**MAKALAH**

**TEORI MICROSERVICES**

**“KEAMANAN DALAM MICROSERVICES”**



**DISUSUN OLEH:**

**SALSA BILA PUTRI SONIA**

**2301081015**

**PROGRAM STUDI TEKNIK KOMPUTER**

**JURUSAN TEKNOLOGI INFORMASI**

**POLITEKNIK NEGERI PADANG**

**2024/2025**

1. **Pendahuluan**

Microservice adalah salah satu arsitektur perangkat lunak yang saat ini banyak digunakan untuk mengembangkan aplikasi modern. Dalam pendekatan ini, aplikasi besar dipecah menjadi layanan-layanan kecil yang saling terpisah dan dapat beroperasi secara independen. Setiap layanan memiliki fungsi spesifik dan berkomunikasi satu sama lain melalui API (Application Programming Interface). Keunggulan utama dari microservice adalah skalabilitas, fleksibilitas, dan kemudahan pengembangan. Namun, di balik keunggulannya, ada tantangan besar yang perlu diperhatikan, yaitu keamanan.

Keamanan dalam microservice menjadi hal yang sangat penting karena arsitektur ini melibatkan banyak komponen yang saling terhubung. Jika salah satu komponen tidak aman, maka seluruh sistem dapat terancam. Oleh karena itu, penting bagi pengembang untuk memahami ancaman keamanan serta menerapkan langkah-langkah perlindungan yang tepat agar aplikasi tetap aman dan dapat berfungsi dengan baik.

1. **Ancaman Keamanan dalam Microservice**

Dalam arsitektur microservice, terdapat beberapa ancaman keamanan yang sering muncul, di antaranya:

1. **Serangan pada API**  
   Microservice menggunakan API untuk berkomunikasi antar layanan. Jika API tidak diamankan dengan baik, maka pihak tidak bertanggung jawab dapat mengeksploitasi celah tersebut untuk mencuri data atau merusak sistem.
2. **Serangan Berbasis Internet**  
   Karena layanan dalam microservice sering diekspos ke internet, risiko serangan seperti DDoS (Distributed Denial of Service), phishing, atau eksploitasi celah keamanan menjadi lebih tinggi dibandingkan aplikasi monolitik.
3. **Kegagalan Berjenjang**  
   Dalam microservice, semua layanan saling terhubung. Jika satu layanan mengalami masalah atau diretas, maka layanan lain juga bisa ikut terkena dampaknya. Hal ini disebut sebagai kegagalan berjenjang (cascading failure).
4. **Ancaman pada Kontainer dan Virtualisasi**  
   Microservice sering berjalan di dalam kontainer seperti Docker. Jika kontainer tidak dikonfigurasi dengan baik atau menggunakan image yang tidak aman, maka sistem dapat menjadi target serangan.
5. **Kurangnya Otentikasi dan Otorisasi**  
   Jika sistem tidak memiliki mekanisme otentikasi dan otorisasi yang kuat, maka pengguna atau pihak luar bisa mendapatkan akses ke layanan yang seharusnya bersifat privat.
6. **Strategi Keamanan dalam Microservice**

Untuk mengatasi berbagai ancaman tersebut, ada beberapa strategi keamanan yang dapat diterapkan:

1. **Mengamankan API**  
   API adalah pintu utama komunikasi antar layanan dalam microservice. Oleh karena itu, penting untuk mengamankan API dengan menerapkan autentikasi menggunakan token seperti JSON Web Token (JWT) atau OAuth 2.0. Selain itu, gunakan enkripsi seperti HTTPS agar data yang dikirim melalui API tetap aman.
2. **Manajemen Identitas dan Akses**  
   Terapkan sistem manajemen akses berbasis peran (Role-Based Access Control/RBAC) untuk memastikan bahwa hanya pengguna atau layanan tertentu yang memiliki izin untuk mengakses data atau fungsi tertentu.
3. **Menggunakan Protokol Komunikasi Aman**  
   Komunikasi antar layanan harus dilakukan melalui protokol yang aman seperti TLS (Transport Layer Security). Ini memastikan bahwa data yang dikirim antar layanan tidak dapat disadap oleh pihak ketiga.
4. **Pemantauan dan Deteksi Ancaman**  
   Gunakan alat monitoring seperti Prometheus atau ELK Stack untuk memantau aktivitas pada sistem secara real-time. Dengan pemantauan ini, tim pengembang dapat mendeteksi potensi ancaman sejak dini sebelum menjadi masalah besar.
5. **Isolasi Layanan dengan Kontainer**  
   Pastikan setiap layanan berjalan di dalam kontainer yang terisolasi satu sama lain. Gunakan alat seperti Kubernetes untuk mengelola kontainer secara efisien dan memastikan keamanan konfigurasi.
6. **Pembaruan dan Patch Secara Berkala**  
   Pastikan semua komponen sistem, termasuk framework dan library pihak ketiga, selalu diperbarui agar tidak ada celah keamanan akibat versi lama.
7. **Penerapan Rate Limiting**  
   Rate limiting adalah teknik membatasi jumlah permintaan ke suatu layanan dalam periode waktu tertentu. Ini berguna untuk mencegah serangan DDoS atau penyalahgunaan API.
8. **Backup dan Recovery**  
   Selalu siapkan mekanisme backup data secara berkala agar jika terjadi serangan atau kegagalan sistem, data tetap aman dan dapat dipulihkan dengan cepat.
9. **Pentingnya Keamanan dalam Microservice**

Keamanan bukan hanya tentang melindungi data atau mencegah serangan; lebih dari itu, keamanan juga berkaitan dengan menjaga kepercayaan pengguna terhadap aplikasi kita. Dalam dunia digital saat ini, pengguna sangat peduli terhadap privasi dan keamanan data mereka. Jika sebuah aplikasi gagal menjaga keamanan data pengguna, maka reputasi perusahaan dapat rusak.

Selain itu, serangan siber juga dapat menyebabkan kerugian finansial yang besar bagi perusahaan. Misalnya, jika sebuah layanan diretas dan menyebabkan downtime pada aplikasi utama, maka perusahaan bisa kehilangan pendapatan selama periode tersebut.

1. **Kesimpulan**

Keamanan dalam arsitektur microservice adalah aspek yang sangat penting untuk diperhatikan oleh pengembang aplikasi modern. Dengan memahami ancaman-ancaman umum serta menerapkan strategi keamanan yang tepat seperti autentikasi API, enkripsi komunikasi, isolasi kontainer, dan pemantauan sistem secara real-time, risiko terhadap sistem dapat diminimalkan.

Meskipun microservice menawarkan banyak keuntungan seperti skalabilitas dan fleksibilitas pengembangan, tanpa langkah-langkah keamanan yang memadai, arsitektur ini bisa menjadi target serangan siber yang serius. Oleh karena itu, pengembang harus selalu mengutamakan aspek keamanan dalam setiap tahap pengembangan aplikasi berbasis microservice agar aplikasi tetap aman dan terpercaya bagi pengguna maupun perusahaan.