

**TUGAS PENDAHULUAN  
PEMROGRAMAN PERANGKAT BERGERAK**

**MODUL XIV  
DATA STORAGE 'API'**



**Disusun Oleh :**  
**Rizky Hanifa Afania / 2211104017**  
**SE-06-01**

**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**

## SOAL

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

Jawab:

### 1. SOAP (Simple Object Access Protocol)

SOAP (Simple Object Access Protocol) adalah layanan web yang menggunakan protokol berbasis XML untuk bertukar data antara klien dan server. SOAP memberikan metode yang lebih terorganisir dan formal dalam mengimplementasikan fungsi layanan web. SOAP juga menyediakan format pesan yang terstandar dan terstruktur untuk mendukung komunikasi yang lancar antara aplikasi yang berbeda. Selain itu, SOAP juga dilengkapi dengan Web Services Description Language (WSDL), yang berfungsi sebagai deskripsi dari layanan yang disediakan.

### 2. REST API

REST API (Representational State Transfer Application Programming Interface) adalah antarmuka yang memungkinkan aplikasi klien berkomunikasi dengan database menggunakan protokol HTTP. Dengan REST API, aplikasi dapat melakukan operasi seperti membaca, menambah, memperbarui, dan menghapus data tanpa perlu terhubung langsung ke database. Selain itu, REST API juga memungkinkan setiap perangkat pengguna untuk memperoleh token unik.

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

Jawab:

Data Storage API adalah antarmuka pemrograman aplikasi yang dibangun untuk menyimpan, mengakses, dan mengelola data secara efisien. API ini menyediakan metode standar untuk berinteraksi dengan penyimpanan data, baik itu di server, database lokal, maupun penyimpanan berbasis cloud.

Cara API Mempermudah Pengelolaan Data:

### 1. Abstraksi Penyimpanan Data

Data Storage API akan menyembunyikan kompleksitas teknis dari sistem penyimpanan data di belakang antarmuka yang sederhana. Sehingga pengembang tidak perlu memahami detail internal penyimpanan karena API menyediakan fungsi yang jelas, seperti `save()`, `fetch()`, `update()`, dan `delete()`.

## **2. Kemudahan Integrasi**

Ketika menggunakan API aplikasi bisa dengan mudah terhubung ke berbagai jenis penyimpanan data (misalnya SQL, NoSQL, atau penyimpanan berbasis file) tanpa memerlukan penyesuaian besar pada kode aplikasi.

## **3. Manajemen Data yang Terorganisir**

API membantu mengatur data melalui pengelolaan otomatis seperti indexing, caching, dan pemrosesan query, sehingga pengembang dapat lebih fokus pada logika bisnis aplikasi.

## **4. Akses Data yang Konsisten**

API menyediakan cara untuk mengakses data, baik itu data lokal maupun jarak jauh. Hal ini memastikan bahwa aplikasi dapat berfungsi dengan baik meskipun menggunakan berbagai jenis penyimpanan data.

## **5. Skalabilitas**

API ini memungkinkan pengelolaan data dalam skala besar dengan performa yang optimal. Misalnya, Data Storage API dapat digunakan untuk memproses data dalam jumlah besar menggunakan teknik paging atau batch processing.

## **6. Cross-Platform**

Data Storage API sering kali dirancang agar dapat digunakan di berbagai platform, sehingga mempermudah pengelolaan data pada aplikasi lintas perangkat

### **c. 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 sebuah Web Service dimulai ketika klien mengirimkan permintaan (request) ke server melalui protokol HTTP. Permintaan ini mencakup URL yang spesifik dan menggunakan metode HTTP seperti GET, POST, PUT, atau DELETE. Server kemudian menerima permintaan tersebut, lalu memverifikasi dan memprosesnya berdasarkan logika yang sesuai.

Jika data dibutuhkan, server akan mengakses database atau sistem eksternal lainnya. Setelah selesai, server akan menyiapkan tanggapan (response) dengan status HTTP untuk menunjukkan hasil, misalnya 200 “OK” untuk sukses atau 400 “Bad Request” untuk pesan error.

Tanggapan ini akan dikirim kembali ke klien, kemudian klien membaca kode status tersebut, mengekstrak data dari payload, dan mengambil tindakan yang diperlukan, seperti menampilkan informasi kepada pengguna atau menampilkan pesan error jika

terjadi kegagalan. Proses ini memastikan komunikasi antara klien dan server berjalan secara terstruktur dan efisien.

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

Jawab:

Keamanan penting dalam penggunaan Web Service karena untuk melindungi data sensitif seperti informasi pribadi dari kebocoran data bisa merugikan individu maupun organisasi. Selain itu Web Service digunakan untuk mencegah penyalahgunaan sistem seperti injection, man-in-the-middle (MITM), atau distributed denial of service (DDoS) untuk merusak atau mengambil alih sistem. Jika tidak menggunakan Web Service, sistem akan rentan terhadap serangan sehingga dapat menurunkan reputasi dan kepercayaan dari pengguna atau mitra bisnis.

**Metode untuk memastikan data tetap aman:**

**1. Autentikasi**

Autentikasi digunakan untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses Web Service.

**2. Enkripsi**

Enkripsi digunakan untuk melindungi data selama pengiriman (in transit) maupun penyimpanan (at rest). SSL/TLS digunakan untuk mengenkripsi data saat berpindah antara klien dan server, sehingga data tidak dapat dibaca oleh pihak ketiga yang tidak sah.

**3. Otorisasi**

Otorisasi digunakan untuk memastikan bahwa klien hanya dapat mengakses sumber daya yang mereka izinkan. Sehingga data atau fitur yang sensitif hanya dapat diakses oleh pihak yang memiliki izin eksplisit.

**4. Firewall dan Rate Limiting**

Web Application Firewall (WAF) digunakan untuk memfilter lalu lintas jaringan yang berpotensi berbahaya sebelum mencapai Web Service. Sedangkan rate limiting digunakan untuk membatasi jumlah permintaan yang dibuat oleh klien dalam jangka waktu tertentu, sehingga mencegah penyalahgunaan layanan.

**5. Input Validation**

Data yang dikirimkan oleh klien harus divalidasi sebelum diproses oleh server untuk mencegah serangan berbasis injeksi. Penggunaannya seperti membatasi panjang input, menggunakan pola tertentu, atau hanya menerima data yang sesuai dengan

format yang diharapkan, sehingga bisa meminimalkan risiko eksploitasi data.