KEAMANAN DATA PADA CLOUD COMPUTING

Ricky Maulana Fajri1n

Program Studi Teknik Informatika Politeknik Sekayu
Universitas Bina Darma
Ricky.maulana85@gmail.com
Jalan Kolonel Wahid Udin LK 1 Kayuara Sekayu, Musi Banyuasin

Abstrak

Keamanan data pada cloud computing adalah sebuah isu baru di dunia teknologi informasi khususnya pada teknologi komputasi awan. Hal ini dikarenakan data yang diunggah ke cloud computing ditempatkan di server yang juga dimiliki oleh orang lain. Sehingga perlu dilakukan teknik pengamanan data pada cloud computing. Penelitian ini bertujuan untuk mencari celah keamanan data pada cloud computing sehingga dapat ditentukan teknik-teknik untuk meningkatkan keamanan data tersebut. Teknik-teknik yang dapat digunakan untuk memaksimalkan keamanan data pada cloud computing adalah single sign on, enkripsi data, secure socket layer dan menajemen bencana.

Kata kunci: *cloud computing, keamanan data, single sign on, enkripsi data, secure socket layer*

1 PENDAHULUAN

Cloud computing (komputasi awan) adalah sebuah trend baru di dunia IT (information technology). Menurut NIST cloud computing adalah sebuah model komputasi yang berfungsi untuk saling berbagi sumber daya jaringan antar sumber daya komputer [7]. Sehingga dengan adanya cloud computing para pengguna dapat saling berbagi sumber daya komputer menggunakan internet.

Keunggulan dari cloud computing adalah pengguna cuma harus terhubung dengan internet, semua aplikasi, platform dan infrastruktur semua nya tersedia di cloud computing. Sehingga dalam cloud computing sangat efisien dalam sumber daya. Besaran biaya pun dapat disesuaikan oleh pelanggan melalui mekanisme pay as you go, maka pelanggan hanya akan membayar berdasarkan servis yang didapat jika tidak lagi digunakan maka pelanggan tidak harus membayar jasa servis dari cloud service provider.

Namun dengan semakin berkembangnya cloud computing, isu keamanan data pada cloud computing juga menjadi sebuah isu yang terus berkembang. Keamanan data adalah sebuah hal yang sangat penting dikarenakan data akan diolah menjadi sebuah informasi yang dibutuhkan oleh perusahaan atau pelanggan. Sehingga sistem keamanan data pada cloud computing harus terus ditingkatkan.

Penelitian ini bertujuan untuk mencari celah keamanan pada cloud computing sehingga dapat ditentukan teknik peningkatan sistem keamanan data pada komputasi awan.

1.1 Perkembangan Cloud computing

Perkembangan cloud computing dimulai pada era ISP (Internet Service Provider) 1.0. ISP menyediakan akses internet baik untuk perusahaan mapun perorangan. Pada masa awal ini ISP menyediakan akses internet menggunakan jasa telepon dial-up. Setelah internet menjadi sebuah kebutuhan, ISP mulai mengembangkan layanan ke layanan email dan server korporat, Masa ini disebut dengan ISP 2.0. Pengembangan ISP 2.0 dilanjutkan menjadi ISP 3.0 pengembangan dilakukan dengan menambah berbagai infrastruktur jaringan yang dapat mensupport berbagai aplikasi seperti menyediakan data center dan storage gear. ISP 3.0 berkembang menjadi ASP (Application Service Provider) sehingga ISP tidak hanya menyediakan akses internet tetapi juga menyediakan jasa aplikasi di internet. Masa cloud computing dimulai dengan menyediakan berbagai jasa yaitu Software As A Service, Platform as a service dan infrastructure as a service [9].

1.2 Karakteristik Cloud computing

Cloud computing memiliki beberapa karakteristik diantaranya adalah [5]

1. Scalable (Aggregate) cloud computing dapat menyesuaikan dengan kebutuhan pengguna. Semakin besar kebutuhan pengguna maka cloud computing dapat menyediakannya.

2. Elastic : cloud computing bersifat elastis, sehingga dapat naik dan turun sesuai dengan kebutuhan pengguna.

3. Ubiquitous Access : cloud computing dapat diakses dari mana saja menggunakan berbagai macam peralatan baik komputer, smartphone atau tablet komputer. Peralatan tersebut hanya memerlukan akses internet untuk dapat menggunakan cloud computing

4. Complete Virtualization: walaupun terdiri dari banyak server, cloud computing harus dapat di modifikasi dan mengembangkan aplikasi selayaknya hanya menggunakan satu server. Hal ini dapat dilakukan dengan menggunakan fasilitas virtualisasi.

5. Relative Consistency : dikarenakan operasional cloud computing cukup kompleks, maka infrastruktur cloud computing dapat dibagi menjadi infrastruktur-infrastruktur yang kecil. Sehingga infrastruktur-infrastruktur tersebut harus dapat bekerja satu sama lain.

6. Comodity : cloud computing adalah tetap dianggap sebuah komoditi yang dapat diperdagangkan seperti halnya komoditi-komoditi yang lain.

1.3 Layanan Cloud computing

Layanan pada cloud computing terbagi menjadi 3 yaitu Software-As-a-Service (SaaS), Platform-As-a-Service (Paas), dan Infrastructure-As-a-Service (Iaas) [9]

1. Software As a service adalah salah satu layanan cloud computing dimana perusahaan dapat menyewa software yang dibuat oleh vendor. Perusahaan hanya menggunakan software pada saat yang dibutuhkan. Hal ini dapat menghemat pengeluaran dalam hal lisensi dan penggunaan server.[9]

2. Platform As a Service vendor penyedia layanan memberikan sarana kelengkapan pengembangan kepada pengembang aplikasi [6]. Vendor memberikan platform komputer kepada pengguna layanan sehingga pengguna tidak harus membeli platform yang mahal dalam pengembangan aplikasi

3. Infrastruktur As a Service penyedia layanan memyediakan infrastruktur yang dibutuhkan oleh pengguna. Pengguna dapat membayar penggunaan infrastruktur sesuai dengan infrastruktur yang digunakan [6].

1.4 Penelitian Terkait

Salah satu penelitian yang terkait dengan penelitian ini adalah penelitian oleh Yuni Fauziah [2]. Di dalam penelitian nya Fauziah menguraikan tinjauan keamanan sistem pada teknologi cloud computing, penelitian tersebut lebih membahas keamanan dari teknologi sistem cloud computing. Secara khusus penelitian ini lebih mengkaji sisi keamanan data dari cloud computing.

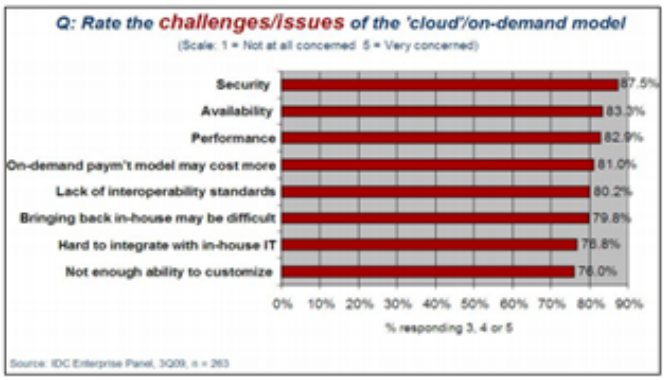
2 PEMBAHASAN

2.1 Metode Penelitian

Penelitian ini menggunakan metode literature review, dimana data-data yang digunakan didapatkan dari jurnal dan penelitian dengan sejenis. Selanjutnya data dianalisis untuk kemudian diolah.

2.2 Isu Keamanan Cloud Computing

Meski memiliki berbagai manfaat, cloud computing juga menyimpan berbagai permasalahan. Permasalahan yang utama dalam cloud computing adalah masalah keamanan [8]. Keamanan data dan informasi dari pengguna cloud computing menjadi sangat riskan dikarenakan data dan informasi tersebut di tempatkan di internet atau di cloud [8]. Hal ini didukung oleh hasil survey tentang permasalahan dari cloud computing yang telah dilakukan oleh IDC.



Gambar 1: Cloud Security Issue (Sumber IDC.com)

Terlihat pada gambar diatas bahwa 87.5 % responden menjawab bahwa security (keamanan) adalah isu utama yang menjadi permasalahan pada cloud computing. Setelah itu ketersediaan dan performance dari cloud computing yang menjadi tantangan yang harus dihadapi pada teknologi cloud computing. Selain dari itu penelitian yang dilakukan oleh Dutta, Peng dan Choudhary juga menunjukkan bahwa data pelanggan menjadi sangat lemah keamanannya ketika diletakkan di internet atau di cloud [1]. Data pada tabel satu menunjukkan hasil 10 jenis permasalahan keamanan data pada cloud computing.

Rank	Risk ID	Top 10 Critical Risk Event For *Cloud computing*	Risk Score
1	LR1.1	Privacy of enterprise or customer data is jeopradised in the cloud	153.50
2	LR 1.3	Incosistent data protection laws adpoted by different coutnries where cloud data are generated and stored	151.75
3	OGR4.2	Difficult for user companies to change cloud vendors even in the case of service dissatifacation (also know as vendor lock-in	148.50
4	OGR5.2	User companies lack disaster recovery and contigency plans to deal with unexpected technical issues in cloud environment	147.75
5	LR3.2	Enterprise data re-migration difficulties at the end of the cloud contract	140.25
6	OPR4.2	Inadegate user training/knowledge on cloud service and usage	139.75
7	OPR5.1	Cloud application become temporarilly unavailable or out of service	137.25
8	OPR2.1	Increasing hidden cost due to non-transparent operating model in the cloud	136.00
9	TR4.3	Denial-of-Service (DOS) attacks in the cloud environment	135.50
10	TR4.1	Unauthorised access to enterprise data/application in the cloud	135.00

Gambar 2: Isu keamanan data pada cloud computing [1]

Terlihat pada tabel diatas bahwa keamanan data dari perusahaan atau pelanggan akan menjadi sangat rentan dirusak ketika diletakkan di cloud. Selain dari keamanan data pelanggan, cloud computing juga sarat permasalahan diantaranya adalah belum adanya hukum yang mengatur mengenai data yang disimpan di cloud, kemampuan pengembalian data setelah terjadi bencana, ketidaksediaan service, akses oleh user yang belum tidak diotentikasi dan serangan denial of service.

2.3 Teknik Peningkatan keamanan data pada Cloud computing

2.3.1 User Authentication

Salah satu metode untuk menghindari pencurian akun pada cloud computing adalah user authentication. Dengan metode ini setiap user yang akan masuk kedalam sistem harus di otentikasi dengan menggunakan berbagai macam metode otentikasi diantaranya adalah username dan password dan single sign on.

1. Username dan password Username dan password adalah metode paling sederhana untuk melakukan otentikasi user. Dengan metode ini user harus memasukkan username dan password yang benar. Username dan password yang dimasukkan oleh pengguna

haruslah tersimpan di database penyedia cloud computing. Namun username dan password sangat rentan untuk dibajak. Sehingga pengguna harus senantiasa menjaga username dan password yang dimiliki. Beberapa cara dapat dilakukan untuk meningkatkan keamanan username dan password seperti tidak membagikan username dan password kepada pihak lain, menggunakan kombinasi antara huruf angka dan simbol untuk username dan password dan selalu

2. Single sign on Selain username dan password penyedia jasa komputasi awan juga dapat menggunakan metode single sign on. Dengan metode ini pihak penyedia mempercayakan identitas user kepada pihak ketiga yang disebut dengan identity provider. Sehingga para pengguna yang akan menggunakan aplikasi komputasi awan akan diarahkan terlebih dahulu ke identity provider, jika identity provider dapat memberikan otentikasi maka selanjutnya pelanggan tersebut akan diberikan otorisasi kedalam aplikasi cloud computing.

Adapun prinsip kerja single sign on adalah sebagai berikut[3]:

1. Pengguna mengirimkan permintaan untuk mengakses aplikasi.
2. SSO client akan meredirect permintaan browser client ke SSO server.
3. Pengguna menginput username dan password untuk di otentikasi oleh server.
4. Jika proses otentikasi benar maka SSO client akan mendapatkan sebuah tiket.
5. SSO client akan memvalidasi tiket yang didapat, jika pengguna dianggap sah.
6. Pengguna yang melewati proses ini akan berhak untuk mengakses informasi yang disediakan.

2.3.2 Enkripsi Data

Selain keamanan data akun dari pengguna, keamanan data yang ditransfer kedalam sistem cloud computing harus juga ditingkatkan keamanannya. Meskipun pembajak tidak dapat masuk kedalam aplikasi cloud karena sistem otentikasi, namun pembajak dapat mengambil data yang ditransfer melalui internet. Oleh karena itu data yang dikirim haruslah di enkripsi sehingga data tersebut tidak dapat dibaca oleh pihak yang tidak berkepentingan. Enkripsi data dapat dilakukan pada sisi pengguna dan sisi server. Terdapat beberapa metode untuk enkripsi data diantaranya adalah AES, DES, 3DES dan RSA.

2.3.3 SSL (Secure Socket Layer)

Setelah data yang ditransfer dapat diamankan dengan cara dienkripsi, namun untuk meningkatkan keamanan nya maka jalur komunikasi data harus juga di amankan. Komunikasi data pada jaringan komputer terjadi pada layer TCP / IP, untuk mengamankan jalur ini SSL (secure socket layer) dapat digunakan. SSL bekerja melalui 3 tahap yaitu pada tahap pertama server dan client berkomunikasi untuk menentukan sistem enkripsi yang akan digunakan, selanjutnya pada tahap kedua dilakukan pertukaran kunci data untuk enkripsi, kunci yang digunakan adalah kunci public, Terakhir pengiriman pesan dilakukan menggunakan kunci enkripsi yang telah ditentukan sebelumnya. [3]

3 KESIMPULAN

Perkembangan cloud computing telah menjadi sebuah fenomena baru di dunia teknologi informatika. Namun perkembangan cloud computing yang pesat tidak diimbangi dengan peningkatan sistem keamanan dari cloud computing. Keamanan data adalah sebuah isu baru di dunia cloud computing. Hasil riset membuktikan bahwa pencurian data di cloud computing adalah isu yang paling ditakutkan oleh pengguna cloud computing. Oleh karena itu, para penyedia jasa cloud computing harus dapat meningkatkan sistem keamanan data pelanggan nya. Hal ini dapat dilakukan dengan berbagai cara seperti user authentication, SSL, dan enkripsi data.

Penelitian mengenai sistem keamanan pada cloud computing harus senantiasa dilaksanakan khususnya di Indonesia, dikarenakan tingkat pengetahuan pengguna tentang keamanan data pada cloud computing di Indonesia masih sangat minim.

4 Referensi

1. Dutta, Amab, Peng, Alex Gou Chao, Choundary Alok, Risks in enterprise cloud computing the perspective of IT Experts The Journal of Computer Information Systems, 2013

2. Fauziah Yuni, Tinjauan keamanan sistem pada teknologi cloud computing jurnal informatika volume 8 nomor 1 januari 2014 ISSN 1978-054

3. Hu, Jian., Sun, Qizhi., Chen Hongping., Application of Single sign-on (SSO) in Digital Campus. International Conference Broadband Network and Multimedia technology (IC-BNMT). Pages 725 727. Beijing 2010

4. L Ertaul, S. Singhal & G. Saldamli, Security challenges in cloud computing

5. Marks, Eric A., et all, 2010, Executives guide to cloud computing, New Jersey: John Willey and Sons.

6. Moedjiono, Cloud computing gelombang informatisasi layanan dunia bisnis masa depan Jurnal Telematika MKOM Vol 2 No 2 September 2010

7. Peter Mell and Timothy Grance The NIST Definition of Cloud computing National Institute of Standards and Technology, U.S Departement Of Commerce 2011.

8. Prashar, Saurabh K. Security Issues in Cloud computing : 2010.

9. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy an enterprise perspective on Risks and Compliance o reilly 2009