**MAKALAH MICROSERVICE**

**KEAMANAN DALAM MICROSERVICE**



**Disusun Oleh :**

**Rosi Maltasari**

**2301083008**

**KELAS 2A TEKNIK KOMPUTER**

**JURUSAN TEKNOLOGI INFORMASI**

**PROGRAM STUDI D3 TEKNIK KOMPUTER**

**POLITEKNIK NEGERI PADANG**

**2025**

# KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya, makalah yang berjudul **“Keamanan dalam Microservices”** ini dapat diselesaikan dengan baik dan tepat waktu.

Makalah ini disusun sebagai salah satu bentuk tugas dalam rangka memperdalam pemahaman mengenai aspek keamanan pada arsitektur microservices, yang saat ini banyak digunakan dalam pengembangan perangkat lunak modern. Penulis berusaha menyajikan informasi yang relevan, mulai dari tantangan keamanan yang dihadapi, strategi pengamanan, hingga contoh implementasi di dunia nyata.

Penulis menyadari bahwa dalam penyusunan makalah ini masih terdapat kekurangan, baik dari segi isi maupun penyajiannya. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca demi perbaikan di masa yang akan datang.

Ucapan terima kasih penulis sampaikan kepada semua pihak yang telah membantu dalam penyusunan makalah ini, khususnya kepada dosen pengampu dan rekan-rekan yang telah memberikan masukan serta dukungan.

Akhir kata, semoga makalah ini dapat memberikan manfaat dan menambah wawasan bagi pembaca.

Padang , 08 April 2025

Penyusun

# DAFTAR ISI

[KATA PENGANTAR ii](#_Toc195017375)

[DAFTAR ISI iii](#_Toc195017376)

[BAB 1 4](#_Toc195017377)

[PENDAHULUAN 4](#_Toc195017378)

[1.1. Latar Belakang 4](#_Toc195017379)

[1.2. Rumusan Masalah 4](#_Toc195017380)

[1.3. Tujuan Penulisan 4](#_Toc195017381)

[BAB II 2](#_Toc195017382)

[PEMBAHASAN 2](#_Toc195017383)

[2.1. Tantangan Keamanan dalam Microservices 2](#_Toc195017384)

[2.2. Strategi Keamanan dalam Microservices 2](#_Toc195017385)

[BAB III 3](#_Toc195017386)

[PENUTUP 3](#_Toc195017387)

[3.1. Kesimpulan 3](#_Toc195017388)

[3.2. Saran 3](#_Toc195017389)

[DAFTAR PUSTAKA 4](#_Toc195017390)

# BAB 1

# PENDAHULUAN

## 1.1. Latar Belakang

Arsitektur microservices telah menjadi pilihan utama dalam pengembangan perangkat lunak modern karena kemampuannya dalam memecah sistem besar menjadi layanan-layanan kecil yang independen. Meskipun menawarkan fleksibilitas dan skalabilitas tinggi, microservices juga memperkenalkan tantangan baru dalam hal keamanan. Tidak seperti sistem monolitik, setiap layanan dalam microservices berkomunikasi melalui jaringan, sehingga membuka banyak celah keamanan.

## 1.2. Rumusan Masalah

* Apa saja tantangan keamanan dalam arsitektur microservices?
* Bagaimana cara mengamankan komunikasi antar layanan?
* Apa peran autentikasi dan otorisasi dalam microservices?

## 1.3. Tujuan Penulisan

* Menjelaskan risiko dan tantangan keamanan pada sistem microservices.
* Menguraikan strategi dan praktik terbaik dalam mengamankan microservices.
* Memberikan pemahaman tentang pentingnya pendekatan keamanan yang terdistribusi.

# BAB II

# PEMBAHASAN

## 2.1. Tantangan Keamanan dalam Microservices

* Kompleksitas Komunikasi Jaringan: Banyaknya titik komunikasi antar layanan membuka lebih banyak celah untuk serangan seperti man-in-the-middle atau packet sniffing.
* Permukaan Serangan yang Lebih Luas: Tiap service memiliki endpoint yang dapat diserang, memperbesar risiko.
* Manajemen Identitas dan Akses: Kesulitan dalam menerapkan kontrol akses yang konsisten di seluruh layanan.
* Pemantauan dan Logging: Membutuhkan sistem pemantauan yang terdistribusi dan mampu mendeteksi anomali secara real-time.

## 2.2. Strategi Keamanan dalam Microservices

* Autentikasi dan Otorisasi Terpusat: Gunakan OAuth2, OpenID Connect, atau JSON Web Token (JWT) untuk manajemen identitas terpusat. Gateway API dapat menangani autentikasi sebelum mengizinkan akses ke layanan.
* Enkripsi Komunikasi: Gunakan HTTPS dan TLS untuk mengamankan komunikasi antar layanan.
* Gateway API sebagai Gerbang Keamanan: Gateway API dapat menyaring permintaan yang masuk, menambahkan autentikasi, rate limiting, dan logging.
* Zero Trust Security Model: Tidak mempercayai layanan manapun secara otomatis. Semua komunikasi antar layanan harus melalui autentikasi dan otorisasi yang kuat.
* Rate Limiting dan Circuit Breaker: Mencegah penyalahgunaan layanan dan menghindari overload.
* Security Testing & DevSecOps: Integrasi keamanan sejak awal dalam pengembangan (DevSecOps), serta penggunaan tools untuk pengujian keamanan secara otomatis (static code analysis, dependency scanning, dll).

# BAB III

# PENUTUP

## 3.1. Kesimpulan

Keamanan dalam arsitektur microservices memerlukan pendekatan yang berbeda dibandingkan sistem monolitik. Setiap layanan harus memiliki lapisan keamanan tersendiri, dan sistem secara keseluruhan harus didesain dengan prinsip "defense in depth".

## 3.2. Saran

Pengembang dan tim keamanan perlu bekerja sama sejak awal pengembangan. Penggunaan tools otomatis dan penerapan DevSecOps menjadi sangat penting untuk menjaga keamanan sistem secara menyeluruh.

# DAFTAR PUSTAKA

<https://www.oreilly.com/library/view/building-microservices/9781491950340/>

[**https://owasp.org/www-project-cloud-native-application-security-top-10/**](https://owasp.org/www-project-cloud-native-application-security-top-10/)

[**https://cheatsheetseries.owasp.org/cheatsheets/Microservices\_Security\_Cheat\_Sheet.html**](https://cheatsheetseries.owasp.org/cheatsheets/Microservices_Security_Cheat_Sheet.html)