Introduction

During active use, user session management makes sure that users' interactions with the system are secure, authorized, and authenticated. By preventing unwanted access and minimizing interruptions for authorized users, proper session management strikes a balance between security and user experience.

Requirements for Session Management

1. Session Initiation

- Only after successful authentication (e.g., username/password, MFA) should user sessions be created.

- A distinct, securely generated session identifier (such as random tokens or JWTs with appropriate signing) is required for every session.

- Session tokens need to be unpredictable and impervious to replay attacks.

2. Session Duration & Expiry

- Idle Timeout: After a predetermined amount of inactivity, such as 15 to 30 minutes, sessions ought to automatically end.

- Absolute Timeout: Regardless of activity, sessions should end after a maximum predetermined amount of time (e.g., 8-12 hours).

- Renewal Policy: Following a timeout or session expiration, users might be asked to re-authenticate.

3. Concurrent Session Control

- Specify if each user is permitted to run multiple concurrent sessions. Choices:
    1. Restrictive: To avoid account sharing, each user may only have one active session.
    2. Permissive with Restrictions: Permit a maximum of three devices to be used concurrently.

- Give users the option to see and control active sessions (for example, "logged in from Chrome on Windows, Kathmandu, Nepal").

- Allow remote logout to end other running sessions.

4. Session Storage & Security

- Session tokens, such as HttpOnly and Secure cookies, should be safely stored.

- To stop CSRF attacks, enforce the SameSite cookie policy.

- Session IDs should not be stored in URLs.

- Encrypt critical session data while it's at rest and in transit (TLS).

5. Session Termination

- Sessions ought to be canceled right away after:
    1. The user logs out.
    2. Resetting your password or changing the security of your account.
    3. The session was terminated by the administrator.

- Make certain that session identifiers are completely erased and unusable.

6. User Experience Considerations

- Give users advance notice of an automatic timeout (e.g., "Your session will expire in 2 minutes").

- Provide a seamless "Remember Me" option (with more stringent guidelines for systems that are sensitive).

- Without sacrificing security, allow for smooth session continuity across reliable devices.

Security Considerations

- For session tokens, use robust cryptographic random values.
- Periodically rotate and refresh the tokens.
- Record any questionable session activity, such as logging in from a different device or location.
- To stop brute-force attacks, limit the rate at which sessions are created.

Expected Outcome

These specifications will be implemented by the system to guarantee:

- Secure session management and authentication.
- Preventing account abuse and session hijacking.
- Increased adherence to security guidelines and user trust.
- A harmony between robust security and seamless user experience.