BAB XII
KEAMANAN SISTEM DATABASE

12.1 Pengertian Keamanan Database

Keamanan database adalah suatu cara untuk melindungi database dari ancaman, baik dalam bentuk kesengajaan atau pun bukan. Ancaman adalah segala situasi atau kejadian baik secara sengaja maupun tidak yang bersifat merugikan dan mempengaruhi sistem serta secara konsekuensi terhadap perusahaan/ organisasi yang memiliki sistem database.Keamanan database tidak hanya berkenaan dengan data yang ada pada database saja, tetapi juga meliputi bagian lain dari sistem 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 Database Administrator. Seorang administrator-lah yang memegang peranan penting pada suatu system database, oleh karena itu administrator harus mempunyai kemampuan dan pengetahuan yang cukup agar dapat mengatur suatu sistem database.

Keamanan merupakan suatu proteksi terhadap pengrusakan data dan pemakaian data oleh pemakai yang tidak punya kewenangan. Sistem yang aman memastikan kerahasian data yang terdapat didalamnya.

Beberapa aspek keamanan yaitu:

a. Membatasi akses ke data dan servis.
b. Melakukan autentifikasi pada user.
c. Memonitor aktivitas - aktivitas yang mencurigakan.[20]

Penyerangan Database, yaitu :

1. Informasi sensitif yang tersimpan di dalam database dapat terbuka (disclosed) bagi orang- orang yang tidak diizinkan (unauthorized).
2. Informasi sensitif yang tersimpan di dalam database dapat altered in an unacceptable manner
3. Informasi sensitif yang tersimpan di dalam database dapat inaccessible bagi orang-orang yang diizinkan.[18]

Untuk menjaga kemanan database dapat dengan :

1. Penentuan perangkat lunak database server yang handal
2. pemberian otoritas kepada user mana saja yang berhak mengakses, serta memanipulasi data-data yang ada.

Secara umum masalah keamanan database dapat dikelompokan sebagai berikut :[20]

1. **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 sistem agar menghindari akses oleh orang yang tidak memiliki kewenangan.

2. **Hilangnya kerahasiaan dan privasi**
   Suatu data dapat memiliki nilai kerahasiaan, karena data tersebut merupakansumber daya yang strategis pada perusahaan, maka pada kasus ini data tersebut harus diamankan dengan memberikan hak akses pada orang tertentu saja.

3. **Hilangnya integritas**
   Integritas ini berkaitan dengan akurasi dan kebenaran data dalam database, seperti data korup. Hal ini akan secara serius mempengaruhi perusahaan/organisasi.

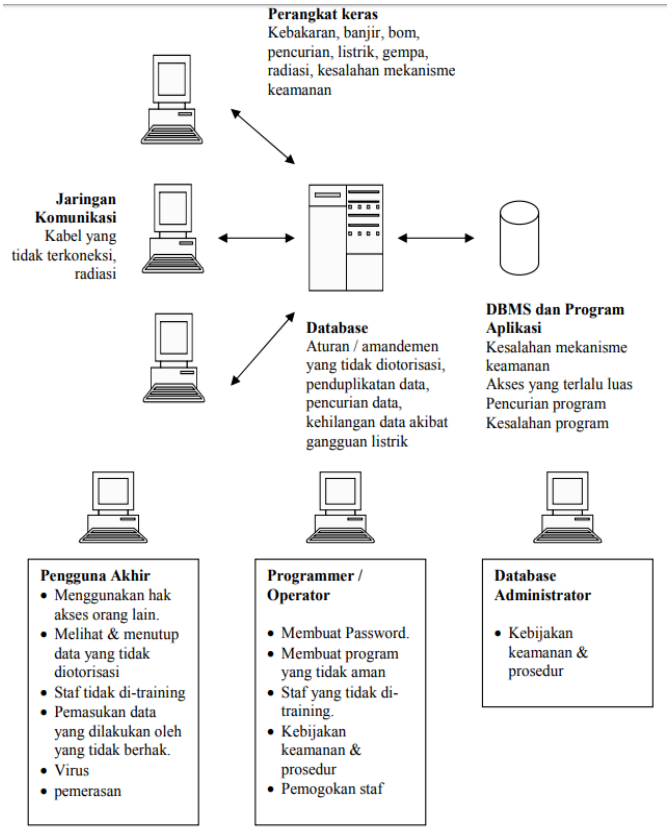
4. **Hilangnya ketersediaan**
   Hilangnya ketersediaan berarti data, sistem, keduanya tidak dapat diakses,servis mati, yang tentunya secara serius sangat mempengaruhi perusahaan/organisasi. Saat ini banyak perusahaan yang membutuhkan kemampuan system yang aktif 7 x 24 , 7 hari 1 minggu.

Ancaman terhadap keamanan database, yaitu :

1. Interruption : sumber daya basis data dirusak atau menjadi tidak dapat dipakai (ancaman terhadap availability)
2. Interception : pemakai atau bagian yang tidak berhak mengakses sumber daya basis data (ancaman secrecy)
3. Modification : pemakai atau bagian yang tidak berhak tidak hanya mengakses tapi juga merusak sumber daya system computer (ancaman integrity)
4. Fabrication : pemakai atau bagian yang tidak berhak menyisipkan objek palsu kedalam system (ancaman integrity)

cara menjaga keamanan database, yaitu:

1. Penentuan perangkat lunak Data Base Server yang handal.
2. Pemberian otoritas kepada user mana saja yang berhak mengakses, serta memanipulasi data yang ada.



Gambar 12.1 Konsep keamanan database

12.2 Bentuk Penyalahgunaan Database

Klasifikasi penyalahgunaan database berdasarkan jenis perlakuannya:

2. 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 mempertahankankonsistensi database.

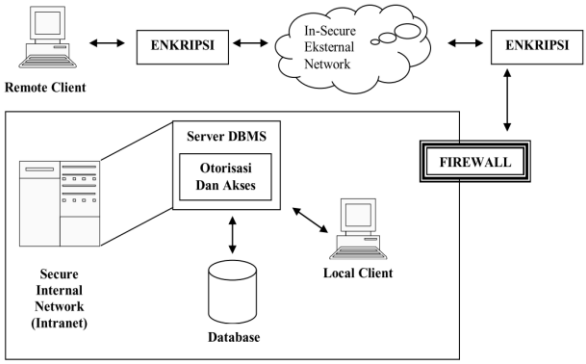
3. Disengaja, jenisnya:
   a) pengambilan data / pembacaan data oleh pihak yang tidak berwenang.
   b) pengubahan data oleh pihak yang tidak berwenang.
   c) penghapusan data oleh pihak yang tidak berwenang.

12.3 Tingkatan Pada Keamanan Database

Tingkatan pada keamanan database antara lain:

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.



Gambar 12.2 Sistem keamanan database

12.4 Kemanan Data

Keamanan merupakan suatu proteksi terhadap pengerusakan data dan pemakaian data oleh pemakai yang tidak punya kewenangan.

a. Otorisasi :

- Pemberian Wewenang atau hak istimewa (priviledge) untuk mengakses sistem atau obyek database
- Kendali otorisasi (kontrol akses) dapat dibangun pada perangkat lunak dengan 2 fungsi :
  a. Mengendalikan sistem atau obyek yang dapat diakses
  b. Mengendalikan bagaimana pengguna menggunakannya
- Sistem administrasi yang bertanggungjawab untuk memberikan hak akses dengan membuat account pengguna.

b. 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 : pengguna diperbolehkan atau tidak diperbolehkan mengakses langsung suatu relasi
2. View : pengguna diperbolehkan atau tidak diperbolehkan mengakses data yang terapat pada view

3. Read Authorization : pengguna diperbolehkan membaca data, tetapi tidak dapat memodifikasi.
4. Insert Authorization : pengguna diperbolehkan menambah data baru, tetapi tidak dapat memodifikasi data yang sudah ada.
5. Update Authorization : pengguna diperbolehkan memodifikasi data, tetapi tidak dapat menghapus data.
6. Delete Authorization : pengguna diperbolehkan menghapus data.

Untuk modifikasi data terdapat otorisasi tambahan :

1. Index Authorization : pengguna diperbolehkan membuat dan menghapus index data.
2. Resource Authorization : pengguna diperbolehkan membuat relasi-relasi baru.
3. Alteration Authorization : pengguna diperbolehkan menambah/menghapus atribut suatu relasi.
4. Drop Authorization : pengguna diperbolehkan menghapus relasi yang sudah ada.

Contoh perintah menggunakan sql :

1. GRANT : memberikan wewenang kepada pemakai
   Syntax : GRANT <priviledge list> ON <nama relasi/view> TO <pemakai>
   Contoh :
   GRANT SELECT ON S TO BUDI
   GRANT SELECT,UPDATE (STATUS,KOTA) ON S TO ALI,BUDI
2. REVOKE : mencabut wewenang yang dimiliki oleh pemakai
   Syntax : REVOKE <priviledge list> ON <nama relasi/view> FROM <pemakai>
   Contoh :
   REVOKE SELECT ON S FROM BUDI
   REVOKE SELECT,UPDATE (STATUS,KOTA) ON S FROM ALI,BUDI
   Priviledge list : READ, INSERT, DROP, DELETE, INDEX, ALTERATION,
3. RESOURCE

c. Backup data dan recovery :

Backup adalah proses secara periodik untuk mebuat duplikat dari database dan melakukan logging file (atau program) ke media penyimpanan eksternal. Proses menyimpan dan mengatur log file dari semua perubahan yang dibuat di database untuk proses recovery yang efektif jika terjadi kesalahan.

Recovery merupakan upaya uantuk mengembalikan basis data ke keadaaan yang dianggap benar setelah terjadinya suatu kegagalan.

Jenis pemulihan terhadap database, yaitu :

1. Pemulihan terhadap kegagalan transaksi : Kesatuan prosedur alam program yang dapat mengubah / memperbarui data pada sejumlah tabel.
2. Pemulihan terhadap kegagalan media : Pemulihan karena kegagalan media dengan cara mengambil atau memuat kembali salinan basis data (backup).
3. Pemulihan terhadap kegagalan sistem : Karena gangguan sistem, hang, listrik terputus alirannya.

Fasilitas pemulihan pada DBMS :

1. Mekanisme backup secara periodik
2. Fasilitas logging dengan membuat track pada tempatnya saat transaksi berlangsung dan pada saat database berubah.
3. Fasilitas checkpoint, melakukan update database yang terbaru.
4. Manager pemulihan, memperbolehkan sistem untuk menyimpan ulang database menjadi lebih konsisten setelah terjadinya kesalahan.

Teknik pemulihan terhadap database, yaitu :

1. defered upate / perubahan yang ditunda : perubahan pada DB tidak akan berlangsung sampai transaksi ada pada poin disetujui (COMMIT). Jika terjadi kegagalan maka tidak akan terjadi perubahan, tetapi diperlukan operasi redo untuk mencegah akibat dari kegagalan tersebut.
2. Immediate Upadate / perubahan langsung : perubahan pada DB akan segera tanpa harus menunggu sebuah transaksi tersebut disetujui. Jika terjadi kegagalan diperlukan operasi UNDO untuk melihat apakah ada transaksi yang telah disetujui sebelum terjadi kegagalan.
3. Shadow Paging : menggunakan page bayangan imana paa prosesnya terdiri dari 2 tabel yang sama, yang satu menjadi tabel transaksi dan yang lain digunakan sebagai cadangan. Ketika transaksi mulai berlangsung kedua tabel ini sama dan selama berlangsung tabel transaksi yang menyimpan semua perubahan ke database, tabel bayangan akan digunakan jika terjadi kesalahan. Keuntungannya adalah tidak membutuhkan REDO atau UNDO, kelemahannya membuat terjadinya fragmentasi.[21]

Kesatuan Data dan Enkripsi

Enkripsi yaitu keamanan data

Integritas yaitu metode pemeriksaan dan validasi data(metode integrity constrain), yaitu berisi aturanaturan atau batasan-batasan untuk tujuanterlaksananya integritas data.

Konkuren yaitu mekanisme untuk menjamin bahwatransaksi yang konkuren pada database multi usertidak saling menganggu operasinya masing-masing.Adanya penjadwalan proses yang akurat (timestamping)**.**

e. Tujuan keamanan database

1. Secrecy/confidentialy : informasi tidak boleh diungkapkan kepada pengguna yang tidak sah. Sebagai contoh mahasiswa seharusnya tidak diperbolehkan untuk memeriksa nilai siswa lainnya.
2. Integrity : hanya pengguna yang berwenang harus diizinkan untuk memodifikasi data. Sebagai contoh siswa mungkin diperolehkan untuk melihat nilai mereka, namun tidak diperbolehkan untuk memodifikasi mereka.
3. Avaibility : pengguna yang terdaftar tidak boleh ditolak akses. Sebagai contoh seorang instruktur yang ingin mengubah kelas harus diizinkan untuk melakukannya.

Fasilitas Keamanan Database

Keamanan database tersedia pada versi Educator ke atas. Keamanan database diatur oleh Properti Database. Berikut ini adalah properti database yang digunakan untuk keamanan database *BOCSoft eQuestion.*

Soal

1. Apa yang di maksud dengan keamanan database?
2. Jelaskan mengenai tujuan keamanan database!