TUGAS PENDAHULUAN
PEMROGRAMAN PERANGKAT BERGERAK

MODUL XIV

DATA STORAGE
‘API’

Disusun Oleh :

Muhammad Abdul Aziz / 2211104026

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

TUGAS PENDAHULUAN

SOAL

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

b. Apa yang dimaksud dengan **Data Storage API**, dan bagaimana API ini mempermudah pengelolaan data dalam aplikasi?

c. Jelaskan bagaimana proses kerja komunikasi antara klien dan server dalam sebuah Web Service, mulai dari permintaan (*request*) hingga tanggapan (*response*).

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

Jawaban

a. Dua Jenis Utama Web Service yang Sering Digunakan dalam Pengembangan Aplikasi

1. RESTful Web Service (REST API)
    - Penjelasan: REST (Representational State Transfer) adalah arsitektur yang menggunakan protokol HTTP untuk komunikasi antara klien dan server. Data dikirim dalam format sederhana seperti JSON atau XML.
    - Kelebihan:
        - Sederhana dan mudah diimplementasikan.
        - Cepat dan ringan karena menggunakan format JSON.
        - Mendukung operasi CRUD (Create, Read, Update, Delete) melalui metode HTTP seperti GET, POST, PUT, DELETE.
    - Contoh Penggunaan: REST API digunakan dalam berbagai layanan seperti aplikasi mobile, website, dan integrasi pihak ketiga.
2. SOAP Web Service
    - Penjelasan: SOAP (Simple Object Access Protocol) adalah protokol komunikasi berbasis XML yang lebih terstruktur dan formal dibanding REST.
    - Kelebihan:
        - Standar keamanan tinggi dengan dukungan WS-Security.
        - Cocok untuk aplikasi enterprise yang membutuhkan transaksi yang kompleks.

- Contoh Penggunaan: SOAP sering digunakan dalam aplikasi keuangan dan layanan yang memerlukan keamanan tinggi.

b. Pengertian Data Storage API dan Bagaimana API Mempermudah Pengelolaan Data

- Pengertian: Data Storage API adalah antarmuka pemrograman aplikasi yang memungkinkan pengembang untuk menyimpan, mengambil, dan mengelola data dalam penyimpanan, baik lokal maupun cloud.
- Kemudahan Pengelolaan Data:
  - Efisiensi: API menyederhanakan interaksi dengan sistem penyimpanan sehingga pengembang tidak perlu menulis kode dari nol.
  - Aksesibilitas: Data dapat diakses dengan mudah melalui panggilan API.
  - Integrasi: Memudahkan integrasi data dengan berbagai layanan atau aplikasi.
  - Skalabilitas: API mendukung pertumbuhan data yang besar melalui penyimpanan cloud seperti Google Firebase, AWS S3, atau Azure Storage.

c. Proses Kerja Komunikasi Antara Klien dan Server dalam Web Service

1. Permintaan (Request):
   - Klien (misalnya aplikasi mobile) mengirimkan permintaan ke server menggunakan protokol HTTP atau HTTPS.
   - Permintaan tersebut berisi metode HTTP seperti:
     - GET: Untuk membaca data.
     - POST: Untuk menambahkan data.
     - PUT: Untuk memperbarui data.
     - DELETE: Untuk menghapus data.
   - Permintaan biasanya berisi header, URL endpoint, dan body (jika diperlukan).
2. Pemrosesan di Server:
   - Server menerima permintaan, memprosesnya, dan berinteraksi dengan database jika perlu.
   - Logika server akan memvalidasi, mengolah data, dan membuat respons sesuai dengan permintaan.

3. Tanggapan (Response):
    - Server mengirimkan respons kembali ke klien dalam format seperti JSON atau XML.
    - Respons biasanya berisi status kode HTTP, seperti:
        - 200 OK: Permintaan berhasil.
        - 400 Bad Request: Permintaan tidak valid.
        - 500 Internal Server Error: Terjadi kesalahan di server.

d. Pentingnya Keamanan dalam Penggunaan Web Service dan Metode Keamanan

- Pentingnya Keamanan:

  Web Service sering digunakan untuk mengirim data sensitif seperti informasi pribadi atau transaksi keuangan. Keamanan mencegah pencurian data, serangan siber, dan akses ilegal.
- Metode Keamanan:
    1. Autentikasi:

       Menggunakan mekanisme autentikasi seperti OAuth 2.0, API Key, atau JWT (JSON Web Token) untuk memastikan hanya pengguna yang sah yang dapat mengakses layanan.
    2. Enskripsi:

       Menggunakan SSL/TLS untuk mengenkripsi data yang dikirim antara klien dan server.
    3. Validasi Input:

       Mencegah serangan seperti SQL Injection atau Cross-Site Scripting (XSS) dengan memvalidasi data input pengguna.
    4. Rate Limiting:

       Membatasi jumlah permintaan dari klien untuk mencegah serangan DDoS.
    5. Penggunaan Firewall:

       Menggunakan Web Application Firewall (WAF) untuk memantau dan memblokir aktivitas mencurigakan.