TUGAS PENDAHULUAN
PEMROGRAMAN PERANGKAT BERGERAK

MODUL XIV

DATA STORAGE ‘API’

Disusun Oleh :

Fikri Khairul Fajri/2211104052

Kelas SE-06-B

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 dalam Pengembangan Aplikasi

SOAP (Simple Object Access Protocol):

- Penjelasan: SOAP adalah protokol berbasis XML yang digunakan untuk pertukaran informasi terstruktur antara aplikasi melalui jaringan. Protokol ini sering digunakan untuk aplikasi yang membutuhkan standar keamanan dan reliabilitas tinggi.

Karakteristik Utama:

- Menggunakan XML sebagai format untuk request dan response.
- Memiliki standar yang ketat untuk pengiriman data.
- Mendukung WS-Security untuk keamanan tambahan.
- Cocok untuk integrasi skala besar antar-sistem.

REST (Representational State Transfer):

- Penjelasan: REST adalah gaya arsitektur yang lebih ringan dan fleksibel dibandingkan SOAP. REST memanfaatkan protokol HTTP untuk komunikasi antara klien dan server.

Karakteristik Utama:

- Menggunakan metode HTTP seperti GET, POST, PUT, DELETE.
- Format data yang umum digunakan adalah JSON atau XML.
- Mudah diimplementasikan dan lebih hemat bandwidth.
- Cocok untuk aplikasi berbasis web dan mobile.

b. Data Storage API

Definisi:

- Data Storage API adalah antarmuka pemrograman aplikasi yang memungkinkan pengembang untuk berinteraksi dengan sistem penyimpanan data seperti basis data, cloud storage, atau file sistem.

Manfaat dan Kemudahan:

- Abstraksi Pengelolaan Data: API menyediakan lapisan abstraksi yang menyembunyikan kompleksitas sistem penyimpanan data sehingga pengembang tidak perlu memahami detail teknis implementasinya.

- Efisiensi: API memungkinkan pengelolaan data seperti membaca, menulis, memperbarui, dan menghapus data secara langsung tanpa harus membuat sistem penyimpanan dari awal.
- Portabilitas: Memungkinkan aplikasi untuk menggunakan berbagai jenis penyimpanan (misalnya SQL, NoSQL, atau penyimpanan berbasis cloud) tanpa harus menulis ulang kode secara signifikan.

c. Proses Komunikasi antara Klien dan Server dalam Web Service

Tahapan Komunikasi:

1. Permintaan (Request):
- Klien mengirimkan permintaan ke server melalui protokol seperti HTTP atau HTTPS.
- Permintaan ini biasanya berisi metode HTTP (GET, POST, PUT, DELETE) dan data tambahan dalam format JSON, XML, atau lainnya.
2. Pemrosesan di Server:
- Server menerima permintaan dan memprosesnya.
- Server dapat memeriksa validitas data, mengakses basis data, atau menjalankan logika bisnis.
3. Tanggapan (Response):
- Setelah memproses permintaan, server mengirimkan tanggapan kembali ke klien.
- Tanggapan ini biasanya berisi data hasil pemrosesan dalam format yang diminta, seperti JSON atau XML, beserta kode status HTTP (misalnya 200 untuk berhasil, 404 untuk tidak ditemukan).

Contoh Skema:

- Request: Klien mengirimkan HTTP GET.
- Server: Memproses permintaan dan mengambil daftar pengguna dari basis data.
- Response: Server mengirimkan daftar pengguna dalam format JSON dengan kode status 200 OK.

d. Pentingnya Keamanan dalam Penggunaan Web Service

Alasan Pentingnya Keamanan:

- Melindungi Data Sensitif: Web service sering mengelola data penting seperti informasi pengguna, transaksi keuangan, atau data perusahaan.
- Mencegah Serangan: Tanpa langkah keamanan, web service rentan terhadap ancaman seperti serangan man-in-the-middle, SQL injection, atau pencurian data.
- Kepatuhan Regulasi: Banyak regulasi seperti GDPR atau HIPAA yang mengharuskan perlindungan data pengguna.

Metode Keamanan:

- HTTPS (SSL/TLS): Mengenkripsi komunikasi antara klien dan server untuk mencegah penyadapan.
- Token-Based Authentication: Menggunakan token seperti OAuth atau JWT untuk memastikan hanya pengguna yang diotorisasi yang dapat mengakses layanan.
- Rate Limiting: Membatasi jumlah permintaan dalam periode tertentu untuk mencegah serangan DDoS.
- Input Validation: Memastikan semua data input aman dan valid untuk mencegah serangan seperti SQL injection atau cross-site scripting (XSS).
- Firewall dan Monitoring: Menggunakan firewall aplikasi dan memonitor log untuk mendeteksi aktivitas mencurigakan.