Software Documentation for API Endpoints and User Roles

Overview

This documentation outlines the available API endpoints and their functionalities within the system. The system has two primary types of users: **Admin** and **Ordinary Users**. The endpoints are designed to cater to the needs of these users, with specific roles and permissions associated with each.

---

1. User Roles and Permissions

1.1. Admin Users

Admin users have the highest level of privileges within the system. They are responsible for managing other users and roles, accessing all available data, and performing actions that could affect the overall system's operation. The following are the key permissions and responsibilities of Admin users:

- **User Management:** Admins can create, update, delete, and retrieve details of any user in the system.
- **Role Management:** Admins can create, update, delete, and retrieve details of roles.
- **Data Access:** Admins have full access to all data endpoints, including those related to sensitive data like AB Testing results and API request logs.
- **Authorization:** Admins can verify other users' roles and ensure that access to certain endpoints is restricted based on user roles.

1.2. Ordinary Users

Ordinary users have limited access to the system's functionalities. Their primary role is to interact with non-sensitive data and perform operations that do not affect the system's overall state. The following are the key permissions and responsibilities of Ordinary users:

- **Self-Management:** Ordinary users can access and update their own user information.
- **Prediction and Data Access:** Ordinary users can perform predictions and access specific data sets allowed by the system.
- **Limited Access:** Ordinary users cannot access or modify other users' data or roles. They are also restricted from accessing sensitive data endpoints.

---

2. API Endpoints

The system's API is organized into several key areas, each representing a set of functionalities. Below is a summary of the available endpoints categorized by their purpose and user roles.

2.1. Authentication Endpoints

- **Login for Access Token**

    - **Endpoint:** `/token`
    - **Method:** `POST`
    - **Description:** Authenticates a user and provides a JWT token for subsequent API calls.
    - **Access:** All users
- **Signup**
    - **Endpoint:** `/signup/`
    - **Method:** `POST`
    - **Description:** Allows a new user to sign up by providing a username, password, and email.
    - **Access:** All users

2.2. User Management (Admin Only)

- **Retrieve All Users**
    - **Endpoint:** `/users/`
    - **Method:** `GET`
    - **Description:** Retrieves a list of all users in the system.
    - **Access:** Admin only
- **Retrieve Specific User**
    - **Endpoint:** `/users/{user_id}`
    - **Method:** `GET`
    - **Description:** Retrieves details of a specific user by user ID.
    - **Access:** Admin only
- **Update User**
    - **Endpoint:** `/users/{user_id}`
    - **Method:** `PUT`
    - **Description:** Updates the details of a specific user.
    - **Access:** Admin only
- **Delete User**
    - **Endpoint:** `/users/{user_id}`
    - **Method:** `DELETE`
    - **Description:** Deletes a specific user from the system.
    - **Access:** Admin only

2.3. Role Management (Admin Only)

- **List Roles**
    - **Endpoint:** `/roles/list/`
    - **Method:** `GET`
    - **Description:** Retrieves a list of all roles within the system.
    - **Access:** Admin only
- **Create Role**
    - **Endpoint:** `/roles/`

    - **Method:** `POST`
    - **Description:** Creates a new role.
    - **Access:** Admin only
- **Retrieve Specific Role**
    - **Endpoint:** `/roles/{role_id}`
    - **Method:** `GET`
    - **Description:** Retrieves details of a specific role by role ID.
    - **Access:** Admin only
- **Update Role**
    - **Endpoint:** `/roles/{role_id}`
    - **Method:** `PUT`
    - **Description:** Updates the details of a specific role.
    - **Access:** Admin only
- **Delete Role**
    - **Endpoint:** `/roles/{role_id}`
    - **Method:** `DELETE`
    - **Description:** Deletes a specific role from the system.
    - **Access:** Admin only

2.4. AB Testing Management (Admin Only)

- **Create AB Testing Result**
    - **Endpoint:** `/ab_testing_results/`
    - **Method:** `POST`
    - **Description:** Creates a new AB Testing result.
    - **Access:** Admin only
- **List AB Testing Results**
    - **Endpoint:** `/ab_testing_results/`
    - **Method:** `GET`
    - **Description:** Retrieves a list of all AB Testing results.
    - **Access:** Admin only
- **Retrieve Specific AB Testing Result**
    - **Endpoint:** `/ab_testing_results/{test_id}`
    - **Method:** `GET`
    - **Description:** Retrieves details of a specific AB Testing result by test ID.
    - **Access:** Admin only
- **Delete AB Testing Result**
    - **Endpoint:** `/ab_testing_results/{test_id}`
    - **Method:** `DELETE`
    - **Description:** Deletes a specific AB Testing result from the system.
    - **Access:** Admin only

2.5. API Request Logs

- **Create API Request Log**
    - **Endpoint:** `/api_request_logs/`
    - **Method:** `POST`
    - **Description:** Logs a new API request.
    - **Access:** Typically internal, available to all users
- **List API Request Logs (Admin Only)**
    - **Endpoint:** `/api_request_logs/`
    - **Method:** `GET`
    - **Description:** Retrieves a list of all API request logs.
    - **Access:** Admin only
- **List User's API Request Logs**
    - **Endpoint:** `/api_request_logs/me`
    - **Method:** `GET`
    - **Description:** Retrieves a list of the current user's API request logs.
    - **Access:** Ordinary users
- **Retrieve Specific API Request Log**
    - **Endpoint:** `/api_request_logs/{request_id}`
    - **Method:** `GET`
    - **Description:** Retrieves details of a specific API request log by request ID.
    - **Access:** Ordinary users for their own logs, Admin for all logs