基于“云服务”的分布式系统移动应用中心建设①

岳轩宇[1,2], 陈远平[1], 杜义华[1], 李镇阳[1], 王 镇[1]

[1](中国科学院 计算机网络信息中心, 北京 100190)
[2](中国科学院大学, 北京 100049)

摘 要: 介绍了在中科院分布式科研管理系统—ARP 系统环境下, 基于“云服务”模式移动应用中心的建设方案及具体技术路线, 并针对建设过程中的关键问题, 如分布式环境下“云”服务功能数据的获取机制、数据访问的安全保障措施以及用户认证机制等方面进行了重点阐述.

关键词: 分布式系统; 移动应用; 云服务; 安全; ARP

Construction of Distributed System Mobile Application Center Based on “Cloud Service”

YUE Xuan-Yu[1,2], CHEN Yuan-Ping[1], DU Yi-Hua[1], LI Zhen-Yang[1], WANG Zhen[1]

[1](Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China)
[2](University of the Chinese Academy of Sciences, Beijing 100049, China)

Abstract: This paper mainly introduces the construction scheme of mobile application center and the specific technical route, based on “cloud services” model, under the Chinese Academy of Sciences large-scale distributed scientific research management system - ARP system environment. In addition, for the key problems in the construction process under distributed environment, such as the “cloud” services function data obtain mechanism, data access safeguards, user authentication mechanism and other aspects, it carries on the key elaboration.

Key words: distributed system; mobile application; cloud service; secure; ARP

中国科学院资源规划项目(Academia Resource Planning, 简称 ARP), 是从院所两级治理结构出发, 以科研计划与执行管理为核心设计并开发的资源配置管理平台[1]. 历经十余年的建设与应用, ARP 系统逐渐形成了十大业务系统(人力资源管理、综合财务管理、科研项目管理、科研条件管理、基本建设管理、知识产权管理、国际合作系统、院地合作管理、教育资源管理和评估评价)、两大应用平台(公共事务处理和信息资源服务), 院所两级联动的应用格局. 到目前为止, ARP 系统在中国科学院内共有 130 个上线单位, 为院所各级领导、管理人员、科研人员提供科研管理核心业务支持, 核心用户近 4000 人, 其中员工自助、网上报销、日常事务管理等子系统涉及全体员工, 直接服务总人数达 5.5 万人, 在提高管理工作效率、促进管理方式变革等方面发挥了重要作用.

ARP 系统采用的是“院-所”两级分布式部署架构, 每个上线单位(各研究所)均拥有一套独立的物理服务器环境并部署了相应的业务管理系统, 各所级业务系统通过数据交换平台与院级业务系统进行交互. ARP 系统院-所两级结构如图 1 所示.

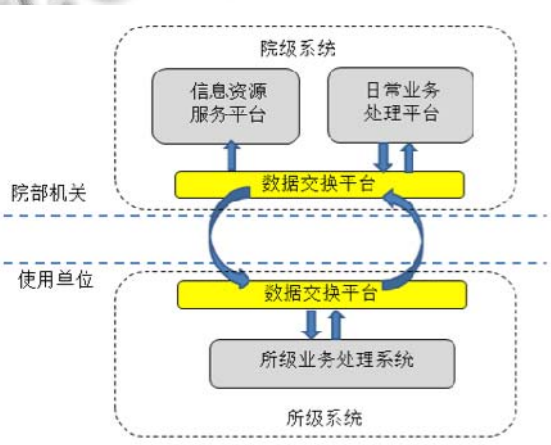

图 1 “院-所”两级系统结构图

① 基金项目:中国科学院计算机网络信息中心一三五规划重点培育方向专项(CNIC_PY_1412)
收稿时间:2016-06-06;收到修改稿时间:2016-07-19 [doi:10.15888/j.cnki.csa.005634]

此外, 在院级系统层面组建了信息资源中心(IRC), 负责完成全院各所级节点业务系统日常运行过程中产生的各类科研管理数据的汇聚任务, 并通过 ETL(抽取、转换、加载)操作构建形成中心数据仓库及数据资源池, 为院、所两级决策者、业务管理人员及科研人员提供信息资源服务[2].

1 ARP系统面临的移动应用需求

目前我们正身处移动互联网时代, 智能手机、平板电脑已普及千家万户, 各类雨后春笋般出现的移动应用正逐渐地改变人们的生活和工作方式[3,4]. ARP 系统作为中国科学院科研管理信息化的重要支持平台, 旨在利用移动终端平台提供业务审批、课题经费查询、个人工资信息查询等常见功能, 使得用户可以随时随地的进行业务处理及信息服务获取, 进一步提高工作效率及工作体验.

2012 至 2013 年, 作为运维支撑部门的 ARP 中心曾尝试开发并实现了 ARP 移动办文项目[5], 然而由于该项目的部署模式仍采用分布式结构, 需要在各 ARP 上线节点部署相应的程序包, 最终由于部署过程复杂、功能拓展不便及系统升级困难等各方面因素导致项目的应用效果并不理想.

随着办公人员对移动应用需求的不断变化和拓展, 若依然按照分布式系统结构进行系统功能应用部署、拓展、升级等操作, 则不可避免的需要在各上线单位持续地增加服务器, 在未来的运维过程中还需反复下发程序补丁, 并要求各 ARP 系统上线单位系统管理员及时部署程序升级包. 可以预见的是, 分布式架构下复杂和繁琐的工作流程势必将严重限制着 ARP 系统应用功能的发挥, 更重要的是分布式架构下不能充分利用院级信息资源中心汇聚的各 ARP 上线单位的数据资源, 从而无法为不同类别用户提供定制服务, 进而严重影响 ARP 系统整体效益的发挥. 此外, 使用分布式架构将面临着系统平台的统一管理的一系列挑战, 诸如用户行为数据的收集、系统安全的统一控制等.

近年来, 伴随着“云服务”概念的兴起以及相关开发技术的日趋成熟, 依托于“云架构”及相关技术在院级系统层面统一开发和部署“云服务”模式的 ARP 移动应用中心, 将能更合理、有效的解决前述问题, 更加充分地利用院所两级的整体资源.

2 系统建设方案

针对目前已经存在的大规模分布式结构的所级 ARP 系统, 建立起一个基于“云服务”模式并能充分兼容原有分布式系统结构的集中式移动应用中心势必充满着一系列的挑战及困难, 主要包括以下几个方面:

① 如何实现分布式系统下 ARP 用户的统一登录及权限验证问题;

② 如何解决分布式环境下业务数据的实时访问、处理问题;

③ 如何解决移动应用 VPN 访问及分布式现状下业务用户应用路由问题.

2.1 系统整体结构

针对上述提出需要解决的问题, 综合考虑设计系统整体结构如图 2 所示.

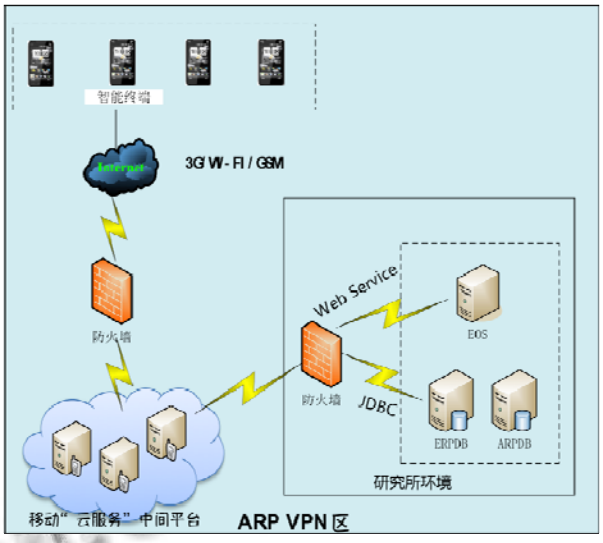

图 2　系统整体结构图

系统由移动“云服务”中间平台、所级业务管理系统、中转路由三部分组成, 针对系统所需要处理的业务而言, 构建伪代码描述如下:

```
GetTheRequestFromUser();
if (CaVerifyNoPassed(userId))
return falseInformationToUser();
else
FindTheInformationForUser();
FindWebServiceAddressFromXml();
CallOnWebServiceAndProcessRequest();
```

“云服务”模式的集中式移动应用中心处理的典型

业务请求如下:

① 处理涉及读写操作的业务数据请求(如公文批示)时, 移动“云服务”中间平台将充当认证门户, 进行统一用户认证保证系统的安全性及控制权限. 若用户没有通过验证, 返回错误提示信息, 若用户通过认证, 通过查询路由信息表判断业务请求数据源, 调用“云服务”中间平台内保存的对应所级业务处理系统 WebService 接口进行请求转发, 在所级系统内进行更进一步的业务逻辑处理;

② 处理仅涉及读操作的业务数据请求(如个人工资查询请求)时, 集中式服务平台为通过统一认证的用户从平台持有的数据库连接池中动态创建 JDBC 连接, 连到远程相应所级数据库, 并为该请求创建一个对应所级数据库系统最小权限(只读)的用户, 通过该连接直接查询远程分布式数据库的数据作为查询结果返回.

2.2 系统网络拓扑结构

VPN 专网作为 ARP 网络安全防护的重要措施之一, 通过 VPN 加密隧道将院机关局域网和各研究所局域网连接起来, 所级用户通过 VPN 加密隧道进行信息交互.

当用户访问集中式云移动应用中心时, 若各类用户均先登录院级 VPN 专网, 需在院级 VPN 服务器上为各所各用户再单独创建帐号, 这样的处理方式不方便且不现实, 且容易造成 VPN 服务器承受过大的性能压力.

为解决上述问题, ARP 移动应用中心部署于院级 VPN 区中, 系统在各上线单位 VPN 防火墙服务器上为本单位用户开通院级 VPN 登录帐号, 使用 ARP 业务系统时用户需先登录本单位 VPN 服务器, 通过 VPN 加密隧道访问院级数据资源. 系统网络拓扑结构如图 3 所示.

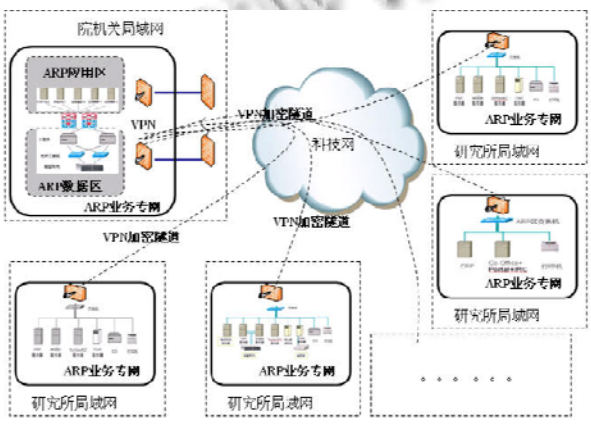

图 3 系统 VPN 网络结构图

系统通过设置严格的防火墙规则, 研究所与研究所之间划分了各自的局域网域, 仅允许对院中心特定 IP 服务器、协议和端口的访问, 从而保证数据访问的安全.

2.3 用户管理认证方案

ARP 移动应用中心的用户群体主要包括全院 ARP 系统核心用户及科研人员, 用户在本单位 ARP 业务系统中已持有帐号及密码, 并且该账户与人力资源模块中的组织结构、人员编号等信息相关联. 集中式移动应用中心不宜重新创建组织结构及用户帐号, 造成资源的重用浪费, 更合理地处理方式是在保障安全地前提下利用已有业务系统的账号密码信息实现用户权限管理的无缝衔接.

因此, 采取将各所级用户信息(如所属研究所信息等)抽取并实时汇聚到集中式移动应用中心的云端, 用户在云端登录验证时使用与所级业务系统相同的加密判断算法的方式, 可以很好地解决集中式登录问题.

用户的登陆认证流程图如图 4 所示.

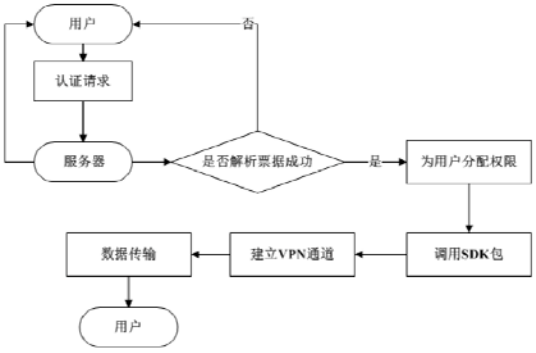

图 4 系统用户登陆认证流程图

① 用户提交认证请求给验证服务器;

② 验证服务器进行用户验证并返回给用户票据信息;

③ 客户端解析票据, 判断如果认证成功, 为用户分配相应的权限, 并调用 VPN 的 sdk 包(ios/安卓)建立一条 VPN 服务通道以便进行数据传输 ;

④ 如果客户端解析认证失败, 则提示给客户端认证失败信息.

由于客户端在提交数据请求时, 数据都是在 VPN 服务通道中传输的, 即使客户端没有使用安全的加密措施, 由于 VPN 服务通道的高安全性, 可以充分地保证数据请求的安全性.

2.4 数据与业务实时性方案

云端院 ARP 信息资源中心(以下简称 IRC)中已按月、周或日汇聚存储或加工整理有全院各类科研管理的基础数据，已能满足各级领导的常用各类查询展示、报表统计和态势分析服务.

当 ARP 移动应用中心需支持快捷办公实现与业务系统交互、面向普通人员提供最新数据服务时，信息资源中心汇聚的集中数据相对实时性不够，且无法回写到源 ARP 业务系统.

采用“集中数据+分布式数据”结合方式，开放云端海端点对点间数据访问通道，对一些涉及交互操作和实时明细数据，程序直接调用原所级 ARP 业务系统，如个人工资明细、课题经费收支明细、批阅待办公文等，可解决常规数据的集中与实时数据的分布、IRC 数据的只读与办公功能的互动问题，同时可减轻 IRC 实时数据汇聚、加载转换的压力，数据汇集过程如图 5 所示.

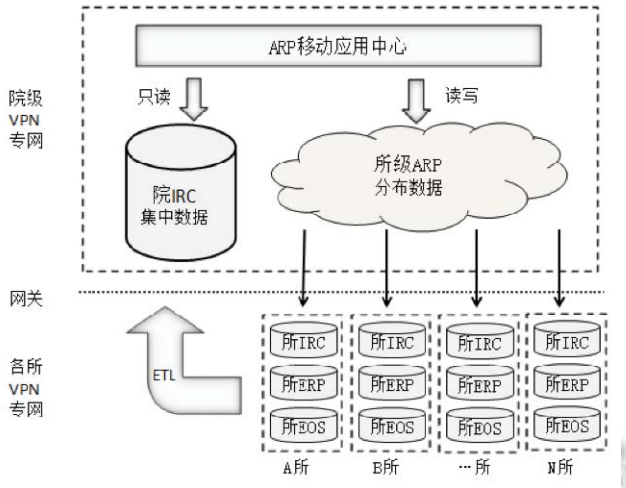

图 5　系统“集中+分布式”数据模式

3　系统技术实现

3.1 开发语言与框架

目前主流的智能移动终端操作系统包括 Android、IOS、WP7 等，根据开发实现方式的不同移动应用可进一步划分为：基于具体的手机操作系统，使用原生程序开发语言编写运行的原生应用(Native App)；基于 Web 系统的，向广大的最终用户发布一组复杂的内容和功能的网页应用(Web App)；介于原生应用(Native App)、网页应用(Web App)这两者之间的混合应用(Hybrid App)，三者的技术特性对比如下：

① 原生应用具备最高的性能，支持离线及各类的设备原生功能，对网络依赖低；

② 网页应用能利用 HTML、CSS 等技术进行界面渲染，不能支持照相机、系统通知等本机设备访问功能，且大部分依赖网络；

③ 混合应用则结合了前两者的优势，虽然损耗了部分性能，但通过 HTML、CSS 等技术的结合保证了界面的美观，同时更好的支持设备的原生功能. 此外，混合应用开发模式还具备跨平台性、低成本、移动终端页面自适应的优势.

综上所述，结合实际需求，对于移动 ARP 应用中心，系统移动端采用混合应用开发的架构. 此外，系统结合了当下流行的 HTML5 技术实现移动终端的界面友好交互、跨浏览器支持、并利用本地存储取代 cookie.

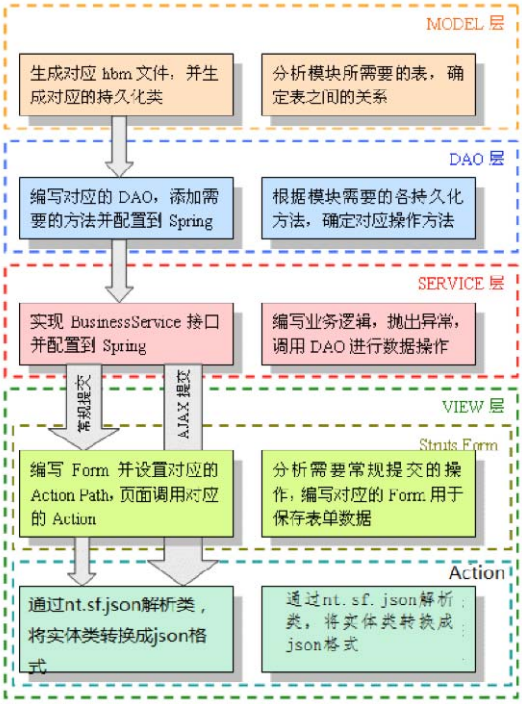

图 6　系统开发技术结构图

通过研究设计 ARP 移动应用中心的整体软件体系架构，在数据接口层中，系统采用 SSHJ 的结构，即 Structs+Spring+Hibernate+Json，数据接口层在原有的 SSH 的框架基础上，增加了 Json 的转换实现，将原有 Structs 中用于 view 展现的实体类，通过数据转换，转换成标准的 Json 数据接口. 通过上述转换力争实现对需求的快速响应，最大程度的降低系统的运维成本. 同时基于该技术路线，研究并探索移动应用缓存管理实现机制，实现在线下载、离线阅读、分类导航、模

糊检索等功能, 提升用户使用体验.

此外, 移动应用中心需要考虑移动应用的安全性, 包括数据传输的安全性、数据存储的安全性、移动用户访问的安全性等. 系统通过数据加密传输、VPN 专网、对移动智能终端的安全管理等技术手段进行控制. 通过认证权限管理实现移动应用访问入口的统一, 保证了 ARP 业务系统的权限控制与移动 ARP 应用中心用户管理的无缝衔接. 同时系统支持 ARP 系统外用户的注册申请, 最终实现用户的统一, 提高用户的使用体验的同时确保系统的安全、健壮. 系统开发技术结构图如图 6 所示.

3.2 动态数据源的生成

由于中科院下属的研究所数目庞大, 如果为每一个数据请求都生成数据源信息显然效率低下、并且造成资源大幅浪费. 为解决该问题, ARP 移动应用中心采取动态生成数据源的策略, 生成数据源的流程如图 7 所示.

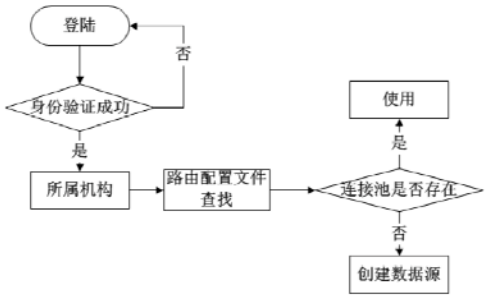

图 7 系统动态数据源的生成

① 用户首先登陆系统并进行相关的身份验证;

② 系统通过用户信息确认用户所属机构信息;

③ 在系统的路由资源配置文件中存有中科院下属各研究所的所有数据源信息, 系统会检测配置文件中是否存在当前请求对应的数据源, 如果存在, 则使用已存在数据源. 如果不存在, 系统会根据 XML 配置信息为当前请求动态生成数据源;

④ 动态生成的数据源将被添加到连接池中以便相同所级机构用户再次请求时重复使用, 同时该数据源将被设定超时时间, 如果在规定超时时间内没有该所级用户的数据请求, 系统回收该数据源资源.

3.3 系统实现展示

系统全部功能展示如图 8 所示.

① 用户可以通过系统进行日程、课题经费、差旅费、院属机构等基本办公信息的查询;

② 用户可以通过系统进行公文办公, 在移动端完成办公提高工作效率.

图 8 系统功能效果展示图

4 结语

基于“云”模式的 ARP 移动应用中心自部署应用以来运行效果良好, 目前基于该应用平台提供了包括移动公文办公、课题经费查询、护照签证、个人工资、通讯录、统计分析等主题服务, 有效的解决了分布式业务环境与集中式全局数据中心信息资源服务的矛盾, 提供了丰富的服务功能, 极大的方便了院、所级业务管理及科研人员的工作, 另一方面也很好的降低了系统运维升级的成本和复杂度.

总而言之, 通过该移动应用中心的建设, 探索了一条大型分布式信息系统下“云服务”模式应用的建设路径, 为“十三五”新一代 ARP 系统的建设提供了宝贵经验和借鉴.

参考文献

1 及俊川.十年辛勤耕耘 服务一流管理--纪念 ARP 项目实施 10 周年.科技促进发展,2012,8(10):11–17.

2 杜义华.大数据背景下中科院科研管理数据中心建设探讨.计算机系统应用,2015,24(1):79–85.

3 Cisco Visual Networking Index: Forecast and Methodology, 2014-2019 White Paper[Technical Report], Cisco, 2015.

4 中国互联网络发展状况统计报告.中国互联网信息中心, 2016.1.

5 刘彦良,孙健英.基于 Android 移动智能终端的 ARP 公文系统设计与实现.科研信息化技术与应用,2014,5(2):82–90.