

Create multiple files and share everything with your team.

Sign Up Free

X

MERN-...

Read Only

Document

Both

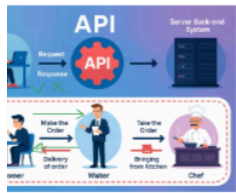
Canvas

Ctrl K

Sign in

Duplicate

Be a waiter



Best for Complex Queries

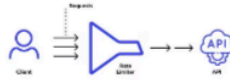
Good when you need relationships between data and orders and customers

Social media app
Bank

Best for Big Data & Real-Time Apps

Good for fast changing or huge amounts of data

RATE LIMITING



Rate limiting is a way to control how often someone can do something on a website or app like how many times they can refresh a page, make a request to an API, or try to log in.

Only 100 requests per user every 15 minutes

RATE LIMITING HELPS WITH

- Preventing abuse (e.g., stopping someone from making 1000 login attempts in a minute)
- Protecting servers from getting overwhelmed

429 Too Many Requests

MIDDLEWARE



Middleware is a function that runs in the middle between the request and the response.

CORS

(Cross-Origin 10% Share)

CORS is a browser security rule.

When a website tries to get data from another website—like your frontend calling an API on a different domain—the browser might block it for security reasons.

Example

You have a frontend at: `http://localhost:3000`
And an API backend at: `http://api.example.com`

Your frontend makes a fetch request to get data:
`fetch('http://api.example.com/users')`

But the browser says:

"You're coming from 'localhost:3000', and you're trying to get data from 'http://api.example.com/users'. That's a different origin. I need to make sure the API allows requests from you."

In short:
CORS error = "You tried to get data from another site, but the browser blocked it."
Fix = "You should tell the backend to allow requests from your frontend."

DEPLOYMENT



API TYPES

REST API

HTTP methods;

- Get some posts on Instagram
- Create a post
- Update a post
- Delete a post

HTTP STATUS CODES

200 OK

400 Bad Request

401 Unauthorized (e.g., after a POST request)

500 Internal Server Error