RISK ASSESSMENT PADA MANAJEMEN RESIKO PENERAPAN TEKNOLOGI *CLOUD COMPUTING* BAGI PEMERINTAH DAERAH

Eka Wahyu Hidayat

Magister Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
Jl. Ganesha. No.10 Bandung
kawahyu@yahoo.com

Abstrak

Seiring dengan meningkatnya frekuensi kebutuhan layanan komputasi dalam organisasi yang semakin komplek, inovasi-inovasi untuk mempermudah penataan dan pengelolaan sumber daya TI di organisasi terus bermunculan. Adanya teknologi *Cloud Computing* memberikan harapan untuk mengoptimalkan layanan TI, infrastruktur TI, dan biaya. Berdasarkan Inpres No. 3/2003 tentang Kebijakan dan Strategi Nasional tentang Pengembangan e-Government, ada ketertarikan dari pemerintah untuk mengadopsi teknologi *Cloud Computing* ini. Dengan beragamnya infrastruktur dan sumber daya TI di daerah, perlu dilakukan analisis menyeluruh, misalnya analisis terhadap manajemen resiko sebelum pemerintah benar-benar akan mengadopsi dan menerapkan teknologi baru ini. Penilaian resiko atau *Risk Assessment* adalah salah satu langkah awal yang bisa dilakukan. Tujuannya adalah untuk mengidentifikasi resiko-resiko yang mungkin muncul dalam penerapan teknologi *Cloud* ini. Dengan mengacu pada *Risk Management Guide for Information Technology Systems* yang dikembangkan oleh The *National Institute of Standards and Technology* (NIST), diharapkan dalam makalah ini menghasilkan usulan manajemen resiko yang bisa dilakukan terhadap implementasi teknologi *Cloud.*

Kata kunci : Teknologi *Cloud Computing*, manajemen resiko, *Risk Assessment*, NIST

1. Pendahuluan

Peran Teknologi Informasi (TI) dalam organisasi saat ini sangat penting sekali, dimana tingkat ketergantungan dunia usaha, badan-badan pemerintahan, dan organisasi, terhadap TI semakin tinggi. TI digunakan sebagai sarana untuk meningkatkan keunggulan kompetitif suatu organisasi melalui efektifitas dan efisiensi dalam otomasi, pengolahan, dan manipulasi data. Seiring dengan meningkatnya frekuensi kebutuhan layanan komputasi dalam organisasi yang semakin komplek, inovasi-inovasi untuk mempermudah penataan dan pengelolaan sumber daya TI di organisasi terus bermunculan. Hal ini dibuktikan dengan munculnya berbagai alternatif teknologi yang bisa di adopsi untuk mencapai tujuan organisasi yaitu mempercepat dan mempermudah pekerjaan, misalnya di bidang pemerintahan telah mengadopsi aplikasi e-*Government* yang memanfaatkan jaringan internet dalam mendukung proses bisnis pemerintahan dan layanan publik.

Adanya Inpres No. 3/2003 tentang "Kebijakan dan Strategi Nasional tentang Pengembangan e-Government" yang bertujuan: Pengembangan e-government merupakan upaya untuk mengembangkan penyelenggaraankepemerintahan yang berbasis (menggunakan) elektronik dalam rangka meningkatkan kualitas layanan publik secara efektif dan efisien. Melalui pengembangan e-government dilakukan penataan sistem manajemen dan proses kerja di lingkungan pemerintah dengan mengoptimasikan pemanfaatan teknologi informasi. Pemanfaatan teknologi informasi tersebut mencakup 2 (dua) aktivitas yang berkaitan yaitu: 1) pengolahan data, pengelolaan informasi, sistem manajemen dan proses kerja secara elektronis; 2) pemanfaatan kemajuan teknologi informasi agar pelayanan publik dapat diakses secara mudah dan murah oleh masyarakat di seluruh wilayah negara [1].

Cloud Computing adalah teknologi bidang TI yang memanfaatkan jaringan internet berupa model komputasi dimana sumberdaya-sumberdaya seperti *storage*, *processor*, *network*, dan *software* menjadi abstrak dan dijadikan sebagai layanan di jaringan menggunakan pola *remote access*. Konten yang ditawarkan seperti *software as a service* (SaaS), *platform as a service* (PaaS), dan *infrastructure as a service* (IaaS) menjadi solusi TI yang praktis dan ekonomis. Sifat jangkauan layanan terbagi menjadi *Public Cloud*, *Private Cloud*, dan *Hybrid Cloud.* Ini adalah salah satu inovasi bidang TI terkini yang sejak tahun 2005 di tingkatkan kemampuannya sehingga bisa mendukung aplikasi e-*Government* dan diharapkan dengan mengadopsi teknologi ini untuk bidang pemerintahan dapat mengurangi biaya investasi TI, meningkatkan produktivitas pegawai, dan meningkatkan pelayanan pemerintah kepada masyarakat sekaligus mampu menyelaraskan proses

bisnis dengan unit pemerintahan lainnya sehingga tercipta efektifitas dan efisiensi operasional pemerintahan. Keuntungan yang dapat diperoleh bagi pemerintah dalam mengadopsi *CloudComputing* adalah ***A clean government with no corruption*** dimana Sistem SOA (*Service Oriented Architecture*) pada *cloudcomputing* yang memungkinkan kolaborasi otomatis di antara *software* yang dimiliki dunia bisnis dengan *software* yang dimiliki pemerintah memungkinkan semua transaksi yang berhubungan dengan pemerintah dilakukan tanpa campur tangan manusia seperti perhitungan dan pembayaran pajak. Hal ini akan menghilangkan korupsi yang biasanya bisa terjadi karena terlibatnya begitu banyak manusia atau petugas didalam proses tersebut, selain itu keuntungan lainnya bagi pemerintah adalah ***A more responsive government services*** dimana setiap warga negara bisa mengakses pelayanan secara *online* dari mana dan kapan saja sehingga dapat meningkatkan kualitas pelayaran pemerintah.

Dengan adanya Inpres tersebut diatas semakin menguatkan alasan perusahaan layanan *Information Communication Technology* (ICT) tanah air untuk menggarap dan memberikan layanan *Cloud Computing* untuk pemerintahan, salah satunya adalah Telkom, perusahaan BUMN yang bergerak di bidang telekomunikasi. Melalui layanan G-Cloud, Telkom berharap dapat membantu efektifitas dan efisiensi operasional pemerintahan. G-Cloud merupakan sebuah layanan ICT yang bersifat *complete*, *affordable* dan *simple* yang menyediakan media untuk meng-kolaborasikan melalui Telkom Collaboration antara modul aplikasi e-Government dan Portal Pemerintahan dalam model *Cloud Computing*. G-Cloud dilengkapi dengan 12 aplikasi e-Goverment penyelenggaraan pemerintahan di daerah yang telah memenuhi kriteria yang ditetapkan Menkominfo. Telkom menargetkan layanan G-Cloud meliputi 87 kota, 348 kabupaten, 5.224 kecamatan dan 6.890 kelurahan di Indonesia [2]. Berdasarkan informasi dalam Konferensi e-Indonesia Initiatives (e-II) Forum VII 2011 yang bertempat di kampus ITB tanggal 14-15 Juni 2011, pemerintah Jawa Barat adalah salah satu provinsi di Indonesia yang akan ikut mengadopsi layanan ini.

2. Permasalahan

Meskipun pemerintah daerah sudah menetapkan tujuannya untuk mengadopsi teknologi *cloud*, perlu disadari bahwa adopsi yang dilakukan tidak semudah yang dibayangkan. Perlu pertimbangan dan analisis menyeluruh mengenai adopsi ini karena adopsi teknologi *cloud* akan melibatkan pihak ketiga (*outsourcing*) sebagai penyedia layananan.Sifat dari layanan yang diberikan yaitu *multi-tenant* maka akan ada banyak pelanggan dalam satu *platform*sehingga kemampuan untuk kustomisasi akan menjadi terbatas.

Implementasi *Cloud Computing* memiliki keuntungan dan juga memiliki resiko yang harus dihadapi saat implementasi. Pihak yang terkait dan terlibat implementasi *cloud* perlu melakukan serangkaian tindakan yang mendukung keberhasilan penerapan *cloud computing* di organisasi. Aspek-aspek resiko yang mungkin timbul saat implementasi *cloud* seperti *Service Level*, *Privacy*, *Compliance*, *Data Ownership*, *Data Mobility* perlu dikelola dengan baik melalui manajemen resiko.

Oleh karena itu dalam makalah ini akan dibahas mengenai:

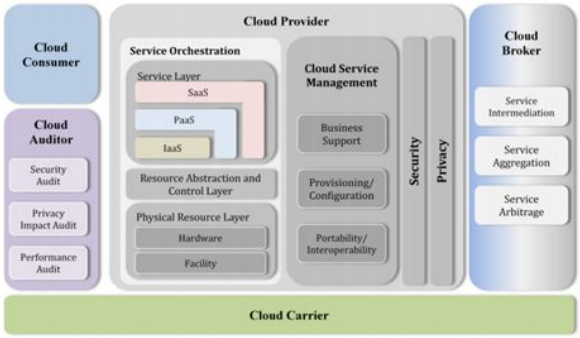
- Melakukan *Risk Assessment* atau penilaian resiko terhadap penerapan teknologi *Cloud Computing*bagi pemerintahan daerah menggunakan rekomendasi penilaian resiko yang disarankan oleh *National Institue of Standards and Technology* (NIST).
- Mendefinisikan karakteristik sistem pada teknologi *Cloud.*
- Melakukan identifikasi ancaman yang mungkin muncul saat implementasi teknologi *Cloud.*
- Melakukan identifikasi kelemahan dari teknologi *Cloud.*
- Memberikan usulan manajemen resiko yang bisa dilakukan terhadap implementasi teknologi *Cloud.*

3. Landasan Teori

Dalam landasan teori pada makalah ini akan dijelaskan secara ringkas mengenai materi yang terkait dengan topik makalah yaitu *Cloud Computing*, Manajemen Resiko, dan *Risk Assessment.*

3.1 *Cloud Computing*

Cloud Computing di definisikan sebagai sebuah model yang memungkinkan kenyamanan, akses on-demand terhadap sekumpulan sumber daya komputasi (seperti jaringan, server, media penyimpanan, aplikasi, dan layanan komputasi) yang konfigurasinya dapat dilakukan dengan cepat dan hanya memerlukan sedikit usaha untuk mengelola dan berhubungan dengan penyedia layanan [3].

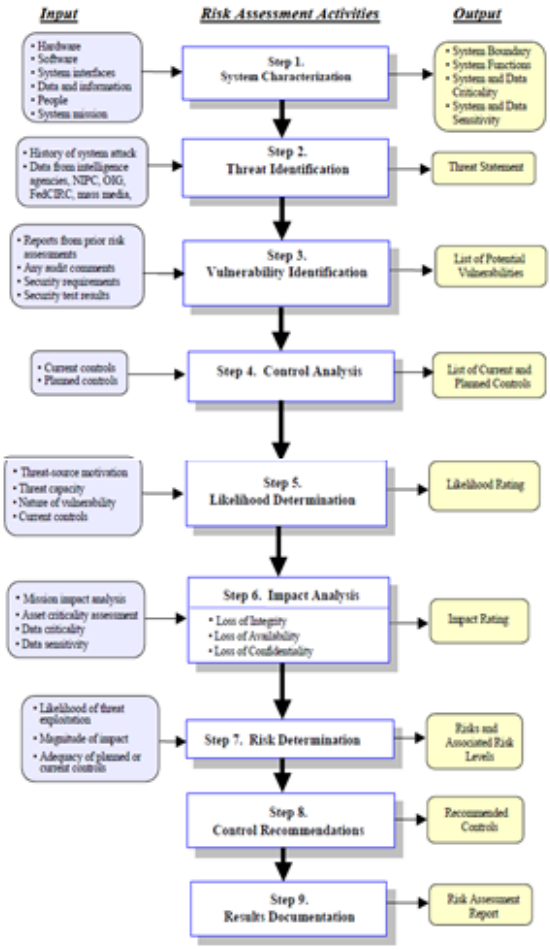


Gambar 1. Arsitektur Cloud Computing

3.2 Manajemen Resiko

Secara umum risiko dapat diartikan sebagai suatu keadaan yang dihadapi seseorang atau perusahaan dimana terdapat kemungkinan yang merugikan. Resiko adalah suatu umpan balik negatif yang timbul dari suatu kegiatan dengan tingkat probabilitas berbeda untuk setiap kegiatan. Pada dasarnya resiko dari suatu kegiatan tidak dapat dihilangkan akan tetapi dapat diperkecil dampaknya terhadap hasil suatu kegiatan. Proses menganalisa serta memperkirakan timbulnya suatu resiko dalam suatu kegiatan disebut sebagai manajemen resiko [4].

Manajemen Resiko terdiri dari 3 proses yaitu, 1) *Risk Assessment*, 2) *Risk Mitigation*, 3) *Evaluation And Assessment*. Manajemen resiko adalah proses yang dilakukan para Manajer TI untuk menyeimbangkan kegiatan operasional dan pengeluaran biaya keuangan, dalam mencapai keuntungan dengan melindungi sistemIT dan data yang mendukung misi organisasinya [5].



Gambar 2. Aktifitas Risk Assessment

3.3 *Risk Assessment*

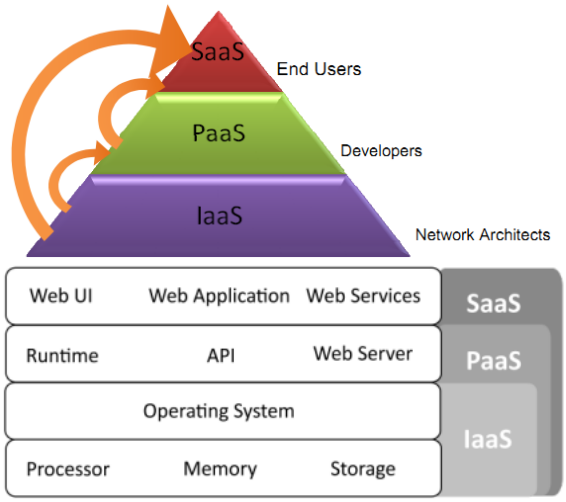
Risk Assessment atauPenilaian Resiko adalah proses pertama yang harus dilakukan dalam metodologi manajemen resiko. *Risk Assessment* digunakan untuk menentukan ancaman potensial dan resiko. Hasilnya adalah identifikasi kendali yang sesuai untuk mengurangi atau menghilangkan resiko, Proses ini terdiri dari 9 langkah, seperti yang diperlihatkan pada gambar 2 [5].

4. Pembahasan

Dalam pembahasan makalah ini, sebagaimana yang dijelaskan sebelumnya yaitu penilaian resiko akan mengikuti langkah-langkah yang disarankan oleh NIST, dengan pembahasan sebagai berikut:

4.1 *System Characterization*

Untuk menetapkan karakteristik sistem *Cloud Computing*, maka perlu dilihat terlebih dahulu dari layanan yang diberikannya yaitu *software as a service* (SaaS), *platform as a service* (PaaS), dan *infrastructure as a service* (IaaS). IaaS berisi perangkat keras (*Processor*, *memory*, *storage*) dan sistem operasi yang merupakan antarmuka antara CPU dengan perangkat menjadi sebuah paket layanan. Layanan ini digunakan oleh konsumen melalui jaringan internet secara remote. PaaS memungkinkan developer untuk membangun suatu aplikasi diatas suatu platform yang dapat dikostumisasi sehingga spesifikasi perangkat Client tidak menjadi masalah untuk membangun dan menjalankan aplikasi dengan performansi apapun. SaaS merupakan layanan dimana pengguna dapat mengeksekusi suatu aplikasi tanpa perlu menginstal aplikasi tersebut, aplikasi yang dibutuhkan telah tersedia di vendor dan dapat diakses melalui jaringan internet [6].



Gambar 3. Services Model dan Layer

Dari layanan yang dapat diberikan oleh *Cloud* maka dapat diketahui karakteristik dari sistem yaitu [5]:

1. *On-demand Self Service*, pengguna dapat menambah dan mengatur layanan tanpa intervensi siapapun.

2. *Ubiquitous Network Access*, layanan *cloud* diakses dengan bantuan internet menggunakan mekanisme dan protokol standardan dapat diakses setiap waktu.
3. *Resource Pooling*, sumberdaya *cloud* yang digunakan untuk layanan *cloud* menggunakan infrastruktur yang homogen dan layanan digunakan bersama dengan pengguna lain.
4. *Rapidly Elasticity*, sumber daya harus dapat ditingkatkan dengan cepat dan elastis.
5. *Measures Services*, sumberdaya dan layanan harus diukur, dukungan optimasi penggunaan sumber daya, memberikan laporan penggunaan dan harus memiliki model bisnis *pay-as-you-go* atau dibayar saat digunakan.

4.2 *Threat Identification*

Cloud Security Alliance [7] mendefinisikan beberapa ancaman dalam teknologi *Cloud* yaitu:

1. *Abuse and Nefarious Use of Cloud Computing*, penyalahgunaan teknologi *cloud* dimana ada kemungkinan terjadinya penyusupan terhadap layanan melalui kegiatan Hacking. Ini bisa terjadi karena layanan IaaS yang ditawarkan tanpa batas terhadap jaringan dan storage sering bersinggungan dimana siapapun yang membayar dengan cara legal ataupun illegal dapat memanfaatkan layanan. Beberapa vendor *cloud* bahkan menyediakan layanan percobaan secara gratis untuk periode waku tertentu. Celah ini dapat dimanfaatkan oleh orang dengan anonimitas yang tidak berkepentingan terhadap layanan untuk melakukan penyalahgunaan layanan *cloud.*
2. *Insecure Interface and APIs*, ketidakamanan antarmuka dan API karena layanan *cloud* tergantung pada keamanan dan ketersediaan layanan umum dari API dasar. Proses otentikasi, akses kontrol, dan log harus dirancang sedemikian rupa sehingga setiap proses selalu melalui *policy* yang ditetapkan.
3. *Malicious Insiders*, ancaman dari orang dalam dimana vendor sebagai penyedia layanan bisa diakatakan sebagai *outsourcing* dari perusahaan yang menyewa layanan. Adanya konvergensi layanan TI dan tidak adanya transparansi akan menyulitkan bagi perusahaan memonitor kegiatan yang dilakukan vendor terhadap asset fisik dan virtual.
4. *Shared Technology Issues*, isu penggunaan teknologi bersama dimana vendorIaaSmemberikan layananmereka dengan cara berbagi infrastruktur.Seringkali, komponen dasaryang membentukinfrastruktur ini(misalnya, CPU cache,GPU) tidak dirancang dengan sifatisolasiyang kuat untukarsitektur multi-penyewa.Kompartementalisasiyang kuatharus digunakanuntuk memastikan bahwa pelangganindividu tidakmempengaruhi operasipenyewalain yang berjalan padavendor *cloud*yang sama.Pelanggan tidakmemiliki akses kedata penyewalain.
5. *Data Loss or Leakage*, kehilangan dan kebocoran datadimana ada banyak carauntuk mengeloladata.Contohnya adalah penghapusanatau perubahandata tanpabackup data darikonten asli. Diperlukan adanya pencegahan untuk mengakses data-data sensitif oleh orang yang tidak berkompeten terhadap data tersebut.
6. *Account or Service Hijacking*, pembajakan account dan layananbukan hal baru. Aktifitas ini sudah ada sejak layanan internet ada. Maka aktifitas yang samapun dapat terjadii di layanan *cloud.*
7. *Unknown Risk Profile*, profil resiko yang tidak diketahui dimana salah satu prinsipdarikepemilikanperangkat *Cloud Computing*adalah pengurangan penggunaan perangkat lunak dan perangkat keras, sehingga perusahaan lebih fokus ke kekuatan usaha bisnis mereka tanpa harus mengelola infrastruktur IT dan proses pemeliharaannya. Faktor keamanan tetap menjadi hal utama yang harus diperhatikan dalam layanan *Cloud.*

Dari definisi diatas, maka dapat diidentifikasi ancaman yang mungkin timbul pada teknologi *Cloud* sebagaimana ditunjukkan oleh tabel 1, sebagai berikut

Threat Source	Motivation	Threat Action
Hacker	*Data burglary, Data hijacking, Data destruction*	*Information bribery, Spoofing System Intrusion, Fraud, Computer crime, DDOS, Launching dynamic attack points, Botnet command and control, Building rainbow tables*
User anonymity	*Thef of data*	*Spoofing, Hosting malicious data, Botnet command and control, Backdoor Trap, Sniffing*
Internal outsourcing	*Hacking hobies, Organized Crime, Corporate Espionage, Sponsored Intrusion*	*Hacking, Monitoring, Accessing asset, Data Modification*

Tabel 1. *Threat Identification*

4.3 *Vulnerability Identification*

Dari hasil identifikasi ancaman, selanjutnya dilakukan *vulnerability identification*atau mengidentifikasi kelemahan dari teknologi *Cloud*. Dalam pembahasan ini materi yang diuji diambil dari hasil identifikasi ancaman dimana ancaman yang teridentifikasi merupakan kelemahan dari sistem pada layanan *Cloud*sebagai berikut:

Vulnerability	Threat Action
Abuse and Nefarious Use of Cloud Computing	Pendaftaran dan proses validasi yang ketat, Meningkatkan pemantauan dan koordinasi terhadap penipuan kartu kredit, Instropeksi komprehensif lalu lintas jaringan pelanggan, Pemantauan publik blacklist.
Insecure Interface and APIs	Menganalisa kelayakan model keamanan antarmuka layanan, Otentikasi dan kontrol akses dalam transmisi yang terenkripsi
Malicious Insiders	Supply chain management yang ketat, Melakukan kontrak secara hukum terhadap outsourcing sebagai penyelenggara layanan dalam hal ini vendor penyedia layanan, Transparansi dalam keamanan informasi secara keseluruhan, Memberikan dan meminta pelaporan pelanggaran keamanan.
Shared Technology Issues	Melakukan instalasi dan konfigurasi secara aman, Pemantauan lingkungan terhadap perubahan yang tidak sah, Audit konfigurasi
Data Loss or Leakage	Menerapkan control akses API yang ketat, Menjaga integritas data dalam jalur dengan enkripsi.
Account or Service Hijacking	Memperkerjakan pemantauan proaktif untuk mendeteksi aktivitas yang tidak sah.
Unknown Risk Profile	Disahkannya pengungkapan log aktifitas dan data, pemantauan informasi.

Tabel 2. *Vulnerability Identification*

4.4 *Risk Management Option*

Berdasarkan hasil pencarian yang dibahas sebelumnya, dengan melihat karakteristik sistem, hasil identifikasi ancaman, dan identifikasi kelemahan, maka dapat dibuat suatu rekomendasi yang dapat dijadikan bahan pertimbangan oleh Pemerintah Daerah dalam mengadopsi teknologi *Cloud*, sebagai berikut [8]:

1. Tidak menempatkan data-data yang bersifat sensitif dalam layanan *cloud*.
2. Untuk data-data yang bersifat kritis, harus dilakukan pengamanan ekstra pada saat data dikirimkan, saat data berada dalam jaringan, dan pada saat data berada dalam layanan*cloud* dengan cara otentikasi, validasi, dan enkripsi.
3. Setiap dokumen dalam layanan *cloud* sebaiknya disertai *Digital Signature*, untuk memberikan keyakinan bahwa dokumen tersebut aman.
4. Pengguna layanan *cloud* harus memahami secara jelas dan mendalam tentang kemampuan dan stabilitas dari vendor penyedia layanan *cloud.*
5. Memiliki alternatif kesiapan untuk menangani gangguan layanan melalui layanan *backup* data pada layanan *cloud* yang lain.
6. Memahami pasal-pasal yang relevan dalam kontrak perjanjian penggunaan layanan *cloud.*
7. Jika pelanggan tidak puas dengan layanan *cloud* dari vendor atau jika vendor menghentikan layanannya, maka biaya dan waktu peralihan harus dibicarakan dalam SLA (*Service Level Agreement*)
8. Adanya jaminan kemanan untuk transisi data, langkah-langkah keamanan, dan protokol yang dibicarakan dan dicantumkan dalam SLA (*Service level Agreement*).

5. Simpulan dan Saran

Pembahasan dalam makalah ini menitikberatkan pada tiga langkah dalam *Risk Assesment* yaitu: *System Characterization*, *Threat Identification*, dan *Vulnerability Identification*. Hasilnya adalah adanya gambaran mengenai bagaimana karakteristik dari sistem *cloud*, apa saja ancaman yang ada dalam teknologi *cloud*, dan kelemahan apa yang ada dalam teknologi ini.

Layanan yang diberikan dalam *cloud* sebenarnya sama saja seperti layanan yang ada di internet, yang membedakannya adalah dalam layanan *cloud* semua infrastruktur dan aplikasi yang seharusnya ada di sisi *Client*, kini semuanya berada di sisi *Server*. Artinya, pengguna cukup menyediakan infrastruktur untuk mengakses internet agar bisa terhubung dalam layanan *cloud* untuk menggunakan berbagai aplikasi yang ditawarkan. Karena sifatnya yang *Multi-Tenant* atau penggunaan beragam layanan secara bersama dalam satu *platform*, maka teknologi ini memiliki beberapa kelemahan.

Kelemahan yang paling penting untuk diperhatikan adalah masalah keamanan. Oleh karena itu, ada beberapa hal yang harus diperhatikan oleh pemerintah daerah apabila ingin mengadopsi teknologi untuk layanan publik, yaitu:

1. Menentukan layanan apa saja yang akan digunakan di *cloud*yang dapat mendukung proses bisnis dan layanan publik yang optimal.
2. Menentukan data apa saja yang layak dan aman untuk disimpan dan digunakan dalam layanan *cloud.*

3. Memiliki sumber daya manusia yang mengerti teknologi *cloud* dan layanannya.
4. Memiliki alternatif penanganan masalah apabila sewaktu-waktu ada gangguan dalam layanan dan mempersiapkan opsi apabila vendor menghentikan layanannya.

Daftar Pustaka:

[1] http://www.bappenas.go.id/node/133/2173/inpres-no3-tahun-2003-tentang-kebijakan-dan-strategi-nasional-pengembangan-e-governmet/. Diakses: 1-4-2012.

[2] http://www.wartaegov.com/berita-1365-cloud-computing-untuk-pemerintahan-yang-efektif.html. Diakses: 1-4-2012.

[3] Mell, P., Grance, T., (2009). The NIST Definition of Cloud Computing. from NIST Information Technology Laboratory: http:// www.nist.gov/itl/cloud/upload/cloud-defv15.pdf. Diakses: 2-4-2012.

[4] Bonham, Stephen S., (2005), IT Project Portfolio Management, Artech House, Boston.

[5] Stoneburner, G., Alice Goguen and Alexis Feringa, Risk Management Guide for Information Technology Systems, Recommendation of The National Institute of Standards and Technology Special Publication 800-30, July, 2002.

[6] Fardani, A., Surendro, K., (2011), Strategi Adopsi Teknologi Informasi Berbasis Cloud Computing Untuk Usaha Kecil dan menengah di Indonesia, Seminar Nasional Aplikasi Teknologi Informasi (SNATI 2011)

[7] Cloud Security Alliance, (2010), Top Threat to Cloud Computing V1.0, csathreat.v1.0.pdf http://www.cloudsecurityalliance.org/topthreats Diakses: 2-4-2012.

[8] Cloud Computing: Benefits, Risks and Recommendations for Information Security, (2009), http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment, Diakses: 3-4-2012.