



Available online at : <http://bit.ly/InfoTekJar>

# InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600



Cloud Computing

## Analisis Keamanan pada *Cloud Computing*

Charles Josua Napitupulu

Universitas Sumatera Utara

### KEYWORDS

Keamanan; *Cloud Computing*; Data

### CORRESPONDENCE

Phone:

E-mail: [khairuddin\\_nst@uisu.ac.id](mailto:khairuddin_nst@uisu.ac.id)

### A B S T R A C T

*Cloud Computing* sudah menjadi salah satu tren baru di era internet ini. *Clouds* dimaksudkan sebagai sebuah Data Center yang letaknya bisa dimana saja sebagai tempat menyimpan dan memproses data, baik data perorangan ataupun profesional. Umumnya faktor keamanan menjadi kekhawatiran utama pengguna karena semua data yang berada di *clouds* dapat diakses siapa saja dan dari mana saja selama terkoneksi di internet. *Paper* ini akan memaparkan analisis keamanan yang diterapkan dan resiko yang dihadapi teknologi *cloud computing* ini.

### PENDAHULUAN

Kehadiran *Cloud Computing* pada era ini telah menjadi bagian yang penting di dunia ini. Kebutuhan orang akan internet dan meningkatnya kecepatan internet mendukung semakin banyak pengguna internet menjadi tergantung pada aplikasi yang berbasis *cloud* untuk menunjang aktivitasnya setiap hari. *Cloud Computing* telah mewujudkan proses komputasi menggunakan internet untuk mengakses aplikasi, analisa data dan proses lain yang berhubungan dengan data secara online. Banyaknya bentuk data yang terkumpul pada teknologi *Cloud* ini baik yang dimiliki oleh perorangan, organisasi, perusahaan dan pemerintahan telah menjadi hal utama bagi penyedia layanan ini untuk menjaga seluruh aspek termasuk aspek keamanan dari data-data tersebut. *Paper* ini akan membahas isu-isu keamanan dan resiko-resiko yang ada pada teknologi *Cloud Computing*.

#### *Pengertian Cloud Computing*

Hingga saat ini belum ada pengertian yang baku untuk *Cloud Computing* ini, namun pada dasarnya *Cloud Computing* ini merupakan kumpulan dari banyak *Data Center* yang saling terhubung oleh jaringan dan di virtualisasikan sehingga membentuk sebuah kolam raksasa yang memiliki sumber daya yang sangat besar baik sumber daya (memproses, menyimpan dan kecepatan) dan dapat dengan otomatis secara cerdas beradaptasi untuk mengatur keperluannya sesuai dengan perubahan kebutuhan pengguna, dengan mengoptimalkan dari ketersediaan dari tiap sumber daya yang *idle* sehingga jika

terjadi *failure* pada salah satu *hardware*, maka teknologi ini akan dapat mengatasinya secara otomatis.

*Cloud Computing* mempunyai tiga layanan yang diberikan kepada pengguna, yaitu:

1. *Infrastructure as Service* : meliputi *Grid* untuk virtualisasi layanan, cth : Amazon
2. *Platform as Service* : memfokuskan pada aplikasi digunakan secara online, sehingga pengguna tidak perlu memikirkan perangkat keras, infrastruktur, Sistem operasi, dll, cth : Microsoft Azure
3. *Software as Service* : hal ini memfokuskan pada *Web Based Service* dan *Web 2.0*, cth : Google apps, Facebook.

#### *Tipe Layanan Cloud*

Ada tiga tipe layanan *Cloud* yang paling sering diimplementasikan pada saat ini, yaitu :

- *Public Cloud* : Layanan dan sumber daya penyimpanan yang dapat diakses secara umum menggunakan koneksi internet. Karena semua khalayak dapat mengaksesnya maka tipe ini yang paling rentan akan keamanannya.
- *Private Cloud* : Layanan dan sumber daya penyimpanan yang hanya dapat di akses khusus kepada pihak yang berhak, dan biasanya digunakan oleh perusahaan untuk kegiatan-kegiatan yang tertutup, seperti riset, pengembangan produk, produksi produk.
- *Hybrid Cloud* : Layanan yang merupakan gabungan dari *public* dan *private cloud*, sehingga keunggulannya merupakan gabungan dari keunggulan dua tipe tersebut.

## Aspek Keamanan

Teknologi *Cloud Computing* berarti memberi izin data tertentu untuk diletakkan di luar dari jangkauan pemilik data, namun ada saat pemeliharaan perangkat keras maka harus dipastikan pihak yang bertugas tetap dapat menjaga keamanan dan integritas data yang ada dengan ketat. Tantangan baru juga muncul dengan semakin banyaknya pengguna *Cloud Computing*, yaitu:

- *E-commerce* yang membutuhkan kepercayaan dari kedua belah pihak dari penjual dan pembeli ataupun penyedia layanan *e-commerce*.
- Melonjaknya permintaan penggunaan *Cloud Computing* untuk generasi baru, baik dari kalangan konsumen ataupun kalangan bisnis untuk aplikasi yang berbasis *Cloud*, sehingga mendorong generasi berikut dari sekarang untuk mengembangkan secara massive dengan tingkat efisiensi yang tinggi, handal dan aman, dalam rangka untuk memenuhi kebutuhan layanan cloud jutaan pengembang aplikasi berbasis cloud dan miliaran pengguna. Akibat dari dua hal tersebut maka akan terjadi lonjakan kebutuhan akan lahan tempat lokasi data center yang besar, listrik dan juga koneksi internet untuk memenuhi kebutuhan tersebut.

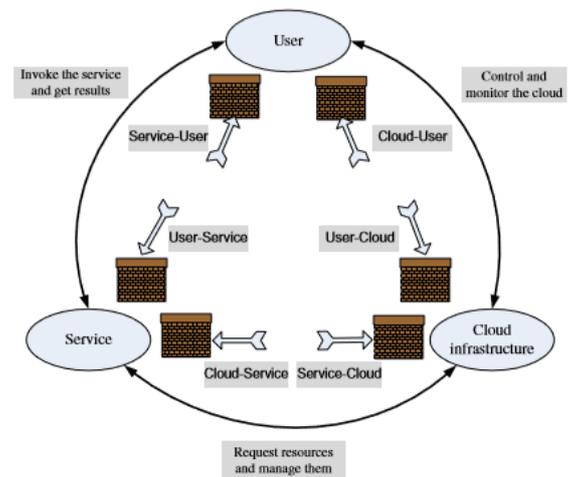
## Keamanan Data

Banyaknya perusahaan-perusahaan besar yang mulai mengadopsi *Cloud Computing* ini mempunyai efek bahwa data-data perusahaan-perusahaan tersebut berarti berada di tempat-tempat yang tidak diketahui lokasi nya secara pasti sesuai dengan posisi *data center* masing-masing layanan, yang berarti data-data yang bersifat sensitif juga tersebar di segala penjuru dunia ini, sehingga akan menyebabkan tantangan tersendiri untuk keamanan data-data tersebut, yaitu :

- Kebutuhan untuk menjaga data bisnis yang bersifat rahasia, data perusahaan dan data pemerintahan.
- Model layanan *Cloud* yang berarti ada kemungkinan menggunakan infrastruktur yang sama dari beberapa pengguna layanan, agar kebocoran data tidak terjadi.
- Dibeberapa Negara seperti Uni Eropa (EU) mempunyai aturan tersendiri mengenai privasi dan integritas data
- Tidak ada standard yang pasti, apakah data-data yang telah di hapus oleh pengguna juga berarti telah benar-benar terhapus dari layanan *cloud*
- Perusahaan *IT Security* dan *Risk Management* akan lebih sulit untuk mendapatkan data-data yang bias mendukung mereka dalam riset
- Ada kemungkinan orang-orang yang tidak bekerja pada suatu perusahaan dapat memiliki akses kontrol data pada suatu perusahaan.

Dengan berkembangnya isu-isu yang berhubungan dengan keamanan data , membuat banyak perusahaan-perusahaan khawatir apakah mereka dapat percaya kepada penyedia layanan *cloud* dalam menjaga keamanan dan integritas data mereka atau kah perlu di membuat suatu sistem kontrol tambahan pada layanan *private cloud*. Ada juga pertimbangan keamanan saat proses perpindahan data dari asal data dalam perusahaan ke penyimpanan *cloud*, dan dengan memastikan tidak adanya data yang hilang atau tertinggal saat proses tersebut berlangsung. Keamanan dan privasi data tetap dan selalu menjadi perbincangan dan pertimbangan untuk layanan *Cloud* ini sehingga baru-baru ini dikenalkan la sistem enkripsi data pada *Cloud Computing*. Untuk menjaga keamanan dan integritas data maka direkomendasikan agar data ditempatkan pada penyimpanan *Cloud* dalam bentuk terenkripsi, dan menjadi

tugas perusahaan untuk memajemen “Key” dari tiap data yang terenkripsi.



Gambar 1 Daerah yang dapat diserang di lingkungan *Cloud Computing* [2]

## Backup Data

Fitur backup ini dikenalkan dan menjadi salah satu solusi dari adanya resiko-resiko yang mungkin terjadi pada layanan *Cloud* jika hal-hal gangguan pada *Data Center* terjadi yang menyebabkan hilangnya data. Fitur backup ini sudah ditawarkan pada pengguna, baik pengguna personal, sampai perusahaan. Bentuk layanan ini biasanya diimplementasikan dengan cara :

- Lokasi backup data biasanya berada pada tempat yang berbeda dengan lokasi penyimpanan awal
- Proses backup otomatis dilakukan secara virtual oleh sistem *Cloud* dengan rentang waktu dari awal pengguna layanan hingga data terbaru.

Namun fitur ini juga menjadi tantangan tersendiri bagi penyedia layanan, yaitu :

- Butuh lokasi lebih untuk menyediakan fitur ini
- Bertambahnya biaya operasional dari semua sisi bisnis

## Resiko Keamanan

Umumnya kekhawatiran pengguna layanan cloud ini adalah apakah data atau infrastruktur telah tersedia secara aman dan *certified*. Meski telah banyak riset-riset dan antisipasi dilakukan untuk menyempurnakan layanan ini tetapi pada praktek nya memiliki resiko yang dihadapi. Berikut beberapa resiko dari layanan *Cloud* ini, yaitu :

- Resiko Keamanan : Persepsi nya bahwa data yang dipercayakan pada penyedia layanan hanya dapat diakses oleh pihak-pihak yang mempunyai otoritas, kehilangan data, ataupun serangan *cyber* yang dapat merusak data.
- Resiko Kompabilitas : *Cloud Computing* yang pada dasarnya masih hal yang baru membuat pengguna enggan menggunakannya secara optimal untuk menggantikan penggunaan sistem yang lama.
- Resiko Ketersediaan : Saat data sudah berada pada penyimpanan *cloud* maka data tersebut sudah berada diluar jangkauan secara fisik, dan jika terjadi gangguan seperti gangguan jaringan internet atau masalah pada data center akan muncul resiko pada saat yang kritis
- Resiko Compliance : Walau pada dasarnya data tersimpan di “awan” namun fisiknya data center tersebar di seluruh penjuru dunia ini, dan dengan adanya regulasi berbeda tiap-

tiap Negara seperti data tidak boleh di simpan di luar dari Negara tersebut.

- Resiko *Lock-In* : Situasi dimana saat pengguna akan berpindah kelayanan lain akan kesulitan untuk mengidentifikasi apa saja kebutuhan agar bisa lebih mengoptimalkan layanan dari teknologi ini.
- Resiko Standarisasi : Belum adanya standard layanan pada *Cloud Computing* ini namun dengan adanya aturan-aturan tersendiri dari penyedia layanan ini, maka pengguna dapat menggunakan layanan ini dengan semakin nyaman.

## KESIMPULAN

- Teknologi Cloud Computing ini menawarkan layanan yang efisien dan memiliki beragam keuntungan dengan bisa menekan low cost di bagian kebutuhan perangkat keras, terhubung dengan sistem penyewaaan yang dilakukan oleh penyedia layanan *Cloud*. Namun di balik itu, keamanan data, *privacy* dan integritas data juga menjadi perhatian paling penting sebelum menggunakan layanan ini. Langkah lain yang dapat dilakukan, yaitu dengan memastikan penyedia layanan *Cloud Computing* ini memiliki standarisasi keamanan dan kerahasiaan data, backup rutin dan juga perusahaan sebaiknya mengenkripsi data-data yang akan disimpan dalam layanan *Cloud* ini.
- Jika keamanan sudah tidak menjadi fokus pada sebuah perusahaan, maka perusahaan tersebut dapat lebih fokus untuk meningkatkan kinerjanya tanpa perlu memikirkan persepsi mengenai keamanan data dan layanan *Cloud*.
- Dari penyedia layanan *cloud* juga ada baiknya sosialisasi terhadap masyarakat untuk mengedukasi pengguna atau calon pengguna, memperbaiki produk dan layanannya, terutama perihal keamanan sehingga pengguna maupun calon pengguna dapat mengoptimalkan layanan Cloud Computing di era *mobile* dan informasi yang serba cepat ini.

## REFERENSI

- [1] Hosam AlHakami, Hamza Aldabbas, and Tariq Alwada'n, "Comparison Between Cloud and Grid Computing: Review Paper", *Journal, IJCCSA*, Leiester, UK, 4 August 2012, pp. 1-21.
- [2] Dan C. Marinescu, *Cloud Computing Theory and Practice*, Morgan Kaufmann, USA, 2013.
- [3] K. Chandrasekaran, *Essentials of Cloud Computing*, Taylor & Francis Group, USA, 2015.