Build a Web Application with Node, Express and MongoDB - From Scratch to Production

A Comprehensive Introduction

Kevin De Notariis

Contents

1 Introduction **3**
1.1 Requirements . . . 3
1.2 Tools . . . 3

2 First Steps **3**
2.1 Initialize Node . . . 3
2.2 Add main dependencies . . . 4
2.3 Create and start the server . . . 4

3 Adding Routes **5**
3.1 `app.use()` . . . 5
3.2 `app.get()` . . . 6

4 More Structure to the Project **8**
4.1 Moving user route into it's own folder . . . 8

5 Render an HTML Page **9**
5.1 Further Step - Pass parameters from routes to views. . . . 11

6 Creating a Layout for our Webpages **12**
6.1 Home Page Creation . . . 13
6.1.1 Bootstrap in Express . . . 13
6.1.2 Serve Bootstrap's CSS and JS to HTML . . . 14
6.1.3 Footer . . . 15
6.1.4 Home Page Body . . . 16

7 Register And Login **20**
7.1 Setting up MongoDB and mongoose . . . 20
7.1.1 Create a Mongoose Schema . . . 20
7.2 User Controller . . . 22
7.2.1 loginRequired . . . 23
7.2.2 register . . . 23
7.2.3 login . . . 24
7.2.4 Set up JWT . . . 25
7.3 Register Route and Page . . . 26
7.4 Body-Parser . . . 27
7.5 Login Route and Page . . . 28
7.6 Serving the /login and /register routes . . . 29
7.7 Validate and Sanitize User Inputs . . . 29

8 Cookies and JWT **32**
8.1 JWT Authentication with Node.js . . . 32
8.2 Add Environment Variables to store secret keys . . . 33
8.3 Create the Refresh Token Model . . . 34
8.4 Login Improved . . . 35

8.5 Home Route and Page 39
8.6 loginRequired Middleware 41
8.7 Test the Project 43
8.8 Implementing the invalidation of a token 45
8.9 Logout 47

List of Tables

List of Figures

1 Introduction

In this course we will be building a simple website called *Handle your Training Sessions* in which most of the features involving the creation of a website will be explored, both *back-end* and *front-end*, using **Node.js**, **Express.js** and **MongoDB**.

1.1 Requirements

I'm going to assume that the reader is (somewhat) familiar with:

- Javascript (ES6) ;
- HTML ;
- JQuery ;
- npm .

1.2 Tools

I'm going to use VSCode as the editor for the tutorial, both because of its huge number of functionalities and its built-in terminals.

2 First Steps

2.1 Initialize Node

Create a folder and name it as you prefer, open the command prompt and navigate inside this folder and type:

```
code .
```

This will open VSCode inside this folder.

In order to start our project, first open the terminal integrated in VSCode and run the following command:

```
npm init
```

There will be asked some questions and we can answer them as we see fit, I will leave almost all of them blank, I'll just write `server.js` when asked about the `entry point` (the default would be `index.js`, but we will use `server.js` instead. note: this is completely arbitrary). I'll also write my name in the `author` entry.

This will create a **`package`**`.json` file in the root folder of the following form:

```
{
    "name": "test_1",
    "version": "1.0.0",
    "main": "server.js",
    "scripts": {
        "test": "echo \"Error: no test specified\" && exit 1"
    },
    "author": "kevin de notariis",
    "license": "ISC"
}
```

2.2 Add main dependencies

We now need to install `express` by typing in the terminal:

```
npm i express
```

This will create a `node_module` folder and a **`package`**`-lock.json`. The `node_module` folder will store all the installed modules, while the **`package`**`-lock.json` will be used by `npm` to check the correct versions and compatibilities of all the modules used.

2.3 Create and start the server

- In order to start a server, create a `server.js` file in the root directory.
- Open it and type:

  ```
  const express = require("express");
  ```

  this will simply import the express module and "store" it into a variable called `express`.
- Define the actual `app`, below the line just written, type:

  ```
  const app = express();
  ```
- Finally, to start the server, the `app` just needs to listen to a given port, and this can be done by employing the method `.listen(PORT, callback)` of `app`, taking the PORT number as first argument and a callaback function. E.g. :ù

  ```
  app.listen(3000, () => {
      console.log("Server listening to port 3000");
  });
  ```
- We can save the file and run the server by typing in the terminal:

```
node server
```

and we will see the following output in the terminal:

```
Server listening to port 3000
```

> **Note:** We can stop the server by hitting `Ctrl-C`.

At this point our root directory will have the following structure:

```
.
├── node_modules
│   └── ...
├── package-lock.json
├── package.json
└── server.js
```

3 Adding Routes

3.1 app.use()

Now that we have a server which will listen to the port `3000`, we can start to add some routes. The syntax is pretty straightforward, in `server.js`, before `app.listen` type:

```
app.use("/", (req, res) => {
    res.send("Hello World");
});
```

Now, if we start the server by typing `node server` and we open the browser and navigate to `http://localhost:3000/`, we will see a "Hello World" response onto the we page sent by our route.

> ***Note:***
>
> We can make use of the `scripts` entry in the **`package.json`** to run our server. Open **`package.json`** and substitute the following entry:
>
> ```
> "scripts": {
>             "test": "echo \"Error: no test specified\" && exit 1"
>         },
> ```
>
> with the following:
>
> ```
> "scripts": {
>             "start": "node server"
>         },
> ```
>
> Now, in the terminal, in order to start the server we will just type:
>
> ```
> npm start
> ```

3.2 app.get()

The middleware `.use` will match every path containing '/', namely every possible route (in fact, one can navigate to, for example, `http://localhost:3000/hello` and we will still get the "Hello world" response)

If we would like to match only the wanted route, we should use the HTTP verb `get` as follows:

```
app.get("/", (req, res) => {
    res.send("Hello World");
});
```

If we now try to go to `http://localhost:3000/hello` we will get a

```
Cannot GET /hello
```

response.

We can now add an arbitrary number of routes, namely we can add the following:

```
app.get("/user", (req, res) => {
    res.send("Hello user page");
});

app.get("/user/:id", (req, res) => {
    res.send(`Hello user with id: ${req.params.id}`);
});
```

If we restart the server, now we can navigate to `http://localhost:3000/user` and we will get the response:

```
Hello user page
```

we can also navigate to whatever route we want from user, examples would be

`http://localhost:3000/user/222`

`http://localhost:3000/user/333`

and as response we will get, respectively:

```
Hello user with id: 222
Hello user with id: 333
```

What we are employing here is a dynamic route. The parameter `id` in the route, can be accessed in `req.params` which stores the parameters in the request.

> ***Note:***
>
> Every time we change the server, we have to stop it and then re-run:
>
> ```
> npm start
> ```
>
> However, we can install a package which will allow us to make changes in the server files and upon saving the file, the server will restart automatically. This module is called `nodemon`, and we can type in the terminal:
>
> ```
> npm i nodemon -D
> ```

> where the `-D` means that we are saving this module under the development dependencies, which will not be carried over in the build. We also modify the `scripts` element in the **`package.json`** as follows:
>
> ```
> "scripts": {
>                 "start": "nodemon server"
>           },
> ```

If we now make some changes in the server file, i.e. we add a route `/hello` and we save the file, we will see the following prompt from `nodemon`:

```
[nodemon] restarting due to changes...
[nodemon] starting `node server.js`
Server listening to port 3000
```

and we will readly be able to navigate to the newly created route.

At this point, the file `server.js` should look like this:

```
const express = require("express");

const app = express();

app.get("/", (req, res) => {
    res.send("Hello World");
});

app.get("/user", (req, res) => {
    res.send("Hello user page");
});

app.get("/user/:id", (req, res) => {
    res.send(`Hello user with id: ${req.params.id}`);
});

app.listen(3000, () => {
    console.log(`Server listening to port 3000`);
});
```

while the **`package.json`** as follows:

```
{
    "name": "test_1",
    "version": "1.0.0",
    "main": "server.js",
    "scripts": {
        "start": "nodemon server"
    },
    "author": "kevin de notariis",
    "license": "ISC",
    "dependencies": {
        "express": "^4.17.1"
    },
    "devDependencies": {
        "nodemon": "^2.0.6"
    }
}
```

4 More Structure to the Project

It is good practice to not clutter the `server.js` file with all the routes of the application by moving them into their own folder and then use the built-in `Router` class to indeed create modular and mountable route handlers.

Let's then create a `routes` folder in the main directory and a `index.js` which will be the entry point. The folder structure will then look like this:

```
.├──
 _node_modules│└──
    ...├──
 _routes│└──
    index.js├──
 package-lock.json├──
 package.json└──
 server.js
```

Let's now open the `index.js` and write the following:

```
const express = require("express");
const router = express.Router();

module.exports = () => {
    router.get("/", (req, res) => {
        res.send("Hello World");
    });

    app.get("/user", (req, res) => {
        res.send("Hello user page");
    });

    app.get("/user/:id", (req, res) => {
        res.send(`Hello user with id: ${req.params.id}`);
    });

    return router;
};
```

We can now delete the routes in `server.js` and instead add the following:

```
...
const routes = require('./routes');
...
app.use('/', routes());
...
```

The server will run exactly as before, but we managed to decouple the routes with the actual server and we will be able to add more routes in a more structured way.

4.1 Moving user route into it's own folder

Now that we have a route folder, we can create another folder inside it called `user` and then create an `index.js` file inside it. The root folder structure should be as follows:

```
.├──
 _node_modules│└──
    ...├──
 _routes│├──
    _user│└──
      index.js│└──
    index.js├──
 package-lock.json├──
 package.json└──
 server.js
```

In `/routes/user/index.js` write:

```
const express = require("express");
const router = express.Router();

module.exports = () => {
    router.get("/", (req, res) => {
        res.send("Hello user");
    });

    router.get("/:id", (req, res) => {
        res.send(`Hello user with id: ${req.params.id}`);
    });

    return router;
};
```

while in the `/routes/index.js` just remove the routes for `/user` and `user/:id` and add:

```
...
const userRoute = require("./user");

module.exports = () => {
    ...
    router.use("/user", userRoute());

    return router;
}
```

Now everything should work as before, we can navigate to `http://localhost:3000/user` as before and to any other route in `/user`.

5 Render an HTML Page

Now that we have set-up some routes, we should consider rendering some actual HTML page. Since we want a dynamic website, namely dynamic webpages, we need to employ a **view engine.**

In this regard, we are going to use `ejs`, to see the documentation check the website https://ejs.co.

But how do we tell express to employ this view engine?

First, we need to install the `ejs` module:

```
npm i ejs
```

Once completed, we can open up the `server.js` file and add the following code:

```
const path = require("path");

app.set("view engine", "ejs");
app.set("views", path.join(__dirname, "./views"));
```

> ***Notes:***
>
> - In the first line we are requiring the node path module used in the last line;
> - The second line will tell express to consider `ejs` as the chosen view engine;
> - The third line instructs express to look for the views in the `./views` folder (in other words, when we will call `res.render()` in our routes, the root folder will be `./views/`), which will be in the root directory and that we are going to create and populate soon.

Our `server.js` will look like:

```
const express = require("express");
const routes = require("./routes");
const path = require("path");

const app = express();

app.set("view engine", "ejs");
app.set("views", path.join(__dirname, "./views"));

app.use("/", routes());

app.listen(3000, () => {
    console.log(`Server listening to port 3000`);
});
```

Let's now create the `views` folder in root directory and a `index.ejs` in it.

The root folder structure should now look like this:

```
.├──
 _node_modules│└──
    ...├──
 _routes│├──
    _user│└──
       index.js│└──
    index.js├──
 _views│└──
    index.ejs├──
 package-lock.json├──
 package.json└──
 server.js
```

Let's open now the `views/index.ejs` file and simply write the base HTML code below:

```
<!DOCTYPE html>
<html>
    <head>
        <title>Project Title</title>
    </head>

    <body>
```

```
        <header>
            <h1>Hello Home Page</h1>
        </header>
    </body>
</html>
```

Open up now the `routes/index.js` file and instead of the line

```
res.send("Hello World");
```

we are going to put the following code:

```
res.render("./");
```

And upon saving all the files and opening the browser at `http://localhost:3000`, we should see the rendered HTML page with "Hello Home Page".

5.1 Further Step - Pass parameters from routes to views.

If we want to render some dynamic parameters in `views/index.ejs`, we can pass them in an object as a second argument to the `res.render()` call in `routes/index.js` file. Let's open it and modify the line:

```
res.render("./");
```

to:

```
res.render("./", {
    pageTitle: "Home Page",
    header: "Home Page Header",
});
```

These parameters can be accessed in `views/index.ejs` by employing the `ejs` syntax, namely as follows

```
<%= pageTitle %>
<%= header %>
```

In particular, we can replace the hard-coded `title` and `h1` in `views/index.ejs` with the above lines, obtaining:

```
<!DOCTYPE html>
<html>
    <head>
        <title><%= pageTitle %></title>
    </head>

    <body>
        <header>
            <h1><%= header %></h1>
        </header>
    </body>
</html>
```

Unpon saving and refreshing the browser we should be able to see the changes.

6 Creating a Layout for our Webpages

In order to not repeat everytime the same HTML code, we can create a common layout and then define different ”components” (in a subdirectory called `pages`) which will be ”mounted” when needed.

In `views` let’s create a `layout` folder and move in there the `index.ejs` file. The structure should look like this:

```
.├──
 _node_modules│└──
    ...├──
 _routes│├──
    _user│└──
       index.js│└
    index.js├──
 _views│└──
    _layout│└──
        index.ejs├──
 package-lock.json├──
 package.json└──
 server.js
```

Also, change in the `routes/index.js` file the `.render()` method by taking into account the change of the `index.ejs`, but also the fact that we will dynamically pass to the layout index page the actual page that we would like to render, namely (we will also remove the ”header” key):

```
res.render("layout", {
    pageTitle: "Home Page",
    template: "index",
});
```

Now, open up `views/layout/index.ejs` and modify it as follows:

```
<!DOCTYPE html>
<html>
    <head>
        <title><%= pageTitle %></title>
    </head>

    <body>
        <header>
            <h1>Welcome to the <%= pageTitle %></h1>
        </header>

        <%- include(`../pages/${template}`) %>
    </body>
</html>
```

> With the `<%- include('../pages/${template}')%>` we are telling `ejs` to take everything in the file `../pages/${template}` and put it in there unescaped.

Create now the `pages` in `views` with a `index.ejs` file in there.

The folder structure should look like:

```
.├──
```

```
_node_modules└──
    ...├──
_routes├──
    _user└──
        index.js└──
    index.js├──
_views├──
    _layout└──
        index.ejs└──
    _pages└──
        index.ejs├──
package-lock.json├──
package.json└──
server.js
```

In `views/pages/index.ejs` let's write the following:

```
<div>
    <h2>h2 in there!</h2>
</div>
```

After saving the files we should see the new `h2` in the Home Page.

6.1 Home Page Creation

Now that we have a base structure for the project, let's add some HTML code to render a nice looking front home page. We are going to use `Bootstrap`, so let's install it.

6.1.1 Bootstrap in Express

```
npm i bootstrap
```

Bootstrap also uses `jquery` so we need to install it too:

```
npm i jquery
```

This will furnish us with lots of cool css and components to ease the front-end building process.

In for us to use the bootstrap `CSS` and components, we need to tell express where to find the static files. In this regard, let's create a **`public`** folder, and inside it a `styles` and a `js` folder. Inside **`public`**`/styles` create a `css` folder. The directory structure should look like:

```
.├──
_node_modules└──
    ...├──
_public├──
    _styles└──
        css└──
    js├──
_routes├──
    _user└──
        index.js└──
```

```
    index.js├──
 _views│├──
    _layout│└──
       index.ejs└──
    _pages└──
        index.ejs├──
 package-lock.json├──
 package.json└──
 server.js
```

In `server.js` let's add:

```
app.use(express.static(path.join(__dirname, "public")));
```

Since the `CSS` we will be using from bootstrap is in `node_modules/bootstrap/dist/css` and the `javascript` is in `node_modules/bootstrap/dist/js`, we need to tell express to consider these as if it were in the newly created **`public`** folder. We also need to tell express where to find `jquery`, so in `server.js` write:

```
app.use(
    "/styles/css",
    express.static(path.join(__dirname, "node_modules/bootstrap/dist/css")
        )
);

app.use(
    "/js",
    express.static(path.join(__dirname, "node_modules/bootstrap/dist/js"))
);

app.use(
    "/js",
    express.static(path.join(__dirname, "node_modules/jquery/dist"))
);
```

6.1.2 Serve Bootstrap's CSS and JS to HTML

Let's create `components` folder inside `layout` in which we will be storing the components commonly used by evey page, then create a `scripts.ejs` file inside it. The folder structure should now look like:

```
.├──
 _node_modules│└──
    ...├──
 _public│├──
    _styles│└──
       css│└──
    js├──
 _routes│├──
    _user│└──
       index.js└──
    index.js├──
 _views│├──
    _layout│├──
```

```
        _components|||└──
           scripts.ejs||└──
        index.js|└──
     _pages|└──
         index.ejs├──
  package-lock.json├──
  package.json└──
  server.js
```

In `scripts.ejs` add the following script tags:

```
<script language="javascript" src="/js/jquery.slim.min.js"></script>
<script language="javascript" src="/js/bootstrap.bundle.min.js"></script>
```

and then in `views/layout/index.ejs` we should serve this `scripts` file and add the `CSS` link. This `index.ejs` should then look like this:

```
<!DOCTYPE html>
<html>
    <head>
        <!-- Meta tags -->
        <meta charset="utf-8" />
        <meta
            name="viewport"
            content="width=device-width, initial-scale=1, shrink-to-fit=no
                "
        />

        <!-- Bootstrap CSS -->
        <link rel="stylesheet" href="/styles/css/bootstrap.min.css" />

        <title><%= pageTitle %></title>
    </head>

    <body>
        <header>
            <h1>Welcome to the <%= pageTitle %></h1>
        </header>

        <%- include(`../pages/${template}`) %>

        <%-include('./components/scripts') %>
    </body>
</html>
```

> ***Note:***
>
> We have added also some meta tags which are recommended by `bootstrap`. For more information visit https://getbootstrap.com/.

Everything should now be set correctly, and we should be able to proceed with the actual implementation of some HTML code using `bootstrap`.

6.1.3 Footer

Let's add a `footer.ejs` component in `views/layout/components`. Open it up and add the following code:

```
<footer class="container fixed-bottom">
    <div class="text-center py-3">
        <p class="footer-text">
            <strong>© 2020 Copyright: Kevin De Notariis</strong>
        </p>
    </div>
</footer>
```

where the class `.footer-text` will be defined in a `.css` file in a moment and the other classes are from bootstrap's `CSS`.

Create `style.css` in **`public`**`/styles/css` and put there the following code:

```
.footer-text {
    color: white;
}
```

At this point, the project structure should look like the following:

```
.├──
 _node_modules│└──
    ...├──
 _public│├──
    _styles│└──
       _css│└──
           style.css│└
    js├──
 _routes│├──
    _user│└──
       index.js│└
    index.js├──
 _views│├──
    _layout│├──
       _components│├──
          footer.ejs│└──
          scripts.ejs│└──
       index.js│└
    _pages│└
        index.ejs├──
 package-lock.json├──
 package.json└──
 server.js
```

6.1.4 Home Page Body

Let's now personalize the body of the front page.

> ***Note:***
>
> This course is not about neither HTML nor CSS, for that reason I'm not going to deeply explain how does the pure HTML and CSS code that I'll put in work.

This is the structure that we will create:

- A background image covering all the screen ;
- a jumbotron header with a welcoming message ;
- a button in center of the screen allowing user to login (or eventually sign in).

As the background image you might use a cool image taken from https://unsplash.com/s/photos/fitness. Download it and create a folder named `img` inside the **`public`** folder and put the image in there. I will call this image `front-image.jpg`.

Open up the `views/pages/index.ejs` and substitute it's content with the following:

```
<div class="homePage">
    <!-- Background Image -->
    <img src="/img/front-image.jpg" class="bg" />

    <!-- Jumbotron header with welcoming message -->
    <div class="jumbotron">
        <div class="col-md-6 px-0">
            <h1 class="display-4 font-italic">
                Welcome to <strong> <%= siteName %></strong>
            </h1>
            <p class="lead">
                A Website built for athletes and people which are
                   regularly
                exercising/going to the gym and would like to keep track
                   of
                their progresses
            </p>
        </div>
    </div>

    <!-- Login Button -->
    <div class="d-flex justify-content-center up-front">
        <a href="/login" class="brk-btn" href="#">Login </a>
    </div>

    <!-- Text below Login Button with link to register page -->
    <div class="d-flex justify-content-center up-front">
        <p style="color: white">
            Login in order to access your profile or
            <a class="underlined-a" href="/register">register here</a>
        </p>
    </div>
</div>
```

I've also added some comments explaining the different parts coded. The `CSS` classes that we have used here can be added in the **`public`**`/styles/css/style.css` and are the following (there is no need to understand how this work, I just post it there for completeness):

```
img.bg {
    min-height: 100%;
    min-width: 1024px;

    width: 100%;
    height: auto;

    position: fixed;
    top: 0;
    left: 0;
}
```

```
@media screen and (max-width: 1024px) {
    img.bg {
        left: 50%;
        margin-left: -512px;
    }
}

.up-front {
    position: relative;
    z-index: 2;
}

.underlined-a {
    text-decoration: none;
    color: white;
    padding-bottom: 0.15em;
    box-sizing: border-box;
    box-shadow: inset 0 -0.2em 0 white;
    transition: 0.2s;
}
.underlined-a:hover {
    color: #222;
    box-shadow: inset 0 -2em 0 white;
    transition: all 0.45s cubic-bezier(0.86, 0, 0.07, 1);
}

.brk-btn {
    position: relative;
    background: none;
    color: rgba(255, 255, 255, 0.356);
    text-transform: uppercase;
    text-decoration: none;
    border: 0.2em solid rgba(255, 255, 255, 0.356);
    padding: 0.8em 2em;
    font-size: 20px;
    transition: 0.3s;
}
.brk-btn:hover {
    color: white;
    border: 0.2em solid white;
    padding: 1em 2.4em;
    text-decoration: underline;
    font-size: 22px;
}

.brk-btn::before {
    content: "";
    display: block;
    position: absolute;
    width: 10%;
    background: #222;
    height: 0.3em;
    right: 20%;
    top: -0.21em;
    transform: skewX(-45deg);
    -webkit-transition: all 0.45s cubic-bezier(0.86, 0, 0.07, 1);
    transition: all 0.45s cubic-bezier(0.86, 0, 0.07, 1);
}
.brk-btn::after {
    content: "";
```

```
    display: block;
    position: absolute;
    width: 10%;
    background: #222;
    height: 0.3em;
    left: 20%;
    bottom: -0.25em;
    transform: skewX(45deg);
    -webkit-transition: all 0.45 cubic-bezier(0.86, 0, 0.07, 1);
    transition: all 0.45s cubic-bezier(0.86, 0, 0.07, 1);
}
.brk-btn:hover::before {
    right: 80%;
}
.brk-btn:hover::after {
    left: 80%;
}
```

Now, in `views/pages/index.ejs` we can see that we have added a line of the form:

```
Welcome to <strong> <%= siteName %></strong>
```

and we have to define the variable `siteName`. Since this will be a global variable shared by every page, we can define it in the `locals` property of our server. In `server.js` just add the following line before the `app.use("/", routes());` and we will be good to procede further:

```
app.locals.siteName = "* Web Site Name *";
```

> We can also change in `views/layout/index.ejs` the following line:
>
> ```
> <title><%= pageTitle %></title>
> ```
>
> with:
>
> ```
> <title><%= siteName %> | <%= pageTitle %></title>
> ```

At this point the structure of the project should look like the following:

```
.├──
 _node_modules│└──
    ...├──
 _public│├──
    _img│└──
       front-image.jpg│├──
    _styles│└──
       _css│└──
          style.css│└
    js├──
 _routes│├──
    _user│└──
       index.js│└
    index.js├──
 _views│├──
    _layout│├──
       _components│├──
          footer.ejs│└──
```

```
            scripts.ejs
        index.js
    _pages
        index.ejs
  package-lock.json
  package.json
  server.js
```

7 Register And Login

Since we have created a login button redirecting to `/login` and a register link redirecting to `/register`, we need to implement these routes and create the suitable pages, controllers and models for the Users. We will be using the **MVC design pattern** (Model - View - Controller) and we start here by incorporating MongoDB in our project.

7.1 Setting up MongoDB and mongoose

First, we need to install the `mongoose` module, which will bring with it the `mongodb` module itself, so let's type in the terminal:

```
npm i mongoose
```

Then open up the `server.js` file and import `mongoose`:

```
const mongoose = require("mongoose");
```

If you do not have mongoDB installed, you can go here https://www.mongodb.com and download it in you local machine and install it as a service, in this way it will be immediately ready to be used.

In `server.js` let's connect to mongoDB utilizing `mongoose`, namely write:

```
mongoose.connect("mongodb://localhost/trainingDB", {
    useNewUrlParser: true,
    useUnifiedTopology: true,
});
```

> - `trainingDB` will be the name of our database;
> - `useNewUrlParser` and `useUnifiedTopology` are two parameters that we need to set, otherwise mongoDB will complain about deprecation issues.

MongoDB does not have a predefined structure, the collections in a database (which can be compared to tables in a SQL-type database) are filled with documents which can have completely different structure. In order to have a predefined structure, mongoose allows us to define so-called *Schemas*.

7.1.1 Create a Mongoose Schema

Let's create a `models` folder in the root directory and then create a `models/userModel.js` file. The structure of the project should look like:

```
.├──
 _models│└──
    userModel.js├──
 _node_modules│└──
    ...├──
 _public│├──
    _img│└──
       front-image.jpg│├──
    _styles│└──
       _css│└──
          style.css│└─
    js├──
 _routes│├──
    _user│└──
       index.js│└─
    index.js├──
 _views│├──
    _layout│├──
       _components│├──
          footer.ejs│└──
          scripts.ejs│└──
       index.js│└──
    _pages│└──
        index.ejs├──
 package-lock.json├──
 package.json└──
 server.js
```

In this newly created file, let's import `mongoose` and `bcrypt`, the latter will be used to hash the password (install it via `npm i bcrypt`):

```
const mongoose = require("mongoose");
const bcrypt = require("bcrypt");
```

Now, we define the `Schema`:

```
const Schema = mongoose.Schema;

module.exports = UserSchema = new Schema({
    email: {
        type: String,
        required: true,
    },
    hashPassword: {
        type: String,
        required: true,
    },
    create_date: {
        type: Date,
        default: Date.now(),
    },
});
```

> We have defined an `email` field of type `String` which is required, a `hashPassword` field also of type `String` and required and a `create_date` which will store the date in which the user was created. Note that we are storing the password not as the user types it, but we store the *hashed password*, so that if someone gains access of our database, they couldn't use the hashed password to login.

Finally, we need to add a method to `UserSchema` which compares the actual password (which will be used by the user to login) with the hashed password stored in the database:

```
UserSchema.methods.comparePassword = (password, hashPassword) => {
    return bcrypt.compareSync(password, hashPassword);
};
```

Now that we have a schema, we can proceed to create a **userController** which will be used to handle the actions of the users.

7.2 User Controller

Create a folder `controllers` in the root directory and a `userController.js` inside it. The folder structure shoul look like this:

```
.├──
 _controllers│└──
    userController.js├──
 _models│└──
    userModel.js├──
 _node_modules│└──
    ...├──
 _public│├──
    _img│└──
       front-image.jpg│├──
    _styles│└──
       _css│└──
          style.css│└──
    js├──
 _routes│├──
    _user│└──
       index.js│└──
    index.js├──
 _views│├──
    _layout│├──
       _components│├──
          footer.ejs│└──
          scripts.ejs│└──
       index.js│└──
    _pages│└──
        index.ejs├──
 package-lock.json├──
 package.json└──
 server.js
```

In `controllers/userController.js` we will define the middlewares that are going to be used by a user in its interactions with the website. To be sure that the user is indeed logged in and authorized to make the requests, we will use **JWTs** (Json Web Tokens) and in node we have a module called `jsonwebtoken` which we install by typing:

```
npm i jsonwebtoken
```

Let's now open up `controllers/userController.js` and first import the needed modules:

```
const mongoose = require("mongoose");
const jwt = require("jsonwebtoken");
const bcrypt = require("bcrypt");

const { UserSchema } = require("../models/userModel");
```

Let's define now the model that we are using, note that (from https://mongoosejs.com/docs/models.html):

> "Mongoose automatically looks for the plural, lowercased version of your model name"

Namely, if we define a model called `User` (first argument of `mongoose.model()`), then mongoose will search for the collection named `users` in the database. Also keep in mind that an instance of a model is a document which will then be saved in the corresponding collection. Using this insight we write:

```
const User = mongoose.model("User", UserSchema);
```

Now we can start adding the middlewares `register`, `login` and a `loginRequired`. The latter will be used before every other middleware to ensure that the user is logged in before doing anything.

7.2.1 loginRequired

in our `userController.js` file let's add:

```
const loginRequired = (req, res, next) => {
    if (req.user) {
        next();
    } else {
        return res.status(401).json({ message: "Not Authorized" });
    }
};
```

> If there is a user we pass to the next middleware, while if the user is not logged in, we return an "unauthorized" error status.

7.2.2 register

Following the `loginRequired` function we add the `register`:

```
const register = (req, res, next) => {
    const newUser = new User(req.body);
    newUser.hashPassword = bcrypt.hashSync(req.body.password, 10);
    newUser.save((err, user) => {
```

```
        if (err) {
            return res.status(400).json({ message: err });
        } else {
            user.hashPassword = undefined;
            return res.json(user);
        }
    });
};
```

> ***Note:***
>
> - First we create an instance of the model, which is nothing but a document (for mongoDB) ;
> - Then we hash the password returned form the user input ;
> - We save the document ;
> - In the callback we check whether there is any error;
> - If no errors occurred, we remove the password from the user document, since we do not want to send back the password.
> - Finally we return the json with the data.

7.2.3 login

Finally we implement the `login` as follow:

```
const login = (req, res, next) => {
    User.findOne(
        {
            email: req.body.email,
        },
        (err, user) => {
            if (err) throw err;
            if (!user) {
                return res
                    .status(401)
                    .json({ message: "Authentication failed" });
            } else {
                if (
                    !user.comparePassword(req.body.password, user.
                       hashPassword)
                ) {
                    return res
                        .status(401)
                        .json({ message: "Authentication failed" });
                } else {
                    user.hashPassword = undefined;
                    return res.json({
                        token: jwt.sign(
                            {
                                email: user.email,
                                _id: user.id,
                            },
                            "QuantumElectroDynamcics4Real"
                        ),
                    });
                }
            }
        }
    );
```

```
};
```

So let's break up this middleware:

> - First we query the database for the existence of a document with `email` field equals to the email typed in by the user ;
> - In the callback we receive an error (if occurs) and the document we asked for (if exists). So here we immediatly check if an error occurred, and if so we throw an error ;
> - If no errors occurred, we check whether there is a user in the database with the given email and if not we return a `401` status with a message telling that the authentication failed ;
> - If a user with the given email exists, then we check whether the password inserted coincide upon hashing with the hashed password stored with the given email. If the passwords do not match, we return a status `401` again with the same message as before ;
> - If the passwords match, we first remove the hashed password from user (since we do not pass to the front-end passwords) and then we return a JWT with the signed in email and user id, with the encryption word "QuantumElectroDynamics4Real".

As for now, we are just returning a response with the JWT token just for testing purposes. Afterwards we will store it in an appropriate cookie session for security purposes.

Finally, let's export all these functions:

```
module.exports = {
    loginRequired,
    register,
    login,
};
```

7.2.4 Set up JWT

In `loginRequired` we have checked for a property of the `request` objecy, namely we checked for the existence of a `req.user`. We need then to define this property. In `server.js` first import `jsonwebtoken`:

```
const jwt = require("jsonwebtoken");
```

and then, before `app.user("/", routes())` , let's implement JWT:

```
app.use((req, res, next) => {
    if (
        req.headers &&
        req.headers.authorization &&
        req.headers.authorization.split(" ")[0] === "JWT"
    ) {
        jwt.verify(
            req.headers.authorization.split(" ")[1],
            "QuantumElectroDynamics4Real",
            (err, decode) => {
                if (err) res.user = undefined;
                req.user = decode;
                next();
            }
        );
```

```
    } else {
        req.user = undefined;
        next();
    }
});
```

Let's break this up:

> - We check whether the incoming message has an header and if this header has an authorization field with first element indeed equal to 'JWT' ;
> - If this is the case, we check for the other part of the header authorization, namely the token itself with the secret word defined before.
> - The result of `.verify` will be a decoded token if the secret word is valid and we will store it in `req.user`. If there is an error, `decode` will be undefined and we respond with a `res.user` undefined.
> - Finally if there is no header / authorization / JWT part, then it means that the user is not authenticated.

7.3 Register Route and Page

Let's first add the register route. Create a `register` folder inside `routes` and a `index.js` inside it. The folder structure should now look like this:

```
.├──
 _controllers│└──
    userController.js├──
 _models│└──
    userModel.js├──
 _node_modules│└──
    ...├──
 _public│├──
    _img│└──
       front-image.jpg│├──
    _styles│└──
       _css│└──
           style.css│└
    js├──
 _routes│├──
    _register│└──
       index.js│├──
    _user│└──
       index.js│└
    index.js├──
 _views│├──
    _layout│├──
       _components│├──
          footer.ejs│└──
          scripts.ejs│└──
       index.js│└──
    _pages│└──
        index.ejs├──
```

```
 package-lock.json
 package.json
 server.js
```

Inside the newly created `routes/register/index.js` add the following code:

```
const express = require("express");

const { register } = require("../../controllers/userController");

const router = express.Router();

module.exports = () => {
    router.get("/", (req, res) => {
        res.render("layout", {
            pageTitle: "Register",
            template: "register",
        });
    });

    router.post("/", register);
};
```

- We first import all the necesary modules, including our `register` created before ;
- We then define a `GET` middleware as we have done in `routes/index`, but we pass a different `template` and `pageTitle` (we are going to create the register view in a moment) ;
- Define a `POST` middleware and passing the `register` we created.

Now, in `views/pages` add a `register.ejs` file. Open it up and put in there the following code:

```
<form type="POST" action="/register">
    <label>email</label>
    <input type="text" name="email" placeholder="email" />
    <label>password</label>
    <input type="password" name="password" placeholder="email" />
    <input type="submit" value="Submit" />
</form>
```

This is just a simple form in order to test our code, in the future we are going to style it more.

Now, when in the homepage `http://localhost:3000` we click on `register here` we will be redirected to `/register` with the form just written.

7.4 Body-Parser

In order to interpret what a form is returning, express needs a middleware called `body-parser` and we can install it:

```
npm i body-parser
```

Then we require it in `server.js` :

```
const bodyParser = require("body-parser");
```

and add the following lines of code (just before the JWT middleware created before), one to parse `x-www-form-urlencoded` and one to parse JSON:

```
app.use(bodyParser.urlencoded({ extended: false }));
app.use(bodyParser.json());
```

7.5 Login Route and Page

Analogously to the register route and page, we create a `login` folder inside `routes` and a `index.js` file inside this folder. Also, create a `login.ejs` inside `views/pages`. At this point the folder structure should look like:

```
.├──
 _controllers│└──
    userController.js├──
 _models│└──
    userModel.js├──
 _node_modules│└──
    ...├──
 _public│├──
    _img│└──
       front-image.jpg│├──
    _styles│└──
       _css│└──
          style.css│└─
    js├──
 _routes│├──
    _login│└──
       index.js│├──
    _register│└──
       index.js│├──
    _user│└──
       index.js│└─
    index.js├──
 _views│├──
    _layout│├──
       _components│├──
          footer.ejs│└──
          scripts.ejs│└──
       index.js│└──
    _pages│├──
        index.ejs│├──
        login.ejs│└──
        register.ejs├──
 package-lock.json├──
 package.json└──
 server.js
```

In the same way as before, open up `routes/login/index.js` and put there the following code:

```
const express = require("express");
```

```
const { login } = require("../../controllers/userController");

const router = express.Router();

module.exports = () => {
    router.get("/", (req, res) => {
        res.render("layout", {
            pageTitle: "Login",
            template: "login",
        });
    });

    router.post("/", login);

    return router;
};
```

while in `views/pages/login.ejs`:

```
<form action="/login" method="POST">
    <label>email</label>
    <input type="text" name="email" placeholder="email" />
    <label>password</label>
    <input type="password" name="password" placeholder="password" />
    <input type="submit" value="Submit" />
</form>
```

7.6 Serving the /login and /register routes

If we now try to start the server and click on the login button or the register link, we will see that the server is not able to get these routes, why is that?

Every route we have defined is inside `/routes` and it passes through `routes/index.js`, meaning that we need to use there the newly defined routes.

Open up `routes/index.js` and require the following:

```
const registerRoute = require("./register");
const loginRoute = require("./login");
```

Now, before the `return router`, just add:

```
router.use("/register", registerRoute());
router.use("/login", loginRoute());
```

If we now try to nagivate to `/login` and `/register` we should see the forms created before.

7.7 Validate and Sanitize User Inputs

At `http://localhost/register` one can register to the website, the email, password (hashed) and the creation date will be stored in the database, in particular in `trainingDB` database and in the collection `users`. However, one can insert everything they want in the email, even a non-email and there is still no way for our website to detect this fact, it will store it in the database regardless of its form.

Also, in order to protect from injections, we need to sanitize the input, namely remove eventual html tags which may compromise our website.

First, install the node module `express-validator`:

```
npm i express-validator
```

then in `controllers/userController.js` import the needed middlewares / functions:

```
const { check, validationResult } = require('express-validator);
```

and then define:

```
const validateAndSanitize = [
    check("email").trim().isEmail().normalizeEmail().escape(),
    check("password").trim().isLength({ min: 8 }).escape(),
];
```

and in both `register` and `login` middlewares, at the beginning, add:

```
const errors = validationResult(req);
```

Then we need to check whether this `errors` is empty, so that immediately after the above line, add:

```
if (!errors.isEmpty()) {
    res.json({ message: errors.toArray() });
} else {
    .........
}
```

and in the **`else`** statement just move all the code that we have written before. The final `register` middleware should look like this:

```
const register = (req, res) => {
    const errors = validationResult(req);
    if (!errors.isEmpty()) {
        res.json({ message: errors.array() });
    } else {
        const newUser = new User(req.body);
        newUser.hashPassword = bcrypt.hashSync(req.body.password, 10);
        newUser.save((err, user) => {
            if (err) {
                return res.status(400).json({ message: err });
            } else {
                user.hashPassword = undefined;
                return res.json(user);
            }
        });
    }
};
```

Now, do the same for `login` and also remember to export it `validateAndSanitize`:

```
module.exports = {
    validateAndSanitize,
    loginRequired,
    register,
    login,
};
```

Now, in `routes/login/index.js` and `routes/register/index.js` we need to import from `controllers/userController.js` also this newly created `validateAndSanitize`. I'll take as an example `routes/register/index.js` but the same thing is be replicated analogously also for `routes/login/index.js`:

```
const {
    validateAndSanitize,
    register,
} = require("../../controllers/userController");
```

and in the `router.post` add it as follows:

```
router.post("/", validateAndSanitize, register);
```

Do the same for `routes/login/index.js` and now let's see how does the site respond to different inputs. Navigate to `http://localhost/register` and:

1. Write:

email	password
kevin	helloworld

   and after pressing the submit, we should see a message telling us that the email we have inserted in not valid:

```
{"message":[{"value":"kevin","msg":"Invalid value","param":"email","
   location":"body"}]}
```

2. Write:

email	password
kevin@example.com[1]	hello

   after pressing the submit, we should see a message telling us that the password is not valid (it has a length < 8 characters):

```
{"message":[{"value":"hello","msg":"Invalid value","param":"password"
   ,"location":"body"}]}
```

3. Write:

email	password
kevin	hello

   here, we should see both error messages:

[1] mailto:kevin@example.com

```
{"message":[{"value":"kevin","msg":"Invalid value","param":"email","
    location":"body"},{"value":"hello","msg":"Invalid value","param":"
    password","location":"body"}]}
```


4. Write:

email	password
kevin@example.com[2]	helloworld

   now, finally, we should see a message telling us that the user has been correctly created, so something of the following form:


```
{"created_date":"2020-10-30T17:08:05.895Z","_id":"5
    f9c4a5726b0dd2018df41d7","email":"kevin@example.com","__v":0}
```


If you now open up the shell, type `mongo` and then switch to the trainingDB, namely type

```
use trainingDB
```

now by querying the database to find all documents in the collection `users`:

```
db.users.find()
```

we should see the new element we have created.

If we now go to the login page `http://localhost:3000/login` and we type the email and password that we have used in the register page (the correct ones) then we should see a response with the token, namely something like this:


```
{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
    eyJlbWFpbCI6ImtldmluQGV4YW1wbGUuY29tIiwiX2lkIjoiNWY5YzRhNTcyNmIwZGQyMDE4ZGY0MWQ3Iiw
    .UOKCKo-bc8y4Il7pjzUUCQF1WS8y6obu1vXMvKF5jH4"}
```


8 Cookies and JWT

We have created the foundations of a register/login process and now we are going to refine these, implementing a way for the user to remain authenticated in one of the most possible secure way.

We will employ a *short-lived* **ACCESS_TOKEN** and a *long-lived* **REFRESH_TOKEN** and below I will try to explain why we will opt for this choice.

8.1 JWT Authentication with Node.js

There are several possible ways to handle the authentication of a user into a website, some more secure and some less secure.

If one wants to use JsonWebTokens (JWT), then once these are created, there must be a process of storing and then retrieving.

[2] mailto:kevin@example.com

Since storing them in *local storage* or *session storage* is more susceptible to XSS (cross-site scripting) attacks, we will store the **ACCESS_TOKEN** in a *Cookie* (since we will use HTTPOnly cookies). This token will have very short life time, this way if an attacker were to steal it, they could use it only for have a short period of time, minimizing the damages.

On the contrary, the **REFRESH_TOKEN** will have a long life time, will be stored in the database (assigned to the user and encrypted) and will be used to generate new **ACCESS_TOKENS** once these will be expired. Clearly if a hacker were to steal these REFRESH_TOKENS, then they could use them to generate the ACCESS_TOKENS, for this reason there must be suitable measures to protect the database and its access.

8.2 Add Environment Variables to store secret keys

As we have already said, JsonWebTokens require a secret key which is used to encrypt the data to be stored in the token. Let's create a `.env` file in the root directory where we are going to put two different secret keys, one for the ACCESS_TOKENS and one for the REFRESH_TOKENS. We are also going to store the different lifetimes of these tokens:

```
ACCESS_TOKEN_SECRET=fWFezBEMEdsFU3RzE95zRd5mt6axbVce
ACCESS_TOKEN_LIFE=120
REFRESH_TOKEN_SECRET=28TcXu8HGpvTFH9vh7QVr3qrff883xAj
REFRESH_TOKEN_LIFE=86400
```

> - In order to have the most possible secure keys, you can go the following site and get some random keys: https://keygen.io
> - The life time of the ACCESS_TOKEN is set to be `120` seconds, namely after 2 minutes the ACCESS_TOKEN will expire.
> - The life time for the REFRESH*TOKEN is, instead, of `86400` seconds which are 24 hours. After this interval of time, the user *must* log in again.

In order to use these variables, we need to install a module called `dotenv`:

```
npm i dotenv
```

and then import it in the `server.js` as follows:

```
require("dotenv").config();
```

We will be able to access these variables anywhere in the project by simply typing `process.env.ACCESS_TOKEN_LIFE` for example.

The folder structure should now be:

```
.├──
 _controllers│└──
    userController.js├──
 _models│└──
    userModel.js├──
 _node_modules│└──
    ...├──
 _public│├──
```

```
    _img
       front-image.jpg
    _styles
       _css
          style.css
    js
 _routes
    _login
       index.js
    _register
       index.js
    _user
       index.js
    index.js
 _views
    _layout
       _components
          footer.ejs
          scripts.ejs
       index.js
    _pages
        index.ejs
        login.ejs
        register.ejs
 .env
 package-lock.json
 package.json
 server.js
```

8.3 Create the Refresh Token Model

In `models` create a new file: `refreshTokenModel.js`, open it up and add the following:

```
const mongoose = require("mongoose");

const Schema = mongoose.Schema;

const RefreshTokenSchema = new Schema({
    user_id: {
        type: String,
        required: true,
    },
    encryptedRefreshToken: {
        type: String,
        require: true,
    },
    created_date: {
        type: Date,
        default: Date.now(),
    },
});

module.exports = RefreshTokenSchema;
```

> - The `user_id` will be used to retrieve the REFRESH_TOKEN for a given user ;
> - The `encryptedRefreshToken` will be created by making use of two functions which we are going to define in `controllers/userController.js`.

The root directory structure should now be as follows:

```
.
├── _controllers
│   └── userController.js
├── _models
│   ├── refreshTokenModel.js
│   └── userModel.js
├── _node_modules
│   └── ...
├── _public
│   ├── _img
│   │   └── front-image.jpg
│   ├── _styles
│   │   └── _css
│   │       └── style.css
│   └── js
├── _routes
│   ├── _login
│   │   └── index.js
│   ├── _register
│   │   └── index.js
│   ├── _user
│   │   └── index.js
│   └── index.js
├── _views
│   ├── _layout
│   │   ├── _components
│   │   │   ├── footer.ejs
│   │   │   └── scripts.ejs
│   │   └── index.js
│   └── _pages
│       ├── index.ejs
│       ├── login.ejs
│       └── register.ejs
├── .env
├── package-lock.json
├── package.json
└── server.js
```

8.4 Login Improved

Let's open up `controllers/userController.js` and first add the above mentioned encryption functions, so let's import the Node built-in module `crypto`:

```
const crypto = require("crypto");
```

and then:

```
const getEncryptedToken = (refreshToken, callback) => {
    crypto.scrypt(
        process.env.REFRESH_TOKEN_CYPHER,
        process.env.REFRESH_TOKEN_SALT,
        24,
        (err, key) => {
            crypto.randomFill(new Uint8Array(16), (err, iv) => {
                const cipher = crypto.createCipheriv("aes-192-cbc", key,
                   iv);
                callback(
                    iv +
                        " " +
                        cipher.update(refreshToken, "utf8", "hex") +
                        cipher.final("hex")
                );
            });
        }
    );
};

const getDecryptedToken = (encryptedRefreshToken, callback) => {
    crypto.scrypt(
        process.env.REFRESH_TOKEN_CYPHER,
        process.env.REFRESH_TOKEN_SALT,
        24,
        (err, key) => {
            let iv = new Uint8Array(
                encryptedRefreshToken.split(" ")[0].split(",")
            );
            const actualToken = encryptedRefreshToken.split(" ")[1];
            const decipher = crypto.createDecipheriv("aes-192-cbc", key,
               iv);
            callback(
                decipher.update(actualToken, "hex", "utf8") +
                    decipher.final("utf8")
            );
        }
    );
};
```

- The `getEncryptedToken` has been created by looking at the documentation of `crypto`, which can be found here https://nodejs.org/api/crypto.html#crypto_class_cipher. We encrypt the refresh token by using a password called REFRESH_TOKEN_CYPHER and a salt called REFRESH_TOKEN_SALT which we are goin to define in `.env`. Let's break down this method:
    1. First we call the `.scrypt` method of `crypto` which allows us to generate a key for the encryption. It uses a password and a salt ;
    2. Then we create a random `iv` (initialization vector) using `.randomFill` of `crypto` ;
    3. Afterwards we create a cypher object by invoking `.createCipheriv` which requires the algorithm (aes-192-cbc), the key and the iv.
    4. Finally we return a string in which we store the `iv` as first element then after a space the encrypted token using the methods of `crypto`. We need to store the `iv` since the decrpyt method will need it.

> - The `getDecryptedToken` works almost analogously with the difference that we do not generate the `iv` but we extract it from the encrypted token.
> - Since the `crypto` methods we are using are async, we pass a callback function to which will be called once the encrypting and decrypting has been completed.

Let's then define the new secret key and the salt in `.env`. Open this file and add the following lines:

```
REFRESH_TOKEN_CYPHER=9d4yvFcC17PIzAep
REFRESH_TOKEN_SALT=amsLIWB06DnG4w9i
```

Now, we need to import the refreshToken model we have created and create its schema. After

```
const User = mongoose.model("User", UserSchema);
```

just put:

```
const RefreshTokenSchema = require("../models/refreshTokenSchema");
```

and then after

```
const User = mongoose.model("User", UserSchema);
```

put:

```
const RefreshToken = mongoose.model("RefreshToken", RefreshTokenSchema);
```

Remove the following lines:

```
user.hashPassword = undefined;
return res.json({
    token: jwt.sign(
        {
            email: user.email,
            _id: user.id,
        },
        "QuantumElectroDynamics4Real"
    ),
});
```

And instead we are going to create the ACCESS_TOKEN and the REFRESH_TOKEN. Add then:

```
let payloadAccess = {
    _id: user.id,
    exp: Math.floor(Date.now() / 1000) + Number(process.env.
       ACCESS_TOKEN_LIFE),
};

let payloadRefresh = {
    _id: user.id,
    exp: Math.floor(Date.now() / 1000) + Number(process.env.
       REFRESH_TOKEN_LIFE),
};
```

> We are creating here the payloads of the JWTs, we pass the user id and the expiration date (we do not need to pass the user email to the front end), which is calculated from the current date (in epoch time) and by adding the seconds corresponding to the chosen life time for ACCESS_TOKENS and REFRESH_TOKENS.

Continuing:

```
let accessToken = jwt.sign(
    payloadAccess,
    process.env.ACCESS_TOKEN_SECRET,
    { algorithm: "HS256" }
);

let refreshToken = jwt.sign(
    payloadRefresh,
    process.env.REFRESH_TOKEN_SECRET,
    { algorithm: "HS256" }
);

getEncryptedToken(refreshToken, (encryptedRefreshToken) => {
    ...
}
```

In this way we have generated the two tokens using the `HS256` algorithm for encryption and the secret keys we have created in the `.env` file. Also, we have called the `getEncryptedToken` method, which will encrpyt the refresh token and then called the callback function.

Now in the callback we need to see whether there already exist a document in the `refreshTokens` collection associated with the given user. Let's then add in the callback:

```
RefreshToken.findOne({ user_id: user.id }, (err, tokenUser) => {
    if (err) {
        return res.status(400).json({ message: err });
    } else {
        if (!tokenUser) {
            let newToken = new RefreshToken({
                user_id: user.id,
            });
            newToken.encryptedRefreshToken = encryptedRefreshToken;
            newToken.save((err, token) => {
                if (err) {
                    return res.status(400).json({ message: err });
                } else {
                    console.log("Refresh token saved successfully");
                }
            });
        } else {
            RefreshToken.updateOne(
                { user_id: user.id },
                {
                    $set: {
                        encryptedRefreshToken: encryptedRefreshToken,
                    },
                },
                (err) => {
                    if (err)
                        return res.status(400).json({
                            message: err,
                        });

                    console.log("Refresh token updated successfully");
                }
            );
        }
    }
```

```
});
```

- First we query the database for the existence of the document with `user_id = user.id` in the `refreshTokens` collection and if any error occurs, we return a `401` status.
- Then we check whether there exists such queried document, if not, we create a new document `newToken` with the `user_id = user.id` and we set the field `encryptedRefreshToken`.
- We then save it while logging a message telling the success of the operation.
- If instead there already exists a document, we just update it, with the new encrypted `refreshToken`.

Now that the checks on the refresh tokens have been made, we can proceed to attach the JWT to a cookie and then redirect to the `/home` route (which we will soon create):

```
res.cookie("jwt", accessToken, {
    //secure: true,
    httpOnly: true,
});
res.redirect("/home");
```

- `httpOnly` will protect against XSS ;
- The secure flag should be omitted when testing on a HTTP (otherwise the cookie will not be sent).

In order to correctly parse cookies, we need to install `cookie-parser`:

```
npm i cookie-parser
```

and then in `server.js` add:

```
...

const cookieParser = require('cookie-parser');

...

app.use(cookieParser());
```

8.5 Home Route and Page

Let's add the `/home` route, which will be the page where users will be redirected after login.

Create a `home` folder in `routes` and then inside it create an `index.js` with the following code:

```
const express = require("express");

const router = express.Router();

module.exports = () => {
    router.get("/", (req, res) => {
        res.render("layout", {
            pageTitle: "Home",
            template: "home",
        });
```

```
    });

    return router;
};
```

in `routes/index.js` we need to serve this route, so let's import it:

```
const homeRoute = require("./home");
const { loginRequired } = require("../controllers/userControllers");
```

> ***Note:***
>
> we have also imported the `loginRequired` middleware, which will be called before the home route in order to check whether the user is indeed logged in.

and use it:

```
router.use("/home", loginRequired, homeRoute());
```

Let's also create the view: in `views/pages` create a `home.ejs` file and inside there just put the following simple text:

```
<h1>This is Home Page</h1>
```

At this point the project structure should look like as follows:

```
.├──
 _controllers│└──
    userController.js├──
 _models│├──
    refreshTokenModel.js│└──
    userModel.js├──
 _node_modules│└──
    ...├──
 _public│├──
    _img│└──
       front-image.jpg│├──
    _styles│└──
       _css│└──
           style.css│└─
    js├──
 _routes│├──
    _home│└──
       index.js│├──
    _login│└──
       index.js│├──
    _register│└──
       index.js│├──
    _user│└──
       index.js│└─
    index.js├──
 _views│├──
    _layout│├──
       _components│├──
          footer.ejs│└──
```

```
          scripts.ejs
       index.js
    _pages
        home.ejs
        index.ejs
        login.ejs
        register.ejs
 .env
 package-lock.json
 package.json
 server.js
```

8.6 loginRequired Middleware

Since we have changed the way we handle authorization, we need to change also the `loginRequired` middleware in `controllers/userController.js`. Before doing that, go to `server.js` and **delete** the following middleware (we do not need this anymore):

```
app.use((req, res, next) => {
    if (
        req.headers &&
        req.headers.authorization &&
        req.headers.authorization.split(" ")[0] === "JWT"
    ) {
        const token = jwt.verify(
            req.headers.authorization.split(" ")[1],
            "QuantumElectroDynamics4Real",
            (err, decode) => {
                if (err) res.user = undefined;
                req.user = decode;
                next();
            }
        );
    } else {
        req.user = undefined;
        next();
    }
});
```

Then, open up `controllers/userController.js` and let's start implementing the new `loginRequired`, namely first of all **delete** everything that was in this function.

Since we have sent the to the client a cookie with the JWT, we first access this token and check whether it exists or not:

```
let accessToken = req.cookie.jwt;

if (!accessToken) {
    return res.status(401).json({ message: "Not Authorized User" });
}
```

Then if it exists, we verify it with the `.verify` method to which we may pass the callback function where the method will return a possible error and the decoded payload of the token:

```
jwt.verify(accessToken, access.env.ACCESS_TOKEN_SECRET, (err, decode) => {
    if (!err) {
```

```
        console.log("user authorized");
        next();
    } else {
        console.log("- There is a problem in the Authentication");
        if (err.name !== "TokenExpiredError") {
            return res.status(401).json({ message: "Not Authorized User"
               });
        } else {
            ...
        }
    }
});
```

- If there are no errors we pass to the next middleware ;
- Then we check whether the token is expired, if the error we received was not the `TokenExpiredError` error, then it means that the token has been compromised in some way and it will be required another login for the user ;
- If the token is expired, then we are going to generate another one below.

In the **`else`** statement, write the following:

```
console.log("- Access token has expired");

let decodedPayload = jwt.decode(accessToken, process.env.
   ACCESS_TOKEN_SECRET);

console.log("- Checking if Refresh token is active");

RefreshToken.findOne(
    {
        user_id: decodedPayload._id,
    },
    (err, refreshTokenDocument) => {
        if (err) {
            return res.status(400).json({ message: err });
        } else if (!refreshTokenDocument) {
            console.log("No refresh token found");
            res.redirect("/login");
        } else {
            console.log("- Refresh token found, checking its validity");
            getDecryptedToken(
                refreshTokenDocument.encryptedRefreshToken,
                (decryptedRefreshToken) => {
                    jwt.verify(
                        decryptedRefreshToken,
                        process.env.REFRESH_TOKEN_SECRET,
                        (err, refreshPayloadDecoded) => {
                            if (err) {
                                console.log(
                                    "- Refresh token is not valid, maybe
                                       it is expired"
                                );
                                res.redirect("/login");
                            } else {
                                console.log(
                                    "- Valid refresh token found,
                                       generating new Access Token"
                                );
                                let newPayloadAccess = {
```

```
                                    _id: decodedPayload._id,
                                    exp:
                                        Math.floor(Date.now() / 1000) +
                                        Number(process.env.
                                            ACCESS_TOKEN_LIFE),
                                };
                                let newAccessToken = jwt.sign(
                                    newPayloadAccess,
                                    process.env.ACCESS_TOKEN_SECRET,
                                    {
                                        algorithm: "HS256",
                                    }
                                );
                                res.cookie("jwt", newAccessToken, {
                                    //secure: true,
                                    httpOnly: true,
                                });
                                console.log(
                                    "New Access Token generated and sent
                                        to the client"
                                );
                                next();
                            }
                        }
                    );
                }
            );
        }
    }
);
```

- First we decode the accessToken which is expired so that we can retrieve the user.
- Then we search in the database for a document in the `refreshTokens` collection which has the corresponding `user_id` , in case of an error we return a `400` status with the error in json format.
- If no errors occur, then we check if the document exists, if not we redirect to login page ;
- If the refresh token document exists, we decrypt the `encryptedRefreshToken` and in the callback we verify the validity of the token.
- If an error occurs, it might mean that the refresh token is expired so we redirect the user to the login page.
- If the refresh token is still valid and not expired, we create a new ACCESS_TOKEN, by defining a new payload and then signing in a new token.
- Finally we set the cookie and call the next middleware.

Note that we have also added some `console.log` and these will be used to track the actual flow of the program since are going to test the above implementations soon

8.7 Test the Project

At this point we should be able to test our project. Let's start the server with `npm start` and then open the browser to `http://locahost:3000`.

- Trying to navigate to: `http://locahost:3000/home` should result in a:

```
  {"message":"Not Authorized User"}
```

- Let's now go to `http://locahost:3000/register` and register a new user:

email	password
hello@world.com[3]	helloworld

  we can also check in the database the correct creation of the new user.

- Now navigate to `http://locahost:3000/login` and insert the newly created user. Upon posting the request, we should be redirected to `http://locahost:3000/home` and checking the console (in the editor), we should see the following lines:

```
- Checking Authorization
user authorized
```

- Wait at least 2 minutes, and then try to refresh the `http://locahost:3000/home` page. Now, since the ACCESS_TOKEN is expired, we should see the following lines in the console:

```
- Checking Authorization
- There is a problem in the Authentication
- Access token has expired
- Checking if Refresh token is active
- Refresh token found, checking its validity
- Valid refresh token found, generating new Access Token
New Access Token generated and sent to the client
```

- Go to the mongoDB shell and swtich to our database:

```
use trainingDB
```

  and then delete the document in the `refreshtokens` collection:

```
db.refreshtokens.remove({})
```

  Now, in the browser, open the developer tools (in chrome just right click and select `inspect`), then in `network` under `name` click `home` and then copy the string under `Request Headers` > `Cookie`.

  Navigate to `http://localhost:3000/login` and login again with the credetials created before. We should see in the console that a new refresh token has been created.

  Go to postman and make a `GET` request to `http://localhost:3000/home` by setting a header with `key`: `Cookie` and `value` the string copied just before. Now, this ACCESS_TOKEN was created before using the refresh token we just deleted, however, upon making this request, the server will respond with a new ACCESS_TOKEN.

  Why?

  This is because the server checks that the received ACCESS_TOKEN is valid, then it checks whether it is expired. If it is expired, then it just looks in the database to find a refresh token and if a refresh

[3] mailto:hello@world.com

token is found (and is not expired valid) then it will send back another ACCESS_TOKEN. This means that a given ACCESS_TOKEN (expired) can always be used to gain a new valid ACCESS_TOKEN, provided there is a REFRESH_TOKEN in the database. We would like to avoid this situation, since we have no way to invalidate a given token.

> In order to resolve this problem, we will attach to every ACCESS_TOKEN the corresponding REFRESH_TOKEN and upon validating the authorization, we will check whether the REFERSH_TOKEN in the payload of the ACCESS_TOKEN coincides with the REFERSH_TOKEN in the database. If these do not coincide we will redirect the user to the login page. In this way, we will have also a way to invalidate ACCESS_TOKEN, namely just deleting the REFRESH_TOKEN and creating a new one.

8.8 Implementing the invalidation of a token

Let's start by adding in the payload of ACCESS_TOKENs the corresponding REFRESH_TOKEN.

In `controllers/userController` scroll to the `login` middleware, and instead of:

```
let payloadAccess = {
    _id: user.id,
    exp: Math.floor(Date.now() / 1000) + Number(process.env.
       ACCESS_TOKEN_LIFE),
};

let payloadRefresh = {
    _id: user.id,
    exp: Math.floor(Date.now() / 1000) + Number(process.env.
       REFRESH_TOKEN_LIFE),
};

let accessToken = jwt.sign(
    payloadAccess,
    process.env.ACCESS_TOKEN_SECRET,
    { algorithm: "HS256" }
);

let refreshToken = jwt.sign(
    payloadRefresh,
    process.env.REFRESH_TOKEN_SECRET,
    { algorithm: "HS256" }
);
```

we are going to first create the REFRESH_TOKEN and then the ACCESS_TOKEN by putting the REFRESH_TOKEN in its payload:

```
let payloadAccess = {
    _id: user.id,
    refresh: encryptedRefreshToken,
    exp: Math.floor(Date.now() / 1000) + Number(process.env.
       ACCESS_TOKEN_LIFE),
};

let accessToken = jwt.sign(payloadAccess, process.env.ACCESS_TOKEN_SECRET,
    {
    algorithm: "HS256",
});
```

and then :

```
getEncryptedToken(refreshToken, (encryptedRefreshToken) => {
    let payloadAccess = {
        _id: user.id,
        refresh: encryptedRefreshToken,
        exp:
            Math.floor(Date.now() / 1000) +
            Number(process.env.ACCESS_TOKEN_LIFE),
    };

    let accessToken = jwt.sign(payloadAccess, process.env.
       ACCESS_TOKEN_SECRET, {
        algorithm: "HS256",
    });

    RefreshToken.findOne(
        ...
```

> Clearly we are setting the REFRESH_TOKEN in the ACCESS_TOKEN encrypted since we do not want to pass it to the front-end as it is.

Now, in `loginRequired` we need to check if the REFRESH_TOKEN in the ACCESS_TOKEN coincide with the REFRESH_TOKEN stored in the database.

Navigate to:

```
RefreshToken.findOne(
    {
        user_id: decodedPayload._id,
    },
    (err, refreshTokenDocument) => {
        if (err) {
            return res.status(400).json({ message: err });
        } else if (!refreshTokenDocument) {
            console.log("No refresh token found");
            return res.redirect("/login");
        } else {
            ...
```

then instead of the three dots we are going to put the following:

```
console.log("- Refresh Token Found");
console.log("- Checking if it coincide with the one in the access token");
if (refreshTokenDocument.encryptedRefreshToken !== decodedPayload.refresh)
    {
    console.log("Refresh tokens do not coincide, login again");
    return res.redirect("/login");
} else {
    console.log(
        "- Refresh tokens coincide, checking validity of refresh token"
    );
    getDecryptedToken(
        ...
```

Lastly, when we generate a new ACCESS_TOKEN from the REFRESH_TOKEN, we need to add in the payload the encrypted REFRESH_TOKEN. So after

```
console.log("- Valid refresh token found, generating new Access Token");
```

in the `newPayloadAccess` add the field:

```
refresh: refreshTokenDocument.encryptedRefreshToken,
```

And everything else is left the same.

8.9 Logout

Let's now implement an API which will allow the user to logout, with the effect of removing the `REFRESH_TOKEN` in the database, invalidating every ACCESS_TOKEN previously generated with it.

Let's create a folder `logout` inside `routes` and an `index.js` file inside it.

Open it up and put the following code:

```
const express = require("express");

const { logout } = require("../../controllers/userController");

const router = express.Router();

module.exports = () => {
    router.get("/", (req, res) => {
        res.render("layout", {
            pageTitle: "Logout",
            template: "logout",
        });
    });

    router.post("/", logout);

    return router;
};
```

We need to create the middleware `logout` in `controller/userController.js`, the page to render in `views/pages` and serve the route in `routes/index.js`.

Let's first create the page: in `views/pages` create a file `logout.ejs` and put in there the following code:

```
<form method="POST" action="/logout">
    <input type="submit" value="Logout" />
</form>
```

then open up `routes/index.js` and add:

```
const logoutRoute = require("./logout");
```

and before `return router` just put:

```
router.use("/logout", loginRequired, logoutRoute());
```

> Clearly the user must be logged in before logout.

Finally in `controllers/userController.js` add the middleware:

```
const logout = (req, res) => {
```

```
    let accessToken = req.cookies.jwt;

    console.log("- Logging out... verifying access token");
    jwt.verify(accessToken, process.env.ACCESS_TOKEN_SECRET, (err, decode)
        => {
        if (err)
            return res.status(401).json({ message: "User not Authenticated
               " });

        console.log("- Access token verified, removing refresh token from
           DB");
        RefreshToken.deleteOne({ user_id: decode._id }, (err) => {
            if (err) return res.status(400).json({ message: err });

            console.log("- Refresh Token removed successfully");
            console.log("- Removing associated cookie");
            res.cookie("jwt", { maxAge: 0 });
            return res.redirect("/");
        });
    });
};
```

> - First we verify the ACCESS_TOKEN, but since this middleware comes after `loginRequired`, it should never pop an error here ;
> - Then we delete the REFRESH_TOKEN in the database and also we delete the cookie carrying the ACCESS_TOKEN.

At this point the folder structure should look like the following:

```
.├──
 _controllers│└──
    userController.js├──
 _models│├──
    refreshTokenModel.js│└──
    userModel.js├──
 _node_modules│└──
    ...├──
 _public│├──
    _img│└──
       front-image.jpg│├──
    _styles│└──
       _css│└──
           style.css│└─
    js├──
 _routes│├──
    _home│└──
       index.js│├──
    _login│└──
       index.js│├──
    _logout│└──
       index.js│├──
    _register│└──
       index.js│├──
    _user│└──
       index.js│└─
```

```
    index.js├──
  _views│├──
    _layout│├──
       _components│├──
          footer.ejs│└──
          scripts.ejs└──
       index.js└──
    _pages├──
        home.ejs├──
        index.ejs├──
        login.ejs├──
        logout.ejs└──
        register.ejs├──
  .env├──
  package-lock.json├──
  package.json└──
  server.js
```