PATRICIA PRACTICAL TEST

AUTHENTICATION USING RSA256 ALGORITHM IMPLEMENTED NODEJS, EXPRESS JS & MONGODB.

Creation of an authentication system with RSA encryption (that uses public & private key) and also create an extra protected POST route where only encrypted payload is sent which is then decrypted by the application. Make sure to write a documentation for your implementation - this should be as concise as possible.

FEATURES

1. Login
2. Register
3. My info (Protected POST route)

Login: This endpoint is used to authenticate users using their email address and password.

TYPE	POST
PARAMETERS	email, password
HEADER	Content-Type: application/json
ENDPOINT	localhost:3000/api/login

Register: This endpoint is used to create new users using their name, email address and password.

TYPE	POST
PARAMETERS	name, email, password
HEADER	Content-Type: application/json
ENDPOINT	localhost:3000/api/register

My info: This endpoint is a protected endpoint which requires Token and RSA key to decrypt and verify the payload sent. The authorization token will be supplied in the header when sending the request.

TYPE	POST
PARAMETERS	-
HEADER	Content-Type: application/json Authorization: Bearer {Token}
ENDPOINT	localhost:3000/api/myinfo

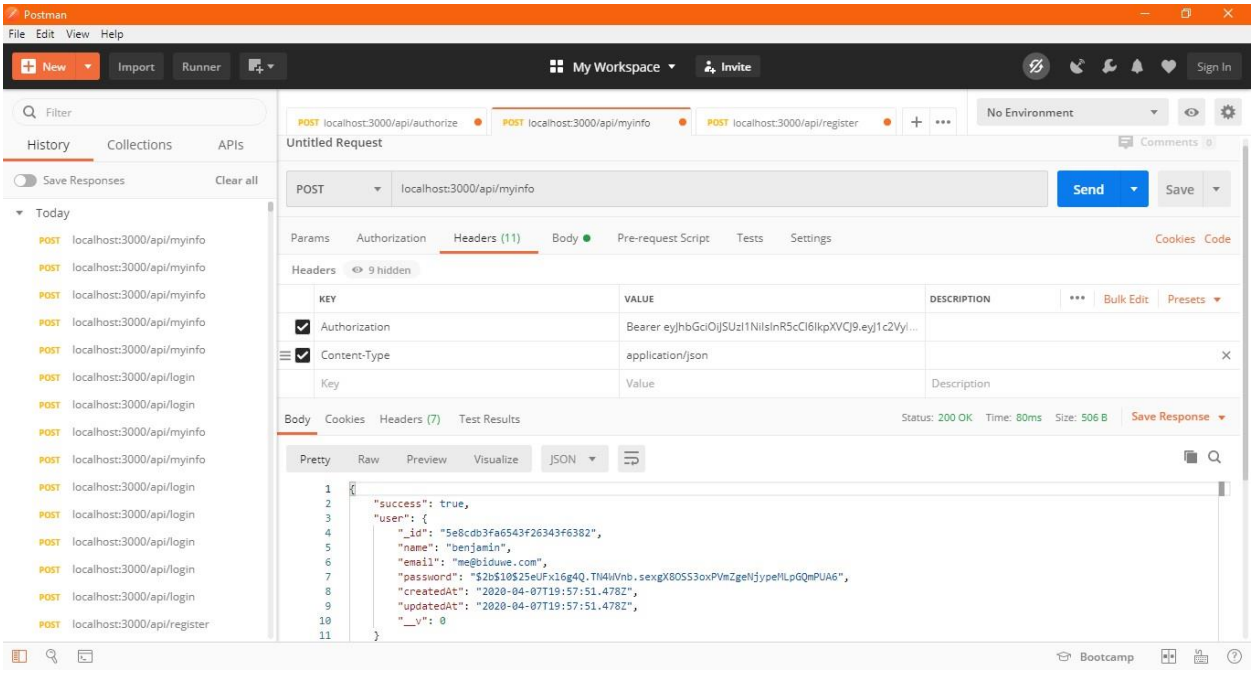

Fig. 1. Testing the endpoint with POSTMAN

FOLDERS STRUCTURE

1. **Config:** The config folder holds the configuration of the project such as Mongo DB connection url, project name etc.
2. **Controllers:** The controllers folder hold the auth controller which handles the request from the api route.

3. **Models:** The model folder holds only the user model, which is used to interact with the user collection. The user model holds the user schema and user methods.
4. **Routes:** The route folder holds two files:
   i. **api route:** The api.js file holds all the routes for the api defined earlier.
   ii. **middleware:** The middleware.js is used to verify the token sent and the token is being decrypted using JWT RC256 Algorithm.
5. **Index.js:** It is used for bootstrapping the Nodejs application.
6. **Public key:** The RSA public key is used for encryption.
7. **Private key:** The RSA private key is used for decryption.

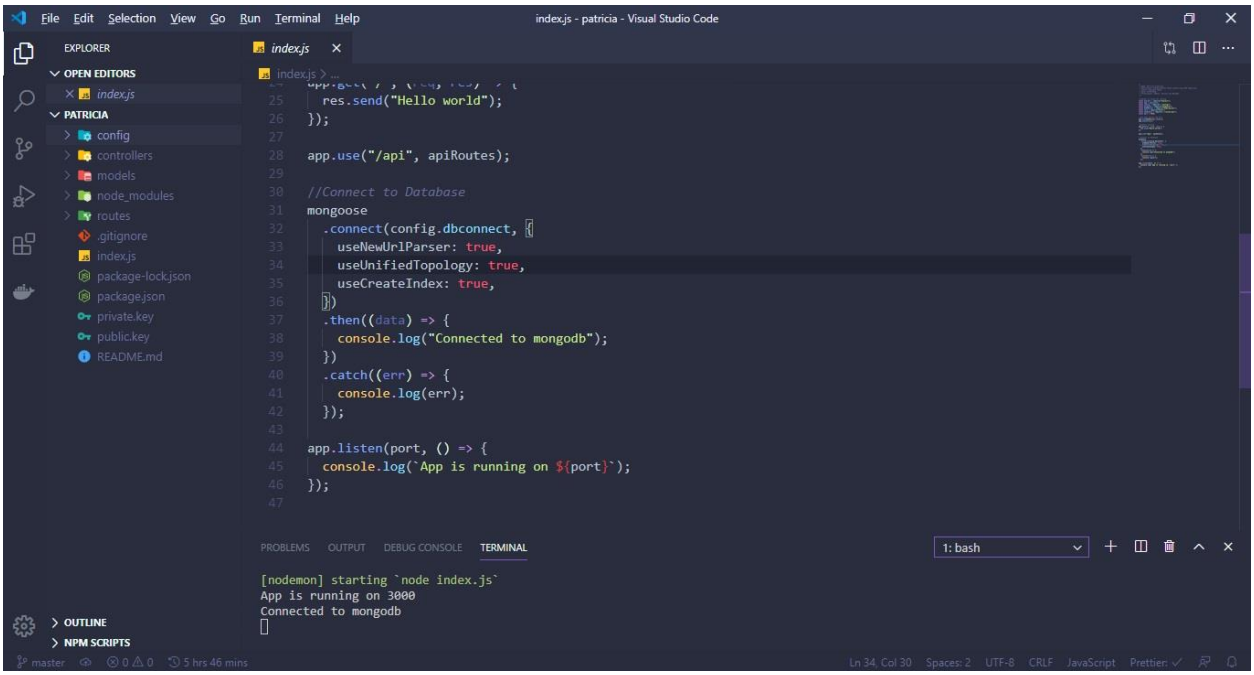

Fig. 2. Folder structure

PACKAGES USED

1. JWT
2. Express
3. Mongoose
4. Cors
5. Body-Parser
6. Bcrypt
7. Nodemon

HOW TO RUN APPLICATION

1. Clone Repository https://github.com/bencoderus/Nodejs-Authentication
2. Change directory to project directory using CLI
3. Run npm install.
4. Run npm start.