**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*

**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].

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].

**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.

3

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]. 4

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]. 5

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 6

*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.*

**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. 9

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, 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.