1. **Pertemuan 8**

**UTS**

1. **Pertemuan 14**

11.1 Pemrosesan Query

Query Language merupakan bahasa khusus yang digunakan untuk melakukan perintah-perintah untuk mengakses data pada sistem basis data.

Query Language atau yang lebih dikenal dengan nama SQL merupakan suatu bahasa yang digunakan untuk membuat sebuah database.

Langkah dasar pemrosesan query :

1. Parsing dan translasi

a. Translasi query menjadi bentuk internal kemudian translasikan ke aljabar relasional

b. Parser memeriksa sintaks dan verifikasi relasi-relasi

2. Optimasi : memilih evaluasi plan yang paling rendah costnya

3. Evaluasi : query-execution engine memakai query-evaluation plan, mengeksekusi plan tersebut, dan mengembalikan hasilnya

Cost umumnya diukur sebagai total waktu diperlukan untuk menyelesaikan query

1. Banyak faktor yang menentukan cost : Kecepatan akses disk, CPU, atau sampai komunikasi jaringan

2. Kecepatan akses disk adalah faktor utama penentu cost dan relatif mudah diperkirakan. Kecepatan ini diukur dengan :

a. Number of seeks \* average-seek-cost

b. Number of blocks read \* average-block-read-cost

c. Number of blocks written \* average-block-write-cost

Cost untuk menulis sebuah blok lebih besar dari cost untuk membaca blok karena setelah menulis, data akan dibaca lagi untuk memastikan data yang ditulis berhasil.

Operasi-operasi dalam pemrosesan query :

1. Selection dengan menggunakan algoritma searching seperti A1,A2,A3,A4,A5,A6,A7,A8,A9,A10,A11

2. Sorting

Untuk relasi yang muat di memori, teknik ini seperti quicksort, sedangkan untuk relasi yang tidak cocok pada memori, external sort-merge cukup bagus.

3. Join diimplementasikan dengan beberapa algoritma seperti nested-loop join, block nested-loop join, indexed nested-loop join, merge-join, hash-join

4. Duplicate elimination dapat diimplementasikan dengan hashing atau sorting

5. Agregation dapat diimplementasikan dengan cara yang sama pada duplicate elimination

6. Projection diimplementasikan dengan melakukan proyeksi pada setiap tupel yang diikuti dengan duplicate elimination

7. Set operations (^,V,-) dapat digunakan sebagai varian dari merge-join setelah sorting atau varian dari hash-join

8. Outer join adalah modifikasi dari join dengan diikuti tambahan NULL sesuai dengan ruas yang diinginkan

1. Struktur Dasar

2. Fungsi Agregasi

3. Nilai Null

4. Manipulasi Data

Bekerja dengan SQL

1. Create Menciptakan tabel, indeks atau pandangan

2. Drop Menghapus tabel, indeks atau pandangan

3. Alter Mengubah struktur tabel

4. Insert Menambahkan sebuah baris pada tabel

5. Update Mengubah nilai pada sebuah baris

6. Delete Menghapus baris pada tabel

1. **Pertemuan 15**

12.1 Proteksi Data dan aplikasi Basis Data

Keamanan database adalah suatu cara untuk melindungi database dari ancaman, baikdalam bentuk kesengajaan atau pun bukan. Ancaman adalah segala situasi atau kejadian baik secara sengaja maupun tidak yang bersifat merugikan dan mempengaruhi system serta secara konsekuensi terhadap perusahaan/organisasi yang memiliki system database.Keamanan database tidak hanya berkenaan dengan data yang ada pada database saja, tetapi juga meliputi bagian lain dari system database, yang tentunya dapat mempengaruhi database tersebut. Hal ini berarti keamanan database mencakup perangkat keras, perangkat lunak, orang dan data.

Agar memiliki suatu keamanan yang efektif dibutuhkan kontrol yang tepat. Seseorang yang mempunyai hak untuk mengontrol dan mengatur database biasanya disebut Administrator database. Seorang administratorlah yang memegang peranan penting pada suatu system database, oleh karena itu administrator harus mempunyai kemampuan dan pengetahuan yang cukup agar dapat mengatur suatu system database Keamanan merupakan suatu proteksi terhadap pengrusakan data dan pemakaian data oleh pemakai yang tidak punya kewenangan.

System yang aman memastikan kerahasian data yang terdapat didalamnya. Beberapa aspek keamanan yaitu :

 •Mambatasi akses ke data dan servis

 Melakukan autentifikasi pada user

 Memonitor aktivitas-aktivitas yang mencurigakan

Keamanan database dapat dikelompokan sebagai berikut :

 Pencurian dan penipuan.

Pencurian dan penipuan database tidak hanya mempengaruhi lingkungan database

tetapi juga seluruh perusahaan/organisasi. Keadaan ini dilakukan oleh orang, dimana seseorang ingin melakukan pencurian data atau manipulasi data, seperti saldo rekening,transaksi,transfer dan lain-lain. Untuk itu fokus harus dilakukan pada kekuatan system agar menghindari akses oleh orang yang tidak memiliki kewenangan.

 Hilangnya kerahasiaan dan privasi

Suatu data dapat memiliki nilai kerahasiaan, karena data tersebut merupakan

sumber daya yang strategis pada perusahaan, maka pada kasus ini data tersebut

harus diamankan dengan memberikan hak akses pada orang tertentu saja.

 Hilangnya integritas

Integritas ini berkaitan dengan akurasi dan kebenaran data dalam database, seperti

data korup.Hal ini akan secara serius mempengaruhi perusahaan/organisasi.

 Hilangnya ketersediaan

Hilangnya ketersediaan berarti data, system, keduanya tidak dapat diakses,servis

mati, yang tentunya secara serius sangat mempengaruhi perusahaan/organisasi.

Saat ini banyak perusahaan yang membutuhkan kemampuan system yang aktif 7

x 24 , 7 hari 1 minggu.

Berdasarkan pengelompokan tersebut, tentunya banyak aspek yang harus kitaperhatikan demi terciptanya keamanan database. Bisa saja seseorang mencuri computer kita yang berisi data penting, mungkin juga karyawan yang diberi hak untuk mengakses data melakukan kejahatan dengan menjual informasi tersebut pada pihak lain demi kepentingan pribadi. Hal-hal tersebut memang termasuk kendala keamanan database yang harus mendapat perhatian, tetapi seorang administrator tidak dapat mengawasi kelemahan tersebut. Seorang administrator hanya fokus pada sistem database itu sendiri, dan hal inilah yang akan kita bicarakan. Tentunya perkembangan teknologi mengharuskan suatu perusahaan untuk mengimplementasikan system database yang bukan hanya aman tetapi juga mudah diakses dan handal, menyala 7×24 jam, 7 hari 1 minggu tanpaoff.

Penyebaran informasi secara global sangat menguntungkan semua pihak. Dengan adanya internet, komunikasi antar cabang, perusahaan, konsumen dan sebagainya semakin mudah. Pemberian informasi mengenai perusahaan kepada masyarakat melalui internet merupakan salah satu strategi komunikasi, marketing, public relation perusahaan tersebut,adanya transaksi on line yang meningkatkan gaya hidup masyarakat dan lainlain. Semua itu tidak terlepas dari suatu perkembangan system database dan tentunya membuat keamanan menjadi rentan. Sangatlah mudah dalam suatu lingkungan database diciptakan suasana yang menakutkan, tanpa kepastian dan keraguan. Sebagai seorang administrator sangat perlu memperhatikan kondisi tersebut. Tentukan resiko yang sebenarnya dan selidiki apa yang dapat dilakukan terhadap kondisi itu. Sebenarnya kebanyakan database terkonfigurasi dalam keadaan yang mudah ditembus, akan tetapi hal ini bukan berarti database tidak dapat dibuat aman sebagaimana mestinya.

12.2 Ancaman terhadap database

Serangan terhadap database

Secara garis besar keamanan database dikategorikan sbb:

 Keamanan Server

Perlindungan Server adalah suatu proses pembatasan akses yang sebenarnya pada database dalam server itu sendiri. Menurut Blake Wiedman ini adalah suatu sisi keamanan yang sangat penting dan harus direncanakan secara hati-hati. Ide dasarnya adalah kita tidak dapat mengakses apa yang kita tidak dapat lihat, atau apakah kita ingin database server kita dapat dilihat diseluruh dunia? Database kita bukanlah suatu web server,koneksi yang tidak dikenali tidak diijinkan.

 Trusted Ip Access

Setiap server harus dapat mengkonfigurasikan alamat ip yang diperbolehkan mengakses dirinya. Kita tidak mengijinkan semua orang dapat mengakses server kita sebagaimana kita tidak mengijinkan orang lain memasuki rumah kita tanpa ijin. Jika server melayani suatu web server maka hanya alamat web server itu saja yang dapat mengakses server database tersebut.Jika server database melayani jaringan internal maka hanya alamat jaringanlah yang boleh menghubungi server. Sangat perlu diperhatikan bahwa jangan pernah menggabungkan server database web dengan server database informasi internal perusahaan anda, ini adalah suatu mental yang buruk untuk seorang admin. Trusted Ip Access merupakan server database terbatas yang hanya akan memberi respon pada Ip yang dikenali saja.

 Koneksi Database

Saat ini semakin banyaknya aplikasi dinamis menjadi sangat menggoda untuk melakukan akses yang cepat bahkan update yang langsung tanpa authentifikasi. Jangan pernah berpikir demikian, ini hanya untuk seorang pemalas. Jika kita ingin mengijinkan pemakai dapat mengubah database melalui web page, pastikan anda memvalidasi semua masukan untuk memastikan bahwa inputan benar, terjamin dan aman.Sebagai contoh, pastikan anda menghilangkan semua code SQL agar tidak dapat dimasukan oleh user.Jika anda seorang admin yang membutuhkan koneksi ODBC,pastikan koneksi yang digunakan unik.

 Kontrol Akses Tabel

Kontrol akses table ini adalah salah satu bentuk keamanan database yang sering diabaikan,karena cukup sulit penerapannya. Penggunaan control akses table yang benar dibutuhkan kolaborasi antara system administrator dengan pengembang database. Hal inilah yang sulit dilakukan. Pemberian ijin user untuk mengakses informasi dapat membuat informasi terbuka kepada public. Jika seorang user mengakses informasi apakah akan dilihat menggunakan session yang sama? Atau jika table digunakan sebagai referensi system mengapa ia diberikan ijin selain hak membaca saja.

12.3 Perlindungan terhadap data yang sensitif

Penyalahgunaan Database :

1. Tidak disengaja, jenisnya :

a. kerusakan selama proses transaksi

b. anomali yang disebabkan oleh akses database yang konkuren

c. anomali yang disebabkan oleh pendistribuasian data pada beberapa komputer

d. logika error yang mengancam kemampuan transaksi untuk mempertahankan

konsistensi database.

2. Disengaja, jenisnya :

a. Pengambilan data / pembacaan data oleh pihak yang tidak berwenang.

b. Pengubahan data oleh pihak yang tidak berwenang.

c. Penghapusan data oleh pihak yang tidak berwenang.

Tingkatan Pada Keamanan Database :

1. Fisikal : Lokasi-lokasi dimana terdapat sistem komputer haruslah aman secara fisik terhadap serangan perusak.

2. Manusia : wewenang pemakai harus dilakukan dengan berhati-hati untuk

mengurangi kemungkinan adanya manipulasi oleh pemakai yang berwenang

3. Sistem Operasi : Kelemahan pada SO ini memungkinkan pengaksesan data oleh pihak tak berwenang, karena hampir seluruh jaringan sistem database menggunakan akses jarak jauh.

4. Sistem Database : Pengaturan hak pemakai yang baik.

Keamanan Data :

1. Otorisasi :

o Pemberian Wewenang atau hak istimewa (priviledge) untuk mengakses sistem atau obyek database

o Kendali otorisasi (=kontrol akses) dapat dibangun pada perangkat lunak dengan 2 fungsi :

• Mengendalikan sistem atau obyek yang dapat diakses

• Mengendalikan bagaimana pengguna menggunakannya

• Sistem administrasi yang bertanggungjawab untuk memberikan hak akses dengan membuat account pengguna.

2. Tabel View :

Merupakan metode pembatasan bagi pengguna untuk mendapatkan model

database yang sesuai dengan kebutuhan perorangan. Metode ini dapat menyembunyikan data yang tidak digunakan atau tidak perlu dilihat oleh pengguna.

Contoh pada Database relasional, untuk pengamanan dilakukan beberapa level :

1. Relasi adalah pengguna diperbolehkan atau tidak diperbolehkan mengakses langsung suatu relasi

2. View adalah pengguna diperbolehkan atau tidak diperbolehkan mengakses data yang terapat pada view

3. Read Authorization adalah pengguna diperbolehkan membaca data, tetapi tidak dapat memodifikasi.

4. Insert Authorization adalah pengguna diperbolehkan menambah data baru, tetapi tidak dapat memodifikasi data yang sudah ada.

5. Update Authorization adalah engguna diperbolehkan memodifikasi data, tetapi tidak dapat menghapus data.

6. Delete Authorization adalah pengguna diperbolehkan menghapus data.

Untuk Modifikasi data terdapat otorisasi tambahan :

1. Index Authorization adalah pengguna diperbolehkan membuat dan menghapus index data.

2. Resource Authorization adalah pengguna diperbolehkan membuat relasi-relasi baru.

3. Alteration Authorization adalah pengguna diperbolehkan menambah/menghapus atribut suatu relasi.

4. Drop Authorization adalah pengguna diperbolehkan menghapus relasi yang

sudah ada.

1. **Pertemuan 16**

UAS

**DAFTAR PUSTAKA**

Korth, H., Silberschats, A., Sudarshan, S., 1998, Database System Concept, McGraw-Hill Ramakrishnan, R., 1998, Database Management Systems, McGraw-Hill

Kadir, A., 1999, Konsep dan Tuntunan Praktis Basis Data, Penerbit Andi Fatansyah, 2004, Basis Data, Penerbit Informatika

Ullman, J.D., 1998, Principles of Database and Knowledge Base Systems, Computer Science Press

Date, C.J., 1990, An Introduction to Database System, Addison-Wesley

Elmasri, R., Navathe, S.B., 2000, Fundamental of Database Systems, 3rd Edition, Addison Wesley

Husni I. Pohan, 2002, SQL + Tutorial plus Studi Kasus dengan Oracle dan Sybase, Penerbit Informatika Bandung

Rebecca M. Riordan, 2005, Designing Effective Database Systems, Addison Wesley Professional