Technical Report

Kajian Keamanan Privasi Data Pada Cloud Computing

Ditujukan sebagai Ujian Akhir Semester (UAS)
Mata Kuliah Keamanan Informasi Lanjut (II5166)

Oleh :
Enda Esyudha Pratama
23512102

Program Studi Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

2013

Abstrak

Masalah privasi dan keamanan jadi isu hangat yang tengah dibahas seputar implementasi *Cloud Computing* di Indonesia. Faktor keamanan dan privasi menjadi dua dari empat isu terpenting seputar implementasi *Cloud Computing* di Indonesia, selain masalah keterbatasan akses internet dan keberadaan data itu sendiri. Tindakan pencegahan dan perlindungan dapat dilakukan pada beberapa aspek untuk menangani masalah tersebut, salah satunya pada aspek data privacy security. Privasi menjadi sangat penting di *Cloud Computing*, karena tingkat privasi yang diinginkan setiap orang berbeda-beda. Dengan kemampuan privasi data, maka setiap orang bisa menentukan siapa yang berhak mengakses atau mengubah suatu informasi sesuai dengan kebutuhan dan keinginannya. Pada makalah ini akan dibahas tentang isu, resiko, kontrol dan perlindungan secara teknis tentang keamanan privasi data tersebut.

***Kata kunci** : cloud computing, data privacy security, manajemen privasi*

Daftar Isi

Daftar Gambar

1. Pendahuluan

Teknologi *cloud computing* atau komputasi awan mulai menjadi tren. Meski masih terdengar asing bagi sebagian kalangan, *cloud computing* diyakini akan banyak diadopsi dan menjadi masa depan dunia TI. Solusi *cloud computing* dinilai menawarkan berbagai kemudahan [1]. Misalnya, memungkinkan karyawan bekerja di mana saja karena data disimpan di awan. Dan pengguna hanya tinggal memakainya dengan membayar biaya langganan.

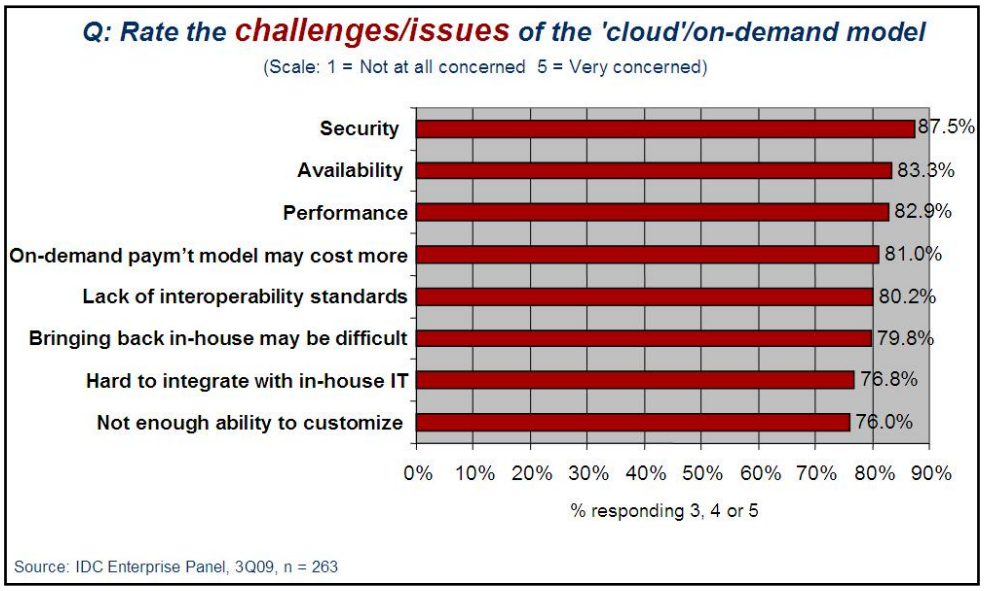
Komputasi awan atau *cloud computing* mengubah segalanya. Mulai dari cara layanan TI diantarkan, sampai caranya dipakai dalam sebuah organisasi [2]. Tanpa keraguan, Asia Pasifik bergerak cepat merangkul arsitektur baru ini. *Cloud computing* sendiri bisa dibilang salah satu fenomena paling menarik dalam industri TI dua dekade terakhir. Namun ini juga gebrakan yang paling mengganggu, melebihi migrasi dari *mainframe* ke aplikasi *client/server*.

Menurut lembaga riset *Forrester*, 52% organisasi di Asia Pasifik di luar Jepang (APEJ) saat ini sudah menggunakan atau secara aktif merencanakan inisiatif awan. Sementara, Gartner menggambarkan komputasi awan sebagai sebuah gaya komputasi dimana kemampuan TI-enabled skalabel dan elastis diantarkan sebagai sebuah layanan bagi para kustomer eksternal melalui internet [3].

Dalam survei yang dilakukan oleh *Symantec* bersama dengan *ReRez Research* dengan koresponden perusahaan di 29 negara termasuk Indonesia, terungkap bahwa pengetahuan tentang *cloud computing* di kalangan korporasi meningkat. Di Indonesia, menurut survei tersebut, sudah 100% organisasi paling tidak sudah membicarakan atau mendiskusikan mengenai *cloud computing*. Ini artinya, ada lonjakan hingga 80% dari sebelumnya [4]. Semakin banyak konsumen memindahkan data mereka ke *server* di mana akan memunculkan pertanyaan, apakah data yang merka temaptkan di ‘awan' ini aman?

Adopsi *cloud computing* di Indonesia perlahan sudah mengalami kenaikan. Namun, peningkatan ini tidak diiringi dengan kesadaran menjaga data. Alhasil, banyak data yang hilang di ‘awan'. Hasil dari survei yang sama dilakukan, menunjukan 69% diantara koresponden yang ditanya kehilangan datanya di cloud [4].

Dalam Presentasi *Security Issues in Cloud Computing*, Saurabh K Prashar [5] menyatakan bahwa masalah keamanan 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 awan atau di internet tepatnya. Hal ini menjadi isu utama dari teknologi *cloud computing* . Hasil survey tersebut dapat dilihat pada diagram di bawah.



Gambar 1. Isu Keamanan Dalam *Cloud Computing*
(sumber : www.idc.com)

2. Kajian Pustaka

National Institute of Standards and Technology (NIST) [6] mendefinisikan cloud computing sebagai model yang memungkinkan penggunaan *resource* bersama secara mudah, dimana - mana, dapat dikonfigurasi, dan on demand. NIST juga mengidentifikasi lima karakterisitk sehingga suatu layanan dapat dikatakan sebagai *cloud computing*, yaitu:

a. *On-demand self-service*. Pengguna dapat memesan dan mengelola layanan tanpa interaksi manusia dengan penyedia layanan, misalnya dengan menggunakan, sebuah portal web dan manajemen antarmuka. Pengadaan dan perlengkapan layanan serta sumber daya yang terkait terjadi secara otomatis pada penyedia.

b. *Broad network access*. Kemampuan yang tersedia melalui jaringan dan diakses melalui mekanisme standar, yang mengenalkan penggunaan berbagai platform (misalnya, telepon selular, laptop, dan PDA).

c. *Resource pooling*. Penyatuan sumberdaya komputasi yang dimiliki penyedia untuk melayani beberapa konsumen menggunakan model multipenyewa, dengan sumberdaya fisik dan virtual yang berbeda, ditetapkan secara dinamis dan ditugaskan sesuai dengan permintaan konsumen. Ada rasa kemandirian lokasi bahwa pelanggan umumnya tidak memiliki kontrol atau pengetahuan atas keberadaan lokasi sumberdaya yang disediakan, tetapi ada kemungkinan dapat menentukan lokasi di tingkat yang lebih tinggi (misalnya, negara, negara bagian, atau datacenter). Contoh sumberdaya termasuk penyimpanan, pemrosesan, memori, *bandwidth* jaringan, dan mesin virtual.

d. *Rapid elasticity*. Kemampuan dapat dengan cepat dan elastis ditetapkan.

e. *Measured Service*. Sistem komputasi awan secara otomatis mengawasi dan mengoptimalkan penggunaa sumberdaya dengan memanfaatkan kemampuan pengukuran (metering) pada beberapa tingkat yang sesuai dengan jenis layanan (misalnya, penyimpanan, pemrosesan, *bandwidth*, dan *account* pengguna aktif). Penggunaan sumberdaya dapat dipantau, dikendalikan, dan dilaporkan sebagai upaya memberikan transparansi bagi penyedia dan konsumen dari layanan yang digunakan.

Cloud computing menawarkan tiga jenis layanan yaitu IAAS, PAAS, dan SAAS. IAAS (*Infrastructure As A Service*) menyediakan *hardware* (*network, storage, processor*) untuk proses komputasi dan bergantung pada virtualisasi. Fiturnya berupa pemilihan virtual machine, sistem operasi, aplikasi perkantoran, *mirror* penyimpanan data, *optimization*, dan pemrosesan multi data/aplikasi/perhitungan rumit. Contohnya pada *Akamai*.

PAAS (*Platform As A Service*) menyediakan platform berbasis *web browser* untuk implementasi dan pengembangan sistem sehingga meminimalkan proses coding. Fitur yang disediakan berupa *software development tool* berbasis *web browser*, *web service* (disertai *scalability*, kontrol akses, keamanan, dan layanan), integrasi yang baik dan mudah dengan perangkat lunak lain dalam satu platform yang sama, penghubung dengan sistem lain di luar jaringan *cloud computing*. Contohnya pada *Amazone Web Service*.

SAAS (*Software As A Service*) menyediakan aplikasi berbasis *web*. Fitur AJAX menyediakan *user experience* menyerupai aplikasi *desktop*. Contoh layanan ini antara lain layanan *Google App Engine*, ZOHO dengan *collaboration application*, dan *Salesforce* dengan CRM (*Customer Relationship Management*).

3. Isu dan Resiko Privasi Data

Infrastruktur *cloud computing* yang memungkinkan akses dan penggunaan secara bersama menimbulkan masalah privasi data, termasuk konsekuesi hukum akibat adanya penyimpangan penggunaan terhadap informasi rahasia suatu bisnis. Dengan menyediakan penyimpanan data secara bersama, meningkatkan kerentanan data sedang diakses atau disalin oleh orang yang tidak berhak. Ancaman privasi data dapat berasal dari pihak internal (penyedia layanan, pengguna dalam perusahaan), dan kebocoran data bisa terjadi karena kegagalan hak akses keamanan di beberapa domain [7].

Konsep privasi sangat berbeda dalam konteks negara, budaya atau yurisdiksi. Definisi yang diadopsi oleh Organisasi Kerjasama Ekonomi dan Pembangunan (OECD), privasi adalah informasi yang berkaitan dengan individu yang diidentifikasi (subjek data). D. Chen dan H. Zhao [3] secara umum mengidentifikasi isu privasi ke dalam *data life cycle* yang terdiri dari pengumpulan, penggunaan, pengungkapan, penyimpanan, dan penghancuran data pribadi.

S. M. Rahaman dan M. Farhatullah [8] mencoba melihat isu privasi dari sudut pandang yang berbeda. Mereka melihat isu privasi ini dari dua sisi yaitu sisi pengguna cloud dan penyedia layanan cloud itu sendiri atau yang lebih dikenal dengan *cloud service provider*. Masing-masing sudut pandang tersebut memiliki fokus yang berbeda dalam melihat keamanan privasi data tersebut.

Dari sudut pandang pengguna layanan cloud itu sendiri harus mempertimbangkan beberapa hal penting seperti : kontrol terhadap sistem dan data, menciptakan fasilitas untuk penggunaan banyak identitas dan membatasi informasi identitas serta autentifikasi untuk transaksi tingkat tinggi atau yang dianggap penting. Semua hal tersebut yang harus dijamin bagi seorang individu agar privasi informasi yang disampaikan kepada cloud provider dapat dipastikan aman.

Sedangkan bagi *cloud service provider* itu sendiri, beberapa hal yang harus diperhatikan dianataranya menyediakan fasilitas untuk mengelola data pribadi pengguna, enkripsi untuk setiap data yang menyimpan informasi pribadi pengguna, pengolahan dan penyimpanan data, mengendalikan pengidentifikasi unik, mengelola eksplisit persyaratan privasi dan keamanan antara penyedia layanan awan. Menurut G. Zhang dan Y. Yang [2], isu privasi dalam CSP terdapat di dalam semua level *cloud environment* yang terdiri dari *cloud service application level, application platform level, cloud management platform level, physical computing, VM management platform level*, dan *storage and network level*.

Dari beberapa isu yang telah dibahas sebelumnya, dapat dilihat secara umum bahwa keperluan menjaga kerahasiaan data dan informasi pribadi menjadi suatu prioritas penting dalam impelementasi *cloud computing* khususnya dalam hal privasi data [7].

4. Perlindungan Privasi Data

Persoalan perlindungan terhadap privasi atau hak privasi muncul karena keprihatinan akan pelanggaran privasi yang dialami oleh orang dan atau badan hukum. Perlindungan privasi merupakan hak setiap warga negara, harus dihormati dan diberikan perlindungan. Termasuk konses *Privacy Information (Security)* dimana sebuah informasi harus aman, dalam arti hanya diakses oleh pihak–pihak yang berkepentingan saja sesuai dengan sifat dan tujuan dari informasi tersebut [7].

Berbagai macam solusi bentuk perlindungan privasi telah ditawarkan oleh penyedia jasa *cloud*, mulai dari yang bersifat prosedural (SOP, *privacy policy*) hingga yang bersifat teknis. Sebagai contoh, Pemerintah Amerika Serikat sangat anti terhadap masalah privasi [7]. Ini terbukti dari larangan ekspor teknologi enkripsi *bit* tinggi ke luar AS. Mereka ingin mengontrol/menyensor semua data yang masuk ke atau keluar dari AS. Dikhawatirkan jika teknologi enkripsi bit tinggi (di atas 64 bit) tersebar ke luar maka agen rahasia AS akan sulit melacak dan mengawasi data yang akan mereka monitor terhadap pihak-pihak tertentu di luar AS yang dicurigai melakukan tindak kejahatan tingkat tinggi/internasional. Enkripsi ber-bit tinggi hanya boleh dipakai di dalam AS karena masih dalam wewenang pemerintah AS.

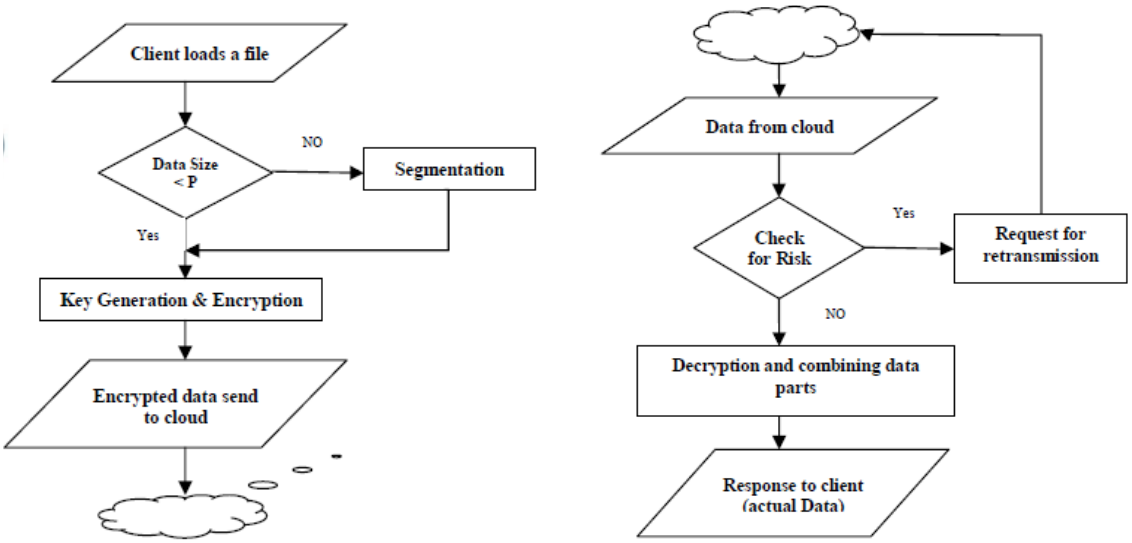
Dalam makalah ini akan dibahas perlindungan privasi data pada cloud computing dari sisi teknis. Beberapa penelitian telah dilakukan dalam hal teknologi keamanan privasi data. Pada makalah ini akan coba dibahas dua macam teknologi sebagai solusi privasi data yaitu: *PaaS (Privacy as a Service)* dan *Cloud Intelligent Track*.

4.1 *Cloud Intelligent Track*

M. R. Aswin dan M.Kavitha dalam penelitiannya tentang privasi data cloud mengusulkan suatu metode baru dalam penanganan privasi yaitu *cloud intelligent track system* [9]. Dalam teknologi ini, data pengguna tidak disimpan langsung di dalam database cloud. Teknologi ini menggunakan *privacy manager* pada *client side* dan *cloud side*. *Cloud intelligent track* sistem menggunakan *privacy manager* and *risk manager*. *Privacy manager* digunakan sebagai sautu algoritma yang membagi data menjadi bagian-bagian yang lebih kecil untuk disimpan disembarang lokasi. Lokasi-lokasi tersebut dikelola dan disimpan berdasarkan database privacy manager. Saat klien mengirmkan request untuk memproses data yang telah disimpannya di *cloud,* algoritma *privacy manager* akan menyusun kembali data yang telah telah dipisah tersebut untuk ditampilkan lagi secara utuh di sisi klien. Pada saat proses transmisi data tersebut, resiko data ada yang hilang atau rusak diperjalanan tetap selalu ada. Untuk mengatasi hal tersebut, algoritma *privacy manager* menggunakan risk manager untuk menghitung jumlah atau besar ukuran suatu data. Sehingga jika besar ukuran data yang telah disusun tersebut tidak sesuai dengan ukuran awal, sistem secara otomatis akan meminta *cloud server* untuk mengirim ulang paket yang hilang.

Proses utama yang dilakukan oleh *privacy manager* adalah pada saat proses data dikirimkan dariklien ke *database*. Setiap klien memiliki *privacy manager* tersendiri yang terpasang di mesinnya. Tetatpi *privacy manager* tersebut secara otomatis dikendalikan oleh cloud server. Sehingga setiap *cloud server* tidak terkoneksi secara langsung dengan klien, melainkan melalui proses yang berjalan di privacy manager klien tersebut. Proses ini seolah-olah menciptakan

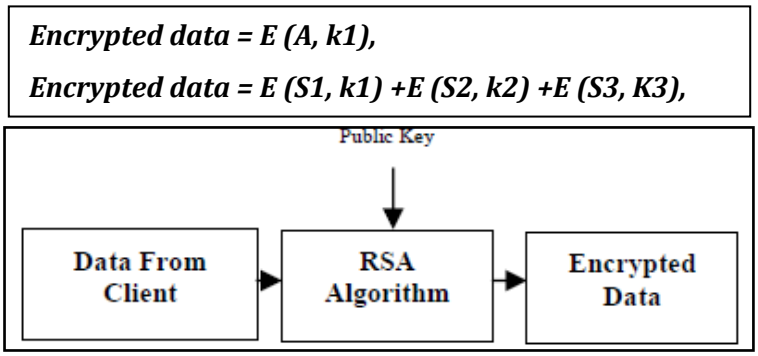
private cloud yang berjalan dibelakang layar. Fungsi atau service yang bekerja pada proses tersebut diantaranya: *working process, encryption, decryption, memory management, keyword generation, risk manager.*



Gambar 2. Proses Kerja Transfer Data Pada *Cloud Intelligent Track*
(sumber : Aswin & Kavitha, 2012)

4.1.1 Encryption

Dalam tahap ini dari *privacy manager*, data yang disimpan klien pada database telah dienkripsi dengan kunci public yang disimpan di tempat yang berbeda. Setelah proses enkripsi yang dilakukan pada sisi klien selesai dilakukan, data kemudian dikirimkan ke dalam *database cloud*. Untuk melakukan decryption data dari cloud, menggunakan private key yang hanya dimiliki oleh *privacy manager*. Alogritma enkripsi yang digunakan yaitu algoritma RSA.



Gambar 3. Proses Enkripsi Data Pada *Cloud Intelligent Track*
(sumber : Aswin & Kavitha, 2012)

E= Encryption,

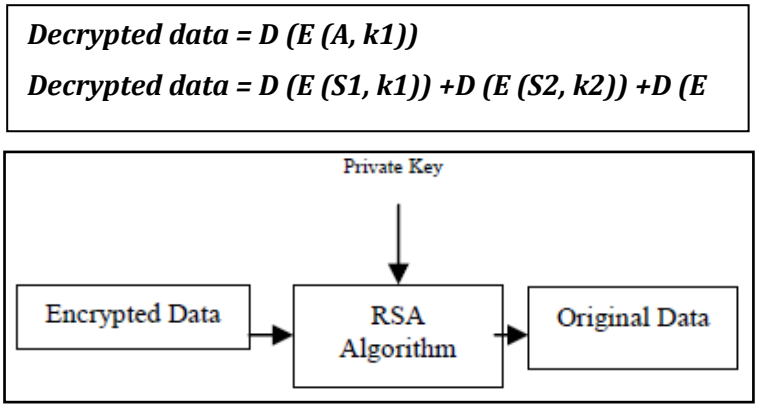
A= Data sent by the client,

S1, S2, S3= Segmented data which is equal to the fixed data size.

k1, k2, k3= key word

4.1.2 Decryption

Dalam tahap ini dari *privacy manager*, data yang dipanggil oleh klien diambil dari *database cloud*. Data yang terenkripsi tersebut akan diterima di sisi *privacy manager* terlebih dahulu. *Privacy manager* melakukan pengecekan pada sisi klien untuk menemukan kombinasi *private key* yang sesuai. Setelah dekiprsi selesai, data ditampilkan di mesin klien



Gambar 4. Proses Dekripsi Data Pada *Cloud Intelligent Track*
(sumber : Aswin & Kavitha, 2012)

4.1.3 Memory Management

Manajemen memori pada *privacy manager* digunakan untuk proses membagi data menjadi beberapa segment atau bagian sebelum disimpan di berbagai lokasi cloud server secara acak, dan juga untuk melakukan proses penyusunannya kembali. Operasi-operasi yang terjadi pada memori manajemen ini terdiri dari.

- Data dipisah menjadi beberapa bagian dan disimpan secara acak di dalam databse cloud. Pengacakan tersebut dilakukan oleh *privacy manager*.
- Lokasi acak dari setiap bagian yang sudah dipisah tersebut disimpan pada *privacy manager* pada mesin klien.
- Lokasi tersebut disimpan dan akan digunakan kembali untuk menyusun kembali data secara utuh oleh *privacy manager*.

4.1.4 Keyword Generation

Dalam tahap ini pada privacy manager, untuk data yang memiliki large size key word akan diproses di dalam privacy manager. Keywords ini disimpan di dalam database privacy manger itu sendiri untuk nantinya didekripsi kembali saat dikembalikan kepada klien. Keyword tersebut tidak hanya bisa dihasilkan oleh privacy manager, tetapi juga oleh klien itu sendiri Algoritma generate keyword yang digunakan adalah algoritma RSA.

Generation of key using RSA algorithm:

Let p and q be the two prime, are of almost equal in size. An integer or public exponent e, 1<e< phi where Gcd (e,phi) =1.

The secret exponent d, i< d< phi where

ed =1(mod phi).

n=pq; Φ (phi) = (p-1) (q-1);

Here public key is k1= (n, e) and private key is (d, p, and q).

4.1.5 Risk Manager

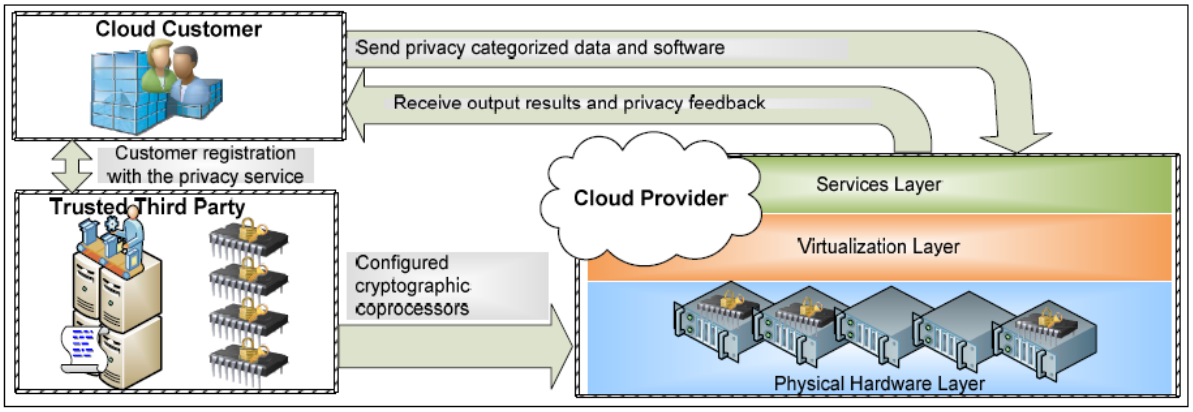
Pada tahap ini, data yang berasal cloud server akan dilakukan pengecekan untuk menghindari resiko. Pengecekan ini bertujuan untuk memeriksa apakah proses penyusunan kembali data dari cloud server telah sempurna. Proses pengecekan pada risk manager menggunakan algoritma cyclic redundancy check algorithm. Proses yang terjadi pada risk manager yaitu:

- Saat data masuk ke dalam risk manager, proses pengecekan dilakukan untuk mengetahui error pada data dengan bantuan cyclic redundancy check algorithm.
- Jika data yang diterima memiliki banyak error, maka data akan ditolak dan dilakukan proses pemanggilan kembali dari server.
- Jika tidak terdapat error, data tersebut dapat disusun manjadi suatu data yang utuh.

4.2 *PaaS (Privacy as a Service)*

Penelitian tentang PaaS ini dilakukan oleh W.Itani, A. Kayssi dan A. Chehab [10]. Mereka mendefinisikan PasS sebagai kumpulan protokol keamanan untuk mengukur kepatuhan terhadap data pengguna di dalama arsitektur *cloud computing*. PasS memungkinkan keamanan dalam hal penyimpanan, proses, dan audit data rahasia dengan menggunakan kemampuan tamper-proof of cryptographic coprocessors. Dengan menggunakan teknologi tersebut, pengguna cloud akan disediakan wilayah yang aman dalam mengeksekusi data baik secara fisik maupun logically. PasS dirancang untuk memaksimalkan kontrol pengguna dalam hal mengelola berbagai macam aspek yang berkaitan dengan sensivitas data. Langkah yang dilakukan dengan menerapkan *user-configurable software protection* and mekanisme pengelompokan data privasi.

PaaS menyediakan akses penuh terhadap mekanisme privasi data di dalam cloud. Tingkat kepercayaan pengguna terhadap layanan dari cloud provider didasarkan pada tingkat sensitivitas informasi pelanggan. PaaS sendiri mengelompokan tingkat kepercayaan tersebut kedalam tiga level, dapat dilihat pada gambar di bawah ini:



Gambar 5. *PasS Cloud Based System Model*
(sumber : Itani, Kayssi, Chehab, 2009)

Dari gambar di atas dapat dikelompokan menjadi 3 macam level tingkat kepercayaan yaitu:

1. *Full trust*: pada level ini pengguna dapat menyimpan dan memproses datanya secara aman tanpa perlu dienksripsi karena dijamin secara penuh terhadapat penyedia jasa.

2. *Compliance-based trust*: This level applies to customer data that needs to be stored encrypted to support legal compliance regulations (misalanya Health Insurance Portability and Accountability Act (HIPAA) untuk mengamankan catatan medis dan informasi pasien, Gramm-Leach-Bliley Act untuk meyakinkan kerahasiaan data catatan keuangan dan transaksi pada setiap lembaga keuangan). Pada level ini, pengguna mempercayakan penyedia cloud untuk menyimpan data dan melakukan enkripsi menggunakan *specific cryptographic key* yang dimiliki cloud provider.

3. *No trust*: Pada level ini, data yang bersifat sangat sensitif bagi pengguna harap dipertimbangkan untuk diletakan pada cloud. Jika pun harus, maka data tersebut harus dienkripsi dengan *customer-trusted cryptographic keys* dan harus diproses dengan *isolated cryptographic* yang berada di cloud. *Isolated cryptographic* tersebut dikelola oleh pihak ketiga diluar pengguna cloud dan penyedia cloud yang dipercaya keduanya.

4.2.1 *System Design And Architecture*

Secure Coprocessor Basics.

Cryptographic coprocessor merupakan seperangkat hardware kecil yang terhubungan dengan komputer server melalui slot PCI. Prosesor ini sebenarnya hamper sama dengan prosesor lainnya. Perbedaannya terdapat pada kompnen utama dari prosesor ini yang dapat memberikan kemampuan keamanan menggunakan *tamper-proof casing*. *Tamper-proof* casing tersebut dapat melindungi dan menolak *physical attacks* yang menuju ke server. Input/output akses pada *cryptographic coprocessor* dapat dilakukan secara lokal lewat main *server system bus* atau secara *remote* menggunakan *network card*. Hal ini meningkatkan tingkat *security* dari prosesor itu sendiri.

Coprocessor Configuration and Distribution

Crypto coprocessor harus dipasang di setiap cloud server yang menjalankan Virtual Machine (VM). Server tersebut terhubung dengan registered user yang menggunakan layanan *privacy manager*. Untuk alasan ekonomis, *crypto coprocessor* dapat digunakan untuk melayani lebih dari satu *cloud customer*. Faktanya, mekanisme pembagian *resource* tersebut mengharuskan kehadiran dari pihak ketiga yang dipercaya (*trusted third-party* (TTP)) untuk mengelola struktur data kripstografi dan dan manajemen kunci public/private cloud customer pada crypto *coprocessor*. TTP dilihat sebagai pihak ketiga yang khusus mengelola layanan privasi di dalam suatu cloud provider. Secara teknis, tanggung jawab utama dari TTP adalah untuk mengelola kumpulan pasangan private/public key di dalam *persistent storage* pada *crypto coprocessor*. Setiap pasangan public/private key (PUCID/PRCID) dialokasikan untuk setiap pengguna cloud yang menggunakan *privacy service*. Setelah proses registrasi, *cloud customer* akan menerima copy dari pasangan public/private key. Proses pengiriman tersebut dapat dilakukan secara face-to-face transaksi atau lewat *secure electronic session*. Pasangan kunci PUCID/PRCID dapat diubah secara *remote* lewat TTP meski *crypto coprocessor* telah dipasang computing cloud. Mekanisme pengubahan remote key sangat penting untuk mendukung proses registrasi dan menghentikan service customer yang sudah ada. Dengan melakukan mekanisme update key tersebut, TTP dapat secara dinamis mengatur penggunaan resource prosesor. Sebagai tambahan, untuk memanggil customer's PUCID/PRCID key pair, TTP juga menggunakan private key sendiri untuk dapat masuk ke dalam database pada crypto coprocessor. Kunci ini dibutuhkan TTP dalam melakukan autentifikasi secara remote untuk masuk kedalam *crypto coprocessor* dan secara aman mengeksekusi perintah-perintah di dalam prosesor tersebut.

Coprocessor Process Structure

Crypto coprocessor memiliki model struktur proses yang sama seperti ABYSS *processor*. Konsep utama dalam pada proses ini adalah melindungi setiap aplikasi pengguna yang jalan di prosesor menggunakan *root highly-privileged process*. Proses ini disebut sebagai RP daemon.

Software Division

Di dalam model keamanan PasS, pengguna cloud bertanggung jawab mengkonfigurasi software applications untuk mendukung penerapan mekanisme keamanan privacy service. Berdasarkan konsep ini, cloud customer harus mengklasifikasikan perangkat lunak yang harus dilindungi dan yang tidak. Klasifikasi yang dilindungi mengindikasikan proses tersebut harus dieksekusi secara aman di dalam space pada crypto coprocessor. Di sisi lain, hasil klasifikasi yang tidak dilindungi mengindikasikan proses tersebut dapat diproses secara normal di server utama. Proses yang diproteksi tersebut berjalan di crypto coprocessor dan terpisah dari proses lainnya yang tidak terproteksi. Proses manajemen tersebut dilakukan oleh RP daemon. Aplikasi yang terproteksi harus disimpan dan terenkripsi di sisi penyedia cloud. Saat bagian tersebut dipanggil kembali pada crypto coprocessor, RP process mengdekripsi content dan mengeksekusinya dalam bentuk binary code.

Data Privacy Specification

Sebelum mengunggah data untuk disimpan dan diproses di computing cloud, pengguana customer harus mengklasifikasikan data terlebih dahulu. Klasifikasi data ini bersifat subjektif berdasarkan significance dan sensitivity *data, Klasifikasi tersebut dikelompokan menajadi 3: No-Privacy (NP), Privacy* with Trusted Provider (PTP), *Privacy with Non-Trusted Provider* (PNTP). Untuk setiap data, *cloud provider* mengalokasikan *logical storage partition* sebagai *storage pool*. *Storage pool* tersebut diberi nama berdasarkan kategori privsi data.

4.2.2 *Privacy Protocols*

Data and Software Transfer Protocol

Protokol ini mengharuskan cloud customer untuk menambah aspek struktur privasi pada software dan data sebelum dikirim ke cloud computing. Struktur tersebut terdiri dari struktur data software privacy, konfigurasi pelanggan pada cloud software menjadi beberapa komponen: privacy tag, protected software part SSID, dan unprotected software part SSID.

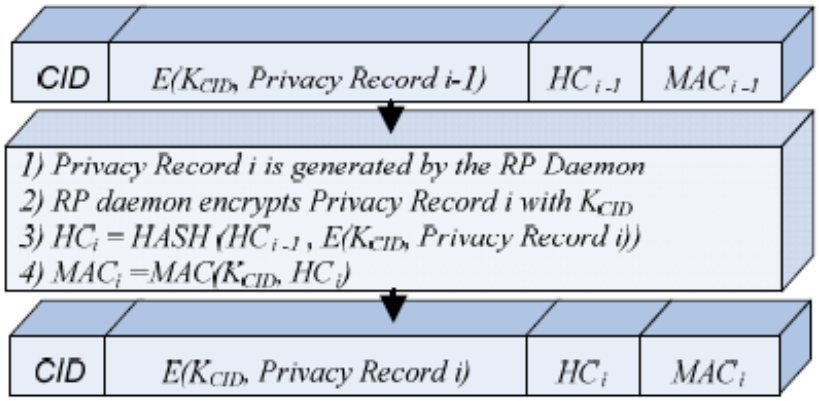
Software Execution and Data Processing Protocol

Protokol ini berfungsi mengelola proses eksekusi *software* dan data. Langkah-langkahnya yaitu:

- Main server memanggil bagian dari unprotected software dan mengirimnya dalam bentuk paket ke *crypto coprocessor*.
- The RP *daemon* pada the *crypto coprocessor* membaca *software privacy tag* and meyakinkan *authenticity* and *integrity* dari *package software* yang dikirim tersebut menggunakan verifikasi *Digital Signature (DS)*.
- Selain itu, the RP daemon akan mengecek validitas dari *timestamp* dan menghasilkan kunci KSID melalui dekripsi E(PUCID,KSID) dikombinasikan *customer's private key*.
- The RP daemon mengdekripsi bagian dari *protected software* E(KSID,SSID) menggunakan KSID dan mengeksekusi bagian tersebut menggunakan pengalamatan pada *trusted coprocessor*.
- The RP process menyimpan KSID disimpan dan diidentifikasi berdasarkan (CID, SID) di dalam *persistent storage pada coprocessor*. Langkah ini digunakan untuk menghindari operasi dekripsi *public-key* yang berulang jika *software* yang sama di load kembali.
- Unprotected part dari aplikasi dapat diproses dengan cara mengelompokannya kedalam NP and PPT pada kategorisasi privasi data.

Privacy Feedback Protocol

Privacy feedback protocol adalah komponen penting yang harus dipertimbangkan dan direncanakan saat mendesain layanan *privasi cloud*. Fungsi utama protokol ini adalah untuk menginformasikan kepada pengguna tentang mekanisme privasi data yang berbeda pada teknologi ini. Selain itu, protocol ini juga dapat memberi tahu kepada pengguna jika terdapat kebocoran data atau risiko yang dapat membahayakan kerahasiaan informasi sensitif mereka..



Gambar 6. Proteksi Terhadap *Confidentiality* dan *Integrity* Data Berdasarkan *Privacy Log*
(sumber : Itani, Kayssi, Chehab, 2009)

5. Kesimpulan

Isu keamanan dan privasi menjadi isu utama di dalam teknologi *cloud computing* saat ini. Penggunaan *resource* secara bersama berdampak dengan rentannya suatu data dan informasi tersebut bocor dan disalahgunakan oleh pihak lain yang tidak seharusnya memiliki informasi tersebut. Ancaman privasi data dapat berasal dari pihak internal (penyedia layanan, pengguna dalam perusahaan), dan kebocoran data bisa terjadi karena kegagalan hak akses keamanan di beberapa domain.

Privasi merupakan suatu hal yang sangat penting baik bagi individu maupun lembaga atau instansi untuk berhadapan dan berinteraksi dengan individu lain atau lembaga lain. Salah dalam menyampaikan informasi yang memiliki kemungkinan bernilai *confidential, classified* dan rahasia tidak dapat dipungkiri akan menyebabkan kerugian baik material maupun non material.

Beberapa tindakan untuk mencegah terjadinya pencurian data ini telah dilakukan khususnya dari sisi teknologi. Berbagai macam teknologi menawarkan berbagai model, algoritma, hingga model data untuk meningkatkan keamanan privasi data pada cloud computing. Beberapa teknologi tersebut yang dibahas pada laporan ini adalah cloud intelligent track dan *privacy as a service* (PaaS).

Cloud intelligent track merupakan suatu mekanisme dimana setiap data privasi maupun informasi penting pengguna cloud yang tersimpan di dalam storage cloud provider, harus melalui tahapan dan proses: *working process, encryption, decryption, memory management, keyword generation, risk manageri.* Setiap data tersebut dipecah menjadi beberapa segmen, dan disimpan pada lokasi acak di database. Semua data yang disimpan telah dienkripsi terlebih dahulu dan lokasi penyimpanannya juga membutuhkan public/private key untuk menemukannya. Ketika data dipanggil kembali oleh pengguna, data disatukan kembali dan dilakukan proses dekripsi data.

Sedangkan PaaS merupakan suatu metode yang menawarkan control privacy lebih untuk pengguna. PaaS memungkin pengguna untuk menetukan sendiri sensivitas dan tingkat pentingnya data. PaaS juga menggunakan trusted-third-party untuk mengelola manajemen privacy pengguna tersebut. Sedangkan di sisi server, cloud provider menggunaka crypto coprocessor dan protocol-protocol yang mengatur tentang privasi data pengguna.

Kedua teknologi tersebut sangat memberikan rasa aman bagi pengguna cloud karena mereka dapat mengetahui bahwa data mereka disimpan secara aman dan memiliki akses control lebih terhadap data tersebut.

Referensi

[1] M. Zhout, R. Zhang, Security and Privacy in Cloud Computing: A Survey. Sixth International Conference on Semantics, Knowledge and Grids. Software Engineering Institute, East China Normal University, Shanghai, China. 2010.

[2] G. Zhang, Y. Yang, Key Research Issues for Privacy Protection and Preservation in Cloud Computing. Second International Conference on Cloud and Green Computing. Faculty of Information and Communication Technologies Swinburne University of Technology Hawthorn, Melbourne, Australia. 2012

[3] D., Chen, H., Zhao. Data Security and Privacy Protection Issues in Cloud Computing. International Conference on Computer Science and Electronics Engineering. College of Information Science and Engineering Northeastern University Shenyang, China. 2012.

[4] "Detik.com" [Online]. Survei: 69% Data yang Disimpan di Cloud Hilang. http://inet.detik.com/read/2013/02/21/153735/2176211/323/survei-69-data-yang-disimpan-di-cloud-hilang. Diakses tanggal 18 Mei 2013.

[5] Prashar, Saurabh K. Security Issues in Cloud Computing : 2010.

[6] F. Tina, Analisis Sistem Penyimpanan Data Menggunakan Sistem Cloud Computing. IJNS – Volume 1 Nomor 1. 2012.

[7] P. Y. Helmy, KEBIJAKAN INFORMASI DAN PRIVACY. FISIP, Universitas Airlangga. 2012.

[8] S. M. Rahaman, M. Farhatullah, PccP: A Model for Preserving Cloud Computing Privacy. Dept. of Computer Science Engineering, India. 2012.

[9] M. R. Aswin, M.Kavitha, Cloud Intelligent Track – Risk Analysis And Privacy Data Management In The Cloud Computing. Department of Information Technology Sri Krishna College of Technology Coimbatore, India. 2012.

[10] W. Itani, A. Kayssi, A. Chehab, Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. Department of Electrical and Computer Engineering American University of Beirut, Lebanon. 2009.