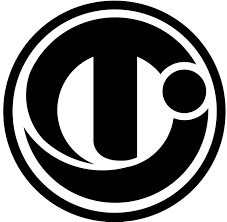
**MAKALAH**

**MICROSERVICE**



**SEMESTER 2**

**Disusun Oleh:**

|  |  |  |
| --- | --- | --- |
| **Nama** | **:** | **Zaki Ramadhan** |
| **Nim** | **:** | **2301082020** |
| **Kelas** | **:** | **2A Teknik Komputer** |

**JURUSAN TEKNOLOGI INFORMASI**

**PROGRAM STUDI TEKNIK KOMPUTER**

**POLITEKNIK NEGERI PADANG**

**2025**

**KATA PENGANTAR**

Puji syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa, karena berkat rahmat dan karunia-Nya, makalah ini dapat diselesaikan dengan baik. Dalam era digital yang terus berkembang, arsitektur perangkat lunak mengalami transformasi yang signifikan. Salah satu pendekatan yang semakin populer adalah arsitektur microservice, yang memungkinkan pengembang untuk membangun aplikasi dengan membagi fungsionalitas menjadi layanan-layanan kecil yang dapat beroperasi secara independen.

Meskipun arsitektur ini menawarkan banyak keuntungan, seperti fleksibilitas, skalabilitas, dan kemudahan dalam pengembangan, tantangan keamanan yang dihadapi juga semakin kompleks. Makalah ini bertujuan untuk memberikan pemahaman yang lebih dalam mengenai keamanan dalam microservice. Dengan membahas tantangan yang ada dan praktik terbaik yang dapat diterapkan, diharapkan pembaca dapat memahami pentingnya keamanan dalam pengembangan aplikasi berbasis microservice.

Saya berharap makalah ini bermanfaat bagi mahasiswa, pengembang, dan profesional di bidang teknologi informasi. Terima kasih kepada teman-teman yang telah memberikan dukungan dan bimbingan dalam penyusunan makalah ini.

Padang, 08 April 2025

Penulis

**DAFTAR ISI**

**KATA PENGANTAR 2**

**DAFTAR ISI 3**

**BAB 1 PENDAHULUAN 4**

1.1Latar Belakang 4

1.2 Rumusan Masalah 4

1.3 Tujuan **4**

**BAB 2 PEMBAHASAN 5**

2.1 Tantangan kemanana dalam microservice 5

2.2 Cara mengamankan komunikasi antar layanan dalam microservice 5

2.3 Langkah-Langkah Efektif untuk Memperkuat Keamanan dalam 6

**BAB 3 PENUTUP 8**

3.1 Kesimpulan 8

**DAFTAR PUSTAKA 9**

**BAB 1**

**PENDAHULUAN**

**1.1 Latar belakang**

Arsitektur microservice telah menjadi pilihan utama dalam pengembangan perangkat lunak modern. Dengan membagi aplikasi menjadi layanan-layanan kecil yang dapat beroperasi secara independen, pengembang dapat meningkatkan efisiensi dan fleksibilitas dalam pengembangan. Namun, dengan banyaknya layanan yang terpisah, tantangan keamanan juga meningkat. Setiap layanan dapat menjadi titik masuk bagi penyerang, dan komunikasi antar layanan yang tidak aman dapat mengakibatkan kebocoran data. Oleh karena itu, penting untuk memahami dan mengimplementasikan langkah-langkah keamanan yang tepat dalam arsitektur microservice.

**1.2 Rumusan Masalah**

1. Apa saja tantangan keamanan yang dihadapi dalam arsitektur microservice?
2. Bagaimana cara mengamankan komunikasi antar layanan dalam arsitektur microservice?
3. Apa Langkah-Langkah Efektif untuk Memperkuat Keamanan dalam Arsitektur Microservice?

**1.3 Tujuan**

1. Untuk mengidentifikasi dan menganalisis tantangan keamanan yang dihadapi dalam arsitektur microservice.
2. Untuk memberikan rekomendasi tentang cara mengamankan komunikasi antar layanan.
3. Untuk menyajikan langkah-langkah terbaik yang dapat diterapkan untuk meningkatkan keamanan dalam microservice.

**BAB 2**

**PEMBAHASAN**

**2.1 Tantangan kemanana dalam microservice**

* **Komunikasi Antar Layanan:**  
  Dalam microservice, layanan saling berkomunikasi melalui API. Jika komunikasi ini tidak dilindungi, data sensitif bisa terekspos. Oleh karena itu, sangat penting menggunakan protokol aman seperti HTTPS serta menerapkan otentikasi dan otorisasi yang kuat untuk menghindari kebocoran data dan serangan seperti injeksi.
* **Manajemen Identitas dan Akses:**  
  Manajemen akses dalam microservice lebih kompleks karena setiap layanan perlu kontrol akses sendiri. Penting untuk menerapkan autentikasi per layanan dan menggunakan prinsip "least privilege", agar layanan hanya memiliki akses yang benar-benar dibutuhkan. Ini mengurangi risiko penyalahgunaan akses oleh pengguna maupun sistem.
* **Ketergantungan pada Layanan Pihak Ketiga:**  
  Microservice sering bergantung pada layanan eksternal seperti API publik atau layanan cloud. Ketergantungan ini bisa menjadi titik lemah jika pihak ketiga tidak memiliki sistem keamanan yang memadai. Maka dari itu, penting melakukan penilaian keamanan sebelum mengandalkan layanan pihak ketiga.
* **Permukaan Serangan yang Lebih Luas:**  
  Banyaknya layanan membuat permukaan serangan semakin luas. Setiap layanan yang tidak aman bisa menjadi pintu masuk penyerang untuk mengakses sistem lain. Karena itu, setiap layanan harus diamankan secara menyeluruh, termasuk validasi input, pembatasan akses, dan pengujian kerentanan secara rutin.

**2.2 Cara mengamankan komunikasi antar layanan dalam microservice**

* **Penggunaan Protokol Aman:** Mengimplementasikan HTTPS untuk mengenkripsi data yang dikirimkan antar layanan. Ini melindungi data dari penyadapan dan memastikan integritas data.
* **Otentikasi dan Otorisasi yang Kuat:** Menggunakan metode otentikasi seperti JSON Web Token (JWT) atau OAuth 2.0 untuk memastikan bahwa hanya pengguna dan layanan yang berwenang yang dapat mengakses layanan. Setiap layanan harus memverifikasi token sebelum memberikan akses.
* **Enkripsi Data:** Menggunakan enkripsi untuk melindungi data sensitif yang dikirimkan antar layanan. Selain itu, data yang disimpan di database juga harus dienkripsi untuk melindungi dari akses yang tidak sah.
* **API Gateway:** Menggunakan API Gateway untuk mengelola komunikasi antar layanan. API Gateway dapat menangani otentikasi, otorisasi, dan pengendalian lalu lintas, serta memberikan logging dan monitoring untuk mendeteksi aktivitas mencurigakan.
* **Rate Limiting dan Throttling:** Menerapkan pembatasan jumlah permintaan yang dapat dilakukan oleh pengguna atau layanan dalam periode waktu tertentu untuk mencegah serangan DDoS

.

**2.3 Langkah-Langkah Efektif untuk Memperkuat Keamanan dalam**

* **Arsitektur Microservice**

Monitoring dan Logging: Mengimplementasikan sistem monitoring dan logging untuk mendeteksi aktivitas mencurigakan dan merespons insiden keamanan dengan cepat. Data log dapat digunakan untuk analisis keamanan dan perbaikan.

* **Pengujian Keamanan Berkelanjutan:** Mengintegrasikan pengujian keamanan ke dalam siklus pengembangan perangkat lunak (SDLC) untuk mendeteksi dan mengatasi masalah keamanan sejak dini.
* **Pendidikan dan Pelatihan**: Memberikan pelatihan keamanan kepada pengembang untuk memastikan mereka memahami praktik terbaik dan potensi risiko yang terkait dengan pengembangan microservice.
* **Audit Keamanan Rutin:** Melakukan audit keamanan secara berkala untuk mengidentifikasi dan memperbaiki kerentanan. Ini termasuk pengujian penetrasi dan analisis kerentanan.
* **Implementasi Prinsip Least Privilege:** Menggunakan prinsip hak akses minimum untuk membatasi akses pengguna dan layanan hanya pada sumber daya yang diperlukan. Ini mengurangi risiko jika akun pengguna atau layanan dikompromikan.
* **Pembaruan dan Patching:** Memastikan semua layanan dan dependensinya selalu diperbarui dengan patch keamanan terbaru untuk melindungi dari kerentanan yang diketahui.

**BAB 3**

**PENUTUP**

**3.1 Kesimpulan**

Dengan memahami tantangan keamanan yang dihadapi dalam arsitektur microservice dan menerapkan langkah-langkah untuk mengamankan komunikasi antar layanan, serta mengikuti praktik terbaik, organisasi dapat membangun sistem yang lebih aman dan tahan terhadap serangan. Keamanan harus menjadi bagian integral dari pengembangan microservice untuk melindungi data sensitif dan menjaga kepercayaan pengguna.

**Daftar Pustaka**

"Microservices Architecture." (n.d.). Martin Fowler. Retrieved from

martinfowler.com

"Microservices Security: A Guide." (2022). Nginx. Retrieved from

nginx.com