**COOKIE:**

**- Ưu điểm:**

- Nhanh chóng và tiện lợi trong việc nhận diện các thông tin của người dùng, các cài đặt, tùy chọn mà không phải mất quá nhiều thao tác đăng nhập hay thao tác lại từ đầu.

- Cookie được lưu trữ dữ liệu ở phía trình duyệt của người dùng, do đó giúp giảm nhu cầu truy xuất dữ liệu từ máy chủ một cách thường xuyên. Người dùng cũng có thể thuận tiện thay đổi các thông tin đã được lưu trữ, hoạt động, nhập liệu,… mà không cần phải kết nối đến phía máy chủ.

- Máy chủ, doanh nghiệp có thể theo dõi hành vi của khách hang thông qua cookie, từ đó nắm bắt được nhu cầu của khách hang và tối ưu hóa dịch vụ.

**- Nhược điểm:**

- Cookie, nếu không được xử lý đúng cách, dễ trở thành mục tiêu tấn công của các hacker nhằm lấy cắp các thông tin nhạy cảm, mang tính cá nhân của người dùng cho những mục đích xấu.

- Cookie có giới hạn nhất định về dung lượng và số lượng (VD: 4KB cho mỗi cookie, 20 cookie cho mỗi tên miền), do đó cũng giới hạn về lượng thông tin có thể lưu trữ được.

- Mỗi HTTP request đều được đính kèm với cookie, do đó những cookie với dung lượng lớn có thể làm tăng thời gian tải của website, đặc biệt là khi mà không phải tất cả các dữ liệu cookie được tải lên đều cần thiết đối với mỗi request.

**-VD:** Các website thương mại điện tử thường xuyên sử dụng cookie để lưu trữ các thông tin về sản phẩm trong giỏ hang của người dùng. Ngay cả khi người dùng đã rời khỏi trang web, khi quay lại, giỏ hàng vẫn sẽ chứa các mặt hàng họ đã thêm vào trước đó nhờ vào dữ liệu được lưu trong cookie.

**SESSION:**

**- Ưu điểm:**

- Session data được lưu trữ ở phía máy chủ, do đó mang tính bảo mật cao hơn so với cookie.

- Không bị giới hạn về kích thước dữ liệu.

- Dễ triển khai và quản lý trên máy chủ.

**- Nhược điểm:**

- Tiêu tốn bộ nhớ máy chủ nếu không có cách quản lý hiệu quả, đặc biệt là đối với số lượng người dùng lớn, ảnh hưởng đến hiệu suất và khả năng mở rộng của máy chủ.

- Thông thường sẽ bị phụ thuộc vào UID được lưu trữ ở cookie phía người dùng nếu không được xử lý đúng cách.

- Vẫn chịu những rủi ro về bảo mật, vd: các đối tượng tấn công có thể mạo danh người dùng nhằm truy cập trái phép các thông tin nhạy cảm nếu như có thể lấy được UID của người dùng.

**- VD:** Các website yêu cầu Đăng Nhập hầu hết sử dụng Session để quản lý trạng thái đăng nhập của người dùng. Khi người dùng đăng nhập, máy chủ sẽ tạo một Session lưu trữ các thông tin của người dùng. ID của Session sẽ được lưu trữ trong Cookie trên thiết bị của người dùng để duy trì trạng thái của họ qua các công đoạn khác nhau, không cần phải xác thực lại.