数字学术信息云服务中的用户安全与权益保障*

曹鹏[1]，石宇[2]
（1. 湖北大学新闻传播学院，武汉 430062；2. 武汉大学信息管理学院，武汉 430072）

摘要：数字学术信息用户的安全和权益保障是组织云服务的基本条件，其保障伴随云服务的各环节。本文按数字学术信息云服务的组织架构进行用户身份安全认证模式研究和跨系统实现，通过联邦机制进行访问控制分析，在基于环节保障和身份认证基础上探索用户隐私信息保护和用户知识产权保护的组织架构，按云服务运行管理关系进行权益保障的实施探索。

关键词：数字信息云服务；用户安全；权益保障
中图分类号：G203
DOI：10.3772/j.issn.1673-2286.2017.07.005

数字学术信息云服务用户分布广泛，包括各行业就业人员、未就业人员，以及为满足多方面需求而对云服务有利用意愿的个体和组织。这些用户对信息服务的需求特点不同，但对学术信息云服务享有利用的权利基本相同，其基本要求是在利用服务的过程中确保自身安全和权益。因此，用户安全和权益保障是组织数字学术信息云服务的基本出发点。从用户安全与权益的关系来看，云服务用户的身份安全管理、隐私保护和知识产权安全是核心功能。

1 数字学术资源云服务用户身份安全管理

在云计算环境下由于用户身份具有跨界特点，且身份管理同时影响云服务的架构和组织，因此在实现中云端进行用户身份管理难度较大。为解决学术信息及服务跨域应用中的用户身份管理问题，有必要进行集中身份安全认证，使云平台可通过Web服务对用户数据进行统一安全构架下的传输与调用。

1.1 数字学术资源云服务用户身份安全管理环节

联邦身份架构以一种安全的方式交换数字身份信息，确立互信关系机制，其目的在于维护用户个人信息的完整性和机密性[1]，对数字学术信息资源云服务而言具有现实性。鉴于这一构架的普遍适应性，在数字学术资源云服务用户安全与基于安全的权益保障中可以按基本的保证架构进行组织。在联邦身份安全管理构架下，为实现云级别身份结构认证，需要进行针对性的身份安全管理，形成针对不同身份的可拓展层次结构，实现身份安全管理概念层次结构面向全域的拓展。在身份构架中，数字信息资源服务中心进行访问控制和授权，用户账户管理在云平台架构框架下进行审计和合规处理。按照安全管理需求，用户身份安全管理包括以下内容和环节。

（1）访问控制和授权。访问控制在三个层次上进行：第一个层次是粗粒度的访问控制，监管用户对应用或资源的访问；第二个层次按数据级别进行访问控制（如通过URL进行）；第三个层次是细粒度的访问控制，控制用户对函数和视图的访问，通过赋权进行[2]。在学术信息资源云服务中，随着用户数量的增长，以及用户对资源利用方式的变化，用户群体通常以用户组的形式出现。用户组访问控制具有伸缩性，对使用规则进行访问控制和授权具有可行性，继而可通过基于角色的访问控制和基于属性的访问控制来处理授权问题。在云端，这些角色和属性可从操作系统中解耦，通过联

* 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。

邦来实现。

（2）联邦验证和单点登录。联邦在防火墙中已成为一种安全域模式，如Windows系统的安全域模型。该模型能定义组织间防火墙内信托关系，允许本地安全域代理验证基于Kerberos的远程安全域信任获取，从而将多个Windows域连接，使登录对于用户安全透明。新一代联邦模型采用基于开放标准的验证和登录控制，该标准基于XML进行构建，可实现安全域间的验证与授权数据交换，从而实现互联网的单点登录[3]。在数字学术信息资源云服务中，联邦验证和单点登录的应用具有较强的现实意义。

（3）用户账号管理与安全准备。数字学术信息资源云服务的难点在于用户数据管理[4]。当前，即便采用联邦方式，应用程序仍需一个本地账号进行用户身份安全管理。实现云端用户管理后，用户对不同应用的调用都将采用不同的方式进行处理，这是必须面对的现实问题。用户管理缺乏标准化手段，面对动态环境的处理缺少灵活性，这也是需要解决的关键问题。同时，在API自动同步本地账号的情况下，对于SAML个性化属性、用户账号准备的整合，需要相应的用户账号管理与安全工具。

（4）审计和合规。云端审计难点之一是SaaS服务的用户访问缺乏可见性，由于互联网有别于机构局域网络，其网络监控工具无法对用户行为进行有效监控，因而需要在组织基于互联网的服务中同步解决。与单一数字信息资源机构的网络服务不同，云服务审计和合规处理必须跨机构进行。同时，监管要求随云平台系统的变化而不同，因此行业云服务审计和合规框架就显得十分重要。数字学术信息资源用户身份管理框架应明确监管要求，围绕用户隐私与访问需求进行合规处理。

1.2 联邦安全管理构架下用户身份安全保障

数字学术信息资源云服务具有Web Services交互松散耦合的特点，不能采用某种独立的安全架构进行管理，而需要完整的安全服务框架支持上层应用开发，提供全面的安全服务。当前，云服务比较普遍的方式是集中式身份管理，其优势在于简化用户管理流程，将对访问控制的管理从本地多个应用系统转移到管理中心，用户数据可通过Web服务访问[5]；存在问题是各系统失去对用户数据的所有权。

针对学术信息资源云服务跨域Web Services的访问控制需求，联邦身份认证是十分有效的方式。它可提供一种简单、灵活的机制，通过联合识别、验证和授权的形式允许机构建立自身数据库，并能以结构化、受控的方式与协作单元共享。

联邦模型在分布式基础上建立安全与策略域的信赖关系，每个域在保持内部目录、元目录、账户服务配置和公钥服务的基础上，共享本地身份和安全信息。数据的信任、完整和隐私是联邦身份认证的核心，同时共享信任可耦合多种不同的身份认证系统。联邦身份认证的实现有集中模式、分散模式和混合模式。集中模式通过构建跨域的中央身份认证平台来统一实现所有域中的身份认证；分散模式在本地构建可以维护跨域身份的认证平台；混合模式是上述两种模式的叠加，旨在解决复杂网络的安全问题。

数字学术信息资源云服务联邦认证逻辑架构可采用安全属性交换框架，以虚拟联合的方式实现联盟的联邦认证。安全属性交换易于实现跨域名环境下的用户认证信息交换，其实质是一个安全门户，使应用在不需要对联合协议或数据交互过程进行特殊处理的情况下，交换认证用户的属性数据。学术信息资源云服务平台认证中的每个分中心既是服务提供者，又是身份提供者。架构服务的作用是进行认证和身份验证引导。

学术信息资源云服务在用户认证和身份安全保障时，用户在统一认证门户提交认证数据，从相应认证或分中心选择IdP进行验证；IdP将认证的请求数据转发给开放接口，由接口负责与数据库用户数据进行比对，并将比对后的验证结果反馈给IdP；若用户验证通过，则由IdP生成认证结果提交给服务操作机构执行访问控制。开放身份验证接口模块可在数字信息资源机构图书馆服务器运行，具有灵活性和普适性。

2 数字学术信息云服务中用户隐私权保障与维护

云服务平台因其基础架构的特性，在隐私保护问题方面存在不足。数据存储于用户无法掌控的云端，极有可能危及用户的隐私安全。隐私安全问题是云计算发展的主要障碍之一，针对该问题，美国政府于2012年公布隐私人权法案，强调在使用私人信息时将更多的控制权交还给用户，随后欧盟也提出一项关于“被遗忘的权力”的法案。另外，公权力与隐私保护的冲突也是

用户选择云服务需要考虑的风险点。通过对国外的隐私保障进展分析可以看出，我国学术信息资源云服务需切实强化用户隐私保护。

2.1 云计算环境下隐私安全隐患防范

学术信息资源云服务的目标是为用户提供安全可靠的数据存储方式，而用户数据存储方式所引发的安全问题也值得关注。学术信息资源云终端若无有效的防护措施，则云应用能无限制地访问终端数据并获取用户个人信息，引发隐私安全风险。

《云计算安全风险评估》列出云计算存在特权用户的接入、可审查性、数据位置、数据隔离、数据恢复、调查支持、长期生存性的风险[6]。从这些风险可知，学术信息资源云服务用户端隐私权存在三方面问题。

（1）登录与交互信息安全。可登录学术信息资源云服务平台的主体包括云计算提供者、网络维护人员和服务使用者等。对云计算提供方而言，保证用户数据不被破坏和非法窃取是基本要求；网络平台运行维护人员负责云服务平台数据的存储安全和备份，在维护过程中需要登录用户系统；云服务使用者在使用云平台时提供个人信息，同时与系统进行交互，其身份和需求应能被识别，并保证安全登录。因此，云服务平台需要进行统一的认证、权限控制、访问审计和攻击防护。

（2）云存储中的用户个人信息安全。用户一旦将数据迁移到云端，那么承载数据的物理硬件的控制权就转移到云服务平台和系统。如果采取的安全措施不当，从云服务提供方处可方便地查询用户记录，获取用户隐私；若云服务提供方存储系统出现故障，将引发用户端数据无法访问，甚至存在丢失的风险。在用户个人信息安全保障中，应确保解决这两方面问题。

（3）云服务提供商的用户审计信息安全。学术信息资源服务的数据存储和操作安全都由云计算提供者负责，因此对其监管和审计显得尤为重要。云计算服务机制决定云内部用户审计信息的存储和调用，虽对用户透明，但若发生安全问题用户无法及时应对。为充分保障用户审计数据的安全，必须制定相应的针对性措施。

2.2 数字学术资源云服务中用户隐私权的保障

用户隐私权保护问题是对学术信息资源云服务发展挑战。面对该挑战需建立一个完整的体系，从多方面进行用户隐私保护，其中技术和监管是两个基本的方面。

（1）隐私增强技术的应用。隐私增强技术可界定为用来保护个人隐私的任何技术，主要包括安全在线访问控制、隐私管理工具，以及用户数据保护框架下的数据安全技术等[7]。许多IT企业不断推出用于云计算安全的新技术。如IBM公司为提高云计算环境的安全性并确保数据保密性，推出Tivoli和Proventia。其中，Tivoli软件为智能基础设施管理提供解决方案，旨在对隐私数据进行安全、有效的管理和保护；Proventia向虚拟网络提供X-Force支持的网络保护，实现对安全云服务维护。

云环境下用户网络隐私权保护的传统技术包括访问控制策略、安全认证机制、加密机制[8-9]。访问控制策略使云端网络资源在非法使用及访问过程中得到有效保护，其中主要的途径包括目录级安全控制、网络权限控制、入网访问控制等；目前安全认证机制发展较完善，已拥有一套可应用的完整技术解决方案，X.500信息发布标准可有效应用于学术信息资源云服务用户隐私安全保障。学术信息资源云服务可结合传统技术和隐私增强技术，以构建完整的保障技术体系。

（2）安全监管机构的设立。设立以政府部门为主导的第三方监管机构，是实现云服务监管（包括数字学术信息资源）的有效手段，能在确保第三方监管机构权威的前提下，提高用户隐私安全保障的可靠性[10]。第三方监管机构主要用于监督、管理、对云服务及其用户隐私安全的评估与审计等。在第三方监管机构监管方式中，服务等级协议能行之有效地明确各参与方责任与权利。一方面，服务等级协议对保证服务中的用户安全和质量有效；另一方面，服务等级协议明确各参与方的赔偿机制及相关责任关系。监管机构为保障服务提供方及用户的各种权益，需对云服务进行多方面监督，尤其是对违反服务等级协议的行为。

学术信息资源云服务涉及信息资源服务机构与支持机构，其用户隐私安全监管需要跨机构进行。鉴于云计算环境下数据对服务器和网络的依赖性，云服务中各种隐私问题尤其是服务器端隐私问题更为突出。如用户数据的调用问题，其有效性和安全性常面临威胁，使用户对云服务应用的个人保密性及安全性产生质疑，影响云服务面向用户的发展。

因此，在引入第三方监管的同时，应着手监管标准

建设。云服务用户隐私安全相关标准的完善将促使隐私权保护问题得到更好的解决。

3 数字学术资源云服务中用户知识产权的保障与监督

面向共享的数字学术信息资源云服务，要将学术信息资源整合进行开发与利用，必然涉及用户知识产权保护问题。百度文库侵犯著作权纠纷案已引起多方关注，云计算环境下用户知识产权利益的博弈已演变为现实[11]。传统知识产权保护框架无法解决云计算环境下用户知识产权保护的问题，因此，有必要将云环境下用户知识产权保护纳入用户权益保护和安全保障的范畴，进行基于云服务框架的组织架构建设。

3.1 数字学术资源云服务用户知识产权安全保障构架

数字学术信息资源云服务的开放性和共享性，使相关知识产权保护难度较大。在我国现有法律框架下以图书馆为代表的学术信息资源服务机构，对侵权赔偿问题的处理办法还有待进一步提高。由于我国学术信息资源服务机构具有公益性质，而云服务提供商离不开商业利益，因此面临如何协调公益服务与用户知识产权保护的问题。OCLC于2009年率先尝试将云计算技术用于图书馆服务并强化图书馆资源的知识产权保护。

针对目前存在的现实问题，学术信息资源服务机构如果不直接提供内容，就不涉及直接的侵权责任。如学术信息资源服务机构对数据进行开发、修改、编辑、复制等操作后进行网络传播，供广大用户使用，按《信息网络传播权保护条例》存在侵权问题；学术信息资源服务机构将单位获取授权的数据传播给其他未授权机构使用，也存在侵权问题。

在数字学术信息资源云服务中，通过合作进行学术信息资源服务的机构，不可避免地面临共同承担侵权的责任风险问题。云服务平台涉及的知识产权保护，所面临的基本问题是数字学术资源著作权、传播权和利用权等权利问题。同时，鉴于数字学术资源服务的公共性和开放服务的公益性，其知识产权保护涉及知识共享协议、云服务中的知识传播和利用问题。

基于知识共享协议，数字学术信息资源云服务可在知识共享协议框架下进行知识产权保护，在允许学术信息资源发布前，由其拥有者根据相关条款自主选择不同类型资源的知识保护程度[12]。通过知识共享协议，知识产权拥有者可选择不同的方式进行授权，以约束不同程度的信息传播与利用，以此规定用户的产权委托或转让，规避云计算环境下学术信息资源侵犯资源拥有者知识产权的风险。学术信息资源云知识共享协议可按授权人指定的方式进行标识，为协议的被授权人员提供使用权限；限制商业性利用，授权公益性利用；同意自由利用具有知识产权的资源，但不能改变其形式和加工其内容；限制在利用中开发新的产品获利等。

此外，在数字学术信息资源云服务中，学术信息资源服务机构可针对知识产权保护进行协商，按知识产权保护条例分配使用权限和衍生成果[13]。

通过对学术信息资源数据进行加密传输、密文存储、统一授权、访问控制等措施，可对用户的学术信息资源的利用与传播进行限制，对有权限的用户进行识别和认可，以确保学术信息资源知识产权的有效保护。同时，将不同知识保护程度的数据进行区分，防止用户过度使用或非授权其他用户的情况发生。从风险控制看，通过技术手段对学术信息资源用户的知识产权保护，有利于降低学术信息资源服务机构和学术信息资源用户知识产权侵权的风险。

3.2 云环境下基于区块链的学术资源知识产权保护

云环境下数字学术信息资源建设的目的在于促进知识交流、鼓励知识创新，对知识产权保护旨在合理控制使用。对数字学术信息资源云服务中的学术交流，以及分享过程中产生的大量网络文献、问答数据、图片和特定的知识成果，需要在云环境下进行保护。其保护拟采用知识产权法律框架下的知识共享协议组合方式进行。

鉴于学术信息资源云服务的组织结构和要素特征，在知识产权保护的技术实现上，可借鉴区块链模式。区块链是一种通过去中心化的方式集体维护可靠数据库的技术方案[14]。区块链中的“区块”指信息块，内部含有特殊信息时间戳。含有时间戳的信息块彼此互联，形成信息块链条。从数据角度看，区块链是一种极难被更改的分布式数据库。“分布式”不仅体现为数

据在互联网中的分布式存储，还体现在数据的分布式记录。从技术角度看，区块链并非单一技术，而是加密技术、分布式传输等多种技术组合，一种新的数据记录、存储和表达方式。

区块链中的信息由参与系统的众多计算设备共同维护，存储其中的用户知识产权数据和数字产权数据由于极难被伪造和篡改，从而避免了中心化审核的系统性风险。区块链技术降低了实体和网络中的信任和认证成本。

针对互联网数字信息产权保护的要求，数字学术信息资源基于区块链的知识产权保护拟从三个方面着手。

（1）进行去中心化的分布式记录，提高安全性。区块链计算使用分布式计算和存储，按学术信息云服务的组织结构，不存在中心化的硬件或管理机构。这意味着任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。当系统部分节点出现问题，并不影响整个系统的数据安全，这种特性使得数字学术信息资源的知识产权保护可达到不中断的安全保障目的，适应构建低成本、高可靠性的互联网数字产权保护的需要。

（2）实现自我监管，提高知识产权保护的效能。区块链采用基于协商的规范和协议（如一套公开透明的算法），使云服务系统中的所有节点能够在信任环境下自由安全地交换数据。在运行中，“人”的信任变为机器的信任，任何人为的干预将不起作用。区块链中信息块的生成有一个工作证明机制，任何一个节点通过参与审批交易并记录，以避免系统中节点间的欺诈。该机制保障了整个云服务系统的产权保护安全性和完整性，无须审查者干预。这可以让系统中每个节点都对其他节点负责，能够通过广泛的节点监督实现去中心化的监管。

（3）实现跟踪保护，提高可操作性。每个信息块一旦经过验证并添加至区块链，就会永久地存储下来，除非能够同时控制系统中超过51%的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。系统是开放的，除交易各方的私有信息被加密外，区块链的数据对所有用户公开，任何用户都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统的信息高度透明。云服务中的数字知识产权所有者将产权信息和产权交易转让信息写入区块链，那么所有人都能通过该信息块追踪到此次知识产权的变更情况。其中，任何写入区块链的记录都是无法篡改的。

基于区块链进行数字产权保护时，可以通过多种机制组合来控制。由此可见，基于区块链的数字信息知识产权保护比现有的集中登记保护更加灵活有效。

4 结语

数字学术信息云服务中的用户安全是权益保障的基础和前提，在面向用户的学术信息资源云服务中，由于用户身份的跨界特征和云服务的交互性，按安全环节构建有效的用户身份认证普适系统十分重要。考虑到云服务链的开放结构，采用跨越多个域的联邦认证和访问控制是一种切实可行的方式。

在基于联邦认证的基础上，数字学术信息云服务的用户隐私权保护在云平台构架中进行，以保障用户登录与交互信息安全。云存储中的用户个人信息安全和服务方对用户审计的信息安全，在技术实现时拟将传统保护技术进行扩展应用，同时采用隐私增强技术进行保护标准建设。

面对数字学术信息的用户知识产权问题，在数字学术信息云服务开放环境下，根据公益性服务和商业服务在云平台中的不同体现，可以按知识产权共享协议进行用户知识产权保护的组合条件选择。按选择标识，采用区块链形式进行保护的全面实施，推进数字学术信息云服务中的用户安全，与基于安全的权益保障进程。

参考文献

[1] REKABY F,EI-AZIZ A A A, MAHMOOD M A,et al.Federated cloud computing security using forward-secure broadcast encryption HIBE[C]//Computer Engineering Conference.[S.1]: IEEE,2016.

[2] NURMI D,WOLSKI R,GRZEGORCZYK C,et al.The eucalyptus open-source cloud-computing system[C]//IEEE/ACM International Symposium on Cluster Computing and the Grid.[S.1]:IEEE,2009.

[3] 王群,李馥娟,钱焕延.云计算身份认证模型研究[J].电子技术应用,2015,41(2):135-138.

[4] 徐云云,白光伟,沈航,等.云存储中基于虚拟用户的数据完整性验证[J].计算机科学,2017,44(5):95-99.

[5] 周长春,田晓丽,张宁,等.云计算中身份认证技术研究[J].计算机科

学,2016,43(s1):339-341,369.

[6] BRODKIN J. Gartner: Seven cloud-computing security risks[EB/OL]. (2008-07-02)[2017-06-20]. http://www.infoworld.com/article/2652198/security/gartner--seven-cloud-computing-security-risks.html.

[7] 李晖,孙文海,李凤华,等.公共云存储服务数据安全及隐私保护技术综述[J].计算机研究与发展,2014,51(7):1397-1409.

[8] ATENIESE G,BURNS R,CURTMOLA R,et al.Provable data possession at untrusted stores[C]//Acm Conference on Computer & Communications Security.[S.l]:ACM,2015.

[9] CHOI K,CHO I,PARK H,et al.An empirical study on the influence factors of the mobile cloud storage service satisfaction[J].Journal of the Korean Society for Quality Management,2013,41(3):381-394.

[10] 王威,吴羽翔,金鑫,等.基于可信第三方的公有云平台的数据安全存储方案[J].信息网络安全,2014(2):68-74.

[11] 戴泳.图书馆云服务的知识产权风险及对策[J].图书馆学刊,2015(12):80-83.

[12] 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.

[13] 秦珂.云计算环境下图书馆的著作权法律风险规避[J].图书馆工作与研究,2013,1(12):10-13.

[14] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016, 42(4):481-494.

作者简介

曹鹏，男，1983年生，博士，讲师，研究方向：信息服务与用户，E-mail：36117646@qq.com。
石宇，女，1993年生，硕士研究生，研究方向：信息服务与用户。

User Security and Rights Protection in Digital Academic Information Cloud Services

CAO Peng[1], SHI Yu[2]
(1. School of Journalism and Communication, Hubei University, Wuhan 430062, China;
2. School of Information Management, Wuhan University, Wuhan 430072, China)

Abstract: The digital academic information users' security and rights protection are the basic conditions for organizing cloud services, and its security is accompanied by various links of cloud services. According to the organization structure of digital academic information cloud service, this paper conducts the research on user identity security authentication mode and cross-system implementation. Through the federal mechanism for access control analysis, the organizational structure of user privacy information protection and user intellectual property protection are explored based on link protection and identity authentication. Then the implementation of rights and interests protection are carried out according to the cloud service operation and management relations.

Keywords: Digital Information Cloud Service; User Security; Rights Protection

（收稿日期：2017-07-06）