**1. Cookie**  
**Ưu điểm:**

* Dễ triển khai và không cần lưu trữ trên máy chủ, giúp giảm tải cho server.
* Tự động gửi kèm theo mỗi request từ trình duyệt, thuận tiện cho việc duy trì trạng thái người dùng.
* Có thể lưu trữ các thông tin cá nhân như ngôn ngữ, giao diện người dùng, tùy chọn hiển thị,…

**Hạn chế:**

* Dung lượng lưu trữ hạn chế (thường chỉ khoảng 4KB cho mỗi cookie).
* Dễ bị sửa đổi hoặc tấn công bởi người dùng (ví dụ: tấn công CSRF, XSS).
* Tính bảo mật thấp nếu lưu trữ thông tin nhạy cảm.
* Người dùng có thể vô hiệu hóa cookie trên trình duyệt, gây ảnh hưởng đến trải nghiệm ứng dụng.

**2. Session**  
**Ưu điểm:**

* Lưu trữ dữ liệu trên máy chủ, an toàn hơn khi xử lý thông tin nhạy cảm như đăng nhập và giao dịch.
* Không bị giới hạn nghiêm ngặt về dung lượng lưu trữ như cookie.
* Thích hợp để quản lý trạng thái người dùng (ví dụ: giỏ hàng, thông tin phiên đăng nhập) trong suốt phiên làm việc.

**Hạn chế:**

* Tốn bộ nhớ máy chủ vì dữ liệu được lưu trữ trên server.
* Quản lý session phức tạp hơn, cần xử lý thời gian hết hạn và làm sạch dữ liệu.
* Khả năng mở rộng gặp khó khăn nếu số lượng người dùng tăng cao, đòi hỏi giải pháp cân bằng tải hoặc lưu trữ session ngoài (ví dụ: Redis).

**3. Ví dụ sử dụng trong ứng dụng Web thực tế**

* **Cookie:**
  + Lưu trữ tùy chọn ngôn ngữ hoặc giao diện của người dùng.
  + Chức năng "Remember me" để giữ thông tin đăng nhập.
  + Lưu trữ dữ liệu không nhạy cảm như các thiết lập cá nhân hay thông tin giỏ hàng (với dữ liệu không quan trọng).
* **Session:**
  + Quản lý trạng thái đăng nhập của người dùng, lưu trữ thông tin tài khoản an toàn.
  + Lưu trữ giỏ hàng với dữ liệu chi tiết và nhạy cảm của người dùng trong quá trình mua sắm.
  + Quản lý quá trình thanh toán và các giao dịch liên quan, giúp theo dõi trạng thái phiên làm việc một cách an toàn và liên tục.