

MANAJEMEN RESIKO PENERAPAN CLOUD COMPUTING DARI SUDUT PANDANG KEAMANAN DATA

Supono

Jurusan Manajemen Informatika
Politeknik Pos Indonesia

Jl. Sariasih No. 54 Bandung 40151, Indonesia Tel. +62-22-200-9570

supono@poltekpos.ac.id

Abstrak

Cloud Computing merupakan mekanisme yang memungkinkan pengguna "menyewa" sumber daya teknologi informasi (*software, processing power, storage, dan lainnya*) melalui internet dan memanfaatkan sesuai kebutuhan pengguna serta membayar sesuai dengan yang digunakan saja. Dengan konsep ini akan memberikan keuntungan bagi organisasi, karena organisasi tidak perlu mengeluarkan biaya operasional, perawatan dan investasi yang besar untuk membeli infrastruktur. Di sisi lain, memberikan manfaat dimana organisasi akan lebih fokus menjalankan bisnis utama mereka.

Selain keuntungan yang ditawarkan, beberapa permasalahan muncul seperti tingkat layanan, privasi dan keamanan data, sehingga perlu ada jaminan bahwa semua stake holder yang ada mendapatkan kepastian akan jaminan layanan yang diberikan. Gartner dalam publikasi khususnya tahun 2008 menyoroti pentingnya keamanan data (*data sensitif*) terkait menilai resiko keamanan pada cloud computing, termasuk permasalahan teritorial hukum dalam penyimpanan data. Di Indonesia sendiri sudah diatur dalam undang-undang Internet dan Transaksi Elektronik (ITE) dan Peraturan Pemerintah No. 82 tahun 2012 terkait data transaksi (*data center*) yang harus disimpan di Indonesia.

Data atau informasi merupakan aset penting dalam sebuah organisasi yang harus dilindungi dan dikelola. Pada makalah ini memberikan penjelasan mengenai resiko pada penerapan cloud computing terutama dalam hal pentingnya keamanan data yang disimpan di 'awan' dalam hal ini penyedia layanan cloud computing, sehingga akan memberikan pertimbangan bagi pengguna atau user dalam memilih model layanan yang diberikan penyedia layanan serta selektif memilih penyedia layanan cloud computing.

Kata Kunci : cloud computing, manajemen resiko, keamanan data, komputasi awan.

Abstract

Cloud Computing is a mechanism that allows users "renting" of information technology resources (software, processing power, storage, and others) via the Internet and utilize according user needs and pay as they used. With this concept will provide benefits for the organization, because organizations do not need to pay for operational, maintenance and investment to buy infrastructure cost. On the other hand, the benefit which the organization will focus on running their core business.

In addition to the benefits offered, some problems arise such as the level of service, privacy and security of data, so it should be no assurance that all existing stakeholders get certainty of assurance services provided. Gartner in particular publication in 2008 highlights the importance of data security (sensitive data) related to assess security risks in the cloud computing, including problems in the legal territorial of data center location. In Indonesia it is set in the law of the Internet and Electronic Transactions (ITE) and Government Regulation No. 82 of 2012 related to the transaction data (data center) to be located in Indonesia.

Data or information is an important asset in an organization that should be protected and managed. In this paper gives a description of the risks in the applying of cloud computing, especially in terms of the importance of the security of the data stored in the cloud computing service providers, so that will give due consideration to the user or the user in selecting a given service model as well as the service providers to selectively choose cloud computing service providers.

Keywords: *cloud computing, risk management, data security.*

I. Pendahuluan

Beberapa tahun terakhir ini, Cloud Computing atau dalam bahasa Indonesia disebut komputasi awan menjadi sebuah model komputasi baru yang memberikan solusi alternatif terhadap kebutuhan komputasi di organisasi, hal ini muncul seiring dengan maraknya aplikasi berbasis elektronik, seperti e-government, e-travel, dan sejenisnya. Penyedia layanan Cloud Computing pun berlomba-lomba menawarkan berbagai model layanan dengan berbagai penawaran yang menarik baik itu dari sudut pandang layanan ataupun dari sudut pandang keamanannya.

John McCarthy, pakar komputasi dari MIT (*Massachusetts Institute of Technology*) yang dikenal juga sebagai salah satu pionir intelegensi buatan pada tahun 1960-an, menyampaikan visinya bahwa "*Suatu hari nanti komputasi akan menjadi infrastruktur publik, seperti halnya listrik dan telepon*" [Philipp, 2011]. Inilah yang menjadi cikal bakal lahirnya *Cloud Computing*. *Cloud Computing* merupakan mekanisme yang memungkinkan pengguna "menyewa" sumber daya teknologi informasi (*software, processing power, storage, dan lainnya*) melalui internet dan memanfaatkan sesuai kebutuhan pengguna dan membayar sesuai dengan yang digunakan saja. Dengan konsep ini, maka organisasi memiliki akses untuk memanfaatkan sumber daya tersebut, karena akan mengurangi biaya operasional, perawatan dan investasi besar-besaran di awal. Di sisi organisasi memberikan manfaat dimana mereka akan lebih fokus untuk menjalankan bisnis utama mereka [Tharam, 2010].

Selain manfaat yang diperoleh dari penerapan Cloud Computing, beberapa hal yang memunculkan resiko harus dianalisis, identifikasi dan dinilai, sehingga penerapan teknologi Cloud Computing sesuai dengan kebutuhan bisnis organisasi dan tidak menimbulkan dampak yang buruk dikemudian hari terhadap organisasi [Spinola, 2009]. Hal yang paling banyak disoroti dalam penerapan teknologi Cloud Computing adalah terkait keamanan data atau informasi, sejauh mana penyedia layanan Cloud Computing memberikan jaminan terkait hak akses data/informasi yang bersifat data sensitif, privasi data, recovery, regulasi, audit keamanan dan standar ISO terhadap penyedia layanan tersebut [Gartner, 2008].

Data atau informasi merupakan aset penting dalam sebuah organisasi yang harus dilindungi dan dikelola. Dari beberapa hal diatas, maka muncul beberapa pertanyaan kritis mengenai resiko penerapan Cloud Computing dan dampaknya dilihat dari sudut pandang keamanan data, antara lain Hal-hal apa saja yang harus diperhatikan dalam penerapan Cloud Computing terkait keamanan data? Bagaimana strategi organisasi untuk meminimalisir resiko atau penanganan manajemen resiko pada saat akan melakukan implementasi penerapan Cloud Computing? Bagaimana agar data atau informasi kita yang disimpan di Cloud aman atau ada terjamin keamanannya.

II. Tinjauan Pustaka

A. Pengertian Cloud Computing

The National Institute of Standards and Technology (NIST) memberikan definisi singkat dan spesifik tentang Cloud computing adalah sebuah mekanisme, dimana sekumpulan IT resource atau sumber daya yang saling terhubung dan nyaris tanpa batas, baik itu infrastruktur maupun aplikasi, dimiliki dan dikelola sepenuhnya oleh pihak ketiga, sehingga memungkinkan customer untuk menggunakan *resource* tersebut secara *on-demand* melalui *network*, baik yang sifatnya jaringan private maupun publik [NIST, 2011].

B. Karakteristik Cloud Computing

NIST telah mendefinisikan 5 karakteristik layanan disebut dikatakan layanan *cloud computing* yaitu (Mell dan Grance, 2011):

1. *On-demand self-service.*
Cloud Consumer bisa mengkonfigurasi secara mandiri layanan yang ingin dipakai melalui sebuah sistem, tanpa perlu interaksi manusia dengan pihak *cloud provider*.
2. *Broad network access.*
Kapabilitas layanan dari *cloud provider* tersedia lewat jaringan internet dan bisa diakses oleh berbagai jenis perangkat, seperti *smartphone*, tablet, laptop, dan *workstation*.
3. *Resource pooling.*
Sumber daya komputasi (*storage*, *CPU*, *memory*, *network bandwidth*, dsb.) yang dikumpulkan oleh penyedia layanan untuk memenuhi kebutuhan banyak pelanggan dengan model *multi-tenant*. Sumber daya komputasi ini bisa berupa sumber daya fisik ataupun *virtual*.
4. *Rapid elasticity.*
Kemampuan dari layanan *cloud provider* bisa dipakai oleh *cloud consumer* secara dinamis berdasarkan kebutuhan. *Cloud consumer* bisa menaikkan atau menurunkan kapasitas layanan.
5. *Measured service.*
Tersedia layanan untuk mengoptimasi dan memonitor layanan yang dipakai secara otomatis. Dengan *monitoring* sistem ini, maka bisa melihat berapa *resources* komputasi yang telah dipakai, seperti: *bandwidth*, *storage*, *processing*, jumlah pengguna aktif.

C. Keuntungan Cloud Computing

Adapun keuntungan atau manfaat dari teknologi *Cloud Computing* ini adalah sebagai berikut (Christopher, 2011):

1. Mengurangi biaya / tanpa investasi awal
Dengan *cloud computing*, konsumen dapat menggunakan sebuah layanan tanpa investasi yang signifikan di awal seperti *server*, aplikasi *server* dan ruangan untuk penyimpanan *server/data center*, serta tak peduli terhadap biaya pemeliharaan.
2. Mengubah CAPEX menjadi OPEX
Dengan *cloud computing*, konsumen dapat melakukan pengeluaran operasional (*Operational Expenditure*, atau OPEX). Jadi, sama persis dengan biaya fasilitas lainnya seperti listrik atau telepon ketika kita cukup membayar bulanan atau tahunan sesuai pemakaian.
3. Fokus pada Bisnis, bukan TI
Dengan menggunakan *Cloud Computing*, organisasi dapat fokus pada bisnis utama perusahaan, dan bukan berkecimpung di dalam pengelolaan TI. Hal ini dapat dilakukan karena pengelolaan TI dilakukan oleh penyedia layanan, dan bukan oleh organisasi itu sendiri.

D. Layanan Cloud Computing

NIST sendiri membagi jenis layanan *Cloud Computing* menjadi tiga sebagai berikut (Mell dan Grance, 2011):

1. *Software as a Service (SaaS)*
SaaS adalah layanan dari *Cloud Computing* dimana pelanggan dapat menggunakan *software* yang telah disediakan oleh *cloud provider*. Pelanggan cukup tahu bahwa perangkat lunak bisa berjalan dan bisa digunakan dengan baik, Contoh: GoogleDocs, Adobe Cloud, YahooMail, LiveMail, Facebook, Skype.

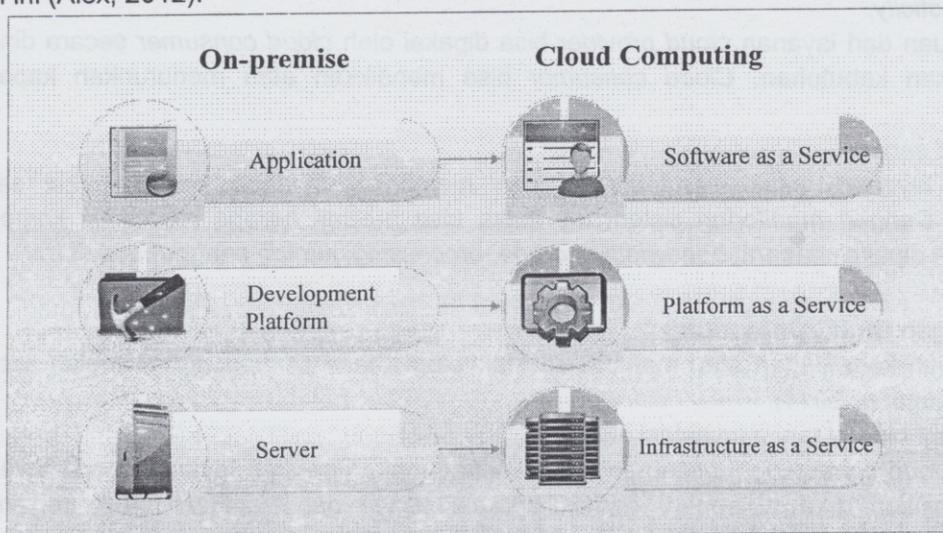
2. Platform as a Service (PaaS)

PaaS adalah layanan dari *Cloud Computing* kita bisa menyewa "rumah" berikut lingkungannya. Pelanggan tidak perlu pusing untuk menyiapkan "rumah" dan memelihara "rumah" tersebut. Yang penting aplikasi yang dibuat dapat berjalan dengan baik. Pemeliharaan "rumah" ini (sistem operasi, *network*, *database engine*, *framework* aplikasi) menjadi tanggung jawab dari penyedia layanan. Contoh: Amazon Web Service.

3. Infrastructure as a Service (IaaS)

IaaS adalah layanan dari *Cloud Computing* sewaktu kita bisa "menyewa" infrastruktur IT (unit komputasi, *storage*, *memory*, *network*). Dapat didefinisikan berapa besar unit komputasi (CPU), penyimpanan data (*storage*), *memory* (RAM), *bandwidth*, dan konfigurasi lainnya yang akan disewa. Contoh: Amazon EC2, Rackspace Cloud, dan Windows Azure

Untuk lebih memudahkan pemahaman mengenai model *cloud computing* dibandingkan dengan bukan *cloud computing*, perhatikan gambar transformasi dari *on-premise* model ke cloud model dibawah ini (Alex, 2012):



Gambar 1: Transformasi on-premise model ke cloud model (Alex, 2012)

E. Deployment Cloud Computing

Menurut NIST, ada empat *deployment model* dari *cloud computing* ini, yaitu (Mell dan Grance, 2011):

1. Public Cloud

Adalah layanan *Cloud Computing* yang disediakan untuk masyarakat umum. Pengguna bisa langsung mendaftar ataupun memakai layanan yang ada. Contoh: GoogleMail, Facebook, Twitter, Live Mail, dsb.

2. Private Cloud

Adalah layanan *cloud computing* yang disediakan untuk memenuhi kebutuhan internal dari organisasi/perusahaan. Biasanya departemen IT akan berperan sebagai *service provider* (penyedia layanan) dan departemen lain menjadi *service consumer*. Sebagai *service provider*, tentu saja departemen IT harus bertanggung jawab agar layanan bisa berjalan dengan baik sesuai dengan standar kualitas layanan yang telah ditentukan oleh perusahaan, baik infrastruktur, *platform*, maupun aplikasi yang ada. Contoh: Mail Server, Database Server untuk keperluan internal, Web Server.

3. Hybrid Cloud

Adalah gabungan dari layanan *Public Cloud* dan *Private Cloud* yang diimplementasikan oleh suatu organisasi/perusahaan. Dalam *Hybrid Cloud* ini, kita bisa memilih proses bisnis mana

yang bisa dipindahkan ke *Public Cloud* dan proses bisnis mana yang harus tetap berjalan di *Private Cloud*.

4. *Community Cloud*

Adalah layanan *Cloud Computing* yang dibangun eksklusif untuk komunitas tertentu, yang *consumer*-nya berasal dari organisasi yang mempunyai perhatian yang sama atas sesuatu/beberapa hal, misalnya saja standar keamanan, aturan, *compliance*. *Community Cloud* ini bisa dimiliki, dipelihara, dan dioperasikan oleh satu atau lebih organisasi dari komunitas tersebut, pihak ketiga, ataupun kombinasi dari keduanya.

F. Data

Menurut Turban et al. (2005, p38), *data adalah deskripsi dasar tentang sesuatu, kejadian, kegiatan, dan transaksi yang ditangkap, direkam, disimpan, dan diklasifikasikan namun tidak terorganisir untuk menyampaikan suatu arti khusus.*

G. Keamanan Data

Keamanan data adalah keadaan dimana data yang berisi kumpulan fakta fakta yang berada dalam keadaan aman tanpa adanya gangguan yang membahayakannya. Meningkatnya kemajuan dalam telekomunikasi perangkat lunak maupun keras yang signifikan sangat memberikan kenyamanan dan kemudahan dalam mengelola suatu data akan tetapi jangan kanget bahwa hal tersebut sangat memberikan kontribusi yang tinggi dalam meningkatkan kerentangan dalam gangguan keamanan data. Keamanan data meliputi keamanan secara fisik, data/file, akses, dan jaringan. Pentingnya keamanan data adalah sebagai berikut:

1. Pentingnya kebutuhan informasi yang dikirim dan diterima oleh pengguna
2. Perlunya kerahasiaan dalam memberi atau menerima informasi
3. Nilai suatu informasi dinilai dari keamanan datanya.
4. Menjaga Integritas data
5. Menghindari penyusupan data

H. Manajemen Resiko

Manajemen risiko adalah suatu proses mengidentifikasi, mengukur risiko, serta membentuk strategi untuk mengelola risiko melalui sumber daya yang tersedia. Manajemen risiko juga dapat diartikan suatu pendekatan terstruktur/metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman; suatu rangkaian aktivitas manusia termasuk: Penilaian risiko, pengembangan strategi untuk mengelolanya dan mitigasi risiko dengan menggunakan pemberdayaan/pengelolaan sumberdaya. Strategi yang dapat diambil antara lain adalah memindahkan risiko kepada pihak lain, menghindari risiko, mengurangi efek negatif risiko, dan menampung sebagian atau semua konsekuensi risiko tertentu (Hopkin, 2004).

III. Manajemen Resiko Keamanan Data Pada Cloud Computing

Adapun hal-hal yang harus diperhatikan dalam keamanan data pada Cloud Computing adalah sebagai berikut:

1. Proteksi Data

Ketika kita sudah memutuskan untuk adopsi atau migrasi data ke Cloud, yang yang diperhatikan adalah bagaimana penyedia layanan Cloud memberikan proteksi terhadap data kita. Dengan metode apa mereka melakukan proteksi sehingga kita yakin data aman, selain itu lokasi penyimpanan data juga adalah pertimbangan penting dimana ini hubungannya dengan Data Center. Dipastikan data center yang mereka buat sudah tersertifikasi/teraudit, misalnya lokasi bebas gempa, standar sumber daya listrik 3 lapis dll.

2. Security Control

Setelah data kita betul-betul terproteksi, selanjutnya adalah bagaimana keamanan dari akses terhadap data kita (role), bagaimana prosedurnya sehingga hanya orang-orang yang berhak saja yang bisa akses data kita. Disini termasuk akses para pekerja/karyawan di penyedia layanan terhadap data kita.

3. Compliance

Standar yang diterapkan pada penyedia layanan Cloud Computing, misalnya untuk keamanan data menggunakan ISO 27001, untuk penyediaan layanan memakai ITIL, COBIT, Cloud Security Alliance, termasuk regulasi internasional dan pemerintah. Sehingga jika ada pelanggaran akan mudah dalam penyelesaian

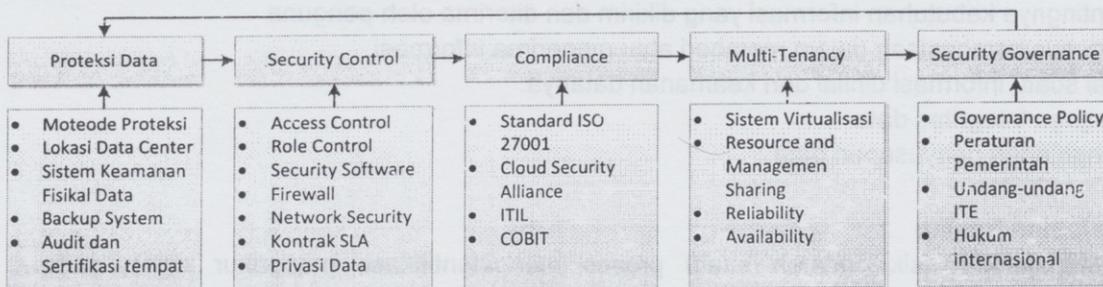
4. Multi-tenancy

Salah satu sifat Cloud computing adalah resource sharing, nah bagaimana ketika ada penyewa lain terdapat melakukan kecurangan atau bocor, apa imbasnya terhadap data kita disana, ini harus dipertimbangkan. Karena secara fisik, data kita bisa jadi ada dalam satu media fisik yang sama dengan yang lain.

5. Security Governance

Ini lebih kepada policy governance dari penyedia layanan atau kita sebagai pemakai layanan, harus dijabarkan dan governance-nya paka apa harus didefinisikan disini.

Kelima hal diatas dapat digambarkan seperti dibawah ini:



Gambar 2: Hal-hal yang Harus Diperhatikan Penerapan Cloud Computing Terkait Keamanan Data

Berikut ini adalah strategi meminimalisir pengelolaan/manajemen resiko keamanan data pada Cloud Computing dari pertimbangan dari hal-hal yang harus diperhatikan diatas, berikut ini adalah langkah-langkahnya, Terdapat enam langkah proses penerapan Cloud Computing, yaitu (Wyld, 2009):

1. Langkah 1: Belajar

Strategi awal dimulai dengan memperkaya wawasan yaitu belajar tentang dasar-dasar Cloud Computing, dengan cara menghadiri seminar/workshop, *networking*, komunikasi dengan vendor/konsultan, dan membaca. Mengertai bagaimana komunikasi data, dan seperti apa data diperlakukan di Cloud.

2. Langkah 2: Menilai Organisasi

Menyesuaikan kebutuhan organisasi dengan layanan yang ada pada Cloud, termasuk menganalisis data yang bersifat sensitif dan aktor yang terlibat nantinya sesuai dengan peran aktor masing-masing.

3. Langkah 3: Cloud Pilot

Membuat sebuah proyek kecil sebagai bahan awal study, misalnya pada awalnya hanya departemen sumber daya manusia yang menerapkan teknologi Cloud, sehingga nanti akan

RANCANG BANGUN SISTEM INFORMASI MANAJEMEN PENERIMAAN BARANG PADA GUDANG MENGUNAKAN METODE BERORIENTASI OBJEK

Viridiandry Putratama, ST ¹⁾, Mubassiran, S.Si.,MT ²⁾
Program Studi Manajemen Informatika, Politeknik Pos Indonesia
¹⁾viridi@poltekpos.ac.id, ²⁾mubassiran@poltekpos.ac.id

Abstrak

Gudang dan pergudangan merupakan salah satu bagian penting dari seluruh proses pabrik. Posisinya berpengaruh besar terhadap lancar tidaknya mekanisme kegiatan unit lain dalam pabrik. Gudang juga memiliki peran penting guna mendukung keberhasilan perusahaan dalam mencapai tujuannya, karena pada bagian gudang ini terjadi proses input(*inbound*)menjadi output(*outbound*). Dalam pengolahan input menjadi output, operasional pergudangan harus berjalan dengan baik. Beberapa hal penting dalam penerimaan barang adalah pertama, bukti pemesanan (*Purchase Order- PO*) barang dari gudang. maka yang kedua dibuat bukti tanda terima barang. Bukti ini digunakan sebagai dasar oleh pihak *supplier* untuk melakukan penagihan ke pemesan barang. Ketiga, pemeriksaan bukti pemesanan dengan fisik barang, dan Keempat, penempatan barang di Rak. Penelitian ini berfokus kepada rancang bangun sistem informasi manajemen gudang untuk modul yang terkait dengan proses bisnis penerimaan barang pada gudang dan penempatan barang. Sistem Informasi ini akan dikembangkan dengan menggunakan Platform .Net dengan bahasa Visual Basic dan dapat digunakan secara bersama oleh beberapa *Business User* dalam lingkungan intranet. Diharapkan dengan adanya sistem informasi ini dapat terjadi sinergitas proses bisnis mulai dari *Purchase Order*, penerimaan barang hingga penyimpanan barang dan penempatan barang di lokasi gudang. Hasil penelitian ini adalah suatu sistem informasi terintegrasi untuk penerimaan barang pada sebuah gudang berbasis *Client Server*.

Abstract

Warehouse and warehousing is one important part of the whole process of the plant. Current position greatly affect whether mechanisms other unit activities in the factory. Warehouse also has an important role to support the company's success in achieving its objectives, as is the case in the warehouse input process (*inbound*) into outputs (*outbound*). In processing the input to output, warehousing operations should run well. Some important things are in receipt of the goods first, proof of booking (*Purchase Order- PO*) of goods from the warehouse. the second made goods. This evidence is used as a basis by the supplier to collect the goods to the buyer. Third, examination of physical evidence by ordering goods, and Fourth, the placement of goods on the shelf. This study focuses on the design of information systems for the warehouse management module associated with the business processes of receipt of goods in the warehouse and item placement. This information system will be developed using the Platform Net with Visual Basic language and can be used jointly by several Business Users within an intranet environment. Hopefully with this information the system can occur synergy of business processes ranging from purchase orders, ceipt of goods to storage location and placement of goods in the warehouse. The result of this study is an integrated information system for the receipt of goods in a warehouse-based Client Server.