RAMAN PERANGKAT BERGERAK

MODUL VII

NAVIGASI

Disusun Oleh : Alfian

Mutakim 2211104024

/ SE0601

Asisten Praktikum :

Muhammad Faza Zulian Gesit Al Barru

Aisyah Hasna Aulia

Dosen Pengampu :

Yudha Islami Sulistya, S.Kom., M.Cs.

PROGRAM STUDI S1 SOFTWARE ENGINEERING FAKULTAS INFORMATIKA

TELKOM UNIVERSITY PURWOKERTO

2024

1. Sebutkan dan jelaskan dua jenis utama Web Service yang sering digunakan dalam pengembangan aplikasi.

   Jawab: Dalam pengembangan aplikasi, dua jenis utama web service yang sering digunakan adalah SOAP dan REST.

   SOAP (Simple Object Access Protocol) adalah protokol berbasis XML yang sangat terstruktur dan cocok untuk aplikasi yang membutuhkan keamanan tinggi dan transaksi kompleks, seperti perbankan. SOAP mendukung berbagai protokol (HTTP, SMTP) dan menggunakan WSDL untuk mendeskripsikan layanan. Namun, karena berbasis XML, SOAP cenderung lebih berat dan lambat dibandingkan REST.

   REST (Representational State Transfer) adalah gaya arsitektur yang menggunakan HTTP untuk mengelola operasi data (CRUD) dengan format yang lebih ringan, biasanya JSON. REST sederhana, fleksibel, dan lebih cepat, sehingga sering digunakan untuk aplikasi modern seperti media sosial atau e-commerce. REST lebih cocok untuk layanan yang mengutamakan kinerja, sementara SOAP lebih ideal untuk kebutuhan keamanan dan keandalan tingkat tinggi.
2. Apa yang dimaksud dengan Data Storage API, dan bagaimana API ini mempermudah pengelolaan data dalam aplikasi?

   Jawab: Data Storage API adalah antarmuka yang memungkinkan aplikasi untuk menyimpan, mengakses, dan mengelola data di berbagai jenis penyimpanan, seperti basis data, cloud storage, atau penyimpanan lokal pada perangkat pengguna. API ini menyediakan cara terstruktur untuk berinteraksi dengan sistem penyimpanan tanpa harus memahami detail teknis di baliknya.

   Contoh penerapannya adalah Firebase Realtime Database API yang memudahkan aplikasi menyimpan dan menyinkronkan data secara real-time di cloud tanpa harus mengelola server secara manual. Hal ini memungkinkan pengembang fokus pada logika aplikasi tanpa terbebani oleh detail teknis penyimpanan data.
3. Jelaskan bagaimana proses kerja komunikasi antara klien dan server dalam sebuah Web Service, mulai dari permintaan (request) hingga tanggapan (response).

   Jawab: Komunikasi antara klien dan server dalam Web Service dimulai dengan klien mengirimkan permintaan (request) ke server melalui protokol HTTP/HTTPS. Permintaan ini berisi endpoint URL, metode HTTP (seperti GET, POST, PUT, DELETE), serta header dan body jika diperlukan. Server kemudian memproses permintaan tersebut, menjalankan logika yang relevan, seperti mengambil data dari basis data atau memvalidasi input, lalu mempersiapkan tanggapan (response).

Tanggapan dikirim kembali ke klien dalam bentuk kode status HTTP (contoh: 200 OK, 404 Not Found) dan data (biasanya dalam format JSON atau XML). Klien menerima tanggapan ini dan menggunakannya untuk menampilkan data kepada pengguna atau melanjutkan proses lain dalam aplikasi.

4. Mengapa keamanan penting dalam penggunaan Web Service, dan metode apa saja yang dapat diterapkan untuk memastikan data tetap aman?

   Jawab: Keamanan sangat penting dalam penggunaan Web Service karena data yang dikirim antara klien dan server sering kali bersifat sensitif, seperti informasi pribadi atau finansial. Tanpa keamanan yang memadai, data ini rentan terhadap ancaman seperti peretasan, penyadapan, atau manipulasi, yang dapat menyebabkan pelanggaran privasi, kerugian finansial, dan hilangnya kepercayaan pengguna.

   Untuk memastikan data tetap aman, beberapa metode yang dapat diterapkan meliputi:

   1. Enkripsi: Menggunakan protokol HTTPS untuk mengenkripsi data yang dikirim antara klien dan server, sehingga data tidak dapat disadap oleh pihak ketiga.
   2. Authentication dan Authorization: Menerapkan mekanisme otentikasi seperti API keys, OAuth, atau JWT (JSON Web Tokens) untuk memastikan hanya pengguna yang berwenang yang dapat mengakses layanan.
   3. Rate Limiting: Membatasi jumlah permintaan dari satu klien untuk mencegah serangan DDoS atau penyalahgunaan API.
   4. Validation and Sanitization: Memastikan bahwa data yang diterima oleh server telah divalidasi dan sanitasi untuk mencegah serangan seperti SQL Injection atau Cross-Site Scripting (XSS).
   5. Monitoring dan Logging: Memantau aktivitas API dan mencatat log untuk mendeteksi dan mencegah aktivitas mencurigakan.