# *PERTEMUAN 12*

# Keamanan dan Administrasi Database

***(Chap. 20 – Conolly)***

# Keamanan *Database*

**Keamanan *Database*** : Mekanisme yang melindungi *database* terhadap ancaman disengaja atau tidak disengaja.

Keamanan database dalam kaitannya dengan situasi berikut:

1. pencurian dan penipuan;
2. hilangnya kerahasiaan;
3. hilangnya privasi;
4. hilangnya integritas;
5. hilangnya ketersediaan.

**Ancaman**

- **Ancaman :** Setiap situasi atau peristiwa, baik disengaja atau tidak disengaja, yang bisa mempengaruhi sistem dan akibatnya organisasi.

**TABEL** Contoh ancaman.

**TABLE 20.1** Examples of threats.

| THREAT | THEFT AND FRAUD | LOSS OF CONFIDENTIALITY | LOSS OF PRIVACY | LOSS OF INTEGRITY | LOSS OF AVAILABILITY |
|---|---|---|---|---|---|
| Using another person's means of access | ✓ | ✓ | ✓ | | |
| Unauthorized amendment or copying of data | ✓ | | | ✓ | |
| Program alteration | ✓ | | | ✓ | ✓ |
| Inadequate policies and procedures that allow a mix of confidential and normal output | ✓ | ✓ | ✓ | | |
| Wire tapping | ✓ | ✓ | ✓ | | |
| Illegal entry by hacker | ✓ | ✓ | ✓ | | |
| Blackmail | ✓ | ✓ | ✓ | | |
| Creating "trapdoor" into system | ✓ | ✓ | ✓ | | |
| Theft of data, programs, and equipment | ✓ | ✓ | ✓ | | ✓ |
| Failure of security mechanisms, giving greater access than normal | | ✓ | ✓ | ✓ | |
| Staff shortages or strikes | | | | ✓ | ✓ |
| Inadequate staff training | | ✓ | ✓ | ✓ | ✓ |
| Viewing and disclosing unauthorized data | ✓ | ✓ | ✓ | | |
| Electronic interference and radiation | | | | ✓ | ✓ |
| Data corruption owing to power loss or surge | | | | ✓ | ✓ |
| Fire (electrical fault, lightning strike, arson), flood, bomb | | | | ✓ | ✓ |
| Physical damage to equipment | | | | ✓ | ✓ |
| Breaking cables or disconnection of cables | | | | ✓ | ✓ |
| Introduction of viruses | | | | ✓ | ✓ |

**Gambar** Ringkasan potensi ancaman sistem komputer.

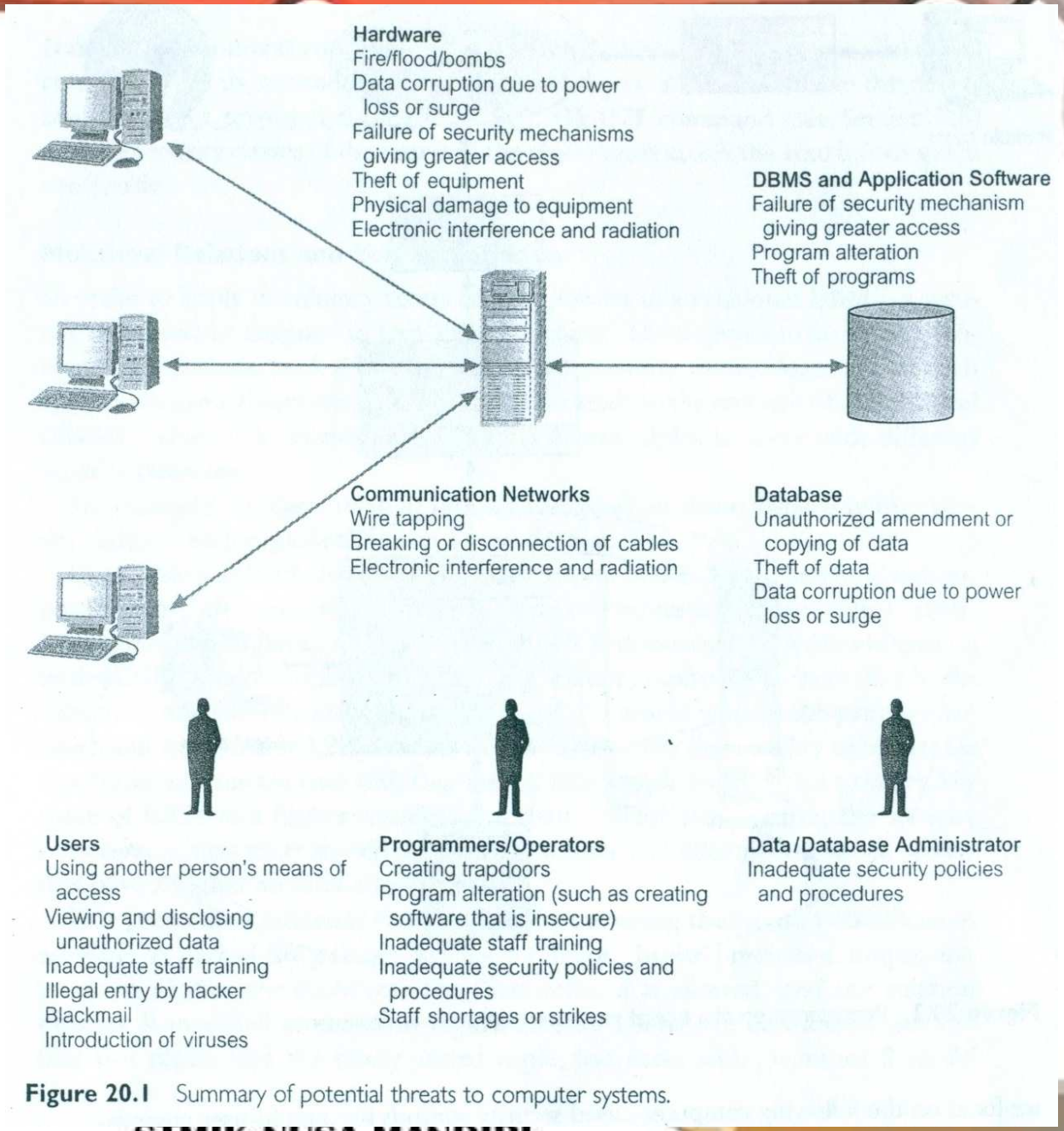



**Figure 20.1** Summary of potential threats to computer systems.

# Penanggulangan-Komputer Berbasis Kontrol

Keamanan untuk lingkungan *multi-user* (beberapa di antaranya mungkin tidak tersedia di lingkungan PC):

1. Otorisasi dan otentikasi

**Otorisasi :**

Pemberian hak atau hak istimewa yang memungkinkan subjek untukmemiliki akses yang sah ke sistem atau objek sistem

**Otentikasi :**

Sebuah mekanisme yang menentukan apakah seorang pengguna bertanggung jawab untuk mengakses komputer dengan menciptakan *account* individu. Dimana setiap *user* diberikan pengenal unik, yang digunakan oleh sistem operasi untuk menentukan siapa mereka.

2. Akses kontrol : *DAC, MAC*

Akses kontrol untuk sistem *database* didasarkan pada pemberian dan pencabutan hak-hak istimewa. Sebuah **hak istimewa** memungkinkan pengguna untuk membuat atau akses (yaitu membaca, menulis, atau memodifikasi) beberapa objek *database* (seperti relasi, melihat,atau indeks) atau untuk menjalankan utilitas tertentu DBMS.

***Discretionary Access Control (DAC)***

DBMS yang paling komersial menyediakan pendekatan untuk mengelola hak istimewa yang menggunakan SQL *Discretionary Access Control disebut* (DAC). Standar SQL mendukung DAC melalui GRANT dan REVOKE perintah. Perintah GRANT memberikan hak istimewa kepada pengguna, dan perintah REVOKE menghapus hak istimewa.

***Mandatory Access Control (MAC)***

Dalam pendekatan ini setiap objek *database* diberikan sebuah keamanan kelas dan setiap pengguna diberikan izin untuk kelas keamanan, dan aturan dikenakan pada membaca dan menulis objek *database* oleh pengguna

3. *Views*,
adalah hasil dinamik dari satu atau lebih operasi relasional operasi pada relasi untuk menghasilkan relasi lainnya. View adalah relasi virtual yang tidak benar-benar ada dalam database, tetapi dihasilkan atas permintaanpengguna tertentu, pada saat ada nya permintaan.
Mekanisme Tampilannya menyediakan keamanan yang kuat dan fleksibel dengan menyembunyikan bagian-bagian dari database dari pengguna tertentu.

4. *Backup* dan Journal,
**Backup** : Proses periodik menyalin database dan file log (dan mungkin program) ke mediapenyimpanan offline.
**Journal :** Proses memelihara sebuah file log (atau jurnal) dari semua perubahan yang dibuat oleh database secara efektif .

5. Enkripsi,
Pengkodean data dengan algoritma khusus yang membuat data terbaca oleh program tanpa kunci dekripsi.
Beberapa DBMS menyediakan fasilitas enkripsi yang dapat mengakses data (setelah decoding itu),meskipun ada degradasi dalam performa karena waktu yang dibutuhkan untuk memecahkan kode tersebut . Enkripsi juga melindungi data yang dikirimkan melalui. jalur komunikasi.

6. RAID Teknologi.
RAID awalnya berdiri untuk *Redundant Array of Independent Disk.*
RAID bekerja pada sebuah array disk besar terdiri dari susunan beberapa disk yang diselenggarakan untuk meningkatkan kehandalan dan kinerja waktu pada tingkatan yang sama.

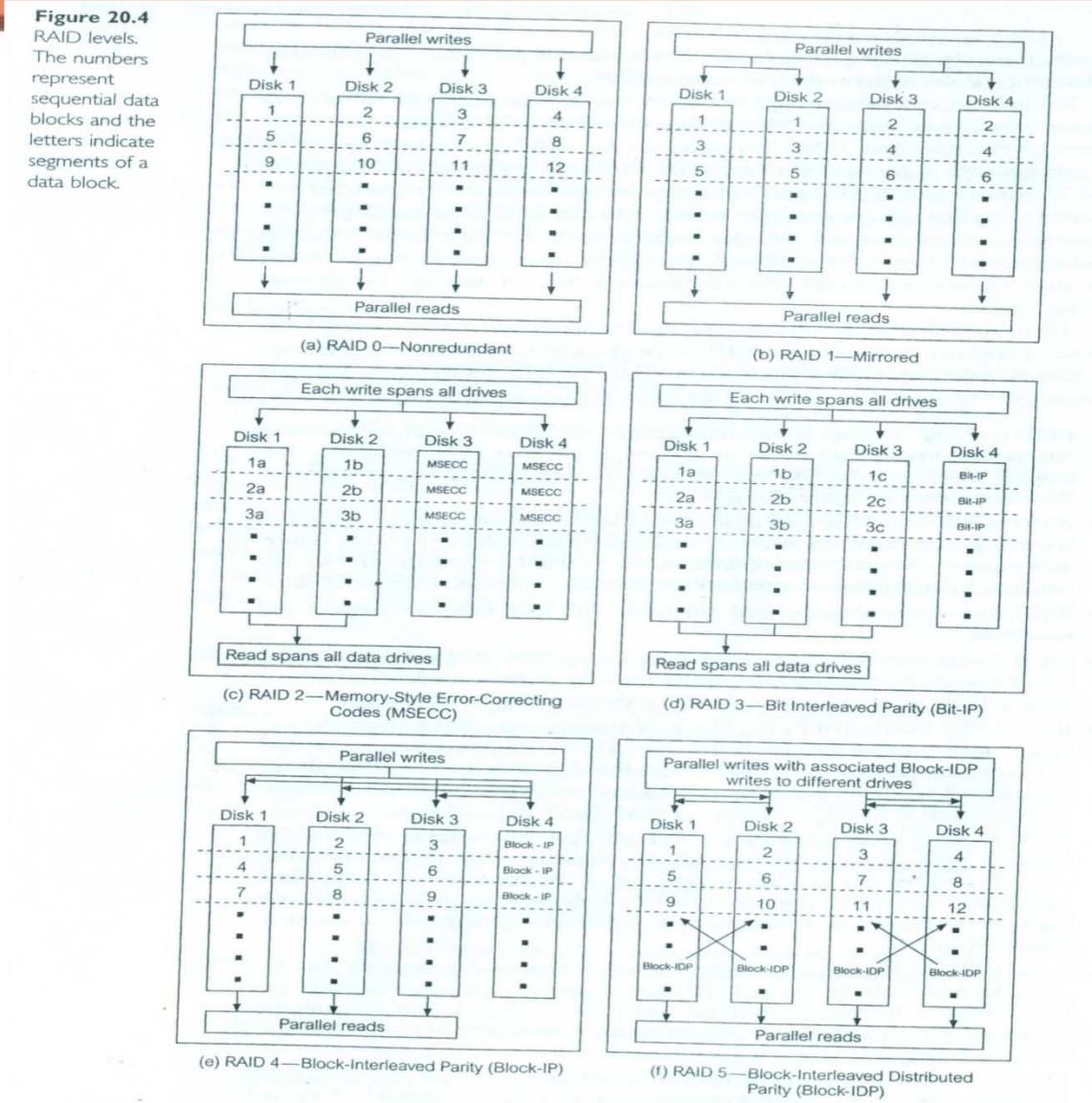



**Figure 20.4** RAID levels. The numbers represent sequential data blocks and the letters indicate segments of a data block.

RAID tingkat. Angka-angka mewakili blok sekuensial data dan surat-surat menunjukkan segmen blok data

# Keamanan di Microsoft Office Access DBMS

Microsoft Office Access menyediakan metode berikut untuk mengamankan database:

1. Memisahkan database;

   Cara yang paling aman untuk melindungi data dalam database adalah untuk menyimpan tabel database terpisah dari objek aplikasi database seperti formulirdan laporan. Tindakan ini disebut sebagai "pemisahan" database;

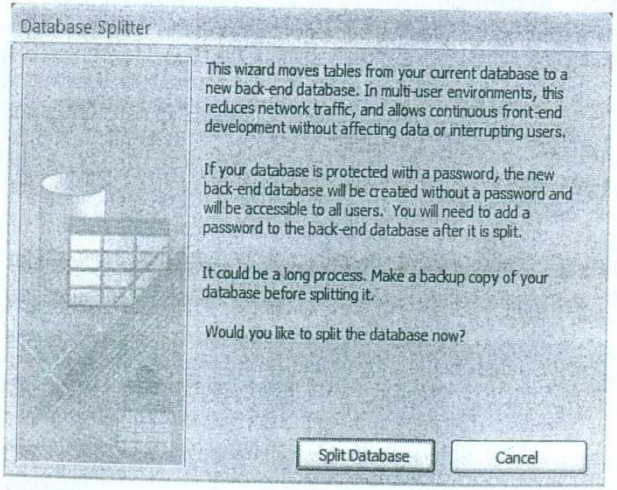



**Figure 20.5**
The Database Splitter Wizard window.

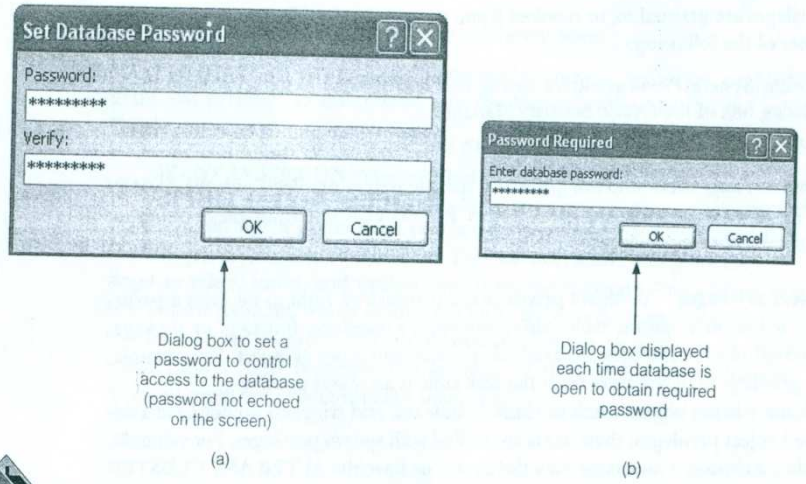



**Figure 20.6** Securing the *DreamHome* database using a password: (a) the Set Database Password dialog box; (b) the Password Required dialog box shown at startup.

2. Menetapkan password untuk database; Sebuah cara sederhana untuk mengamankan database adalah untuk menetapkan password untuk membuka database. Menyetel kata sandi tersedia melalui Enkripsikan dengan opsi Password di bagian database Tools.
3. Mempercayai (memungkinkan) isi dinonaktifkan dalam database;
4. Kemasan, penandatanganan, dan menggunakan database

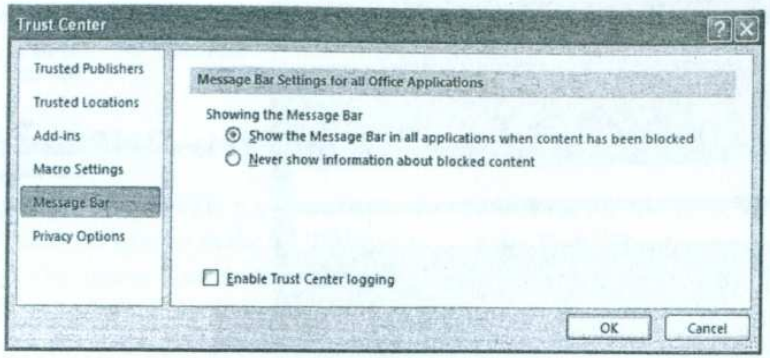



**Figure 20.7** The Microsoft Office Access Trust Center.

An overview of Microsoft Office Access 2007 DBMS is provided in Appendix H (available on the Web site).

# Keamanan di Oracle DBMS

- **Keistimewaan** :

  Beberapa contoh hak Oracle mencakup hak untuk : Terhubung ke database (membuat sesi); Membuat tabel; Pilih baris dari tabel pengguna lain.

  Dalam Oracle, ada dua kategori yang berbeda dari hak istimewa : Sistem hak istimewa; Obyek hak istimewa.

- **Sistem hak istimewa**

  Hak istimewa sistem yang diberikan kepada, atau dicabut dari, pengguna dan peran (dibahas di bawah) menggunakan salah satu dari berikut:

  - Hibah Keistimewaan Sistem/kotak Peran dialog dan Mencabut KeistimewaanSistem/Peran kotak dialog Manajer Keamanan Oracle;
  - SQL GRANT dan laporan REVOKE

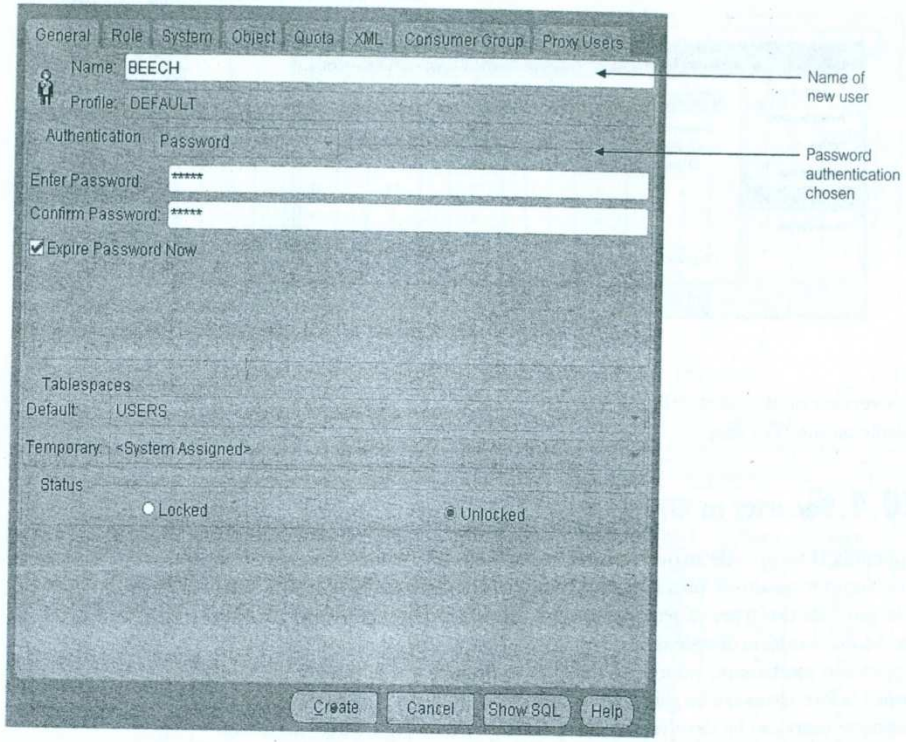
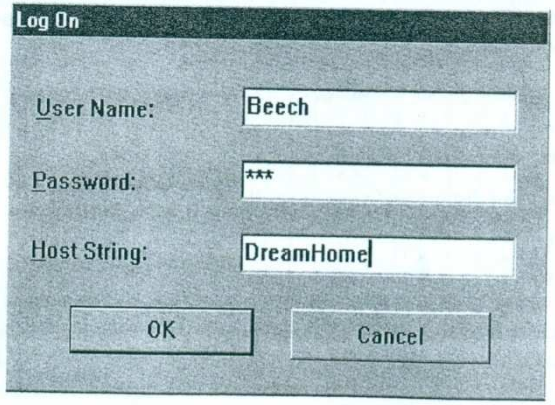



**Figure 20.8** Creation of a new user called Beech with password authentication set.

**Figure 20.9** Log On dialog box requesting user name, password, and the name of the database the user wishes to connect to.



# DBMS dan Keamanan Web

## 1. Proxy Server :

Dalam lingkungan Web, proxy server adalah sebuah komputer yang berada di antara Web browser dan server Web.

Proxy server memiliki dua tujuan utama:

a. **Meningkatkan kinerja, yaitu** proxy server menyimpan hasil dari semua permintaan untuk jumlah waktu tertentu secara signifikan

b. **Filter permintaan** yaitu Proxy server dapat digunakan untuk menyaring permintaan. Sebagai contoh, sebuah organisasi yang menggunakan server proxy untuk mencegah karyawan mengakses satu set spesifik situs Web.

**2. Firewall** , adalah sebuah sistem yang dirancang untuk mencegah akses tidak sah ke atau dari jaringan pribadi. Firewall dapat diimplementasikan baik sebagaiperangkat keras dan perangkat lunak atau kombinasi keduanya.

**3. *Algoritma Message Digest dan Digital Signatures***
Sebuah tanda tangan digital terdiri dari dua potongan informasi: string bit yangdihitung dari data yang sedang "ditandatangani," bersama dengan kunci privat dari individu atau organisasi yang ingin tanda tangannya. Tanda tangan dapat digunakan untuk memverifikasi bahwa data berasal dari individu atau organisasi.

***4. Digital Certificates***
adalah lampiran ke sebuah pesan elektronik yang digunakan untuk tujuan keamanan, verifikasi pengguna akan mengirimkan sebuah pesan yang dia klaim, untuk penerima dengan menyediakan kodekan jawaban. standar paling banyak digunakan adalah sertifikat digital X.509.

***5. Kerberos ,*** Kerberos memiliki fungsi mirip dengan server sertifikat: untuk mengidentifikasi dan memvalidasi pengguna
Pentingnya Kerberos adalah bahwa ia menyediakan satu server keamanan terpusat untuk semua data dan sumber daya pada jaringan. Akses database, login, kontrol otorisasi, dan fitur keamanan lainnya yang terpusat di server

***6. Secure Socket Layer dan Secure HTTP***

Secure Socket Layer (SSL) yang dikembangkan oleh Netscape untuk transmisi dokumen pribadi melalui Internet.SSL bekerja dengan menggunakan sebuah kunci pribadi untuk mengenkripsi data yang ditransfer melalui sambungan SSL. Baik Firefox dan Internet Explorer mendukung SSL, dan banyak situs Web menggunakan protokol ini untuk mendapatkan informasi pengguna rahasia,

**7.Transaksi Elektronik Aman dan Aman Teknologi**

Transaksi Secure Electronic Transaction (SET) adalah protokol standar, terbuka interoperabel untuk pemrosesan cardtransactions kredit melalui Internet,yang diciptakan bersama oleh Netscape, Microsoft,
Visa, Mastercard, GTE, SAIC,Terisa Sistem, dan VeriSign. SETS tujuannya adalah untuk memungkinkantransaksi kartu kredit menjadi sesederhana dan aman di Internet seperti yang di toko-toko ritel.

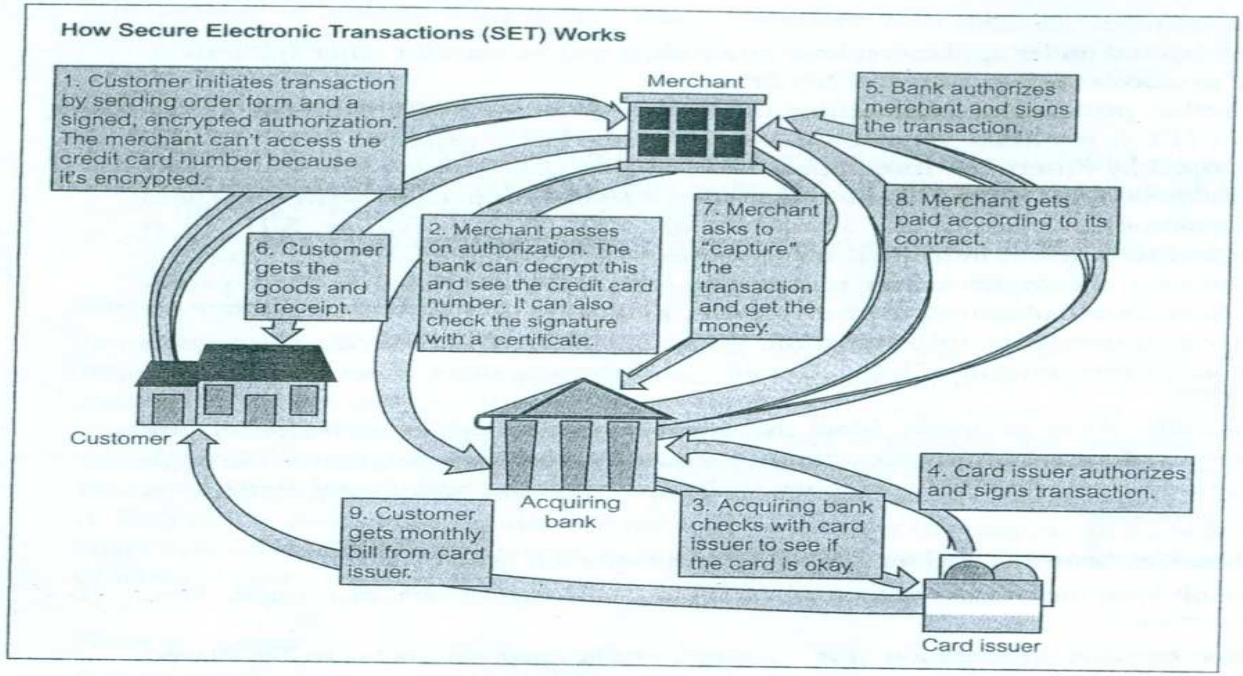



**Figure 20.11** A SET transaction.

**Gambar Transaksi Elektronik Aman dan Aman Teknologi**