**MAKALAH**

**KEAMANAN DALAM MICROSERVICES**

**PEMROGRAMAN MICROSERVICES TEORI**

**Dosen Pengampu :**

Ervan Asri, S.Kom., M.Kom



**Disusun Oleh:**

**Miftahud Dini 23010081009**

**SEMESTER 3**

**PROGRAM STUDI D3 TEKNIK KOMPUTER**

**JURUSAN TEKNOLOGI INFORMASI**

**POLITEKNIK NEGERI PADANG**

**2024/2025**

**DAFTAR ISI**

[BAB I 3](#_Toc2898)

[PENDAHULUAN 3](#_Toc31251)

[1.1. Latar Belakang3](#_Toc22457)

[1.2. Rumusan Masalah 3](#_Toc16183)

[1.3. Tujuan Penulisan 3](#_Toc19670)

[1.4. Manfaat Penulisan 3](#_Toc18274)

[BAB II 4](#_Toc24182)

[KONSEP DASAR MICROSERVICES 4](#_Toc29245)

[2.1. Devinisi Microservice 4](#_Toc9296)

[2.2. Arsitektur Microservices 4](#_Toc7318)

[2.3. Perbandingan dengan Momolitc 4](#_Toc17465)

[BAB III 5](#_Toc10272)

[TANTANGAN KEAMANAN DALAM MICROSERVICE 5](#_Toc1897)

[3.1. Permukaan Serangan yang Lebih Luas 5](#_Toc13887)

[3.2. Komukasi Antar Layanan 5](#_Toc15003)

[3.3. Dependency dan Service Discovery 5](#_Toc22047)

[3.4. Manajemen Konfigurasi dan Secret 5](#_Toc14392)

[BAB IV 6](#_Toc10413)

[STRATEGI KEAMANAN MICROSERVICE 6](#_Toc13566)

[4.1. Autentikasi dan Otorisasi 6](#_Toc20777)

[4.2. API Gateway dan Rate Limiting 6](#_Toc27329)

[4.3. TLS/SSL dan Enkripsi 6](#_Toc32611)

[4.4. Zero Trust Architecture 6](#_Toc23084)

[4.5. Logging dan Monitoring 6](#_Toc2287)

[BAB VI 7](#_Toc25531)

[PENUTUP 7](#_Toc28873)

[5.1. Kesimpulan 7](#_Toc14652)

[5.2. Saran 7](#_Toc31038)

[DAFTAR PUSTAKA 8](#_Toc29847)

# BAB I

# PENDAHULUAN

## Latar Belakang

Microservices adalah pendekatan arsitektur perangkat lunak di mana aplikasi dibagi menjadi layanan - layanan kecil yang dapat dikembangkan, diuji dan di-deploy secara mandiri. Pendekatan ini memungkinkan fleksibilitas dan skalabilitas, namun juga memperluas permukaan serangan karena adanya komunikasi antar layanan. Oleh karena itu, keamanan dalam sistem microservices menjadi aspek penting yang perlu diperhatikan sejak awal perancangan.

## Rumusan Masalah

Apa saja tantangan keamanan dalam penerapan arsitektur microservice, dan bagaimana strategi yang dapat diterapkan untuk mengatasi tantangan tersebut?

## Tujuan Penulisan

Tujuan dari penulisan makalah ini adalah untuk:

* Mengidentifikasi tantangan keamanan dalam arsitektur microservices
* Menjelaskan strategi keamanan yang dapat diterapkan

## Manfaat Penulisan

Makalah ini diharapkan dapat memberikan wawasan kepada mahasiswa, pengembang, dan profesional TI tentang pentingnya memperhatikan aspek keamanan dalam implementasi arsitektur microservices.

# BAB II

# KONSEP DASAR MICROSERVICES

## 2.1. Devinisi Microservice

Microservices merupakan pendekatan pengembangan aplikasi yang membagi sistem menjadi layanan-layanan kecil yang dapat bekerja secara independen. Setiap layanan biasanya memiliki fungsionalitas spesifik dan dapat dikembangkan menggunakan teknologi yang berbeda.

## 2.2. Arsitektur Microservices

Dalam arsitektur ini, setiap layanan memiliki basis data dan logika bisnis sendiri, serta berkomunikasi melalui API atau message broker. Komunikasi ini memungkinkan integrasi tetapi juga menimbulkan tantangan keamanan.

## 2.3. Perbandingan dengan Momolitc

Pendekatan monolithic menyatukan seluruh komponen dalam satu unit aplikasi. Sebaliknya, microservices memisahkan fungsionalitas ke dalam layanan-layanan independen. Walau memberikan skalabilitas dan fleksibilitas, pendekatan ini memerlukan pengelolaan keamanan yang lebih kompleks.

# BAB III

# TANTANGAN KEAMANAN DALAM MICROSERVICE

## 3.1. Permukaan Serangan yang Lebih Luas

Dalam arsitektur microservices, banyaknya layanan berarti lebih banyak titik masuk yang dapat diserang. Setiap API endpoint menjadi potensi celah keamanan jika tidak dilindungi secara menyeluruh.

## 3.2. Komukasi Antar Layanan

Komunikasi antar layanan sering dilakukan melalui HTTP atau gRPC. Tanpa autentikasi dan enkripsi yang tepat, data sensitif bisa dengan mudah diakses oleh pihak yang tidak berwenang.

## 3.3. Dependency dan Service Discovery

Microservices sering menggunakan dependency eksternal dan mekanisme service discovery otomatis. Jika layanan tidak divalidasi, pihak luar bisa menyusup dengan berpura-pura sebagai layanan internal.

## 3.4. Manajemen Konfigurasi dan Secret

Penggunaan file konfigurasi dan penyimpanan kunci API harus dijaga dengan baik. Kegagalan dalam melindungi konfigurasi dapat membuka celah serangan besar.

# BAB IV

# STRATEGI KEAMANAN MICROSERVICE

## 4.1. Autentikasi dan Otorisasi

Gunakan protokol modern seperti OAuth 2.0 dan OpenID Connect untuk memastikan hanya pengguna dan layanan yang berwenang dapat mengakses sistem. JWT (JSON Web Token) juga umum digunakan untuk mengelola otorisasi antar layanan.

## 4.2. API Gateway dan Rate Limiting

API Gateway berfungsi sebagai perantara semua permintaan masuk. Dengan mengatur rate limiting dan validasi request, gateway mencegah serangan brute-force dan DoS.

## 4.3. TLS/SSL dan Enkripsi

Semua komunikasi antar layanan harus dienkripsi menggunakan TLS untuk menjaga kerahasiaan dan integritas data. Hindari pengiriman data dalam bentuk plain text.

## 4.4. Zero Trust Architecture

Dalam pendekatan zero trust, tidak ada layanan yang dipercaya secara default. Setiap layanan harus saling mengautentikasi dan diverifikasi untuk setiap komunikasi.

## 4.5. Logging dan Monitoring

Aktivitas layanan harus dipantau secara real-time. Logging dan monitoring dapat membantu mendeteksi aktivitas mencurigakan dan mengurangi waktu respons terhadap insiden.

# BAB VI

# PENUTUP

## 5.1. Kesimpulan

Keamanan dalam arsitektur microservices merupakan tantangan yang signifikan. Kompleksitas sistem yang tinggi menuntut penerapan strategi keamanan yang holistik, dari autentikasi, enkripsi, hingga pemantauan layanan secara aktif.

## 5.2. Saran

Pengembangan berbasis microservices harus selalu mempertimbangkan aspek keamanan sejak tahap desain. Penggunaan tools keamanan modern dan prinsip best practice sangat disarankan.

# DAFTAR PUSTAKA

Fowler, M. (2015). Microservices. martinfowler.com.

Newman, S. (2019). Building Microservices: Designing Fine-Grained Systems. O'Reilly Media.

Richardson, C. (2018). Microservices Patterns. Manning Publications.

AWS. (2023). Microservices Security Best Practices. aws.amazon.com