

**TUGAS PENDAHULUAN
PEMROGRAMAN PERANGKAT BERGERAK**

**MODUL XIV
DATA STORAGE 'API'**



Disusun Oleh :

**Muhammad Chairul Anam/2211104072
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

TUGAS PENDAHULUAN

SOAL

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

Jawab :

Terdapat dua jenis utama Web Service yang sering digunakan yaitu:

- Representational State Transfer (REST) adalah arsitektur berbasis web service yang ringan dan fleksibel. REST menggunakan protokol HTTP untuk berkomunikasi antara klien dan server.
- Simple Object Access Protocol (SOAP) adalah protokol yang lebih formal dan berbasis XML untuk berkomunikasi antara aplikasi. SOAP dirancang agar lebih ketat dalam spesifikasinya dan mendukung standar yang lebih tinggi untuk keamanan dan transaksi.

- 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 (API) yang dirancang untuk menyediakan mekanisme menyimpan, mengambil, dan mengelola data secara terorganisir dalam aplikasi.

Berikut Data Storage mempermudah pengelolaan data dalam aplikasi:

- Abstraksi Teknologi: API menyediakan fungsi sederhana untuk operasi seperti `save()`, `get()`, dan `delete()` sehingga pengembang tidak perlu memahami detail teknis penyimpanan data.
- Konsistensi Akses: API menyediakan cara standar untuk mengakses data, terlepas dari platform atau perangkat yang digunakan, sehingga pengembang dapat fokus pada logika aplikasi.
- Efisiensi dan Optimasi: Banyak Data Storage API telah dioptimalkan untuk performa, keamanan, dan manajemen sumber daya, yang mengurangi beban kerja pengembang.
- Dukungan Skalabilitas: API memungkinkan aplikasi menangani volume data yang besar dan mendukung pengguna dalam jumlah besar tanpa perlu

infrastruktur tambahan.

- Keamanan Data: Beberapa API memiliki mekanisme bawaan untuk enkripsi, kontrol akses, dan autentikasi, sehingga memastikan data aman dari ancaman.

- 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 Web Service dimulai dengan klien mengirimkan permintaan melalui protokol HTTP atau HTTPS. Permintaan ini mencakup URL atau endpoint, metode HTTP seperti GET atau POST, header untuk informasi tambahan, dan body data jika diperlukan. Server menerima permintaan, memvalidasi data dan autentikasi, lalu menjalankan logika aplikasi seperti mengambil atau menyimpan data. Setelah itu, server menyusun tanggapan yang berisi kode status HTTP, header dengan format data, dan body berisi hasil pemrosesan, biasanya dalam format JSON atau XML. Tanggapan dikirim kembali ke klien, yang memprosesnya dengan membaca kode status, memarsing data, dan melakukan tindakan lanjutan seperti menampilkan informasi atau menyimpan data. Proses ini menggunakan protokol standar untuk memastikan interoperabilitas dan efisiensi.

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

Jawab :

Keamanan dalam Web Service penting untuk melindungi data sensitif seperti informasi pribadi, kredensial pengguna, atau data bisnis dari ancaman seperti peretasan atau pencurian data. Untuk menjaga keamanan, dapat diterapkan metode seperti penggunaan HTTPS untuk enkripsi data selama transmisi, autentikasi dan otorisasi untuk memastikan akses hanya oleh pengguna yang sah, serta enkripsi data saat disimpan. Validasi input mencegah serangan seperti SQL Injection, sementara pembatasan akses seperti rate limiting dan IP whitelisting mengurangi risiko penyalahgunaan. Firewall, manajemen token dengan masa berlaku terbatas, serta audit dan logging membantu mendeteksi dan merespons ancaman.