基于信息技术的医院统一认证鉴权与资源共享平台的设计与实践

李文山
浙江医院　浙江　杭州　310030

摘　要：针对医院应用系统用户账号密码记忆使用不便、统一整合困难、资源数据孤立等常见应用统一管理与资源数据安全保护问题，设计并实现了一整套医院统一认证与资源共享平台。本系统采用了基于Java的Spring Boot、Spring Cloud &Alibaba的微服务框架[1]，集成了网关服务、接口服务、资源服务和授权服务，实现了简化账号识别操作、统一用户鉴权管理、资源数据互通保护和信息互联安全共享。

关键词：医院；认证鉴权；统一认证平台；资源共享平台

1 背景及现状

随着信息技术的进步与发展，越来越多的新方式、新技术和新系统被应用到医院信息化建设中，用以提高医院自身服务能力与信息化水平。而伴随医院信息化建设的稳步推进，更多的信息化医疗软件系统随之引进，这使得医院专业化服务能力随之提高，致使医院医护人员登录与使用的软件系统随之增加，这些往往会让用户为了便于密码记忆而使用相同、复杂度低、容易破解的账号密码组合，这些行为将埋下严重数据信息安全隐患，严重影响信息化系统的应用和管理。

在传统模式下，用户输入账号密码，软件系统调用后台服务读取数据库用户数据，解密并校验用户名与密码，校验通过即可完成验证并登录系统跳转主页。而医院内部例如文本、PDF、图片、影像、数据接口等数据资源的访问，通常是通过FTP协议（File Transfer Protocol）或HTTP协议（Hypertext Transfer Protocol），院内网直接访问获取数据资源，无法做到数据资源限制保护或访问控制。在该模式下，存在用户账号密码记忆使用困难、用户登录注销控制困难、多应用状态共享困难、资源数据保护困难等常见应用数据安全与资源共享保护问题，还存在信息孤立、控制不便、整合困难等常见应用统一管理与控制问题，所以，迫切需要开发针对医院应用系统的统一认证管理与资源共享保护的软件系统。

针对上述提出的问题与现状，本文提出面向医院内部种类各异、类型各异、架构各异和管理各异的应用软件系统与数据资源，整合院内人员组织架构，结合部门及人员管理特点、权限与角色管理需求、账号控制及单点登录管理需要，构建一整套符合医院实际管理需求的统一账号管理与资源共享的应用平台，保障医院应用系统管理的统一性、一致性和完整性，以实现简化操作、统一管理、数据互通和信息共享。

2 医院统一认证与资源共享平台设计与实现

2.1 系统总体设计

医院统一认证鉴权与资源共享平台主要由网关服务、接口服务、资源服务和授权服务组成。网关服务充当服务间代理，处理多个服务间数据请求，通过程序内部一系列逻辑处理，结合后台关联配置项控制，把数据内容请求转发到对应服务上；接口服务整合已完成接入的内部数据接口与外部互联网数据接口，鉴别客户端接口请求，分流认证请求与匿名请求，辅助认证服务完成登录验证操作与互联网服务接入；资源服务识别认证客户端请求，响应对应用户权限和资源信息，并将响应请求返回到网关服务上；授权服务提供账号密码验证和第三方客户端授权验证识别服务，并将结果返回到网关服务上。系统架构图如下图1，系统UML图下如图2。

2.2 系统详细设计

2.2.1 网关服务

网关服务面向内部和外部业务系统，实现路由转发、负载均衡、路径重写等功能。网关服务通过接收客户端或业务系统请求，在路由规则器中查找并匹配对应路由规则，分离请求之前（pre）或之后（post）并调用过滤器过滤筛选有效已认证请求和内部服务间请求，再结合内部负载均衡器，将多个路由请求发送至对应逻辑执行服务单位，最后响应逻辑执行服务的执行结果。具体要实现如下功能：

（1）服务认证过滤，保证业务服务稳定安全。

（2）路由转发代理，保证服务间互联互通。

（3）服务负载均衡，保证服务稳定高效运行。

（4）服务路径重写，保证服务场景多样支持。

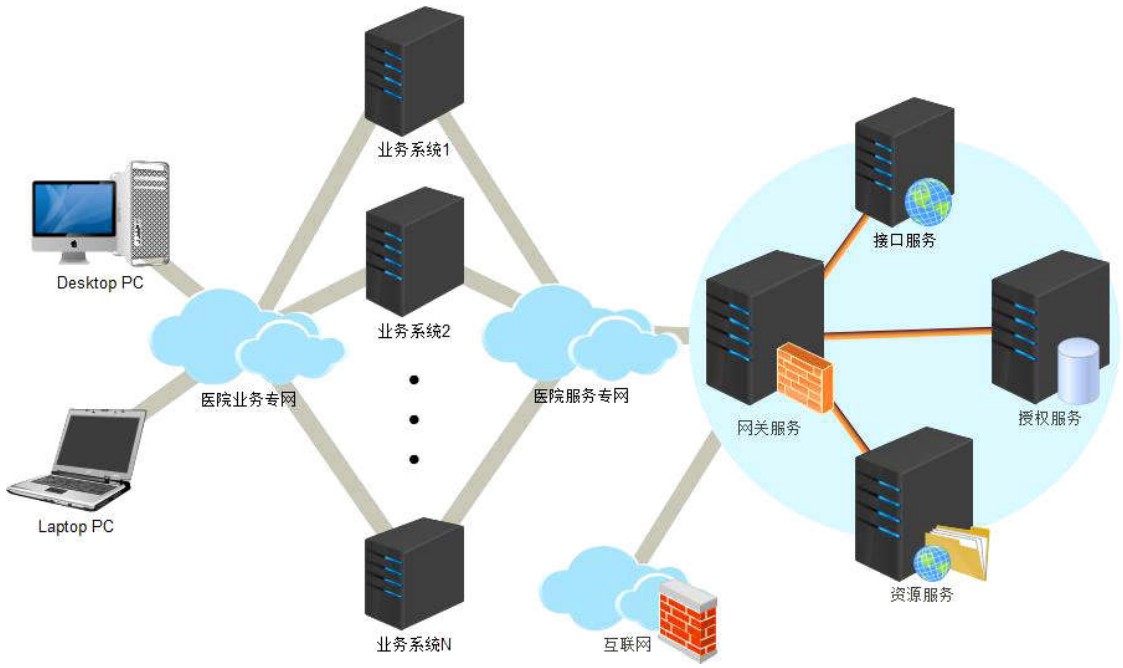

图1

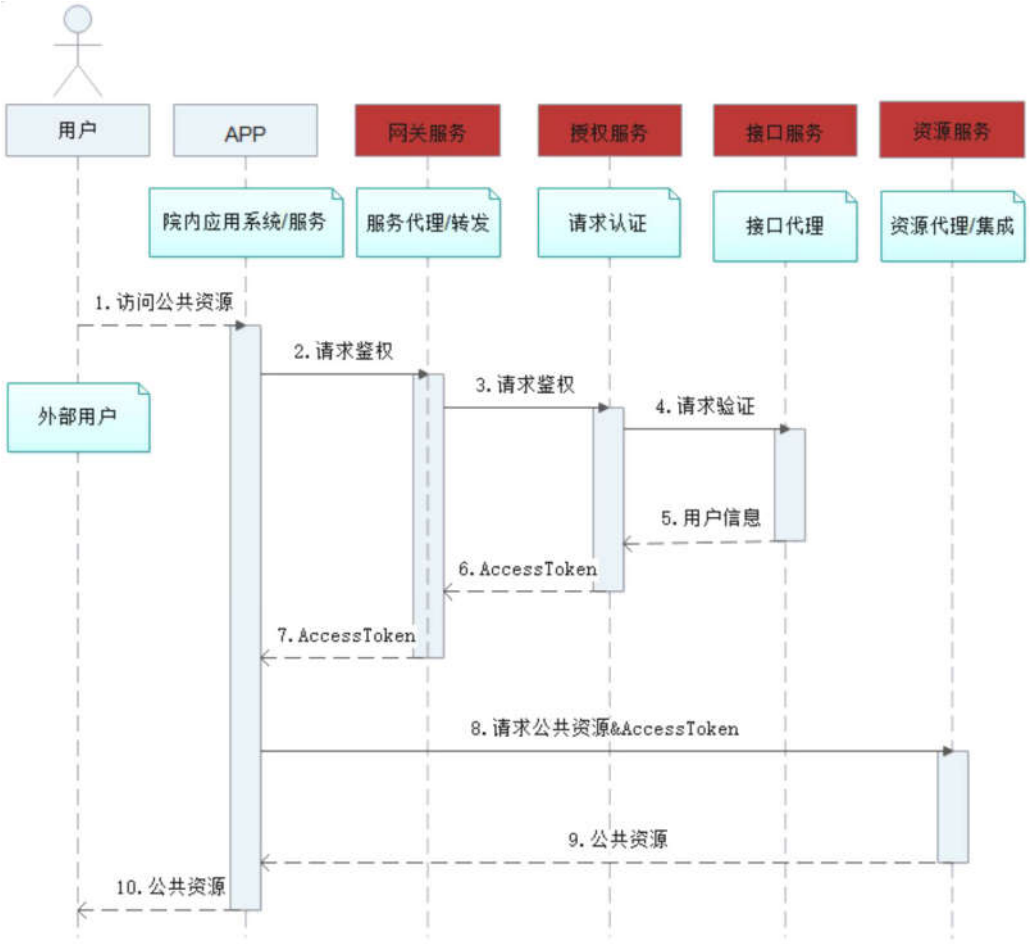

图2

2.2.2 接口服务

接口服务面向医院内部数据接口与外部互联网接口，提供应用系统服务内高效安全的数据接口访问与响应服务。接口服务将整合目前市场主流第三方用户认证识别登录接口，包括微信端扫码识别登录接口、钉钉扫码认证登录接口、短信动态码登录、北京CA“医网信”扫码认证登录接口等互联网接入方式与常规接入方式，通过该接口接入，可高效安全响应客户端或服务器验证结果，同时，还可以将该结果转发至平台认证服务上。具体实现如下功能：

（1）内部数据接口与外部互联网接口互联，提供安全可靠内部数据接入与外部互联网访问。

（2）支持接入主流第三方账号验证接口代理，提供多样互联网客户端验证访问，支持包括微信、钉钉、北京CA“医网信”等主流客户端扫码验证接口方式接入。

2.2.3 资源服务

资源服务整合医院内部数据资源，提供院内各类文本、图片、影像、Webservice接口、API（Application Programming Interface）接口等资源数据与数据接口认证访问，还可以提供多源异构数据集成访问。资源服务整合JDBC（Java DataBase Connectivity）组件，通过代理驱动（Driver），提供基于过滤器链（Filter Chain）模式的插件数据库连接访问，实现异构多源数据集成访问。客户端或者应用服务服务端可通过平台认证服务获取访问令牌（Access Token），而后，仅需在每个请求中携带该令牌，就可以在指定时限内访问账号角色权限内授权资源[2]。具体现实如下功能：

（1）提供院内各类文本、图片、影像、Webservice接口、API接口等数据资源的认证代理和安全保护。

（2）整合JDBC组件，提供多源异构数据连接访问代理和安全防护。

2.2.4 授权服务

授权服务整合用户账号密码、用户角色权限关系、用户组织机构归属等用户基础信息数据，提供基于平台内账号密码验证、已完成外部接入接口服务的第三方互联网用户信息验证识别、用户基本信息维护管理、用户角色信息管理、组织机构信息管理等基础识别维护功能，同时，对成功完成验证的客户端请求响应访问令牌、用户角色权限、用户基本信息和令牌过期时间。具体实现功能如下：

（1）提供用户基本信息、用户角色信息、用户组织信息等基本维护与管理。

（2）提供基于单点登录的用户登录验证和认证鉴权，同时，应能够实现访问令牌过期。

3 系统实现

医院统一认证鉴权与资源共享服务将采用B/S架构，前后端分离的设计模式，前端采用基于国产Element UI组件库的Vue.js前端响应式框架，后端采用基于Java的Spring Boot、Spring Cloud &Alibaba的后端微服务框架，同时，使用WEB应用方面，目前市场上最流行的RDBMS（Relational Database Management System）的MySQL作为系统的核心数据库系统，Redis（Remote Dictionary Server）作为系统的高性能缓存数据库，各服务模块化独立部署运行。整套软件系统分为网关服务、接口服务、资源服务和授权服务等4个服务，其中，网关服务负责服务间负载均衡、路由转发、路由重写等服务代理转发服务；接口服务集成接入了医院内部业务系统接口和外部互联网接口，实现接口服务集成接入互联；资源服务集成医院内各类数据资源，让授权客户端或应用系统能直接访问到这部分数据；认证服务通过接收客户端认证请求，联通平台接口服务验证用户认证请求，校验用户账号密码，响应访问令牌、用户信息、权限信息和密钥过期实际。

3.1 网关服务现实

在平台整体微服务架构中，网关服务是非常重要的组成部分，它负责路由转发、负载均衡、路径重写等重要功能。Spring Cloud Gateway是Spring Cloud官方推出的一个基于Spring 5、Spring Boot 2和Project Reactor的API网关实现。本文将采用Spring Cloud Gateway技术框架作为平台的网关服务，实现对路由指定断言（Predicate）和过滤器（Filter），有效筛选分离认证请求与内部服务请求，并将指定路由请求发送对应逻辑执行服务中，最后将逻辑执行服务的执行结果响应给请求方。

3.2 接口服务实现

接口服务是平台与互联网接入交互的入口，提供平台内部与第三方接入验证的重要服务单元。接口服务通过Webservice、WebFlux、RESTful等技术方式集成接入了包括微信公众号扫码识别登录接口、钉钉扫码认证登录接口、北京CA“医网信”APP扫码验证接口、短信动态验证码验证等市面主流身份识别验证接入方式，通过接收以上第三方接口内部或者外部验证信息，并在成功识别用户身份结果信息后，将该结果转发到平台对应的认证服务上。

3.3 资源服务实现

资源服务是平台集成与整合各类数据资源的重要服务单元，提供平台内部数据资源代理与访问。接口服务

通过接口代理实现各类文本、图片、影像、Webservice接口、RESTful接口等资源与数据接口的认证访问，同时，通过集成性能强大的数据连接池Druid，它结合了C3P0、DBCP、Proxool等开放源代码的数据库连接池的优点，可快速搭建并构成满足医院需求的多源异构数据访问环境，提供快速、高效、稳定的数据驱动代理与数据集成访问。客户端用户可便捷的通过平台访问令牌，访问到指定时间内、指定权限内和指定资源内的授权资源。

3.4 授权服务实现

授权服务是平台整合用户、角色、权限、组织机构等对象与关系，管理维护各类信息的基础服务单元，为平台提供基础信息管理、第三方互联网客户端接入接口验证、客户端账号密码验证与角色权限识别等授权验证与识别功能。通过接收客户端或者应用服务验证账号密码的认证请求，通过平台内接口服务识别验证，对验证通过的客户端请求生成访问令牌，保存访问令牌至高速缓存数据库（Redis），同时，识别重复授权认证请求，刷新高速缓存数据库的数据，最后，响应访问令牌、用户角色权限、用户基本信息和令牌过期时间。

结束语

本文介绍并实现了一套医院统一认证鉴权与资源共享平台。通过本平台的应用与推广，院内每位用户可便捷的通过统一的账号密码或者互联网应用客户端完成登录验证，还可以通过例如微信、钉钉、北京CA“医网信”APP、短信等互联网应用客户端完成登录验证，同时，还实现了院内数据资源的认证访问和安全共享。在本平台的应用推广下，极大的降低用户登录复杂度，极大的简化用户登录操作，极大保障数据资源认证访问和安全共享。同时，我们也遇到了不少关于系统并发不够、厂商集成困难等问题，为此，我们将积极探索，不断改进。

参考文献

[1]庄璐,路学刚.微服务架构中认证与鉴权的探讨[J].金融科技时代,2018,000(10):40-42

[2]张小梅,何菊,佘侃侃,戴彩艳.Django框架下的用户鉴权机制分析与研究[J].无线互联科技,2023,(18):146-148