数字学术信息资源云存储安全保障*

李霜双，胡昌平
（武汉大学信息资源研究中心，武汉 430072）

摘要：数字图书馆作为数字学术信息资源服务的主体，面向用户的云存储服务的拓展具有重要的现实性。在服务组织中，由于云存储的开放性和服务调用关系，其安全保障是开展服务的前提。本文从存储服务安全需求出发进行数字学术信息资源安全保障的层次分析和基于安全层次的保障实施，以云存储平台安全保障为核心，探讨其中的安全规范和基于安全规范的数字学术信息资源云存储平台运行安全保障。

关键词：学术信息；云存储服务；安全保障
中图分类号：G203
DOI：10.3772/j.issn.1673-2286.2017.07.002

随着云存储技术的发展，数字学术资源的信息存储、组织与利用处于新的变革中。云存储应用于数字学术资源建设不仅能提高资源的存储和利用效率，也能节约成本，便于对数字学术资源进行统一管理。然而，云存储中的数字学术资源安全也面临众多挑战。当前，安全已成为云存储服务进一步发展的关键。云存储环境下数字学术资源的开放和共享所涉及的权益保护问题，使其安全问题变得更加复杂和突出[1]。因此，有必要对数字学术资源云存储服务和利用的安全进行全面分析，对数字学术资源云存储安全保障进行系统研究。

1 云存储安全保障的层次结构与基于层次结构的安全保障

在数字学术资源云存储安全保障研究中，刘芳等对国内外现有的安全评估技术进行分析，针对云存储系统存在的问题进行评估方案的优化[2]；毛剑等针对隐私信息保护需要，提出基于可信服务器的云存储技术架构，以实现数据和用户个人信息的隔离[3]；王健宗分析了公有云平台的稳定性、可获得性及可靠性保障机制等[4]。2015年12月31日，全国信息技术标准化技术委员会云计算标准工作组制定《信息技术云计算参考框架》（GB/T32399—2015）、《信息技术云计算概论与词汇》（GB/T32400—2015），将全国信息技术标准化技术委员会及其云计算工作组已发布的六项标准纳入管理框架，从而确定云存储安全保障的基本层次和基于全面安全保障的实施框架[5-6]。

1.1 学术信息资源云存储安全层次结构

在国家基本实施框架下，基于云存储平台和系统的基本结构决定云存储安全的层次结构。金瑜等认为对数字学术资源机构来说，其面临的安全问题是如何确认和保证数字学术资源的安全，并指出可以通过SLA安全等级协议和资源备份，同时依托云服务提供方等级协议来实现[7]。对用户而言，其个人信息和隐私安全也依赖于云服务安全保障体系。基于此，云存储的安全层次可分为访问层、应用接口层、基础设施层、虚拟化层、数据中心层（见图1）。数字学术资源云存储安全保障着重解决以下问题。

（1）在访问层对用户实行身份认证和访问授权控制。云存储环境下数字学术资源服务面对的应用系统烦多、用户数量庞大，包括对用户账号、身份认证、用户授权进行有效管理等，同时操作审计的难度也在不断加大。因此，需要进行用户安全管理，其中涉及用户身

* 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。

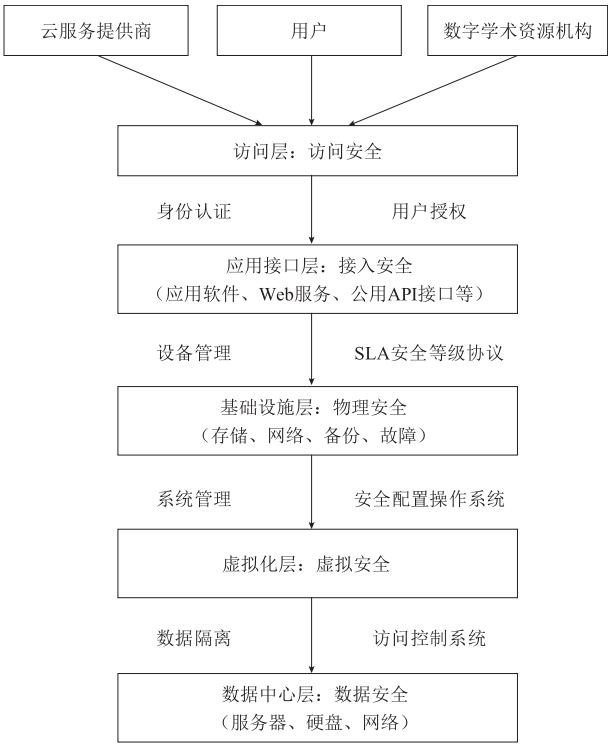

图 1 云存储安全层次结构

份管理、认证与授权管理等多方面。

（2）在应用接口层实现网络虚拟化，需要从多租户网络拓扑结构出发，针对不同云服务模式进行网络安全部署。在SDN架构中，底层基础设施和网络服务的应用程序被抽象化，需构建具有弹性的可信网络，利用可信网络实现学术信息传输安全保障，防范学术信息资源数据传输的安全风险。

（3）基础设施层主要是设备的物理安全问题。通过设置物理安全边界保护基础设施安全，对安全域实行物理访问控制。物理安全管理模块涉及软硬件基础设施、安全域管理、物理环境安全等。

（4）在虚拟化层实现多租户环境下软件和数据的共享安全，通过虚拟化云计算资源为用户提供安全部署模式，实现以虚拟机监视器为基础的安全隔离、虚拟化内部监控和虚拟化外部监管，从多方面保障虚拟安全。

（5）在数据中心层，将学术信息资源数据存储在云端，可在迁移前通过加密技术对数据加密，保障数据在传输和云存储过程中的安全。同时，也要提供学术信息资源窃取、攻击、篡改的应对措施以降低风险。由于数字学术资源建设涉及多元主体，在采用加密技术保障数据安全的同时，还需对密钥进行有效管理。

1.2 基于安全层次结构的保障实施

在云存储中，数据存储在云端，主要依靠云服务提供方的内部人员进行管理，一旦内部人员进行不安全操作、非授权访问或恶意攻击，数字学术资源服务机构、云服务提供方、用户将遭受难以计算的损失[8]。计算机犯罪调查报告和其他损失评估报告均显示，内部人员的攻击约占恶意攻击的一半，且比外部攻击造成的损失更大[9]。因此，对云存储安全来说，内部人员的管理至关重要，这也是对数字学术资源云存储安全实现全面保障的重要环节。云存储安全结构的保障措施主要包括存储资源安全保障和过程安全保障。

云存储安全管理的目标是保障云存储平台和系统基础设施的正常工作，以及云存储平台中资源的安全。为实现该目标，可以在网络安全管理的基础上部署相应设施（如防火墙、入侵检测系统、入侵防护系统、漏洞扫描和防病毒等）。同时，在系统运行过程中也要实施全面质量管控。

用户使用中的存储资源安全保障主要通过用户访问控制和身份权限管理来实现。由数字学术资源服务机构和云服务提供方共同管理，协同负责。数字学术资源服务机构负责用户身份准入信息和访问权限的管理，控制数字学术资源的服务对象和可操作范围。云服务提供方根据数字学术资源服务机构提供的用户信息，通过技术操作以确保实现用户访问控制和权限管理[10]。同时，以云服务提供方内部人员的组织结构为基础，建立统一的用户身份信息管理视图，为用户的账号管理、访问控制、认证授权和安全审计提供可靠的数据支持。

过程安全保障主要指数字学术资源机构对云服务方的选择和对数字学术资源云存储过程的监管。对云服务提供方的选择，主要考虑云存储平台的服务模式能否满足数字学术资源机构的资源安全保障需求，包括云存储服务应具有的安全能力、数字学术资源机构对其运行监管的接受程度和提供监管接口的能力，以及云存储服务的可持续性和服务安全等级协议等。对数字学术资源云存储过程的监管需明确安全分工和各主体职责，注重对数字学术资源云存储各个环节和过程的控制，适时对安全保障进行评估，及时处理安全事故等。

按照安全策略和网络连接规则进行统一管理，在于有效保障虚拟安全管理措施的全面落实。对此，云存

储服务中应对云存储平台进行周期性安全测试，及时发现缺陷，并将缺陷带来的影响降到最低。当前，补丁管理是保障云存储平台安全运行的重要措施，可有效应对随时变化的环境影响，其前提是要注意及时性、严密性和有效性。

2 云存储平台运行安全保障

数字学术资源服务机构期望通过云存储平台实现数字学术资源的开放获取和共享。由于数字学术资源的传输、存储、处理等离不开网络，资源和用户的数据均存储在云端，针对云数据面临的诸多存储安全问题，维护云平台上信息资源的安全显得尤为重要和迫切。

2.1 云存储平台安全规范

云存储平台的数据来源于学术资源机构和用户群，如果云存储平台发生服务不可用等问题，造成的影响将远超过传统信息系统对其造成的影响。服务终端的威胁可能来自云存储平台和系统，系统内部的威胁主要是云平台和系统自身可靠性、安全性和可用性问题，系统外部的威胁主要是内部人员行为造成的威胁。

云存储平台的基本安全规范包括云存储平台构建和运行使用等内容。云存储平台可通过定级、备案、建设改进、等级测评和监督检查等落实其等级保护制度[11]。在这一制度前提下，云存储平台的组织和运行环节应根据基本的安全保障原则进行安全规范的落实。在日常管理中，拟进行云计算环境下的数字学术资源云存储平台安全定级评定，明确云计算中心的安全等级保护和基于等级的安全保障实施。

各种行业系统的云平台建设都要满足《信息系统安全等级保护基本要求》，数字学术资源云存储平台也应遵循该要求。在平台安全规范中，数字学术资源存储平台应加强云存储平台的物理安全、网络安全、虚拟安全规范的建设，在管理上加强对信息、用户和环境的维护管理。

数字学术资源云存储平台的基本安全规范一方面要符合信息系统安全防护的一般性要求；另一方面，《加拿大标准协会指南》是对云环境下新的安全特性的指导性要求。因此，可以将这两个要求结合起来，作为学术信息资源云平台安全体系的构建依据，同时针对云技术环境下的测评要求和指南对云存储平台进行等级测定。

数字学术信息资源云存储平台运行的安全规范应包括云存储平台及系统的设备规范、接口规范、云平台架构及软件的规范、云平台运行安全规范等。目前尚没有针对数字学术信息资源云存储安全标准和规范的规定，因此本文认为在制定规范时，应借鉴相关平台、系统和设施的安全标准，多部门共同参与，在实践中形成共识。按统一的基本原则规范，数字学术信息资源云存储平台应从源头上控制云存储资源、用户与服务的安全影响因素，实现云存储平台和安全操作的标准化、规范化。

数字学术资源存储在云平台中，云服务提供方通过云存储平台和系统为数字学术资源机构提供服务，用户通过云存储平台和系统实现数字学术资源的访问和利用，从一定程度上可以认为云存储平台是实现数字学术资源云存储的核心和关键。从总体看，安全规范直接关系到云存储平台能否正常运行，是保障云服务提供方、数字学术资源机构，以及用户实现云存储服务的前提，因此，安全规范是云存储安全管理的基本准则。

2.2 云存储安全管控中的平台运行安全

安全管控是保障云平台安全的重要条件。云存储安全管控主要依据规范对云平台运行的物理安全和虚拟安全进行保障。在此过程中，首先，需要分析其面临的安全威胁；其次，有针对性地实施安全保障措施，维护云平台和系统的信息安全、用户安全和环境安全；最后，实现云平台运行与服务的安全保障。

在基于安全管控的数字学术信息资源云存储平台安全保障中，物理安全、虚拟安全和使用安全是保障云存储平台运行最重要的三个方面（见表1）。物理安全为云平台的正常运行提供实体设备支撑，虚拟安全为云存储平台的正常运行提供技术和系统支撑，使用安全为云存储平台使用中的数据提供可靠保障，并且三个方面相辅相成。

在云存储平台运行安全中，物理安全是最容易被忽视的部分，而大部分故障由此引发。Sage Research的一项研究表明，有80%的安全问题都归结于物理安全[12]。由此可见，物理安全是云存储安全的起点，也是

表 1 数字学术信息资源云存储平台运行安全及其管控

平台安全问题	平台运行安全管控
物理安全包括网络自然环境和设施安全、平台构建硬件安全、分布式文件数据安全、物理攻击防范安全、管理误操作安全、电磁干扰防护安全等方面	物理安全管控包括自然灾害的影响防范、设施突发事故中的安全转换、数据硬件设施管理、物理攻击监控、外部干扰的全面检测与控制等
虚拟安全包括虚拟系统结构安全，分布虚拟机创建与调用安全，虚拟化攻击影响、拒绝服务安全，虚拟数据篡改、窃取安全等	虚拟安全管控包括设定虚拟安全边界、控制虚拟运行节点、清理虚拟运行隐患、适时虚拟攻击应对、防范数据窃取和篡改、实行虚拟机安全隔离等
使用安全包括平台使用中的数据资源安全、用户信息安全、平台维护数据安全、运行日志管理安全、身份认证安全、权限安全、平台使用审计安全、平台使用对环境安全的影响等	使用安全管控包括平台存储信息通信安全管控、平台使用协议管控、用户访问控制管控、平台信息资源下载安全控制、平台使用稳定性保障、基于安全规则的安全使用管理、使用风险识别与应对等

云存储平台运行和保障的重要基础。

在云存储平台和系统中，各种设备、网络线路、供电链接、媒体数据以及存储介质等都是物理安全保护的对象，其安全性直接决定云存储系统的保密性、完整性和可用性。对于云存储介质来说，不仅要保障介质自身的安全性，还要保障介质数据的安全，防止数据信息被破坏。

虚拟化是实现数字学术信息资源云存储的大规模、高性能、可扩展、动态组合，以及面向庞大用户群体服务的关键技术。虚拟化的环境，使云计算和云存储成为可能，但随着支撑和改善云存储环境等新技术的出现，也带来新的安全挑战。加上虚拟机窃取和篡改、拒绝服务攻击等问题[13]，给云存储造成重大影响。因此，在安全保障中应针对这些问题进行有效的安全监控和防范。在虚拟化环境中，虚拟机间的隔离程度是虚拟化平台的安全性指标之一[14]。借助隔离机制，虚拟机独立运行、互不干扰。学术信息资源虚拟安全可以通过对虚拟机系统的有效监控，及时发现不安全因素，保障虚拟机系统的安全运行，从而保障云存储平台运行的虚拟安全。

云存储平台使用安全主要涉及两方面：一是维护云存储平台中学术信息和资源本身；二是对用户访问行为的监管和控制，以保证用户对云存储平台资源安全使用的合法性。对这两方面的安全管控，可根据云存储平台上的信息类型来进行。云存储平台上的个人信息需专门集中地进行存储和管理，在强化其安全等级的基础上，对云存储平台上的用户信息进行组织管理。考虑到海量访问认证请求和复杂用户权限管理的问题，可采用基于多种安全凭证的身份认证方式和基于单点登录的联合身份认证技术进行授权管理。

3 云存储安全监测与服务安全监管

云存储平台的通信基于互联网，其中一部分是数字学术信息资源云存储平台内部的通信网络，另一部分是云存储平台和外部环境的通信网络。云存储平台的通信网络直接关系到用户对平台的访问及通过平台检索、下载等业务的安全性。云存储平台环境是否安全直接关系到云存储平台的安全使用。因此，有必要对云存储平台的网络环境进行监测，以确保云存储平台和系统的正常运行。

3.1 云存储服务中的信息资源安全监测

数字学术资源云存储服务的安全监管需通过数字学术资源云存储过程中的全程信息安全监测来实现，可通过对信息安全相关活动的数据收集，来寻求合理的安全监管方案。以此出发，在安全监测框架下，实现安全事故预警与应急响应，以数字学术资源云存储服务中信息资源安全事故防范为目的，在预测基础上进行事故的防范与控制。

（1）安全监测过程。云存储服务中的数字学术资源安全监测主要是对云信息系统和云服务过程中的安全事件数据进行收集、分析和报告，涉及信息资源平台用户、应用程序和系统等[15]。在监测中，需要将收集的云信息安全相关数据进行汇集，为数字学术信息资源云存储安全事件的评估提供量化参考，以便将安全事件控制在合理范围内。

（2）安全监测内容。数字学术资源云存储服务中的安全监测，存在于数字学术资源云存储服务的整个过程。云存储平台信息资源安全监测的重要内容是对

云存储平台和系统可用性的监测，目的是监控云存储平台和系统是否处于正常运行状态，一般通过分析云存储平台和系统的工作过程和状态，对其可用性指标进行评测，以此来判断云存储平台和系统的可用性。此外，安全监测还包括云存储平台和系统的可维护性和可靠性测评，可维护性主要指云存储平台和系统具有的被修复和被修改能力，可靠性指云存储平台正常运行的概率。

（3）安全监测风险。数字学术资源云存储安全监测的风险包括风险识别、量化处理和风险评估。在进行风险测评时，首先必须识别数字学术信息资源云服务所具有的不同风险；其次，有针对性地设计问卷调查项目；最后，按量化的风险要素计算风险度，风险度可作为数字学术信息资源机构的安全管控依据，以此来提高数字学术资源信息云存储的安全性。

3.2 云存储服务中的监管实施

数字学术信息资源云存储服务中的安全监管实施建立在风险管理和安全监测基础上，云存储服务中的监管可通过引入第三方监管机制，以协同方式让可信第三方进行全面监管和响应。

数字学术信息资源云存储涉及数字学术资源、云存储平台系统、云存储服务的可用性以及云存储服务中用户等的安全问题。由于数字学术信息资源云存储安全保障涉及云服务提供方、数字学术资源机构和用户主体，因此数字学术资源机构和相关方应依靠协议对数字学术信息资源云存储过程的安全进行全面监督和管理。

数字学术信息资源机构将其拥有的数字学术信息资源交由云服务提供方进行管理，意味着数字学术信息资源机构对数字学术资源控制权的部分转移，数字学术信息资源的安全保障在很大程度上也逐渐由云服务提供方决定。在这种背景下，需要考虑引入可信第三方机构，对数字学术资源云存储过程中的云服务提供方以及数字学术资源云存储平台和系统进行全面监督，其中可信第三方机构和数字学术信息资源机构的合作至关重要。通过第三方数字学术信息资源机构发现云服务提供方在安全协议内容和安全保障中未履行的问题。同时，可信第三方机构也可将监管过程中所发现的安全问题反馈给数字学术信息资源机构和云服务提供方，然后在可信第三方机构督促下，及时采取针对性的安全保障措施应对云存储服务的安全风险。

需特别关注的是，引入的第三方监管机构必须是“可信”的，这就需要建立完善的、合理的、可操作的可信第三方监管机构选择制度，构建合理的评估指标体系，对待定的第三方监管机构进行可信度评估。只有这样，才能保证云存储服务的有效监管。

4 结语

数字学术信息资源云存储服务是数字图书馆面向用户的平台服务，包括数字图书馆在内的数字信息资源服务机构正从多方面拓展基于云存储的服务业务，因此，构建数字学术信息资源云存储安全保障系统十分重要。

本文立足这一现实问题，从安全层次结构、保障关系和过程出发，探讨了基于安全层次结构的保障实施策略，按数字学术信息资源机构、云服务方、用户和环境的交互关系，提出协议基础上的云存储平台安全规范原则和安全规范基础上的平台安全管控，物理安全、虚拟安全和使用安全的维护，以及寻求信息资源云存储服务的安全监控与保障措施。本文所进行的探索，是现有理论研究的拓展，其面向现实的分析具有针对性，基于问题分析的措施有待在实践中进一步完善。

参考文献

[1] 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,2016,39(11):17-21,27.

[2] 刘芳,刘艳.云安全问题探讨[J].信息通信,2012(1):119-120.

[3] 毛剑,李坤,徐先栋.云计算环境下隐私保护方案[J].清华大学学报(自然科学版),2011(10):1357-1362.

[4] 王健宗.云存储服务质量的若干关键问题研究[D].武汉:华中科技大学,2012.

[5] 中国国家标准化管理委员会.信息技术云计算参考架构:GB/T 32399—2015[S].北京:中国标准出版社,2015.

[6] 中国国家标准化管理委员会.信息技术云计算概论与词汇:GB/T32400—2015[S].北京:中国标准出版社,2015.

[7] 金瑜,王凡,赵红武,等.云计算环境下信任机制综述[J].小型微型计算机系统,2016,37(1):1-11.

[8] 2013年云计算的九大威胁[EB/OL].[2017-06-20].http://www.csdn.net/article/2013-02-27/2814283-clouds-risks-spur-notorious-nine-threats-for-2013.

[9] 不只是无间道——真实的内部威胁程度[EB/OL].[2017-06-29]. http://safe.zol.com.cn/180/1804831.html.

[10] 雷蕾,蔡权伟,荆继武,等.支持策略隐藏的加密云存储访问控制机制[J].软件学报,2016,27(6):1432-1450.

[11] 陈驰,于晶.云计算安全体系[M].北京:科学出版社,2014.

[12] 物理层入侵是数据中心安全面临的较大威胁[EB/OL].(2009-06-04)[2017-06-20].http://datacenter.it168.com/a2009/0604/583/000000583140.shtml.

[13] XIE X, WANG W. Rootkit detection on virtual machines through deep information extraction at hypervisor-level[J].Communications and Network Security,2013,411(6):498-503.

[14] WEN Y,LIU B, WANG H M.A safe virtual execution environment based on the local virtualization technology[J].Computer Engineering & Science,2008,31(3):154-162.

[15] GOGOUVITIS S V,ALEXANDROU V,MAVROGEORGI N et al. A monitoring mechanism for storage clouds[C]//International Conference on Cloud & Green Computing.[S.1]:[s.n.],2012.

作者简介

李霜双，女，1995年生，硕士研究生，研究方向：信息服务与用户，E-mail：1596309796@qq.com。
胡昌平，男，1945年生，上海师范大学特聘教授，信息资源研究中心主任，武汉大学信息资源研究中心学术委员会副主任，博士生导师，研究方向：情报学理论、信息资源管理与服务，E-mail：hcpwhu@163.com。

Security Assurance of the Digital Academic Information Resources in Cloud Storage

LI ShuangShuang, HU ChangPing
(Center for Studies of Information Resources, Wuhan University, Wuhan 430072, China)

Abstract: As the main part of the digital academic information resources service, digital library has great practical significance for the development of user oriented cloud storage service. Based on the security requirements of storage services, this paper carries out the hierarchical structure and implementation framework of digital academic information resources security. Then taking the security of cloud storage platform as the core, the security specification and the cloud storage platform security of digital academic information resource based on security specification are analyzed. At last, this paper puts forward the organization and implementation strategy of the platform safe operation and supervision.

Keywords: Academic Information; Cloud Storage Service; Security Guarantee

（收稿日期：2017-07-06）