

Perbandingan *Data Warehouse Cloud Computing* Menggunakan Konvensional Berbasis Kriptografi

Faustina Gunadi, Septian Rheno Widiyanto

Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI, Bandung, Indonesia

Email: v.tinagunadi@yahoo.com, septian.rheno@likmi.ac.id

Abstrak—Penelitian ini melakukan analisa perbandingan *data warehouse cloud computing* dengan *data warehouse* konvensional yang pada umumnya semua *data* yang tersimpan pada *data warehouse* tersebut harus dilindungi dengan menggunakan protokol kriptografi dengan algoritma yang paling aman. Sehingga data yang tersimpan pada *warehouse* tersimpan dengan aman dan terkontrol. Selain itu, setiap jenis usaha perlu menjabarkan kebutuhannya dalam memilih penyimpanan *data* sentralisasi, desentralisasi, atau kedua cara penyimpanan serta pertimbangkan efektifitas dan efisiensi bagi perusahaan memilih *cloud* atau konvensional. Keterkaitan antara *data warehouse* dan kriptografi ini akan menunjukkan kehandalan dari suatu sistem dalam menjaga kode rahasia antara pihak terkait.

Kata Kunci: Data, Sistem Informasi, Teknologi Informasi, Data Warehouse, Cloud Computing, Kriptografi, Algoritma

1. PENDAHULUAN

Kemajuan teknologi internet, media digital seperti gambar, audio, video dan file teks dapat dibagi dan dikirimkan melalui Internet dengan lebih mudah dengan bermacam media. Salah satu tantangan utama dalam berbagi dan mentransmisikan semua jenis informasi melalui saluran publik adalah keamanan data [1].

Perkembangan penggunaan teknologi informasi menginjak tahun 2000 di Indonesia semakin pesat, salah satu yang dapat dirasakan adalah perkembangan teknologi *internet* yang tadinya berkapasitas *byte* sampai dengan saat ini mencapai *megabyte*. Selain itu, perkembangan teknologi jaringan yang tadinya membutuhkan kabel bermeter-meter, semakin berkembangnya jaman kabel sudah tergantikan dengan teknologi *wireless*.

Perkembangan teknologi ini juga membuat *hardware* semakin canggih mulai dari *smartphone*, *laptop*, dan perangkat keras lainnya. Yang perlu diperhatikan adalah perkembangan teknologi di perusahaan karena saat ini pengusaha luar negeri lebih mudah untuk memasarkan produk dari negaranya ke Indonesia karena sudah terfasilitasi dengan *online shop*. Selain itu, pelaku usaha yang tidak berjualan di *online* lebih mudah untuk *supply* barang dari *vendor* di negara manapun karena ada teknologi.

Perkembangan teknologi di perusahaan dan pemerintah tentunya perlu diikuti infrastruktur yang baik juga. Salah satu infrastruktur utama adalah terkait dengan *data warehouse*. *Data warehouse* menjadi salah satu bagian terpenting dikarenakan menyimpan histori pencatatan transaksi selama perusahaan dan pemerintah beroperasi.

Kegunaan *data warehouse* ini akan menjadi sangat berharga ketika *data* yang dikumpulkan menjadi banyak atau sering disebut *Big Data*. Kegunaan *Big Data warehouse* ini sangatlah penting karena mengandung informasi baik itu *user experience*, *product development*, *market respond*, *market research*, tipe pelanggan. Mengapa *data warehouse* sangat diperlukan? Karena data yang terkumpul merupakan aset perusahaan untuk mengembangkan dan berinovasi. Akan ada perbedaan antara *data* bisnis perusahaan yang 3 tahun beroperasi dengan *data* transaksi bisnis perusahaan yang sudah berjalan 30 tahun karena didalamnya mengandung informasi yang sangat berharga. Apabila jatuh ke tangan kompetitor maka pasar akan diambil dan besar kemungkinan kompetitor lebih unggul.

Teknologi yang semakin berkembang menyediakan berbagai macam kemudahan mulai dari aplikasi berbasis *web base* sehingga dapat mudah diintegrasikan satu sama lain. Kemudahan untuk mengakses sejumlah informasi pada segala macam perangkat keras. Teknologi memudahkan informasi tersampaikan dengan cepat kepada pihak yang membutuhkan.

Perkembangan teknologi pun membuat para pakar berpikir terkait dengan seberapa aman teknologi bagi penggunaannya. Keamanan teknologi semakin lama semakin menjadi fokus, dikarenakan semakin berkembang teknologi ada beberapa pihak yang mencoba keahliannya untuk menembus informasi perusahaan atau pemerintah. Berangkat dari hal ini muncul Kriptografi.

Kriptografi sebagai salah satu cara untuk meningkatkan sekuritas *data warehouse* karena dokumen penting akan diterjemahkan ke dalam Kriptografi. Supaya pengguna informasi atas data tersebut adalah pihak yang berkepentingan saja. Kriptografi memiliki banyak algoritma yang dipakai. Kriptografi perlu dipertimbangkan jenis *data warehouse* yang dipilih, jenis data yang disimpan sehingga Kriptografi yang digunakan sesuai dengan kebutuhan.

2. METODOLOGI PENELITIAN

Sebelum memasuki pembahasan terkait dengan informasi, tentunya perlu mengetahui perbedaan antara *data* dan informasi. Definisi *Data* (Sugiyono, 2012:5) adalah bahan mentah yang perlu diolah sehingga menghasilkan informasi atau keterangan, baik kualitatif maupun kuantitatif yang menunjukkan fakta sehingga dapat memberi manfaat bagi peneliti atau memberi gambaran kepada peneliti tentang kondisi atau suatu keadaan [2].

Sedangkan informasi adalah sekumpulan data yang sudah diolah sehingga menghasilkan suatu Analisa untuk digunakan oleh pihak yang membutuhkan. Secara keterkaitan dapat dihubungkan sebagai berikut:



Gambar 1. Proses Perubahan Data menjadi Informasi

Informasi merupakan data yang dapat digunakan oleh pihak yang membutuhkan dikarenakan data tersebut sudah menghasilkan informasi yang dibutuhkan, contoh: *data* transaksi pembelian dan penjualan setelah diproses dan dianalisa oleh bagian *Finance & Accounting* dalam suatu perusahaan maka akan menjadi informasi laporan keuangan yang dapat digunakan untuk pelaporan ke pihak manajemen atau pihak ketiga

Kegiatan sehari – hari yang dilakukan oleh individu atau grup dapat disebut sebagai sistem informasi. Sistem informasi yang digabungkan dengan komputer akan menjadi sistem informasi yang terkomputerisasi. Sistem informasi pada suatu lingkungan kerja akan menjadi Sistem Informasi Manajemen yang penggunaannya ditujukan untuk pengambilan keputusan manajemen, dapat disimpulkan berbeda antara sistem informasi dan sistem informasi manajemen.

Sistem menurut Jogiyanto (2005:2) adalah kumpulan dari elemen – elemen yang berinteraksi untuk tujuan tertentu. *Data* yang sudah diproses menjadi informasi dan diproses menggunakan sistem akan menghasilkan analisa yang diperlukan oleh pihak yang berkepentingan [3].

Sistem informasi tersebut diproses dengan menggunakan teknologi informasi untuk menyimpan, mengolah informasi, dan mendistribusikannya kepada pihak yang membutuhkan. Teknologi informasi menurut (Wawan & Grisna, 2015: 2) UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yaitu: Suatu teknik mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan / atau menyebarkan informasi [4].

Ruang lingkup teknologi informasi mengutip dari (Wawan & Grisna, 2015: 4-5) Berdasarkan *United States Department of Commerce*, ruang lingkup teknologi informasi di Amerika Serikat terdiri atas [4]:

1. Industri perangkat lunak dan jasa teknologi informasi yang meliputi perangkat lunak, penerbit, pengembang aplikasi perangkat lunak, pemasok jasa pemrograman komputer,
2. Perusahaan desain sistem komputer, dan perusahaan manajemen fasilitas. Dalam industri perangkat lunak terdapat beberapa subsektor, di antaranya: *Layanan cloud computing* (pengembang sistem cloud), *Entertainment software* (pengembang aplikasi *video games*), *Electronic commerce (e-commerce)*
3. Industri perangkat keras yang meliputi pengembangan produk baru, desain dan pembuatan perangkat komputer (CPU, tablets PC, ultra-minimal dekstop), perakitan komputer, infrastruktur jaringan, dan peripherals lainnya (*keyboard, mice, printers, servers, electronic security*).
4. Jasa teknologi informasi yang meliputi perusahaan konsultan dan implementasi teknologi informasi (perangkat lunak, perangkat keras, dan jaringan), *internet service provider (ISP)*, dan penyimpanan *data* di *internet (hosting)*.

Perkembangan teknologi informasi yang sangat cepat pada masa kini adalah penggunaan aplikasi ERP (*Enterprises Resources Planning*) untuk mendukung operasional usaha, penggunaan *web base system* untuk mempermudah *integrasi data*, penggunaan *media* komunikasi seperti *media social*. Dapat dilihat perkembangan teknologi informasi cukup pesat. Akan tetapi, untuk menyingkapi semua data yang tersebar itu aman perlu dikaji *media* penyimpanan dan keamanannya.

Sistem Informasi yang beredar tersebut disimpan pada tempat yang disebut *data warehouse*. Penyimpanan Sistem Informasi pada *data warehouse* bertujuan untuk menjaga data tersebut supaya tersimpan dan terpasang *level* sekuritas aksesnya.

Mengutip dari Jurnal (Muhammad Rifqi, Rusdah, Moedjiono) berjudul Penerapan *Data Warehouse* pada PT XYZ dengan menggunakan Metode Kriptografi. *Data warehouse* adalah sebuah *basis data* komprehensif yang mendukung semua analisis keputusan yang diperlukan oleh suatu organisasi dengan menyediakan ringkasan dan rincian informasi. [5]

Penyimpanan sistem informasi pada *data warehouse* terbagi menjadi beberapa jenis berdasarkan arsitektur teknologi informasinya, yakni:

1. Arsitektur tersentralisasi

Penyimpanan data yang tersentralisasi tersimpan di komputer yang memiliki kapasitas simpan yang besar dan mampu memproses jutaan data transaksi. Yang saat *data* tersebut diperlukan maka komputer tersebut dapat merespon dengan cepat. Tipe penyimpanan sentralisasi ini biasanya digunakan oleh perusahaan yang semua datanya disimpan terpusat, tidak memiliki anak cabang karena hanya kantor utama, atau melihat dari sisi sekuritas *data* perusahaan disentralkan

2. Arsitektur desentralisasi

Penyimpanan *data* yang tersebar, yang setiap perangkat tersebut antara satu sama lain terhubung dan memiliki spesifikasi yang serupa, desentralisasi ini sering disebut dengan *peer to peer*. Biasanya sistem yang terdistribusi seperti ini digunakan untuk perusahaan yang memiliki banyak sekali cabang. Arsitektur seperti ini secara biaya lebih murah, tidak ada ongkos perawatan, cepat dan mudah diakses, tanggung jawab sesuai komputer tersebut berada, ada data cadangan untuk *back up*. Semua dapat dicapai dengan baik apabila perancangan dan *standard control* untuk arsitektur desentralisasi sudah dibuat secara jelas dan terarah.

3. Arsitektur *client/server*

Arsitektur ini mengarahkan konektifitas komputer, *client* yang dimaksud adalah piranti lunak yang menerima perintah untuk menjalankan suatu aplikasi yang terkoneksi ke *server*, sedangkan *server* tempat menyimpan data informasi yang diminta oleh *client*. Contoh sederhana: data X disimpan pada server untuk akses dan permintaan *data* tersebut butuh akses

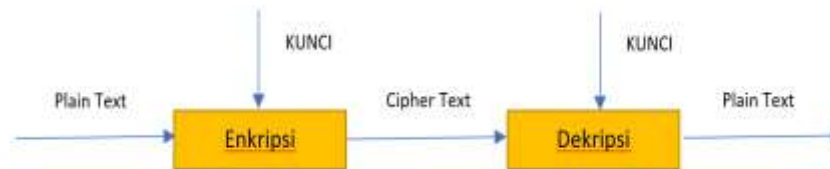
yang disetting atas *client* yang berkaitan atau aplikasi yang diinstall pada *server* akan tetapi dapat di *remote server* oleh komputer yang memiliki akses untuk membuat aplikasi pada *server* tersebut.

4. Arsitektur *cloud*

Arsitektur *cloud* gabungan antara arsitektur desentralisasi dan sentralisasi tapi semuanya berbasis *Web Base*. Mengutip dari *IEEE Interner Computing* suatu paradigma di mana informasi secara permanen tersimpan di *server* di *internet* dan tersimpan secara sementara di komputer pengguna (*client*) termasuk di dalamnya adalah *desktop*, komputer *tablet*, *notebook*, *handheld*, sensor-sensor, monitor dan lain-lain.

Berkenaan dengan pembahasan arsitektur *cloud* sebelumnya; *Cloud Computing* ini mulai dikenal sekitar tahun 2005 setelah salah satu *web* terkenal menggunakan metode ini. Diikuti kompetitor kenamaan lainnya. *Cloud computing* sudah sering digunakan dalam dunia usaha dan keseharian tiap individu, yakni: *email*, *google drive*, *virtual office*. Akan tetapi, yang perlu diperhatikan untuk metode penyimpanan *cloud computing* adalah keamanan. Seberapa aman data tersebut disimpan pada *cloud* yang sistemnya *web base*.

Peningkatan keamanan untuk kerahasiaan *data* yang sudah diproses dan tersimpan dalam teknologi informasi dijaga keamanannya dengan enkripsi menggunakan kriptografi. Penjelasan sederhana Kriptografi adalah merumuskan secara rahasia dengan menggunakan ilmu matematika. Secara keamanan kriptografi memiliki sistem keamanan *confidentiality*, *authentication*, *nonrepudiation*, dan *integrity*.



Gambar 2. Proses Kriptografi

Meningkatkan keamanan dengan menggunakan algoritma kriptografi, sebagai berikut [6]:

1. Algoritma simetris adalah kriptografi konvensional, yang enkripsi dan dekripsi menggunakan kunci yang sama dengan 2 kategori, yakni algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*), contohnya adalah: DES (*Data Encryption Standard*).
2. Algoritma asimetris adalah algoritma yang berbeda antara enkripsi dan dekripsi. Biasanya disebut algoritma kunci umum (*public key algorithm*) karena diketahui semua orang, tapi kunci dekripsi hanya diketahui oleh orang yang mengetahui kata sandinya disebut kunci pribadi (*private key*), contohnya adalah: RSA (*Rivest Shamir Adleman*), *Rabin Miller*, *Greatest Common Divisor*, *Fast Exponentiation*.

Menurut (Munir, Rinaldi) Protokol adalah aturan yang berisi rangkaian langkah – langkah, yang melibatkan dua orang atau lebih orang, yang dibuat untuk menyelesaikan suatu kegiatan. Protokol Kriptografi adalah protokol yang dibuat menggunakan algoritma Kriptografi. [7]

Penggunaan Kriptografi merupakan suatu protokol untuk mengantisipasi adanya peretas atau pihak yang tidak berkepentingan mengakses *file* tersebut. Protokol yang tersedia:

1. Protokol rahasia homomorfik
2. Protokol skema komitmen
3. Tanda tangan buta
4. Protokol uang elektronik

3. HASIL DAN PEMBAHASAN

Tahapan yang dilakukan adalah sebagai berikut:

1. Membandingkan *Data Warehouse Cloud Computing* dengan Konvensional
2. Membandingkan penggunaan Kriptografi untuk *Data Warehouse*
3. Menarik kesimpulan atas hasil perbandingan

Dari perbandingan *data warehouse cloud computing* dengan konvensional didapatkan perbandingan sebagai berikut:

Tabel 1. Perbandingan *Data Warehouse Cloud Computing* dan Konvensional

Deskripsi	<i>Cloud Computing</i>	<i>Server Konvensional</i>	Keterangan
infrastruktur	<i>public cloud</i> , <i>private cloud</i> , <i>hybrid cloud</i>	<i>private server</i>	Penyediaan infrastruktur konvensional akan banyak menyita biaya
kriptografi	<i>Public</i> = sederhana, contoh: otentifikasi <i>user</i>	Kontrol dan keamanan ditentukan perusahaan sendiri	Lebih baik kontrol dan keamanan yang konvensional

Deskripsi	Cloud Computing	Server Konvensional	Keterangan
	<i>Private</i> = firewall / <i>maintenancenya</i> di perusahaan penyewa		
	<i>Hybrid</i> = gabungan <i>private</i> dan <i>public</i>		
biaya	Biaya lebih rendah dibandingkan membuat dan <i>maintain data warehouse</i> sendiri	Biaya relatif tinggi karena harus <i>maintenance, control</i> , menyediakan tenaga kerja	Sisi efisien lebih menguntungkan yang <i>cloud</i>
keamanan	Masih menjadi perbincangan karena semua bergantung pada jenis <i>cloud</i> yang digunakan	Kontrol lebih baik karena dilakukan sendiri	Lebih cenderung pilihan <i>Private</i> lebih baik untuk keamanan
Jenis layanan	<i>Infrastructure as a service</i> <i>Platform as a service</i> <i>Software as a service</i>	Sentralisasi Desentralisasi	sesuai dengan kebutuhan perusahaan
Perlindungan legal	sesuai keberadaan <i>server</i> utama tersebut, sehingga Hukum sesuai negara tempat <i>server</i> tersebut	Terjamin	Sulit diidentifikasi karena <i>server cloud</i> menggunakan desentralisasi dan sentralisasi yang dikendalikan penyediannya

Berdasarkan perbandingan diatas pemilihan penyimpanan *data warehouse* disesuaikan dengan kebutuhan perusahaan, apabila perusahaan memiliki banyak cabang perlu kombinasi antara *cloud computing* untuk data umum, sedangkan untuk *data private* dapat *maintain server* sendiri atau menggunakan layanan IaaS dari penyedia seperti : *Google, Yahoo, Microsoft, Facebook, Amazon* serta *Apple*. Sedangkan *data* yang bersifat rahasia dapat *maintain* perusahaan menggunakan infrastruktur konvensional atau menggunakan *private cloud* yang bagian kontrol dan keamanan diserahkan kepada usernya

Tabel 2. Tabel Perbandingan Penggunaan Kriptografi pada *data warehouse cloud* dan konvensional

Deskripsi	Cloud Computing	Server Konvensional	Keterangan
kriptografi	<i>Public</i> = sederhana, contoh: otentifikasi <i>user</i> <i>Private</i> = firewall / <i>maintenancenya</i> di perusahaan penyewa <i>Hybrid</i> = gabungan <i>private</i> dan <i>public</i>	Kontrol dan keamanan ditentukan perusahaan sendiri	Lebih baik kontrol dan keamanan yang konvensional
Algoritma yang digunakan	<i>Public</i> = cukup otentifikasi user <i>Private</i> = penggunaan metode Kriptografi RSA	Kriptografi RSA	Dikarenakan Kriptografi RSA membedakan antara enkripsi dan dekripsi, yang perhitungannya menggunakan kombinasi ilmu matematika yang cukup beragam, seperti pada rumusan RSA: 1. $p \& q$ adalah bilangan prima 2. kemudian mencari bilangan prima acak dari rumusan $(p-1) * (q-1)$ untuk menentukan $d \& e$ 3. kemudian dapat perhitungan $k =$ bilangan prima dari point 2 yang dapat di faktorisasi 4. kemudian 2 angka faktorisasi digunakan untuk menentukan $E =$ public exponent, $D =$ private exponent 5. setelah itu tentukan enkripsi dan dekripsi dengan memasukan : enkripsi = $p * q$ dan e dekripsi = $p * q$ dan d

Berdasarkan keamanan data maka sebaiknya baik *private cloud* dan *data warehouse* konvensional menggunakan protokol kriptografi dengan menggunakan RSA supaya *data* dapat tersimpan lebih aman. Penggunaan algoritma RSA ini dapat menjadi solusi bagi tiga pihak terkait pihak 1 dan pihak 2 punya *public exponent* dan *private exponent*nya sendiri dan pihak

provider membuat korelasi antara 2 pihak tersebut lebih aman dengan adanya *public exponent* dan *private exponent* yang direleaseny.

4. KESIMPULAN

Berdasarkan hasil perbandingan *data warehouse* mana yang terbaik sebaiknya perusahaan berskala besar memilih *hybrid cloud* beserta dengan menggunakan algoritma RSA sebagai kontrol keamanannya. Perusahaan skala besar pasti membutuhkan akses yang cepat dan terdesentralisasi untuk distribusi informasinya sehingga *hybrid cloud* merupakan solusi yang tepat; yang secara layanan dapat menggunakan IaaS untuk kontrol dan keamanan data penting.

Semua akses data sudah terhubung dengan internet sebaiknya tipe *data warehouse* konvensional perlu mengembangkan sekuritasnya, dikarenakan jika hanya otentifikasi akan mudah diretas, lain halnya jika menggunakan algoritma dalam sistem keamanan *data*.

Penelitian menghasilkan baik *data warehouse cloud computing* dan konvensional memiliki fokus utama pada keamanan. Hal ini yang sebaiknya lebih difokuskan dalam penelitian selanjutnya

REFERENCES

- [1] Abbas, Abdul Jamal. *Perbankan Syariah Kontemporer: Prinsip, Nilai dan Perkembangannya di Indonesia*. Jakarta: Bintang Pustaka, 2011.
- [2] Antonio, Muhammad Syafi'i. *Bank Syariah dari Teori & Praktik*. Jakarta: Gema Insani, 2005.
- [3] Antonio, Muhammad Syafi'i. *Bank Syariah Bagi Bankir & Praktisi Keuangan*. Jakarta: Bank Indonesia dan Tazkia Institute, 1999.
- [4] Antonio, Muhammad Syafi'i. *Perkembangan Lembaga Keuangan Islam*. Jakarta: BAMUI dan BMI, 2006.
- [5] Arifin, Zainul. *Memahami Bank Syariah: Lingkup, Peluang, Tantangan dan Prospek*. Jakarta: Alva Bet, 2000.
- [6] Chapra, M. Umer. *Sistem Moneter Islam*. Jakarta: Gema Insani Press, 2000.
- [7] Hartanto, Agus. *Pengantar Perbankan Syariah di Indonesia: Teori dan Praktek*. Jakarta: Elfa Indonesia Madani, 2012.
- [8] Hisyamuddin. *Dilema Perbankan Syariah Nasional: Antara Kebutuhan, Kenyataan dan Keharusan*. Bandung: Mitra Abadi Press, 2011.
- [9] Karim, Adwarman. *Ekonomi Islam: Suatu Kajian Kontemporer*. Jakarta: Gema Insani, 2001.
- [10] Kartadijaya, Usman. *Menyoroti Fenomena Perbankan Syariah di Indonesia*. Bandung: PT.Insan Madani, 2011.
- [11] Kotler, Philip. *Marketing Management, The Millennium Edition*. New Jersey: Practice Hall Internitonal inc, 2000.
- [12] Mannan, M. Abdul. *Teori dan Praktek Ekonomi Islam*. Yogyakarta: PT. Dana Bhakti Wakaf, 2001.
- [13] Notoadmadjo, Soekidjo. *Pengembangan Sumber Daya Manusia*. Jakarta: Rineka Cipta, 2003.
- [14] Sjahdeini, Sutan Remy. *Perbankan Islam dan Kedudukannya Dalam Tata Hukum Perbankan Indonesia*. Jakarta: Grafiti, 1999.