**Use case story for the Authorization and Authentication:**

**Register flow:**

At first any user is treated as the Guest. When he/she explores the website then they will be directed to the login page/register page. If they got already account then they can login in and if not then they are redirected to the Register page.

At first user must fill all of the form including Full Name, email, address, phone number, password, confirm password and specially Role, profile image. The frontend and backend both will verify if the inputted data is validated or not. If the data provided is valid then server will generate the activation token with expiry time and sent to the email address the customer they provided.

If there is file such as image then first it will make path for that image to the local storage with multer and fs will make the new path for the file. The file will save to the CDN as third-party website such as cloundinary which will optimize and manipulate the file.

During this time server will save user data to data base by making the status inactive and this time the password must be encrypted and the image will save as the link that is provided by cloudinary. The database such as pgadmin will save the data in the format of the JSON.

User will get the link with the activation token to their email address. When they click to the link then server will start all the activation process. During this time the user provided activation token and data base activation token will be matched and if that time matched then the status will be update to active and response to the user as the register successful. If not then the response to user by message as “activation token does not match or is expired”

**Login**:

User must provide email and password by the login form. First the both backend and frontend will validate that form. If the data provided is valid then backend/ server will find out the user information from the data base with the help of email. If the email will be matched to the database then server will match again the password with database. During this time, password form the database will be decrypted and compare the password, if all of them matched then user is directed to the panel as per as their role base and if not, then server will response by message “email and password does not match”. This process include the status active from the inactive after matching all credentials and start generating the JsonwebToken. This token will save in the local storage for the few times by the client side. As this will store the ID for the User which will take during the Rest API call and response to the user as per as the user ID basis for the access to the server.

Admin can login in admin panel, seller can access the authorized protion of the website and customer are for the customer portal.

**Update Profile**

**Admin**: Admins can update their profile details such as name, email, and contact information. This typically happens through a dedicated admin dashboard. Admins may also be able to update their profile picture and notification preferences. Any changes are validated and saved, often requiring re-authentication as by sending email verification, for sensitive updates.

**Seller**: Sellers access their profile via a seller dashboard. They can update store-related information (store name, business address), personal details, and contact info. Also require seller verification for major changes, especially those affecting store identity or payment details.

**Customer**: Customers can update their personal information, shipping addresses, and contact details from their account settings. Need immediate updates, but for sensitive changes (like email), a confirmation step (such as email verification) may be required.

**Update Password**

**Admin**: Admins can change their password from the security section of their dashboard. The process typically requires entering the current password and the new password (with confirmation). For security, the platform may log out all sessions or require re-authentication after a password change.

**Seller**: Sellers follow a similar flow—entering the old password, then the new one. Some systems may send an alert or require two-factor authentication to confirm the change, especially if the account manages financial transactions.

**Customer**: Customers can update their password from their profile or security settings. They must provide their current password and the new password. After a successful change, the system may send a notification email and log out sessions on other devices for security.

**Logout**

**Admin**: Logging out ends the admin session and invalidates the authentication token, ensuring no unauthorized access. This is especially important for admin accounts due to elevated privileges.

**Seller**: Sellers log out from their dashboard, which ends their session and clears any session tokens or cookies. This is crucial if using shared or public devices.

**Customer**: Customers can log out from any device, which ends their session and clears authentication data. This protects their account, especially on shared computers.

**Forget Password**

**Admin**: If an admin forgets their password, they initiate a password reset by entering their registered email. The system sends a secure reset link to the email.

**Seller**: Sellers use the “Forgot Password” link, enter their email, and receive a reset link or code. Some platforms may require answering security questions or additional verification for sellers due to the financial implications.

**Customer**: Customers initiate the process by providing their email. They receive a reset link or code to their email or phone. The system guides them through the steps to set a new password.

**Reset Password**

**Admin**: After receiving the reset link or OTP, the admin accesses a secure page to enter and confirm a new password. Once reset, all active sessions may be logged out, and a notification is sent for security.

**Seller**: Sellers follow the reset link or enter the OTP, then set a new password. The system may prompt for additional verification, and a confirmation email is sent upon success.

**Customer**: Customers use the reset link/code to set a new password. After resetting, they can log in with the new password. The system may notify the user of the change and log out all other sessions for added security.

**Actor for the website:**

**1.Admin**

**2. Seller**

**3. Customer**

Role and their authorities:

At first any of the Users who visited the website treated as the guest unless they are assign in any role. They can just to see the normal landing page, all the products, categories, specials, promotions, sale items. Also if they want to register then they can go to register page to register the new user. As the role may be the admin, seller or customer. If they are just the customer then then they can choose the items, fill to the cart and to checkout they must create the user account or the customer account.

**1. User Management**

* **User Registration:** Customers and shop owners can register an account.
* **Email verification:** Must be send the time of registration and forget password, reset password time.
* **User Login/Logout:** Users can securely log in and log out of the system.
* **User Profile Management:** Customers can view and update their personal and payment information.
* **User Role Management:** System supports roles such as Admin, Seller (Shop Owner), and Customer.
* **User Listing (Admin Only):** Administrators can view a list of all registered users.

**2. Product Management**

* **Product Creation:** Admins and sellers can add new products with images and details.
* **Product Listing:** Users can view lists of products; sellers and admins can view all products.
* **Product Detail View:** Users can view detailed information for each product, including images.
* **Product Update:** Admins and sellers can update product information and images.
* **Product Deletion:** Admins and sellers can delete products.
* **Product Search and Filtering:** Users can search and filter products by category, brand, price, etc. (implied by e-commerce best practices and your code’s public product listing endpoints).

**3. Category Management**

* **Category Creation:** Admins can create new product categories.
* **Category Listing:** Users can view lists of categories; admins can view all categories.
* **Category Detail View:** Users can view details and products under each category.
* **Category Update:** Admins can update category information and images.
* **Category Deletion:** Admins can delete categories.

**4. Cart Management**

* **Add to Cart:** Customers can add products to their shopping cart.
* **View Cart:** Customers can view the contents of their cart.
* **Remove from Cart:** Customers can remove items from their cart.
* **Cart Quantity Update:** Customers can change the quantity of items in the cart (implied by typical e-commerce behavior).

**5. Order and Checkout Management**

**Checkout Process:** Customers can proceed to checkout from their cart.

* **Order Placement:** Customers can place orders, which are stored with relevant details.
* **Order Listing:** Customers can view their order history.
* **Order Detail View:** Customers can view details of each order.
* **Order Status Management:** System supports order statuses such as pending, processing, shipped, delivered, canceled (implied by typical e-commerce behavior).
* **Payment Integration:** Multiple payment options are available at checkout (implied by your code’s transaction and payment references).

**6. Authentication and Authorization**

* **Authentication:** All sensitive actions require user login.
* **Role-Based Access Control:** Different roles (Admin, Seller, Customer) have different permissions for actions and data access.

**7. Public and Guest Access**

* **Public Product Listing:** Guests can browse and view product and category listings.
* **Public Product Detail View:** Guests can view detailed product information.
* **Registration Requirement:** Guests must register to add to cart, checkout, or place orders (implied by your login checks on cart and order endpoints)[2](https://elogic.co/blog/functional-and-non-functional-requirements-for-ecommerce-websites/)[4](https://www.scribd.com/document/649078086/Functional-and-Non-Functional-requirements-of-online-Shopping-platform).

**8. Image and Media Management**

* **Product Image Upload:** Admins and sellers can upload images for products and categories.
* **Image Display:** Users can view product and category images on the website[6](https://www.linkedin.com/advice/1/what-some-examples-functional-requirements-e-commerce).

**9. Data Validation**

* **Input Validation:** All user inputs (product, category, cart, order) are validated before processing.