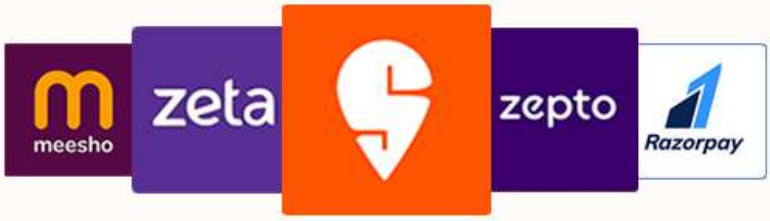
AccioJob

How would you protect an API from unauthorised access and overuse?

(asked in 8-15 LPA Roles in companies like)



CANDIDATE: "I'll just add an API key so only authorised people can access it." ❌

OR

"I'll use JWT tokens for authentication." ❌

SWIPE RIGHT FOR THE CORRECT APPROACH ⟶

[SWIPE RIGHT]

AccioJob

AUTH GATEWAY

GOAL: Verify only valid users get access
TECH: Spring Boot, Spring Security, JWT, OAuth2
EXAMPLE: In a banking app, users log in and get a JWT token.

Every API call checks if the token is still valid before allowing access.

02

[SWIPE RIGHT]

AccioJob

RATE LIMITER

GOAL: Prevent too many requests in short time
TECH: Bucket4j, Redis, Spring Cloud Gateway
EXAMPLE: A stock API allows 60 requests/minute.

If someone crosses that, their requests are throttled.

03

[SWIPE RIGHT]

AccioJob

API KEY VALIDATOR

Goal: Identify and manage external clients
Tech: Spring Interceptor, Database, Swagger (API key header)
Example: A weather API requires a valid API key from each client before responding.

If someone crosses that, their requests are throttled.

04

[SWIPE RIGHT]

AccioJob

AUDIT LOGGER

Goal: Track every API call for accountability
Tech: ELK Stack, Spring AOP, OpenTelemetry
Example: An e-commerce platform logs which user accessed which order and when.

If someone crosses that, their requests are throttled.

05

[SWIPE RIGHT]

AccioJob

RBAC & SCOPES

Goal: Ensure fine-grained access control
Tech: Spring Security, OAuth2 scopes, Keycloak
Example: In an HR system, employees can only view their own data, while admins can view all.

06

[SWIPE RIGHT]

AccioJob

CANDIDATE: So, protecting an API is more than about one tool — it's about combining layers of security:

- Authentication
- Rate Limiting
- API Keys
- Logging
- Role-based Access

Together, these prevent unauthorised access, overuse, and data misuse.

Follow AccioJob for more such Interview Question breakdown