Authentication Requirements

User Registration

- Users must register by providing a name, email, and password.
- The name must be at least 3 characters long.
- The email must follow a valid format and be unique in the system.
- The password must be at least 5 characters long.
- The password must be hashed using bcrypt before storing in the database.
- If an existing user attempts to register with the same email, return an error.
- On successful registration, return a JWT token for authentication.

User Login

- Users must log in using a registered email and password.
- The system must validate that both fields are present and properly formatted.
- If credentials are valid, return a JWT token for session handling.
- If credentials are invalid, return an appropriate error message without revealing which part was incorrect.
- Rate-limiting or throttling should be considered to prevent brute-force attacks (optional enhancement).

Fetching Authenticated User

- Provide an endpoint to fetch the currently logged-in user's profile.
- The endpoint must require a valid JWT token.
- User's password should never be sent in the response.
- Middleware should decode the token and attach the user info to the request object.

CRUD Operations Requirements

Creating Notes

- Users must be able to create notes with a title, description, and tag.
- Title must be at least 3 characters long.
- Description must be at least 5 characters long.
- Tag must be at least 3 characters long.
- Each note must be associated with the logged-in user.
- Return the saved note in the response.

Fetching Notes

- Users must be able to fetch all notes they have created.
- The request must be authenticated using a valid JWT token.
- Only notes belonging to the authenticated user must be returned.

Updating Notes

- Users must be able to update a note's title, description, or tag.
- Only fields that are provided should be updated.
- Only the owner of the note must be allowed to update it.
- Return the updated note in the response.

Deleting Notes

- Users must be able to delete a note.
- Only the owner of the note must be allowed to delete it.
- Return a success message along with the deleted note in the response.

Security and Access Control

- All note operations (create, read, update, delete) must be accessible only to authenticated users.
- Unauthorized access attempts must return appropriate error messages (401 or 403).

- Ensure notes are securely linked to users to prevent access by others.