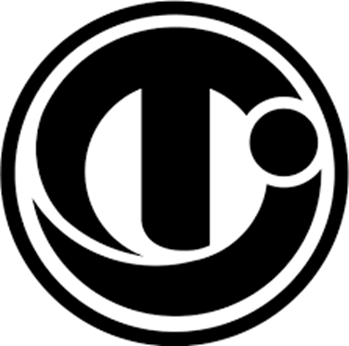
**MAKALAH KEAMANAN DALAM MICROSERVICE**

**Dosen Pengampu:**

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

****

**Disusun Oleh:**

**Nafilah Az Zahra**

**2301082016**

**SEMESTER 3**

**PROGRAM STUDI TEKNIK KOMPUTER**

**JURUSAN TEKNOLOGI INFORMASI**

**POLITEKNIK NEGERI PADANG**

**2024/2025**

# KATA PENGANTAR

Segala puji dan syukur kami panjatkan ke hadirat Allah Swt. atas limpahan rahmat, taufik, serta hidayah-Nya, sehingga makalah yang berjudul “Keamanan dalam Arsitektur Microservice” ini dapat disusun dan diselesaikan dengan baik.

Penyusunan makalah ini merupakan bagian dari upaya akademik untuk memperdalam pemahaman serta mengkaji aspek keamanan dalam penerapan arsitektur microservice, yang saat ini menjadi salah satu pendekatan utama dalam pengembangan sistem perangkat lunak modern. Diharapkan makalah ini dapat memberikan kontribusi ilmiah, baik secara teoritis maupun praktis, khususnya bagi kalangan akademisi, mahasiswa, serta praktisi di bidang teknologi informasi.

Ucapan terima kasih kami sampaikan kepada seluruh pihak yang telah memberikan dukungan, baik secara langsung maupun tidak langsung, dalam proses penyusunan makalah ini. Tanpa adanya bantuan, bimbingan, serta masukan dari berbagai pihak, niscaya makalah ini tidak dapat terselesaikan secara optimal.

Kami menyadari bahwa makalah ini masih memiliki keterbatasan, baik dari segi substansi maupun penyajiannya. Oleh karena itu, kami sangat terbuka terhadap kritik dan saran yang membangun guna penyempurnaan karya ini di masa yang akan datang.

Akhir kata, semoga makalah ini dapat memberikan manfaat dan menambah khazanah keilmuan bagi pembaca sekalian.

# **DAFTAR ISI**

Contents

[KATA PENGANTAR ii](#_Toc195044406)

[**DAFTAR ISI** iii](#_Toc195044407)

[**BAB I PENDAHULUAN** 1](#_Toc195044408)

[**BAB II PEMBAHASAN** 3](#_Toc195044409)

[**BAB III PENUTUP** 4](#_Toc195044410)

[**DAFTAR PUSTAKA** 5](#_Toc195044411)

# **BAB I PENDAHULUAN**

* 1. **Latar Belakang**

Seiring berkembangnya teknologi informasi, arsitektur perangkat lunak telah mengalami perubahan signifikan, salah satunya dengan munculnya arsitektur microservice. Microservice merupakan pendekatan arsitektur di mana aplikasi dibangun sebagai sekumpulan layanan kecil yang saling terpisah dan berkomunikasi satu sama lain melalui protokol ringan seperti HTTP atau messaging queue. Pendekatan ini memberikan banyak keuntungan seperti skalabilitas, kemudahan pengembangan, dan fleksibilitas teknologi.

Namun, di balik keunggulan tersebut, arsitektur microservice juga menghadirkan tantangan tersendiri dalam hal keamanan. Kompleksitas sistem yang terdiri dari banyak layanan independen menyebabkan permukaan serangan menjadi lebih luas. Masalah-masalah seperti otentikasi dan otorisasi antar layanan, komunikasi aman melalui jaringan, serta perlindungan terhadap serangan umum seperti man-in-the-middle, injection, atau distributed denial-of-service (DDoS) menjadi lebih kompleks dan krusial untuk diatasi.

Oleh karena itu, penting untuk memahami dan menerapkan prinsip serta praktik keamanan yang tepat dalam pengembangan dan pengelolaan sistem berbasis microservice agar integritas, kerahasiaan, dan ketersediaan layanan tetap terjaga.

* 1. **Rumusan Masalah**

1. Bagaimana tantangan keamanan dalam arsitektur microservice berbeda dari sistem monolitik?
2. Apa saja kerentanan (vulnerabilities) umum yang muncul dalam sistem microservice?
3. Strategi apa yang dapat diterapkan untuk meningkatkan keamanan microservice, termasuk otentikasi, otorisasi, dan proteksi data?
4. Bagaimana mengimplementasikan monitoring dan logging yang efektif untuk mendeteksi ancaman keamanan secara real-time?
   1. **Tujuan Penulisan**
5. Menganalisis risiko dan tantangan keamanan unik dalam arsitektur microservice.
6. Mengidentifikasi praktik terbaik (best practices) untuk mengamankan komunikasi, data, dan akses antar-layanan.
7. Memberikan rekomendasi solusi teknologi (seperti API Gateway, JWT, Service Mesh, dan enkripsi) untuk mitigasi risiko.
8. Menjelaskan pentingnya security-by-design dan continuous monitoring dalam siklus hidup pengembangan microservice.

# **BAB II PEMBAHASAN**

1. **Tantangan Kemanan dalam Microservice**

Microservice memperkenalkan kompleksitas baru karena banyaknya layanan yang berinteraksi satu sama lain. Beberapa tantangan umum dalam hal keamanan meliputi:

* Otentikasi dan otorisasi: Menyediakan kontrol akses yang aman untuk setiap layanan.
* Manajemen identitas layanan: Memastikan bahwa layanan yang berkomunikasi memang layanan yang sah.
* Keamanan komunikasi: Data yang ditransmisikan antar layanan harus dienkripsi.
* Permukaan serangan yang luas: Setiap endpoint layanan merupakan titik potensi serangan.

1. **Otentikasi dan Otoritasi Antar Layanan**

Implementasi otentikasi dan otorisasi dapat dilakukan dengan beberapa cara:

* OAuth 2.0 dan OpenID Connect: Digunakan untuk mengelola identitas pengguna dan layanan.
* JWT (JSON Web Token): Token yang membawa klaim pengguna dan digunakan untuk mengautentikasi permintaan antar layanan.
* API Gateway: Sebagai titik masuk utama, API Gateway dapat mengelola otentikasi dan otorisasi sebelum permintaan diteruskan ke layanan internal.

1. **Keamanan Komunikasi Antar Layanan**

* Transport Layer Security (TLS): Menyediakan enkripsi untuk komunikasi antar layanan.
* Service Mesh: Teknologi seperti Istio atau Linkerd dapat digunakan untuk mengamankan komunikasi antar layanan secara otomatis.

1. **Praktik Terbaik Keamanan Microservice**

* Gunakan prinsip least privilege dalam pengaturan akses.
* Implementasikan rate limiting dan circuit breaker untuk mencegah serangan DoS.
* Gunakan logging dan monitoring untuk mendeteksi anomali.
* Terapkan scanning otomatis terhadap kerentanan dalam image container dan dependencies.

# **BAB III PENUTUP**

1. **KESIMPULAN**

Keamanan dalam arsitektur microservice adalah aspek krusial yang tidak boleh diabaikan. Kompleksitas dan banyaknya layanan yang berinteraksi memperluas permukaan serangan dan memerlukan pendekatan keamanan yang menyeluruh dan sistematis. Dengan mengimplementasikan otentikasi yang kuat, komunikasi terenkripsi, serta praktik terbaik keamanan lainnya, sistem microservice dapat dibangun dengan lebih aman dan andal.

# **DAFTAR PUSTAKA**

Hutasuhut, N. R. P., Amri, M. G., & Aji, R. F. (2024). Security Gap in Microservices: A Systematic Literature Review. International Journal of Advanced Computer Science and Applications, 15(12), 165–171.

Atmojo, S., Utami, R., Dewi, S., & Widhiyanta, N. (2022). Implementasi Arsitektur Microservice dalam Sistem Informasi Desa. SMATIKA Jurnal: STIKI Informatika Jurnal, 12(01), 55–66.

Haris, A. I., Ferianda, R. A., Riyanto, B., Nugraha, F. I., & Abadi, J. (2020). Pengamanan Container Orchestration Berbasis Kubernetes di Lembaga Penerbangan dan Antariksa Nasional (LAPAN). Jurnal TEKNOINFO, 14(1), 1–8.

Amri, M. G., & Aji, R. F. (2022). Pedoman Keamanan Microservice dan Application Programming Interface (API).

Sutanto, A. (2021). Implementasi Autentikasi dari Sisi Backend pada Arsitektur Microservice. Jurnal INFOTRONIK, 6(2).