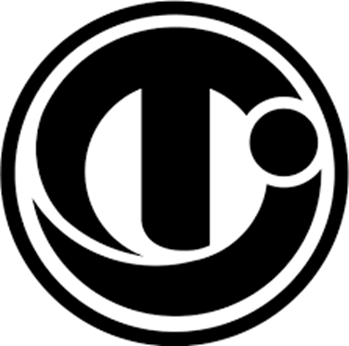
**MAKALAH KEAMANAN DALAM MICROSERVICE**

**Dosen Pengampu:**

**Ervan Asri, S.Kom., M.Kom**

****

**Disusun Oleh:**

**Nadila Dwi Putri**

**2301082015**

**SEMESTER 3**

**PROGRAM STUDI TEKNIK KOMPUTER**

**JURUSAN TEKNOLOGI INFORMASI**

**POLITEKNIK NEGERI PADANG**

**2025/2026**

# BAB I: PENDAHULUAN

## 1.1 Latar Belakang

Arsitektur microservices merupakan pendekatan dalam pengembangan perangkat lunak yang membagi aplikasi besar menjadi layanan-layanan kecil yang berjalan secara independen. Meskipun memberikan banyak keuntungan seperti skalabilitas, fleksibilitas, dan kemudahan dalam pengembangan, arsitektur ini juga membawa tantangan besar dalam hal keamanan. Setiap layanan yang saling berkomunikasi dapat menjadi titik lemah apabila tidak dikelola dengan baik.

## 1.2 Rumusan Masalah

* Apa saja tantangan keamanan dalam arsitektur microservices?
* Bagaimana cara mengamankan komunikasi antar layanan dalam arsitektur microservices?
* Strategi dan teknologi apa saja yang dapat diterapkan untuk meningkatkan keamanan sistem microservices?

## 1.3 Tujuan Penulisan

* Menjelaskan tantangan-tantangan keamanan dalam microservices.
* Memberikan gambaran metode pengamanan dalam sistem microservices.
* Menyajikan strategi dan praktik terbaik (best practices) dalam membangun microservices yang aman.

# BAB III: PEMBAHASAN

## 3.1 Tantangan Keamanan pada Microservices

* Permukaan serangan lebih luas: Karena banyaknya layanan yang terbuka melalui API.
* Komunikasi antar layanan: Rentan terhadap serangan seperti Man-in-the-Middle (MITM).
* Pengelolaan identitas dan akses: Harus disentralisasi atau dikelola dengan metode khusus.
* Logging dan monitoring: Sulit dilakukan karena sistem yang terdistribusi.

## 3.2 Strategi Keamanan dalam Microservices

* Autentikasi dan Otorisasi: Gunakan protokol seperti OAuth 2.0 dan OpenID Connect.
* API Gateway: Mengelola semua permintaan dari luar ke dalam microservices serta
* menambahkan lapisan keamanan seperti rate limiting dan validasi token.
* TLS/SSL: Semua komunikasi antar layanan harus dienkripsi.
* Service Mesh: Seperti Istio atau Linkerd, untuk keamanan dan observabilitas komunikasi antar layanan.
* Zero Trust Security Model: Jangan pernah percaya secara default, walaupun dari dalam jaringan.
* Security Scanning dan DevSecOps: Integrasi keamanan dalam setiap tahap pipeline pengembangan.

# BAB II: TINJAUAN PUSTAKA

## 2.1 Microservices

Microservices adalah pendekatan arsitektur di mana aplikasi dibangun sebagai sekumpulan layanan kecil yang dapat dikembangkan, diuji, dan dideploy secara independen.

## 2.2 Keamanan Sistem Informasi

Keamanan sistem informasi mencakup perlindungan terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem. Dalam konteks microservices, ini mencakup keamanan komunikasi, autentikasi, otorisasi, dan kontrol akses.

# BAB IV: KESIMPULAN

Arsitektur microservices menawarkan fleksibilitas dan skalabilitas, namun membawa tantangan besar dalam aspek keamanan. Untuk menjaga keamanan dalam microservices, diperlukan strategi komprehensif mulai dari autentikasi yang kuat, komunikasi terenkripsi, hingga pengawasan secara menyeluruh menggunakan tools modern. Mengadopsi prinsip Zero Trust dan pendekatan DevSecOps dapat menjadi solusi dalam menjaga integritas dan keamanan sistem secara keseluruhan.

# DAFTAR PUSTAKA

Newman, S. (2015). Building Microservices: Designing Fine-Grained Systems. O'Reilly Media.

Richardson, C. (2018). Microservices Patterns: With examples in Java. Manning Publications.

NIST. (2020). Zero Trust Architecture. Special Publication 800-207.

<https://istio.io/latest/docs/concepts/what-is-istio/>

https://oauth.net/2/