Jurnal Sistem Informasi ISSN P : 2598-599X; E: 2599-0330

PERSPEKTIF KEAMANAN PENGGUNA TENTANG ADOPSI DAN MIGRASI TEKNOLOGI MOBILE CLOUD

Munirul Ula[1], Rizal Tjut Adek[2], dan Bustami[3]
[1] Sistem Informasi Universitas Malikussaleh Lhokseumawe
[2,3] Teknik Informatika Universitas Malikussaleh Lhokseumawe
Jl. Cot Tgk Nie-Reulet, Aceh Utara, 141 Indonesia
email: munirulula@unimal.ac.id

Abstrak

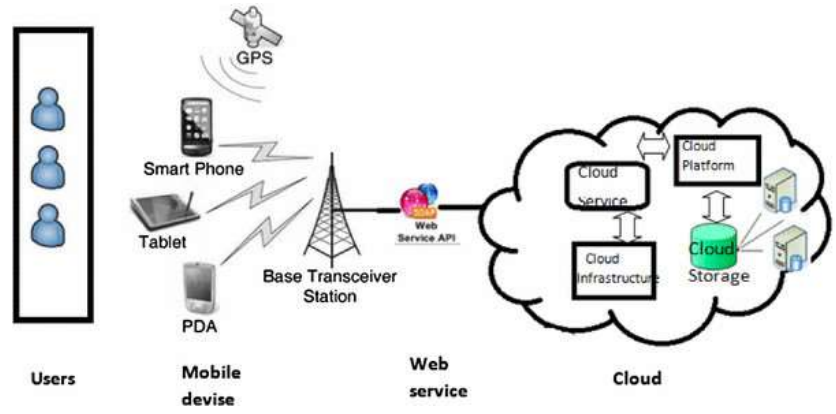
Keamanan adalah salah satu perhatian utama mereka yang ingin mengadopsi dan bermigrasi ke teknologi Cloud Computing. Masalah keamanan yang digunakan oleh teknologi cloud mengungkapkan bahwa mobile cloud computing meningkatkan masalah privasi dan keamanan seperti masalah identifikasi dan otentikasi, karena terkadang identitas dan otentikasi pemilik perangkat atau pemilik data yang terdapat di cloud dapat terdeteksi. Ini adalah beberapa contoh yang dapat dianggap sebagai kemunduran besar pada adaptasi Mobile Cloud Computing dan alasan mengapa beberapa perusahaan masih enggan merangkul, mengadopsi, dan bermigrasi ke teknologi ini. Penelitian ini mengulas fenomena mobile cloud computing, dan masalah keamanan dan privasi dalam area aplikasi mobile dan Cloud Computing dengan lebih menekankan pada pertimbangan keamanan dan privasi untuk merangkul dan bermigrasi ke mobile cloud computing.

***Kata kunci**: Cloud Computing, Keamanan Informasi, Privasi, Mobile Cloud Computing*

1. Pendahuluan

Saat ini, pasar ponsel meningkat dengan kecepatan yang sangat tinggi. Laporan International Data Corporation (IDC) menunjukkan bahwa 44% dari populasi dunia sekitar 3,2 miliar orang, akan memiliki akses ke Internet pada tahun 2016. Sementara lebih dari 2 miliar akan menggunakan perangkat seluler untuk mengakses internet dengan $32 miliar dihitung dihabiskan untuk infrastruktur TI cloud per tahun. Ini menyumbang 33% dari total pengeluaran infrastruktur TI. Pada tahun 2019, pengeluaran infrastruktur cloud diperkirakan mencapai $52 miliar, yang dianggap sebagai 45% dari total pengeluaran TI (IDC, 2018). Seiring dengan peningkatan eksplosif aplikasi seluler dan munculnya serta kebutuhan fenomena komputasi cloud, konsep Mobile cloud computing telah diluncurkan untuk menjadi teknologi kemungkinan untuk perangkat dan

layanan seluler, menurut Krishnan, ketika server aplikasi tersebut ingin bermigrasi ke struktur cloud, perhatian utama akan keamanan yang sering terdengar di berita [2].



Gambar 1. Arsitektur Mobile Cloud Computing

Mobile Cloud Computing (MCC) menggabungkan konsep komputasi cloud ke dalam lingkungan atau lingkungan seluler dan mengatasi masalah yang terkait dengan lingkungan dan kinerja. Terlepas dari evolusi luar biasa dan manfaat signifikan yang diwujudkan oleh Mobile Cloud Computing, Pengguna Telepon selulernya masih belum puas, karena risiko privasi dan keamanan terkait (Gasparis, 2017). Ancaman ini memainkan peran penting dalam mengecilkan hati organisasi dan pengguna tunggal untuk mengadopsi dan bermigrasi ke lingkungan dan lingkungan Mobile Cloud Computing. Menurut data dari IDC, Indonesia tetap menjadi salah satu pembelanja teratas untuk layanan TI di kawasan Timur Tengah dan Afrika. Pada tahun 2014, investasi layanan cloud di negara tersebut mencapai $50,4 juta dan diperkirakan mencapai $77,4 juta pada tahun 2015. Sebuah survei yang dilakukan oleh "Dun & Bradstreet" telah mengungkapkan sektor publik Indonesia meningkatkan penggunaan "komputasi cloud", selama forum berjudul “Reshaping Information Technology Future Features” digelar baru-baru ini di Jeddah, Indonesia. Survei tersebut memberikan ekspektasi untuk peningkatan pengeluaran untuk teknologi informasi di sektor industri transformatif di Kerajaan dengan CAGR sebesar 7,5 persen dari 2013 hingga 2018, menurut laporan yang dikeluarkan oleh "IDC" [1]. Kerajaan akan lebih suka bahwa cloud publik dikelola setidaknya di wilayah tersebut, bukan di luar negeri untuk mengatasi masalah keamanan dan privasi. Sebagian besar pertumbuhan ini

didorong oleh pengeluaran untuk layanan cloud publik seperti Software as a Service (SaaS), Platform as a Service (PaaS), dan Infrastructure as a Service (IaaS). Jenis-jenis teknologi cloud computing dapat dilihat dari dua cara yang berbeda. Cara pertama berdasarkan akses dan cara kedua berdasarkan kemampuan [2].

Mobile Cloud Computing telah muncul dari dua hal, cloud dan mobilitas. Namun demikian, sementara teknologi ini menghadirkan beberapa keuntungan dan memungkinkan pengguna ponsel memiliki akses ke aplikasi dan sumber daya komputasi yang andal dan kuat kapan saja dan di mana saja, ada kebutuhan untuk mempertimbangkan beberapa masalah penting yang dihadirkannya, yaitu masalah privasi dan keamanan. Penelitian ini terutama membahas tentang keamanan mobile cloud computing. Oleh karena itu, studi ini akan memungkinkan untuk menghilangkan keraguan dan kekhawatiran yang menghentikan pengguna di semua tingkatan untuk mengadopsi dan bermigrasi ke teknologi ini. Teknologi komputasi cloud adalah pola baru di sektor TI dan telah secara mencolok mengubah cara penyampaian dan pemanfaatan teknologi informasi. Oleh karena itu, berdasarkan fakta-fakta ini, hanya ada sedikit penelitian yang dilakukan di bidang ini. Penelitian ini akan dilakukan di sekitar sektor publik, industri jasa keuangan di Indonesia (Gasparis, 2017).

2. TINJAUAN PUSTAKA

Cloud Computing telah mengembangkan dirinya sebagai teknologi yang berkembang dan muncul di dunia Teknologi Informasi (TI), yang menawarkan model pendekatan baru bagi perusahaan dan individu untuk menggunakan perangkat lunak, sumber daya perangkat keras, dan aplikasi. Mobile cloud computing menyediakan platform bagi Pengguna telepon seluler untuk memungkinkan mereka menggunakan layanan cloud di perangkat seluler mereka. Terlepas dari kemunculan dan evolusi luar biasa yang diwujudkan oleh mobile cloud computing, penggunanya masih di bawah ekspektasi karena risiko terkait, terutama privasi dan keamanan seluler yang menjadi semakin penting. Risiko-risiko ini secara signifikan telah menghentikan organisasi untuk merangkul lingkungan Mobile cloud computing telah menyajikan gambaran umum arsitektur keamanan mobile cloud (Jones, 2017).

Gupta dkk (2017), mengevaluasi keamanan browser seluler dan menemukan sebagian besar serangan dalam bentuk skrip lintas situs,

mereka menyediakan kerangka kerja untuk keamanan browser berbasis cloud. Gupta dan Gupta (2017) menunjukkan bahwa hampir semua aplikasi rentan terhadap ancaman keamanan. Penulis menemukan bahwa aplikasi berbasis PHP dan Java bertanggung jawab atas sebagian besar ancaman. Amrutkar, dkk. (2012) mengevaluasi keamanan browser seluler dan menyimpulkan bahwa sebagian besar browser menjadi sasaran serangan Man-in-the-Middle. Ini menyajikan pendekatan untuk membuktikan identifikasi lokasi pengguna dengan mudah dengan menggunakan serangan waktu, yaitu sniffing, pada cache browser pengguna. Hosmer, dkk. (2011) yang menunjukkan hasil serupa menyerang cache browser pengguna untuk mengumpulkan informasi penting tentang sejarah, mengusulkan pendekatan serupa. Dinh, dkk. (2013), telah mengusulkan kerangka kerja bersama dengan survei dan menjelaskan hal tersebut. Ini menyajikan semua solusi yang diusulkan dengan perincian tentang cara mengamankan infrastruktur mobile cloud dan juga mengidentifikasi semua kemungkinan masalah dalam Mobile cloud computing. Selain itu, penulis mengusulkan kerangka kerja baru untuk Mobile cloud computing. Kerangka yang diusulkan terutama difokuskan pada kepercayaan, manajemen risiko, dan keamanan perutean yang akan meningkatkan kerja jaringan seluler dan ad-hoc. Jouini, dan Rabai (2016), mempresentasikan kerangka kerja evaluator untuk mendeteksi ancaman keamanan terkait cloud. Mereka menggunakan analisis kegagalan biaya rata-rata dengan mempertimbangkan beberapa parameter dan melakukan analisis kuantitatif untuk mendeteksi ancaman. De (2016) dan Alizadeh, dkk. (2013) dalam penelitiannya menemukan definisi untuk Mobile cloud computing yang merupakan campuran dari komputasi cloud dan web seluler; yang merupakan instrumen paling terkenal bagi Pengguna Telepon seluler untuk memiliki akses ke berbagai layanan dan aplikasi yang ditawarkan di cloud melalui Internet. Banyak survei dan penelitian pendukung cloud potensial menunjukkan bahwa keamanan dan privasi adalah perhatian utama dan nomor satu yang menunda adopsi untuk bermigrasi ke teknologi ini (Abolfazli, dkk., 2014). Ada sejumlah besar kendala yang ada di bidang PKS, termasuk replikasi informasi, ketersediaan, skalabilitas, keamanan, integrasi, dan kelangsungan bisnis sumber daya cloud karena kurangnya standar infrastruktur cloud. Menurut survei yang dilakukan oleh Subashini dan Kavitha (2011), 74% Eksekutif TI dan Chief Information Officer tidak didorong untuk memigrasikan teknologi yang ada ke cloud karena risiko terkait terutama keamanan dan privasi. Beberapa peneliti menunjukkan ketertarikan

mereka pada teknologi baru ini; namun demikian, ada beberapa tantangan dan masalah di MCC karena beberapa batasan atau keterbatasan perangkat seluler seperti kapasitas penyimpanan yang terbatas, bandwidth yang terbatas dan daya baterai yang rendah, dan sejenisnya. Namun, keamanan adalah masalah utama di PKS. Dalam rangka membangun dan menjaga kepercayaan konsumen pada platform mobile. Dai dan Zhou (2010), berpendapat bahwa ini hanya dapat dicapai dengan perlindungan aplikasi dan data mereka dari musuh; dan dia mengusulkan platform 3G E-commerce yang menggabungkan keunggulan jaringan 3G dan komputasi cloud untuk meningkatkan kecepatan pemrosesan data dan tingkat keamanan. Platform ini menggunakan kontrol akses berbasis enkripsi PKI (infrastruktur kunci publik) untuk memastikan privasi akses pengguna ke data yang dialihdayakan.

2.1 Keamanan untuk Pengguna Telepon seluler

Perangkat seluler seperti telepon pintar, telepon seluler, dan asisten digital pribadi terpapar pada beberapa ancaman keamanan seperti kode berbahaya (seperti kuda Troya, worm, dan virus) serta kerentanan dan kelemahannya. Selain itu, dengan perangkat seluler yang menggabungkan peralatan sistem penentuan posisi global (GPS), mereka dapat menimbulkan masalah keamanan bagi pengguna (Fernando, Loke & Rahayu, 2013). Dua isu atau tantangan utama adalah sebagai berikut:

2.1.1 Keamanan Untuk Aplikasi Mobile

Keamanan model aplikasi atau aplikasi seluler cukup penting karena aplikasi ini menawarkan layanan yang lebih baik kepada klien dengan menggunakan sumber daya cloud; aplikasi seluler ini memanfaatkan layanan cloud untuk meningkatkan kemampuan perangkat seluler. Instalasi dan fungsi perangkat lunak keamanan seperti perangkat lunak antivirus AVG, Kaspersky dan McAfee di ponsel adalah cara termudah untuk mengidentifikasi ancaman keamanan pada perangkat, seperti kode berbahaya, worm, dan virus. Namun demikian, ponsel atau perangkat terhambat dalam kekuatan dan pemrosesannya, akibatnya, melindungi secara efektif dari ancaman dan ancaman keamanan lebih sulit dibandingkan dengan perangkat yang banyak akal seperti laptop. Misalnya, sangat tidak mungkin untuk tetap memfungsikan perangkat lunak penemuan virus di ponsel dan

perangkat. Dai dan Zhou (2010) mengusulkan pendekatan untuk menggeser atau memindahkan kemampuan deteksi ancaman ke cloud. Pendekatan ini merupakan perluasan dari platform Cloud Anti-Virus (CAV) saat ini yang menawarkan layanan in-cloud untuk deteksi virus.

2.1.2 Mengamankan Data di Cloud

Tantangan utama dalam memanfaatkan sistem pengamanan adalah melindungi data pelanggan seluler yang disimpan dalam mobile cloud. File atau data klien seluler sangat penting dan sensitif, dan perlu diamankan secara memadai karena setiap orang atau penyusup yang tidak berwenang dapat melakukan perubahan di dalamnya untuk memengaruhi data atau merusak data. Akibatnya, perhatian utama penyedia layanan cloud adalah menawarkan keamanan file atau data yang dibuat dan dikelola di server cloud atau perangkat seluler. Keamanan file atau data cukup penting dan esensial bagi pemilik file atau data, karena dapat berisi beberapa informasi sensitif dan rahasia pengguna ponsel (Morrow, 2012). Namun, baik pengembang aplikasi maupun Pengguna Telepon seluler memanfaatkan penyimpanan sejumlah besar data dan aplikasi di cloud, mereka harus berhati-hati dalam menangani aplikasi dan data terkait autentikasi, hak digital, dan integritas mereka (Morrow, 2012). Akibatnya, kekhawatiran terkait data dalam Mobile cloud computing adalah sebagai berikut:

Integritas

Terkadang Pengguna Telepon seluler menunjukkan kekhawatiran terkait integritas data mereka di dalam cloud. Banyak solusi tersedia untuk mengatasi masalah ini (Morrow, 2012). Namun demikian, solusi ini memperhitungkan konsumsi energi pengguna ponsel. Itani, dkk., (2010) telah mempertimbangkan konsumsi energi; paradigma mereka mencakup tiga elemen utama: layanan penyimpanan cloud, klien seluler, dan pihak ketiga yang tepercaya.

Autentikasi

Itani, dkk., (2010) telah menyajikan pendekatan otentikasi yang memanfaatkan komputasi cloud untuk melindungi akses data yang memadai untuk lingkungan seluler. TrustCube adalah berbasis kebijakan platform otentikasi cloud yang menggunakan standar terbuka dan menerima integrasi berbagai pendekatan dan teknik otentikasi. Penulis membangun sistem otentikasi tersembunyi yang memanfaatkan data seluler, seperti SMS, log panggilan, akses situs web, lokasi dan pesan,

untuk pengaturan seluler yang ada. Penulis membangun sistem otentikasi tersembunyi yang memanfaatkan data seluler, seperti SMS, log panggilan, akses situs web, lokasi dan pesan, untuk pengaturan seluler yang ada. Sistem menuntut pembatasan input yang mempersulit klien seluler untuk menggunakan hard password. Akibatnya, ini terkadang menghasilkan penggunaan kata sandi yang pendek dan sederhana. Dalam kasus di mana server web mendapat permintaan dari Pengguna Telepon seluler, server web mengarahkan ulang permintaan ke layanan terotentikasi terintegrasi (IA) dengan detail permintaan. IA kemudian mengambil kebijakan untuk permintaan akses, mengutip informasi yang perlu dikumpulkan, dan mengirim permintaan ke server IA melalui protokol dedicated network connect (TNC) yang terpercaya. Server IA mendapatkan pemeriksaan, menghasilkan laporan dan mengarahkannya kembali ke layanan IA. Setelah itu, layanan IA mengimplementasikan norma otentikasi dalam kebijakan, mengidentifikasi hasil otentikasi (apakah pengguna berhasil diautentikasi untuk pemeriksaan akses atau tidak), dan mentransfer hasil otentikasi kembali ke server web (Morrow, 2012).

2.1.3 Deteksi dan pencegahan penyusupan

Popularitas perangkat seluler yang semakin meningkat memikat penyusup untuk menyusup ke platform ini dengan memanfaatkan beragam kelemahan perangkat seluler, seperti malware dan kelemahan keamanan jaringan seluler. Misalnya, survei keamanan perangkat seluler yang dilakukan oleh Itani, dkk., (2010), mengungkapkan bahwa Trojan digunakan untuk merampok informasi rahasia yang dibicarakan melalui perangkat seluler dengan memanfaatkan dan menggunakan algoritma pengenalan suara. Ada banyak jaringan berbasis dan deteksi intrusi pada perangkat dan teknik jawaban yang sudah disarankan dalam literatur untuk mengatasi masalah keamanan perangkat seluler (Morrow, 2012). Sebagian besar dari mereka menyarankan solusi pada perangkat tidak memadai karena keterbatasannya yang besar seperti sumber daya komputasi, daya baterai, dan kapasitas memori. Selain itu, sebagian besar solusi yang disarankan mendeteksi pengguna yang berperilaku tidak semestinya atau malware dengan mengandalkan tanda tangan yang mereka peroleh dari database pusat tetapi memiliki penyimpanan kecil untuk menyimpan tanda tangan. Selain itu, deteksi terkait tanda tangan dapat dihindari dengan mudah dengan meluncurkan ancaman zero-day.

Solusi terkait jaringan mengatasi pembatasan sumber daya solusi pada perangkat, tetapi karena kurangnya umpan balik dan pengetahuan dari perilaku internal perangkat seluler, kinerja dan akurasinya terpengaruh secara intensif. Tahap yang sangat dibutuhkan setelah mendeteksi dan menyerang adalah respons otomatis terhadap serangan dan pemulihan keadaan sebelumnya, yang tidak ditangani oleh solusi terkait jaringan maupun pada perangkat yang disarankan sebelumnya (Abolfazli, dkk., 2014).

.

3. METODELOGI PENELITIAN

Penelitian ini terutama didasarkan pada pendekatan penelitian deduktif, karena hasilnya akan memverifikasi atau mengukur hubungan antara variabel atau teori yang ada; dan untuk membuktikan bahwa teori-teori yang ada yang dikembangkan dalam tinjauan pustaka sejalan dengan hasil dan temuan penelitian. Selain itu, pada bagian rekomendasi penelitian akan menganut pendekatan induktif, karena beberapa orientasi baru akan diberikan untuk menghasilkan teori-teori realitas baru. Dalam penelitian ini, berbagai pertanyaan dan solusi potensial didiskusikan dengan pemangku kepentingan yang berbeda seperti (Pengguna Telepon seluler, Praktisi IT, dan Perusahaan) selama penelitian, untuk meningkatkan pengetahuan peneliti dan penyedia Mobile cloud computing di lapangan. Selain itu, penelitian ini akan mengadopsi pendekatan kualitatif dan kuantitatif; karena data yang dikumpulkan akan dikuantifikasi dan juga akan bersifat kualitatif. Penelitian ini akan mengadopsi survei sebagai instrumen pengumpulan data dan survei secara tepat melalui kuesioner dari beberapa responden karena memungkinkan untuk mengumpulkan data mengenai situasi, praktik atau fenomena pada satu titik waktu melalui wawancara atau kuesioner. Untuk tujuan penelitian ini, 62 orang akan menjadi ukuran sampel, dan mereka semua akan dipilih di antara mahasiswa dan personel, yang memiliki latar belakang di bidang IT dan berlokasi di Indonesia.

4. HASIL DAN PEMBAHASAN

4.1 Hasil

Ada total 62 orang yang mengikuti survei, dan berdasarkan tabel di atas, dari 62, 54 adalah laki-laki dan 8 sisanya adalah perempuan. Dari 62

responden, 9% berusia 15 hingga 25 tahun; 37% berusia antara 25 hingga 35 tahun; 42% berusia antara 35 hingga 45 tahun; 10% berusia 45 hingga 55 tahun; dan hanya 3% berusia 55-65 tahun.

Pengetahuan tentang Mobile Cloud Computing

Sebagian besar responden 78% sudah mengenal dengan konsep komputasi cloud mobile karena kebanyakan dari mereka di mana individu dengan latar belakang TI; jadi konsep TI baru ini dikenal oleh sebagian besar dari mereka, dan dikenal dari yang lain. Sebagian besar responden memiliki sudut pandang positif mengenai mobile cloud Computing, karena sebagian besar dari mereka setuju bahwa teknologi ini telah merevolusi bidang teknologi untuk perangkat seluler; karena konsep ini memudahkan penggunaan perangkat seluler dan memberikan akses ke berbagai data dan informasi yang terkandung di cloud. Responden mengungkapkan bahwa, mobile cloud Computing menawarkan kepada pengguna ponsel dengan layanan penyimpanan dan pengolahan data di cloud. Perangkat seluler tidak perlu memiliki konfigurasi yang kuat seperti kecepatan unit prosesor pusat dan kapasitas memori yang besar; mengingat fakta bahwa semua tugas komputasi yang canggih dapat dieksekusi di cloud, dan bukan di ponsel, di mana kelebihan dari konsep ini.

Menyimpan informasi/dokumen sensitif di mobile cloud computing

Mengenai penyimpanan informasi/dokumen sensitif di mobile cloud computing, sebagian besar responden setuju (35% responden), Netral (25% responden) atau sangat setuju (20%) bahwa mereka menyimpan informasi/dokumen sensitif pada mobile cloud computing, sementara hanya 10% dan 9% yang tidak menyimpan data atau dokumen di mobile cloud computing.

Informasi tentang Data Sensitif dan Aman

Sebagian besar responden menyatakan bahwa informasi dan dokumen mereka yang disimpan di cloud aman; 40% responden tidak setuju 21% sangat tidak setuju. 17% setuju dan 5% Sangat setuju responden percaya

bahwa data yang disimpan di cloud aman, dan sisanya 17% netral. Selain itu, dari 62 responden, sebagian besar (90%) responden sangat setuju dan setuju, bahwa data pribadi harus dirahasiakan di cloud. Hanya sedikit (2%) yang tidak yakin dengan fakta bahwa ada kurangnya privasi untuk data di cloud; dan (8%) lainnya menyatakan netral.

Tantangan keamanan mobile cloud Computing

Tantangan keamanan umum yang meningkat dari responden terkait mobile cloud Computing dan perangkat yang terkait adalah; kehilangan atau pencurian perangkat seluler, kerentanan perangkat seluler terhadap ancaman berbahaya, kerentanan aplikasi seluler terhadap worm, virus, dan sejenisnya. Hasil survey menunjukkan bahwa pengguna telepon seluler percaya, perangkat seluler mudah dicuri atau hilang. Hal ini ditunjukkan dari hasil survey, dimana 25% responden sangat setuju dan 45% setuju bahwa perangkat seluler sering dicuri atau hilang dan sebagian besar di antara responden wanita. Hanya 10% yang tidak setuju, sedangkan 20% sisanya netral. Penyusupan adalah pelanggaran keamanan lain yang terpapar pada perangkat seluler di cloud, karena 15% responden setuju sepenuhnya dan 50% setuju bahwa mereka telah menjadi korban penyusupan di mobile cloud dan sisanya 15% skeptis tentang aspek ini. Sebagian besar pengguna, menyatakan bahwa aplikasi mobile yang diunduh di cloud rentan terhadap serangan virus, worm, dan trojan horse. Sebagian besar responden, 15% setuju sepenuhnya dan 60% setuju dengan fakta bahwa keamanan aplikasi terancam oleh worm, virus, dan trojan horse. Hanya 20% bersikap netral dan 5% tidak setuju.

Solusi yang ditawarkan

Beberapa solusi dapat diterapkan untuk mengatasi masalah keamanan dan privasi dalam mobile cloud Computing berdasarkan prespektif pengguna.

- Hasil survei ini menunjukkan bahwa 25% responden percaya, perlu ada solusi untuk memenuhi masalah privasi dan keamanan dalam mobile cloud computing, karena mereka percaya bahwa ini adalah salah satu faktor yang masih menahan orang untuk menerima

teknologi baru ini. Hanya 25% yang tidak setuju dan 50% yang netral.

- Berdasarkan data yang dikumpulkan dari peserta survei, 31% setuju bahwa anti virus pada telepon seluler seperti dapat digunakan untuk mengatasi ancaman keamanan dalam mobile cloud computing. 18% responden tidak percaya bahwa anti virus itu solusi untuk masalah keamanan dalam mobile cloud computing dan 39% di antaranya netral.
- 64% setuju dan 25% setuju sepenuhnya dengan pernyataan bahwa harus ada akses rahasia ke data mereka di mobile cloud computing, sehingga pihak ketiga tidak boleh memiliki akses ke data ini dan oleh karena itu, menjaga privasi data rahasia. 5% responden tidak setuju karena mereka percaya bahwa beberapa data mereka yang tidak sensitif dapat diakses oleh pihak ketiga, dan 6% netral
- Hasil dari perpektif responden terkait biometrik dapat digunakan untuk memberikan akses ke data atau perangkat seluler seperti sidik jari atau nada suara adalah sebagai berikut; 55% responden setuju dan 16% setuju sepenuhnya bahwa penggunaan biometrik dapat digunakan untuk mengontrol akses ke data atau perangkat seluler, karena informasi seperti sidik jari adalah unik untuk setiap pengguna dan oleh karena itu tidak dapat diduplikasi oleh orang lain. Ini tampak bagi mereka sebagai cara yang efektif untuk mengontrol akses ke data.

4.2 Pembahasan

Responden dari penelitian ini adalah kelompok terpilih, yang semuanya ahli TI, memberikan beberapa jawaban menarik yang secara signifikan berkontribusi pada penyelesaian penelitian ini. Meskipun teknologi mobile cloud masih baru, mereka semua sudah mengenal dengan teknologi ini. Perbedaan utama antara komputasi cloud dan mobile cloud computing adalah mobilitas pengguna dan perangkat yang digunakan untuk mengakses layanan atau aplikasi dari cloud. Responden mengungkapkan bahwa mobile cloud computing meningkatkan masalah

privasi dan keamanan yang dihadapi. Timbul masalah dalam identifikasi dan autentikasi, karena terkadang identitas dan autentikasi pemilik perangkat atau pemilik data yang ada di cloud tidak sepenuhnya diremote. Selain itu, mereka juga menyatakan masalah pada kontrol akses yang mengharuskan ada cara untuk mengatur atau mengontrol siapa yang mengakses apa saja dan memastikan bahwa orang hanya mengakses layanan, data, dan aplikasi yang mereka sudah berhak atau yang mereka miliki. Disarankan juga bahwa pengguna harus memiliki privasi dalam akses mereka ke cloud, dan akses ke konten hanya milik mereka untuk menjaga kerahasiaan dan kerahasiaan mereka dan sementara itu memastikan bahwa data mereka dilindungi. Dan tidak dapat diakses oleh pihak lain. Solusi yang dapat ditawarkan berdasarkan prespektif pengguna adalah penggunaan antivirus untuk untuk menghambat serangan virus dan malware di perangkat seluler. Hasil survei juga menyarankan penerapan biometrik terenkripsi untuk mengakses ke cloud dan dokumen.

5. KESIMPULAN

Penelitian ini terutama mengelaborasi keamanan data yang disimpan di cloud dan pentingnya keamanan data. Sementara mobile cloud computing memiliki potensi yang cukup besar untuk memungkinkan mobile server memiliki akses ke sumber daya dan aplikasi yang andal dan kuat kapan saja dan di mana saja, kita harus mempertimbangkan banyak tantangan yang terdiri dari keamanan dan privasi, dan juga keandalan dalam menerapkan mobile cloud computing. Kami telah mengidentifikasi masalah privasi dan keamanan pada mobile cloud computing dan juga telah membahas beragam mekanisme untuk mengatasi masalah ini. Penelitian ini telah menguraikan beberapa cara untuk memberikan keamanan data, kontrol akses, kerahasiaan serta integritas data dan pengguna seluler, sehingga sejumlah besar pengguna seluler di masa depan dapat mengadopsi mobile cloud computing secara luas.

.

Daftar Pustaka

[1] IDC 2018 International Data Corporation, report 2015 available at http://www.idc.com/research/Predictions15/index.jsp

[2] Krishnan, R. (2017). Security and Privacy in Cloud Computing.

[3] Gasparis, I. (2017). Ensuring Users' Privacy and Security on Mobile Devices (Doctoral dissertation, University of California, Riverside).

[4] Jones, S., Irani, Z., Sivarajah, U., & Love, P. E. (2017). Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies. Information Systems Frontiers, 1-24.

[5] Gupta, B. B., Gupta, S., & Chaudhary, P. (2017). Enhancing the Browser-Side Context-Aware Sanitization of Suspicious HTML5 Code for Halting the DOM-Based XSS Vulnerabilities in Cloud. International Journal of Cloud Applications and Computing (IJCAC), 7(1), 1-31.

[6] Gupta, S., & Gupta, B. B. (2017). Detection, Avoidance, and Attack Pattern Mechanisms in Modern Web Application Vulnerabilities: Present and Future Challenges. International Journal of Cloud Applications and Computing (IJCAC), 7(3), 1-43.

[7] Amrutkar, C., Traynor, P., & Van Oorschot, P. C. (2012). Measuring SSL indicators on mobile browsers: Extended life, or end of the road?. In International Conference on Information Security (pp. 86-103). Springer, Berlin, Heidelberg.

[8] Hosmer, C., Jeffcoat, C., Davis, M., & McGibbon, T. (2011). Use of mobile technology for information collection and dissemination. Data & Analysis Center for Software, 77.

[9] Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18), 1587- 1611.

[10] Jouini, M., & Rabai, L. B. A. (2016). A Security Framework for Secure Cloud Computing Environments. International Journal of Cloud Applications and Computing (IJCAC), 6(3), 32-44.

[11] De, D. (2016). Mobile cloud computing: architectures, algorithms and applications. CRC Press.

[12] Alizadeh, M., Hassan, W. H., Behboodian, N., & Karamizadeh, S. (2013). A brief review of mobile cloud computing opportunities. Research Notes in Information Science, 12, 155-160.

[13] Abolfazli, S., Sanaei, Z., Ahmed, E., Gani, A., & Buyya, R. (2014). Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges. IEEE Communications Surveys & Tutorials, 16(1), 337-368.

[14] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
[15] Dai, J., & Zhou, Q. (2010). A PKI-based mechanism for secure and efficient access to outsourced data. In Networking and Digital Society (ICNDS), 2010 2nd International Conference on (Vol. 1, pp. 640-643). IEEE.
[16] Khan, A. N., Kiah, M. M., Khan, S. U., & Madani, S. A. (2013). Towards secure mobile cloud computing: A survey. Future Generation Computer Systems, 29(5), 1278-1299.
[17] Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. Network Security, 2012(12), 5-8.
[18] Itani, W., Kayssi, A., & Chehab, A. (2010). Energy- efficient incremental integrity for securing storage in mobile cloud computing. In Energy Aware Computing (ICEAC), 2010 International Conference on (pp. 1-2). IEEE.