TINJAUAN KEAMANAN SISTEM PADA TEKNOLOGI *CLOUD COMPUTING*

Yuli Fauziah
Program Studi Teknik Informatika Fakultas teknologi Industri
UPN "Veteran" Yogyakarta
yuli.if@gmail.com

Abstrak

Dalam perspektif teknologi informasi, cloud computing *atau komputasi awan dapat diartikan sebagai suatu teknologi yang memanfaatkan internet sebagai* resource *untuk komputasi yang dapat di*-request *oleh pengguna dan merupakan sebuah layanan dengan pusat server bersifat virtual atau berada dalam* cloud *(internet) itu sendiri. Banyak perusahaan yang ingin memindahkan aplikasi dan storage-nya ke dalam cloudcomputing. Teknologi ini menjadi trend dikalangan peneliti dan praktisi IT untuk menggali potensi yang dapat ditawarkan kepada masyarakat luas. Tetapi masih banyak isu keamanan yang muncul, karena teknologi yang masih baru. Salah satu isu keamanannya adalah Theft of Information, yaitu pencurian terhadap data yang disimpan di dalam Storage aplikasi yang menggunakan teknologi Cloud Computing. Kerugian yang akan diperoleh oleh pengguna teknologi ini sangat besar, karena informasi yang dicuri menyangkut data rahasia milik perusahaan, maupun data-data penting lainnya.*

Beberapa tindakan untuk mencegah terjadinya pencurian data ini, yaitu dengan menghindari jenis ancaman keamanan berupa kehilangan atau kebocoran data dan pembajakan account atau service, serta Identity Management *dan* access control *adalah kebutuhan yang utama bagi SaaS Cloud computing perusahaan. Dan salah satu metode yang digunakan dalam keamanan data aspek autentikasi dan otorisasi pada aplikasi atau service cloud computing adalah teknologi Single-sign-on. Teknologi Single-sign-on (SSO) adalah teknologi yang mengizinkan pengguna jaringan agar dapat mengakses sumber daya dalam jaringan hanya dengan menggunakan satu akun pengguna saja. Teknologi ini sangat diminati, khususnya dalam jaringan yang sangat besar dan bersifat heterogen, juga pada jaringan cloud computing. Dengan menggunakan SSO, seorang pengguna hanya cukup melakukan proses autentikasi sekali saja untuk mendapatkan izin akses terhadap semua layanan yang terdapat di dalam jaringan.*

Kata Kunci : *Storage, Aplikasi, Software as a Service, Cloud Computing,* Identity Management, access control, *Single Sign On*

1. PENDAHULUAN

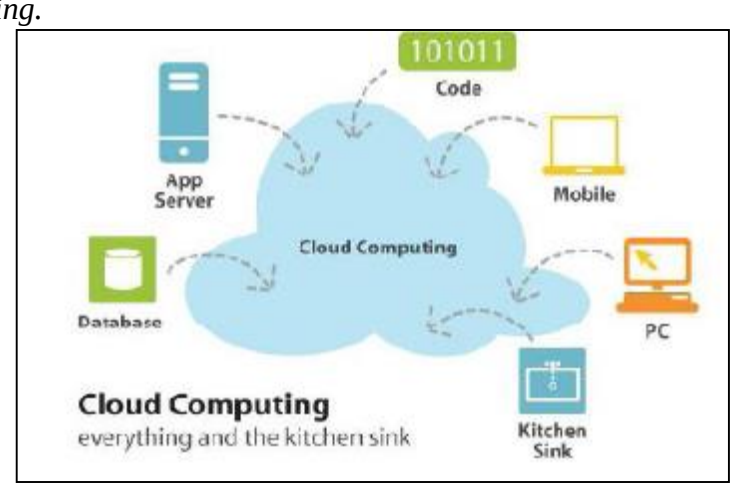
Komputasi awan (*cloud computing*) adalah gabungan pemanfaatan teknologi komputer (komputasi) dan pengembangan berbasis Internet (awan). Awan (*cloud*) adalah metefora dari internet, sebagaimana awan yang sering digambarkan di diagram jaringan komputer. Sebagaimana awan dalam diagram jaringan komputer tersebut, awan dalam *cloud computing* juga merupakan abstraksi dari infrastruktur kompleks yang disembunyikannya. *cloud computing* adalah suatu metoda komputasi di mana kapabilitas terkait teknologi informasi disajikan sebagai suatu layanan, sehingga pengguna dapat mengaksesnya lewat Internet, tanpa mengetahui apa yang ada di dalamnya.

Dikutip dari sebuah makalah tahun 2008 yang dipublikasi IEEE *Internet Computing*, komputasi awan adalah suatu paradigma di mana informasi secara permanen tersimpan di server di internet dan tersimpan secara sementara di komputer pengguna, termasuk di dalamnya adalah desktop, komputer tablet, notebook, dan lain-lain.

2. TEKNOLOGI *CLOUD COMPUTING*

Teknologi *Cloud Computing* dapat didefinisikan secara sederhana sebagai sebuah perusahaan dengan pusat data yang menyediakan rental *Space Storage*. Perusahaan ini hanya menyediakan Infrastruktur untuk tempat penyimpanan data dan aplikasi dari suatu perusahaan.

Menurut A. Rifai ZA (2010) dalam e-book "Cloud Computing Strategies" karangan Dimitris N. Chorafas menjelaskan *Cloud Computing* sebagai *Teknologi On-Demand*, yaitu teknologi *Cloud Computing* merupakan teknologi yang berbasiskan pada permintaan dari *User*. Teknologi ini merupakan salah satu titik perubahan (*Inflection Point*), tidak hanya aplikasi perangkat lunak yang berbasiskan *Cloud Computing* juga meliputi *plaform*, infrastruktur basis data maupun pelayanan dapat berbasiskan *Cloud Computing.*



Gambar 1. Permodelan dalam Teknologi *Cloud Computing*

2.1. Manfaat *Cloud Computing*

Ada banyak alasan mengapa teknologi *cloud computing* menjadi pilihan bagi pengusaha dan praktisi IT saat ini, yakni adanya beberapa keuntungan yang dapat dimanfaatkan dari perkembangan *Cloud Computing* ini (Marks, 2010), seperti :

1. Lebih efisien karena menggunakan anggaran yang rendah untuk sumber daya
2. Membuat lebih *eglity*, dengan mudah dapat berorientasi pada profit dan perkembangan yang cepat
3. Membuat operasional dan manajemen lebih mudah, dimungkinkan karena sistem pribadi atau perusahaan yang terkoneksi dalam satu *cloud* dapat dimonitor dan diatur dengan mudah
4. Menjadikan koloborasi yang terpecaya dan lebih ramping

5. Membantu dalam menekan biaya operasi biaya modal pada saat *reliability* ditingkatkan dan kritikal sistem informasi yang dibangun.

2.2. Karakteristik *Cloud Computing*

Cloud computing memiliki beberapa karakteristik dasar, diantaranya (Marks, 2010):

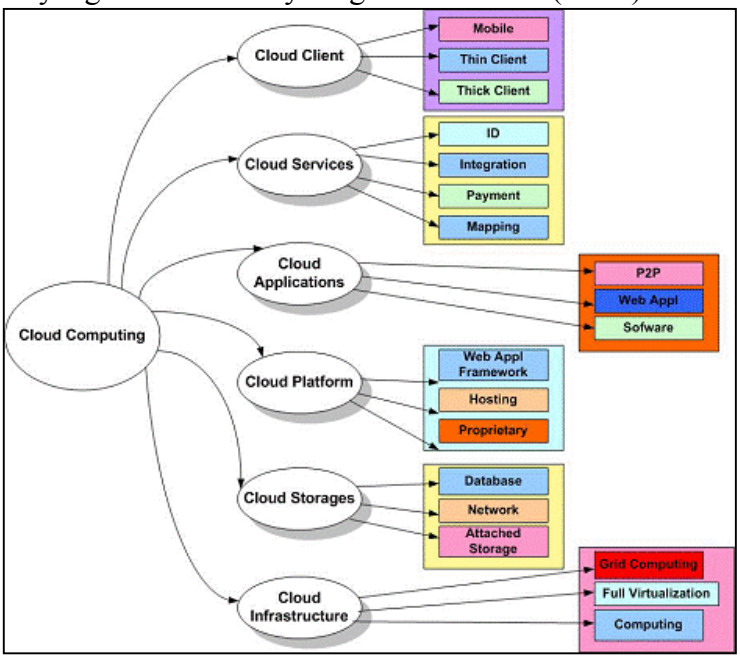
1. *Scalable* (*Aggregate*), Pada karakteristik ini cloud computing memiliki kemampuan untuk menyediakan kebutuhan sesuai dengan permintaan yang diperlukan oleh user.
2. *Elastic*, pada karakterisktik ini cloud computing memiliki kemampuan untuk menaikkan atau menurunkan daya operasional terhadap aplikasi yang sedang digunakan.
3. *Self-service on demand*, Kebutuhan aplikasi disesuaikan dengan permintaan dari user.
4. *Ubiquitous access* (service and more), kemampuan untuk dapat diakses dari mana saja menggunakan perangkat apa saja (device atau application) .
5. *Complete virtualization*: acts as one, pada sejarahnya komputasi komputer terkait dengan teknologi mengenai mainframes, SAN (storage area networks), NAS (network attach storage), dan yang lainnya hanya berjalan pada sebuah infrastruktur. Pada karakteristik ini diubah cara kerjanya sehingga dapat bekerja pada beragam infrastruktur yang dikenal dengan istilah virtualization. Untuk mendukung kemampuan ubiquitous.
6. *Relative consistency*, mendukung dari teknologi virtualisasi maka dapat menghemat biaya dalam pemanfaatan teknologi informasi.
7. *Commodity*, jika argumen mengenai *cloud computing* dapat menjalankan beberapa infrastruktur maka sudah tentu menjadi kebutuhan utama dalam penyediaan perangkat teknologi informasi atau memungkinkan penyewa bisa lebih untuk sebuah aplikasi.

2.3. Layanan *Cloud Computing*

Sementara layanan utama yang disediakan oleh cloud computing dibagi menjadi 3 bagian, diantaranya (Balboni, 2009) :

1. *IaaS* (*Infrastructure as a Service*), kemampuan dalam menetapkan ketersediaan perangkat keras kepada konsumen meliputi: *processing*, *storage*, *networks* dan *other fundamental computing resource*. Termasuk sistem operasi dan aplikasi-aplikasi.
2. *PaaS* (*Platform as a Service*), kemampuan dalam menyediakan layanan kepada konsumen untuk dapat membangun aplikasi yang mendukung kedalam infrastruktur *cloud computing* dengan menggunakan bahasa pemrograman sehingga aplikasi tersebut dapat berjalan pada platform yang telah disediakan.
3. *SaaS* (*Software as a service*), kemampuan dalam menyediakan layanan yang ditujukan kepada konsumen untuk dapat menjalankan aplikasi di atas infrastruktur *cloud computing* yang telah disediakan.

Trend saat ini adalah dapat memberikan berbagai macam layanan secara terdistribusi dan pararel secara *remote* dan dapat berjalan di berbagai *device*, dan teknologinya dapat dilihat dari berbagai macam teknologi yang digunakan dari proses informasi yang dilakukan secara *outsourcing* sampai dengan penggunaan eksternal data center (Balboni, 2009). *Cloud Computing* merupakan model yang memungkinkan dapat mendukung layanan yang disebut ”Everything-as-a-service” (XaaS).



Gambar 2. Struktur cloud computing
(sumber : deris.unsri.ac.id/materi/jarkom/mengenal_cloudcomputing.pdf)

3. PEMBAHASAN

3.1 Keamanan Jaringan Informasi

Kemanan jaringan informasi pada *cloud computing* adalah topik yang sangat luas. Keamanan jaringan informasi pada *cloud computing*, khususnya dari segi komunikasi datanya (*secure communication*). Faktor-faktor Kemanan jaringan informasi pada cloud computing (komunikasinya) :

- Struktur,
- Metode transmisi,
- Transport formats,
- Perhitungan keamanan yang mendukung : integrity, availability, dan authentication (untuk *private* dan *public* jaringan komunikasi).

Diketahui juga komunikasi pada *cloud computing* dikatakan aman jika telah memastikan beberapa hal yaitu :

1. ***Confidentiality***
   Kepastian bahwa hanya orang/bagian yang berhak atau yang seharusnya, yang boleh mengakses data dan menerima data. Beberapa hal yang

menjadi bagian dari kebutuhan telekomunikasi dalam menjamin *confidentiality* :

- *Network security protocols*
- *Network authentication services*
- *Data encription services*

2. ***Integrity***

   kepastian bahwa data tidak berubah karena suatu yang tidak direncanakan atau tidak diinginkan. *Integrity* berarti menjamin pesan telah terkirim dan diterima. Dan pesan tersebut tidak berubah.

   Beberapa bagian dari *integrity* yaitu :

   - *Firewall servicess*
   - *Communications Security Management*
   - *Intrusion detection services*

3. ***Availability***

   Kepastian bahwa data atau informasi pada jaringan dapat diakses di waktu dan dimana data/informasi itu dibutuhkan. User yang terotorisasi dapat diijinkan mengakses jaringan atau sistem saat dibutuhkan. Beberapa bagian yang harus diperhatikan untuk menjamin *availability* yaitu :

   - *Fault tolerance* untuk *availability* data, seperti *backups, redundant disk system*
   - *Acceptable logins and operating process performances*
   - *Reliable and interoperable security processes and network security mechanisms*

   Selain *secure communications* , yang harus diperhatikan yaitu *secure execution environments*, namun hal tersebut tidak dibahas dalam makalah ini.

3.2 Keamanan Teknologi *Cloud Computing*

Cloud Computing menyajikan banyak tantangan organisasi. Bila organisasi berpindah ke layanan komputasi awan publik tentu infrastruktur sistem komputasi dikendalikan oleh pihak ketiga yaitu *Cloud Service Provider* (CSP) dan tantangan ini harus ditangani melalui inisiatif manajemen. Inisiatif manajemen ini akan memerlukan gambaran jelas peran kepemilikan dan tanggung jawab dari CSP dan organisasi yang berperan sebagai pelanggan. Dalam Presentasi yang dilakukan oleh *Security Issues in Cloud Computing*, Saurabh K Prashar menyatakan bahwa masalah *security* merupakan masalah utama yang timbul dengan adanya teknologi *Cloud Computing*. Dengan adanya teknologi ini, keamanan data dari setiap *user* tidak dapat terjamin, karena setiap data dan informasi yang dimiliki terdapat di *Cloud* atau di internet tepatnya. Hal ini menjadi isu utama dari teknologi *Cloud Computing*

Cloud Computing merupakan teknologi yang sekarang sedang banyak diadopsi dan menjadi trend dalam proyek-proyek teknologi informasi. Kemanan jaringan informasi pada *cloud computing* adalah topik yang sangat luas. Ada banyak Aspek yang dapat dilihat dalam mengkaji celah keamanan pada *cloud computing*. Misalnya berdasarkan model layanan-layanan pada *cloud computing* dapat dilihat, apakah celah keamanan jaringan informasi

tersebut berada pada model layanan *Software as a Service*, dan atau *Platform as a Service*, dan atau apakah pada *Infrastructure as a Service*.

3.2.1 Bahaya pada Teknologi Cloud Computing

Dengan adanya aspek keamanan, dapat mencegah *danger* atau bahaya dan *vulnerabilities* atau aspek kerentanan terhadap suatu aplikasi yang mengadaptasi teknologi *Cloud Computing*. Untuk aspek *danger* yang dapat timbul dari penggunaaan teknologi *Cloud Computing* antara lain (Setiawan, 2010) :

a. *Disrupts Services*
   Maksudnya adalah layanan terganggu, biasanya hal ini terjadi karena faktor alam, karena cuaca yang kurang baik sehingga koneksi tidak dapat berjalan dengan baik atau adanya bencana alam yang membuat server penyedia layanan bermasalah dan tidak dapat berjalan sebagaimana semestinya.
b. *Theft of Information*
   Hal inilah yang akan dibahas secara lebih mendalam di dalam makalah ini. Pencurian data menjadi isu yang cukup menarik, karena banyaknya cara-cara pencurian data seperti DoS (*Denial of Service*) maupun tipe pencurian data yang lain. Aplikasi dengan teknologi *Cloud Computing* merupakan aplikasi yang sangat rentan dengan pencurian data. Hal ini karena data disimpan di server yang berada di internet, sedangkan jaringan di internet sangat rentan untuk disadap atau dicuri.
c. *Loss of Privacy*
   Bahaya ini adalah dengan hilangnya *Privacy* dari User atau pengguna karena menyerahkan dokumen yang dianggap penting dan rahasia kepada pihak penyedia pelayanan. Hal ini cukup membahayakan bila terjadi kebocoran data. Selain itu hal – hal pribadi milik pengguna sudah tidak dapat terjamin lagi kerahasiannya.
d. *Damage information*
   Data yang dimasukkan melalui jaringan internet dapat rusak, hal ini karena koneksi jaringa yang kurang baik, sehingga data menjadi *corrupt* dan juga tidak digunakan kembali. Hal ini cukup mengganggu bila data yang rusak cukup banyak dan tidak memiliki *Backup*.

3.2.2 Keamanan Data dan Layanan

Pencurian data dalam teknologi *Cloud Computing* merupakan salah satu isu keamanan yang cukup besar. Hal ini karena setiap *hacker* dapat menggunakan berbagai cara untuk mendapatkan informasi yang dibutuhkan dari suatu perusahaan tertentu. Ada beberapa cara untuk dapat mencegah hal ini dapat terjadi. Beberapa cara pencurian data dapat dilakukan dengan cara sebagai berikut (Setiawan, 2010) :

- *Denial of Service*
- *QoS Violation*

- *IP Spoofing*
- *Port Scanning*
- *ARP Cache Attack*

Keamanan untuk *Cloud Computing* dilakukan pada level – level seperti di bawah ini :

- *Server access security*
- *Internet access security*
- *Database / Datacenter access security*
- *Data privacy security*
- *Program access Security*

Setiap level di atas, harus diberikan keamanan yang baik. Misal untuk *server acces* akan diberikan *firewall* yang baik, agar tidak dengan mudah server ditembus oleh *hacker*. Secara khusus akan dibahas mengenai keamanan di dalam *datacenter access security*. Data dapat dicuri secara fisik yaitu mengambil data langsung ke pusat pata/*data* center maupun dapat mencuri dengan cara *hacking* langsung ke dalam basis data. Untuk keamanan di dalam Sebuah data center diperlukan beberapa hal untuk mencegah terjadinya pencurian informasi, hal ini lebih kearah fisik untuk pengamanan data center. Pengamanan ini dilakukan oleh pihak penyedia layanan.

Adapun prosedur keamanan (Setiawan, 2010) yang dapat dilakukan adalah sebagai berikut :

- Penggunaan petugas keamanan yang profesional yang dilengkapi dengan kamera pengawas dan berbagai sistem keamanan yang lainnya.
- Untuk setiap petugas yang sudah tidak bertugas di dalam pusat data harus dihapus hak aksesnya untuk dapat masuk ke dalam pusat data. Bila hal ini tidak dilakukan, maka akan sangat dimungkin bila pencurian data dapat dilakukan.
- Setiap akses secara elektronik dan akses secara fisik ke dalam pusat data yang dilakukan oleh pegawai harus dilakukan audit secara rutin. Hal ini dimaksudkan agar perusahaan dapat mengetahui *track record* dari setiap pegawai.
- Digunakan aplikasi untuk melakukan proses audit,hal ini dilakukan agar dapat mengetahui bagaimana data disimpan, dijaga, digunakan dan data tersebut akan diverifikasi dengan peraturan yang sudah ada.

Selain itu untuk keamanan sebuah pusat data diperlukan tempat penyimpanan yang mudah dijangkau tetapi dengan tingkat keamanan yang tinggi dan juga diperlukan sebuah *Backup Storage.*

Sedangkan untuk pengamanan dari segi digital (Setiawan, 2010), dapat digunakan beberapa cara sebagai berikut :

- Dapat dibuat 1 buah server yang berada di *Front-End*. Server ini berfungsi untuk menjadi server palsu, yang di dalamnya bukan berisi data asli milik Perusahaan Penyedia Pelayanan, dapat dibuat juga beberapa *server storage* seperti ini agar dapat mengelabui para *hacker* yang akan melakukan pencurian data.

- Untuk keamanan juga dapat digunakan authentifikasi yang berlapis. Hal ini dimaksudkan agar keamanan dapat berlapis dan juga hanya beberapa user saja yang memiliki *Privilledge* khusus yang dapat mengakses Data Center utama.
- Dapat menggunakan koneksi VPN (*Virtual Private Network*), dimana antara Server dan User dapat saling berhubungan di dalam satu jalur saja. Jalur Khusus ini dapat membantu keamanan jaringan.
- Diperlukan juga satu layer khusus untuk *Anti-Virus*, hal ini juga dapat mencegah bila ada penyusup yang akan masuk ke dalam aplikasi.

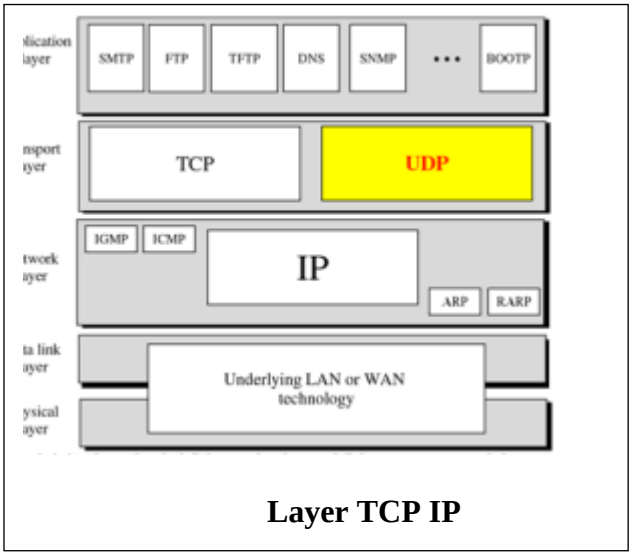
3.2.3 Keamanan cloud computing dari sisi model layanan *Software as a Service*

Ada banyak isu seputar keamanan pada cloud computing. Dari sebuah dokumen penelitian yang dikeluarkan oleh *Cloud Security Alliance's* yang berjudul *Top Threats to Cloud Computing*. Dengan teknologinya yang memudahkan konsumen untuk dapat mengakses layanan *cloud* melalui *web browser* atau layanan *web*, ada tiga contoh masalah keamanan yaitu :*XML Signature Element Wrapping, Browser Security, Cloud Malware Injection Attack and Flooding Attacks*.

Ancaman keamanan pada *cloud computing* yaitu kehilangan atau kebocoran data dan pembajakan account atau service (Krutz, 2010). Dua ancaman tersebut sangat krusial karena mempengaruhi reputasi, kepercayaan mitra, karyawan, dan juga pelanggan sehingga mempengaruhi bisnis. Pembajakan *account* juga dapat berakibat buruk jika *attackers* mengakses bagian yang sangat penting dari servis dalam *cloud computing*, memudahkan *attackers* kemudian untuk melakukan hal-hal yang dapat mempengaruhi aspek *confidentiality*, *integrity*, dan *availability* dari servis yang ada. Untuk menghindari jenis ancaman keamanan di atas, *Identity Management* dan *access control* adalah kebutuhan yang utama bagi *SaaS Cloud computing* Perusahaan.

Identity Management pada *cloud computing* juga terkait dengan fokus bahasan pada paper ini, yaitu keamanan cloud computing dari sisi model layanan *Software as a Service*-nya. Dengan penjelasan detail sebelumnya mengenai komponen-komponen pembentuk sebuah *SaaS* pada *Cloud Computing yaitu* menggunakan *Service Oriented Architecture (*SOA*)* dengan *Web Services standart* (bahasa xml).

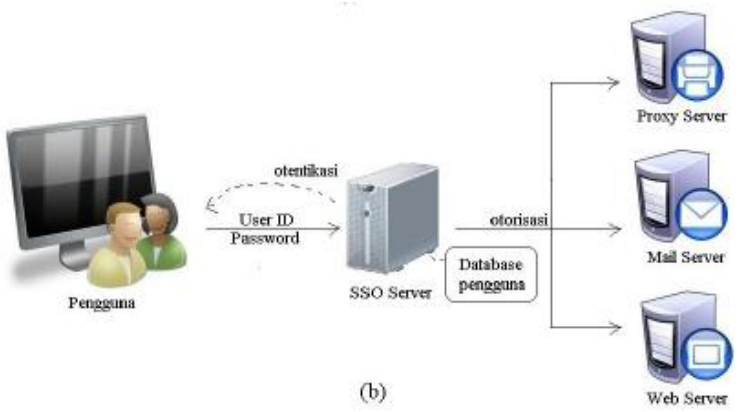
Berdasarkan model layanan-layanan pada cloud computing dapat dilihat, apakah celah keamanan jaringan informasi tersebut berada pada model layanan *Software as a Service*, dan atau *Platform as a Service*, dan atau apakah pada *Infrastructure as a Service.* Selanjutnya sisi keamanan cloud computing juga dapat dilihat dari letaknya pada protokol yang mengatur komunikasi data tersebut di dalam jaringan. Protokol yang dijadikan referensi dalam paper ini yaitu protokol TCP/IP *(Transmission Control Protocol/Internet Protocol).* Pembagian layer-layer pada protokol TCP/IP dapat dilihat pada gambar berikut :



Gambar 3. Layer-Layer pada protokol TCP/IP

3.2.4 Metode *Single Sign On* sebagai solusi keamanan *SaaS* pada *Cloud Computing*

Salah satu solusi untuk *identity management* dan *access control* adalah dengan mengunakan metode *Single Sign On*. Teknologi *Single-sign-on* (sering disingkat menjadi SSO) adalah teknologi yang mengizinkan pengguna jaringan agar dapat mengakses sumber daya dalam jaringan hanya dengan menggunakan satu akun pengguna saja (Wikipedia, 2007). Teknologi ini sangat diminati, khususnya dalam jaringan yang sangat besar dan bersifat heterogen (di saat sistem operasi serta aplikasi yang digunakan oleh komputer adalah berasal dari banyak *vendor*, dan pengguna dimintai untuk mengisi informasi dirinya ke dalam setiap *platform* yang berbeda tersebut yang hendak diakses oleh pengguna). Dengan menggunakan SSO, seorang pengguna hanya cukup melakukan proses autentikasi sekali saja untuk mendapatkan izin akses terhadap semua layanan yang terdapat di dalam jaringan.



Gambar 4. Sistem Single Sign On

Dalam sistem *single sign on*, *service providers* percaya sepenuhnya kepada *identity providers*. Para pengguna web yang mencoba untuk mengakses *service providers*-nya akan diarahkan langsung ke *identity providers* .Setelah pengguna terotentikasi oleh *identity providers, user* tersebut dapat mengakses servisnya yang lain tanpa memasukkan *username* dan *password* kembali. Dengan tidak diperlukannya memasukkan *username* dan *password* berulang kali di beberapa tempat, selain dapat memberikan kenyamanan bagi *user* juga dapat mengurangi kemungkinan adanya *phising* .

3.2.4.1 Arsitektur Sistem *Single Sign-On*

Beberapa arsitektur dari sistem SSO telah muncul, masing-masing dengan berbagai keunggulan dan infrastruktur yang berbeda. Pada umumnya sistem SSO memiliki beberapa keuntungan, antara lain (Wikipedia, 2007) :

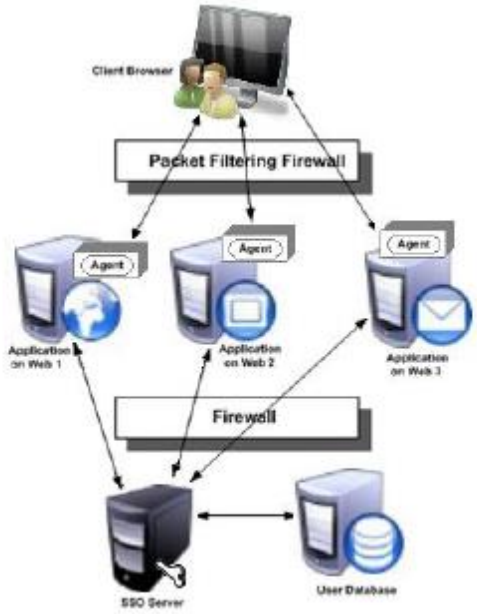
1. Pengguna tidak perlu mengingat banyak *username* dan *password*.
   Cukup dengan satu *credential*, sehingga pengguna cukup melakukan proses otentikasi sekali saja untuk mendapatkan izin akses terhadap semua layanan aplikasi yang tersedia di dalam jaringan.
2. Kemudahan pemrosesan data.
   Jika setiap layanan aplikasi memiliki data pengguna masing-masing, maka pemrosesan data pengguna (penambahan, pengurangan, perubahan) harus dilakukan pada setiap aplikasi yang ada. Sedangkan dengan menggunakan sistem SSO, cukup hanya melakukan sekali pemrosesan pada *server database backend*-nya. Hal ini menyatakan bahwa penggunaan sistem SSO meningkatkan efisiensi waktu dan kepraktisan dalam memproses data.
3. Tidak perlu membuat data pengguna yang sama di setiap aplikasi
   Karena setiap layanan aplikasi dalam jaringan dapat terhubung langsung dengan *server database backend* ini, maka hanya dengan sekali saja meng*input*data kedalam *database, credential* pengguna akan *valid* di seluruh layanan aplikasi.
4. Menghemat biaya untuk pemeliharaan *password*.
   Ketika harus me-*reset password* karena pengguna lupa pada *password*-nya, pengelola layanan tidak perlu menghabiskan waktu dan *bandwith* untuk menemukan data *credential* pengguna.

Solusi sistem SSO didasarkan pada salah satu dari dua tingkat pendekatan, yaitu pendekatan *script* dan pendekatan *agent* (Nurdeni, 2010). Pendekatan *agent* lebih digunakan dalam makalah ini karena dianggap lebih cocok untuk layanan

aplikasi berbasis *web* atau dikenal juga sebagai *service provider* (SP). Gambar 5 menunjukkan pembagian dari pendekatan sistem SSO.

Gambar 5. Pendekatan sistem SSO

Agent merupakan sebuah program kecil yang berjalan pada tiap-tiap *web server*. *Agent* ini membantu mengkoordinir aliran kerja dari sistem SSO dalam hal otentikasi pengguna dan penanganan sesi. Solusi dari arsitektur sistem SSO ditunjukkan oleh Gambar 6.



Gambar 6 Arsitektur Sistem SSO

Arsitektur Sistem SSO (Nurdeni, 2010) memiliki dua bagian utama, yaitu *agent* yang berada di *web server*/Layanan aplikasi dan sebuah *server* SSO berdedikasi yang mana akan dijelaskan berikut ini:

- ***Agent*:** Sebuah *agent* akan menterjemahkan setiap permintaan *HTTP* yang masuk ke *web server*. Hanya ada satu agent di tiap-tiap *web server*, yang mana *host* bagi layanan aplikasi. Agent

tersebut akan berinteraksi dengan *web browser* pada sisi pengguna, dan dengan *server* SSO pada sisi layanan aplikasi.

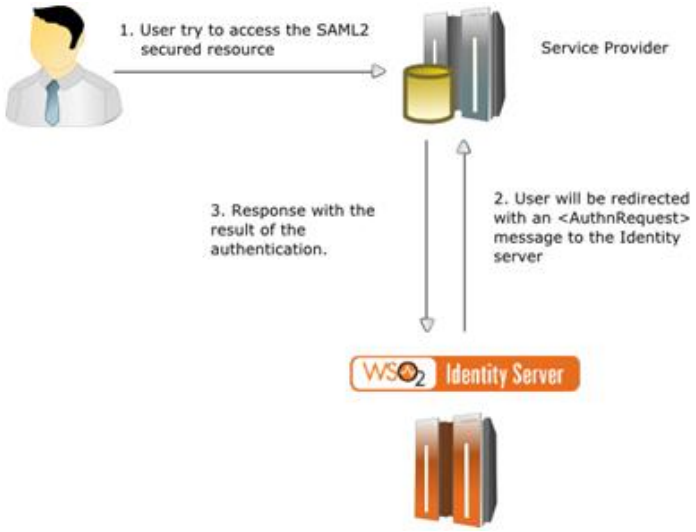
- **SSO *server*:** *Server* SSO menggunakan *cookies* temporer (sementara) untuk menyediakan fungsi manajemen sesi. Sebuah *cookies* terdiri dari informasi seperti *user-id, session-id, session creation time, session expiration time* dan lain-lain.

Produk-produk sistem SSO yang berbasis *open source* yang umum digunakan saat ini seperti CAS (*Central Authentication Service*), OpenAM (*Open AccessManager*), dan JOSSO (*Java Open Single Sign-On*).

3.2.4.2 OpenAM (Open Access Manager)

OpenAM adalah produk sistem SSO yang berbasis *open source*, merupakan infrastruktur yang mendukung layanan berbasis identitas dan implementasi solusi dari *Single Sign-on* (SSO) transparan sebagai komponen keamanan dalam infrastruktur jaringan (Nurdeni, 2010). *OpenAM* ini berbasis pada solusi *Identity Management* yang dikembangkan oleh *Sun Microsystems, Inc*. Tujuan dari *OpenAM* adalah untuk memberikan landasan yang luas sebagai infrastruktur pelayanan identitas dalam ranah publik dan untuk memfasilitasi sistem *Single Sign-On* untuk layanan aplikasi *web* dalam *server*.

Keunggulan *OpenAM* dibandingkan produk SSO lainnya terletak pada *Agent* yang dapat ditempatkan ke berbagai aplikasi *server* seperti Apache, *Sun Java System Web Server, Microsoft IIS*, dan *Domino*. Konfigurasinya dapat dilakukan dengan menulis otentikasi modul yang dilengkapi dengan keamanan layanan *web* menggunakan SAML (*Security Assertion Markup Language). OpenAM* merupakan pilihan yang tepat jika dibutuhkan dukungan terhadap lingkungan yang terpisah dan memerlukan otentikasi menggunakan SSL (*Secure Socket Layer*). OpenAM bekerja seperti gerbang utama pada sistem *Single Sign-On,* karena terhubung langsung dengan pengguna dan seluruh aplikasi yang ada dalam jaringan. OpenAM bekerja sama dengan aplikasi *backend* melakukan proses otentikasi dan otorisasi berdasarkan *database credential* pengguna. Beberapa tipe aplikasi yang sering dijadikan *Backend database* pada jaringan dengan OpenAM antara lain seperti Kerberos, Active Directory, LDAP, OpenDS, NIS, dan MySql.



Gambar 7. Arsitektur keamanan mengunakan Metode Single Sign On

4. KESIMPULAN

Komputasi awan (*cloud computing*) adalah gabungan pemanfaatan teknologi komputer (komputasi) dan pengembangan berbasis Internet (awan). Bila organisasi berpindah ke layanan komputasi awan publik tentu infrastruktur sistem komputasi dikendalikan oleh pihak ketiga yaitu *Cloud Service Provider* (CSP) dan tantangan ini harus ditangani melalui inisiatif manajemen. Inisiatif manajemen ini akan memerlukan gambaran jelas peran kepemilikan dan tanggung jawab dari CSP dan organisasi yang berperan sebagai pelanggan. Isu keamanan di dalam teknologi *Cloud Computing* saat ini menjadi isu utama, terutama isu pencurian data yang dilakukan oleh *hacker* maupun pencurian secara langsung ke dalam pusat data secara fisik. Bila pencurian data tersebut terjadi dapat merugikan *user* secara umum, karena selain data rahasia diambil, perusahaan tidak dapat menjalankan perusahaan dengan baik.

Beberapa tindakan untuk mencegah terjadinya pencurian data ini, yaitu dengan menghindari jenis ancaman keamanan berupa kehilangan atau kebocoran data dan pembajakan account atau service, serta *Identity Management* dan *access control* adalah kebutuhan yang utama bagi *SaaS Cloud computing* Perusahaan. Dan salah satu solusi untuk *identity management* dan *access control* adalah dengan mengunakan metode *Single Sign On*.

DAFTAR PUSTAKA

[1]Balboni, paoli., 2009, *Cloud computing for ehealth data protection issues*. ENISA Working Group on Cloud Computing.

[2]Krutz, Ronald L. And Vines, Russell Dean., 2010, *CLOUD SECURITY*, a comprehensive guide to secure cloud computing. Wiley Publishing Inc. Kanada, USA.

[3]Marks, Eric A., et all, 2010, *Executive's guide to cloud computing*, New Jersey: John Willey and Sons.
[4]Nurdeni, Deden A., 2010, *Implementasi Teknologi SSO di Lingkungan Teknik Informatika ITS*, Tugas Akhir. Jurusan Teknik Informatika ITS. Surabaya.
[5]Rifai, A., ZA, 2010, *Pencurian Data di Dalam Teknologi Cloud Computing*, Institut Teknologi Bandung.
[6]Setiawan, Deris, 2010, *Teknologi Cloud Computing*, Fasilkom, Universitas Sriwijaya.
[7]Zarlis, M., 2011, *Menelaah Janji-janji Cloud Computing dalam Bidang Teknologi Informasi*, Prosiding Seminar Nasional ke-3, Fakultas Teknik Universitas Islam Sumatera Utara.
[8]_____, 2010, *Use cases and functional requirements for inter-cloud computing*, Global Inter-Cloud Technology forum.
[9]_____, http://deris.unsri.ac.id/materi/jarkom/mengenal_cloudcomputing.pdf, accessed: 2014-01-14.
[10]_____, http://id.wikipedia.org/komputasi-awan, accessed: 2013-03-13.
[11]_____, http://teknik-informatika.com, accessed: 2013-03-13.
[12]_____,Wikipedia (2007n). Single sign-on - Wikipedia, the free encyclopedia. Online: http://en.wikipedia.org/wiki/Single_sign-on, accessed: 2012-03-13.
[13]_____,SAML Single Sign-On (SSO) Service for Google Apps, http://code.google.com/apis/apps /sso/saml_reference_implementation.html, accessed: 2013-03-13.