PAYROLL MANAGEMENT SYSTEM

Introduction:

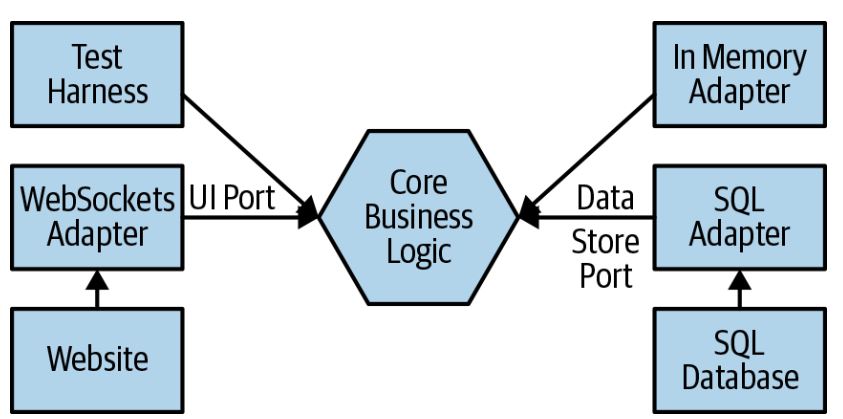
**SOFTWARE DESIGN**

This project is designed using **microservices** to manage different domain modules regarding the payroll management system.

**HEXAGONAL ARCHITECTURE SOLUTION WITH OUR MICROSERVICES**

We use the (ports and Adapters) or Hexagonal architecture introduced by Alister Cockburn to implement our **microservices** approach to solving this problem.

This will help separate the **business logic** from different implementation choices. **Events** from the outside world would arrive and depart from the business logic core through a port. An **adapter** is technology-specific implementation code that plugs into the port.



The ports of the system, would allow

1. Authentication services from external applications to log in users and into our system.
2. User Management, where various users can perform operations against our application, which is then persisted to our database using persistence frameworks.

**MANDATORY SERVICES FOR GOOD MICROSERVICES**

There are a few patterns/services that should be in place for implementing microservice-based design. This list consists of the following:

* Service discovery and registration
* Edge or proxy server
* Load balancing
* Circuit breaker
* Monitoring

And this conforms to the hexagonal architecture implementation to developing our microservices.

**SERVICE DISCOVERY AND REGISTRATION**

The **Netflix Eureka server** is used for service discovery and registration. We created the Eureka service in the last chapter. It not only allows you to register and discover services, but also provides load balancing using Ribbon.

**EDGE SERVERS**

An edge server provides a single point of access to allow the external world to interact with your system. All of your APIs and frontends are only accessible using this server. Therefore, these are also referred to as gateway or proxy servers. These are configured to route requests to different microservices or frontend applications. We'll use the **Netflix Zuul server** as an edge server in this application.

**LOAD BALANCING**

**Netflix Ribbon** is used for load balancing. It is integrated with the Zuul and Eureka services to provide load balancing for both internal and external calls.

**CIRCUIT BREAKERS**

A fault or break should not prevent your whole system from working. Also, the repeated failure of a service or an API should be handled properly. Circuit breakers provide these features**. Netflix Hystrix** is used as a circuit breaker and helps to keep the system up.

**MONITORING**

The **Hystrix dashboard** is used with **Netflix Turbine** for microservice monitoring. It provides a dashboard to check the health of running microservices.

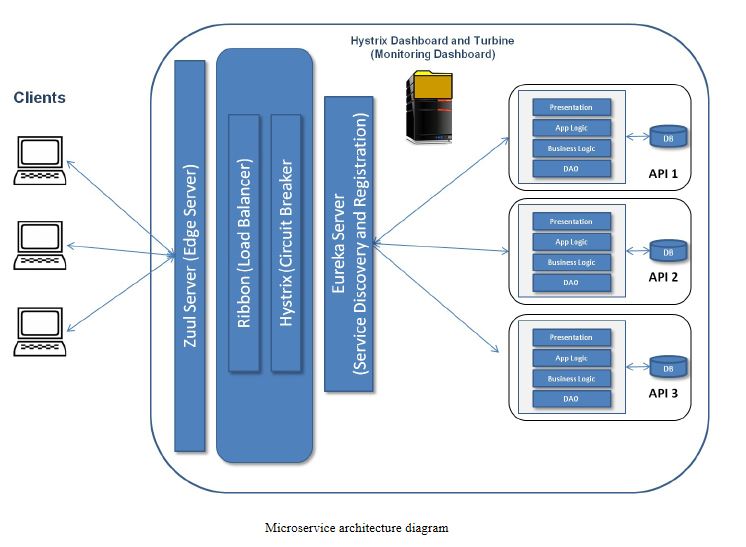
**AN OVERVIEW OF MICROSERVICES ARCHITECTURE USING Netflix OSS**

Netflix are pioneers in microservice architecture. They were the first to successfully implement microservice architecture on a large scale. They also helped increase its popularity and contributed immensely to microservices by open sourcing most of their microservice tools with Netflix **Open-Source Software Centre** (**OS**).

According to the Netflix blog, when Netflix was developing their platform, they used Apache Cassandra for data storage, which is an open-source tool from Apache. They started contributing to Cassandra with fixes and optimization extensions. This led to Netflix seeing the benefits of releasing Netflix projects with the name OSS.

Spring took the opportunity to integrate many Netflix OSS projects, such as Zuul, Ribbon, Hystrix, the Eureka server, and Turbine, into Spring Cloud. This is one of the reasons Spring Cloud provides a ready-made platform for developing production-ready microservices.

Now, let's take a look at a few important Netflix tools and how they fit into microservice architecture:



* **Edge server**: We use the Netflix Zuul server as an edge server.
* **Load balancing**: Netflix Ribbon is used for load balancing.
* **Circuit breaker**: Netflix Hystrix is used as a circuit breaker and helps to keep the system up.
* **Service discovery and registration**: The Netflix Eureka server is used for service discovery and registration.
* **Monitoring dashboard**: The Hystrix dashboard is used with Netflix Turbine for microservice monitoring. It provides a dashboard to check the health of running microservices.

**LOAD BALANCING**

Load balancing is required to service requests in a manner that maximizes speed and capacity utilization, and it makes sure that no server is overloaded with requests. The load balancer also redirects requests to the remaining host servers if a server goes down. In microservice architecture, a microservice can serve internal or external requests. Based on this, we can have two types of load balancing—client-side and server-side load balancing.

* We use server-side load balancing because of the following tradeoffs:

1. **Throughput**

Server side load balancers can handle a very high throughput than client side load balancers. Normally serverside LB vendors manufacture hardware load balancers as well. They are even more optimized to handle hundreds of thousand requests per second.

1. **Lite Weight Client Support**

For lite weight client applications (Single Page Applications, Mobile Application, IoT device) server side load balancing is the best option. Since lite weight devices have limited memory and processing power, it is difficult for them to tolerate the additional overhead of a client side load balancer.

1. **Client to Server Hight Network Latency**

Client side load balancers send heart beats to available service instances periodically (or contact discovery server to refresh available service instances). These connections get delayed or timeout might occurs if the latency is high. If the load balancing happens at the server side, then client does not need to send additional requests.

**CIRCUIT BREAKERS AND MONITORING**

In general terms, a circuit breaker is a*n automatic device for stopping the flow of current in an electric circuit as a safety measure.*

The same concept is used for microservice development, known as the **circuit breaker** design pattern. It tracks the availability of external services such as the Eureka server, API services such as restaurant-service, and so on, and prevents service consumers from performing any action on any service that is not available.

It is another important aspect of microservice architecture, a safety measure  
(failsafe mechanism) when the service does not respond to a call made by the service consumer, which is called a circuit breaker.

We'll use Netflix Hystrix as a circuit breaker. It calls the internal fallback method in the service consumer when failures occur (for example, due to a communication error or timeout). It executes embedded within its consumer of service. In the next section, you will find the code that implements this feature.

Hystrix opens the circuit and fail fast when the service fails to respond repeatedly, until the service is available again. When calls to a particular service reach a certain threshold (the default threshold is 20 failures in five seconds), the circuit opens and the call is not made. You must be wondering, if Hystrix opens the circuit, then how does it know that the service is available? It exceptionally allows some requests to call the service.

**MONITORING**

Hystrix provides a dashboard with a web UI that provides nice graphics of circuit breakers:

Netflix Turbine is a web application that connects to the instances of your Hystrix applications in a cluster and aggregates information, which it does in real time (updated every 0.5 seconds). Turbine provides information using a stream that is known as a Turbine stream.

If you combine Hystrix with Netflix Turbine, then you can get all of the information from the Eureka server on the Hystrix dashboard. This gives you a landscape view of all of the information about the circuit breakers.

To use Turbine with Hystrix, just type in the Turbine URL http://localhost:8989/turbine.stream (port 8989 is configured for the Turbine server in **application.properties**) in the first textbox shown in the preceding screenshot, and click on Monitor Stream.

Netflix Hystrix and Turbine use RabbitMQ, an open-source message queuing software. RabbitMQ works on **Advance Messaging Queue Protocol** (**AMQP**). It is a software in which queues can be defined and used by connected applications to exchange messages. A message can include any kind of information. A message can be stored in the RabbitMQ queue until a receiver application connects and consumes the message (taking the message off the queue).

Hystrix uses RabbitMQ to send metrics data feed to Turbine.

***Before we configure Hystrix and Turbine, please install the RabbitMQ application on your platform. Hystrix and Turbine use RabbitMQ to communicate between themselves.***

**CREATING TURBINE SERVICES**

Turbine aggregates all **/hystrix.stream** endpoints into a combined **/turbine.stream** for use in the Hystrix dashboard, which is more helpful as it allows to see the overall health of the system in a single dashboard rather than monitoring the individual services using **/hystrix.stream**. We'll create another service project in the IDE like the others. Then, we'll add Maven dependencies for Turbine in pom.xml.

**PASSWORDS AND SECURITY**

Because storing passwords as plain texts is a bad practice, as malicious users can log on to our system and pretend to be the users, we apply a **cryptographic hash function** to the password. This is a function that takes some arbitrarily sized **input string**  and converts it to **some output**, called a **digest.** Cryptographic hash functions are **deterministic** , so if we hash the same input again we get the same result. This is essential in order to be able to check the **hashed password later.** Another key property is that while it should be quick to go from the **input**  to the **digest**, the reverse function should take so long or use so much memory that it is impractical for an attacker to reverse the digest. We use an established Java library called **Bouncy Castle.** This is open source and has undergone heavy peer review. We use the **Scrypt** hashing function, which is a modern algorithm specifically designed for storing passwords.

**SOFTWARE and TOOLS USED**

1. Spring Tool Suite
2. Spring cloud APIS, which provides a cloud-ready solution that is available through SpringBoot.
3. Wamp Server
4. MySQL Workbench
5. Angular SPA framework (for UI)
6. Maven
7. To manage dependencies, and packaging in a specific format such as WAR or JAR.
8. To automate repetitive tasks including building, testing and deploying your application.

**MAVEN PROJECT STRUCTURE**

The great thing about Maven is that from the get-go it comes with structure to help maintenance. A Maven project starts with two main folders:

**/src/main/java**

This is where you will develop and find all the Java classes required for your project.

**src/test/java**

This where you will develop and find all the tests for your project.

There are two additional folders that are useful but not required:

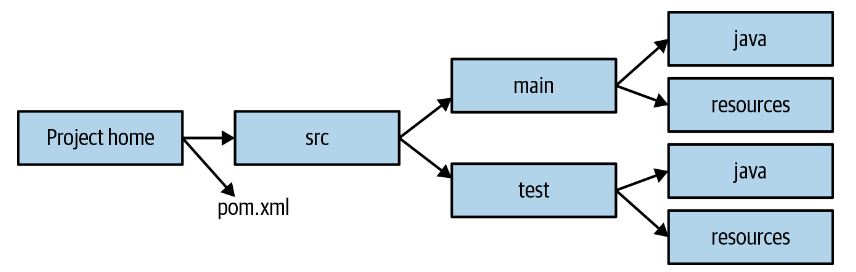
**src/main/resources**

This is where you can include extra resources such as text files needed by your application.

**src/test/resources**

This is where you can include extra resources used by your tests.

Having this common directory layout allows anyone familiar with Maven to be immediately able to locate important files. To specify the build process, you will need to create a *pom.xml* file where you specify various XML declarations to document the steps required to build your application. The figure summarizes the common Maven project layout.



**EXAMPLE BUILD FILE**

The next step is to create the *pom.xml* that will dictate the build process. The code snippet in [Example 3-26](file:///C:\Users\STHIGWGFWB\AppData\Local\Temp\pmtoq3eq.pqt\OEBPS\ch03.xhtml#maven_pom_simple) shows a basic example that you can use for building the Bank Statements Analyzer project. You will see several elements in this file:

**project**

This is the top-level element in all *pom.xml* files.

**groupId**

This element indicates the unique identifier of the organization that created the project.

**artifactId**

This element specifies a unique base name for the artifact generated by the build process.

**packaging**

This element indicates the package type to be used by this artifact (e.g., JAR, WAR, EAR, etc.). The default is JAR if the XML element packaging is omitted.

**version**

The version of the artifact generated by the project.

**build**

This element specifies various configurations to guide the build process such as plug-ins and resources.

**dependencies**

This element specifies a dependency list for the project.

**DEVELOPING AND IMPLEMENTING OUR MICROSERVICE**

We use a domain-driven implementation and approach to implement the microservices using **Spring Cloud.**

1. Entities

These are categories of objects that are identifiable and remain the same throughout the states of the product/services. These objects are *not* defined by their attributes, but by their identities and threads of continuity. Entities have traits such as identity, a thread of continuity, and attributes that do not define their identity.

1. Value Objects

just have the attributes and no conceptual identity. A best practice is to keep VOs as immutable objects. In the Spring Framework, entities are pure POJOs; therefore, we'll also use them as VOs.

1. Service Objects

These are common in technical frameworks. These are also used in the domain layer in domain-driven design. A service object does not have an internal state; the only purpose of it is to provide the behavior to the domain. Service objects provide behaviors that cannot be related with specific entities or VOs. Service objects may provide one or more related behaviors to one or more entities or VOs. It is best practice to define the services explicitly in the domain model.

1. Repository objects

A repository object is a part of the domain model that interacts with storage, such as databases, external sources, and so on, to retrieve the persisted objects. When a request is received by the repository for an object reference, it returns the existing object reference. If the requested object does not exist in the repository, then it retrieves the object from storage.

**REGISTRATION AND DISCOVERY SERVICE**

We need a place where all microservices get registered and can be referenced—a service discovery and registration application. **Spring Cloud** provides the state-of-the-art service registry and discovery application **Netflix Eureka**

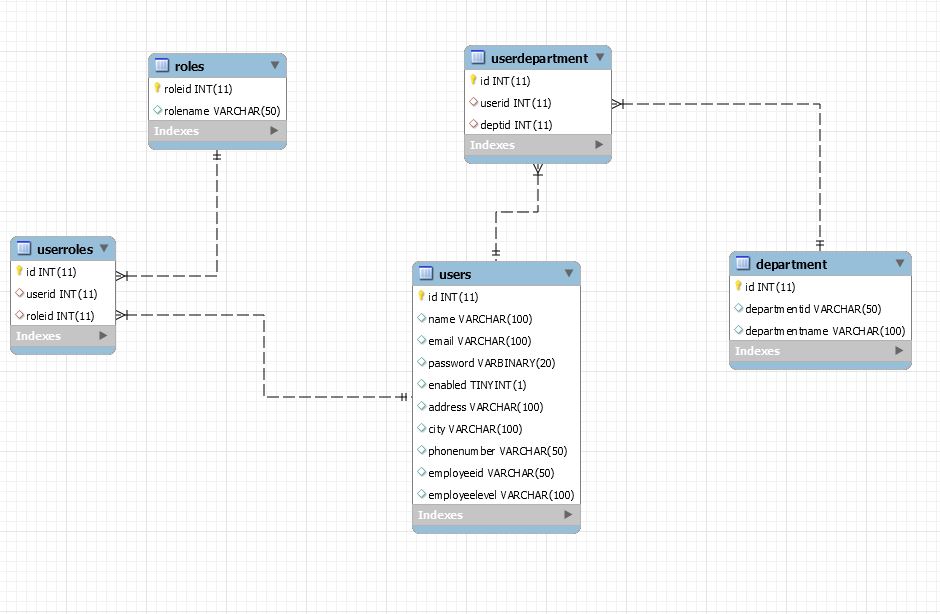
Once you have configured the Eureka service as described in this section, it will be available for all incoming requests to list it on the Eureka service. The Eureka service registers/lists all microservices that have been configured by the Eureka client. Once you start your service, it pings the Eureka service configured in your **application.properties** and once a connection is established, the Eureka service registers the service.

It also enables the discovery of microservices through a uniform way to connect to other microservices. You don't need any IP, hostname, or port to find the service, you just need to provide the service ID to it. Service IDs are configured in the **application.properties** of the respective microservices.

**EUREKA CLIENT**

Similar to the **Eureka server**, each service should also contain the **Eureka client** configuration, so that a connection between the Eureka server and the client can be established. Without this, the registration and discovery of services is not possible.

DATABASE SCHEMA



DATABASE CODES

create database payrollusermanagement;

use payrollusermanagement;

########################################

#create table users

########################################

create table users (

id int primary key auto\_increment,

name varchar (100),

email varchar (100) unique,

password varbinary (20),

enabled boolean,

address varchar (100),

city varchar(100),

phonenumber varchar (50) unique,

employeeid varchar (50) unique,

employeelevel varchar (100)

) engine =InnoDb;

########################################

#create table roles

########################################

create table roles (

roleid int primary key auto\_increment,

rolename varchar(50) unique

) engine =InnoDB;

########################################

#create table userroles

########################################

create table userroles (

id int primary key auto\_increment,

userid int,

roleid int,

foreign key(userid) references users(id) on delete set null,

foreign key(roleid) references roles(roleid) on delete set null

) engine = InnoDB;

########################################

#create table department

########################################

create table department (

id int primary key auto\_increment,

departmentid varchar (50) unique,

departmentname varchar (100)

) engine = InnoDB;

########################################

#create table userdepartment

########################################

create table userdepartment (

id int primary key auto\_increment,

userid int,

deptid int,

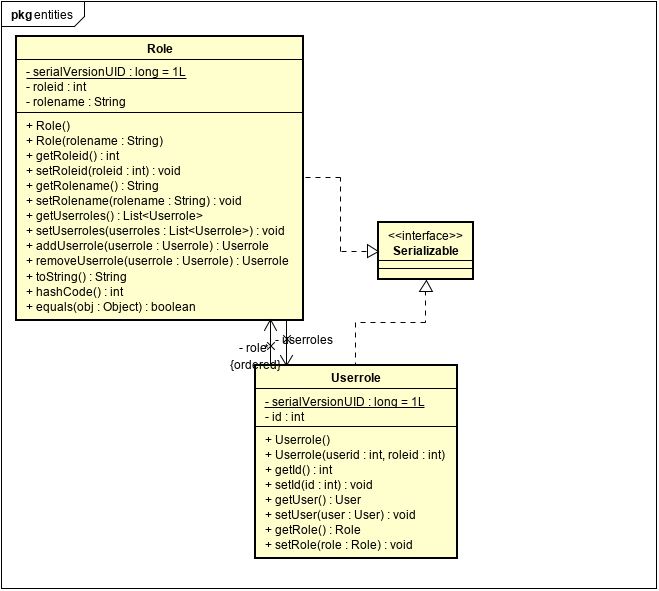
foreign key(userid) references users(id) on delete set null,

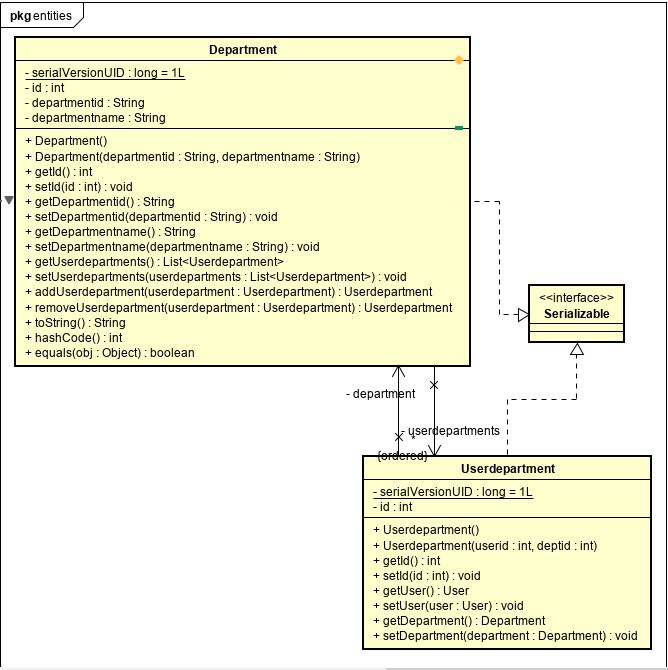
foreign key(deptid) references department(id) on delete set null

) engine = InnoDB;

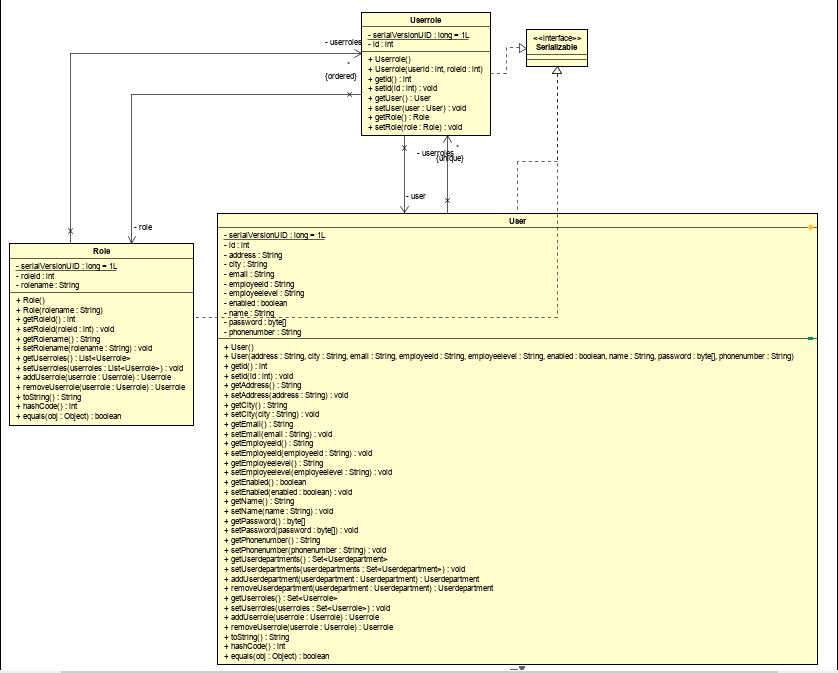
ENTITIES CLASS DIAGRAM

ROLE



DEPARTMENT#

USERROLE

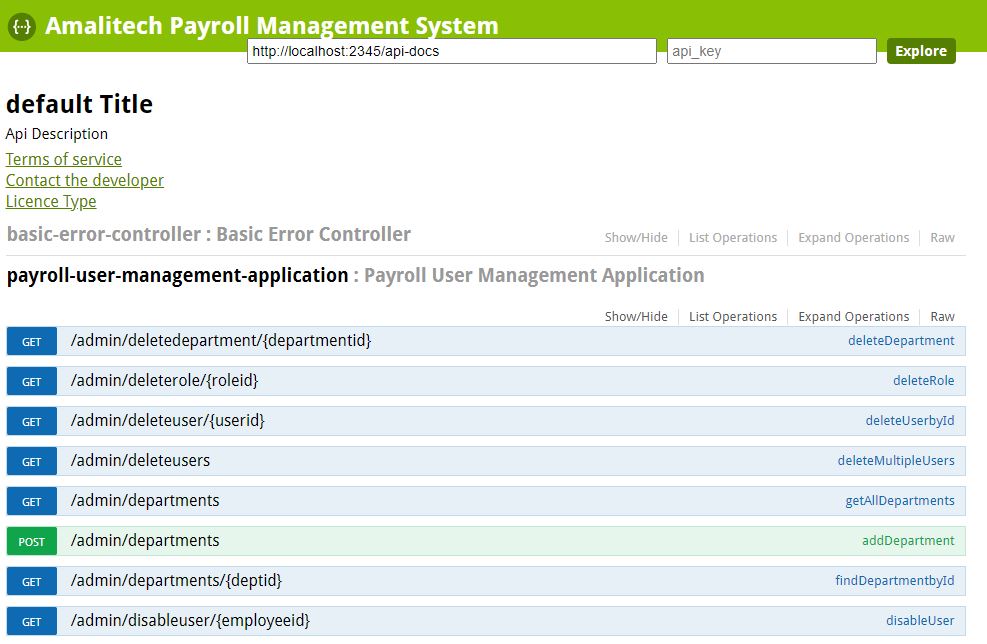


DOCUMENTING THE PROJECT WEB SERVICES WITH SWAGGER UI

1. Download the the swaggerUI from github
2. Extract the folder
3. Create a folder (foldername) under src/main/resources in the  **static folder**
4. Copy the content the of the **dist**  in the extracted folder and paste it in the (foldername) you created under the  **static**  folder
5. Add the (swagger) maven dependency in **pom.xml**  file
6. Add the annotation @EnableSwagger in the main class
7. Edit the **index.html** file of swagger dist files and within the url:
8. Change it to point to your localhost url, just like this



1. Launch your application and all **restEndpoints**  will be populated in the **swaggerUI**  browser, where you can perform all operations to the restful endpoints.



API **VERSONING, PAGING AND SORTING**

**URI VERSONING**

We use URI versoning approach for this approach.

In this approach, version information becomes part of the URI. For example,

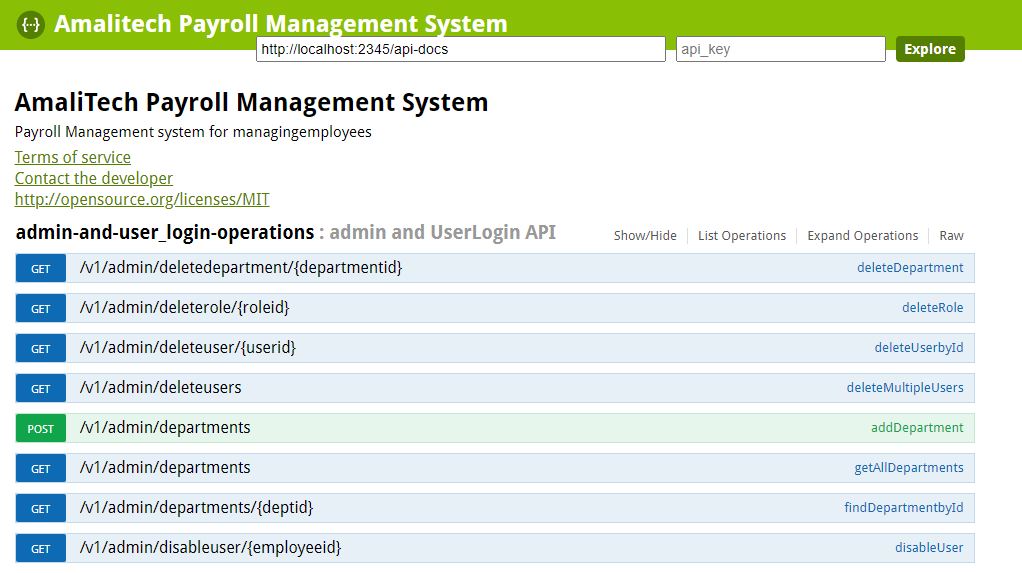
**http://api.example.org/v1/users**  
and [**http://api.example.org/v2/users**](http://api.example.org/v2/users)

represent two different versions of an application API. Here we  
use v notation to denote versioning and the numbers 1 and 2 following the v indicate the first and second  
API versions.

To achieve version, **@RequestMapping(“/v1”)** is placed on the @**RestController**  endpoints and referenced in swagger sample code is shown below:



Now all **uri endpoints starts with /v1/resourcename..**  as can be seen on the swagger window



**PAGINATION**

REST APIs are consumed by a variety of clients ranging from desktop applications to Web to mobile devices.  
Hence, while designing a REST API capable of returning vast datasets, it is important to limit the amount of  
data returned for bandwidth and performance reasons. The bandwidth concerns become more important  
in the case of mobile clients consuming the API. Limiting the data can vastly improve the server’s ability to  
retrieve data faster from a datastore and the client’s ability to process the data and render the UI. By splitting  
the data into discrete pages or *paging data*, REST services allow clients to scroll through and access the  
entire dataset in manageable chunks.

To support large poll datasets in a **AmaliTech Payroll Management System** application, we will be implementing the page number  
pagination style and will include the paging information in the response body.

Spring Data JPA and Spring MVC provides out of the box support for the page number pagination style,  
making our **AmaliTech Payroll Management System** paging implementation easy. Central to paging (and sorting) functionality in Spring Data JPA  
is the org.springframework.data.repository.PagingAndSortingRepository interface shown below: **Spring Data JPA’s paging and sorting repository  
public interface PagingAndSortingRepository<T, ID extends Serializable> extends  
CrudRepository<T, ID> {  
Page<T> findAll(Pageable pageable);  
Iterable<T> findAll(Sort sort);  
}**

**Implementing it in the project**

Iterable<User> getAllUsers(Pageable pageable);

<http://localhost:8762/payrollusers/v1/admin/user?page=0&size=2>

SORTING

Sorting allows REST clients to determine the order in which items in a dataset are arranged. REST services  
supporting sorting allow clients to submit parameters with properties to be used for sorting

Implementation in the project:

Sort ASCENDING

<http://localhost:8762/payrollusers/v1/admin/user?sort=name>

Sort DESCENDING

<http://localhost:8762/payrollusers/v1/admin/user?sort=name,desc>

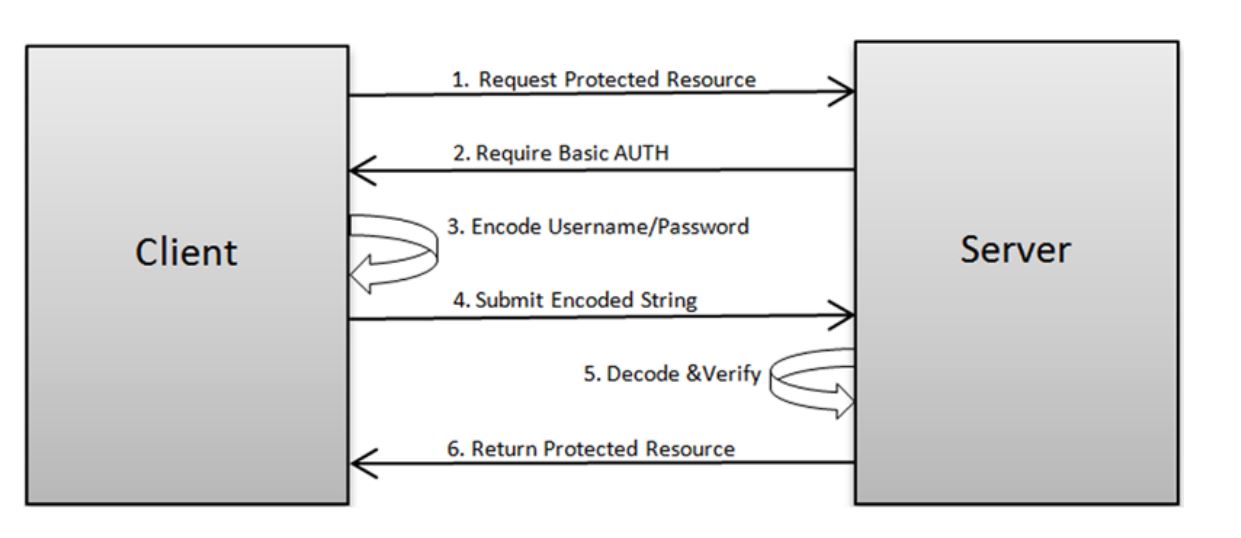
**SECURITY**

**Using Spring Security**

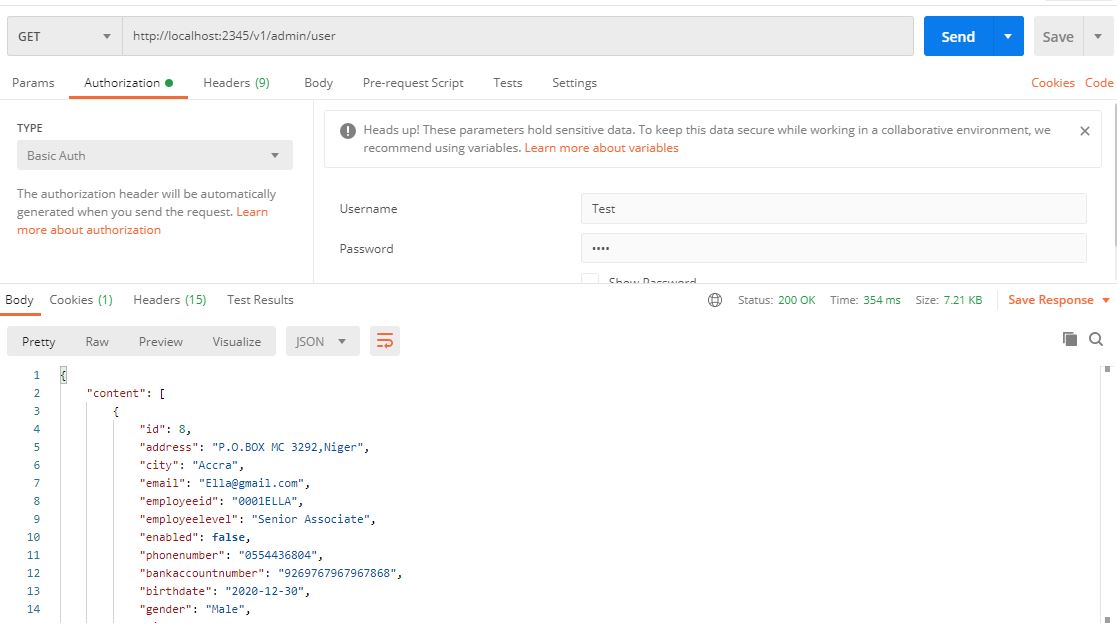
BCrypt algorithm generates a String of length 60, so we need to make sure that the password will be stored in a column that can accommodate it. A common mistake is to create a column of a different length and then get an Invalid Username or Password error at authentication time.

Successfully implemented **bCrypt**  encryption algorithm in verifying users of the system.

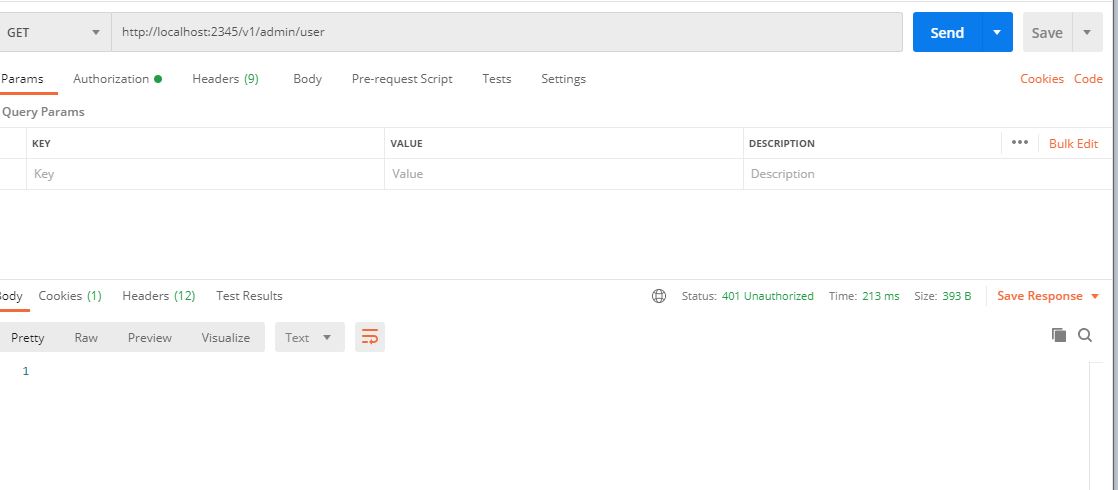
BASIC AUTHENTICATION WORKLOW DIAGRAM



Snapshot of verifying authentication via **POSTMAN**



Without Authentication:



**SECURING URIs**  
To secure the **restEndpoints**  we override the **configure**  in **WebSecurityConfigurerAdapter**

Sample code showing which **URIs** need authentication and which ones do not



Cross-site request forgery, or CSrF (http://en.wikipedia.org/wiki/Cross-site\_request\_  
forgery), is a type of security vulnerability whereby a malicious website forces the end user to execute  
unwanted commands on a different website in which they are currently authenticated. Spring Security by  
default enables CSrF protection and highly recommends using it for requests submitted by a user via a  
browser. For services that are used by nonbrowser clients, the CSrF can be disabled. By implementing custom  
RequestMatchers, it is possible to disable CSrF only for certain urLs or http methods

**Sample**

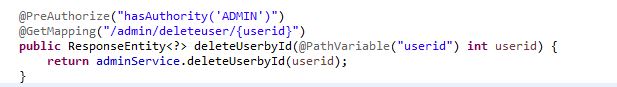
In this application, only users with **ADMIN**  roles can delete a user from the system so, we add the annotation

@EnableGlobalMethodSecurity(prePostEnabled = **true**)

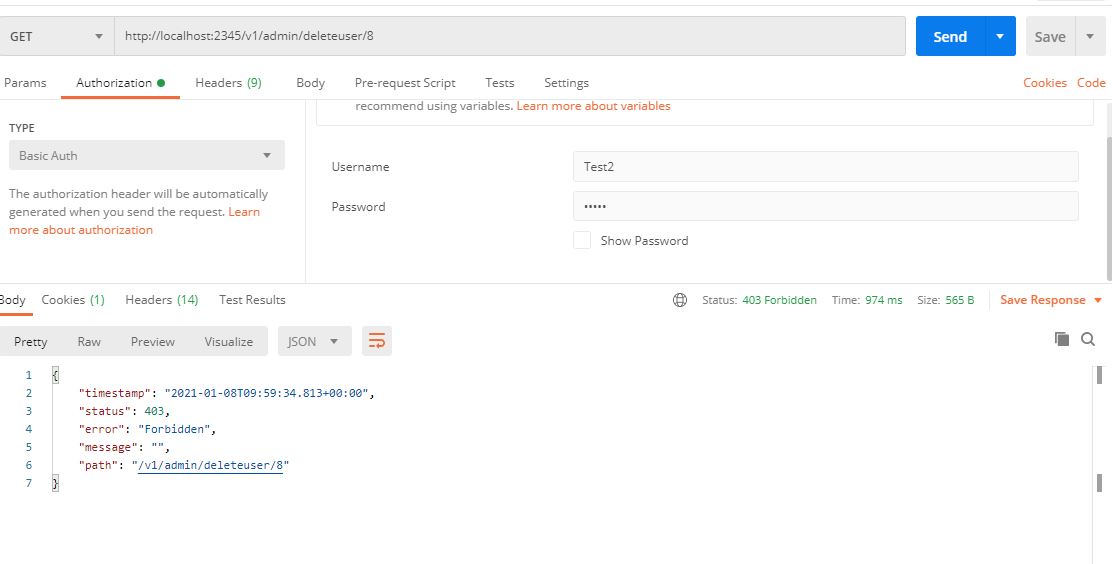
To allow for **URI** method security features

The **URI**  is annotated with

@PreAuthorize("hasAuthority('ADMIN')") , to check if a user has an **ADMIN role** before they can delete a user



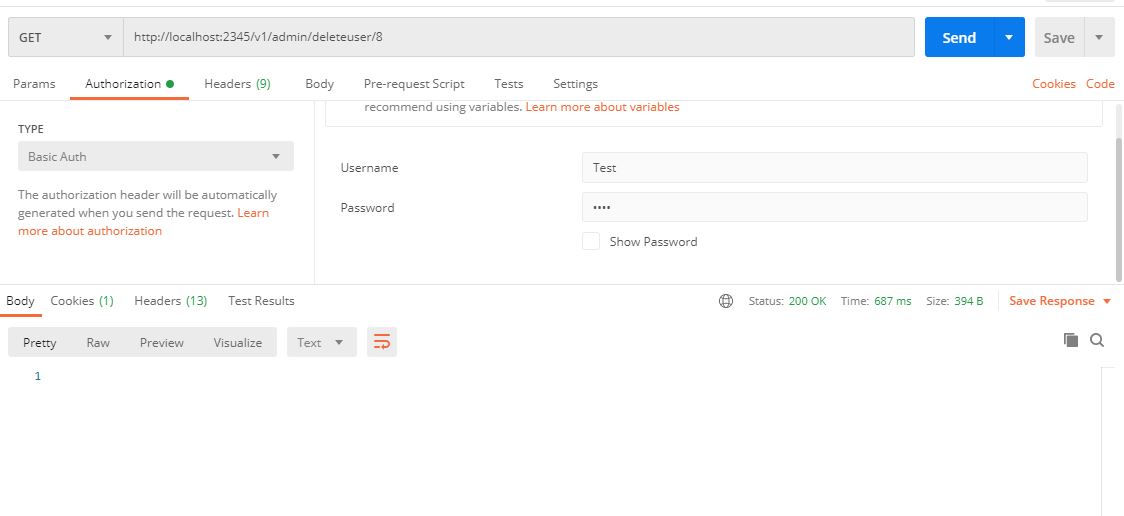
Now we use POSTMAN to test **TWO users,** with which one has **ADMIN role** and can **DELETE a user ,** whiles the other does not have **ADMIN role**  and thus cannot delete a user from the system.



User (**Test2 with his authentication)** is forbidden to delete a user, as can be seen from the **POSTMAN** interface

Above.

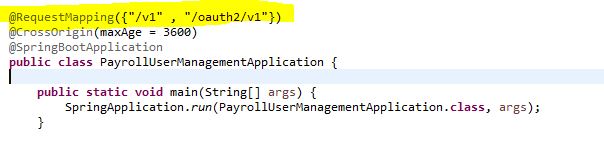
Now with a User(**Test with his authentication)**  has response **200 OK,** and thus has deleted the user with **Id 8 ,** successfully as can be seen from the **POSTMAN**  interface

****

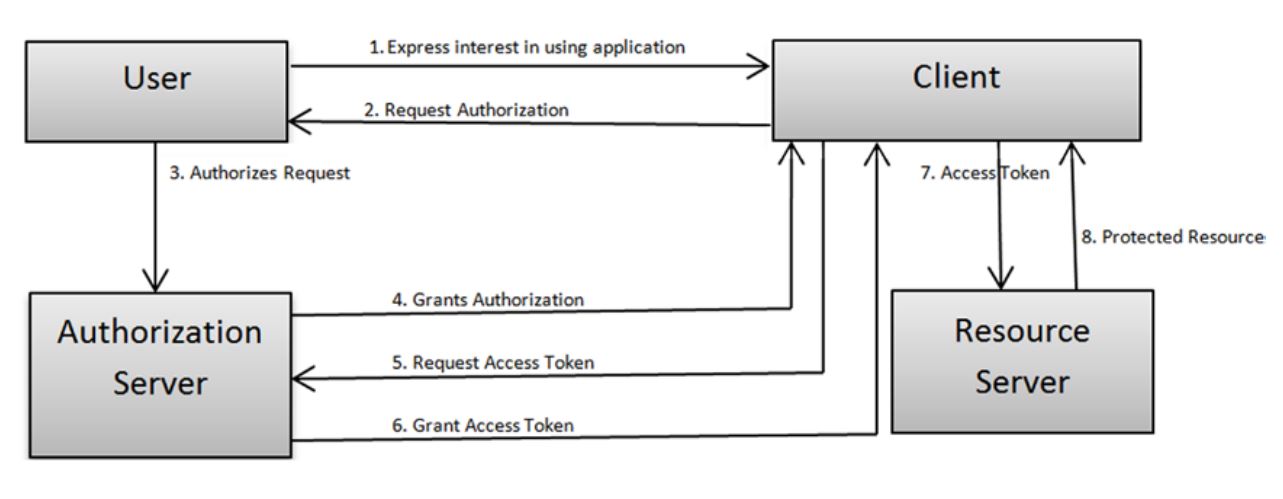
ADDING **OAUTH2** authentication to our project

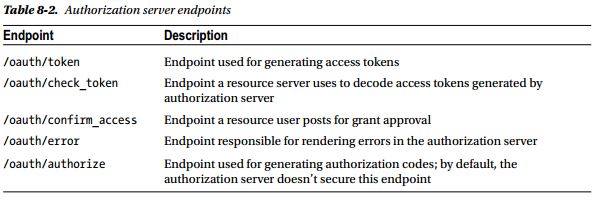
We want to ensure that adding OAuth to **Amalitech Payroll Management System** shouldn’t break other clients currently using Basic  
Authentication (or any future authentication mechanism implementations such as Form-based login).

To achieve this, we will add another request mapping to the **PayrollUserManagementApplication class**.  
The new mapping **/oauth2/v1** allows us to access the same **PayrollUserManagementApplication resources** via an additional set  
of URIs such as **/oauth2/v1/admin/\*\*** and **/outh2/v1/user/12**. It will also allow us to apply additional OAuth security to these **PayrollUserManagementApplication** resources.



**OAUTH2 security workflow diagram**



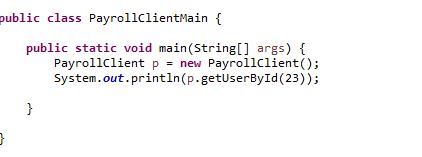


**BUILDING A JAVA RESTCLIENT TO CONSUME THE (rest APIs)**Central to Spring’s support for building REST clients is the org.springframework.web.client.  
RestTemplate. The RestTemplate takes care of the necessary plumbing needed to communicate with REST  
services and automatically marshals/unmarshals HTTP request and response bodies. The RestTemplate  
like Spring’s other popular helper classes such as JdbcTemplate and JmsTemplate, is based on the Template  
Method design pattern

RestTemplate provides convenient methods to perform API requests using six commonly used HTTP  
methods

\*\*We need to create the **Value Objects** which will be returned by the **restAPIs,** so that outputs will correspond to json data returned by **restEndpoints**







* To retrieve these results, the **API\_ URLs** should be up and running.

**TESTING REST SERVICES**

Testing is an important aspect of every software development process. Testing comes in different flavors  
BUT we will focus on unit and integration testing.

Unit testing verifies that individual, isolated ***units*** of code are working as expected. It is the most common type of testing that developers typically  
perform.

Integration testing typically follows unit testing and focuses on the interaction between previously  
tested units

**HATEOAS**

We will review HATEOAS, a constraint that allows us to build resilient REST services that function like a website.

The **H**ypermedia **A**s **T**he **E**ngine **O**f **A**pplication **S**tate, or HATEOAS, is a key constraint of REST architecture. The term “hypermedia” refers to any content that contains links to other forms of media such as images,  
movies, and text

The idea behind HATEOAS is simple—a response would include links to other resources. Clients would use these links to interact with the server and these interactions could result in possible state changes.

Similar to a human’s interaction with a website, a REST client hits an initial API URI and uses the serverprovided links to dynamically discover available actions and access the resources it needs. The client need not have prior knowledge of the service or the different steps involved in a workflow. Additionally, the clients no longer have to hard code the URI structures for different resources. This allows the server to make URI changes as the API evolves without breaking the clients.

Here, the consuming clients can use the rel value to identify and navigate to the related resources. As long as the rel value doesn’t change, the server can release new versions of the URI without breaking the client. It also makes it easy for consuming developers to explore the API without relying on heavy documentation.

. the same applies to many public/open-source reSt apIs being consumed today. In 2008,  
roy Fielding expressed frustration in his blog (http://roy.gbiv.com/untangled/2008/rest-apismust-be-hypertext-driven) at such apIs being called reStful but that are not hypermedia-driven:  
*“What needs to be done to make the REST architectural style clear on the notion that*  
*hypertext is a constraint? In other words, if the engine of application state (and hence the*  
*API) is not being driven by hypertext, then it cannot be RESTful and cannot be a REST API.*  
*Period. Is there some broken manual somewhere that needs to be fixed?”*