

Nama : Isep Lutpi Nur  
NPM : 2113191079  
Kelas : Informatika / A2  
Mata Kuliah : Cloud Computing  
Semester : 5 (Ganjil)  
Tugas : Pertemuan 12 Cloud Security

---

**Buat resume dari materi cloud security silahkan ditambahkan dari sumber-sumber lain diluar slide.**

## **1. Cloud security**

Keamanan komputasi awan atau mengacu pada serangkaian kebijakan, teknologi, dan kontrol yang diterapkan untuk melindungi data, aplikasi, dan infrastruktur komputasi awan yang terkait. Ini adalah sub-domain keamanan komputer, keamanan jaringan, dan lebih luas lagi, keamanan informasi.[1]

Perjanjian Tingkat Layanan (Service Level Agreements (SLA)) tidak memberikan perlindungan hukum yang memadai bagi pengguna komputer cloud, sering kali dibiarkan untuk menangani peristiwa di luar kendali mereka.

## **2. Risiko keamanan cloud**

Terdapat beberapa risiko keamanan cloud diantaranya:

- **Ancaman tradisional (Traditional threats):** dampak diperkuat karena banyaknya sumber daya cloud dan populasi pengguna yang besar yang dapat terpengaruh. Batas tanggung jawab yang kabur antara penyedia layanan cloud dan pengguna dan kesulitan untuk mengidentifikasi penyebabnya secara akurat.
- **Ancaman baru (New threats):** server cloud menghosting banyak VM; beberapa aplikasi dapat berjalan di bawah setiap VM. Kerentanan multi-tenancy dan VMM membuka saluran serangan baru untuk pengguna jahat. Mengidentifikasi jalur yang diikuti oleh penyerang lebih sulit di lingkungan cloud.
- **Otentikasi dan otorisasi prosedur:** yang berlaku untuk satu individu tidak mencakup perusahaan.
- **Kontrol pihak ketiga:** menimbulkan spektrum kekhawatiran yang disebabkan oleh kurangnya transparansi dan kontrol pengguna yang terbatas.

- **Ketersediaan layanan cloud:** kegagalan sistem, pemadaman listrik, dan peristiwa bencana lainnya dapat mematikan layanan untuk waktu yang lama.

### **3. Keamanan dan Privasi**

#### **A. Manajemen Identitas**

Setiap perusahaan akan memiliki sistem manajemen identitasnya sendiri untuk mengontrol akses ke informasi dan sumber daya komputasi. Penyedia Cloud mengintegrasikan sistem manajemen identitas pelanggan ke dalam infrastruktur mereka sendiri, menggunakan teknologi federasi atau SSO, atau sistem identifikasi berbasis biometrik,[1] atau menyediakan sistem manajemen identitas mereka sendiri. CloudID,[1] misalnya, menyediakan identifikasi biometrik berbasis cloud dan lintas perusahaan yang melestarikan privasi. Ini menghubungkan informasi rahasia dari pengguna ke biometrik mereka dan menyimpannya secara terenkripsi. Memanfaatkan teknik enkripsi yang dapat dicari, identifikasi biometrik dilakukan dalam domain terenkripsi untuk memastikan bahwa penyedia cloud atau penyerang potensial tidak mendapatkan akses ke data sensitif atau bahkan isi dari pertanyaan individu.[1]

#### **B. Keamanan fisik**

Penyedia layanan cloud secara fisik mengamankan perangkat keras TI (server, router, kabel, dll.) Terhadap akses tidak sah, gangguan, pencurian, kebakaran, banjir, dll. Dan memastikan bahwa pasokan penting (seperti listrik) cukup kuat untuk meminimalkan kemungkinan gangguan. Ini biasanya dicapai dengan melayani aplikasi cloud dari 'kelas dunia' (yaitu pusat data yang ditentukan secara profesional, dirancang, dibangun, dikelola, dipantau dan dipelihara).

#### **C. Keamanan personil**

Berbagai masalah keamanan informasi yang berkaitan dengan TI dan profesional lain yang terkait dengan layanan cloud biasanya ditangani melalui kegiatan pra-, para dan pasca-kerja seperti perekrutan potensi perekrutan keamanan, kesadaran keamanan dan program pelatihan, proaktif.

#### **D. Pribadi**

Penyedia memastikan bahwa semua data penting (nomor kartu kredit, misalnya) ditutupi atau dienkripsi dan hanya pengguna yang berwenang yang memiliki akses ke data secara keseluruhan. Selain itu, identitas dan kredensial digital harus dilindungi sebagaimana seharusnya data apa pun yang dikumpulkan atau dihasilkan oleh penyedia tentang aktivitas pelanggan di cloud.

#### **4. Referensi dari luar**

[1] dari K. Keamanan komputasi awan. Wikipedia.org. Published October 21, 2018. Accessed December 22, 2021. [https://id.wikipedia.org/wiki/Keamanan\\_komputasi\\_awan](https://id.wikipedia.org/wiki/Keamanan_komputasi_awan)

[2]