ISBN 978-602-70361-1-6

Aspek Keamanan pada Mobile Cloud Computing

Zen Munawar
Jurusan Manajemen Informatika
Politeknik LP3I Bandung
Jl. Pahlawan No. 59, Bandung
munawarzen@gmail.com

Abstrak— Mobile cloud computing adalah pengembangan dan perluasan komputasi, juga menunjang mobilitas dan skalabilitas. Mobile cloud computing sebagai kombinasi dari mobile computing, dan cloud computing dan mobile internet, saat ni telah berkembang sangat pesat serta dikenal sebagai suatu teknologi yang potensal untuk layanan mobile. Makalah ini menyajikan gambaran umum cloud computing, layanan cloud, penyebaran cloud, dan akses ke jaringan internet. Banyaknya informasi yang ditempatkan ke dalam awan baik oleh individu maupun perusahaan , maka diperlukan keamanan informasi. Aspek keamanan pengguna mobile cloud computung, integritas data serta aplikasi menjadi salah satu isu yang perlu diperhatikan oleh penyedia cloud. Makalah ini penulis akhiri dengan penggunaan pedoman keamanan pada mobile cloud computing.

Kata kunci— mobile cloud computing, mobile computing, cloud computing, mobile cloud computing security

I. PENDAHULUAN

Perkembangan teknologi yang terjadi saat ini semakin pesat, perkembangan terjadi pada perangkat lunak (*software*) maupun perangkat keras (*hardware*) dalam waktu yang singkat. Kinerja sistem komputer dapat di lihat melalui penyelarasan tiga komponennya yaitu *brainware, software dan hardware*. Tanpa adanya penyelarasan ketiga hal tersebut maka sistem komputer belum dapat dikatakan bekerja secara optimal. *Cloud computing* atau komputasi awan merupakan teknologi yang menggunakan layanan internet dan bertujuan melakukan pemeliharaan data dan aplikasi, dengan *cloud computing* memungkinkan akses data dari mana saja baik menggunakan perangkat tetap maupun perangkat *mobile* yang terhubung dengan *internet cloud* untuk menyimpan data dan aplikasi, maka dengan mudah mengambil data, aplikasi serta berpindah dari satu *cloud* ke *cloud* lainnya. *Cloud Computing* menawarkan manfaat potensial seperti penghematan biaya dan peningkatan hasil bisnis. Peluang yang diberikan oleh *cloud computing* tersedia untuk perusahaan dari semua ukuran yang memungkinkan dapat memberikan layanan yang lebih terukur terhadap karyawan, mitra dan pelanggan dengan biaya yang lebih rendah dan fleksibilitas bisnis yang lebih tinggi. *Mobile cloud computing* memberikan layanan ketersediaan layanan *cloud computing* dalam lingkungan *mobile*, hal ini juga merupakan gabungan elemen jaringan *mobile* dan *cloud computing* sehingga memberikan pelayanan yang optimal bagi pengguna *mobile*.

Banyaknya Individu dan perusahaan yang menyimpan informasi di *cloud*, maka akan semakin rentan terhadap serangan dan ancaman internet. Keunggulan *cloud computing* untuk mendapatkan akses cepat ke aplikasi bisnis dan meningkatnya sumber daya infrastrukur dengan biaya yang lebih kecil akan menempatkan dunia bisnis akan menjadi beresiko. Aspek keamanan untuk *cloud computing* perlu diperhatikan dengan seksama. Adanya resiko yang bervariasi sangat tergantung kepada kepekaan pada data yang akan disimpan atau diproses, serta pemilihan jasa penyedia *cloud*.

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

II. METODE

A. 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 [5].

Terdapat definisi lain tentang cloud computing. Menurut Hayes [3] *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* [2].

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 [6]. Sedangkan tiga jenis model layanan dijelaskan oleh NIST [6] 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).

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 komputasi awan, sumber daya yang berkumpul bersama-sama untuk muncul sebagai bidang baru Mobile Cloud Computing.

B. Mobile Cloud Computing

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 *backend* , serta memanfaatkan kelebihan dari perangkat mobile yang mudah dalam mengakses dan komputasi yang universal di *front-end* [8].

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 1. Arsitektur mobile cloud computing [1]

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 [1].

III. ASPEK KEAMANAN

A. 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* [4].

1) Keamanan Pengguna Jaringan Mobile.

Banyak kerentanan keamanan dan ancaman seperti kode berbahaya yang dikenal dengan perangkat mobile yang berbeda seperti Smartphone, PDA, telepon seluler, laptop, dan sejenisnya. Beberapa aplikasi untuk perangkat ini dapat menyebabkan masalah privasi bagi pengguna mobile [4]. 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 awan. 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 server awan keamanan.

Adanya beberapa keuntungan dalam lingkungan mobile cloud , namun terdapat beberapa masalah dan tantangan dalam mobile cloud computing. Aspek keamanan dalam Kepemilikan Data , Privasi , Keamanan Data dan masalah keamanan lainnya [7].

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 awan. 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 [4].

ISBN 978-602-70361-1-6

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.

B. Keamanan pada Cloud Computing

Untuk mewujudkan manfaat penuh dari *cloud computing*, aspek keamanan dan risiko harus ditangani dengan benar. Pertimbangan berikut dalam mengevaluasi, melaksanakan, mengelola, dan memelihara solusi *cloud computing* harus dieksplorasi.

Kepatuhan dan manajemen Risiko: Perusahaan yang bergeser ke *cloud* bertanggung jawab atas kepatuhan, risiko, dan manajemen keamanan. Hal ini penting bagi mereka untuk memahami kepatuhan dan manajemen resiko bahkan jika tanggung jawab untuk eksekusi dapat ditransfer ke penyedia cloud.

Layanan Integritas: layanan berbasis cloud harus direkayasa dan dioperasikan dengan keamanan dalam pikiran; proses operasional harus diintegrasikan ke dalam manajemen keamanan organisasi.

Endpoint Integritas: Keamanan, kepatuhan, dan integritas titik akhir harus menjadi bagian dari pertimbangan keamanan.

Perlindungan Informasi: Layanan Cloud memerlukan proses yang dapat diandalkan untuk melindungi informasi sebelum, selama, dan setelah transaksi.

C. Pedoman Keamanan dan Privasi di Public Cloud Computing

Pedoman keamanan dan privasi di *public cloud computing* memberikan gambaran tentang keamanan dan privasi tantangan yang dihadapi komputasi awan publik dan menyajikan rekomendasi bahwa organisasi harus mempertimbangkan ketika *outsourcing data*, aplikasi dan infrastruktur untuk lingkungan *cloud* publik. Dokumen ini memberikan pemahaman tentang ancaman, risiko teknologi dan pengamanan yang berkaitan dengan lingkungan awan publik untuk membantu organisasi membuat keputusan tentang penggunaan ini teknologi ini [9]. Pedoman utama termasuk :

- Hati-hati merencanakan aspek keamanan dan privasi solusi *cloud computing* sebelum menerapkannya.
- Memahami lingkungan *public cloud computing* yang ditawarkan oleh penyedia *cloud* .
- Pastikan bahwa sumber *cloud computing* sudah baik, *cloud* dan aplikasi berbasis *cloud* harus memenuhi persyaratan keamanan dan privasi organisasi.
- Mempertahankan akuntabilitas atas privasi dan keamanan data dan aplikasi diimplementasikan dan digunakan dalam lingkungan *public cloud computing*.

D. 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 [1]. 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:

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

Selanjutnya, adalah mungkin untuk mencapai keamanan dengan menerapkan mekanisme enkripsi homomorphic dengan kombinasi

ISBN 978-602-70361-1-6

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.

- Data dan aplikasi yang di-*download* hanya diverifikasi dengan kegiatan yang abnormal harus diblokir.
- Melalui *broadcast* SSID, informasi dapat bocor dan pengguna yang tidak sah dapat memperoleh akses.
- 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.

1. Siapkan respon terhadap serangan canggih yang tak terelakkan.
2. Dengan evolusi ancaman terus-menerus maju, *hacker* bertujuan untuk menemukan kerentanan.
3. 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.

IV. KESIMPULAN

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

Makalah ini memaparkan konsep *mobile cloud 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 dibahas aspek keamanan mengenai *mobile cloud 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 jaringan *mobile* 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, "Mobile Cloud Security Issues and Challenges: A Perspective. International Journal of Engineering and Innovative Technology (IJEIT)", vol. 3, pp. 401-406, Juli 2013.

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

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

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

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

[6] Mell, P and Grance T, "NIST Definition of Cloud Computing v1", 2009

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

ISBN 978-602-70361-1-6

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

[9] W. Jansen, T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing". NIST Special Publication. pp. 800-144, 2011.