PERTIMBANGAN UMUM KEAMANAN PADA MOBILE COMPUTING

Zen Munawar, S.T, S.Kom., M.Kom
Dosen Tetap Prodi Manajemen Informatika
Politeknik LP3I Bandung
E-mail: munawarzen@gmail.com

Abstrak : Kegunaan perangkat *mobile* telah meningkat sangat dalam beberapa tahun terakhir, pengguna memungkinkan untuk melakukan lebih banyak tugas di perangkat *mobile*. *Mobile Computing* adalah penggabungan elemen jaringan *mobile* dan *computing*.

Aplikasi *mobile* dan teknologi komputasi saat ini telah berkembang sangat pesat yang menawarkan layanan yang optimal bagi pengguna *mobile*, juga menunjang mobilitas dan skalabilitas Makalah ini menyajikan ulasan mengenai latar belakang dan prinsip-prinsip *mobile computing*, *mobile cloud computing,* arsitektur dan tantangan bersama dengan solusi yang memungkinkan. Keamanan pengguna mobile computing, integritas data serta aplikasi menjadi salah satu isu yang perlu diperhatikan oleh penyedia jaringan mobile.

Makalah ini juga membahas isu-isu keamanan yang berbeda yang muncul tentang seberapa aman lingkungan *mobile computing*. Daftar pertimbangan untuk keamanan diidentifikasi perlu dibahas, dipahami dan terakhir menilai risiko yang berkaitan.

Kata kunci : jaringan *mobile*, masalah keamanan , *mobile computing mobile cloud computing,*

1. Pendahuluan

Industri Teknologi Informasi pernah fenomenal dengan penemuan revolusioner sejak adanya komputer generasi pertama. Pada enam dekade terakhir tujuan dari komputer untuk melakukan tugas yang berbeda dan aplikasi menjadi berubah, perbedaan yang mencolok adalah bahwa saat ini tugas dilakukan menjadi lebih murah, cepat dan portabel. Konsumen dapat menggunakan layanan dan aplikasi yang tersedia di perangkat *mobile* melalui koneksi internet jaringan *mobile*. Mobilitas / ada dimana-mana adalah fitur utama dari jaringan ini Dengan demikian, kombinasi dari perangkat elektronik seperti *smartphone*, PDA, tablet PC, jaringan *mobile*, sumber daya berkumpul bersama-sama yang muncul sebagai bidang baru penunjang *mobile computing*.

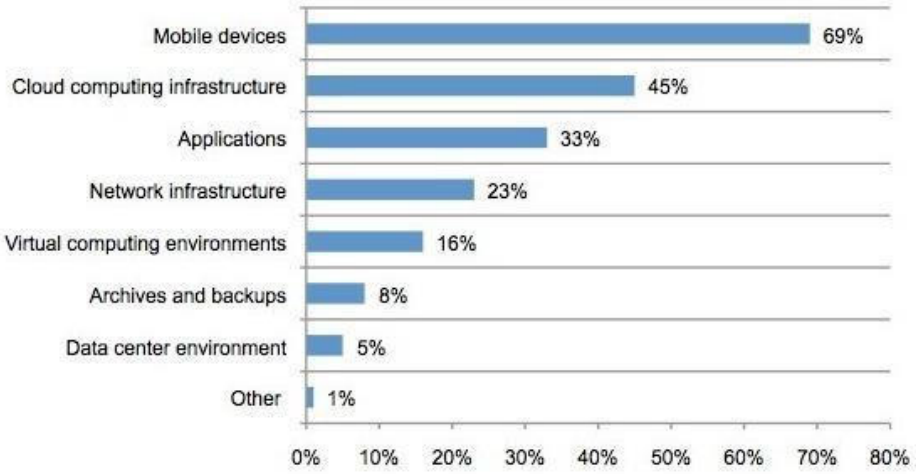
Banyaknya pengguna yang menyimpan informasi baik di perangkat *mobile* atau di server *cloud*, maka akan semakin rentan terhadap serangan dan ancaman internet. Keunggulan aplikasi *mobile computing* untuk mendapatkan akses cepat dan meningkatnya sumber daya infrastrukur dengan biaya yang lebih kecil akan berdampak kepada pengguna menjadi lebih beresiko. Keamanan untuk *mobile computing* perlu diperhatikan dengan seksama. Adanya resiko yang bervariasi

sangat tergantung kepada kepekaan pada data yang akan disimpan atau diproses, serta pemilihan jasa penyedia.

Manfaat potensial yang mencakup penghematan biaya dan peningkatan hasil dapat ditawarkan oleh penyedia. Hal ini menuntut ketersediaan *software* , kekuatan pemrosesan dan penyimpanan pada permintaan . Hal ini sudah menjadi kebutuhan tetap akan layanan yang berorientasi konsumen seperti email , penyimpanan dan media sosial (Syramun : 2015)[8].

Semakin banyak informasi yang ditempatkan di *cloud* oleh individu atau perusahaan, semakin rentan terhadap serangan dan ancaman internet yang ditawarkan . Berbagai risiko keamanan informasi untuk komputasi awan perlu dipertimbangkan dengan cermat . Risiko ini bervariasi tergantung pada kepekaan data yang akan disimpan atau diproses , dan bagaimana penyedia *cloud* yang dipilih telah menerapkan jasa *cloud* mereka .

Perangkat mobile telah menjadi begitu terintegrasi di lingkungan *cloud* yang benar-benar telah membantu orang-orang yang bekerja di dunia usaha/bisnis untuk mendapatkan pekerjaan mereka dapat dilakukan dengan mudah. Hal ini adalah kenyataan bahwa *cloud mobile services* yang telah digunakan oleh pelanggan dan perusahaan berlomba untuk menggunakannya untuk kebutuhan mereka sendiri. *Mobile cloud computing* dapat dipertimbangkan sebagai keuntungan yang unik dalam *mobile computing*. Saat ini, terdapat berbagai jenis aplikasi *mobile cloud* yang tersedia. Aplikasi bisa berupa seperti pengolahan citra, pengolahan bahasa alami, GPS bersama, berbagi akses internet, aplikasi data sensor, *query*, *pool computing* dan *multimedia searching* (Kun Yang:2013). Meskipun terdapat berbagai manfaat, ada beberapa masalah yang harus ditangani dan diselesaikan. Gambar 1 menunjukkan risiko perlindungan data untuk mengatur data. Jaringan ketergantungan koneksi, berbagi data dan aplikasi mengintegrasikan dan keamanan adalah beberapa tantangan di lingkungan ini. Tantangan utama lain untuk *mobile cloud computing* adalah *intermittency* dan ketersediaan jaringan.



Gambar 1. Risk Data Protection (M. Rajendra Prasad:2012)

Makalah ini membahas gambaran umum teknologi *mobile computing* serta tantangan serta *manfaat*, dengan adanya aplikasi pada teknologi *mobile computing*, *cloud computing* serta perlunya perhatian keamanan terhadap resiko pada lingkungan pengguna serta memahami pertimbangan keamanan pada *mobile computing.* yang diperlukan.

2. Gambaran Umum

2.1. Mobile Computing

Dari segi bahasa, *computing* artinya komputasi atau sesuatu yang bisa berjalan dengan fungsi seperti komputer. Sedangkan *mobile* adalah sesuatu barang (khususnya elektronik) yang mudah dibawa kemana mana.

Jadi secara umum bisa kita simpulkan bahwa *mobile computing* adalah seperangkat benda atau teknologi yang memiliki teknologi secanggih komputer dan mampu melakukan komunikasi walaupun pangguna dari alat tersebut sedang melakukan perpindahan.

Mobile computing merupakan teknologi yang dapat melakukan sistem distribusi data saat bergerak bebas dan dapat melakukan koneksi kembali pada lokasi jaringan yang berbeda.

Mobile Computing sebagai produk kemajuan teknologi komputer, sering disebut sebagai *mobile computer* (*portable computer*) yang dapat berkomunikasi dengan jaringan tanpa kabel (nirkabel).

Mobile Computing adalah sebuah komputasi menggunakan teknologi yang tidak terhubung secara fisik, atau dalam jarak jauh atau lingkungan mobile (non statik). Secara umum *mobile computing* adalah interaksi antara manusia dan komputer dalam lingkungan bergerak. *Mobile computing* terdiri dari perangkat lunak, perangkat keras dan jaringan *mobile*. Masing-masing, perangkat lunak *mobile* berkaitan dengan persyaratan aplikasi mobile. Juga, *hardware* termasuk komponen dan perangkat yang diperlukan untuk mobilitas.

Kata "mobilitas" telah menjadi sangat populer dalam dunia komputasi. Hal yang sama terlihat dari peningkatan serta pengembangan penjualan perangkat *mobile*. Pengguna memilih perangkat ini sebagai pilihan pertama mereka untuk kegiatan kerja dan hiburan.

Hal ini membawa kita pada pertanyaan tentang apa itu *mobile computing*? Ini adalah platform manajemen informasi yang independen dari lokasi dan kendala berbasis waktu. Otonomi *platform* ini memungkinkan pengguna untuk mengakses data dari mana saja di ruang dan setiap saat. Dengan demikian, apapun keadaan pengguna stasioner atau *mobile*, tidak mempengaruhi kemampuan kerja platform. Dengan demikian, muncul kesan bahwa sumber daya yang tersedia dan daya komputasi yang tersedia di suatu tempat, sedangkan pada kenyataannya jauh dari lokasi itu.

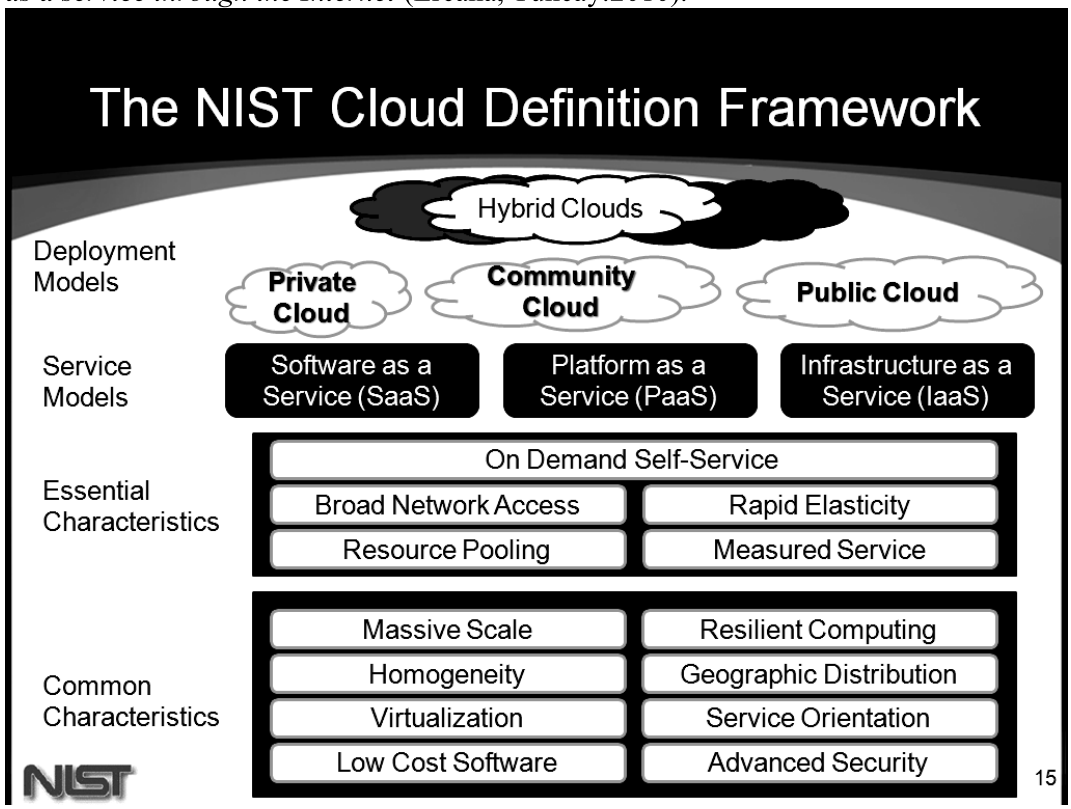
2.2 Cloud Computing

Cloud Computing adalah bentuk baru dari aplikasi di era internet dan telah menjadi topik hangat penelitian dalam komunitas industri dan ilmiah. Hal ini memberikan konsumen sumber daya dan infrastruktur komputasi sesuai kebutuhan mereka. Konsumen dapat menggunakan layanan dan aplikasi yang tersedia di awan melalui koneksi internet mereka. Beberapa ahli di bidang teknologi informasi telah menyumbangkan pemikiran tentang definisi cloud computing. *Cloud computing can be defined as simply the sharing and use of applications and resources of a network environment to get work done without concern about ownership and management of the network's resources and applications. With cloud computing, computer resources for getting work done and their data are no longer stored on one's personal computer, but are hosted elsewhere to be made accessible in any location and at any time (*Mark-Shane E. Scale:2019).

Terdapat definisi lain tentang cloud computing. Menurut Hayes (Hayes B:2008)

> *Cloud computing is a kind of computing which is highly scalable and use virtualized resources that can be shared by the users. Users do not need any background knowledge of the services. A user on the Internet can communicate with many servers at the same time and these servers exchange information among themselves*.

Definisi lain *Cloud computing is becoming an adoptable technology for many of the organizations with its dynamic scalability and usage of virtualized resources as a service through the Internet* (Ercana, Tuncay:2010).



Gambar 2.1 The NIST Definiton Framework (Mell & Grance, 2009)

Karakteristik Komputasi Awan

NIST mengidentifikasi lima karakteristik penting dari komputasi awan (Mell & Grance, 2009) sebagai berikut:

1. *On-demand self-service.* Pengguna dapat memesan dan mengelola layanan tanpa interaksi manusia dengan penyedia layanan, misalnya dengan menggunakan, sebuah *portal web* dan manajemen antarmuka. Pengadaan dan perlengkapan layanan serta sumberdaya yang terkait terjadi secara otomatis pada penyedia.
2. *Broad network access.* Kemampuan yang tersedia melalui jaringan dan diakses melalui mekanisme standar, yang mengenalkan penggunaan berbagai platform (misalnya, telepon selular, laptop, dan PDA).
3. *Resource pooling.* Penyatuan sumberdaya komputasi yang dimiliki penyedia untuk melayani beberapa konsumen menggunakan model multi-penyewa, dengan sumberdaya fisik dan virtual yang berbeda, ditetapkan secara dinamis dan ditugaskan sesuai dengan permintaan konsumen. Ada rasa kemandirian lokasi bahwa pelanggan umumnya tidak memiliki kontrol atau pengetahuan atas keberadaan lokasi sumberdaya yang disediakan, tetapi ada kemungkinan dapat menentukan lokasi di tingkat yang lebih tinggi (misalnya, negara, negara bagian, atau *datacenter*).

   Contoh sumberdaya termasuk penyimpanan, pemrosesan, memori, bandwidth jaringan, dan mesin virtual.
4. *Rapid elasticity.* Kemampuan dapat dengan cepat dan elastis ditetapkan.
5. *Measured Service.* Sistem komputasi awan secara otomatis mengawasi dan mengoptimalkan penggunaan sumberdaya dengan memanfaatkan kemampuan pengukuran (*metering*) pada beberapa tingkat yang sesuai dengan jenis layanan (misalnya, penyimpanan, pemrosesan, *bandwidth*, dan *account* pengguna aktif). Penggunaan sumberdaya dapat dipantau, dikendalikan, dan dilaporkan sebagai upaya memberikan transparansi bagi penyedia dan konsumen dari layanan yang digunakan.

Cloud computing sebagai model pengiriman untuk layanan teknologi informasi didefinisikan oleh National Institute of Standards and Technology (NIST) sebagai model untuk memungkinkan kenyaman, *on-demand* akses jaringan untuk memanfaatkan bersama suatu sumberdaya komputasi yang terkonfigurasi (misalnya, jaringan, server, penyimpanan, aplikasi, dan jasa) yang dapat dengan cepat ditetapkan dan dirilis dengan upaya manajemen yang minimal atau interaksi penyedia layanan (Mell, P and Grance T:2009).

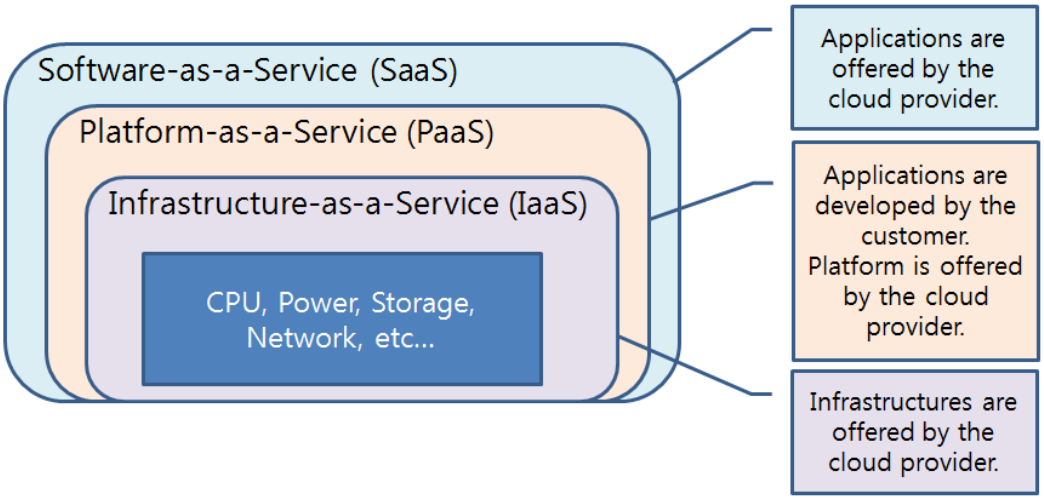
Keuntungan Cloud computing

Menurut Furht (2010), teknologi *cloud computing* memberikan keuntungan sebagai berikut (a) **Flexibility,** *They can decide how much storage space to use, and how much processing power is required. While working to update software applications, the process can be pushed out much faster and more efficiently.*

Administrators can choose when to update an application enterprise-wide all in real time. It is up to them and how much they want to spend on IT with cloud technology. (b) **Scalability,** *With cloud computing one person can go from small to large quickly*. (c) **Capital Investment,** *With cloud computing, many rudimentary IT purchases for things like hardware are no longer an issue as long as that task or set of tasks can be performed by the cloud.* (d) **Portability,** *With cloud computing technology, organizations are able to use their computing power wherever their people are as long as users are able to access thin clients.*
Thin client access is pretty much available everywhere that companies do business today, so this should not even be an issue. With thin client technology the scale of geography and time variation is flattened somewhat and this allows companies that are trying to globally integrate to be able to be more flexible than ever before.

Sedangkan tiga jenis model layanan dijelaskan oleh NIST (Mell, P and Grance T:2009) sebagai berikut :

1. *Software as a Service (SaaS)*. Kemampuan yang diberikan kepada konsumen untuk menggunakan aplikasi penyedia dapat beroperasi pada infrastruktur awan. Aplikasi dapat diakses dari berbagai perangkat klien melalui antarmuka seperti web browser (misalnya, email berbasis web). Konsumen tidak mengelola atau mengendalikan infrastruktur awan yang mendasari termasuk jaringan, server, sistem operasi, penyimpanan, atau bahkan kemampuan aplikasi individu, dengan kemungkinan pengecualian terbatas terhadap pengaturan konfigurasi aplikasi pengguna tertentu.
2. *Platform as a Service* (PaaS). Kemampuan yang diberikan kepada konsumen untuk menyebarkan aplikasi yang dibuat konsumen atau diperoleh ke infrastruktur komputasi awan menggunakan bahasa pemrograman dan peralatan yang didukung oleh provider. Konsumen tidak mengelola atau mengendalikan infrastruktur awan yang mendasari termasuk jaringan, server, sistem operasi, atau penyimpanan, namun memiliki kontrol atas aplikasi disebarkan dan memungkinkan aplikasi melakukan hosting konfigurasi.
3. *Infrastructure as a Service* (IaaS). Kemampuan yang diberikan kepada konsumen untuk memproses, menyimpan, berjaringan, dan komputasi sumberdaya lain yang penting, dimana konsumen dapat menyebarkan dan menjalankan perangkat lunak secara bebas , dapat mencakup sistem operasi dan aplikasi. Konsumen tidak mengelola atau mengendalikan infrastruktur awan yang mendasari tetapi memiliki kontrol atas sistem operasi, penyimpanan, aplikasi yang disebarkan, dan mungkin kontrol terbatas komponen jaringan yang pilih (misalnya, *firewall host*).



Gambar 2.2 Layanan pada Cloud Computing (Sun Microsystems, Inc:2009)

Cloud computing tidak hanya terbatas pada komputer pribadi; tetapi memiliki dampak yang besar bahkan pada teknologi *mobile*. Mobilitas dan mana-mana adalah fitur utama dari jaringan generasi berikutnya. Dengan demikian, kombinasi dari perangkat elektronik seperti *smartphone*, PDA, tablet, jaringan selular di mana-mana dan *cloud computing*, sumber daya yang berkumpul bersama-sama untuk muncul sebagai bidang baru yaitu *mobile cloud computing*.

Model penyebaran komputasi awan menurut NIST terdiri dari empat model (Mell dan Grance, 2009), yaitu:

1. *Private cloud*. Infrastruktur awan yang semata-mata dioperasikan bagi suatu organisasi. Ini mungkin dikelola oleh organisasi atau pihak ketiga dan mungkin ada pada *on premis* atau *off premis*.
2. *Community cloud.* Infrastruktur awan digunakan secara bersama oleh beberapa organisasi dan mendukung komunitas tertentu yang telah berbagi *concerns* (misalnya, misi, persyaratan keamanan, kebijakan, dan pertimbangan kepatuhan). Ini mungkin dikelola oleh organisasi atau pihak ketiga dan mungkin ada pada *on premis* atau *off premis*.
3. *Public cloud.* Infrastruktur awan yang dibuat tersedia untuk umum atau kelompok industri besar dan dimiliki oleh sebuah organisasi yang menjual layanan awan.
4. *Hybrid cloud.* Infrastruktur awan merupakan komposisi dari dua atau lebih awan (swasta, komunitas, atau publik) yang masih entitas unik namun terikat bersama oleh estándar atau kepemilikan teknologi yang menggunakan data dan portabilitas aplikasi

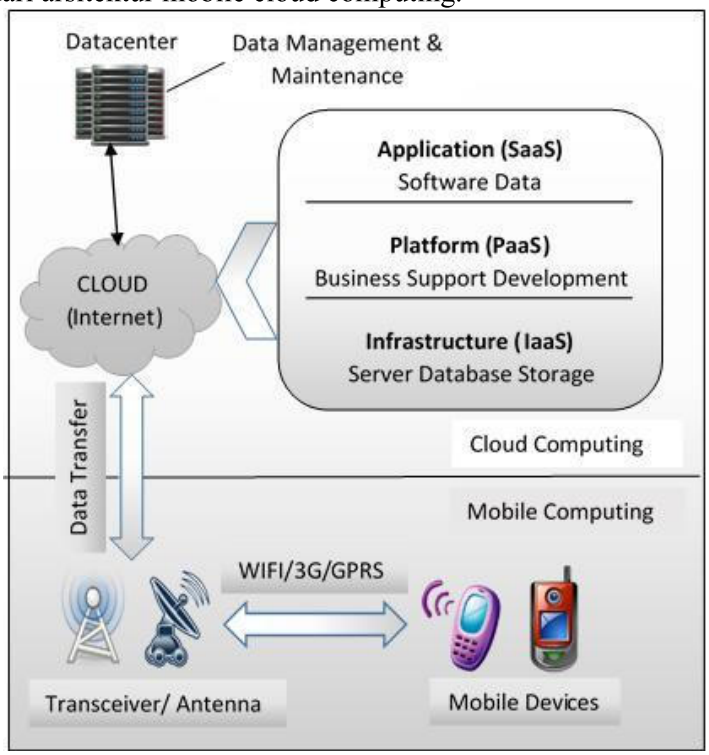
2.3. Hubungan antara Mobile Computing dan Cloud Computing

Hubungan antara *mobile computing* dan *cloud computing* disebut juga *mobile cloud computing* adalah sebuah paradigma peningkatan komputasi dengan akses

cepat ringan dengan menggunakan perangkat *mobile* untuk pengguna akhir serta penyebaran yang cepat melalui server *cloud*. *Mobile cloud computing* memanfaatkan kelebihan dari server *cloud* yang menyediakan kemampuan fleksibel dalam hal perhitungan dan penyimpanan di *back-end* , serta memanfaatkan kelebihan dari perangkat *mobile* yang mudah dalam mengakses dan komputasi yang universal di *front-end* (Waghmare Monika, Chavan T. A:2013)

Dalam makalah ini, membahas gambaran teknologi cloud computing bersama-sama dengan tantangan cloud computing dan manfaat yang terkait. Banyaknya isu-isu yang berbeda yang muncul dengan adanya mobile cloud computing yang telah diidentifikasi dan dibahas, sehingga terdapat gambaran dan pentingnya mewujudkan keamanan risiko lingkungan cloud yang ditawarkan. Makalah ini juga menyampaikan aspek keamanan cloud computing yang diperlukan untuk memahami dan menilai resiko.

Penggunaan cloud computing dalam kombinasi dengan perangkat mobile dikenal sebagai mobile cloud computing. Ini adalah kombinasi antara jaringan mobile dan komputasi awan , sehingga memberikan pelayanan yang optimal bagi pengguna mobile. Cloud computing terjadi ketika file dan data disimpan di internet bukan pada perangkat individu , menyediakan akses on-demand. Gambar 1 menunjukkan gambaran dari arsitektur mobile cloud computing.



Gambar 2.3. Arsitektur *Mobile Cloud Computing*.

Perangkat *mobile* terhubung ke BTS jaringan nirkabel *mobile*. Beberapa BTS satelit dan *Base Transceiver Station* (BTS), selanjutnya bertindak sebagai antarmuka yang menetapkan koneksi jaringan antara perangkat *mobile* dan

internet. Permintaan pengguna yang dikirim melalui jaringan nirkabel untuk mengakses server *cloud* oleh Otentikasi, Otorisasi dan mekanisme Akuntansi. Setelah pengiriman permintaan pengguna ke *cloud*, pengendali *cloud* memproses permintaan tersebut untuk menyediakan pengguna dengan layanan *cloud* yang sesuai (Donald A. Cecil:2013)

3. Pertimbangan Umum Keamanan

3.1 .Keamanan pada Mobile Cloud Computing

Mengamankan privasi pengguna *mobile cloud computing* dan integritas data atau aplikasi adalah salah satu isu utama yang paling diperhatikan oleh penyedia *cloud*. *Mobile cloud computing* merupakan kombinasi jaringan *mobile* dan *cloud computing*, kemudian terkait dengan masalah keamanan dibagi menjadi dua kategori: keamanan pengguna jaringan mobile; dan keamanan *cloud* (H. T. Dinh, C. Lee, D. Niyato and P. Wang:2011).

1. Keamanan Pengguna Jaringan Mobile.

Banyak kerentanan keamanan dan ancaman seperti kode berbahaya yang dikenal dengan perangkat *mobile* yang berbeda seperti s*martphone*, PDA, telepon seluler, laptop, dan sejenisnya. Beberapa aplikasi untuk perangkat ini dapat menyebabkan masalah privasi bagi pengguna *mobile* (H. T. Dinh:2011).

Ada dua isu utama tentang keamanan pelanggan.

Keamanan untuk aplikasi *mobile*: Cara paling sederhana untuk mendeteksi ancaman keamanan akan menginstal dan menjalankan perangkat lunak keamanan dan antivirus program pada perangkat *mobile*. Tapi karena perangkat *mobile* dibatasi dengan pengolahan dan daya keterbatasan, untuk melindunginya dari ancaman ini bisa lebih sulit dibandingkan dengan komputer biasa. Beberapa pendekatan telah dikembangkan mentransfer mekanisme deteksi ancaman dan keamanan ke *cloud*. Sebelum pengguna *mobile* bisa menggunakan aplikasi tertentu, harus melalui beberapa tingkat evaluasi ancaman. Semua kegiatan file yang akan dikirim ke perangkat *mobile* akan diverifikasi jika berbahaya atau tidak. Alih-alih menjalankan software anti-virus atau deteksi ancaman program lokal, perangkat mobile hanya melakukan kegiatan ringan seperti jejak eksekusi ditransmisikan ke keamanan server *cloud*.

> Adanya beberapa keuntungan dalam lingkungan *mobile cloud* , namun terdapat beberapa masalah dan tantangan dalam *mobile cloud* computing. Keamanan dalam Kepemilikan Data , Privasi , Keamanan Data dan masalah keamanan lainnya (Soeung-Kon Victor Ko:2012).

Kepemilikan Data: Isu lain yang muncul dari *mobile cloud computing* berkaitan dengan kepemilikan media digital yang dibeli. Dengan *cloud computing* menjadi mungkin untuk menyimpan file media yang dibeli, seperti audio, video atau e-buku jarak jauh daripada lokal. Hal ini dapat menyebabkan kekhawatiran mengenai kepemilikan sebenarnya dari data. Jika media pembelian pengguna menggunakan layanan yang diberikan dan media itu sendiri disimpan jauh ada risiko kehilangan akses ke media yang dibeli.

Privasi: Memberikan informasi pribadi seperti menunjukkan lokasi Anda saat ini dan informasi pengguna penting menciptakan skenario untuk masalah privasi. Sebagai contoh, penggunaan *location base service* (LBS) /layanan berbasis lokasi

yang disediakan oleh *global positioning system* (GPS) perangkat. Ancaman untuk mengungkap informasi pribadi dapat diminimalkan melalui pemilihan dan menganalisis kebutuhan perusahaan dan membutuhkan hanya layanan yang akan diperoleh ditentukan dan pindah ke *cloud*. Hal ini menyebabkan kekhawatiran bahwa perusahaan akan menggunakan atau menjual informasi ini serta kekhawatiran bahwa informasi dapat diberikan kepada instansi pemerintah tanpa izin atau sepengetahuan pengguna.

Akses Data dan Keamanan: isu-isu terkait akses dan keamanan yang signifikan untuk aplikasi yang mengandalkan penyimpanan data jarak jauh dan akses internet agar dapat berfungsi. Misalnya data semua pengguna toko, jadwal dan kontak informasi mereka secara online, listrik padam dapat mempengaruhi kemampuan untuk berfungsi dari hari ke hari. *mobile cloud computing* rentan karena beberapa titik di mana akses dapat terganggu. Penerimaan dan ketersediaan kecepatan tinggi dapat sangat bervariasi untuk perangkat mobile yang digunakan oleh pengguna.

2. Keamanan Cloud.

Individu dan perusahaan dapat menggunakan manfaat untuk menyimpan sejumlah besar data atau aplikasi di cloud. Namun, masalah dalam hal integritas, otentikasi, dan hak-hak digital harus diperhatikan (H. T. Dinh:2011).

Integritas: Setiap pengguna *mobile cloud* harus memastikan integritas informasi yang disimpan di atas cloud. Setiap akan mengakses data atau aplikasi, maka harus dikonfirmasi dan diverifikasi. Pendekatan yang berbeda dalam integritas menjaga informasi seseorang yang disimpan di *cloud* sedang diusulkan. Misalnya, setiap informasi yang disimpan oleh masing-masing individu atau perusahaan dalam awan ditandai atau diinisialisasi kepada mereka dimana mereka adalah satu-satunya untuk memiliki akses (bergerak, update atau menghapus) informasi tersebut. Setiap akses mereka membuat harus disahkan meyakinkan bahwa mereka informasi sendiri dan dengan demikian memverifikasi integritas.

Otentikasi: Berbagai mekanisme otentikasi telah disajikan dan diusulkan menggunakan komputasi awan untuk mengamankan akses data yang sesuai untuk lingkungan *mobile*. Beberapa menggunakan standar terbuka dan bahkan mendukung integrasi berbagai metode otentikasi. Sebagai contoh, penggunaan akses atau *log-in* ID, *password* permintaan otentikasi, dll.

Manajemen hak digital: distribusi ilegal dan pembajakan konten digital seperti video, gambar, audio, dan *e-book*, program menjadi lebih dan lebih populer. Beberapa solusi untuk melindungi isi ini dari akses ilegal diimplementasikan seperti penyediaan enkripsi dan dekripsi kunci untuk mengakses konten tersebut. Sebuah *coding decoding* atau platform yang harus dilakukan sebelum setiap pengguna mobile dapat memiliki akses ke konten digital tersebut.

3.2. Solusi yang Mungkin untuk Masalah Keamanan

Dari semua masalah di atas dibahas, hal yang paling umum selama transfer data adalah keamanan data. Berikut disampaikan beberapa solusi yang mungkin sesuai (Donald A. Cecil:2013). Solusi pertama adalah dengan keamanan model baru di

mana layanan deteksi seperti *Intrusion Detection System* (IDS) dan *Cloud Intrusion Detection System Services* (CIDSS) berlangsung di *cloud* jelas menghemat proses CPU perangkat dan memori.

Solusi layanan deteksi ini memiliki beberapa manfaat:

1. Deteksi yang lebih baik dari kode berbahaya.
2. Mengurangi konsumsi sumber daya pada perangkat mobile.
3. Mengurangi kompleksitas Software perangkat mobile.

Selanjutnya, adalah mungkin untuk mencapai keamanan dengan menerapkan mekanisme enkripsi homomorphic dengan kombinasi enkripsi tingkat-6 yang dapat diadopsi ketika data melewati antara *cloud*, dan *mobile* tanpa persyaratan aplikasi eksternal. Enkripsi tingkat-6 ini terutama digunakan untuk *encode* teks yang aman dan *decode* yang mengharuskan penggunaan JavaScript dan *browser*. Untuk menghemat sumber daya *mobile*, enkripsi tingkat-6 harus mengandalkan dan dieksekusi dari jarak jauh di atas *cloud* itu. Dengan solusi yang terbaik ini memberikan keamanan dan skalabilitas fitur saat berbagi data.

Jika data dengan kode berbahaya di-*download* oleh pengguna, akun *cloud* dan data akan diambil dan akuntansi yang tidak adil akan terjadi.\

1. Data dan aplikasi yang di-*download* hanya diverifikasi dengan kegiatan yang abnormal harus diblokir.
2. Melalui *broadcast* SSID, informasi dapat bocor dan pengguna yang tidak sah dapat memperoleh akses.
3. Nonaktifkan *broadcast* SSID dan memanfaatkan algoritma otentikasi kunci yang ditingkatkan.

Berikut adalah beberapa langkah yang diberikan untuk memenangkan pertempuran pelanggaran:

1) ***Prioritaskan tujuan dan mengatur toleransi risiko.***

Melindungi aset data di tempat kerja telah menjadi tantangan bagi profesional keamanan selama beberapa dekade. Yang benar adalah bahwa tidak ada hal seperti 100 persen aman. Keputusan sulit harus dibuat pada berbagai tingkat perlindungan yang dibutuhkan untuk bagian yang berbeda dari bisnis.

2) ***Lindungi data dengan rencana keamanan proaktif.***

Perencanaan dalam keamanan bukanlah tugas yang mudah bagi sebuah organisasi. Ini termasuk memahami jenis ancaman (yaitu serangan *hacking*, kejahatan *cyber*, media & penipuan sosial, dll) dan untuk melindungi organisasi terhadap ancaman ini, mengharuskan kedua kebijakan dan teknologi.

3) ***Siapkan respon terhadap serangan canggih yang tak terelakkan.***

Dengan evolusi ancaman terus-menerus maju, *hacker* bertujuan untuk menemukan kerentanan.

4) ***Mempromosikan budaya kendali keamanan.***

Penting untuk dicatat bahwa kesalahan ceroboh seorang karyawan akan mempengaruhi rencana induk kepala petugas keamanan. Itu sebabnya setiap karyawan harus bekerja dalam kelompok dengan keamanan profesional untuk menjamin keamanan data perusahaan. Keamanan harus dibangun di atas budaya organisasi.

4. Kesimpulan

Mobile cloud computing menyediakan layanan yang optimal bagi pengguna *mobile computing* sebagai salah satu tren teknologi *mobile* di masa depan karena menggabungkan keunggulan dari kedua *mobile computing* dan *cloud computing*.

Makalah ini memaparkan konsep *mobile computing*, masalah tantangan keamanan, berbagai kerangka keamanan yang ada dan akhirnya beberapa solusi yang meningkatkan keamanan di lingkungan mobile *cloud*. Sebagian besar kerangka kerja keamanan privasi data pengguna, penyimpanan data dan usaha menjaga proses berbagi data diabaikan,. Jelaslah bahwa privasi data pengguna dan aplikasi *mobile* yang menggunakan *cloud* adalah faktor yang paling menantang. Untuk mencapai keamanan lebih di lingkungan *mobile cloud*, maka perlu dipelajari berbagai ancaman yang ada.

Telah di dibahas aspek keamanan mengenai *mobile computing*. mengamankan privasi *mobile cloud computing* pengguna dan integritas data atau aplikasi adalah masalah utama yang harus diperhatikan oleh sebagian besar penyedia *cloud*. *Mobile cloud computing* merupakan kombinasi *mobile computing* dan *cloud computing*, masalah keamanan terkait kemudian dibagi menjadi dua kategori : keamanan pengguna jaringan *mobile* ; dan keamanan *mobile cloud* secara umum.

Daftar Pustaka

[1] Donald A. Cecil, Oli S. Arul, Juli 2013, *Mobile Cloud Security Issues and Challenges: A Perspective*. International Journal of Engineering and Innovative Technology (IJEIT)", vol. 3, pp. 401-406.

[2] Ercana, Tuncay, 2010, *Use of Cloud Computing in Educational Institutions*, Procedia Social and Behavioral Sciences 2, pp. 938–942.

[3] Furht, Borko & Armando Escalante, 2010, *Handbook of Cloud Computing,* Springer : New York.

[4] Hayes B, 2008, *Cloud Computing. Communications of the ACM*, vol. 51, pp. 9-11.

[5] H. T. Dinh, C. Lee, D. Niyato and P. Wang, 2011, *A Survey of Mobile Cloud Computing*: *Architecture, Applications, and Approaches*, Wireless Communications and Mobile Computing. Wiley.

[6] Kun Yang, Dr. Shumao Ou, Professor Hai Jin, Huazhong and Professor Amiya Nayak,2013, *Mobile Cloud Computing and Networking*, Proceedings of IEEE conference.

[7] Mark-Shane E. Scale, 2009, *Cloud Computing and Collaboration*, Library Hi Tech News, vol. 26, pp. 10-13.

[8] Mell, P and Grance T, 2009, *NIST Definition of Cloud Computing v1*.

[9] Soeung-Kon Victor Ko, Jung- Hoon Le and Sung Woo Kim, 30 April 2012, *Mobile Cloud Computing Security Considerations*

[10] Sun Microsystems, Inc., 2009, *Introduction to Cloud Computing Architecture*, White Paper, 1st Edition.

[11] Syrasmamun, "Cloud Computing Architecture, Hub Page Inc, 2015

[12] Waghmare Monika, Chavan T. A,2013, *Outsourcing with Secure Accessibility in Mobile Cloud Computing*, International Journal of Computer Trends and Technology (IJCTT), vol. 4, pp. 526