

**TUGAS PENDAHULUAN
PEMROGRAMAN PERANGKAT BERGERAK**

**MODUL XIV
DATA STORAGE API**



Disusun Oleh :

Muhammad Agam Nasywaan / 2211104085

SE-06-1

Asisten Praktikum :

Muhammad Faza Zulian Gesit Al Barru

Aisyah Hasna Aulia

Dosen Pengampu :

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

PROGRAM STUDI S1 REKAYASA PERANGKAT LUNAK

FAKULTAS INFORMATIKA

TELKOM UNIVERSITY PURWOKERTO

2024

TUGAS PENDAHULUAN

SOAL TP

1. Sebutkan dan jelaskan dua jenis utama Web Service yang sering digunakan dalam pengembangan aplikasi.
2. Apa yang dimaksud dengan Data Storage API, dan bagaimana API ini mempermudah pengelolaan data dalam aplikasi?
3. Jelaskan bagaimana proses kerja komunikasi antara klien dan server dalam sebuah Web Service, mulai dari permintaan (request) hingga tanggapan (response).
4. Mengapa keamanan penting dalam penggunaan Web Service, dan metode apa saja yang dapat diterapkan untuk memastikan data tetap aman?

JAWABAN

1. Jenis web service yang sering digunakan adalah :
 - a. **REST (Representation State Transfer) :**
 - Arsitektur berbasis HTTP yang memanfaatkan metode standar HTTP seperti GET, POST, PUT, dan DELETE
 - Data ditransfer dalam format ringan seperti JSON, XML, atau bahkan plain text
 - Tidak memerlukan WSDL, sehingga lebih sederhana
 - b. **SOAP (Simple Object Access Protocol) :**
 - protokol berbasis XML yang digunakan untuk pertukaran informasi terstruktur antara aplikasi melalui HTTP, SMTP, atau protokol lainnya
 - Menggunakan WSDL (Web Services Description Language) untuk mendefinisikan layanan yang disediakan, format pesan, dan endpoint
 - dirancang untuk mendukung berbagai protokol transportasi dan menawarkan tingkat keamanan serta keandalan yang tinggi
2. Data storage API adalah Application Programming Interface (API) yang memberikan pengembang kemampuan untuk mengelola penyimpanan data dengan efisien dalam aplikasi. API tersebut menawarkan metode dan fungsi standar untuk menyimpan, mengambil, memperbarui, dan menghapus data dari berbagai jenis media penyimpanan, termasuk database, sistem file, atau penyimpanan berbasis cloud. Bagaimana API mempermudah :
 - a. API menyediakan fungsi untuk mengelola detail teknis penyimpanan data yang sudah jadi dan mudah digunakan,
 - b. Dengan menggunakan API, kita dapat dengan cepat mengimplementasikan fitur penyimpanan tanpa membangun sistem dari awal,
 - c. Banyak data storage API sudah mendukung fitur keamanan bawaan, seperti enkripsi dan kontrol akses, sehingga tidak perlu membangun mekanisme keamanan sendiri,
 - d. API seperti Firebase menyediakan sinkronisasi otomatis antara server dan klien, memungkinkan data tetap konsisten di berbagai perangkat,
 - e. API memungkinkan aplikasi beradaptasi dengan berbagai jenis penyimpanan, seperti cloud dan lokal tanpa perubahan besar pada kode.

3. Proses kerja komunikasi antara klien dan server :

Tahap	Deskripsi
Klien (request)	Membuat dan mengirimkan permintaan melalui HTTP dengan metode dan data.
Server	Menerima, memvalidasi, dan memproses permintaan, lalu menyiapkan tanggapan.
Response	Server mengirimkan data atau pesan status ke klien.
Klien (response)	Klien memproses tanggapan dan menampilkan hasil kepada pengguna.

Langkah-langkah sebagai berikut :

- a. Klien membuat request
 - b. Server menerima dan memproses permintaan
 - c. Server menyusun response
 - d. Server mengirim response ke klien
 - e. Klien menerima dan memproses response
4. Keamanan sangat penting dalam penggunaan web service karena layanan ini sering digunakan untuk mengelola data sensitif seperti informasi pribadi, kredensial pengguna, atau transaksi keuangan. Metode yang digunakan sebagai berikut :
- a. **Menggunakan protokol HTTPS**
HTTPS mengenkripsi data yang dikirimkan antara klien dan server menggunakan SSL/TLS, sehingga mencegah penyadapan
 - b. **Menerapkan otentikasi dan otorisasi**
Untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses layanan
 - c. **Enkripsi data**
Data dienkripsi dengan menggunakan algoritma seperti AES (Advanced Encryption Standard)
 - d. **Validasi input**
Memastikan bahwa data yang diterima dari klien valid dan sesuai dengan format yang diharapkan untuk mencegah serangan injeksi, seperti SQL Injection atau XML Injection
 - e. **Penggunaan token JWT (JSON Web Token)**
JSON Web Token (JWT) digunakan untuk memberikan akses sementara kepada klien, dengan data token yang terenkripsi dan memiliki masa berlaku tertentu untuk mencegah penyalahgunaan
 - f. **Rate limiting dan throttling**
Menerapkan batasan pada jumlah permintaan dari klien dalam periode waktu tertentu untuk mencegah serangan DDoS