ISSN 1002-4956
CN11-2034/T

实 验 技 术 与 管 理
Experimental Technology and Management

第35卷 第5期 2018年5月
Vol. 35 No. 5 May. 2018

DOI:10.16791/j.cnki.sjg.2018.05.038

多租户系统的轻量级实现及其在大型仪器设备共享平台中的应用

肖 健[1]，于 策[2]，崔辰州[3]，樊东卫[3]，王传军[4]，张 戈[5]

（1. 天津大学 软件学院，天津 300350；2. 天津大学 计算机科学与技术学院，天津 300350；3. 中国科学院 国家天文台，北京 100012；4. 中国科学院 云南天文台，云南 昆明 650011；5. 阿里云计算有限公司，北京 100102）

摘 要：针对大型仪器设备共享平台在用户管理、权限控制、过程管理方面的需求，借鉴软件即服务（SaaS）的架构设计了一个支持多租户的轻量级系统框架，并成功应用于中科院天文望远镜共享平台。该框架利用规则引擎实现灵活的权限定义和细粒度的数据访问控制，通过工作流引擎实现具体设备的定制扩展要求，能够快速完成新增设备的集成。该框架全部基于开源技术实现，构建过程简单且实用性强，可方便部署和推广。

关键词：大型仪器；多租户系统；开放共享；仪器设备管理

中图分类号：TP393.09；TP391 **文献标识码**：A **文章编号**：1002-4956(2018)05-0146-05

Lightweight realization of multi-tenant system and its application in large-scale instrument and equipment sharing platform

Xiao Jian[1], Yu Ce[2], Cui Chenzhou[3], Fan Dongwei[3], Wang Chuanjun[4], Zhang Ge[5]

(1. School of Software, Tianjin University, Tianjin 300350, China; 2. School of Computer Science and Technology, Tianjin University, Tianjin 300350, China; 3. National Astronomical Observatory, Chinese Academy of Sciences, Beijing 100012, China; 4. Yunnan Astronomical Observatory, Chinese Academy of Sciences, Kunming 650011 China; 5. Ali Cloud Computing Co., Ltd., Beijing 100102, China)

Abstract: In view of the needs for the user management, authority control and process management of large-scale instrument and equipment sharing platform and based on the architecture of the software-as-a-service (SaaS), a lightweight system framework which supports multi-tenants is designed and it is successfully applied to the astronomical telescope sharing platform of the Chinese Academy of Sciences. This framework realizes the flexible permission definition and fine-grained data access control by using the rule engine, achieves the customized extension requirements of specific equipment through the workflow engine, and can quickly complete the integration of new equipment. This framework is realized all based on the open source technology, the construction process is simple and practical, and it can be easily deployed and popularized.

Key words: large-scale instruments; multi-tenant system; opening and sharing; instrument and equipment management

近年来，随着国家不断加大对高等教育和科研事业的投入，各高校和科研院所也拥有了越来越多的大型仪器设备和科学装置（以下简称“大仪”）。由于大仪属于稀缺资源，前期投入成本高，因此，如何最大限度地发挥这些大仪的价值，是设备的运维部门和主管单位的重要工作之一。借助信息化技术建设仪器设备共享平台，能够有效提高仪器设备利用率，加强仪器设备的开放共享，在更高的层面优化资源配置[1-2]。很多高校的大仪管理平台已取得了很好的效果[3-4]，但也有许多具体功能有待优化，使设备的教育科研产出最大化。

大仪具有两个显著特点：(1)大仪本身的构造和操作十分复杂，需要有专业人员负责运行和维护，在某些

收稿日期：2017-11-30

基金项目：国家自然科学基金-天文联合基金项目（U1731125，U1731243）；中国科学院信息化专项项目（XXH12503-05-05）

作者简介：肖健（1978—），男，河北玉田，博士，工程师，主要研究方向为天文信息技术、高性能计算.

E-mail：xiaojian@tju.edu.cn

特殊情况下，用户可以不到现场，专业技术人员也能够按照标准流程完成实验并反馈结果；(2)大仪的平均单次作业周期较长，除了实验本身的时间外，某些实验还需更换辅助部件。目前，大部分大仪共享平台都以相对通用的线上预约功能为主，而对具体设备的使用特点考虑较少，不能很好地支持设备共享的完整工作流程，例如实验内容管理、实验数据归档、远程下载、成果统计等。因此，很难将用户、运维团队以及主管部门紧密地连接在一起，形成一个相互促进的闭环流程。

由于很多大仪是高度定制的，精细化的开放与共享管理也需要高度定制的信息平台。在互联网应用领域广泛应用的多租户技术[5]可以有效地解决这类问题。但完全按照商用标准建立的多租户平台，对于设备共享管理而言又过于复杂，成本也比较高。因此，本文结合中科院天文大科学中心对望远镜共享管理平台的实际需求，提出了一个多租户系统的轻量级设计方案。该方案采用工作流技术规范设备的预约、使用以及管理流程，利用规则引擎保证各类用户的数据安全，实现了仪器预约申请、实验准备、数据管理、效益评价、辅助决策的闭环流程。文本旨在分享该系统的设计方案、关键细节、实际使用情况以及推广建议，为大仪共享平台的建设和完善提供参考。

1　多租户技术与大仪共享平台

要针对设备的使用特点进行精细化管理，关键是设备运维团队的高度参与，这就需要共享平台作为一个软硬件基础设施，为各个大仪团队提供可定制的二级平台。从技术角度看，就是“软件即服务”(SaaS)的模式[6]，典型的例子就是互联网上各类电商平台。大仪团队可类比于店铺，为用户提供服务；使用仪器的用户可类比于消费者，订购服务。

在 SaaS 的架构中，核心的功能是对多租户的支持。本文中的租户指的是使用大仪的实验团队。各个团队可以在共享平台之上，针对设备的特点建立高度定制化的二级平台，并在其上完成共享安排、预约管理、实验数据管理、成果统计、使用情况分析等一系列工作；而主管部门也可以实现单位内大仪的统筹管理。多租户技术对各类需求的支持非常灵活，甚至可以在实体设备之上构建虚拟设备。

具体来说，每种仪器都有特定的功能。有些科学实验需要使用 1 种以上的仪器设备，如果该类仪器设备的使用组合比较常见，相关实验团队就可以联合建立一个专门的二级平台，把关联的设备都纳入进来，在特定情况下实现协同管理，提高整体的工作效率和效果。本文的成果之一——天文望远镜共享平台中就有虚拟望远镜的应用范例。

2　多租户框架的设计与实现

要实现多租户功能，需要一整套的技术规范，主要包括定制化、数据安全、水平扩展性和系统稳定性[6-7]，而对于中小规模的大仪共享平台而言，主要考虑定制化和数据安全即可。数据安全主要包括访问控制机制和数据隔离策略。鉴于与电商平台类似的定制化非常复杂，本文采用一个折中的方案，即先利用工作流技术规范设备共享管理的标准处理流程，又在每个处理阶段预留了扩展接口，使得交互界面和业务逻辑的定制化只需要少量编码即可完成。对于数据隔离和访问控制，在参考基于角色的权限控制(RBAC)[8]的标准之上，利用动态脚本解析和规则引擎技术实现了灵活的权限定义和细粒度的访问控制。

2.1　基于工作流的定制化设计

由于仪器设备的共享管理流程基本一致，系统首先利用工作流技术对整个流程进行了抽象，规定了各个主要处理步骤的通用操作，对于系统内任何设备的共享使用，都要遵守这一标准的流程。如图 1 所示，除了现场实验过程本身之外，整个流程形成了一个闭环，将用户、设备运维团队、管理部门紧密地联系在一起，方便用户按统一标准使用不同的设备，也有利于管理规范化和提供系统层面的统计分析。

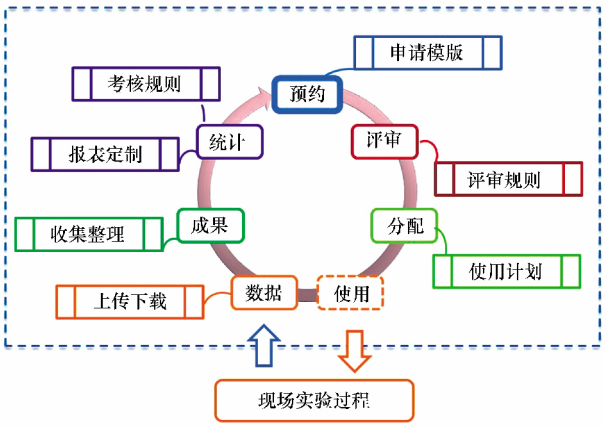

图 1　可定制的设备共享管理流程

在对整个处理流程提供了标准的处理模板之后，为解决多租户的定制化需求，在各个步骤的模板中插入扩展点。模板本身只规定了该工作节点的基本信息和处理过程，运维团队可以根据具体需要，增加设备专用属性和处理方法。对于暂时不需要的处理模板，也可以直接略过，由系统按照默认方法处理。例如：不同的设备可以定制专属的预约申请模板，在提供更多的选项给用户的同时，也为实验准备提供必要的信息；某些供不应求的特殊设备需要事

先评估使用申请的科学价值和重要性，再制定用户的排队计划，这可以通过配置评审规则和邀请专家进行在线评审来实现。

为方便科学用户和运维团队存储和利用数据，大仪共享平台还提供了实验数据的管理功能。对于某些通用类型的实验，如果没有必要重复进行，用户可以直接下载系统的归档数据，有利于节约时间和资源。

关于实验数据的使用，还需要考虑数据的知识产权。在默认情况下，只有实验和数据的描述信息（元数据）对所有用户是可见的，实验内容数据都是受保护的，数据的所有者是该实验的科学用户，其他用户可以向数据所有者发送数据使用请求，数据所有者也可以将特定数据设置为向所有用户开放。

2.2 基于规则引擎的访问控制机制

无论是二级平台的定制需求，还是用户的数据使用，都需要一套安全机制来保障。基于角色的访问控制是一套成熟的访问控制机制，在国际上有标准的 RBAC96/97 模型[8]。在 RBAC 中，权限与角色相关联，用户通过成为适当角色的成员而得到这些角色的权限。用户可以很容易地从一个角色被指派到另一个角色。虽然 RBAC 极大地简化了权限的定义，但具体实现起来并不容易。

在设计实现阶段，RBAC 模型通常被映射到经典的 7 表模式（用户表、角色表、权限表、功能表、用户角色关联表、角色权限管理表、权限功能关联表）。当用户比较多时，可能还需要对用户进行分组管理，因而增加 2 个表。在一些大型、复杂系统中，完整的 RBAC 模型可能需要大约 15 个表，这势必会大大增加编码的复杂性和实现的难度[9]。即使在 Web 系统中应用最广泛的 Spring Framework[10]，在数据级别的权限控制方面，也需要对每一条数据记录单独进行权限定义，应用起来十分不便。

本文在满足权限控制基本需求之上，基于规则引擎和动态脚本解析技术，提出更为简化、灵活的权限描述方式，权限表之间的映射关系如图 2 所示。在数据库层面一共有 5 张表（含关联表），能够满足 BRAC 模型的大部分规范。该方式是理论模型与设计实现在面对具体问题时的一个良好折中，其具体实现需要借助 Web 框架的拦截器功能和底层语言的反射机制。

拦截器可以按照预定的规则截获部分或所有的处理请求，能够在真正的业务逻辑执行前后进行一些通用性的处理，从而为应用程序提供面向切面编程（AOP）[11]的类似功能，非常适用于日志、权限等贯穿于每个处理之中的通用行为。如图 2 所示，当一个请求到来时，权限拦截器解析 URL，并利用反射机制得到处理该请求的类对象（Controller）及其方法名，然后解析并验证相关的权限规则。如果发现匹配操作且规则验证通过，则触发实际的业务代码；反之，拒绝该用户的操作请求。

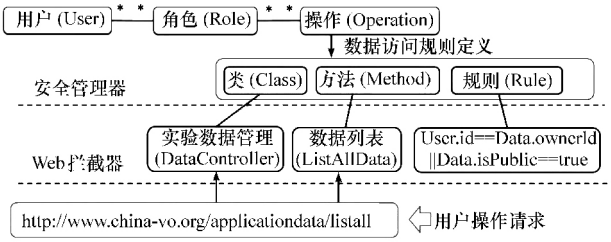

图 2 基于拦截器和规则引擎的细粒度访问控制机制

图 2 中，从面向对象编程的实现角度来说，在对象层面，用户对应 User，角色对应 Role，操作对应 Operation。在 Operation 类中，权限的描述信息包括类（class）、方法（method）和规则（rule）3 个属性。

类（对象）＋方法，标识一个具体操作，是操作级别的过滤。

规则代表数据访问的限制，即什么样的数据能够被访问或操作。按照对数据的操作类别，这里定义了 2 类规则：

（1）查询规则：读操作，对应一条或多条数据的读取；

（2）决策规则：写操作，对应数据的新增、修改和删除。

权限控制可以总结为“什么样的用户能看到哪些数据，操作哪些数据”；而此处的“规则”也可以形象地表达为“多少权限事，尽在规则中”。

图 2 展示了一个读操作的处理过程。用户要查询实验数据，首先，这个查询操作被映射成 DataController 对象的 ListAllData 方法；然后被权限拦截器拦截，解析对应的操作规则：只有该用户私有的数据以及向所有用户公开的数据才可以访问；最后，按照这个规则将过滤后的数据返回给用户。这里所有的过程都是系统框架自动完成的，这种非侵入式（no-intrusive）方法避免了传统的硬编码实现方式[11]，从而使得开发人员不必关心权限部分，只专注于业务逻辑。权限定义和管理通过图形化界面，经过简单配置即可完成，也方便系统在运行时更改权限配置。这一功能对定制化要求较高的多租户平台也十分重要。

2.3 关键功能的实现方法

多租户系统的框架采用 Java Web 技术实现，主要组件和交互方式如图 3 所示，其整体遵循典型的 MVC 模式[12]，分别在控制层、视图层、模型层以及存储层对定制化进行了特殊支持。

首先，基于 Java 的泛型（图中＜T＞）和 ORM 技

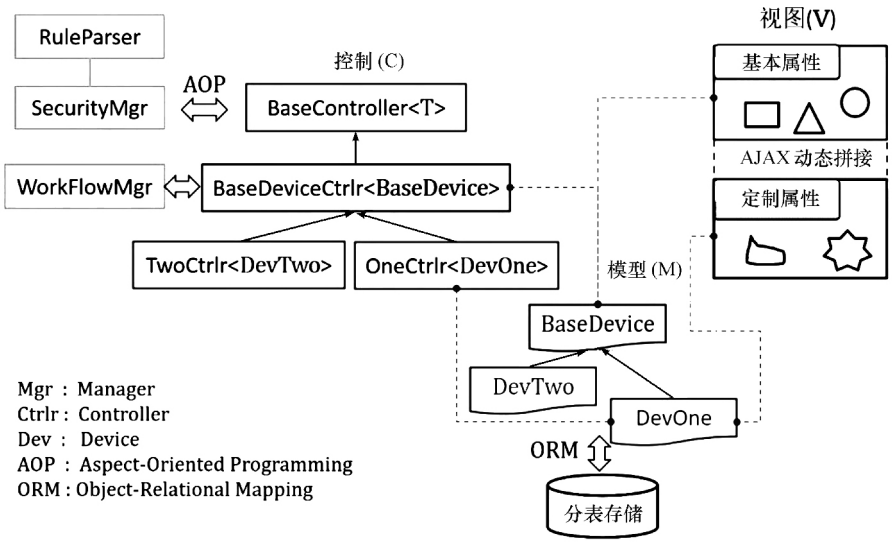

图 3　多租户框架的核心组件及组成结构

术，实现了通用的增删改查(CURD)以及报表导出等常用功能，其子类几乎不需要关心数据库相关操作，只关注业务逻辑即可。

然后，利用面向对象的继承机制，并借助 template 和 bridge 的设计模式[12]，在中间层提供全面的缺省功能，实现和扩展接口。子类只需要实现具体设备的扩展部分，对应的视图部分则利用了 AJAX 技术的异步请求功能，动态加载设备的定制信息，并与基本信息拼接成完整页面。

最后，利用泛型和继承机制，不同设备的定制信息可以自动保存在不同的数据表中，实现不同设备之间数据的隔离。

贯穿所有处理流程的权限控制，主要基于 Spring MVC 提供的拦截器和嵌入式的 Java 源代码解释器 BeanShell[13] 来实现。如图 2 所示，安全拦截器按照既定的过滤规则，在业务处理之前调用规则引擎，检查用户身份和权限。利用 BeanShell 对 Java 代码的动态解释能力，很容易实现自定义的微型规则引擎。只须完整地定义出代表操作对象的环境变量，就可以通过 Java 代码的形式来描述权限规则(见图 2 中的示例)；而 BeanShell 能够在运行时对规则进行解析并求值。如求值为真，则继续执行；否则拒绝请求。安全管理器负责加载权限信息，并提供规则引擎所需要的运行时上下文。整个权限控制组件能够以面向切面的形式装配到系统中，从而不必侵入具体的业务代码。

工作流管理器通过一系列的状态转换和控制，负责管理具体设备的预约和使用流程。同安全管理器类似，工作流管理器控制的对象也是上层的基类，具体设备对应的子类只需关注业务逻辑。特别指出的是，图 3 只是框架的设计思路和典型处理流程，而工作流的具体处理步骤也是类似的结构，不再赘述。

3　应用与推广情况

本文提出的轻量级多租户系统框架，已经成功应用于国内天文领域的基础信息化平台——天文科技领域云[14]。图 4 所示基于该多租户系统框架构建的天文望远镜开放共享平台已于 2014 年上线运行，现部署在阿里云(aliyun)的专用节点上。目前已经集成了兴隆 2.16 m 光学望远镜、丽江 2.4 m 光学望远镜、抚仙湖 1 m 红外太阳塔、新疆 26 m 射电望远镜以及大科学工程的郭守敬望远镜(LAMOST)等，贵州 500 m 球面射电望远镜(FAST)也即将接入该平台，用户数量已达到千人以上。

值得一提的是，该平台上还有 2 个虚拟望远镜：一个是国内 2 m 级的望远镜的联合体，另一个是中科院国外望远镜使用计划中相关望远镜的联合体。借助多租户平台定制化的优势，可以快速地构建虚拟设备，实现望远镜之间的协同调度

天文望远镜的整个工作流程比其他大型仪器设备更复杂，因此也有力证明了该多租户系统框架的实用性。对于新望远镜的加入，平台的开发人员只需要对应望远镜的特有需求(终端设备参数、观测计划分解等)，而其他处理流程则完全通过配置方式实现。望远镜的运维团队、用户可以在标准的工作流程下，充分发挥和使用望远镜的特有功能，上级主管部门也可以将望远镜的使用细节报告(例如观测频繁程度、终端利用率等)作为参考依据之一，制定针对性的支持政策。

除了天文望远镜开放共享平台，该框架还应用在

图 4 中科院天文望远镜开放共享平台

面向民间天文台和望远镜的科普项目(http://psp.china-vo.org)以及天津市数字媒体实验教学中心的设备共享管理。此外，中国木版年画数据库[15]以及天津市城建热线平台[16]也基于本框架构建，充分体现出该框架的适用性和灵活性。

4 结语

针对大型仪器设备开放共享精细化管理需求提出的支持多租户模式的轻量级实现方案，综合衡量了系统的复杂度、扩展性和实用性，利用开源软件、工作流和规则引擎对商用多租户系统的复杂实现过程进行了必要的简化，大大降低了系统的技术门槛，能够满足大型仪器设备共享平台的实际需求，方便推广和使用。目前，为进一步推进天文望远镜的开放共享，阿里云的技术工程师也参与了该框架的完善和升级的工作。下一步的工作重点将是进一步增强系统对定制化的支持，不再采用硬编码的扩展形式，而是通过配置实现新增设备的扩展需求，进一步降低系统运行维护的技术难度，推出更稳定的开源版本为广大社区使用。

参考文献(References)

[1] 王松梅，赵举忠，胡雪梅. “互联网+”助推大型仪器设备高效使用[J]. 实验科学与技术，2017，15(2)：152-154.

[2] 张晶晶，殷曦敏，王锡昌，等. 大型仪器设备平台建设现状与运行建议[J]. 实验室研究与探索，2016，35(1)：261-263，274.

[3] 胡炜，周洁，蒙冰. 国家重点实验室大型仪器设备平台建设的探索研究[J]. 中国教育技术装备，2013(23)：26-28.

[4] 刘宁，郭爽，徐召，等. 国家重点实验室大型仪器设备平台建设与管理[J]. 实验技术与管理，2017，34(4)：265-267.

[5] Aulbach S，Grust T，Jacobs D，et al. Multi-tenant databases for software as a service：schema-mapping techniques[C]//ACM International Conference on Management of Data. Vancouver，Canada，2008：1195-1206.

[6] 叶伟，赵进，叶军. 互联网时代的软件革命：SaaS 架构设计[M]. 北京：电子工业出版社，2009.

[7] 子柳. 淘宝技术这十年[M]. 北京：电子工业出版社，2013.

[8] Sandhu R S，Coyne E J，Feinstein H L，et al. Role-Based Access Control Models[J]. Computer，1996，29(2)：38-47.

[9] Oh S，Park S. Task-role-based access control model[J]. Information Systems，2003，28(6)：533-562.

[10] Johnson R，Hoeller J，Arendsen A，et al. Professional Java Development with the Spring Framework [M]. Birmingham，UK：Wrox Press Ltd，2005.

[11] Kiczales G，Lamping J，Mendhekar A，et al. Aspect-oriented programming[C]// European Conference on Object-Oriented Programming. Jyväskylä，Finland，1997：220-242.

[12] Gamma E，Helm R，Johnson R E，et al. Design patterns：elements of reusable object-oriented software[M]. Pearson Education India，1994.

[13] Niemeyer P. Beanshell：lightweight scripting for Java[EB/OL]. [2017-11-21]. http://www.beanshell.org.

[14] 肖健，于策，崔辰州，等. 天文科技领域云：大数据时代的天文教育和科研信息化平台[J]. 实验技术与管理，2017，34(10)：133-138.

[15] 王坤. 论中国木版年画数据库的建立与开发：兼及非物质文化遗产保护[J]. 天津大学学报(社会科学版)，2013，15(6)：567-570.

[16] 郝彬. 天津市 12319 城建热线业务系统设计与实现[D]. 天津：天津大学，2015.

(上接第 145 页)

[3] 郑耀涛. 信息化背景下中职学校核心竞争力系统构建研究[D]. 广州：广东技术师范学院，2014：34-37.

[4] 邵冬华，蒋敏. 基于智慧校园多方式认证下的高校多媒体教室设计与实践[J]. 西南师范大学学报，2016(3)：101-107.

[5] 刘贻新，陈宗术，陈浪诚，等. 新时期高校多媒体教室管理的创新工作[J]. 实验技术与管理，2015，32(2)：219-223，227.

[6] 陶祥亚，贾长云，杨成. 高校教育信息化建设的定位探析：以江苏高校淮海工学院为例[J]. 现代教育技术，2011，21(11)：62-65.

[7] 周丽，冯建平. 新媒体语境下自带设备(BYOD)在外语教学中的应用研究[J]. 外语电化教学，2016(3)：64-67.

[8] 游小荣，潘强，钟茫. 教室用电数据采集系统的上位机软件设计[J]. 物联网技术，2014(8)：45-46.

[9] 徐明，周恕义，乔虹. 协同论指导下的数字化多媒体教室建设和管理[J]. 现代教育技术，2013，23(5)：52-54.

[10] 薛胜兰. 基于智能手机移动授课平台的构建与应用[J]. 中国电化教育，2017(3)：112-116.

[11] 王永斌. 以投影机为中心的网络控制多媒体教室建设方案研究[J]. 中国教育技术装备，2016(4)：28-30.

[12] 中国教育技术协会技术标准委员会. 多媒体教学环境工程建设规范[M]. 北京：清华大学出版社，2011.