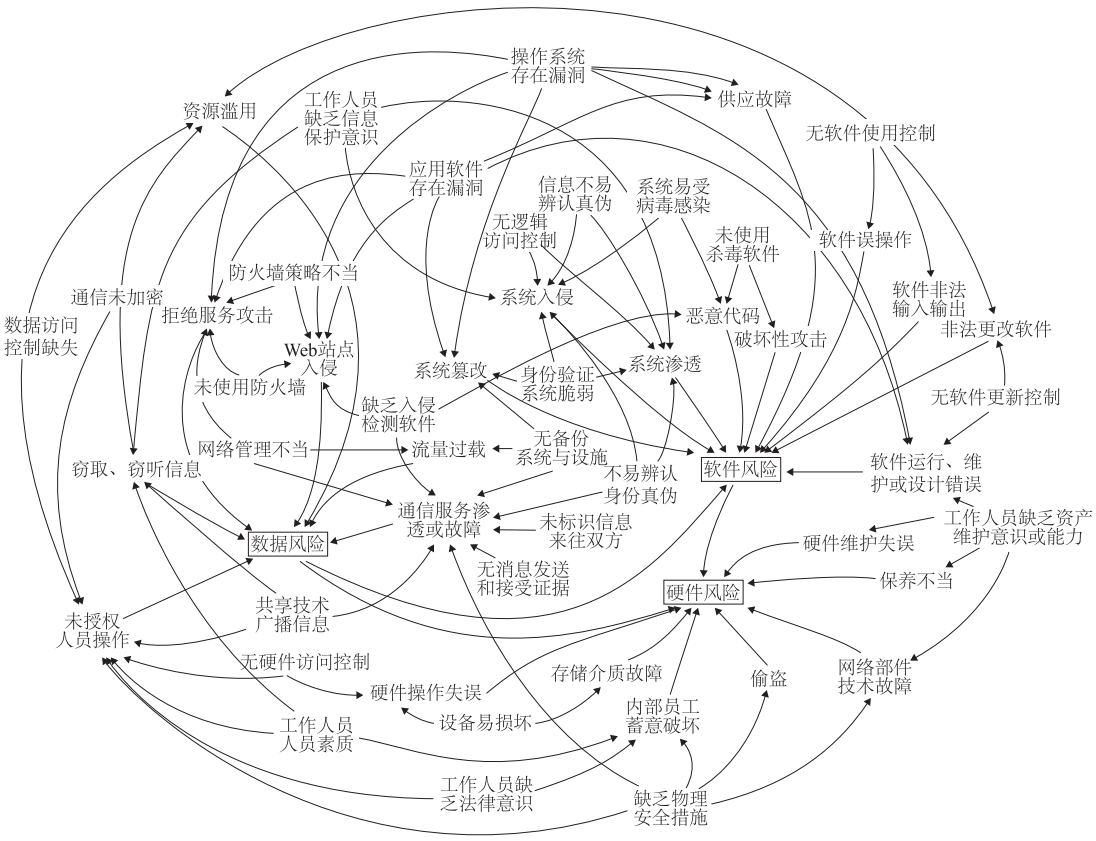

图 2 云服务中的数字学术信息资源风险关联机制

识或能力（脆弱性）—保养不当/硬件维护失误/网络部件技术故障（威胁）—硬件风险（资产）；缺乏物理安全措施（脆弱性）—偷盗/内部员工蓄意破坏/网络部件技术故障（威胁）—硬件风险（资产）；工作人员人员素质（脆弱性）—内部员工蓄意破坏（威胁）—硬件风险（资产）；设备易损坏（脆弱性）—存储介质故障/硬件操作失误（威胁）—硬件风险（资产）；无硬件访问控制（脆弱性）—硬件操作失误（威胁）—硬件风险（资产）。

（2）云服务中的软件风险关联机制。软件资产的侵害路径包括供应故障、恶意代码、破坏性攻击、系统入侵、系统渗透、系统篡改、软件误操作、软件非法输入输出、非法更改软件及软件运行、维护或设计错误。

风险连带关系包括：应用软件存在漏洞（脆弱性）—供应故障/系统篡改/软件运行、维护或设计错误（威胁）—软件风险（资产）；操作系统存在漏洞（脆弱性）—供应故障/系统篡改/软件运行、维护或设计错误（威胁）—软件风险（资产）；未使用杀毒软件（脆弱性）—恶意代码/破坏性攻击（威胁）—软件风险（资产）；系统易受病毒感染（脆弱性）—恶意代码/系统入侵/系统渗透（威胁）—软件风险（资产）；缺乏入侵检测软件（脆弱性）—恶意代码（威胁）—软件风险（资产）；不易辨认身份真伪（脆弱性）—系统入侵/系统渗透（威胁）—软件风险（资产）；信息不易辨认真伪（脆弱性）—系统入侵/系统渗透（威胁）—软件风险（资产）；无逻辑访问控制（脆弱性）—系统入侵/系统渗透（威胁）—软件风险（资产）；身份验证系统脆弱（脆弱性）—系统入侵/系统渗透（威胁）—软件风险（资产）；无备份系统与设施（脆弱性）—系统篡改（威胁）—软件风险（资产）；无软件使用控制（脆弱性）—软件误操作/软件非法输入输出/非法更改软件（威胁）—软件风险（资产）；工作人员缺乏资产维护意识或能力（脆弱性）—软件运行、维护或设计错误（威胁）—软件风险（资产）；无软件更新控制（脆弱性）—软件非法输入输出/非法更改软件（威胁）—软件风险（资产）。

（3）云服务中的数据风险关联机制。给数据资产造成直接破坏的威胁包括：Web站点入侵、拒绝服务攻击、未授权人员操作、流量过载、窃取或窃听信息、资源滥用通信服务故障或渗透6项直接风险，及因硬件资产、软件资产受破坏后带来的连带风险。

风险连带关系包括：应用软件系统漏洞（脆弱性）—Web站点入侵/拒绝服务攻击（威胁）—数据风险（资产）；操作系统漏洞（脆弱性）—Web站点入侵/拒绝服务攻击（威胁）—数据风险（资产）；未使用防火墙（脆弱性）—Web站点入侵/拒绝服务攻击（威胁）—数据风险（资产）；缺乏入侵检测软件（脆弱性）—Web站点入侵/通信服务故障（威胁）—数据风险（资产）；防火墙策略不当（脆弱性）—Web站点入侵/拒绝服务攻击（威胁）—数据风险（资产）；共享技术广播信息（脆弱性）—未授权人员操作/窃听、窃取信息（威胁）—数据风险（资产）；工作人员素质（脆弱性）—未授权人员操作/窃听、窃取信息（威胁）—数据资产（风险）；工作人员缺乏法律意识（脆弱性）—未授权人员操作/窃听、窃取信息（威胁）—数据资产（风险）；数据访问控制缺失（脆弱性）—未授权人员操作/窃听、窃取信息（威胁）—数据资产（风险）；无硬件访问控制（脆弱性）—未授权人员操作（威胁）—数据风险（资产）；缺乏物理安全措施（脆弱性）—未授权人员操作/通信服务故障（威胁）—数据风险（资产）；通信未加密（脆弱性）—未授权人员操作/窃听、窃取信息/资源滥用（威胁）—数据风险（资产）；无备份系统与设施（脆弱性）—流量过载（威胁）—数据风险（资产）；无软件使用控制（脆弱性）—资源滥用（威胁）—数据风险（资产）；不易辨认身份（脆弱性）—通信服务渗透或故障（威胁）—数据风险（资产）；无消息发送或接受证据（脆弱性）—通信服务渗透或故障（威胁）—数据风险（资产）；未标识信息来往双方（脆弱性）—通信服务渗透或故障（威胁）—数据风险（资产）。

2 云服务中的数字学术信息资源风险防范体系

云服务中数字学术信息资源因其固有的脆弱性，在多风险联动的过程中时刻受到威胁。在明确发生机制和关联机制的基础上，构建对应全面防范的体系需考虑风险影响因素（包括内在与外在、故意人为和无意人为），并基于此构建面向数据处理关键环节的防范体系。

2.1 云服务中数字学术信息资源风险影响因素

在云服务中数字学术信息资源风险发生机制和关联机制的作用下，多种影响因素对系统资源构成威胁。

因此需明确影响因素类型，基于此提出相关防范体系框架。

（1）环境因素。环境因素主要影响系统硬件资产，威胁发生形式包括物理环境问题（断电、静电、灰尘、潮湿等）和自然灾害（洪灾、火灾、地震等）。环境因素以最简单直接的方式对硬件资产造成无差别、难以修复的破坏。由于涉及软件的运行和数据的调用与恢复，对硬件资产的完整性和可用性要求较高，而环境因素的不可控、伤害程度难以预测、潜在问题难以发现等均对硬件资产产生影响，并经由硬件资产对数据资产造成破坏。硬件资产的完整性和可用性直接影响软件的运行以及数据的调用与恢复，环境因素的不可控、伤害程度难以预测、潜在问题难以发现等特征均对硬件资产造成直接威胁，并最终对软件与数据造成破坏。

（2）内部恶意人为。内部恶意人为破坏性较大，具有一定的隐蔽性。内部人员因具有合法身份，可方便地绕过系统的访问控制和认证环节，进而对资产的完整性和可用性造成破坏。通常技术程度较低的内部人员对硬件资产造成直接损害，有一定技术能力的内部人员则修改源代码或对敏感数据进行窃取。

（3）内部非恶意人为。内部非恶意人为行为主要由于内部人员的能力和意识方面存在欠缺，而导致员工误操作或造成系统安全漏洞。如云服务管理数据误删、权限过度开放、云服务硬件设施维护不及时或维护失误、云服务软件系统补丁更新不及时、访问控制密码设置简单、系统安全评估工作不及时等。

（4）外部恶意人为。外部恶意人为是系统威胁的主要来源，这种行为有明确的目的性和指向性，针对云服务系统特定资产进行破坏。外部恶意行为破坏性较强，是云服务系统的主要防范对象。

（5）外部非恶意人为。云服务系统是依照权限开放的系统，系统外部用户在权限范围内需要调用系统资源，但安全意识稍弱的外部用户通常会成为系统的人因漏洞。将自身的安全信息泄露给其他非授权人士等。除本身的误操作行为外，其自身也可能成为外部恶意人员利用目标。外部非恶意人为行为需要内外部共同控制，以保障系统资源的安全性、完整性、保密性。

2.2 面向关键环节的数字学术信息资源安全防范体系构建

数字学术信息资源的安全问题伴随数据的生命周期产生，因此，安全防范应针对云服务系统中数据流程开展。

2.2.1 云服务中数字学术资源存储环节风险防范体系

云服务中数字学术资源的数据存储流程：第一，通过内部平台客户端登录数据采集系统；第二，利用云服务管理系统进行数据采集；第三，对数据进行预处理后存入云存储分布系统。根据流程得知风险防范要求包括内部人员登录云服务系统时的认证与控制环节，应用程序采集环节，数据传输和入库环节。针对这些问题，需要部署相应的风险防范措施（见图3）。

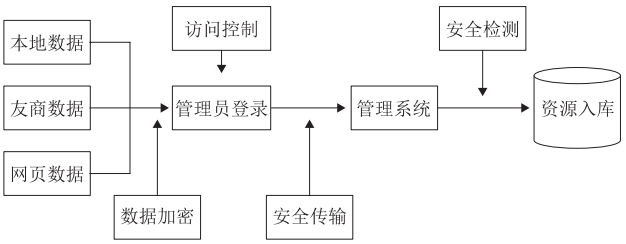

图 3 云服务中的数字学术信息资源采集环节风险防范

（1）访问控制。数字学术资源云服务存储涉及系统数据库变更与系统调度使用，其过程复杂，易产生安全问题。未授权用户操作是权限和认证环节最重要的风险，所以必须在风险的源头进行控制。一方面，要提高工作人员风险意识与控制风险能力，采取多维认证机制[4]，如提交动态口令；另一方面，在访问控制上细化访问粒度，对不同等级的用户赋予不同的权限[5-6]。

（2）数据加密。云服务系统中不同的数字学术资源保密等级不同，对于保密等级较低的资源（如数字化的期刊论文、报纸等）可使用明文传输；而如E-science平台的科研数据、中国高等教育文献保障系统的未公开学位论文等仍有较高的密级，这类资源既要保证不被外部恶意人员通过技术手段窃听、窃取，也要保证内部人员不滥用合法权限使用。对保密周期短、重要性低的数据，采用简单、低成本的加密算法；对保密周期长、重要性高的数据采用复杂的加密算法，同时加密数据可能在密级到期之前涉及部分高权限用户的使用，因此需要支持检索或内容挖掘的加密算法[7]。

（3）安全传输。云服务系统的数字学术信息资源在传输过程中容易发生问题，为保证数据在传输过程

中不被恶意篡改或窃取，需要利用好各种安全协议，如安全套接字层协议、网络安全协议等。

（4）安全检测。云服务系统中的数据来源广泛，包括互联网数据。而入侵检测系统无法检测到互联网中包含的恶意代码，所以在组织数据入库前应对数据内容进行安全检测，通过文本过滤、安全等级划分等技术对数据进行初步控制，采用攻击特征码匹配、校验法进行深入检测。

2.2.2 云服务中数字学术资源开发环节风险防范体系

云服务系统资源开发形式多样，为实现资源的充分利用和信息服务的知识化、综合化，系统通常对资源进行充分开发，形成一系列的应用，如信息检索、知识挖掘、信息推荐、学科门户、嵌入式服务等[8]。资源开发后，既可以形成新的二次信息，也可能形成新的服务形式。在资源开发过程中，需保证云服务系统中数据资源的完整性和保密性。数据未完成加工前不得向外泄露，在此过程中需采用访问控制、基础安全、共享安全等手段进行风险防范（见图4）。

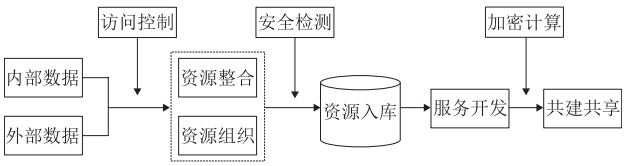

图 4 云服务中的数字学术信息资源开发环节风险防范

（1）访问控制。云服务系统中数据的开发涉及数据调用和系统操作，因此，需要通过认证机制和等级权限，对资源加工系统的访问进行等级划分，同时设置相应的密码机制进行访问控制。

（2）基础安全。云服务系统中学术数字资源的开发过程包括一系列单独过程，如文件操作、程序编码、控制变更、开发容错。每一环节都需要进行安全管理与控制，将数字学术资源的开发视作完成的流程，针对流程进行管理，制定管控标准。其中开发容错并非对不符合标准的数据容忍入库，而是需要接受数据前对数据的安全检测。

（3）共享安全。资源开发可能涉及其他相关系统或第三方合作伙伴，离不开数据共享技术，而共享技术可能导致恶意入侵，因此基于保密性考虑，共享的数据应用加密技术进行保护。此时需要处在主导地位的学术信息系统进行密钥管理与分配，保证数据不受内部误操作和外部篡改破坏的影响。

2.2.3 云服务中数字学术资源服务环节风险防范体系

云服务的服务流程与一般系统的服务流程没有明显区别，即用户通过服务界面发出服务请求，由系统对用户的身份与权限进行验证，并提供相应服务。如果服务需要用户不断细化要求，则用户与系统继续交互，直到用户得到相应结果或在某一步终止服务。

系统在向外部提供服务的过程中涉及数据传输，因此，在保障服务的同时需充分维护自身数据资产安全，针对服务环节部署风险防范措施。根据风险识别结果，流量过载、通信服务故障、拒绝服务攻击均为重要威胁点，这些风险可造成服务失败与数据不可用，云服务中的数字学术信息资源服务环节风险防范如图5所示。

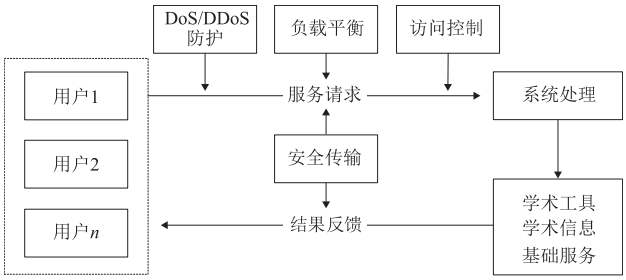

图 5 云服务中的数字学术信息资源服务环节风险防范

（1）拒绝服务攻击。拒绝服务攻击或DDoS（Distribute Denial of Service）对云服务系统造成破坏，致使数据无法调用、服务中断。系统应将拒绝服务攻击外包或在系统内部自建，措施包括基于行为分析的控制和基于测试的控制[9-10]。

（2）网络负载均衡。随着数据量增大和访问频发，流量过载成为系统待解决的主要问题之一。流量过载造成访问超时，系统可用性变差。利用负载均衡技术可将用户的服务请求分布到多个后台进行处理，该环节工作也可外包或自建，使用IP分流或多线程的方法进行均衡处理[11]，或采用第三方外包服务，利用云服务的复杂存储均衡能力对该部分进行风险防范。

（3）访问控制。针对云服务系统特点，对用户访问采取不同等级区分控制方法。软件下载、论文元数据、学界动态等信息开放访问，无须认证；资源内容查看、

文献传递等内容服务，需根据用户权限信息有选择地开放访问入口，对有合作的科研院所或高校可使用基于IP网段的访问控制；对个人用户可使用账号密码验证的方式进行控制。

3 结语

随着科研第四范式时代到来，科学数据量增长迅速，用户需求复杂，传统的本地数据服务很难满足用户需求，云服务逐渐成为知识服务机构的主要服务方式，然而云服务中的数字学术信息资源安全问题较复杂，在风险发生机制和关联机制的影响下其表现形式多种多样。这些问题对用户隐私、数据安全造成直接的威胁，影响到服务开展和资源开发。本文在充分分析云服务中数字学术信息资源风险发生机制与关联的基础上，对风险的造成因素进行分析。明确了以关键环节为核心的风险防范方式，对云服务中数字学术资源的采集、开发、服务环节进行针对性防范。面对这种情况，本文在分析其风险机制的基础上，对造成风险的要素进行分析，提出一种面向关键环节的安全风险防范体系，为云服务中的数字学术资源安全实践提供参考。

参考文献

[1] 苏新宁.大数据时代数字图书馆面临的机遇和挑战[J].中国图书馆学报,2015(6):4-12.

[2] 胡昌平,黄书书.公有云存储服务中的用户权益保障[J].情报理论与实践,2016(11):17-21,27.

[3] 黄水清,任妮.数字图书馆信息安全风险评估的方法与模型[J].图书情报工作,2014,58(2):14-20.

[4] BANYALR K,JAIN P,JAIN V K.Multi-factor authentication framework for cloud computing[C]//5th International Conference on Computational Intelligence,Modelling and Simulation.IEEE Computer Society,2013.

[5] 李凤华,苏铓,史国振,等.访问控制模型研究进展及发展趋势[J].电子学报,2012(4):805-813.

[6] 苏铓,李凤华,史国振.基于行为的多级访问控制模型[J].计算机研究与发展,2014(7):1604-1613.

[7] LIU Z,WANG Z,CHENG X, et al.Multi-user searchable encryption with coarser-grained access control in hybrid cloud[C]//4th International Conference on Emerging Intelligent Data and Web Technologies.IEEE Computer Society,2013.

[8] 数字图书馆推广工程[EB/OL].[2017-07-01].http://www.ndlib.cn/xtjs2012/201201/t20120113_57991_1.htm.

[9] 文坤,杨家海,张宾.低速率拒绝服务攻击研究与进展综述[J].软件学报,2014(3):591-605.

[10] 李禾,王述洋.拒绝服务攻击/分布式拒绝服务攻击防范技术的研究[J].中国安全科学学报,2009(1):132-136.

[11] 陈佐,杨秋伟,万新,等.一种多线程负载均衡分析方法研究[J].计算机应用研究,2011(5):1752-1755,1760.

作者简介

周知，男，1989年生，博士研究生，研究方向：用户行为研究、信息资源管理与服务，E-mail：zhouzhi@whu.edu.cn。
吕美娇，女，1987年生，博士研究生，研究方向：信息安全，E-mail：416852559@qq.com。

Digital Academic Information Resources Security Risk Prevention in Cloud Services

ZHOU Zhi, LV MeiJiao
(Center for Studies of Information Resources, Wuhan University, Wuhan 430072, China)

Abstract: With the arrival of the era of big data, the storage and service of digital academic resources are increasingly relying on cloud technology, and cloud services have become the main framework of digital academic information services. In the digital library and othe institutunions,the applications are more and more widely used. However, with the technical environment, users call the change of digital information resources of academic security problems in cloud service tend to be complicated, this paper proposes a key link for the cloud service digital academic resources security framework.

Keywords: Cloud Service; Digital Academic Information Resources; Risk Prevention

（收稿日期：2017-07-06）