**MAKALAH MICROSERVICE**

**KEAMANAN DALAM MICROSERVICE**



**Disusun Oleh :**

**Farid Fadlizil Ikram**

**2301083013**

**TK 2A**

**JURUSAN TEKNOLOGI INFORMASI**

**PROGRAM STUDI D3 TEKNIK KOMPUTER**

**POLITEKNIK NEGERI PADANG**

**2024/2025**

**KATA PENGANTAR**

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena berkat rahmat dan karunia-Nya, makalah yang berjudul "Keamanan dalam Microservices" ini dapat diselesaikan dengan baik dan tepat waktu.

Makalah ini disusun sebagai bagian dari tugas untuk memperdalam pemahaman mengenai aspek keamanan dalam arsitektur microservices, yang semakin banyak diterapkan dalam pengembangan perangkat lunak modern. Penulis berusaha menyajikan informasi yang relevan mengenai tantangan-tantangan keamanan yang dihadapi, strategi pengamanan yang dapat diterapkan, serta contoh implementasi di dunia nyata.

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

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

Semoga makalah ini dapat memberikan manfaat dan wawasan tambahan bagi pembaca.

Padang, 08 April 2025

Penyusun

# DAFTAR ISI

[KATA PENGANTAR ii](#_Toc195020427)

[DAFTAR ISI iii](#_Toc195020428)

[BAB 1 1](#_Toc195020429)

[PENDAHULUAN 1](#_Toc195020430)

[1.1. Latar Belakang 1](#_Toc195020431)

[1.2. Rumusan Masalah 1](#_Toc195020432)

[1.3. Tujuan Penulisan 1](#_Toc195020433)

[BAB II 2](#_Toc195020434)

[PEMBAHASAN 2](#_Toc195020435)

[2.1. Tantangan Keamanan dalam Microservices 2](#_Toc195020436)

[2.2. Strategi Keamanan dalam Microservices 2](#_Toc195020437)

[BAB III 3](#_Toc195020438)

[PENUTUP 3](#_Toc195020439)

[3.1. Kesimpulan 3](#_Toc195020440)

[3.2. Saran 3](#_Toc195020441)

[DAFTAR PUSTAKA 3](#_Toc195020442)

# BAB 1

# PENDAHULUAN

# Latar Belakang Arsitektur microservices telah menjadi pilihan utama dalam pengembangan perangkat lunak modern karena kemampuan untuk membagi aplikasi besar menjadi layanan-layanan kecil yang dapat berjalan secara independen. Walaupun menawarkan fleksibilitas dan kemampuan skalabilitas yang tinggi, penggunaan microservices juga menghadirkan tantangan signifikan dalam aspek keamanan. Berbeda dengan sistem monolitik, komunikasi antar layanan dalam microservices dilakukan melalui jaringan, yang membuka lebih banyak potensi celah keamanan.

# Rumusan Masalah • Apa saja tantangan utama dalam menjaga keamanan arsitektur microservices? • Bagaimana cara mengamankan komunikasi antara layanan dalam sistem microservices? • Apa peran penting dari autentikasi dan otorisasi dalam arsitektur microservices?

# Tujuan Penulisan • Mengidentifikasi berbagai risiko dan tantangan keamanan yang dihadapi dalam sistem berbasis microservices. • Menyediakan panduan mengenai strategi dan praktik terbaik dalam mengamankan arsitektur microservices. • Menggambarkan pentingnya pendekatan keamanan yang terdistribusi dalam microservices.

# BAB II

# PEMBAHASAN

# 2.1. Tantangan Keamanan dalam Microservices

# Kompleksitas Komunikasi Jaringan: Banyaknya titik komunikasi antar layanan memberikan lebih banyak kesempatan bagi potensi serangan, seperti man-in-the-middle atau penyadapan paket data.

# Permukaan Serangan yang Lebih Luas: Setiap layanan dalam arsitektur microservices memiliki endpoint yang dapat diserang, yang meningkatkan potensi risiko.

# Manajemen Identitas dan Akses: Implementasi kontrol akses yang konsisten di seluruh layanan menjadi tantangan tersendiri.

# Pemantauan dan Logging: Sistem pemantauan yang mendalam dan terdistribusi diperlukan untuk mendeteksi ancaman dan anomali secara real-time.

# 2.2. Strategi Keamanan dalam Microservices

# Autentikasi dan Otorisasi Terpusat: Menggunakan protokol seperti OAuth2, OpenID Connect, atau JSON Web Token (JWT) untuk pengelolaan identitas secara terpusat. API Gateway dapat bertanggung jawab untuk autentikasi sebelum mengizinkan akses ke layanan lainnya.

# Enkripsi Komunikasi: Menggunakan HTTPS dan TLS untuk memastikan komunikasi antar layanan tetap aman.

# API Gateway sebagai Pengontrol Keamanan: API Gateway bertindak sebagai titik pemeriksaan untuk permintaan yang masuk, menambahkan lapisan autentikasi, pembatasan akses (rate limiting), dan pencatatan aktivitas (logging).

# Model Keamanan Zero Trust: Semua komunikasi antar layanan harus melewati autentikasi dan otorisasi yang ketat, tanpa mengandalkan kepercayaan otomatis antar layanan.

# Pembatasan Akses dan Circuit Breaker: Mengurangi kemungkinan penyalahgunaan layanan serta menghindari beban yang berlebihan pada sistem.

# Pengujian Keamanan dan DevSecOps: Mengintegrasikan keamanan sejak awal dalam siklus pengembangan perangkat lunak (DevSecOps), serta menggunakan alat untuk pengujian otomatis terhadap kerentanannya, seperti analisis kode statis dan pemindaian ketergantungan.

# BAB III

# PENUTUP

# 3.1. Kesimpulan Keamanan dalam sistem berbasis microservices memerlukan pendekatan yang lebih kompleks dibandingkan dengan arsitektur monolitik. Setiap layanan harus dilengkapi dengan lapisan keamanannya sendiri, dan seluruh sistem harus dibangun dengan prinsip pertahanan berlapis (defense in depth).

# 3.2. Saran Penting bagi pengembang dan tim keamanan untuk bekerja sama sejak awal proyek. Penggunaan alat otomatis dan penerapan pendekatan DevSecOps akan sangat membantu dalam menjaga keamanan sistem secara menyeluruh.

# DAFTAR PUSTAKA

# <https://terralogiq.com/microservices-architecture/>

# <https://owasp.org/www-project-cloud-native-application-security-top-10/>

# <https://cheatsheetseries.owasp.org/cheatsheets/Microservices_Security_Cheat_Sheet.html>

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