KEAMANAN BASIS DATA PADA SISTEM INFORMASI DI ERA GLOBAL

Gatot Susilo[1]
[1]Program Studi Sistem Informasi, STMIK Bina Patria Magelang
Jl. Raden Saleh No. 2, Magelang
E-Mail : b199h05t@gmail.com[1]

Abstract

The development of information and communication technology provides an enormous impact in most institutions, both private and government ones. One of its impacts is the utilization of information system to support operational works, and most importantly, to generate information used by various levels of management. Database implementation has long been a part of the information system in running the business, with the objectives of assisting people and organizations to discover certain issues. It indicates that database has a pivotal role in an organization, thus, its security must be seriously watched. Threats towards database may bring impacts on the reducing of data integrity, data availability, and data confidentiality. Countermeasures against database security threats in multiuser environment can be classified into 2 main items, i.e. physical control on its computer system and its administrative procedure. If an incident happens on the information system, particularly related to the database security, several phases of handling need to be conducted, they are: preparation, identification, containment, eradication, recovery, and follow-up phases.

Keywords : *Database, Database Security, Countermeasures on Database Security Threats.*

Abstrak

Perkembangan teknologi informasi dan komunikasi memberikan dampak yang sangat besar pada hampir semua institusi, baik swasta maupun pemerintah. Salah satu dampaknya adalah penggunaan sistem informasi untuk membantu pekerjaan operasional dan yang paling penting adalah untuk menghasilkan informasi yang digunakan oleh berbagai level manajemen. Implementasi database sudah lama menjadi bagian dari sistem informasi dalam menjalankan bisnis, dengan tujuan membantu orang dan organisasi menelusuri hal-hal tertentu. Hal ini menunjukkan bahwa database memiliki peran penting dalam organisasi, sehingga sangat perlu diperhatikan dari sisi keamanannya. Ancaman pada database dapat berdampak pada berkurangnya integritas data, ketersediaan data dan kerahasiaan data. Penanggulangan terhadap ancaman keamanan basis data dalam lingkungan *multi user* dapat dikelompokkan pada 2 hal utama, yaitu kontrol secara fisik sistem komputernya dan prosedur administrasinya. Apabila terjadi insiden terhadap sistem

informasi, terutama yang berkaitan dengan dengan keamanan basis data, maka perlu dilakukan tahap - tahap penanganan meliputi : tahap persiapan *(Preparation),* identifikasi, *containment*, pemberantasan, pemulihan, tindak lanjut

Kata kunci : Basis data *(database),* keamanan basis data, penanggulangan ancaman keamanan basis data.

1. Pendahuluan

Saat ini, dapat dikatakan hampir semua institusi swasta, pemerintah ataupun perusahaan telah menggunakan sistem informasi untuk dapat menghasilkan informasi yang digunakan oleh berbagai level manajemen. Berbagai istilah, seperti data, data base, informasi dan sistem informasi muncul. Aplikasi dalam organisasi, aplikasi *client - server*, aplikasi *e-Commerce*, aplikasi *e-bussines* merupakan fungsi utama dari basis data. Tujuan basis data adalah membantu orang dan organisasi menelusuri hal-hal tertentu.

Database (dan khususnya SQL) telah lama menjadi bagian integral dari sistem dalam menjalankan bisnis, baik dalam bentuk awalnya, yaitu *file database* biasa maupun dalam bentuk sekarang ini,yaitu database yang berorientasi pada tingkat lanjut. Kebutuhan atas penyimpanan dan pengaksesan informasi secara cepat menjadi hal-hal yang mendesak bagi tiap bisnis atau aplikasi, begitu pula *web*. Aplikasi-aplikasi *web* sekarang ini berpasangan dengan database. Database dipakai untuk beragam kegunaan mulai dari menyimpan nama-nama *user* dan *password-pasword* untuk akses resmi, sampai untuk menyimpan alamat-alamat *e-mail user*, dan informasi kartu kredit untuk mempermudah pengiriman produk dan pembayarannya. Oleh karena itu, pemahaman menyeluruh mengenai keamanan *web* harus mencakup juga lapisan databasenya dan terpenting memahami juga bagaimana penyusup berusaha memasuki aplikasi untuk memperoleh akses ke bagian-bagian datanya (GCSIRT dan BPPT :19:2014).

2. Landasan Teori

Pada basis data *(database)*, terdapat istilah dasar yang disebut dengan data. Data adalah fakta-fakta mentah yang dapat mewakili kejadian-kejadian yang berlangsung dalam organisasi atau lingkungan fisik sebelum ditata dan diatur ke dalam bentuk yang dapat dipahami dan digunakan orang (Laudon dan Laudon, 1998). Data juga didefinisikan sebagai fakta, angka, bahkan simbol mentah, secara bersama-sama merupakan masukan bagi suatu sistem informasi (Wilkinson, 1992).

Istilah yang seringkali rancu dengan data adalah informasi. Walaupun demikian, perbedaan kedua istilah tersebut perlu dijelaskan. Informasi adalah data yang telah diolah menjadi bentuk yang lebih bermakna dan berguna bagi manusia (Laudon dan Laudon, 1998). Informasi juga

didefinisikan data yang telah diproses sedemikian rupa sehingga meningkatkan pengetahuan seseorang yang menggunakannya (Hoffer, dkk, 2005).

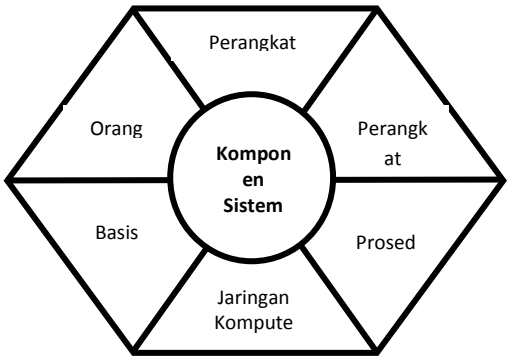
Sebuah database adalah sekumpulan record yang saling berhubungan yang menggambarkan dirinya sendiri. Untuk semua database relasional (hampir semua database yang ada sekarang), kita dapat memodifikasi definisi ini dengan mengatakan sebuah database adalah sekumpulan tabel yang berhubungan yang menggambarkan dirinya sendiri (Kroenke :10:2005).

A database is a collection of data, typically describing the activities of one or more related organizations. For example, a university database might contain information about the following: Entities such as students, faculty, courses, and classrooms. Relationships between entities, such as students' enrollment in courses, faculty teaching courses, and the use of rooms for courses (Raghu R.:3:2010).

Ada beragam pengertian sistem informasi. Turban, McLean dan Wetherbe (1999), mendefinisikan sebuah sistem informasi mengumpulkan, memproses, menyimpan, menganalisis dan menyebarkan informasi untuk tujuan yang spesifik. Sedangkan Hall (2001), mendefinisikan sistem informasi sebagai sebuah rangkaian prosedur formal di mana data dikelompokkan, dproses menjadi informasi dan disitribusikan kepada pemakai.

Menurut Abdul Kadir (2014), komponen-komponen yang dikandung oleh sistem informasi, antara lain :

a. Perangkat keras *(hardware)*, yang mencakup peranti fisik seperti komputer dan printer.
b. Perangkat lunak *(software)* atau program, yaitu sekumpulan instruksi yang memungkinkan perangkat keras memproses data.
c. Prosedur, yaitu sekumpulan aturan yang dipakai untuk mewujudkan pemrosesan data dan pembangkitan keluaran yang dikehendaki.
d. Orang, yaitu semua pihak yang bertanggung jawab dalam pengembangan sistem informasi, pemrosesan dan penggunaan keluaran sistem informasi.
e. Basis data *(database)*, yaitu sekumpulan tabel, hubungan dan lain-lain yang berkaitan dengan penyimpanan data.
f. Jaringan komputer dan komunikasi data, yaitu sistem penghubung yang memungkinkan sumber *(resources)* dipakai secara bersama atau diakses oleh sejumlah orang.



Gambar 1. Komponen Sistem Informasi (Abdul Kadir :72:2014)

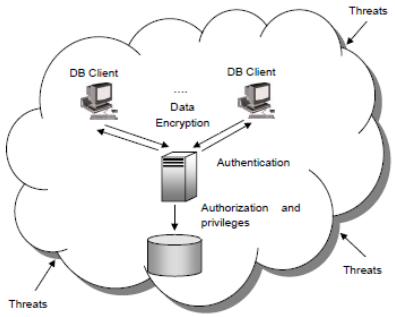
3. Pembahasan

a. Keamanan *Database*

Perkembangan organisasi / perusahaan mempunyai dampak pada bertambahnya volume data yang harus disimpan mengenai segala aspek kegiatan operasionalnya. Data-data tersebut dapat digunakan oleh organisasi untuk dijadikan dasar dalam pengambilan keputusan yang penting. Hal ini menunjukkan bahwa data-data tersebut mempunyai peran yang sangat penting bagi organisasi, sehingga perlu diperhatikan dari sisi keamanannya. Berdasarkan alasan ini pula, setiap personil dalam sebuah organisasi harus peka terhadap ancaman keamanan dan mengambil tindakan-tindakan untuk melindungi data pada organisasi mereka.

Masalah keamanan data sangatlah komplek. Seringkali masalah keamanan data dapat melibatkan aspek hukum, sosial atau etika, kebijakan yang berhubungan dengan pelaksanaan atau terkait dengan pengendalian peralatan secara fisik. Keamanan *database* berkaitan dengan perlindungan terhadap *database* terhadap ancaman yang disengaja atau tidak disengaja, dengan menggunakan elemen kontrol peralatan komputasi atau yang tidak.

Analisis untuk keamanan *database* (basis data) tidak hanya cukup pada layanan yang disediakan oleh DBMS, tetapi juga mencakup masalah-masalah yang terkait dengan *database* dan keamanan lingkungannya. Pertimbangan keamanan tidak hanya berlaku untuk data yang terdapat dalam database saja, karena kesenjangan keamanan pada bagian lain dapat mempengaruhi sistem, yang pada gilirannya dapat mempengaruhi keamanan *database*. Sehingga, dengan berfokus pada keamanan *database* saja tidak akan menjamin bahwa *database* akan aman. Semua bagian dari sistem harus aman, antara lain : *database*, jaringan, sistem operasi, bangunan di mana *database* berada secara fisik dan orang-orang yang memiliki kesempatan untuk mengakses sistem.



Gambar 2. Keamanan *Database* (Sharma, dkk :222:2010)

Ancaman terhadap database dapat mengakibatkan berkurangnya atau bahkan hilangnya tujuan dari keamanan database, yaitu menjamin : integritas data, ketersediaan data, dan kerahasiaan data. (Elmasri & Navathe : 836: 2011)

1) Hilangnya integritas, mengacu pada kebutuhan informasi yang dilindungi dari modifikasi yang tidak benar. Modifikasi data meliputi penciptaan,

penyisipan, update, mengubah status data, dan penghapusan.

2) Kehilangan ketersediaan data mengacu pada penyediaan informasi untuk pengguna yang memiliki hak akses yang sah.
3) Kehilangan kerahasiaan. Kerahasiaan database mengacu pada perlindungan data dari pengungkapan yang tidak sah.

Menurut GCSIRT dan BPPT (6:2014), penyebab adanya gangguan dari database bisa berasal dari dalam sistem komputer maupun dari manusia sebagai pengguna sistem komputer. Dari dalam sistem komputer yang digunakan, penyebabnya bisa berasal dari :

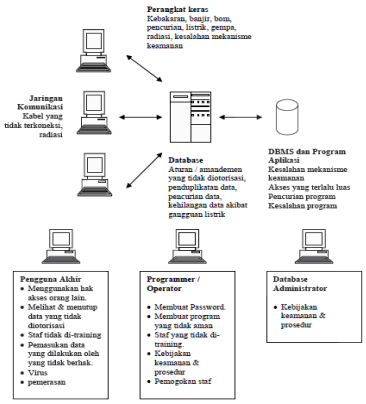
a. *Malware* yang menyerang sistem komputer.
   Malware yang menyerang pada sistem dan jaringan komputer bisa menyebabkan juga terjadinya gangguan pada *server* database. Gangguan yang ditimbulkan bisa berupa terganggunya akses terhadap layanan data dan bahkan bisa merusak data-data pada komputer maupun *server* database. Hal- hal berikut bisa menjadi ciri-ciri terjadinya gangguan akses terhadap database yang disebabkan oleh *malware*, antara lain :
   1) Anti virus tidak berfungsi seperti yang diharapkan;
   2) Kegagalan membuka utilitas sistem pada sisi *client;*
   3) Lambatnya Respon CPU;
   4) Sistem / Aplikasi *crash*.

b. Gangguan sistem jaringan komputer.
   Salah satu faktor penting dari keamanan database adalah ketersediaan dari database itu sendiri. Saat ini, hampir semua database ditempatkan pada mesin khusus yang berupa *server* database. Untuk mengakses data-data dalam database, bisa dilakukan dengan menggunakan model *client server*. Pada model *client server*, peranan dari jaringan komputer sangatlah penting. Gangguan keamanan pada jaringan komputer bias mengakibatkan gangguan pada layanan database. Pengamatan pertama yang bisa dilihat pada gangguan adalah lamanya waktu yang dibutuhkan untuk mengakses *server* database, bahkan koneksi terhadap database bisa terputus. Gangguan lain pada sistem jaringan adalah terdapatnya proses pemindaian dan *capture* data-pada yang keluar masuk pada *server* database. Proses ini bisa terdeteksi dengan menggunakan tool IDS berbasis *host* pada *server*, maupun IDS berbasis jaringan. Identifikasi bisa dilakukan dengan melakukan pemeriksaan pada log dari IDS tersebut. Disamping memasang IDS, tool lainnya yang bisa digunakan adalah *snort, TCPdump, ettercap*.

c. Kerentanan aplikasi database yang digunakan.
   Konfigurasi dan manajemen *patch* adalah pendekatan prinsip untuk memperbaiki kelemahan dari sistem basis data. Fitur-fitur default dari aplikasi pembangun database harus diubah. Identifikasi dapat dilakukan dengan melihat *patch* yang pernah dilakukan dan memeriksa fitur-fitur default dari sistem aplikasi database.

d. Kerentanan kode / program
Kerentanan kode-kode (program) yang digunakan untuk mengakses database, dapat dimanfaatkan oleh penyerang untuk menembus sistem keamanan dari database. Kode-kode itu meliputi kode-kode SQL maupun kode-kode yang digunakan untuk membangun aplikasi dari sistem database. Pemeriksaan terhadap kode-kode itu bisa dilakukan untuk mengidentifikasi dari adanya gangguan keamanan pada database. Contoh dari serangan pada rentannya kode-kode adalah *SQL Injection*, *buffer overflow*, *cross site scripting*.

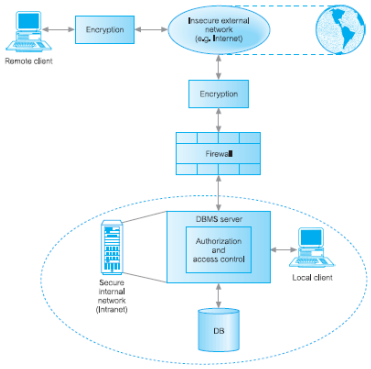
e. Kelalaian pengguna database.
Apabila tidak ditemukannya adanya tanda-tanda bahwa penyebabnya berasal pada sistem komputer, maka identifikasi harus diarahkan kepada para pengguna sistem komputer. Beberapa perilaku dari pengguna komputer yang bisa membahayakan keamanan data, antara lain:
   1) Penggunaan *password* yang sembarangan.
      Kerahasiaan *password* yang tidak terjaga dengan baik, bisa mengakibatkan *password* jatuh ke pihak yang tidak diinginkan. Akibatnya adalah pihak-pihak yang tidak memiliki akses ke dalam database dapat mengakses database tersebut. Dengan demikian maka pihak tersebut akan dengan mudah menguasai database.
   2) Lupa melakukan *log off* dari sistem komputer.
      Kealpaan dalam melakukan *log off* pada sistem komputer dapat dimanfaatkan oleh pihak lain untuk mengambil dan bahkan menghapus data-data penting yang terdapat pada sistem komputer. Identifikasi dari kasus ini bisa berupa ditolaknya akses ke dalam database (*record* telah diubah atau dihapus), padahal tidak ditemukannya gejala *malware*, gangguan pada sistem jaringan komputer, dan kerentanan kode- kode SQL dan program aplikasi database yang digunakan. Sedangkan pada kasus tercurinya database, identifikasi sulit dilakukan, karena dampak dari pencurian database tidak bisa dirasakan secara langsung. Pemilik data baru menyadari bahwa data-data telah tercuri apabila pihak pencuri telah melakukan ekspose terhadap data-data yang telah dicuri tersebut. Pada tahap identifikasi ini, disamping melakukan identifikasi untuk mengetahui penyebab terganggunya sistem database, juga dilakukan identifikasi terhadap penting atau tidaknya data / informasi yang telah mengalami gangguan. Hal itu dilakukan untuk melihat dampak yang diakibatkan oleh terganggunya data / informasi yang memiliki tingkat kerahasiaan tinggi.



Gambar 3. *Summary of potential threats to computer systems* (Connolly&Begg:545:2005)

b. Metode Penanggulangan Terhadap Ancaman Dalam Keamanan Basis Data

Menurut Connolly dan Begg (545: 2005), jenis penanggulangan terhadap ancaman keamanan database yang digunakan pada lingkungan *multi user* dapat difokuskan pada 2 hal, yaitu kontrol secara fisik sistem komputernya dan prosedur administrasi.



Gambar 4. Representation of a typical multi-user computer environment (Connolly&Begg:546:2005)

Kontrol keamanan basis data berbasis komputer pada lingkungan *multi user* dapat dilakukan dengan beberapa cara, antara lain :

1. *Authorization*
   Yaitu pemberian wewenang atau hak istimewa *(priviledge)* untuk mengakses sistem atau obyek database. Kendali otorisasi dapat dibangun pada perangkat lunak dengan 2 fungsi, yaitu : mengendalikan sistem atau obyek yang dapat diakses dan mengendalikan bagaimana pengguna menggunakannya. Dalam hal ini, seorang sistem administrasi yang bertanggung jawab untuk memberikan hak akses dengan membuat *account* pengguna.
2. *Access Controls*
   Kontrol akses merupakan teknik keamanan yang dirancang untuk mengatur siapa atau jadi apa dan apa yang dilakukan pada penggunaan sumber daya dalam lingkungan komputasi. Penggunaan kontrol akses yang benar membutuhkan kolaborasi antara sistem administrator dan pengembang database.
3. *Views*
   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.

4. *Backup And Recovery*
   Backup adalah proses secara periodik untuk mebuat duplikat dari database dan melakukan *logging file* (atau program) ke media penyimpanan eksternal. Sedang *recovery* merupakan upaya untuk mengembalikan basis data ke keadaaan yang dianggap benar setelah terjadinya suatu kegagalan. Terdapat 3 jenis pemulihan pada saat terjadi kegagalan, antara lain :
   a) Pemulihan terhadap kegagalan transaksi, yaitu kesatuan prosedur dalam program yang dapat mengubah atau memperbarui data pada sejumlah tabel.
   b) Pemulihan terhadap kegagalan media, yaitu pemulihan karena kegagalan media dengan cara mengambil atau memuat kembali salinan basis data *(backup).*
   c) Pemulihan terhadap kegagalan system, yaitu pemulihan yang dilakukan karena adanya gangguan sistem, hang, listrik terputus alirannya.
5. *Integrity*
   Integritas juga memberikan kontribusi dalam menjaga keamanan database, guna menjaga data tetap valid, sehingga sistem informasi dapat memberikan informasi yang benar dan akurat.
6. *Encryption*
   Untuk melakukan pencegahan terhadap kemungkinan ancaman dari luar *(eksternal)*, maka dipandang perlu dilakukan *encode* terhadap data-data yang bersifat sensitif. Saat ini, beberapa DBMS telah menyediakan fasilitas untuk melakukan *encoding* (enkripsi). DBMS dapat mengakses data setelah dilakukan *decoding* terlebih dahulu terhadap data. Metode enkripsi dapat membantu dalam keamanan database, meskipun ada penurunan kinerja karena penambahan waktu yang digunakan untuk memecahkan kode enkripsi.
7. *Redundant Array of Independent Disks* (RAID) *technology*
   Perangkat keras yang bekerja pada DBMS harus dapat berjalan dengan toleran, artinya DBMS harus terus beroperasi bahkan jika salah satu komponen *hardware* mengalami kegagalan. Komponen *hardware* yang harus dapat berjalan dengan toleran antara lain *disk drive*, kontroler *disk*, CPU, pasokan listrik dan kipas pendingin. Diantara semua *hardware* tersebut, *disk drive* mempunyai tingkat kerentanan yang paling tinggi. Solusi untuk mengatasi hal tersebut adalah penggunaan *Redundant*

Array of Independent Disks (RAID) *technology*. RAID *technology* menggabungkan beberapa *hard disk* fisik ke dalam sebuah unit logis penyimpanan, dengan menggunakan perangkat lunak atau perangkat keras khusus.

c. Penanganan Terhadap Insiden Dalam Keamanan Basis Data

Penanganan suatu insiden ditujukan untuk mencapai hal-hal sebagai berikut (GCSIRT dan BPPT :4:2014) :

1) Mengumpulkan informasi sebanyak mungkin tentang sifat insiden;
2) Menghalangi atau mencegah eskalasi kerusakan yang disebabkan oleh insiden tersebut, jika mungkin;
3) Memperbaiki kerusakan yang disebabkan oleh insiden tersebut;
4) Mengumpulkan bukti insiden itu, yang sesuai;
5) Memulihkan layanan sesegera mungkin;
6) Mengambil langkah - langkah proaktif untuk mengurangi insiden masa depan.

Supaya tujuan di atas dapat terlaksana dengan baik, maka perlu ditentukan tahap - tahap untuk melakukan penanganan terhadap insiden yang terjadi. Tahap – tahap tersebut dapat digambarkan sebagai berikut (GCSIRT dan BPPT :4:2014) :

1) Tahap Persiapan *(Preparation)*
   Langkah-langkah yang harus diambilpada tahap ini adalah : Penyiapan Personil (orang), Dokumen Kebijakan dan Prosedur
2) Tahap Identifikasi
   Tahap ini adalah tahap di mana penelusuran terhadap insiden yang terjadi pada data / database organisasi mulai diidentifikasi.
3) Tahap *Containment*
   tahap ini akan dilakukan pencegahan lebih lanjut terhadap kerusakan atau kebocoran lebih lanjut dari data - data penting / rahasia dari organisasi.
4) Tahap Pemberantasan
   Tahap ini merupakan tahapan untuk melakukan pemberantasan terhadap penyebab dari terjadinya insiden pada data / database.
5) Tahap Pemulihan
   Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula.
6) Tahap Tindak Lanjut
   Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk dimasa mendatang. Fase ini dapat memberikan masukan kepada tahap persiapan untuk meningkatkan pertahanan.

4. Kesimpulan

Basis data dalam sebuah perusahaan / organisasi mempunyai peran dan manfaat yang sangat besar sekali. Basis data dapat digunakan sebagai dasar pada proses pengambilan

keputusan yang penting. Peran dan manfaat yang sangat besar dari basis data juga harus diikuti dengan keamanan terhadap basis data tersebut. Keamanan basis data harus mendapatkan perhatian khusus, karena saat basis data kehilangan integritas data, ketersediaan data, dan kerahasiaan data, maka akan berdampak pada berkurangnya atau bahkan hilangnya tujuan dari keberadaan basis data itu sendiri.

5. Referensi

Abdul Kadir, 2014, *Pengenalan Sistem Informasi ; Edisi Revisi*, Andi Offset, Yogyakarta.

Connolly, Thomas & Begg, Carolyn, 2005, *Database Systems : A Practical Approach To Design, Implementation and Management 4Th Edition*, Pearson Education, Publishing as Addison Wesley.

Elmasri, Ramez; Navathe, Shamkant, 2011, *Fundamental Of Database Systems 6th Edition*, Pearson Education, Publishing as Addison Wesley.

Government Computer Security Incident Response Team (GCSIRT) dan BPPT, 2014, *Panduan Penanganan Insiden Keamanan Database*, BPPT & CSIRT, Kemenkominfo Republik Indonesia.

Hall, J. A, 2001, *Accounting Information Systems, 3rd Editon*, South Western College Publishing.

Hoffer, Jeffre A., Prescott, Mary B., McFadden, Fred R., 2005, *Modern Database Management,* New Jersey: Pearson Education, Inc.

Kroenke, David M., 2005, *Dasar-dasar Desain, dan Implementasi Database Processing, Jilid I*, Penerbit Erlangga.

Laudon, Kenneth C. Laudon, Jane, P., 1998, *Management Information Systems New Approaches to Organization & Technology*, New Jersey : Prentice Hall, Inc.

Raghu Ramakrishnan, Johannes Gehrke, 2010, *Database Management Systems, Second Edition*, _____.

Sharma N., Perniu L., Chong R., et.al, 2010, *Database Fundamentals : Ideal for application developers and administrators*, IBM Corporation, Canada.

Turban, E; McLean, E; Wetherbe, J., 1999, *Information Technology for Management Making Connections ofr Strategis Advantage, 2nd Edition*, John Wiley & Sons, Inc.

Wilkinson, Joseph W., 1992, *Accounting and Information System*, John Wiley & Sons, Inc.