

DATA WAREHOUSE DAN KEAMANAN OLAP

**Oleh
SUPAWI / 23203133**



**Program Magister Teknik Elektro
Bidang Khusus Teknologi Informasi-Dikmenjur
Institut Teknologi Bandung
2004**

Kata Pengantar

Puji syukur kehadiran Allah SWT yang dengan rahmat-Nya penulis dapat menyelesaikan tugas akhir mata kuliah Sistem Keamanan Lanjut yang berjudul Data Warehouse dan Keamanan Olap di Magister Teknik Elektro Bidang Khusus Teknologi Informasi ITB selama kurang lebih empat bulan.

Di dalam tugas akhir ini diperoleh pengetahuan dan pengalaman dalam menangani masalah Data Warehouse dan Keamanan Olap terutama menyangkut Keamanan Olap yang kemudian dituangkan dalam laporan tugas akhir ini. Penulis juga mendapatkan bimbingan dan arahan dari berbagai pihak yang sangat membantu kelancaran pelaksanaan tugas akhir yang dilakukan. Pada kesempatan kali ini penulis ingin mengucapkan terimakasih yang sebesar-besarnya kepada :

1. Bapak Dr.Ir. Budiraharjo selaku dosen pengasuh mata kuliah Sistem Keamanan Lanjut.
2. Teman-teman seangkatan yang telah banyak membantu.
3. Serta pihak yang tidak dapat penulis sebutkan satu-persatu yang telah membantu dalam proses penyelesaian tugas ini.

Penulis menyadari bahwa masih banyak kekurangan dalam laporan tugas akhir ini, oleh karena itu penulis menerima masukan, saran, maupun kritikan dari semua pihak. Penulis juga berharap agar laporan ini dapat berguna bagi kita semua. Amin.

Bandung, Juni 2003

Penulis

DAFTAR ISI

HALAMAN MUKA

KATA PENGANTAR

DAFTAR ISI

ABSTRAKSI

I. PENDAHULUAN	4
1.1 Kebutuhan General Security	5
1.2 Access Control	6
1.3 Rancangan OLAP Security	7
2. PERSYARATAN dan POLICIES OLAP SECURITY	10
2.1 Basic Requirements	11
2.2 Advanced Requirements	11
2.3 Inference Control	12
3. MEKANISME OLAP SECURITY	13
3.1 Komponen Arsitektur Security	13
3.2 Pendekatan Umum	14
3.3 Permasalahan dalam Menyembunyikan Information dalam Kubus	15
4. IMPLEMENTASI Pada SISTEM COMERSIAL	17
4.1 ROLAP Based Tools (SQL Views)	17
4.2 Microsoft SQL Server (OLAP/Analysis Services)	18
4.3 MicroStrategy 7	19
4.4 Cognos PowerPlay	19
4.5 Oracle Express	20
5. KESIMPULAN	21
DAFTAR PUSTAKA	22

Abstraksi

Kemanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui oleh pihak yang berhak saja, apalagi pengirimannya dilakukan melalui jaringan publik, apabila keamanan data tersebut tidak maksimal maka data tersebut dapat disadap oleh pihak yang tidak berhak.

Online Analytical Processing (OLAP) merupakan salah satu aplikasi keamanan memutuskan untuk mendukung system keamanan data warehouse dalam system data base, ketika cakupan para pemakai data warehouse akses terus berkembang setelah sistem data warehouse dibangun dengan open source.

Tujuan paper ini adalah untuk memperkenalkan metodologi disain keamanan OLAP, dan menghadirkan kemungkinan akses kontrol pada kompleksitas database. Mekanisme keamanan OLAP dan implementasinya dalam sistem komersil diteliti kemudian diperkenalkan, apakah memenuhi persyaratan kebutuhan atau tidak.

1. Pendahuluan

Keterkaitan data warehouse dengan *online analytical processing* (OLAP) dengan cepat berkembang dalam beberapa kurun waktu. Pada sisi lain, sensitivitas keamanan informasi dan privacy juga sangat dibutuhkan.

Tidak banyak pendekatan yang telah dibuat untuk mengintegrasikan dua bidang ini. Data warehouse dengan alami menciptakan security. Di lain pihak, kebutuhan agar semua data penting dapat diakses semudah mungkin. Sementara data ini pada umumnya sangat berharga dan sensitive.

Konsep keamanan pada dasarnya sangat luas (mencakup isu sosial dan etis, isu moral, privacy dan undang-undang yang sah). Pada paper ini, di fokuskan pada sebagian besar tentang teknis otoritas dan akses kontrol.

Penelitian security pada makalah ini dalam konteks mengarahkan untuk mempelajari pengintegrasian *geographical information systems* (GIS) dan teknologi data warehouse. Dimana kita bertanggung jawab pada integritas data dan keamanan. Konsep yang dikembangkan harus bisa diterapkan untuk semua aplikasi OLAP.

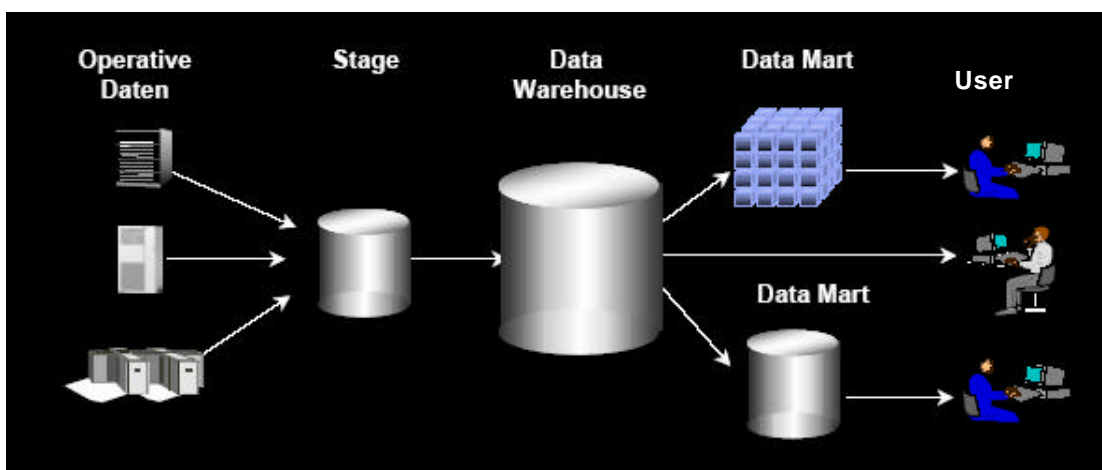
Metoda penulisan makalah ini adalah :

1. Topik utama diarahkan kepada keamanan general data warehouse dan identifikasi akses kontrol OLAP.
2. Persyaratan akses kontrol digolongkan oleh kompleksitasnya pada bagian 2.
3. Bagian 3 tentang sukses mekanisme keamanan OLAP dan permasalahan mereka pada konsep penjualan.
4. Pada bagian 4 merupakan perbandingan dengan implementasi sistem yang berbeda.
5. Akhirnya, bagian 5 merupakan kesimpulan dan sketsa alur riset masa depan..

1.1 Kebutuhan General Security

Sangat banyak komunikasi terjadi pada sistem data warehouse, menciptakan kebutuhan keamanan komunikasi yang sesuai dengan kebutuhan Proses pengambilan data (transfer source data dari operasional database kepada data warehouse) membutuhkan satu persyaratan untuk suatu infrastruktur jaringan. Independent atau mungkin sharing source database harus diperkuat. Ketika data mungkin sangat sensitip maka penting untuk melindunginya dari eavesdropping dan ancaman yang lain. Untuk komunikasi antara aplikasi awal dan akhir serta OLAP server (atau data warehouse dalam 2 lingkungan) biasanya koneksi client/server akan digunakan, termasuk pada lokasi remote. Walaupun informasi pada chanel ini adalah hampir pasti bisa dikumpulkan dan sedikit komplet, mungkin saja keamanan sangat kritis. Penggunaan Internet atau jaringan lain mungkin diperlukan security. Hanya beberapa tools support encrypted komunikasi pada level aplikasi seperti teknologi *virtual private network* (VPN) yang mungkin sesuai.

Authentication dan ketelitian adalah ukuran keamanan lain yang harus dilakukan di lingkungan data wrehouse. Bukti suatu identitas pemakai yang bersih diperlukan dalam rangka menjaga keamanan dan untuk menghindari akses oleh para pemakai yang tidak syah. Proses aplikasi data ware house dapat dilihat pada gambar 1 berikut.



Gambar 1. Proses Aplikasi Data Warehouse

Hubungan identifikasi pemakai dan mekanisme authentication memeriksa keaslian identitas yang mengaku pemilik identitas, dalam frontend perkakas, atau dengan menggunakan mekanisme authentication yang disediakan oleh tools atau sistem operasi modern disebut dengan strategi "single sign-on" Keputusan yang penting untuk pemerikasan dalam data warehouse adalah untuk menempatkan sasaran yang tepat pada arsitektur. Penggunaan kemampuan auditing dasar DBMS membuat data warehouse tidak mencukupi kebutuhan, seperti ketika memasukkan akses pada tabel bagan star/snowflake (atau object yang serupa) tidak akan menyingkapkan multidimensional query yang telah dibuat (terutama dalam sistem berbasis MOLAP). Kesimpulannya adalah bahwa auditing perlu juga dilakukan pada multidimensional level satu engine OLAP yaitu. pada level yang sama di mana otoritas ilmu semantik digunakan).

1.2 Access Control

Akses kontrol pada sisi back-end melibatkan pengendalian akses pada data warehouse dan source database pada saat proses transform/load dan akses pada prosedur ini (permohonan seperti halnya administrasi). Pada otoritas berbasis role model untuk proses administratif dalam data warehouse terdapat dua katagori identifikasi. Pengembang tulis penyaringan, integrasi dan transformasi scrif. Mereka membutuhkan akses terutama pada metadata, bukan datanya sendiri. Personil operasi meminta proses coresponden tersebut. Mereka tidak memerlukan ijin untuk mengakses data secara langsung, hanya untuk menjalankan program. Bagaimanapun, ketika permasalahan timbul, pengembang dan personil operasi mungkin memerlukan akses tambahan beberapa data seperti untuk strategi membersihkan data atau untuk menentukan kesalahan. Satu kekuatan mengijinkan, jika meyakinkan bahwa pengguna ijin seperti itu secara ekstensif dimonitor oleh auditing.

Pada sisi front-end banyak akses kontrol muncul. Biasanya data warehouse disangsikan oleh para pemakai eksekutif (manajemen eksekutif, analis bisnis), dengan meminta OLAP vendor untuk tidak menyediakan peralatan pendukung untuk akses yang berjangkauan halus akses kontrol. Hal tidak lagi sesuai. Cakupan pemakai potensial

tentang analisis tools queryng satu data warehouse terus berkembang, sampai pada pelanggan dan mitranya. Proteksi sensitive data dari akses yang tidak syah terus diperdebatkan, menuju ke arah kebutuhan kebijakan akses kontrol untuk akses enduser pada data warehouse . Tidak tiap pemakai bisa mengakses semua data.

Aplikasi Front-End termasuk laporan statis (berjalan dan menciptakan/memodifikasi laporan), OLAP, dan data mining/KDD. Dalam aplikasi laporan statis, di mana pemakai hanya menggunakan query statis sudah dikenal, akses kontrol dapat digambarkan sebagai suatu basis per laporan . Pada sisi lain sangat sulit untuk mengaplikasikan keamanan pada data mining. Data mining diarahkan pada penemuan data baru; hasilnya (dan kepekaannya) tidaklah dikenal sebelumnya. Bagaimanapun, beberapa kebijakan (seperti partisi data warehouse) dapat diterapkan pada satu teknologi mart-like data. Tools utama Fron-tend untuk data warehouse adalah aplikasi OLAP, menyediakan ad-hoc analisis interactive dari struktur multidimensi data. Suatu data warehouse dibangun dengan sistem terbuka.

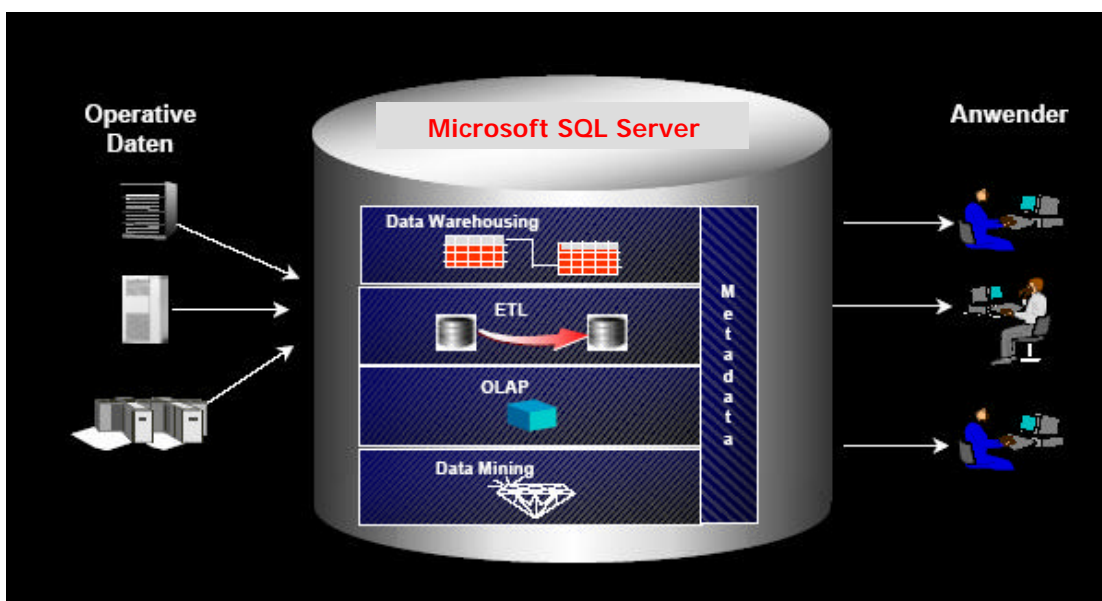
Pada akhirnya adalah untuk membuat semua data yang penting dapat diakses semudah mungkin. Terutama penelitian analisis OLAP memerlukan sifat terbuka; kontrol keamanan bisa saja menghalangi proses penemuan analitis. Kita sudah mengenal keamanan komunikasi, mengidentifikasi pemakai dan authentication, auditing, dan keamanan akses kontrol merupakan hal yang penting. Ketika kita memfokuskan pada akses kontrol dalam ad-hoc aplikasi OLAP kita akan menggunakan istilah keamanan OLAP pada bahasan makalah ini.

1.3 Rancangan OLAP Security

Menurunkan kebijakan akses kontrol dari operasional data source sangat sulit walaupun beberapa riset telah dilakukan. Data dari sistem yang berbeda dengan kebijakan yang berbeda akan di konsolidasikan. Para pemakai sistem operasional tidak sama dengan pemakai data warehouse. Masalah utama adalah, bahwa relational model mendominasi dalam sistem operasional ketika sistem OLAP menggunakan nontraditional multidimensional model. Rencana akses kontrol tidak mudah dipetakan.

Proteksi tidak digambarkan dalam kaitan dengan tabel, tetapi dimensi, alur hirarkis, granularas level. Sehingga dibutuhkan desain keamanan OLAP.

Telah dijelaskan bahwa perancangan akses OLAP harus dilakukan dengan teliti, ketika analisis ditolak atau hasil adalah salah. Apalagi kemampuan keamanan tool sangat proprietary dan sintak security tidak mungkin untuk didesain dan didokumentasi dari pembatasan akses.

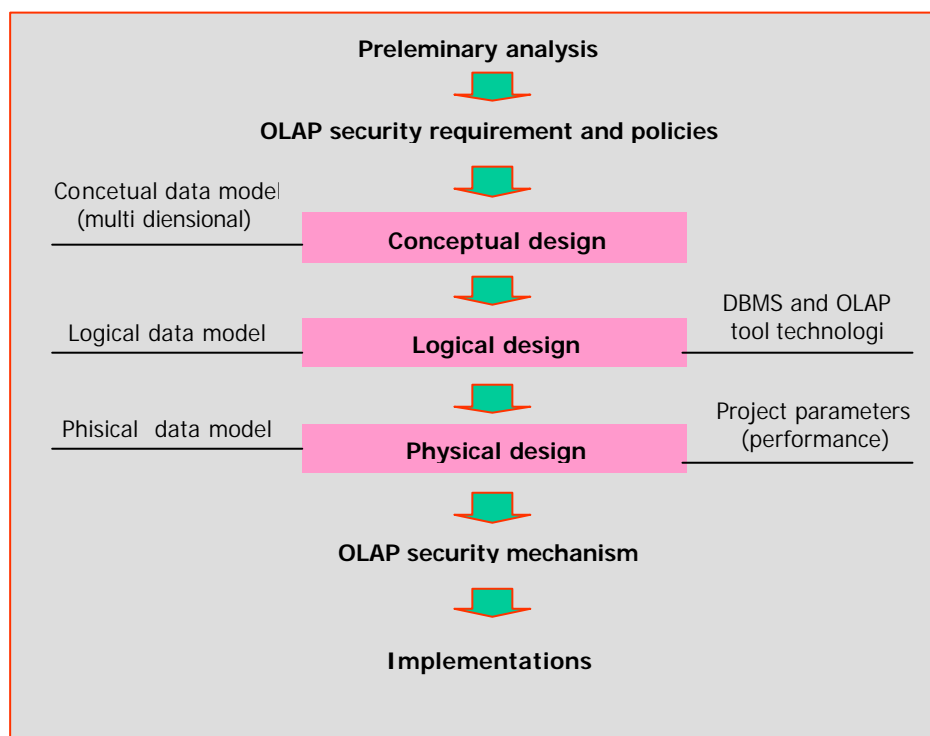


Gambar 2. Posisi Olap Security pada Data Warehouse sistem

Dalam rangka mendekati topik dari sisi aplikasi, metodologi desain klasikal database (persyaratan analisis, konseptual, logis, dan desain fisik) harus diplikasikan pada keamanan OLAP. Gambar 2 diadopsi dari yang menyarankan model keamanan database reguler. Perbedaan yang penting, adalah konseptual multidimensional data model dan mekanisme keamanan OLAP yang jelas berbeda dengan kemampuan relational manajemen sistem database. Tahap pertama pada makalah ini adalah proses menandai [Bold] pada diagram, tahap kedua adalah desain.

Suatu pendekatan metodologis multiphase mengijinkan kebijakan keamanan untuk terpisah dari mekanisme keamanan. Separasi ini menghasilkan keuntungan antara lain :

1. Kemampuan menggambarkan aturan akses kontrol dan pemikiran tentang implementasinya (dengan tidak ada beban tentang detail implementasi).
2. Memungkinkan untuk dibandingkan dengan kebijakan akses kontrol yang berbeda, atau mekanisme yang berbeda pada kebijakan yang sama. Terutama berguna untuk banyaknya tools OLAP yang heterogen.
3. Kemampuan mekanisme perancangan pada kebijakan yang berbeda. Keuntungan ini menjadi suatu hal yang penting ketika kebijakan berubah seperti konsekwensi dari berubah organisasi.

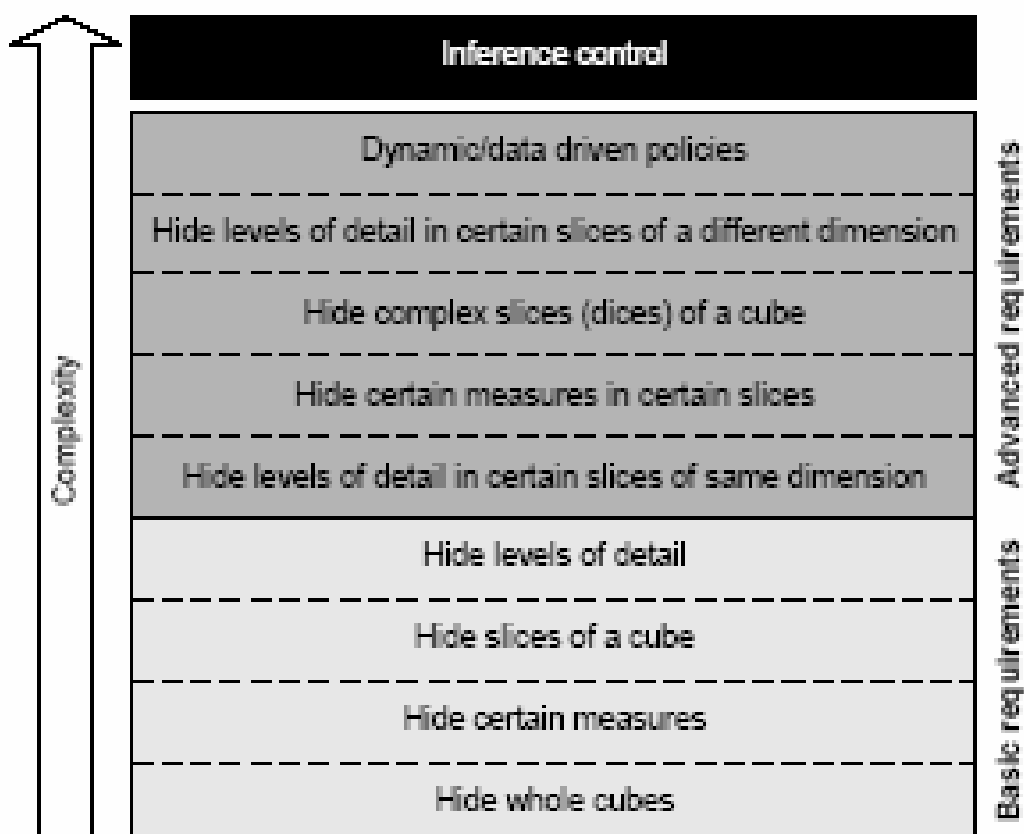


Gambar 3. Metodologi Rancangan Olap Security

2. Persyaratan dan Policies Olap Security

Aplikasi yang berbeda akan mendorong kearah persyaratan yang sangat berbeda pula yaitu. kebijakan yang mungkin untuk akses kontrol OLAP. Hasil analisis persyaratan adalah petunjuk tingkat tinggi yang dapat diterjemahkan dalam aturan format, yang pantas untuk formalitas dan tahap disain. Bagaimanapun, pondasi yang sesuai untuk konsep keamanan model multidimensional tidak tersedia.

Gambar 2 menggambarkan persaratan basic dan advance akses kontrol yang akan dibahas :



Gambar 4. Pesyaratan Olap acces control lain

2.1 Basic Requirements

Menyembunyikan kubus yang utuh merupakan persyaratan langsung. Dalam konteks akhir satu aturan korespondence akses menetapkan pemakai tertentu hanya dapat melihat data Services kubus dan bukan dari kubus individu.

Jika satu dimensi tertentu mencerminkan struktur para pemakai, maka diperlukan untuk menyembunyikan irisan tertentu dari suatu kubus. Menyembunyikan ukuran tertentu sama dengan menyembunyikan irisan. Sesungguhnya, tidak ada perbedaan yang konseptual jika satuan ukuran ditafsirkan sebagai dimensi flat. Data yang detil sering dipertimbangkan lebih sensitip dibanding data ringkas. Bisa diperlukan untuk membatasi akses terhadap data di bawah tingkatan dimensi yang detil. Ini terbentang dari level kecil penyembunyian suatu dimensi keseluruhan.

2.2 Advanced Requirements

Jika data detil sangat sensitip seperti tersebut di atas, dan pemakai bertanggung jawab atas anggota yang tertentu dari suatu dimensi (yaitu. irisan kubus), ini membawa ke arah kebijakan di mana dibutuhkan untuk menyembunyikan tingkat detil dalam irisan tertentu dari suatu kubus. Mempertimbangkan kebijakan akses kontrol untuk para manajer: " Seorang manajer dapat memperoleh informasi apapun tentang kebutuhannya, data hanya terbatas untuk object yang lain."

Ketika perancangan kebijakan seperti itu menimbulkan perbedaan substansial apakah dimensi yang di atasnya merupakan irisan dan level dimensi detil untuk disembunyikan sama atau tidak. Sebagai suatu contoh untuk menyembunyikan level detil dalam irisan tertentu dari dimensi yang berbeda, diasumsikan seorang manajer diijinkan untuk melihat data sehari-hari miliknya, tetapi data bulanan hanya untuk yang lain.

Dalam dinamis atau aturan kebijakan data akses tidak digambarkan oleh unsur-unsur struktur tertentu dari multidimensional model data. Ijin akses tergantung dari datanya sendiri. Suatu contoh adalah satu grup pemakai dapat mengakses object lebih

dari 5,000 pengunjung per bulan saja (katakan, object ini dianggap sebagai kepentingan publik). Ketika ini dapat berubah dari tiap load data, disebut kebijakan dinamis.

2.3 Inference Control

Sistem OLAP terfokus kepada kesimpulan permasalahan ketika mereka bertumpu pada ringkasan atau kumpulan data. Keterkaitan dengan akses kumpulan data seperti itu, smart query (disebut tracker) mendapatkan data yang tidak dapat diakses secara langsung.

Kesimpulan informasi telah dikenali pada riset keamanan database statistik. Permasalahan dasarnya adalah untuk melindungi data individu ketika kumpulan query diijinkan. Suatu masalah yang serupa muncul dalam OLAP melalui penggolongan yang paralel. Dalam praktek, dimensi tidak sama dengan orthogonal seperti dalam teori. Jika suatu tingkatan detail tertentu disembunyikan, tetapi dimensi klasifikasi paralel masih tetap ada (tak terlarang), nilai detail tersembunyi mungkin diungkapkan oleh otoritas query tunggal. Suatu pendekatan kepada kesimpulan single-query adalah menyangkal query yang disertakan kurang dari jumlah arsip tertentu (query-set kontrol), disebut indikator kepicikan. Bagaimanapun, telah ditunjukkan bahwa suatu kombinasi yang diperbolehkan (kumpulan) tracker query dapat digunakan untuk menyimpulkan detail data tersembunyi.

Pada riset lebih lanjut, usaha yang diperlukan adalah mungkin tidak feasibly untuk kebanyakan "realita kehidupan" rancangan. Menyajikan suatu indikator pendekatan yang dilandaskan pada mengarahkan kesimpulan singlequery. Bagaimanapun, tidak berarti melawan tracker yang dengan cerdas mengkombinasikan berbagai query. Satu pendekatan yang menarik adalah penggunaan data mining tool untuk mendeteksi potensi permasalahan kesimpulan dalam audit pembukuan query.

3. Mekanisme OLAP Security

Dalam persyaratan analisis dan konsep tahapan desain keamanan, perlu difokuskan kepada aspek semantik tanpa terlebih dahulu mempertimbangkan detail implementasinya. Bagaimanapun, dalam rangka mengembangkan metodologi desain yang bermanfaat, diperlukan kemampuan konkret sistem. Disini akan dijelaskan mekanisme keamanan OLAP pada level independen vendor, dan pada bagian berikutnya meliputi implementasi konkret sistem komersil.

Mekanisme security secara umum menyediakan menggambarkan subject security (pemakai, kelompok, aturan) boleh atau tidak mengakses object keamanan tertentu (yaitu. data sensitip) pada umumnya akses pada OLAP. Asumsi akhir menetapkan apakah segalanya terlarang kecuali jika diijinkan (dunia yang tertutup) atau sebaliknya (dunia yang terbuka). Dalam kaitan dengan para pemakai level atas, aplikasi OLAP membuka kebijakan dunia yang mungkin sesuai. Sesungguhnya semua evaluasi sistem komersil mengikuti dunia kebijakan. Aspek lain adalah applicabilitas prinsip masing-masing. Jika object keamanan adalah hal utama dalam keamanan, maka akan menuju kearah suatu didesentralisasi kebijakan. Seperti Ketika "pemilik" data warehouse merupakan pemilik dari koresponden operasional data, ini merupakan persyaratan artinya menurunkan kebijakan akses kontrol dari sumber data operasional. Bagaimanapun, seperti disebutkan sebelumnya, adalah sulit untuk memutuskan kepemilikan kumpulan sumber data yang berbeda. Pusat kebijakan administrasi standar adalah alternatif.

3.1 Komponen Arsitektur Security

Salah satu cara mengkatagorikan mekanisme security yang berbeda dengan komponen arsitektur yang digunakan antara lain :

1. Relasional DBMS data warehouse (star/snowflake dalam skema OLAP atau kompleksitas lingkungan). Akses kontrol diterapkan dengan menciptakan berbagai database physic (data mart) atau dengan menggunakan SQL views. Batasan akses

yang dinyatakan dalam multi-dimensional model harus di terjemahkan dalam relational model.

2. Jika tersedia OLAP server. Ini harus merupakan pendekatan dari multidimensional model yang digunakan dalam lingkungan client/server menyediakan perlindungan yang memerlukan proteksi terhadap bypass mekanisme keamanan.
3. Aplikasi front-end. Model Multidimensional digunakan untuk menyatakan pembatasan, tetapi mencegah akses yang tidak sah dengan membypass system, bisa jadi sangat sulit. Ketika dua pendekatan hanya menyediakan satu batasan implisit analisa tool (data tertentu tidak disajikan oleh OLAP server atau DBMS), pendekatan ini dapat diperluas dengan membatasi hubungan pemakai. Fungsi Import/Export atau visualisasi komponen dapat dilumpuhkan untuk para pemakai tertentu.

Bagaimanapun, berbagai kemungkinan yang tersedia tergantung dengan arsitektur yang dikembangkan. Dalam solusi keamanan server OLAP tidak bisa digunakan 2-tier fat-client lingkungan ROLAP dan penggunaan SQL views dalam relational data warehouse level tidak sesuai untuk MOLAP sistem.

3.2 Pendekatan Umum

Cara lain menggolongkan mekanisme keamanan yang tersedia adalah untuk melihat ciri dan dasar aturan pendekatan.

Views adalah cara menerangkan gambaran subsets sistem secara keseluruhan. Analisis tool adalah terbatas untuk diberi hak query dengan pembatasan kemampuan navigasi (menyembunyikan metadata dimensi anggota atau unsur-unsur yang struktural). Bagaimanakah menyembunyikan keberadaan data sensitip tidak hanya datanya sendiri. Pemakai yang berbeda, melihat kubus yang berbeda, menurutnya semua dibangun dari sumber data yang sama. Konsepnya adalah transparan untuk end-user ketika tidak ada query ditolak. Bagaimanapun, ketransparanan ini juga baha ya ketika kehilangan data yang mungkin cendrung dipalsukan.

Views dapat diciptakan menggunakan SQL views dengan bagan views multidimensional OLAP level engine jika support. Walaupun persyaratan dinyatakan dalam terminologi multidimensional, suatu notasi yang umum untuk melihat pada level ini tidak tersedia. Dalam relational world views dinyatakan seperti hasil dari relational query. Bagaimanapun, pendekatan ini tidak bisa secara langsung diterjemahkan ke dalam dunia multidimensional. Satu query SQL pada suatu hasil hubungan dirinya sendiri, tetapi multidimensional query dilakukan atas suatu hypercube tidak perlu menghasilkan hypercube. Apalagi tidak ada bahasa query yang umum (walaupun pendekatan yang pertama dibuat, seperti MDX Microsoft).

Aturan yang didasarkan pendekatan tidak menyajikan (structurally) kubus lain kepada pemakai. Semua pemakai mengetahui keberadaan kubus secara keseluruhan (dengan semua dimensi dan ukuran), mereka hanya tidak diijinkan untuk melihat semua itu. Aturan mengakses (pada umumnya dalam bentuk ekspresi Boolean) menggambarkan apa yang dapat dilihat seorang pemakai dan apa yang ia tidak boleh dilihat. Aturan ungkapan ini, bagaimanapun, menjadi sangat kompleks dan susah untuk dipelihara.

Dalam aturan didasarkan pada otoritas sistem OLAP, laporan boleh jadi ditolak atau mendapatkan sel yang kosong. Kebijakan yang kompleks dapat dinyatakan menggunakan aturan berdasarkan pendekatan dengan cell-level granularity. Untuk menginformasikan kepada pemakai tentang hasil yang dipalsukan, sel yang telah ditinggalkan kosong untuk alasan keamanan adalah umumnya ditandai dengan " N/A".

Ketika pendekatan (view dan rule) mempunyai keuntungan kombinasi kedua konsep yang diinginkan. hibryd pendekatan mengijinkan untuk menetapkan kompleks (cell-level) aturan batasan seperti halnya definisi pandangan untuk menyaring elemen metadata dan dimensi anggota untuk menyediakan level derajat tertentu tentang transparansi pemakai akhir.

3.3 Permasalahan dalam Menyembunyikan Information dalam Kubus

Sifat Multidimensional data OLAP, timbulnya beberapa masalah ketika akan menyembunyikan informasi dalam kubus. Jika irisan kubus tertentu tersembunyi, data

pada suatu Region level akan dipalsukan (object yang seandainya kelihatan dimasukkan), atau, jika tak diubah, tracker query menduga data yang tersembunyi mungkin menjadi tersedia.

Persyaratan keamanan yang kompleks, seperti menyembunyikan level detail dalam irisan tertentu dari suatu dimensi yang berbeda, telah diperkenalkan. Ini hanya dapat implementasikan menggunakan pendekatan rule-based dan mungkin akan mengakibatkan penolakan. Jika esekusi parsial digunakan, semantik total dalam laporan belum jelas, karena itu, ada tidaknya digambarkan apakah sel yang dimasukkan tersembunyi atau tidak.

Sebagai contoh, seorang manajer pada satu daerah mengakses obyek data sehari-hari. Query ini diijinkan Untuk dilakukan. Ia kemudian mengeluarkan operasi drill-down pada dimensi waktu untuk data sehari-hari. Jika query tidak ditolak, hasil akan menjadi tidak sempurna (data sehari-hari untuk beberapa object tidak dapat diakses). Tetapi bagaimana pada laporan total ? Mereka dapat mengulang yang lain yang belum dirubah dan refleksi "riil" total (yaitu. semua object), meninggalkan laporan dalam status yang tidak konsisten. Atau dapat dijumlahkan atas display nilai yang aktual, yang artinya bahwa penjumlahan sudah merubah dari satu query kepada yang lain walaupun menyangsikan daerah (yakni semua object). Sesungguhnya, kedua pendekatan dapat ditemukan dalam sistem komersil masa kini (kadang-kadang hasil genap tergantung dengan perumusan yang berhubungan dengan sintaksis dari query).

4. Implementasi Pada Sistem Comersial

Pada bagian ini, merupakan ikhtisar singkat kemampuan akses kontrol dari sistem OLAP komersil dan menyajikan penggunaan views SQL dalam ROLAP. Untuk lebih jelasnya, kemampuan beberapa system keamanan olap dapat dilihat pada table 1.

Table 1. Security feature comparison of the evaluated products

	Product	ROLAP based products	Microsoft SQL Server 2000	MicroStrategy 7	Cognos PowerPlay	Oracle Express
Info	Evaluated release	N/A	8.0 BETA	7.0 BETA	6.0	6.2
	Supported security feature(s)	SQL views	Cell-level and dimension security	Access control list and security filters	User class and dimension views	Permission programs
	Security enforcing architecture component	DBMS	OLAP server or OLAP front-end	OLAP server or OLAP front-end	OLAP front-end	OLAP server
	General approach	View	Hybrid ²	View	View	Rule
	Security policy	Closed world	Open world	Open world	Open world	Open world
	Security administration	Ownership	Administrator	Ownership	Administrator	Administrator
Requirements	Hide whole cubes	●	●	●	●	●
	Hide certain measures	●	●	●	●	● ³
	Hide slices of a cube	●	●	●	●	● ³
	Hide levels of detail	●	●	●	●	● ³
	Hide levels of detail in certain slices of same dimension	● ⁴	●	○ ⁶	●	●
	Hide certain measures in certain slices	● ⁵	●	○ ⁶	–	●
	Hide complex slices (dices) of a cube	● ⁵	●	● ⁵	–	●
	Hide levels of detail in certain slices of a different dimension	○ ^{5,7}	●	○	–	●
	Dynamic/data driven constraints	○ ^{5,8}	○ ⁸	○ ^{5,8}	–	○ ⁸
Inference control	–	–	–	–	–	

4.1 ROLAP Based Tools (SQL Views)

Dalam projex *ROLAP tools relational views* digunakan jika produk tidak support pada akses kontrol OLAP server level. Penggunaan SQL views serupa dengan membangun data mart dari satu data warehouse. Bagaimanapun, SQL views dalam relational data warehouse level dapat menjadi sangat kompleks dan sulit untuk dipelihara. Masalah lain yang muncul ketika precalculated (materialized) kumpulan ada. Ini harus disaring dengan selalu berhubungan. Mekanisme tambahan harus digunakan

untuk penyaringan metadata dalam rangka menyembunyikan unsur-unsur struktur tertentu.

Dasar persyaratan pada umumnya diterapkan dengan mudah terhadap relational views. Ukuran dapat disembunyikan dengan menerapkan penyaringan vertikal (menyembunyikan kolom) dalam tabel sebenarnya. Dalam rangka menyembunyikan irisan kubus horizontal penyaringan harus diberlakukan bagi tabel dimensi. Tergantung dari arsitektur filtering, dimensi tabel mungkin cukup dengan membatasi query atau melalui tools analisa. Dalam praktek extra (akses kontrol list) ACL, kolom dalam tabel ini dapat digunakan untuk menyederhanakan pemeliharaan views.

Kebijakan yang kompleks lebih menantang. Level Menyembunyikan detail dalam irisan tertentu dari dimensi yang sama menciptakan fakta dengan dasar granularas yang berbeda. Bagaimanapun, tidak semua sistem mendukung tabel fakta partisi (bisa ditirukan oleh views) pada berbeda granularas. Sebagai alternatif, dimensi "gadungan" anggota digunakan. Kebijakan yang lebih rumit adalah mungkin, tetapi berbahaya seperti menyaring bersesuaian fakta mungkin didorong kearah falsi- analisa fied lanjutan. Tidak ada pengingkaran yang eksplisit tentang query atau " N/A" tanda-tanda dari sel dapat terpenuhi.

4.2 Microsoft SQL Server (OLAP/Analysis Services)

Model Keamanan untuk release yang pertama MICROSOFT OLAP service sebagian terbesar sangat sederhana. Hanya dua lingkup akses kontrol tersedia (server dan level kubus). Pada service pack 1 (SP1) diperkenalkan keamanan realese cell-level, menyediakan derajat tingkat pendenda dari kontrol. Menggunakan keamanan cell-level, para pemakai mendapatkan garansi atau ditolak untuk mengakses data hingga menuju ke sel individu dalam suatu kubus. Cell-Level keamanan adalah aturan didasarkan pendekatan.

Pembatasan digambarkan dengan aturan akses menggunakan ungkapan MDX Boolean. Bahkan batasan yang kompleks dapat dinyatakan dengan aturan cell-level keamanan. Bagaimanapun, query dengan tegas ditolak atau dikembalikan. Sql Server

2000 meningkatkan model keamanan jasa OLAP (disebut Analysis service), sebagai tambahan terhadap cell-level keamanan, suatu dimensi keamanan menonjolkan metadata dan penyaringan anggota dimensi untuk menyediakan ketransparanan pemakai akhir. Dengan ukuran dimensi keamanan, tingkatan hirarki, dan anggota dimensi (yaitu. irisan) dapat tersembunyi.

4.3 MicroStrategy 7

Microstrategy 7 membuat dua arti tentang kendali akses. Pertama, suatu daftar akses kontrol memelihar seluruh objek metadata, termasuk atribut (seperti. hirarki dimensi level) dan ukuran matrik, tetapi juga menyaring, templates dan laporan. Owner atau pengurus memutuskan siapa yang boleh mengakses obyek tersebut. Sebagai contoh, jika seorang pemakai tidak diizinkan membaca akses level dimensi hirarki tertentu, ia tidak akan bisa membuat laporan pada granularas tingkatan itu, atau mengakses level tersebut dari laporan yang ada. Bagaimanapun, jika seseorang dengan akses pada level tersebut membuat laporan seperti itu dan pemakai lain yang mengakses, ia akan bisa menjalankannya.

Cara yang kedua untuk mengontrol data akses dalam *Microstrategy 7* disebut filter keamanan. Ini akan mencegah pemakai untuk melihat data tertentu dalam database tersebut. Suatu filter dibangun untuk menghadirkan slicing dari OLAP query. Saringan dapat didasarkan pada atribut (dimensi) anggota atau ukuran matrik. Filter Security secara implisit mengakibatkan dimana terkandung SQL kode yang dihasilkan (*Microstrategy 7* adalah suatu RELATIONAL OLAP tool). Jika aturan penyaringan yang kompleks tertentu tidak bisa terpenuhi oleh filter keamanan, SQL views layer dapat diletakkan pada tempatnya.

4.4 Cognos PowerPlay

Dalam Cognos Powerplay keamanan dipaksa oleh penggunaan alat awal dan akhir menggunakan ecurity file otorisasi (mungkin encrypted). Kontrol Akses digambarkan atas kategori (Cognos terminologi untuk dimensi anggota), ukuran, atau level dimensi, penggunaan pendekatan multidimensional views. Itu diterapkan dengan

menciptakan berbagai pandangan dimensi penggunaan kubus dan untuk kelompok pemakai yang berbeda, atau dengan penjelasan kelas view pemakai pada kubus bersama.

Cognos Powerplay sangat fleksibel dalam menyembunyikan kategori dari dimensi tunggal. Bagaimanapun, tidaklah mungkin menggambarkan batasan kompleks yang menyertakan berbagai dimensi. Pembatasan seperti itu harus diterapkan dengan populasi berbagai kubus dengan data yang berbeda subsets (seperti data mart).

4.5 Oracle Express

Dalam Oracle express akses database dikendalikan dengan penggunaan program ijin database, menyediakan aturan berdasarkan pendekatan. Pada setiap database, program ijin dapat diciptakan Fungsi Boolean user-defined. Ketika suatu database dibuka, Oracle express berjalan bersesuaian ijin program. Dalam program ijin database, mengizinkan perintah digunakan untuk menetapkan kondisi-kondisi akses untuk object pada database. Kondisi-Kondisi untuk mengabulkan ijin atas suatu obyek database terdiri dari satu atau lebih Ungkapan Boolean.

Dimensi anggota pada granularas tingkatan yang berbeda diperlakukan dengan bebas (data dipegang secara berlebihan). Oleh sebab itu, Oracle express sangat fleksibel dalam menetapkan batasan yang kompleks. Pada sisi lain, ketika program ijin menyediakan data filtering, sisa-sisa anggota dimensi dan metadata tanpa perubahan, tidaklah mungkin menyembunyikan keberadaan data yang sensitip.

5. Kesimpulan

Pada paper ini diperoleh, pertama ikhtisar data warehouse dan keamanan OLAP. Dalam kaitan dengan fakta bahwa cakupan dari para pemakai mungkin mengakses data warehouse via aplikasi OLAP terus meningkat, keperluan mekanisme kendali akses yang sesuai adalah rumit dalam rangka memastikan kerahasiaan data yang sensitip.

Kita sudah memperkenalkan metodologi desain keamanan OLAP dan mengenali persyaratan kendali akses yang berbeda. Sistem komersil masa kini menyediakan beberapa mekanisme untuk mengatasi persyaratan ini. Bagaimanapun, pendekatan adalah sangat dibutuhkan.

Untuk masa depan di dalam dan di luar tujuan proyek, kita akan berkonsentrasi pada modeling ilmu keamanan semantik. Seperti tersebut sebelumnya, tidak ada lapisan yang konseptual untuk desain keamanan OLAP.

DAFTAR PUSTAKA

1. Inmon, W.H., *Building the Data Warehouse*. John Wiley, 1992.
2. <http://www.olapcouncil.org>
3. Codd, E.F., S.B. Codd, C.T. Salley, "Providing OLAP (On-Line Analytical Processing) to User Analyst: An IT Mandate." Available from Arbor Software's web site <http://www.arborsoft.com/OLAP.html>.
4. Kimball, R. *The Data Warehouse Toolkit*. John Wiley, 1996.
5. Barclay, T., R. Barnes, J. Gray, P. Sundaresan, "Loading Databases using Dataflow Parallelism." *SIGMOD Record*, Vol.23, No. 4, Dec.1994.
6. Zhuge, Y., H. Garcia-Molina, J. Hammer, J. Widom, "View Maintenance in a Warehousing Environment, *Proc. Of SIGMOD Conf.*, 1995.
7. Harinarayan V., Rajaraman A., Ullman J.D. "Implementing Data Cubes Efficiently" *Proc. of SIGMOD Conf.*, 1996.
8. Chaudhuri S., Krishnamurthy R., Potamianos S., Shim K. "Optimizing Queries with Materialized Views" *Intl. Conference on Data Engineering*, 1995.
9. Kim W. "On Optimizing a SQL-like Nested Query" *ACM TODS*, Sep 1982.
10. Gupta A., Harinarayan V., Quass D. "Aggregate-Query Processing in Data Warehouse Environments", *Proc. of VLDB*,1995.
11. Dewitt D.J., Gray J. "Parallel Database Systems: The Future of High Performance Database Systems" *CACM*, June 1992.
12. Agrawal S. et.al. "On the Computation of Multidimensional Aggregates" *Proc. of VLDB Conf.*, 1996.
13. Chatziantoniou D., Ross K. "Querying Multiple Features in Relational Databases" *Proc. of VLDB Conf.*, 1996.
14. Wu, M-C., A.P. Buchmann. "Research Issues in Data Warehousing." *Submitted for publication*.