**ST10355439**

**INSY7314**

**Research**

Rate limiting is a technique used to control how much traffic a system, network, or application receives over a specified period of time.

Rate limiting is critical for authentication endpoints because it limits the user’s password attempts for logging in, and in so doing, provides protection against brute force and credential stuffing attacks.

A per-IP limit involves limiting the number of requests that can be sent from a single IP address in a specified period and a per-identifier limit specifies a numeric threshold such as the maximum number of requests or connections allowed for the specific identifier (e.g., email) within a specified period.

When using a reverse proxy, the req.ip value in a node.js application may not be the same as the actual IP address of the client making the request, but instead, it may often be the same as the IP address of the reverse proxy itself. When a reverse proxy/load balancer faces issues when scaling across multiple instances, implementing rate limiting effectively becomes difficult.

Fail-safe defaults allow a system to remain operational or revert to a safe state if it fails to minimize the impact of system failures.