

铁路企业统一身份认证平台的设计与实现

梁建辉 李世春 何靖刚 蒋松年 蒲 伟

(中国铁路兰州局集团有限公司信息技术所 兰州 730000)

摘 要 针对铁路企业工作人员使用多个应用系统需要同时记忆多套用户账号信息的现状,文中基于铁路统一用户管理系统的用户数据,设计了一种铁路应用系统用户的统一身份认证系统。该系统采用单点登录、Token、Cookie、Session 共享等技术,实现了用户信息与应用系统的分离、统一用户管理、统一认证、一处登录、处处共享等功能,从根本上解决了不同应用系统重复维护用户信息的问题,使用户能够更便捷地访问不同的应用系统,并保证了不同应用系统间用户信息的一致性、安全性和共享性。

关键词: 单点登录;统一身份认证;统一用户管理;认证平台;用户信息共享

中图法分类号 TP311.5;U29-39

Research on Unified Identity Authentication and Single Sign on Integration

LIANG Jianhui, LI Shichun, HE Jinggang, JIANG Songnian and PU Wei

(Information Technology Institute of China Railway Lanzhou Bureau Group Co., Ltd., Lanzhou 730000, China)

Abstract In view of the current situation that railway enterprise staff need to memorize multiple sets of user account information when using multiple application systems, this paper designs a unified identity authentication system for railway application system users based on the user data of the railway unified user management system. The system uses technologies such as single sign-on, Token, Cookie, Session sharing, etc. to realize the functions of user information and application system separation, unified user management, unified authentication, one login, and sharing everywhere, fundamentally solving the problem of repeated maintenance of user information in different application systems, enabling users to access different application systems more conveniently, and ensuring the consistency of user information between different application systems security and sharing.

Keywords Single sign on, Unified identity authentication, Unified user management, Certification platform, User information sharing

0 引言

随着信息化技术的飞速发展,铁路企业的信息化也逐步深入发展,铁路企业管理和业务运作中存在员工岗位优化、部门组织调整、业务服务升级等需求。为提高铁路企业管理和业务的运作效率,计算机在铁路企业日常工作的重要性日益凸显,相比于传统手工作业,信息化技术极大地提升了工作效率。今后将会有更多的信息化应用系统被研发上线,并应用于铁路企业的相关工作。

信息化应用系统的增加,使得铁路企业研发人员的自主研发工作剧增。由于各系统间身份认证相互独立,研发时间、成本等存在差异,因此对信息管理人员及用户都造成了身份信息管理的挑战。对于管理人员,其需依靠传统的手动操作的方式进行人员账号信息、重置密码、角色修改等复杂但不可或缺的用户信息管理工作。对于用户而言,如果其使用多个信息系统,则需牢记多套用户账号信息和密码。在铁路企业中,用户使用多个信息系统,需频繁切换信

息系统进行登录,这给铁路职工的日常工作带来了诸多不便。尤其是随着信息系统的增加,职工记忆系统账号和密码的难度也会增大^[1-2],安全性则会相应降低。

针对上述问题,研发一个只需一套用户账号和密码就能访问不同应用系统的平台非常有必要。使用统一身份认证系统^[3-4],利用单点登录^[5]、共享会话等技术,可以实现铁路企业职工用一套账号和密码进行身份认证的目的,认证通过后,职工就可以访问多个被授权的应用系统,实现应用系统单点登录。通过该系统,可以解决铁路职工忘记密码、频繁切换应用系统的问题,提高使用不同应用系统的便捷性,降低用户记忆账号和密码的难度,提升用户的体验质量,减少因忘记密码而无法登录系统的问题。

1 铁路企业统一身份认证平台系统设计

1.1 总体架构

统一身份认证系统采用 B/S 模式架构,用户界面通过浏览器展示,系统提供统一的界面,方便用户操作。系统的

收稿时间:2023-01-13

作者简介:梁建辉(1973—),本科,高级工程师,研究方向为计算机系统。

部署、修改、维护等功能全部在服务器端。系统架构划分为数据层、服务层、网络层、应用层,如图 1 所示。

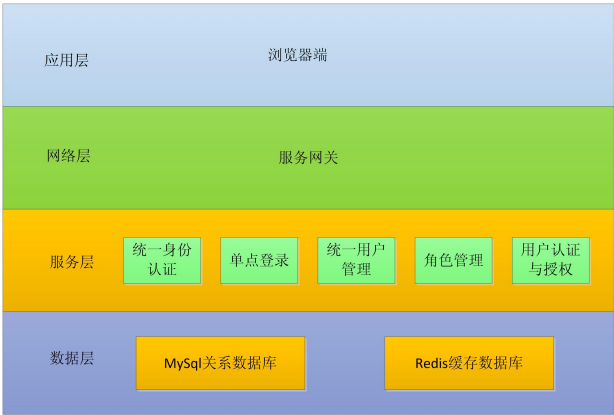


图 1 系统总体架构

(1)数据层

使用 Mysql 数据库和 Redis 内存,高速缓存统一身份认证用户账号、权限等数据,在保证存储量的同时提供高效的服务。

(2)服务层

运用微服务技术,实现统一用户管理、用户认证和授权、角色管理、应用资源的访问控制、应用系统统一身份认证及单点登录等服务。

(3)网络层

网络层利用网关服务提供统一的入口,有效解决了大量用户高并发访问时,系统服务器压力过大的问题。

(4)应用层

应用层提供用户操作的人机交互界面,用户通过浏览器登录系统,同时界面展示出用户已授权的应用,点击应用系统即可跳转至相应的应用。

系统开发基于前后端分离的方式,通过浏览器端通过 API 调用后台服务器进行服务。前端使用 Vue 框架,基于 Element UI 组件库构建页面,并使用 Js 语言动态获取 Token 值,同时使用 HTML 和 CSS 语言修饰及美化页面。后端开发采用 Java 语言,主要基于 Spring Boot, Spring Security, Mybatis 等技术,实现系统微服务的体验,基于微服务的系统每个功能相互独立,方便扩展。

2 铁路企业统一身份认证平台系统的功能

依据系统逻辑架构分析设计,统一身份认证系统为用户提供访问相应授权应用的入口,实现各应用系统之间的互通互联。统一身份认证系统功能主要包括统一用户管理模块、用户角色和权限管理模块、单点登录模块及统一身份认证管理模块。

2.1 用户管理模块

用户管理模块对用户账号信息进行维护,其主要功能包括新增、修改、删除及用户账号状态管理;用户账号状态包括正常与停用;用户账号的基本信息包括用户 ID、办公账号、用户昵称、用户名称、性别、手机号、单位等。该模块会

对用户密码进行加密处理,当用户忘记密码时,只能对密码进行重置。考虑到账号安全问题,只允许管理员对用户账号进行修改,只支持用户维护个人手机号、办公帐号和修改密码,不支持用户自己修改其他信息。

用户信息可单独管理,也可依据部门进行批量管理。基于用户与部门的一对一模式,通过对部门的查询即可获取该部门下的用户,查看用户所处岗位。

2.2 用户角色和权限管理模块

用户角色和权限管理功能可以对用户角色信息进行维护。用户角色包括超级管理员、管理员、单位管理员及普通用户等。超级管理员可以对角色进行新增、修改、删除等操作。用户角色和权限管理模块可以对各角色的权限进行修改,被赋予权限的角色,可以对角色进行分配和修改等操作。

2.3 单点登录模块

单点登录模块的主要功能是将其他应用系统集成到统一身份认证平台上。在统一身份认证平台点击集成的应用系统,登录界面在跳转之前,会验证 Token 是否有效,若有效,则直接跳转到应用系统,否则将登录保存 Token。对于已集成单点登录功能的应用系统,在访问应用系统时,应用系统会自动查找由其他应用系统共享的登录信息。若查到,则会尝试自动登录应用系统;若未查到,则将显示登录页面,输入用户信息并手动登录应用系统,这一过程也会共享登录信息。

2.4 统一身份认证管理模块

对于和统一身份认证系统结合的应用系统,访问时可以通过标识鉴别用户身份,判断该用户是否具有访问目标应用系统的权限^[6-8]。用户在访问系统时,其会自动在浏览器 Cookie 中查找是否存在已登录的用户信息,若查到,则会尝试自动登录;否则会显示登录页面,输入用户信息并手动登录应用系统。统一身份认证流程如图 2 所示。

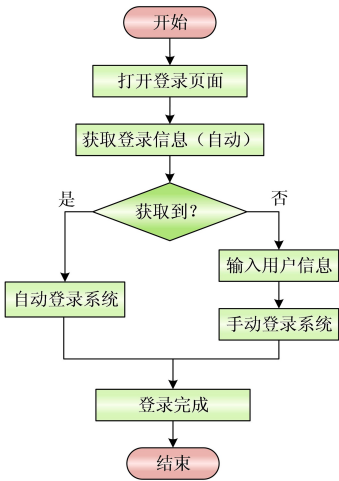


图 2 统一认证方式登录流程示意图

2.5 应用管理

应用管理模块可以实现管理员对应用的新增、修改、

删除等操作。应用管理模块中新增的应用,可在统一身份认证平台的门户页面进行展示,同时对应用进行权限管理并实现单点登录。

3 关键技术

3.1 单点登录技术

系统采用单点登录技术作为访问的认证机制。用户通过统一身份认证系统进行一次认证,认证通过后即可访问被授权的应用,不需要在每次访问时都进行身份认证。将单点登录技术运用到统一身份认证系统中,可以极大地提升用户访问应用系统时的效率。单点登录技术可以将其他应用系统集成到统一身份认证系统中,通过统一身份认证系统点击集成的应用,登录界面会跳转并验证 Token 是否有效,如果有效,则会直接跳转应用系统,否则将会登录保存 Token。用户只需要身份认证成功一次,就可以访问多个被授权的应用系统,减少登录应用系统时的认证次数,降低用户账号、密码泄露或遗忘的风险。

3.2 统一身份认证

用户初次访问统一身份认证系统时,会依据用户名和口令进行验证,如验证成功,则会跳转到统一身份认证系统主页,若验证失败,则会进行相应的提示,并返回至登录界面。

用户登录成功后,需要存储获取到的 Token 值,通过系统的后端把该 Key 值作为参数,并调用第二个接口进行 Token 验证,如果验证成功,则能通过本系统的认证流程。认证实现过程如图 3 所示。

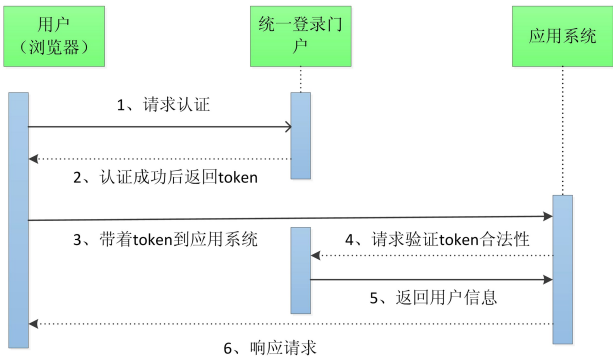


图 3 统一身份认证实现示意图

用户注销应用系统时,点击退出登录按钮就会清空 Session 和 Cookie 值。如果用户直接关闭浏览器,则只会清空 Session 值,不会清空 Cookie 值,如果用户勾选了记住选项,则下次打开网页,即可直接登录。

4 系统应用

目前,铁路企业统一身份认证平台的研发已经完成,在统一身份认证平台中,已集成 OA 系统、组织人事工作平台等应用系统。职工通过统一身份认证平台,可以直观、快速地访问平台集成的其他应用系统,减少工作中频繁切换应用系统及登录多个应用系统的操作,免去日常工作中记忆多个账号和密码的烦恼,提升工作的效率和安全性。

5 结语

统一身份认证系统采用 B/S 应用模式,以统一用户管理系统为基础,对现有业务应用系统的用户管理、组织管理、权限管理模块等进行整合,实现了集团公司职工一人一账号的目标。统一身份认证系统完成了对现有应用系统的统一管理、统一认证、统一授权和统一审计,可提供统一身份认证、登录入口等服务。单点登录功能的集成可以充分利用已有的登录信息实现应用系统的自动登录,并共享登录信息以供其他应用系统使用。

该系统建成后,中国铁路兰州局集团有限公司的全部职工,实现了一人只要一套账号,就可以访问被授权的全部应用系统,且只要第一个应用系统登录一次,其他应用系统就可以实现自动登录,免去了记忆多套用户账号的烦恼和每个应用系统都要分别登录的重复操作。下一步,铁路企业将对系统在测试和使用过程中出现的问题进行优化和完善,不断提升系统的适用性、安全性和可靠性。

参考文献

[1] 郑子秋,张卫东,刘宁,等.信息安全技术在企 ER 系统中的应用[J].科技创新与应用,2019(18):174-176.
[2] 李德兵,徐铁山,傅成兵.单点登录技术研究与应用[J].电子技术,2008(9):52-54.
[3] 李庆林.基于 WEB 的单点登录和权限管理技术研究与实现[D].北京:北京邮电大学,2017.
[4] 邱素华.基于身份认证技术的统一认证系统研究与实现[J].中国信息化,2021(12):59-60.
[5] 苏星晔,徐方南.统一身份认证技术研究[J].中国新通信,2015,17(2):58.
[6] 裴艳华,王焕民.铁路企业单点登录平台的研究与实现[J].铁路计算机应用,2014,23(4):49.
[7] 柳丽娜.浅谈 Session 机制与 Cookie 机制[J].电脑编程技巧与维护,2008(16):28-29.
[8] 郭晓宇.统一认证授权技术浅析[J].网络安全和信息化,2022(1):24-26.