

运输系统设计报告 v2.0

目录

1 引言	1
1.1 编写目的	1
1.2 项目背景	1
1.3 项目概述	2
1.4 参考资料	2
2 设计概述	3
2.1 需求概述	3
2.2 条件与限制	3
3 系统详细需求分析	5
3.1 详细功能需求分析	5
3.2 详细性能需求分析	6
3.3 详细资源需求分析	7
4 系统界面设计	9
5 Restful 设计	11
5.1 POST 用户登录	11
5.2 POST 用户注册	11
5.3 GET 获得公司名下所有车辆和司机	11
5.4 POST 新增一位司机	12
5.5 POST 新增一辆车	12
5.6 POST 承运商接单创建订单	12
5.7 POST 更新订单状态和所在地址	13
5.8 POST 更新订单状态为已签收	13
5.9 POST 商家新建商品	13
6 数据库系统设计	15
6.1 设计要求	15
6.2 信息模型设计	15
6.3 数据库设计	15
7 系统设计	18
7.1 关键技术	18
7.2 Spring Boot 框架开发	20
7.3 安全认证	21
8 总结	24

1 引言

本部分介绍了本份智能公路运输调度管理系统设计报告的编写目的和技术栈和框架。该系统的开发目标在于实现一个高效、智能、可靠的运输调度管理系统，提供给货主、货代和承运商等相关方便利的服务。同时，本份设计报告详细说明了系统的各个模块、各个组成部分的设计和实现细节，以确保系统能够达到其预期的功能和性能要求。系统的开发基于 **Spring MVC** 技术栈和框架，提供了灵活的 **MVC** 架构支持。

1.1 编写目的

本份软件系统详细设计报告是为了实现智能公路运输调度管理系统的开发目标。本系统的开发目标在于实现一个高效、智能、可靠的运输调度管理系统，提供给货主、货代和承运商等相关方便利的服务。通过本份详细设计报告，详细说明了系统的各个模块、各个组成部分的设计和实现细节，以确保系统能够达到其预期的功能和性能要求。

同时，本系统的开发基于以下技术栈和框架：

- **Spring MVC**：用于实现 Web 应用程序的开发框架，提供了灵活的 **MVC** 架构支持。
- **MyBatis**：用于实现数据访问层的框架，提供了便捷的数据库操作和查询功能。
- **Thymeleaf**：用于实现 Web 页面的模板引擎，支持动态数据绑定和页面渲染。
- **Spring Boot**：用于快速构建基于 **Spring** 的应用程序的框架。
- **Spring Cloud**：用于构建分布式系统的微服务框架，提供了服务发现、断路器、负载均衡、配置管理、API 网关等功能。

此外，本系统也重视身份验证和授权的必要性，以确保只有经过授权的用户可以访问系统的功能和数据。我们将采用 **Spring Security** 来实现身份验证和授权机制，以确保系统的安全性和可靠性。

测试也是开发过程中的重要环节。为了确保系统的质量和稳定性，我们将进行单元测试和集成测试，其中单元测试用于测试存储库层面的功能，而集成测试将验证控制器层的功能和系统整体的交互。

1.2 项目背景

当前，公路运输行业是我国交通运输领域的重要组成部分，具有广阔的市场前景和发展空间。然而，由于公路运输行业存在着信息不对称、运力利用率低、服务质量难以保障等问题，导致了运输行业的低效率和服务质量不稳定的局面。

因此，开发一种智能公路运输调度管理方法成为了当前行业的需求之一。本软件系统旨在解决公路运输行业中存在的问题，提高运输效率和服务质量，为用户提供更好的使用体验和服务。

本系统将利用现有的承运商运力资源信息和车联网运力资源信息，加入运单调度管理系统中的运力池匹配管理系统中，实现运单管理匹配和分配调度运单给承运商系统执行。同时，智能监控中心将通过接口连接承运商系统和车联网系统，对运单进行在途跟踪、服务质量管理及预警与事件管理，以确保运输过程的安全和可靠。通过本软件系统，运输行业可以实现智能化调度和管理，提高行业的效率和服务质量，为行业的发展注入新的动力。

1.3 项目概述

本系统采用了 Spring Boot 框架进行开发，使用 MySQL 数据库进行数据存储和管理。系统的前后端分离，后端采用 Restful API 设计和实施运输和运输服务，并使用 Spring Security 和 JWT 进行 API 认证和授权，以确保系统的安全性和可靠性。前端 Thymeleaf 进行页面渲染和交互。通过连续单元测试、应用 OpenAPI 文档和速率限制等措施，系统的功能和性能得到了进一步的改进。整体而言，新系统的设计和实现使得运输和运输管理变得更加高效和便捷。

1.4 参考资料

智能公路运输调度管理方法说明书

2 设计概述

本部分详细介绍了智能公路运输调度管理系统的设计和实现细节。

2.1 需求概述

主要业务需求：

- 实现货主或货代对货物进行发货下运输订单，根据需要预先选择运输产品和运输要求。
- 对运输产品、运输要求、货物运输运单和承运商运力资源信息进行运单管理匹配，分配调度运单给承运商系统进行运力执行。
- 对运单进行在途跟踪、服务质量管理和预警与事件管理，保障运输服务质量。

输入和输出：

- 输入：货物运输运单、运输产品和运输要求、承运商运力资源信息、车联网运力资源信息等。
- 输出：运单管理匹配状态、在途跟踪、服务质量管理和预警与事件管理状态。

主要功能：

- 发货系统：支持货主或货代对货物进行发货下运输订单，并预先选择运输产品和运输要求，生成统一标准的货物运输运单。
- 运单调度管理系统：管理和匹配承运商运力资源信息、车联网运力资源信息、运输产品信息和货物运输运单信息，分配调度运单给承运商系统进行运力执行。
- 智能监控中心：对运单进行在途跟踪、服务质量管理和预警与事件管理。

性能要求：

- 系统需要支持大规模的运单管理和监控服务，能够处理高并发的业务请求。
- 系统需要实现快速响应和高效处理，保证服务的实时性和可靠性。
- 系统需要保证数据的准确性和完整性，避免数据丢失或错误。
- 系统需要具备一定的安全性和稳定性，避免系统被攻击或崩溃。

综上所述，该系统的性能要求主要集中在系统的响应速度、处理能力、数据准确性和系统稳定性等方面。需要具备高效、稳定、安全的性能特点，以满足用户的实际业务需求。

2.2 条件与限制

该智能公路运输调度管理方法受到以下内部和外部条件的约束和限制：

1.业务条件与限制：

(1)承运商系统和车联网系统的接口标准需与运单调度管理系统和智能监控中心进行协商，以实现信息互通和交互。

(2)发货系统需要支持运输产品和运输要求的预先选择，以生成统一标准的货物运输运单。

(3)运单调度管理系统需要实现对承运商运力资源信息、车联网运力资源信息、运输产品信息和货物运输运单信息的管理和匹配分配，以实现运单的调度管理。

(4)智能监控中心需要实现对运单的在途跟踪、服务质量管理和预警与事件管理，以保障运输服务质量。

2.技术条件与限制：

(1)运单调度管理系统和智能监控中心需要具备一定的计算能力和存储能力，以支持大规模的运单管理和监控服务。

(2)所有系统之间需要建立稳定的网络连接，以支持数据传输和信息交互。

(3)所有系统需要保证信息安全和数据隐私，需要具备一定的安全管理和数据隐私保护能力。

(4)车联网设备需要覆盖运输车辆所在的区域，以实现对运输车辆和运输过程的监控和管理。

3.进度与管理方面的限制：

(1)该系统需要经过设计、开发、测试和部署等多个阶段，需要有一定的开发和运维人员支持。

(2)系统的实现需要根据实际业务需求进行调整和优化，需要一定的业务分析和需求管理能力。

(3)系统的部署和运行需要进行维护和监控，需要具备一定的系统管理和运维能力。

(4)系统需要满足政府和行业的相关法规和标准要求，需要具备相关的合规管理和认证。

综上所述，该智能公路运输调度管理方法受到多方面的约束和限制，需要根据实际情况进行评估和调整。同时需要具备一定的业务和技术能力，以保证系统的正常运行和维护。

3 系统详细需求分析

3.1 详细功能需求分析

1. 发货系统功能需求：

- 用户认证功能：使用 Spring Security 进行用户身份验证和授权，包括注册和登录功能。
- 发货功能：用户可以输入货物基本信息、运输要求、承运商信息和车辆信息等，生成货物运输运单。
- 查看订单功能：用户可以查询和查看已经下单的货物运输运单信息。
- 取消订单功能：用户可以对未被承运商接单的订单进行取消操作。

2. 运单调度管理系统功能需求：

- 运单匹配功能：根据货物基本信息、运输要求、承运商运力资源信息和车联网运力资源信息，对运单进行匹配。
- 运单调度功能：根据运单匹配结果，将运单分配给合适的承运商进行运力执行，并进行运单调度管理。
- 运单状态监控功能：对承运商运力执行情况进行监控，及时反馈运单状态。

3. 智能监控中心功能需求：

- 在途跟踪功能：通过车联网系统实现对运输车辆的实时定位，实现对运单的在途跟踪。
- 服务质量管理功能：对承运商的服务质量进行监管和管理，及时发现和处理服务质量问题。
- 预警与事件管理功能：通过对运单数据进行处理，实现预警和事件管理。

4. 系统管理功能需求：

- 用户管理功能：对用户信息进行管理和维护，包括用户注册、登录、权限管理等。
- 数据管理功能：对系统的数据进行管理和维护，包括货物信息、运单信息、承运商信息等。

- **系统配置功能：**对系统的配置信息进行管理和维护，包括运输产品信息、运输要求信息等。

5. 系统性能需求：

- **高并发处理：**系统需要支持高并发的业务请求，保证快速响应和高效处理。
- **数据准确性和完整性：**系统需要保证数据的准确性和完整性，避免数据丢失或错误。
- **安全性和稳定性：**系统需要具备一定的安全性和稳定性，使用 Spring Security 进行身份验证和授权，使用 Cookies 和会话管理确保安全性，使用拦截器/过滤器等技术来改进系统的功能。

综上所述，智能公路运输调度管理系统的功能需求主要包括发货系统、运单调度管理系统、智能监控中心和系统管理等四个部分。通过对这些功能进行详细的分析和设计，可以确保系统能够满足用户的实际业务需求，提高系统的使用价值和用户满意度。同时，系统需要具备高效、稳定、安全等性能特点，以保证系统的正常运行和服务质量。

3.2 详细性能需求分析

1. 登录

- 至少支持一百个左右用户同时并发登录，登录的响应时间不能超过 5 秒。

2. 业务

- **货主或货代：**货主或货代管理模块包括两个业务过程，进入货主或货代管理界面和新增货主或货代并提交。进入货主或货代管理界面的响应时间不能超过 5 秒，提交新增货主或货代的响应时间不能超过 8 秒。
- **承运商：**承运商管理模块包括两个业务过程，进入承运商管理界面和新增承运商并提交。进入承运商管理界面的响应时间不能超过 5 秒，提交新增承运商的响应时间不能超过 8 秒。
- **运输订单：**运输订单管理模块包括两个业务过程，进入运输订单管理界面和生成统一标准的货物运输单。进入运输订单管理界面的响应时间不能超过 5 秒，生成统一标准的货物运输单的响应时间不能超过 10 秒。
- **货物管理：**货物管理模块包括三个业务过程，获取货物运单，根据货物运单分配货物，更新仓库货物余量。获得货物运单的响应时间不得超过

8 秒，根据货物运单分配货物的响应时间不得超过 10 秒，更新仓库货物余量的响应时间不得超过 8 秒。

- 运单调度：运单调度管理模块包括四个业务过程，获得货物运单，分配运单给承运商系统执行，更新运单调度匹配状态，并将运单管理匹配状态返回给发货状态系统。获得货物运单的响应时间不得超过 8 秒，分配运单给承运商系统执行的响应时间不得超过 10 秒，更新运单调度匹配状态的时间不得超过 8 秒，将运单管理匹配状态返回给发货状态系统的响应时间不得超过 5 秒。
- 运力调度：运力调度管理模块包括四个业务过程，获得货物运单，根据货物运单分配司机和车辆，更新司机池和车辆池。获得货物运单的响应时间不得超过 8 秒，根据货物运单分配司机和车辆的响应时间不得超过 10 秒，更新司机池和车辆池的响应时间不得超过 10 秒。
- 发货状态：发货状态管理模块包括两个业务过程，进入发货状态界面和获得当前发货状态。进入发货状态界面的响应时间不能超过 5 秒，获得当前发货状态的响应时间不能超过 8 秒。
- 智能监控中心：智能监控中心管理模块包括四个业务过程，获得运单信息，对运单在途跟踪，对运单进行服务质量管理，对运单进行预警与事件管理状态。获得运单信息的响应时间不得超过 8 秒，对运单在途跟踪的响应时间不得超过 15 秒，对运单进行服务质量管理的响应时间不得超过 15 秒，对运单进行预警与事件管理状态的响应时间不得超过 20 秒。

3.3 详细资源需求分析

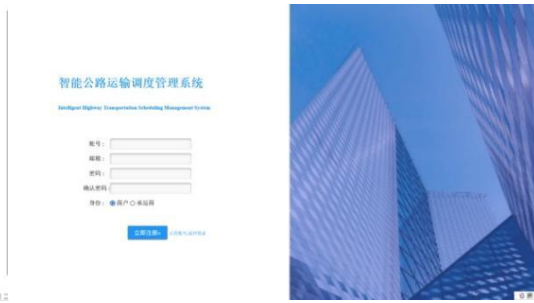
- 计算资源：需要具备一定的计算能力的计算机服务器，以支持运单调度管理系统和智能监控中心的运行。
- 存储资源：需要具备一定的存储能力的计算机服务器，以存储运单调度管理系统和智能监控中心所需的数据，包括承运商运力资源信息、车联网运力资源信息、运输产品信息、货物运输运单信息、运单管理匹配状态信息等。
- 网络资源：需要具备一定的网络带宽和稳定性，以支持承运商系统、车联网系统、发货系统、运单调度管理系统和智能监控中心之间的数据传输和信息交互。
- 接口资源：需要具备一定的接口能力，以实现承运商系统、车联网系统、发货系统、运单调度管理系统和智能监控中心之间的信息互通和交互。

- 人力资源：需要具备一定的技术支持和运维人员，以保证系统的正常运行和维护。
- 安全资源：需要具备一定的安全管理和数据隐私保护能力，以保护系统的信息安全和数据隐私。
- 车联网设备资源：需要具备车联网设备，以实现运输车辆的实时监控和管理。

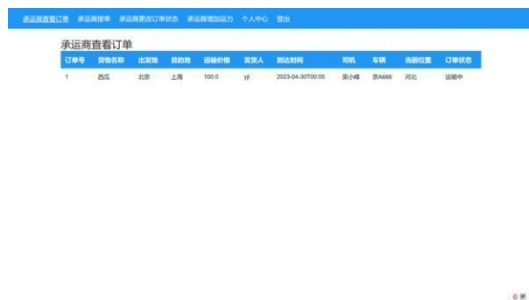
4 系统界面设计



4.1 登录界面



4.2 注册界面



4.3 承运商查看订单界面



4.4 承运商接单界面



4.5 承运商更改订单状态界面



4.6 承运商增加运力界面



4.7 承运商个人中心界面



4.8 商户查看订单界面

4.9 商户添加订单界面

4.10 商户个人中心界面

5 Restful 设计

本系统接口设计采用 HTTP 协议进行通信。通过使用 Spring Security 进行身份验证和授权,使用 Cookies 和会话管理来维护用户状态,以及使用拦截器/过滤器等技术来改进系统的功能和安全性。

5.1 POST 用户登录

(1)URL:/index

(2)请求参数:

名称	位置	类型	必选	说明
body	body	object	否	none
username	body	string	否	none
password	body	string	否	none

(3)返回示例: 200 Response

(4)返回结果:

状态码	状态码含义	说明
200	[OK](https://tools.ietf.org/html/rfc7231#section-6.3.1)	成功

5.2 POST 用户注册

(1)URL:/user

(2)请求参数:

名称	类型	必选	说明
username	string	否	none
password	string	否	none
email	string	否	none
role_id	string	否	none

(3)返回示例: 200 Response

(4)返回结果:

状态码	状态码含义	说明
200	[OK](https://tools.ietf.org/html/rfc7231#section-6.3.1)	成功

5.3 GET 获得公司名下所有车辆和司机

(1)URL:/company/{id}/cars-drivers

(2)请求参数:

名称	类型	必选	说明
Cookie	string	否	none

(3)返回示例: 200 Response

(4)返回结果:

状态码	状态码含义	说明
200	[OK](https://tools.ietf.org/html/rfc7231#section-6.3.1)	成功

5.4 POST 新增一位司机

(1)URL: /company/{id}/driver

(2)请求参数:

名称	类型	必选	说明
drivename	string	否	none
phone	string	否	none
age	string	否	none
driving_age	string	否	none
Cookie	string	否	none

(3)返回示例: 200 Response

(4)返回结果:

状态码	状态码含义	说明
200	[OK](https://tools.ietf.org/html/rfc7231#section-6.3.1)	成功

5.5 POST 新增一辆车

(1)URL:/company/{id}/car

(2)请求参数:

名称	类型	必选	说明
id	string	否	none
car_age	string	否	none
limit_weight	string	否	none
Cookie	string	否	none

(3)返回示例: 200 Response

(4)返回结果:

状态码	状态码含义	说明
200	[OK](https://tools.ietf.org/html/rfc7231#section-6.3.1)	成功

5.6 POST 承运商接单创建订单

(1)URL:/consigner/{id}/order

(2)请求参数:

名称	类型	必选	说明
Cookie	string	否	none

(3)返回示例: 200 Response

(4)返回结果:

状态码	状态码含义	说明
200	[OK](https://tools.ietf.org/html/rfc7231#section-6.3.1)	成功

5.7 POST 更新订单状态和所在地址

(1)URL:/company/{id}/order/{orderId}/{status}/{now_addr}

(2)请求参数:

名称	类型	必选	说明
orderId	string	否	none
status	string	否	none
now_addr	string	否	none
Cookie	string	否	none

(3)返回示例: 200 Response

(4)返回结果:

状态码	状态码含义	说明
200	[OK](https://tools.ietf.org/html/rfc7231#section-6.3.1)	成功

5.8 POST 更新订单状态为已签收

(1)URL:/company/{id}/order/{orderId}/statue/signed

(2)请求参数:

名称	类型	必选	说明
orderId	string	否	none
Cookie	string	否	none

(3)返回示例: 200 Response

(4)返回结果:

状态码	状态码含义	说明
200	[OK](https://tools.ietf.org/html/rfc7231#section-6.3.1)	成功

5.9 POST 商家新建商品

(1)URL:/consigner/{id}/goods

(2)请求参数:

名称	类型	必选	说明
goods_description	string	否	none
dest_addr	string	否	none
price	string	否	none
dest_time	string	否	none
begin_addr	string	否	none
create_time	string	否	none
demands	string	否	none

(3)返回示例: 200 Response

(4)返回结果:

状态码	状态码含义	说明
200	[OK](https://tools.ietf.org/html/rfc7231#section-6.3.1)	成功

6 数据库系统设计

6.1 设计要求

- 1.数据库需要存储承运运力资源信息和车联网运力资源信息，包括车辆信息、司机信息、车辆状态、车辆位置、车辆能力等。
- 2.数据库需要存储货物运输运单信息，包括发货人信息、收货人信息、货物信息、运输产品信息、运输要求信息、运单状态等。
- 3.数据库需要存储运单调度管理系统中的运力池匹配管理信息，包括运力匹配结果、承运商信息、分配结果等。
- 4.数据库需要存储智能监控中心对运单的在途跟踪、服务质量管理及预警与事件管理信息，包括车辆位置、车辆状态、货物状态、服务质量信息、预警与事件信息等。
- 5.数据库需要支持多用户并发访问和操作，要求具有较高的性能和可靠性。

6.2 信息模型设计

- 1.承运商运力资源信息模型：该模型包括承运商信息、车辆信息、司机信息、车辆状态、车辆位置、车辆能力等属性，以及它们之间的关系。
- 2.车联网运力资源信息模型：该模型包括车辆信息、车辆状态、车辆位置、车辆能力等属性，以及它们之间的关系。
- 3.货物运输运单信息模型：该模型包括发货人信息、收货人信息、货物信息、运输产品信息、运输要求信息、运单状态等属性，以及它们之间的关系。
- 4.运单调度管理系统中的运力池匹配管理信息模型：该模型包括运力匹配结果、承运商信息、分配结果等属性，以及它们之间的关系。
- 5.智能监控中心对运单的在途跟踪、服务质量管理及预警与事件管理信息模型：该模型包括车辆位置、车辆状态、货物状态、服务质量信息、预警与事件信息等属性，以及它们之间的关系。

6.3 数据库设计

1.cars 表

Column	Type	Comment	PK	Nullable	Default
id	varchar(255)	Primary Key	YES	NO	
company_id	int			NO	
driver_id	int			YES	

car_age	int	车龄		YES	
limit_weight	int	载重		YES	

2.driver 表

Column	Type	Comment	PK	Nullable	Default
id	int	Primary Key	YES	NO	
drivername	varchar(255)	司机名字		YES	
phone	varchar(12)	司机手机号		YES	
company_id	int	所属承运商		YES	
sex	char(50)			YES	
statue	int	司机的状态		NO	0
age	int	年龄		YES	18
driving_age	int	驾龄		YES	

3.goods 表

Column	Type	Comment	PK	Nullable	Default
id	int	Primary Key	YES	NO	
create_time	datetime	Create Time		YES	
goods_description	varchar(255)	货物描述信息		NO	
begin_addr	varchar(255)	出发地址		NO	
dest_addr	varchar(255)	目的地		NO	
price	float	运输价格		NO	
consigner_id	int	发货人		NO	
dest_time	datetime	货物要求达到时间		NO	
demands	varchar(255)	运输要求		YES	

4.order 表

Column	Type	Comment	PK	Nullable	Default
id	int	Primary Key	YES	NO	
create_time	datetime	Create Time		NO	
price	float	order price		NO	
status	varchar(20)	order status		NO	
begin_addr	varchar(255)	出发地		NO	
dest_addr	varchar(255)	目的地		NO	
now_addr	varchar(255)	当前所在		YES	
goodsId	int	货品		NO	
companyId	int	承运商		NO	

driverId	int	司机		NO	
dest_time	datetime	货物到达时间		YES	
car_id	varchar(255)			NO	

5.role 表

Column	Type	Comment	PK	Nullable	Default
role_id	int	Primary Key	YES	NO	
role_key	varchar(20)	用户角色		YES	

6.user 表

Column	Type	Comment	PK	Nullable	Default
id	int	Primary Key	YES	NO	
username	varchar(255)	Username		NO	
password	varchar(255)	Password		NO	
email	varchar(30)	User email		NO	
sex	varchar(5)	User's sex		YES	
role_id	int	用户对应的角色		NO	

7 系统设计

7.1 关键技术

1. Spring Boot: 使用 Spring Boot 作为后端开发框架，提供了快速构建和部署的能力。
2. Spring Data REST: 使用 Spring Data REST 简化 REST API 的创建和管理，可以基于领域模型自动生成 RESTful 服务。
3. Spring Security: 使用 Spring Security 实现 API 的认证和授权功能，确保 API 的安全性。

```
SecurityFilterChain filterChain(HttpSecurity http) throws Exception {  
    return http.csrf().disable()  
        //设置过滤器  
        .addFilterBefore(jwtAuthenticationFilter,  
            beforeFilter:UsernamePasswordAuthenticationFilter.class)  
        //设置请求认证  
        .authorizeHttpRequests()  
            .requestMatchers(...patterns:"/css/**").permitAll()  
            .requestMatchers(...patterns:"/js/**").permitAll()  
            .requestMatchers(...patterns:"/**-view").permitAll()  
            .requestMatchers(...patterns:"/api-docs").permitAll()  
            .requestMatchers(...patterns:"/api-docs.yaml").permitAll()  
            .requestMatchers(...patterns:"/swagger-ui.html").permitAll()  
            .requestMatchers(...patterns:"/index").anonymous()  
            .requestMatchers(...patterns:"/user").anonymous()  
            //其它的请求都需要登录后才能访问  
            .anyRequest().authenticated()  
        .and()  
        //允许表单登录  
        .formLogin()  
        //登录页面路径  
        .loginPage(loginPage:"/login-view")  
        .loginProcessingUrl(loginProcessingUrl:"/login")  
        .and()  
    }
```

图 7.1 -- Spring Security 配置

4. Redis: 使用 Redis 作为缓存数据库，提高系统的性能和响应速度。
5. FastJson: 使用 FastJson 作为 JSON 序列化和反序列化库，处理 API 请求和响应的数据转换。

6. JWT (JSON Web Token)：使用 JWT 进行身份验证和令牌管理，实现无状态的身份认证。

```
    @Override
    protected void doFilterInternal(HttpServletRequest request,
        HttpServletResponse response, FilterChain filterChain)
        throws ServletException, IOException {
        //获取token
        String token = request.getHeader(name:"token");
        if(!StringUtils.hasText(token)){
            filterChain.doFilter(request, response);
            return ;
        }
        //解析token
        String userId;
        try{
            Claims claim = JwtUtil.parseJWT(token);
            userId = claim.getSubject();
        }catch(Exception e){
            e.printStackTrace();
            throw new RuntimeException(message:"非法token");
        }
        //从redis中获取用户信息
        String redisKey = "Login:"+userId;
        LoginUser loginUser = JSON.parseObject(JSON.toJSONString(redisCache.
            getCacheObject(redisKey)), objectClass:LoginUser.class);
```

图 7.2 -- JWT 身份验证

7. Thymeleaf: 使用 Thymeleaf 作为前端模板引擎，生成动态 HTML 页面。
8. MyBatis: 使用 MyBatis 作为持久层框架，简化数据库操作和数据访问。
9. Spring Session: 使用 Spring Session 实现分布式会话管理，支持在集群环境中进行会话共享。
10. Lombok: 使用 Lombok 库简化 Java 代码的编写，通过注解自动生成常用的代码，如 Getter、Setter 等。
11. MySQL Connector/J: 使用 MySQL Connector/J 驱动程序连接 MySQL 数据库。
12. Spring Boot DevTools: 使用 Spring Boot DevTools 提供的开发工具，支持热部署和自动重启。
13. Spring Boot Test: 使用 Spring Boot Test 进行单元测试和集成测试。
14. OpenAPI: 使用 OpenAPI 规范（以前称为 Swagger）描述和定义 API，提供自动生成 API 文档和客户端代码的能力。

```
/**
 * Controller 获得公司名下所有的车辆和司机
 * @return ResponseResult
 */
@RequestMapping(value = "/company/cars-drivers", method = RequestMethod.GET)
@PreAuthorize("hasAuthority('company')")
```

图 7.3 – API 鉴权

```
{
  "openapi": "3.0.1",
  "info": {
    "title": "shippingManagement",
    "description": "",
    "version": "1.0.0"
  },
  "tags": [
    {
      "name": "user_service"
    },
    {
      "name": "CarsDriverController"
    },
    {
      "name": "GoodsController"
    },
    {
      "name": "OrderController"
    },
    {
      "name": "ViewController"
    }
  ]
}
```

图 7.4 – 生成 openapi 文档

15. Bucket4j: 使用 Bucket4j 实现限流和速率控制, 保护 API 免受过多请求的影响, 提高系统的可用性和稳定性。

```
private final Bucket bucket;

public CarsDriversController() {
    long num = 20;
    Bandwidth limit = Bandwidth.classic(capacity:20, Refill.greedy(num,
        Duration.ofMinutes(minutes:1)));
    this.bucket = Bucket.builder()
        .addLimit(limit)
        .build();
}
```

图 7.5 – 使用 Bucket4j 限流

7.2 Spring Boot 框架开发

此代码实现了一个基于 Spring Boot 的运输和运输服务应用程序, 使用了 MVC 架构和 RESTful API 设计风格。它通过 Controller 类处理 HTTP 请求, 调用 Service 类处理业务逻辑, 通过 Dao 类与 MySQL 数据库交互。同时, 它还具备权限控制、统一的 API 响应格式、缓存和身份验证等功能, 以提供安全、高效和可扩展的运输和运输服务。

1. 使用了 MVC (Model-View-Controller) 架构模式: 代码中的各个 Controller 类负责处理不同的 HTTP 请求, 并根据业务逻辑返回响应结果。这种分离了请求处理、业务逻辑和视图渲染的架构模式有助于代码的可维护性和可扩展性。

2. 使用了 RESTful API 设计: 代码中的 Controller 类使用了 Spring 的注解(如 '@RestController'、'@RequestMapping') 来定义 RESTful 风格的 API 接口。每个 API 接口对应一个 URL 路径, 通过不同的 HTTP 方法 (GET、POST、PUT 等) 实现不同的操作。

3. 使用了权限控制: 代码中使用了 '@PreAuthorize' 注解来标识需要进行权限验证的接口, 确保只有具有相应权限的用户才能访问。这种权限控制机制可以保护敏感数据和操作, 提高系统的安全性。

4. 使用了 Service 层进行业务逻辑处理: 代码中的 Controller 类通过注入相应的 Service 类来调用业务逻辑的方法, 实现了控制器与业务逻辑的解耦。Service 类负责处理具体的业务逻辑, 并与数据访问层 (如 Dao 类) 交互, 完成相应的操作。

5. 使用了 ResponseEntity 类封装 API 响应结果: 代码中定义了一个通用的 ResponseEntity 类, 用于封装 API 接口的响应结果, 包括状态码、消息和数据。这种统一的响应结果格式可以提高代码的可读性和一致性, 并方便客户端解析。

6. 使用了 Redis 缓存和 JWT (JSON Web Token): 代码中使用了 RedisCache 来缓存用户信息, 提高系统性能和访问速度。同时, 使用了 JWT 来生成和解析身份验证令牌, 实现了无状态的身份验证机制, 简化了用户身份验证流程。

7. 使用了 MySQL 数据库: 根据代码中的实体类和服务类, 可以推断出使用了 MySQL 作为持久化存储数据库。代码中的服务类通过调用相应的 Dao 类来访问和操作数据库。

7.3 安全认证

7.3.1 SpringSecurity 和 JWT 的认证授权

使用 Spring Security 和 JWT 进行身份验证和授权的基本工作流程:

1. 用户进行身份验证: 用户在登录页面输入用户名和密码。
2. 身份验证: 应用程序使用 Spring Security 的身份验证机制验证用户提供的凭据。这可能涉及将凭据与数据库中的用户存储进行比较或与外部身份验证服务进行交互。
3. 生成 JWT: 如果用户凭据有效, 则应用程序生成一个 JWT, 并将其返回给客户端作为身份验证成功的响应。JWT 包含了用户的身份信息以及其他相关信息, 如过期时间和权限。

4. 客户端存储 JWT: 客户端（通常是浏览器）将收到的 JWT 保存在本地，通常是在 Cookie 或本地存储中。
5. 后续请求中的授权: 在后续的请求中，客户端将 JWT 包含在请求的标头或其他适当的位置中。这允许服务器对请求进行授权并验证用户身份。
6. 服务器验证和解析 JWT: 服务器使用与生成 JWT 时相同的密钥对 JWT 进行验证和解析。这确保 JWT 没有被篡改或伪造，并且仍然有效。
7. 授权和访问控制: 服务器根据 JWT 中的用户身份信息和权限进行授权和访问控制决策。这可能涉及检查用户是否具有请求资源的适当权限。

使用 Spring Security 和 JWT 进行身份验证和授权的好处包括:

1. 无状态: JWT 是无状态的，服务器不需要在会话或数据库中存储任何用户状态。这使得应用程序可以更容易地水平扩展，并使负载均衡变得更简单。
2. 松耦合: JWT 允许应用程序和身份验证服务之间的松耦合。应用程序只需验证 JWT 的有效性，而不需要直接与身份验证服务进行通信。
3. 可扩展性: 通过使用 JWT，您可以将身份验证和授权机制与其他服务（如单点登录）进行集成，从而提供更强大和可扩展的解决方案。

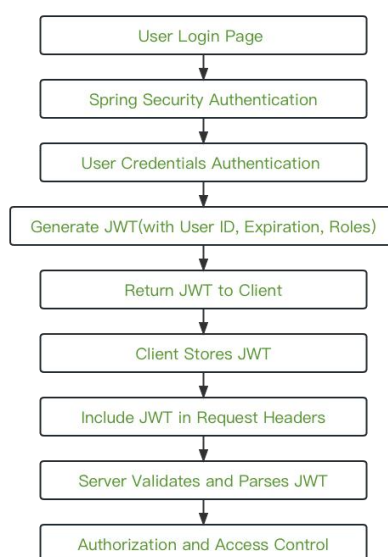


图 7.1 安全认证流程图

7.3.2 保护敏感数据和防止安全漏洞 —— 密码加密

`new BCryptPasswordEncoder()` 是使用 Spring Security 提供的 `BCryptPasswordEncoder` 类创建一个密码编码器的示例。`BCryptPasswordEncoder` 是一种密码哈希算法，它结合了哈希函数和盐值，提供了安全的密码存储和验证机制。


```

19      * spring security配置
20      */
21      @Configuration
22      @EnableWebSecurity
23      @EnableGlobalMethodSecurity(prePostEnabled = true)
24      public class WebSecurityConfig{
25          @Autowired
26          private AuthenticationConfiguration authenticationConfiguration;
27
28          @Autowired          通过 BCryptPasswordEncoder() 函数来实现加密解密
29          private JwtAuthenticationFilter jwtAuthenticationFilter;
30
31          @Bean
32          public PasswordEncoder passwordEncoder() { return new BCryptPasswordEncoder(); }

```

8 总结

本项目重新开发了一个运输和运输管理的 Web 应用程序，使用 REST API 和 Thymeleaf 模板引擎进行通信和页面渲染。通过采用 Restful API 设计和实施运输和运输服务，并使用 Spring Security 和 JWT 进行 API 认证和授权，系统实现了更加安全和可靠的数据传输和访问。通过连续单元测试、应用 OpenAPI 文档和速率限制等措施，系统的功能和性能得到了进一步的改进。整体而言，新系统的设计和实现使得运输和运输管理变得更加高效和便捷。