

Komputasi Awan

Oleh:

Tim Penyusun Komputasi Awan
PENS

Materi Ajar

1. Pengenalan terhadap Komputasi Awan
2. Layanan Komputasi Awan
3. Kerangka dan Teknologi Komputasi Awan
4. Integrasi dan Standarisasi Komputasi Awan
- 5. Keamanan Komputasi Awan**
6. Aplikasi Awan pada AWS dan GCP
7. Aplikasi Awan dengan Openstack
8. Big Data dan Analytics pada Komputasi Awan
9. Performa, Keandalan dan Ketersediaan Komputasi Awan
10. Migrasi dan Manajemen Komputasi Awan
11. SKKNI Komputasi Awan
12. Prospek Komputasi Awan

Keamanan Komputasi Awan

Outline

- Keamanan Komputasi Awan: Isu dan perhatian
 - Kerahasiaan, integritas dan ketersediaan
 - Isu dan tantangan
- Mengamankan *Cloud*: Metodologi dan penerapan
 - Manajemen keamanan
 - Mekanisme dan teknik keamanan
 - Audit dan penilaian
 - Deteksi intrusi dan respon kebencanaan
 - Keberlanjutan bisnis dan perencanaan pemulihan

Pendahuluan

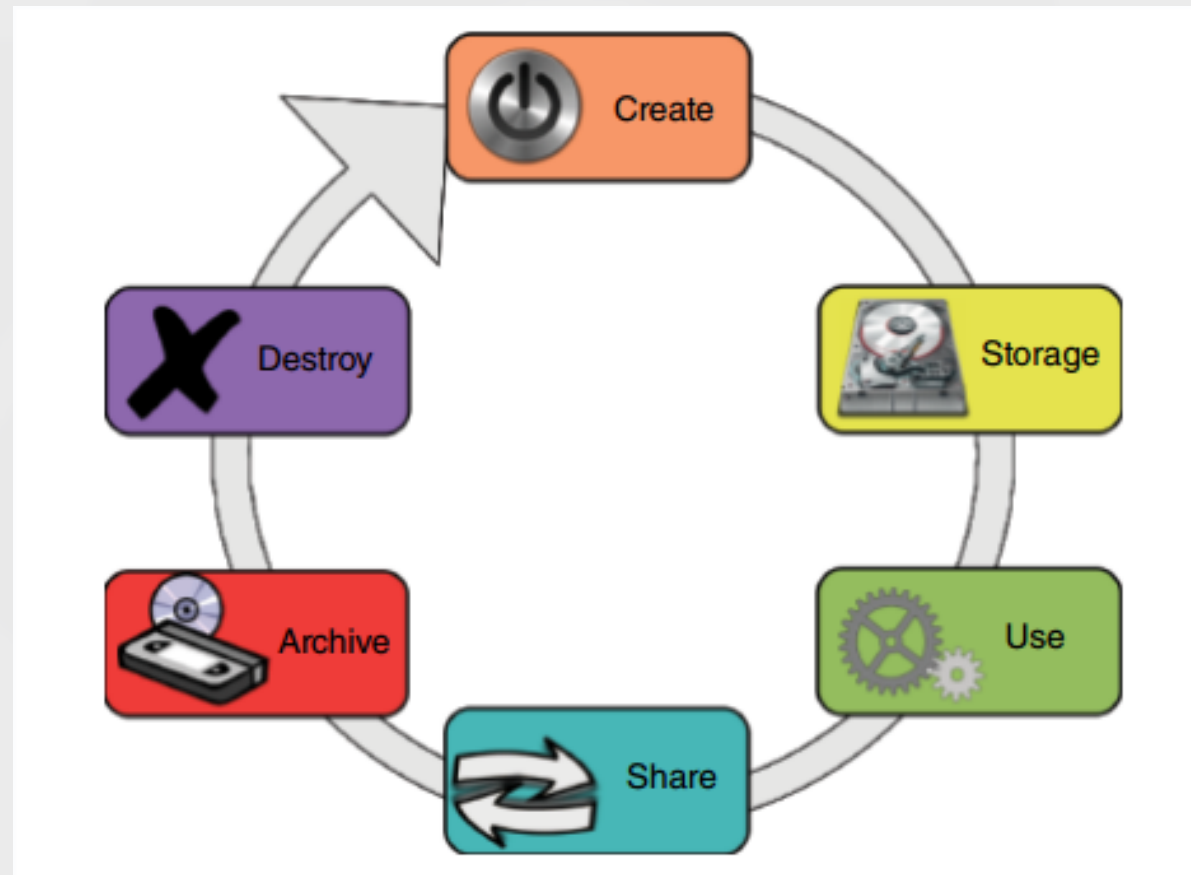
- Ancaman keamanan dapat muncul karena kompleksitas pada komputasi awan (mis. distribusi dinamis, virtualisasi, dan multi-tenan)
- Penyedia layanan komputasi awan mungkin tidak sepenuhnya dapat **dipercaya**.



CIA

- Masalah keamanan dapat diklasifikasikan dengan CIA:
 - Confidentiality (kerahasiaan)
 - Integrity (integritas)
 - Availability (ketersediaan)
- Tipe penyedia layanan komputasi awan:
 - *Fully trusted providers*: contoh riilnya adalah *private cloud* dimana kendali penuh ada dipengguna.
 - *Curious providers*: media penyimpanan atau pemrosesan yang melibatkan data sensitif harus dijaga kerahasiaannya oleh penyedia layanan.
 - *Lazy providers*: media penyimpanan atau pemrosesan dianggap dapat dipercaya dengan nota perjanjian layanan saja.
 - *Malicious (byzantine) providers*: penyedia layanan mungkin secara sengaja dapat salah dalam manajemen, penyimpanan, dan pemrosesan data, dengan mengorbankan kerahasiaan, integritas, atau ketersediaan layanan.

Siklus hidup keamanan data



Isu dan tantangan komputasi awan(1)

- Perlindungan Data:
menjamin kerahasiaan, integritas, dan ketersediaan data
- *Fine-Grained Access*:
memungkinkan pengambilan data dan eksekusi query secara “halus” pada data yang telah dilindungi.
- Akses Selektif
memungkinkan pengguna dapat menerapkan pembatasan ACL

Isu dan tantangan komputasi awan(2)

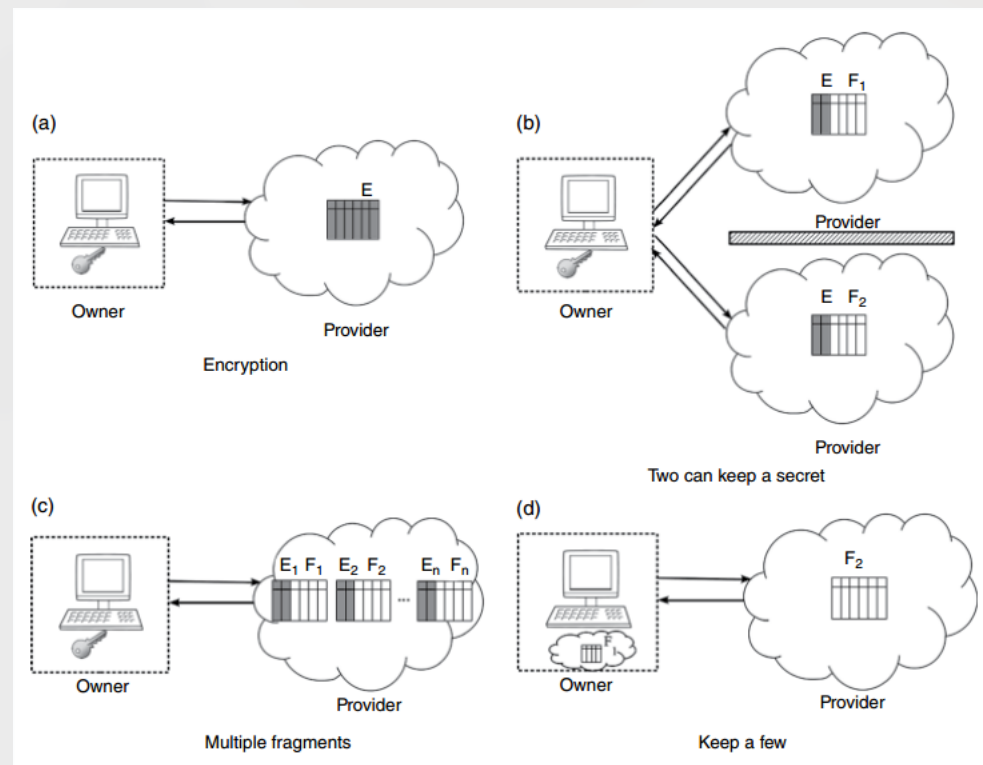
- Privasi Pengguna
meyediakan privasi dalam melakukan komputasi mengakses data
- Privasi *Query*
meyediakan privasi terhadap semua aktifitas/kegiatan pengguna.
- Integritas Komputasi dan *Query*
memungkinkan koreksi, kelengkapan dan pembaharuan terhadap komputasi dan kueri

Isu dan tantangan komputasi awan(3)

- Kolaborasi *Query* dengan Banyak Penyedia
memungkin untuk berbagi kueri dengan penyedia layanan lain.
- SLA dan Audit
spesifikasi dan evaluasi keamanan yang dijaminan oleh penyedia layanan
- Multi-tenant dan Virtualisasi
penyediaan “isolasi” terhadap data dan aktifitas pada lingkungan virtualisasi bersama.

Perlindungan data

- Ingat CIA!!
- Solusi untuk melindungi kerahasiaan adalah “*honest-but-curious*”



Manajemen Keamanan

- Tantangan yang paling mendasar dari keamanan komputasi awan adalah hilangnya kendali atas sistem, aplikasi, keamanan data, dan sumber daya lainnya.
- Untuk mengelola keamanan secara efektif maka harus fokus pada:
 - Tata kelola
 - Kebijakan keamanan
 - Persyaratan kontrak dan aturan (bahasa)
 - SLA

Mekanisme dan Teknik Keamanan (1)

- Terdapat 3 mekanisme keamanan di komputasi awan:

1. Keamanan jaringan: keamanan yang mencakup perlindungan data saat berada di jaringan yang meliputi:

- *Network access control (NAC)*
- Kontrol terhadap *Firewall* (parameter dan subtier)
- *Access Control List (ACL)*
- Inspeksi dan kontrol terhadap konten
- Mitigasi/proteksi terhadap DDoS

Mekanisme dan Teknik Keamanan (2)

- Terdapat 3 mekanisme keamanan di komputasi awan:

2. Kemanan data dan privasi: data adalah pusat utama dari komputasi awan. Ada 3 isu yang harus diperhatikan yaitu: **ketersediaan, enkripsi dan proteksi**. Berikut adalah tips untuk menghadapi isu tersebut:

- Hindari untuk menyimpan informasi yang sensitif di *Cloud*.
- Tinjau ulang perjanjian kontrak.
- Gunakan password yang kuat
- Gunakan layanan enkripsi untuk *Cloud*.

Mekanisme dan Teknik Keamanan (3)

- Terdapat 3 mekanisme keamanan di komputasi awan:

3. Keamanan aplikasi: Keamanan aplikasi berbasis *cloud* wajib tersedia tanpa harus berasumsi apa pun tentang lingkungan *cloud*. Hal ini dikarenakan pengembangan aplikasi di cloud berbeda dengan aplikasi yang dikembangkan secara tradisional dimana:

- di *cloud*, kontrol terhadap keamanan fisik terbatas
- Potensi ketidakcocokan lingkungan ketika adanya migrasi
- Proteksi data melalui siklus hidup aplikasi harus diperhatikan.
- Proses pengambil alihan data ketika terjadi kegagalan juga harus diperhatikan
- Kombinasi web-service di komputasi awan berpotensi terhadap ancaman keamanan.

Mekanisme dan Teknik Keamanan (3) cont.

- Terdapat 3 mekanisme keamanan di komputasi awan:

3. Keamanan aplikasi: Beberapa hal yang harus diperhatikan dalam mengembangkan aplikasi berbasis *cloud* adalah:

- *SSDLC (Secured Software Development Life Cycle)*
- Arsitektur keamanan aplikasi: Autentikasi, otorisasi, dan administrasi.
- Pemantauan aplikasi *cloud*: pemantauan *log*, pemantauan performa, pemantauan pelanggaran kebijakan dan pemantauan pengguna jahat.

Audit dan Penilaian Keamanan (1)

- Keamanan *cloud* harus dapat diaudit dan dapat dinilai agar:
 - dapat dievaluasi secara berkelanjutan
 - diketahui apakah solusi yang diberikan/diterapkan dapat memberikan keamanan.
- Audit:
 - Proses audit dilakukan untuk memastikan solusi *cloud* telah bekerja seperti yang diharapkan.
 - Proses audit dapat dilakukan oleh internal maupun eksternal
 - Keamanan yang diaudit (berdasar NIST):
 - Dokumentasi prosedur, standarisasi, kebijakan, dll
 - Informasi tentang konfigurasi standar dan konfigurasi yang saat ini
 - Keberlanjutan *logging* dan pemantauan informasi

Audit dan Penilaian Keamanan (2)

- **Penilaian**: Penilaian terhadap *cloud* meliputi pelaksanaan proses *scanning* dan pemeriksaan kerentanan beserta dampak kerentanan tersebut. Data hasil penilaian sangatlah sensitif dan harus diamankan/dirahasiakan.
- **Tes penetrasi**: mekanisme untuk menilai suatu keamanan adalah dengan melakukan tes penetrasi. Tes ini dijalankan dengan melakukan simulasi skenario serangan. Umumnya IaaS dan PaaS yang dilakukan tes penetrasi.

Deteksi dan respon kejadian terhadap Intrusi

- Tujuan dari **deteksi intrusi** adalah memantau adanya intrusi yang dapat menurunkan performa komputasi awan. Ada dua teknik deteksi intrusi:
 - Deteksi berbasis jaringan
 - Deteksi berbasis kejadian/aktifitas
- **Respon kejadian** bertujuan untuk mengambil aksi untuk menghindari, memblok dan menghentikan serangan.

Keberlanjutan bisnis dan perencanaan pemulihan bencana

- Kata kunci: kehandalan dan ketersediaan yang tinggi.
- Komponen dari **keberlanjutan bisnis** dan **pemulihan bencana** diantaranya:
 - Mengamankan cadangan: sistem cadangan selalu tersedia
 - Infrastruktur yang dinamis: pengguna tidak merasa khawatir jika dikemudian hari ingin memperluas sistem.
 - Membayar hanya saat digunakan: pengguna hanya membayar saat menggunakan layanan saja.

Referensi

- Liu, Simon. "Securing the Clouds: Methodologies and Practices." Encyclopedia of Cloud Computing (2016): 220.
- Samarati, Pierangela, and Sabrina De Capitani di Vimercati. "Cloud Security: Issues and Concerns." Encyclopedia of Cloud Computing (2016): 205-219.

TERIMA KASIH