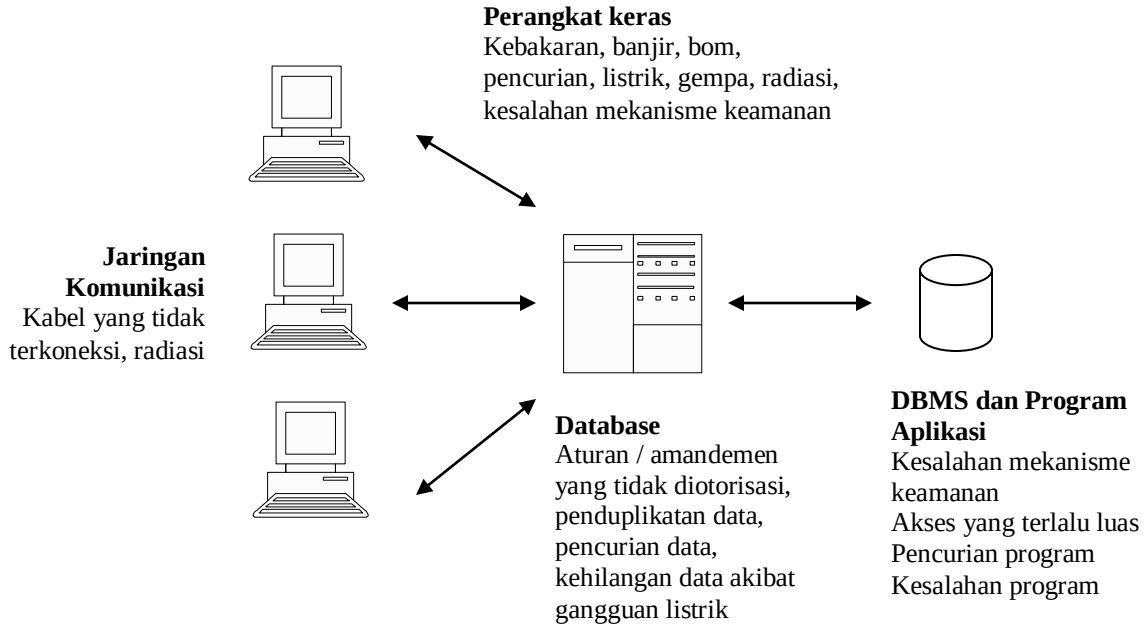
KEAMANAN DATABASE

Keamanan merupakan suatu proteksi terhadap pengrusakan data dan pemakaian data oleh pemakai yang tidak punya kewenangan.
Untuk menjaga keamanan Basis Data dgn :
(1) Penentuan perangkat lunak Data Base Server yang handal.
(2) Pemberian Otoritas kepada user mana saja yang berhak mengakses, serta memanipulasi data-data yang ada.



Pengguna Akhir
- Menggunakan hak akses orang lain.
- Melihat & menutup data yang tidak diotorisasi
- Staf tidak di-training
- Pemasukan data yang dilakukan oleh yang tidak berhak.
- Virus
- pemerasan

Programmer / Operator
- Membuat Password.
- Membuat program yang tidak aman
- Staf yang tidak di-training.
- Kebijakan keamanan & prosedur
- Pemogokan staf

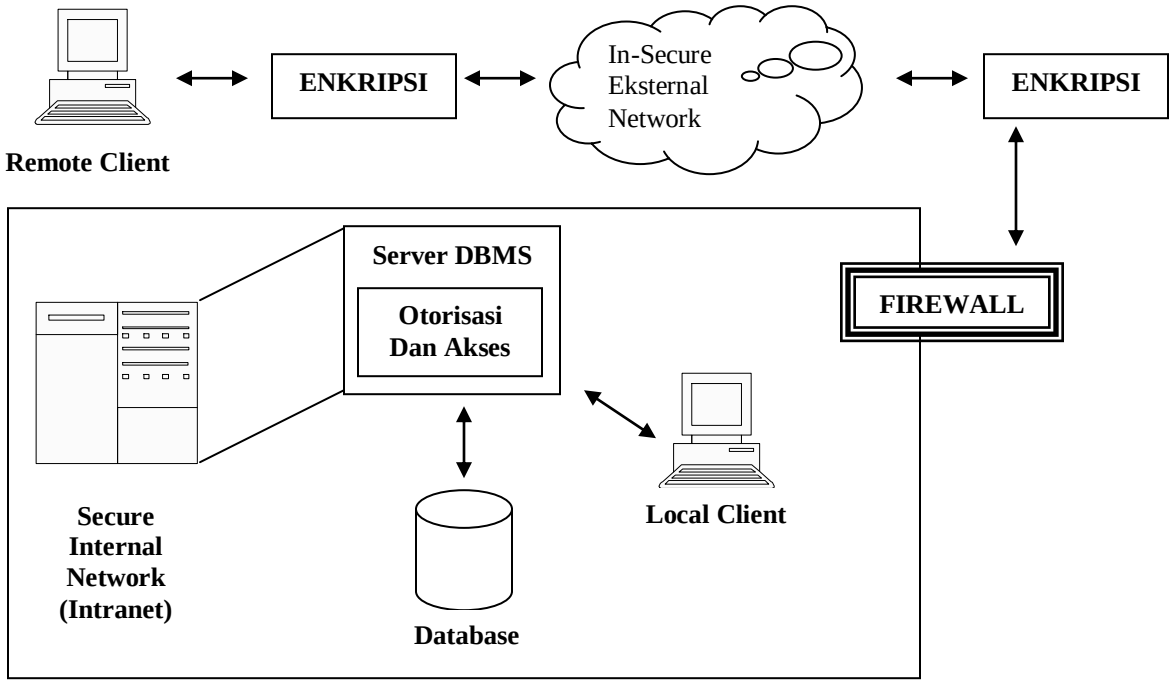
Database Administrator
- Kebijakan keamanan & prosedur

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 :

- Pemberian Wewenang atau hak istimewa (priviledge) untuk mengakses sistem atau obyek database
- 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 → 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 :

  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

  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, RESOURCE

3. Backup data dan recovery :

Backup : proses secara periodik untuk mebuat duplikat ari database dan melakukan logging file (atau program) ke media penyimpanan eksternal.

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

3 Jenis Pemulihan :

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 :

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 Upadte / 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.

4. Kesatuan data dan Enkripsi :

- Enkripsi : keamanan data
- Integritas :metode pemeriksaan dan validasi data (metode integrity constrain), yaitu berisi aturan-aturan atau batasan-batasan untuk tujuan terlaksananya integritas data.
- Konkuren : mekanisme untuk menjamin bahwa transaksi yang konkuren pada database multi user tidak saling menganggu operasinya masing-masing. Adanya penjadwalan proses yang akurat (time stamping).