BAB II

TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 *E-Commerce*

Electronic Commerce mendeskripsikan hal yang luas mengenai teknologi, proses dan praktek yang dapat melakukan transaksi bisnis tanpa menggunakan kertas sebagai sarana mekanisme transaksi, karena hal-hal tersebut dapat dilakukan dengan cara menggunakan *E-mail*, *Electronic Data Interchange* (EDI), bahkan dengan menggunakan jalur *World Wide Web* (*WEB*).

Definisi dari *E-Commerce* tidak dapat distandarkan dengan pasti, Menurut David Baum**,** pengertian *E-Commerce* adalah: "*E-Commerce is a dynamic set of technologies, applications, and business process that link enterprise, consumers, and communities through electronic transactions and the electronic exchange of goods, services, and information"* [7].

Namun secara umum *e-Commerce* merupakan satu set dinamis teknologi, aplikasi dan proses bisnis yang menghubungkan perusahaan, konsumen dan komunitas tertentu melalui transaksi elektronik seperti perdagangan barang atau jasa. Sebenarnya dalam *E-Commerce* banyak sebutan yang dipakai untuk memudahkan orang mengucapkannya. Ada beberapa sebutan untuk *E-Commerce* yaitu *Internet Commerce* atau *Electronic Commerce* yang pada dasarnya semua sebutan diatas mempunyai makna yang sama. Istilah-istilah tersebut berarti membeli atau menjual secara elektronik, dan kegiatan ini dilakukan pada jaringan *internet*.

2.1.1.1 Klasifikasi *E-Commerce*

Penggolongan *E-Commerce* yang lazim dilakukan orang ialah berdasarkan sifat transaksinya, antara lain:

1. ***Business to Business*** **(B2B)**

Jenis transaksi dimana pembeli biasanya membeli dalam jumlah besar karena akan dijual kembali. Contoh penjualan grosir.

2. ***Business to Consumer*** **(B2C)**

Jenis transaksi dimana pembelinya perorangan dan tidak punya tujuan untuk menjualnya kembali biasanya semacam toko *online* yang menjual berbagai macam barang.

3. ***Consumer to Consumer*** **(C2C)**

Jenis transaksi dimana pembelinya perorangan yang tidak mempunyai tujuan untuk dijual kembali dan penjualnya juga perorangan yang tidak menyediakan bermacam-macam barang melainkan hanya beberapa barang saja. Contoh: *online advertising*.

4. ***Consumer to Business*** **(C2B)**

Termasuk kedalam kategori ini adalah perseorangan yang menjual produk atau layanan kepada organisasi, dan perseorangan yang mencari penjual, berinteraksi dengan mereka dan menyepakati suatu transaksi.

2.1.1.2 Manfaat *E-Commerce*

E-commerce memiliki beberapa manfaat, baik itu organisasi, perusahaan dan masyarakat itu sendiri, berikut beberapa manfaat dari *e-commerce*

a. Manfaat yang diperoleh bagi organisasi pemilik *e-Commerce*:
    1. Memperluas *market place* hingga kepasar nasional dan internasional.
    2. Dengan *capital outplay* yang minim, sebuah perusahaaan dapat dengan mudah menemukan lebih banyak pelanggan, supplier yang lebih baik dan partner bisnis yang paling cocok dari seluruh dunia.
    3. *E-Commerce* menurunkan biaya pembuatan, pemrosesan, pendistribusian, penyimpanan, dan pencarian informasi yang menggunakan kertas.
    4. *E-Commerce* mengurangi waktu antara *outlay madal* dan penerimaan produk dan jasa.
    5. *E-Commerce* mendukung upaya-upaya *business process reengineering*. Dengan mengubah prosesnya, maka produktivitas *sales-people*, pegawai yang berpengetahuan, dan administrator bisa meningkat 100% atau lebih.
    6. Akses informasi menjadi lebih cepat.
b. Manfaat bagi konsumen antara lain:
    1. *E-Commerce* memungkinkan pelanggan untuk berbelanja atau melakukan transaksi selama 24 jam sehari sepanjang tahun dari hamper setiap lokasi.
    2. *E-Commerce* memberikan lebih banyak pilihan kepada pelanggan, mereka bisa memilih berbagai produk dari banyak vendor.

3. *E-Commerce* menyediakan produk dan jasa yang tidak mahal kepada pelanggan dengan cara mengunjungi banyak tempat dan melakukan perbandingan secara cepat.
4. Pelanggan bisa menerima informasi yang relevan secara detil dalam hitungan detik, bukan lagi hari atau minggu.
5. *E-Commerce* memberi tempat kepada para pelanggan untuk berinteraksi dengan pelanggan lain di *electronic community* dan bertukar pikiran serta pengalaman.

c. Manfaat bagi masyarakat lain:

1. *E-Commerce* memungkinkan orang untuk bekerja didalam rumah dan tidak harus keluar rumah untuk berbelanja. Ini berakibat menurunkan arus kepadatan lalu lintas dijalan serta mengurangi polusi udara.
2. *E-Commerce* memungkinkan orang dinegara-negara dunia ketiga dan wilayah pedesaan untuk menikmati aneka produk dan jasa yang akan susah mereka dapatkan tanpa *E-Commerce.*

2.1.1.3 Keamanan *E-Commerce*

Keamanan *E-Commerce* sangat penting sekali untuk menjaga data rahasia yang dimiliki oleh *user* atau *admin.* Berikut beberapa konsep dasar keamanan *e-commerce:*

1. *Security Policy* (Kebijaksanaan keamanan yang digunakan) merupakan satu set aturan yang diterapkan pada semua kegiatan-kegiatan pengamanan dalam *security domain. Security domain* merupakan satu set sistem komunikasi dan komputer yang dimiliki oleh organisasi yang bersangkutan.

2. *Authorization* (Otorisasi) berupa pemberian kekuatan secara hukum untuk melakukan segala aktifitasnya
3. *Accountability* (kemampuan dapat diakses) memberikan akses ke *personal security*.
4. *A Threat* (Ancaman yang tidak diinginkan) merupakan kemungkinan munculnya seseorang, sesuatu atau kejadian yang bisa membahayakan aset-aset yang berharga khususnya hal-hal yang berhubungan dengan *confidentiality, integrity, availability* dan *legitimate use.*
5. *An Attack* (Serangan yang merupakan realisasi dari ancaman), pada sistem jaringan Komputer ada dua macam tipe serangan, yaitu *passive attack* (misalnya *monitoring* terhadap segala kegiatan pengiriman informasi rahasia yang dilakukan oleh orang-orang yang tidak berhak) dan *active attack* (misalnya perusakan informasi yang dilakukan dengan sengaja dan langsung mengena pada sasaran).
6. *Safeguards* (Pengamanan) meliputi kontrol fisik, mekanisme, kebijaksanaan dan prosedur yang melindungi informasi berharga dari ancaman-ancaman yang mungkin timbul setiap saat.
7. *Vulnerabilities* (Lubang-lubang keamanan yang bisa ditembus).
8. *Risk* (Resiko kerugian) merupakan perkiraan nilai kerugian yang ditimbulkan oleh kemungkinan adanya *attack* yang sukses.
9. *Risk Analysis* (Analisa Kerugian) merupakan proses yang menghasilkan suatu keputusan apakah pengeluaran yang dilakukan terhadap *safeguards* bisa menjamin tingkat keamanan yang diinginkan.

2.1.2 *Internet*

Internet adalah sekumpulan komputer yang saling terkoneksi satu sama lain melalui jaringan komputer berbasis pada TCP/IP (*Transfer Control Protocol Internet Protocol)* sebagai standar jaringan *internet*. Protokol inilah yang memungkinkan transmisi data dapat dilakukan, ke hampir semua tipe komputer yang ada di dunia ini biasanya terhubung melalui *line telephone*, satelit dan kabel UTP (*Unshield Twisted Paired).*

2.1.2.1 *Web Server*

Web server adalah suatu layanan yang dapat memungkinkan untuk pengguna *internet* dapat saling terhubung atau terkoneksi untuk melakukan pertukaran data melalui *web server. Web server* merupakan suatu tipe *server* khusus yang dapat berkomunikasi langsung dengan *client* menggunakan metode HTTP.

Cara kerja *Web server* adalah menerima permintaan dari *client* dan meresponnya, biasanya dengan mengembalikan sebuah dokumen atau gambar yang sudah tersimpan.

2.1.2.2 *Web Browser*

Web browser adalah *software* yang digunakan pada komputer pemakai (*client*) yang meminta informasi dari *web server* dan penerjemah dari kod-kode instruksi yang ada pada halaman *web* untuk ditampilkan pada monitor komputer sesuai dengan yang diinginkan oleh user.

2.1.2.3 *Website*

Website merupakan suatu *webpage* beserta *homepage*, yang menawarkan suatu informasi kepada semua orang yang terhubung pada jaringan *internet*. Informasi dapat berupa teks, gambar, suara, dan tipe data *link*. Tipe data *link* merupakan suatu cara untuk berpindah ke *website* lainnya (*hyperlink*). *Homepage* adalah halaman pertama saat *website* ditampilkan.

2.1.2.4 *Hyper Text Markup Languange* (HTML)

HTML merupakan suatu bahasa kode-kode instruksi untuk menuliskan informasi pada sebuah *homepage*. Penulisan HTML dapat dilakukan menggunakan alat bantu sederhana seperti Notepad yang terdapat pada windows. Selain notepad masih banyak program yang dapat membantu dalam penulisan HTML misalnya Macromedia Dreamweaver. HTML merupakan kode-kode instruksi yang menjadi standar dalam membuat suatu halaman *web*.

2.1.2.5 *Cascading Style Sheet* (CSS)

Cascading Style Sheet (CSS) atau yang biasa disingkat dengan CSS, merupakan suatu dokumen yang digunakan untuk melakuakan pengaturan halaman *web* yang ditulis dengan HTML atau XHTML. Penggunaan CSS tidak memerlukan perangkat lunak tertentu karena CSS merupakan *script* yang telah *embedded* dengan HTML. CSS digunakan oleh *Web Designer* untuk menentukan warna, jenis, huruf, tata letak, dan berbagai aspek tampilan dokumen. CSS digunakan terutama untuk memisahkan antara isi dokumen dengan presentasi dokumen. Pemisah ini ditujukan agar dapat memisahkan aksesibilitas isi,

memberikan lebih banyak keleluasaan dan kontrol terhadap tampilan, dan mengurangi kompleksitas serta pengulangan pada strukur isi.

2.1.2.6 PHP (*Personal Home Page*)

PHP (*Personal Home Page*) adalah server-s*ide programming* yang populer digunakan untuk membuat *web-based application*. PHP dikenal sebagai sebuah bahasa *scripting* yang menyatu dengan tag-tag HTML yang diekseskusi di server dan digunakan untuk membuat halaman *web* yang dinamis seperti *guestbook,* statistik pengunjung, *polling, email,* dan masih banyak lagi. Adapun keunggulan yang dimiliki oleh bahasa pemrograman PHP adalah sebagai berikut :

a. *Life Cycle* yang sangat singkat , sehingga PHP selalu *up to date* mengikuti perkembangan teknologi *internet*.

b. *Cross Platform*, yakni PHP dapat dipakai di hampir semua *web*server yang ada di pasaran (terutama Apache dan Microsoft IIS) dan dijalankan pada berbagai sistem operasi (Linux, Windows, FreeBSD).

c. PHP mendukung koneksi ke banyak database baik yang gratis maupun komersil, seperti MySQL, mSQL, Oracle, Microsoft SQL Server, Interbase, dan banyak lagi.

d. PHP bersifat *open source* dan gratis. Kemudahan dalam mendapatkan dokumentasi. Sehingga tidak akan sulit untuk mencari referensi kode-kode PHP yang sudah jadi kemudian banyak juga pertanyaan pada grup-grup diskusi yang di dalamnya banyak sekali para *master* PHP.

PHP pertama kali dibuat oleh Rasmus Lerdorf pada tahun 1994 dari setumpuk *script perl CGI* yang digunakan untuk melacak siapa saja yang mengakseses resumenya di *web.* Versi pertamanya dirilis pada tahun 1995, untuk ditulis ulang *script-script perl* tersebut dengan menggunakan bahasa C guna meningkatkan kecepatannya kemudian menambah fasilitas *form* HTML dan dukungan koneksi ke *database* MySQL. Selanjutnya PHP dikembangkan oleh banyak *programmer* yang sangat antusias pada PHP, sampai saat ini versi PHP terbaru yang dipakai merupakan bahasa PHP versi 5.

2.1.2.7 Javascript

Javascript merupakan *cross-platform* yang dikembangkan oleh Netscape dan pertama kali digunakan dalam *browser* Netscape. Javascript dibuat agar mudah diintegrasikan kedalam program dan aplikasi lain, misalnya *browser*. Sebagian besar *browser* saat ini sudah mendukung javascript. Oleh karena itu, *script* dari javascript biasanya dimasukkan kedalam suatu HTML dan dieksekusi di *browser* lain.

2.1.2.8 Layanan Aplikasi *Internet*

Terdapat banyak sekali layanan aplikasi di internet dan masih terus akan berkembang dengan perkembangan teknologi informasi, beberapa contoh aplikasi yang banyak digunakan diantaranya adalah sebagai berikut:

1. *Electronic mail (email)*

Aplikasi ini adalah yang paling banyak digunakan dan termasuk salah satu dari aplikasi pertama di *internet.* Dengan *email*, kita dapat mengirim dan

menerima surat, pesan, dokumen secara elektronik dengan pemakai lain di *internet* yang mempunyai alamat *email*.

2. *World Wide Web* (WWW)

Awalnya informasi dapat dicari pada *internet* dengan menggunakan fasilitas *information service* berbasis archie, gopher dan WAIS (*Wide Area Information System*). Pencarian informasi berdasarkan menu pada sistem-sistem tersebut dan output yang dihasilkan berbasis teks. Saat ini teknologi WWW memungkinkan untuk mengakses informasi secara interaktif dan bentuk informasinya berupa tampilan grafis maupun teks. Hal ini dimungkinkan dengan adanya HTTP yang digunakan untuk mengakses suatu informasi yang disimpan pada suatu situs web (*website*). Untuk dapat menggunakan sarana ini dibutuhkan aplikasi *web browser*.

3. *Universal Resource Locater* (URL)

Pada penggunaan WWW, penunjukan suatu sumber informasi menggunakan metode URL yang merupakan konsep penamaan lokasi standar dari suatu file, direktori, komputer, lokasi komputernya dan metoda yang digunakan. URL tidak hanya dapat menunjuk ke suatu file tapi dapat juga menunjuk suatu query, dokumen dalam suatu database atau hasil dari perintah. Dengan URL ini didefinisikan lokasi dan metoda pengaksesan file tersebut.

4. *Hypertext Transfer Protocol* (HTTP)

HTTP (*HyperText Transfer Protocol*) adalah protokol yang dipergunakan untuk mentransfer dokumen dalam *World Wide Web* (WWW). Pengembangan HTTP dikoordinasi oleh Konsorsium *World Wide Web* (W3C) dan grup bekerja

Internet Engineering Task Force (IETF). HTTP bertugas menangani permintaan dari browser untuk mengambil dokumen web. HTTP bisa dianggap sebagai sistem yang bermodel *Client-Server*. Browser web sebagai klientnya, mengirimkan permintaan ke *web server* untuk mengirimkan dokumen *web* yang dikehendaki. *Web server* lalu memenuhi permintaan tersebut dan mengirimkannya melalui jaringan kepada *browser*.

5. *Hypertext Transfer Protocol Secure* (HTTPS)

Https adalah versi aman dari HTTP, protokol komunikasi dari *World Wide Web*. Ditemukan oleh *Netscape Communications Corporation* untuk menyediakan autentikasi dan komunikasi tersandi dan penggunaan dalam komersi elektris. Selain menggunakan komunikasi plain text, HTTPS menyandikan data sesi menggunakan protokol SSL (*Secure Socket layer*) atau protokol TLS (*Transport Layer Security*). Kedua protokol tersebut memberikan perlindungan yang memadai dari serangan *eavesdroppers* dan *man in the middle attacks*. Pada umumnya port HTTPS adalah 443. Tingkat keamanan tergantung pada ketepatan dalam mengimplementasikan pada browser web dan perangkat lunak server dan didukung oleh algorithma penyandian yang aktual. Oleh karena itu, pada halaman web digunakan HTTPS dan URL yang digunakan dimulai dengan ‘https://’ bukan dengan ‘http://’. Kesalahpahaman yang sering terjadi pada pengguna kartu kredit di web ialah dengan menganggap HTTPS “sepenuhnya” melindungi transaksi mereka. Sedangkan pada kenyataannya, HTTPS hanya melakukan enkripsi informasi dari kartu mereka antara *browser* mereka dengan *web server* yang menerima informasi. Pada *web server*, informasi kartu mereka secara tipikal

tersimpan di database *server* dan *server database* inilah yang paling sering menjadi sasaran penyerangan oleh pihak-pihak yang tidak berkepentingan.

2.1.3 Pemograman *Database*

Definisi dari *database* adalah kumpulan dari data yang saling terhubung yang memiliki suatu tujuan tertentu. *Database* secara global terdiri dari kumpulan tabel yang berisi baris dan kolom. Tiap baris dan tabel memiliki satu unit data yang disebut *record* dan kolom didalam tabel merupakan keterangan dari masing-masing *record*. Pemrograman sebuah *database* banyak dilakukan dengan menggunakan bahasa standar internasional untuk penulisan *database* disebut dengan *Structure Query Language* (SQL). Selain SQL, Pemrograman *database* juga meliputi manipulasi objek-objek *database*, analisa *query*, dan juga interaksi *database* dengan *Open Database Connectivity* (ODBC*).*

Pemrograman *database* yang akan digunakan pada skripsi ini, menggunakan *software* database bernama MySQL. MySQL adalah sebuah *Relational Database Management System* (RDBMS) yang didistribusikan secara gratis dibawah lisensi *General Public Lisence* (GPL).

Kelebihan MySQL bila dibandingkan dengan produk-produk lain yang sejenis:

1. MySQL merupakan *software database* yang memiliki kecepatan dan reliabilitas yang tinggi dalam pemroses data.

2. MySQL mudah digunakan dan memiliki dukungan *user* yang luas.

3. Memiliki sekuritas yang baik, karena didukung oleh para ahli pemograman sehingga dapat diatasi secara cepat jika terjadi *bug* (Celah keamanan).

4. Bisa berjalan dibanyak *platform* selain PC.

5. Mendukung banyak bahasa pemrograman seperti C, C++, *Perl*, *Phyton, Java*, dan PHP.

2.1.4 Macromedia Dreamweaver

Dreamweaver merupakan suatu HTML *editor* profesional yang digunakan untuk merancang, *coding*, dan mengembangkan *web* dan aplikasi berbasis *web*. Dreamweaver memudahkan *user* dalam bekerja dalam lingkungan *editing* visual yang tentunya dilengkapi dengan kontrol *hand-coding* HTML. Dreamweaver juga dapat mengembangkan *workflow* dan juga dapat menambahkan animasi dari Flash ke dalamnya. Selain itu, Dreamweaver menyediakan *interface* yang *full-featured coding* yang termasuk *tools code-editing* dan materi CSS, Javascript, CFML, dan bahasa lainnya.

Aplikasi yang dibangun dapat berupa aplikasi dinamis, dimana Dreamweaver kompatibel dengan teknologi *server* seperti ASP.NET, ASP, JSP dan PHP. Selain itu juga kompatibel dengan XML data dan menyertakan *file* XML dan memajangnya di halaman *web*. *Dreamweaver is fully customizable* artinya dapat menciptakan objek sendiri, mengatur dan memodifikasi *shortcut* untuk *keyboard*, bahkan menulis Javascript untuk memperluas kemampuan Dreamweaver dengan *behavior, property inspector,* dan *site reports* yang baru.

2.1.5 Windows Apache MySQL PHP (WAMP)

WAMP adalah suatu bundel *web server* yang populer digunakan untuk alat bantu sebagai pengganti peran dari *web server* yang digunakan pada *windows* sebagai *operating system* (OS). Sebuah bundel program *open source* tersebut berisi antara lain *web server* Apache, *interpreter* PHP, dan basis data MySQL. Setelah menginstall WAMPP, kita bisa memulai pemrograman PHP di komputer sendiri maupun mencoba menginstall aplikasi-aplikasi *web seperti* Joomla, Aura CMS (*Content Management System*) dan lainnya.

2.1.6 *Entity Relationship Diagram* (ERD)

Entity Relationship Diagram merupakan model data berupa notasi grafis dalam pemodelan data konseptual yang menggambarkan hubungan antara entitas. Model data sendiri merupakan sekumpulan cara, peralatan untuk mendeskripsikan data-data yang berhubungan satu sama lain, semantiknya, serta batasan konsistensi. Model data terdiri dari model hubungan entitas dan model relasional. Diagram hubungan entitas ditemukan oleh Peter Chen dalam buku Entity Relational Model-Toward a Unified of Data. Chen mencoba merumuskan dasar-dasar model dan setelah itu dikembangkan dan dimodifikai oleh Chen dan banyak pakar lainnya.

Diagram hubungan entitas digunakan untuk mengkonstruksikan model data konseptual, memodelkan struktur data dan hubungan antar data dan mengimplementasikan basis data secara logika maupun secara fisik dengan DBMS (Database Management system). Diagram hubungan entitas dapat membantu dalam menjawab persoalan tentang data yang diperlukan dan

bagaimana data tersebut saling berhubungan. Simbol-simbol yang terdapat pada ERD diantaranya sebagai berikut :

1. Entitas

   Entitas adalah suatu objek yang dapat didefinisikan dalam lingkungan pemakai, sesuatu yang penting bagi pemakai dalam konteks sistem yang akan dibuat. Sebagai contoh pelanggan, pegawai, dan lain-lain. Berdasarkan atribut kuncinya, entitas terbagi menjadi dua, yaitu:

   a. Entitas kuat

      Entitas yang mempunyai atribut kunci. Entitas ini bersifat mandiri, keberadaanya tidak bergantung pada entitas lainnya. Kebanyakan entitas dalam suatu organisasi dapat digolongkan sebagai entitas kuat *(strong entity).* Entitas kuat memiliki karakteristik yang unik (dinamakan *identifier*), yaitu sebuah atribut tunggal atau gabungan atribut yang secara unik dapat digunakan untuk membedakannya dari entitas kuat yang lain.

   b. Entitas lemah

      Entitas yang tidak mempunyai atribut kunci. Entitas lemah diidentifikasikan dengan menghubungkan entitas tertentu dari tipe entitas yang lain ditambah atribut dari entitas lemah. Tipe entitas lain yang dipakai untuk mengidentifikasikan suatu entitas lemah disebut *identifying owner* dan relasi yang menghubungkan entitas lemah dengan owner disebut *identifying relationship.*

2. Atribut

   Atribut adalah properti atau karakteristik yang dimiliki oleh suatu entitas. Misalnya untuk entitas pegawai mungkin memiliki atribut-atribut nomor induk pegawai, nama, alamat, gaji pokok. Setiap diagram hubungan entitas bisa terdapat lebih dari satu atribut.

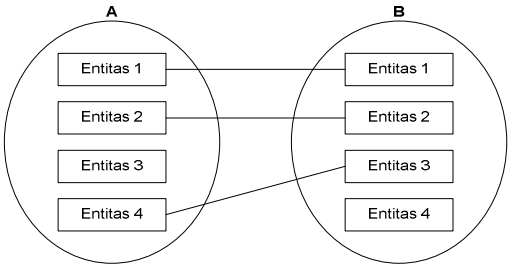
3. Relasi

   Relasi adalah hubungan antara suatu himpunan dengan himpunan entitas yang lainnya. Relasi menunjukkan adanya hubungan di antara sejumlah entitas yang berasal dari himpunan entitas yang berbeda.

4. Kardinalitas

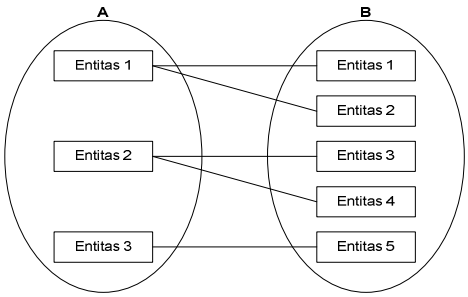
   Kardinalitas relasi menunjukkan jumlah maksimum entitas yang dapat berelasi dengan entitas pada himpunan entitas yang lain. Kardinalitas relasi yang terjadi di antara dua himpunan entitas dapat berupa.

   a. Satu ke satu (*one to one*)



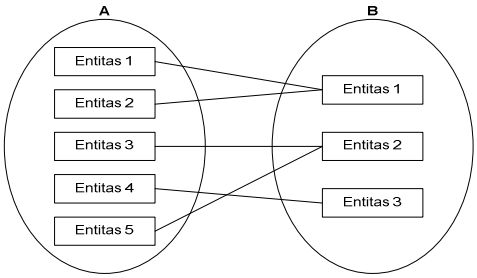
Gambar II-1 Kardinalitas Satu ke Satu

b. Satu ke banyak (*one to many*)



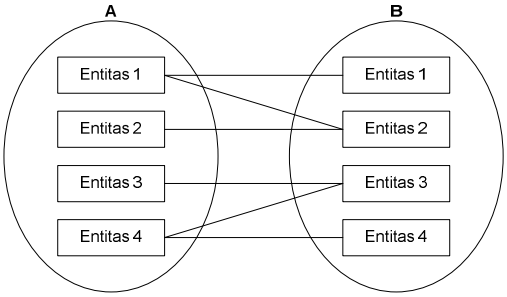
Gambar II-2 Kardinalitas Relasi Satu ke Banyak

c. Banyak ke satu (*many to one*)



Gambar II-3 Kardinalitas Relasi Banyak ke Satu

d. Banyak ke banyak (*many to many*)



Gambar II-4 Kardinalitas Banyak ke banyak

2.1.7 Hiraki *Database*

Data terdiri dari aksara-aksara (*characters*) yang tersusun secara sistematik serta dirangkaikan satu dengan yang lain sehingga memenuhi tujuan

pengolahannya. struktur penyajian data yang paling rendah, yaitu dari "*bit*"sampai"*database*".

1. *BIT*

Bit merupakan kepanjangan dari *BINARI DIGIT*. *Bit* dimaksudkan untuk menyajikan kondisi *ON*/*OFF* dari aliran (pulsa-pulsa) elektronik mesin (komputer) yang diberi symbol "0" dan "1". Jadi *Bit* merupakan unit terkecil dari data. Dan *bit-bit* ini tidaklah selalu tetap jumlah digit dalam sistem komputer, tetapi tergantung dari sitem komputer (dari pabrik pembuat komputer itu sendiri).

2. *BYTE*

Byte sama dengan karakter, yaitu merupakan kumpulan dari *bit*. Yang disebut karakter (aksara) seperti huruf A-Z, a-z, angka 0-9, *blank*(spasi), dan spesial karakter (karakter khusus berupa simbol-simbol, seperti: !@#$^&*(* titik(.) tanda petik ('/") dan lain sebagainya.

3. *FIELD*

Field merupakan kumpulan satu atau lebih *byte* (karakter) yang mempunyai makna. Contoh : nama, nomor induk mahasiswa, umur dan sebagainya.

4. *RECORD*

Record merupakan kumpulan satu atau lebih *field* yang membentuk satu kesatuan. Contoh : *Record* mahasiswa terdiri dari nomor induk mahasiswa, nama mahasiswa, tempat tanggal lahir, alamat dan sebagainya.

5. *FILE*

File merupakan kumpulan satu atau lebih *record-record* yang mempunyai kesamaan logik (kesamaan stuktur *file*-nya). Contoh: *file* mahasiswa, *file* Dosen, *file* siswa dan sebagainya**.**

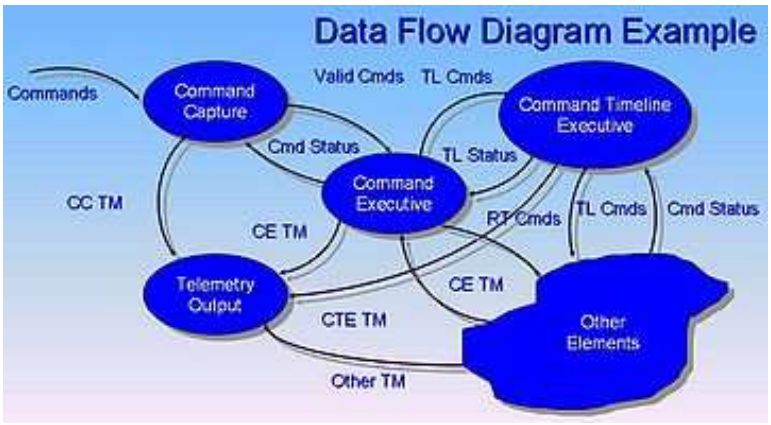
6. *DATABASE*

Database merupakan kumpulan satu atau lebih *file-file* yang saling berhubungan, yang menunjang suatu manajemen pengolahan data. Dalam suatu data Mahasiswa di butuhkan beberapa *file* yang menunjang suatu pengolahan nilai mahasiswa, *file-file* tersebut seperti: *File* induk yang menyimpan data mahasiswa dan data nilai.

2.1.8 *Data Flow Diagram* (DFD)

Data Flow Diagram (DFD) adalah suatu alat pembuatan model yang memungkinkan profesional sistem untuk menggambarkan sistem sebagai suatu jaringan proses fungsional yang dihubungkan satu sama lain dengan alur data, baik secara manual maupun komputerisasi [6]. Pendekatan terstruktur dilengkapi dengan alat-alat (*tools*) dan teknik (*techniques*) yang dibutuhkan dalam pengembangan sistem, sehingga hasil akhir dari sistem yang dikembangkan akan diperoleh sistem yang strukturnya didefinisikan dengan baik dan jelas. Melalui pendekatan terstruktur, permasalahan yang komplek di organisasi dapat dipecahkan dan hasil dari sistem akam mudah untuk dipelihara, fleksibel, lebih memuaskan pemakainya, mempunyai dokumentasi yang baik, tepat waktu, sesuai

dengan anggaran biaya pengembangan, dapat meningkatkan produktivitas dan kualitasnya akan lebih baik (Gambar II-5).



Gambar II-5 *Data flow diagram* (DFD)

DFD didesain untuk menunjukkan sebuah sistem yang terbagi-bagi menjadi suatu bagian sub-sistem yang lebih kecil dan untuk menggaris bawahi arus data antara kedua hal yang tersebut diatas. Diagram ini lalu dikembangkan untuk melihat lebih rinci sehingga dapat terlihat model-model yang terdapat di dalamnya.

Menggambarkan sebuah sistem kontektual *data flow diagram* yang akan pertama kali muncul adalah interaksi antara sistem dan entitas luar. DFD juga memiliki beberapa syarat yang tidak boleh dilanggar, yaitu

1. Tidak boleh menghubungkan antara *entity* luar dengan *entity* luar yang lain secara langsung.
2. Tidak boleh menghubungkan data store yang satu dengan yang lainnya.
3. Tidak boleh menghubungkan data store dengan *entity* luar secara langsung.

4. Setiap proses harus memiliki data yang masuk dan juga yang keluar.

DFD dirancang untuk menunjukkan sebuah sistem yang terbagi-bagi menjadi suatu bagian subsistem yang lebih kecil. Beberapa simbol yang digunakan dalam DFD adalah sebagai berikut:

a. Kesatuan luar (*external entity*) atau batas sistem (*boundary*) merupakan kesatuan (*entity*) di lingkungan luar sistem yang dapat berupa orang, organisasi atau sistem lainnya yang berada di lingkungan luarnya yang akan memberikan masukan atau menerima keluaran dari sistem.
b. Arus data (*data flow*) ini mengalir diantara proses (*process*), simpanan data (*data store*) dan kesatuan luar (*external entity*). Arus data ini menunjukan arus dari data yang dapat berupa masukan untuk sistem atau hasil dari proses sistem.
c. Proses (*process*) merupakan kegiatan yang dilakukan oleh orang, mesin atau komputer dari hasil suatu arus data yang masuk ke dalam proses untuk dihasilkan arus data yang akan keluar dari proses.
d. Simpanan data (*data store*) merupakan simpanan dari data yang dapat berupa suatu file atau *database* di sistem komputer, suatu arsip atau catatan manual, suatu kotak tempat data di meja seseorang, suatu tabel acuan manual, dan suatu agenda atau buku.

2.1.9 *Flowmap* (Aliran Data)

Flowmap adalah suatu *tools* yang digunakan untuk mengetahui dan menganalisis suatu interaksi atau aliran data. Sebuah lokasi tempat mulai mengalir

dan tujuan lokasi dimana arus data berakhir. *Flowmap* merupakan campuran dari peta dan *flowchart,* yang menunjukkan pergerakan dari suatu benda dari satu lokasi ke lokasi lainnya. *Flowmap* secara spesifik dapat digunakan untuk :

1. Menyimpan, menampilkan, analisa pola aliran spasial, seperti migrasi.
2. Menghitung jarak, waktu tempuh, biaya transportasi menggunakan peta jaringan transportasi.
3. Pemodelan wilayah pemasaran.

Flowmap menolong analis dan programmer untuk memecahkan masalah kedalam segmen-segmen yang lebih kecil dan menolong dalam menganalisis alternatif-alternatif lain dalam pengoperasian. Bila seorang analisis dan programmer akan membuat flowmap, ada beberapa petunjuk yang harus diperhatikan, seperti :

1. *Flowmap* digambarkan dari halaman atas ke bawah dan dari kiri ke kanan.
2. Aktivitas yang digambarkan harus didefinisikan secara hati-hati dan definisi ini harus dapat dimengerti oleh pembacanya.
3. Kapan aktivitas dimulai dan berakhir harus ditentukan secara jelas. Setiap langkah dari aktivitas harus berada pada urutan yang benar.
4. Lingkup dan *range* dari aktifitas yang sedang digambarkan harus ditelusuri dengan hati-hati.
5. Gunakan simbol-simbol *flowmap* yang standar.

2.1.10 Advetorial

Advetorial adalah suatu iklan yang dibuat untuk membentuk suatu citra yang baik pada publik. Advetorial merupakan salah satu jenis penggelembungan bahasa, kalimat ini berasal dari bahasa Inggris yang merupakan gabungan dari *Advertisement* dan *Editorial.*

Advertisement (iklan) adalah suatu format dari komunikasi diharapkan untuk membujuk suatu pendengar (penonton, pendengar atau pembaca). Meliputi nama dari suatu produk atau jasa dan bagaimana yang produk atau jasa bisa bermanfaat bagi konsumen, membujuk pelanggan potensial untuk membeli atau untuk mengkonsumsi merek yang tertentu itu.

2.1.11 *Internet Banking*

2.1.11.1 Pengertian *Internet Banking*

Internet Banking atau *e-banking* bisa diartikan sebagai aktifitas perbankan di *internet* yang memungkinkan pelanggan untuk melakukan transaksi keuangan pada web yang aman. Layanan ini memungkinkan nasabah sebuah bank untuk melakukan hampir semua jenis transaksi perbankan melalui sarana *internet,* khususnya via web. Mirip dengan penggunaan mesin ATM, lewat sarana *internet* seorang nasabah dapat melakukan pengecekan rekening, transfer dana antar rekening, hingga pembayaran tagihan-tagihan rutin bulanan (listrik, telepon, dan sebagainya.) melalui rekening bank.

2.1.11.2 Sejarah *Internet Banking* di Indonesia

Tahun 2000, implementasi *e-Banking* dan *mobile banking* mulai di lakukan oleh beberapa Bank di Indonesia. Bank di Indonesia mulai memasuki dunia maya. Beberapa situs *Internet Banking* di Indonesia adalah sebagai berikut:

1. 1998, Bank Internasional Indonesia https://www.bankbii.com/
2. 2001, Bank Sentral Asia (BCA) https://ibank.klikbca.com/
3. 2003, Bank Mandiri https://ib.bankmandiri.co.id/
4. 2005, Bank PermataNet https://www.permatanet.com
5. 2006, Bank Permata e-Business https://www.permatae-business.com/
6. 2007, Bank Negara Indonesia https://ibank.bni.co.id/
7. Bank Lippo https://ebanking.lippobank.co.id/

2.1.11.3 Keamanan *Internet Banking*

Saat ini transaksi via *Internet Banking* semakin banyak dilakukan. Segala urusan, kecuali pengambilan tunai dapat dilakukan melalui *Internet Banking*. Kegiatan perbankan menjadi lebih mudah dan cepat. Nasabah pun tidak perlu datang lagi ke bank atau ATM hanya untuk sekedar transfer antar rekening maupun antar bank, atau membayar segala jenis tagihan. Beberapa cara pengamanan yang digunakan dalam *Internet Banking* adalah sebagai berikut

1. Penggunaan HTTPS, adalah salah yang menunjang keamanan. Banyak situs menggunakan HTTPS dimana penggunaan ini akan memungkinkan halaman berganti-ganti secara berurutan dan tidak menggunakan session. Sehingga jika didiamkan dalam waktu yang relatif lama maka akan

kembali kehalaman depan lagi. Selain itu *cookies* dari web langsung terhapus setiap saat sehingga seorang *cracker* tidak dapat menggunakan informasi *cookies* untuk melakukan pencurian data.

2. Penggunaan PIN acak. Beberapa bank menggunakan alat yang bernama token yang memungkinkan pengguna selalu menggunakan PIN dinamis sehingga PIN hanya dapat digunakan satu kali saja karena setiap kali login pin selalu berubah-ubah.

2.1.11.4 Keuntungan *Internet Banking*

Banyak keuntungan yang bisa didapatkan oleh nasabah dengan memanfaatkan layanan ini, terutama bila dilihat dari waktu dan tenaga yang dapat dihemat karena transaksi e-banking jelas bebas antrian dan dapat dilakukan dari mana saja sepanjang nasabah dapat terhubung dengan jaringan *internet*. Beberapa keuntungan menggunakan *Internet Banking* adalah sebagai berikut:

1. *Hemat waktu*, melakukan aktivitas perbankan cukup menggunakan personal komputer atau laptop yang dilengkapi dengan koneksi *internet*
2. *Kapan saja*, tak terbatas waktu untuk bertransaksi atau sekedar melakukan cek saldo dan melihat mutasi rekening
3. *Dimana saja*, dapat melakukan transaksi dari belahan dunia manapun selama ada akses ke *Internet*
4. *Mudah*, menu transaksi jelas dengan navigasi yang simple, walaupun baru pertama kali menggunakannya

5. *Aman*, dilengkapi sistem keamanan berlapis, yaitu nasabah pengguna melakukan akses dengan user id dan password dan untuk melakukan transaksi finansial nasabah pengguna wajib menggunakan token. Jadi walaupun seseorang yang tidak berhak mengetahui username dan password untuk login ke *Internet Banking*, orang tersebut tidak dapat melakukan transaksi finansial di *Internet Banking* tersebut, karena setiap transaksi finansial membutuhkan *challenge code* yang digenerate oleh token *Internet Banking*.
6. *Satu akses untuk semua produk*, dengan login hanya menggunakan user id dan password, nasabah pengguna dapat sekaligus mengakses seluruh produk dari bank yang bersangkutan.
7. *Registrasi mudah*, registrasi dapat dilakukan melalui ATM bank yang bersangkutan dan aktivasinya dapat dilakukan di situs *Internet Banking* bank tersebut. Untuk mendapatkan token, nasabag dapat memperolehnya dengan mendatangi bank yang bersangkutan dengan biaya administrasi yang relatif murah.

2.1.11.5 Kelemahan *Internet Banking*

Internet Banking memiliki kelemahan dengan memanfaatkan celah keamanan user yang tidak waspada terhadap keamanan. Beberapa cara dan celah yang umum digunakan oleh para *cracker* adalah sebagai berikut:

1. Membuat halaman palsu dari situs bank. Cara ini bisa dibilang ampuh seperti kejadian klikbca yang dibuat situs palsunya dengan nama clickbca.com. Pengguna yang tidak sadar akan masuk ke halaman yang

salah yang kemudian informasi mengenai akun akan dengan cepat berpindah ke situs lain. Namun hal ini cukup sulit dilakukan karena sudah semakin banyak bank menggunakna token pin dan pin dinamis pada setiap kali login.

2. Penggunaan *spyware*, trojan maupun backdoor yang dapat memata-matai kegiatan pengguna sehingga informasi akun dapat dicuri.
3. *Cookies browser* yang tertinggal. Sering kali kita mengaktifkan fitur "*remember me*" yang akan membuat *browser* menyimpan data login kita secara otomatis. Hal ini akan mempermudah *spyware* mendapatkan data dari pengguna tersebut.
4. Penggunaan *keylogger*. Beberapa tempat umum yang menyediakan *internet* seperti warnet kadang memasang *keylogger* yang dapat berupa *software* atau *hardware*, sebenarnya hal ini melanggar *privacy* dan etika. Sebagai pengguna, kita harus jeli mengenali *keylogger* ini dan untuk lebih aman jangan menggunakan *internet* di tempat umum seperti warnet untuk transaksi.

2.1.12 PayPal

2.1.12.1 Pengertian PayPal

PayPal adalah salah satu alat pembayaran (*Payment procesors*) menggunakan *internet* yang terbanyak digunakan didunia dan teraman saat ini. Pengguna *internet* dapat membeli barang di situs *e-commerce*, lisensi software original, keanggotaan situs, urusan bisnis, mengirim dan menerima donasi atau sumbangan, mengirim uang ke pengguna PayPal lain di seluruh dunia dan banyak

fungsi lainnya dengan mudah dan otomatis menggunakan *internet*. PayPal mengatasi kekurangan dalam pengiriman uang tradisional seperti Cek atau *Money order* yang prosesnya lambat.

2.1.12.2 Sejarah PayPal

Perusahaan Paypal (Paypal corp.) seperti yang dikenal sekarang adalah penggabungan antara perusahaan Confinity dan X.com pada tahun 2000. Confinity didirikan pada desember 1998 oleh Peter Thiel dan Max Levchin, awalnya sebagai alat pembayaran Palm Pilot dan sebagai perusahaan kriptograpi (ilmu pembacaan sandi, tulisan-tulisan atau angka-angka rahasia). Sedangkan X.com didirikan oleh Elon Musk pada maret 1999, yaitu perusahaan penyedia jasa perencanaan keuangan. Kedua perusahaan lokasi pertamanya adalah kantor di 165 *University* Avenue di Palo Alto, California, rumah dari beberapa pemula di Silicon Valley. Ebay melihat perkembangan penggunaan Paypal dan menyimpulkan Paypal cocok sebagai salah satu alat pembayaran di ebay. Pada mei 1999 ebay membeli Billpoint dan menjadikan Billpoint sebagai alat pembayaran utama ebay saat itu dan membuat Billpoint khusus hanya untuk alat pembayaran di ebay saja, karenanya Paypal hanya tampil beberapa kali sebagai pilihan alat pembayaran di ebay dibandingkan Billpoint. Tetapi karena masyarakat lebih menyukai Paypal karena mudah dan lebih aman, pada Februari 2000 rata-rata ada 200.000 penawaran barang perhari yang menggunakan Paypal sedangkan Billpoint hanya 4.000 penawaran. Pada april 2000 lebih dari 1 juta penawaran menggunakan Paypal.

2.1.12.3 Keamanan Transaksi pada PayPal

PayPal lebih aman bila dibandingkan dengan alat pembayaran *online* yang lain. Hal ini karena pembeli yang merasa dirugikan atau tidak sesuai deskripsi yang diberitahukan, bisa meminta uang kembali kepada penjual dalam waktu maksimal 45 hari setelah terjadi pembayaran. Jika pembeli menggunakan kartu kredit akan mendapatkan pengembalian uang *chargeback* dari perusahaan kartu kreditnya. PayPal juga melindungi penjual dari pengembalian uang atau komplain yang tidak benar dari pembeli sesuai pembuktian.

Perlindungan untuk penjual dirancang untuk melindungi penjual dari klaim pembeli yang mengaku telah mengirim uang yang tidak mempunyai catatan bukti pembayaran dan deskripsi transaksi, setiap pembelian dan pembayaran menggunakan PayPal selalu ada catatan bukti pembayarannya di *account* PayPal pengirim dan penerima uang, sebagai bukti jika benar telah terjadi pengiriman uang antara keduanya.

Bisa diambil kesimpulan bahwa menggunakan PayPal lebih aman dari alat pembayaran online lain bagi pengirim dan penerima uang karena ada bukti pembayaran dan catatan deskripsi, serta dapat melakukan komplain yang benar jika terjadi sesuatu atau terhindar dari komplain yang salah.

2.1.12.4 Perbedaan Akun pada PayPal

Terdapat tiga buah jenis akun yang disediakan oleh PayPal untuk para konsumennya, diantaranya adalah sebagai berikut:

1. Akun *Personal*

   Dengan akun tipe ini, pengguna sudah dapat mengirim dan menerima uang dan melakukan penjualan dengan eBay. Pada tipe ini, pengguna bisa menerima pembayaran dari akun Paypal lain, namun tidak bisa menerima pembayaran dari *credit* atau *debit card*. Tidak ada biaya untuk setiap transaksi yang dilakukan pada tipe ini. Terdapat limit berapa banyak uang yang dapat diterima per bulannya. Tipe personal ini tidak cocok untuk pengguna PayPal yang merencanakan untuk berjualan produk dalam jumlah yang besar.

2. Akun *Premier*

   Tipe ini hampir sama dengan akun Personal, bedanya pada tipe ini pengguna bisa menerima pembayaran dari *credit card, debit card* dan rekening bank. Pengguna juga bisa menggunakan fasilitas *shopping cart* dan fasilitas laporan pembayaran (payment reporting tool). Akun Premier cocok digunakan untuk penjual yang ingin menjual produknya secara reguler. Untuk pengguna yang memiliki akun personal, pengguna tersebut dapat melakukan upgrade ke akun Premier.

3. Akun *Business*

   Tipe ini cocok digunakan untuk bisnis yang berskala besar atau *online store*. Pada tipe ini pengguna diperbolehkan menggunakan laporan dan *tool* eBay tanpa adanya persyaratan mengenai jenis transaksi. Pengguna akan dikenakan biaya dalam menggunakan akun tipe ini. Jika saat ini

pengguna memiliki akun Personal atau Premier, pengguna dapat melakukan upgrade ke akun *Business*. PayPal tidak mengenakan biaya pada pembeli dalam mengirimkan uang ke penjual. PayPal akan mengenakan biaya kepada pengguna sebagai penjual (penerima uang) sebesar 1.9% hingga 2.9% dari jumlah uang yang diterima.

2.1.12.5 Cara Mendaftar PayPal

Proses pendaftaran untuk memperoleh akun PayPal memerlukan data seperti email, nama, alamat, nomor telepon, nomor kartu kredit jika pendaftar memiliki kartu kredit, dan nomor rekening bank. Langkah-langkah untuk memperoleh akun PayPal, diantaranya adalah sebagai berikut:

1. Masuk ke situs www.paypal.com
2. Klik *SignUp* untuk mendaftar
3. Selanjutnya ada pilihan negara dan tipe akun yang diinginkan. Setelah memilih negara dan tipe akun yang diinginkan, tekan *Continue*.
4. Selanjutnya masukan informasi seperti nama, alamat, nomor telepon, email. Untuk jenis mata uang disarankan memilih U.S. Dollar karena mata uang rupiah belum tersedia di PayPal. Email yang dimasukan akan menjadi usernae PayPay untuk melakukan proses login atau transaksi. Isi password dengan kombinasi huruf dan angka, minimal delapan karakter. Pada password *recovery* pilih dan isikan dua pertanyaan dan jawaban pribadi untuk mendapatkan password kembali jika suatu saat pengguna lupa akan passwordnya.

5. Baca *User Agreement* dan *Privacy Policy* jika diperlukan, lau beri tanda *cheklist* pada pilihan *Yes* dan ketikan kode pengaman yang berwarna kuning pada kolom yang tersedia tanpa ada spasi.
6. Jika data yang dimasukan sudah sesuai, tekan *SignUp*.
7. Selanjutnya sistem akan meminta pengguna untuk memasukan nomor kartu kredit yang akan digunakan untuk memasukan dana ke akun PayPal, kemudian klik *Add Card*. Apabila pengguna tidak ingin memasukan data kartu kredit atau pengguna tidak mempunyai kartu kredit, klik *Cancel*.
8. Pengguna akan menerima email konfirmasi bahwa pengguna telah mendaftar dan untuk mengaktifkan akun PayPal. Buka *email* dari PayPal tersebut dan klik link konfirmasi yang terdapat didalamnya untuk konfirmasi kepemilikan akun PayPal.
9. Setelah itu pengguna akan dibawa kembali ke situs PayPal dan sistem akan meminta pengguna untuk memasukan password, setelah itu pengguna akan masuk ke halaman *My Account*.
10. Jika pengguna sudah memasukan data kartu kredit di halaman *My Account* akan muncul bacaan *Expanded Option*. Baca instruksinya dan tekan tombol *Get Number* untuk menjadi *Verified* member PayPal.
11. Untuk mendaftar menjadi *Verified member* PayPal, tekan tombol *Get Number* untuk mendapatkan empat digit kode keamanan dari PayPal yang akan dikirimkan ke dalam pernyataan bulanan kartu kredit pengguna dan akan dikenakan biaya sebesar $ 1,95 untuk keperluan ini. Jika sudah mendapatkan empat digit kode keamanan tersebut dari pernyataan bulanan

kartu kredit, login dengan *account* PayPal kemudian pada halaman *My Account* klik bagian *Active Account-Complete Expanded User Enrollment*. Setelah memasukan empat digit kode keamanan tersebut, akun PayPal akan menjadi *Verified* member dan akan ditambahkan $ 1,95 ke dalam akun PayPal pengguna.

2.1.12.6 Cara Verifikasi Akun PayPal Menggunakan Rekening Bank

Cara verifikasi akun PayPal dapat menggunakan kartu kredit, rekening bank atau *Virtual Credit Card* (VCC). Langkah-langkah untuk melakukan verifikasi akun PayPal dengan menggunakan rekening bank adalah sebagai berikut

1. Untuk melakukan verifikasi, klik *Get Verified* pada halaman *My Account*.
2. Setelah itu, klik pilihan *Link My Bank Account* kemudian isi formulir yang disediakan. Pastikan nama yang diisikan pada formulir sama dengan nama di rekening bank. Isi nama bank penerima dan kode bank penerima.
3. Kemudian klik *Add Bank Account* setelah data yang dimasukan benar dan lengkap.
4. Setelah itu, akan muncul konfirmasi dari PayPal bahwa pengguna telah melakukan verifikasi akun PayPal dengan menggunakan rekening bank.
5. Tunggu dua sampai tiga hari. PayPal akan mengirimkan deposit ke rekening pengguna. Kemudian masukan dua buah deposit tersebut untuk memverifikasi akun PayPal. Setelah itu, akun PayPal sudah terverifikasi secara gratis dan bisa menggunakannya untuk proses transaksi *online*.

2.1.13 *Secure Socket Layer* (SSL)

SSL adalah protokol *client-server*, yang dalam hal ini *web browser* adalah *client* dan *website* adalah *server*. *Client* yang memulai komunikasi, sedangkan *server* memberi respon terhadap permintaan *client*. SSL pertama kali dikembangkan oleh Netscape *communications* pada tahun 1994. *SSL* beroperasi antara protokol komunikasi *TCP/IP* (*Transmission Control Protocol*/*Internet Protocol*) (Tabel II-1).

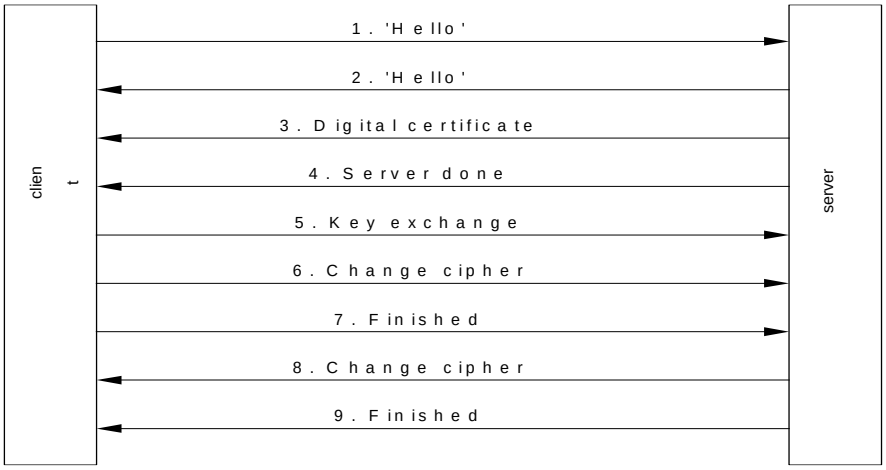
Kebanyakan transmisi pesan di *Internet* dikirim sebagai kumpulan potongan pesan yang disebut **paket**. IP bertanggung jawab untuk merutekan paket (lintasan yang dilalui oleh paket). Pada sisi penerima, TCP memastikan bahwa suatu paket sudah sampai, menyusunnya sesuai nomor urut, dan menentukan apakah paket tiba tanpa mengalami perubahan.Jika paket mengalami perubahan atau ada data yang hilang, TCP/IP meminta pengiriman ulang. TCP/IP tidak memiliki pengamanan komunikasi yang bagus. *TCP/IP* tidak dapat mengetahui jika pesan diubah oleh pihak ketiga (*man-in-the-middle attack*).

Tabel II-1 Tingkatan SSL (*Secure Socket Layer*)

Application (*HTTP*, *FTP*, *Telnet*)
Security (*SSL*)
Transport (*TCP*)
Network (*IP*)
Data link (*PPP*)
Phyiscal (*modem*, *ADSL*, *cable* TV)

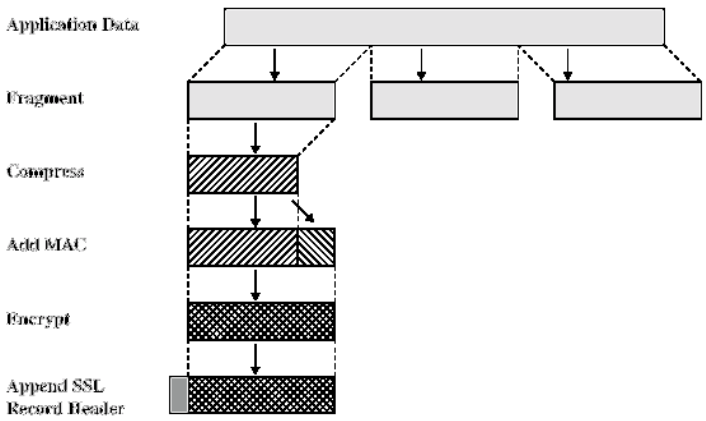
SSL Memiliki dua buah sub protokol yang berjalan saat SSL dijalankan pada *web browser*, yaitu

1. *SSL handshaking*, yaitu sub-protokol untuk membangun koneksi (kanal) yang aman untuk berkomunikasi (Gambar II-6). Sampai di sini, proses pembentukan kanal yang aman sudah selesai. Bila sub-protokol ini sudah terbentuk, maka *http://* pada *URL* berubah menjadi *https://* (*http secure*).



Gambar II-6 SSL *Handshaking*

2. *SSL record*, yaitu sub-protokol yang menggunakan kanal yang sudah aman. *SSL Record* membungkus seluruh data yang dikirim selama koneksi (Gambar II-7).



Gambar II-7 Protokol SSL *Record*

Di tempat penerima, sub-protokol *SSL Record* melakukan proses berkebalikan: mendekripsi data yang diterima, mengotentikasinya (dengan *MAC*), mendekompresinya, lalu merakitnya. Protokol SSL membuat komunikasi menjadi lebih lambat. Piranti keras, seperti kartu *peripheral component interconnect* (*PCI*) dapat dipasang ke dalam *web server* untuk memproses transaksi *SSL* lebih cepat sehingga mengurangi waktu pemrosesan.

2.1.14 MD5

Dalam kriptografi, MD5 (Message-Digest algortihm 5) adalah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan dan MD5 juga umum digunakan untuk melakukan pengujian integritas sebuah file.

MD5 di desain oleh Ronald Rivest pada tahun 1991 untuk menggantikan hash function sebelumnya, MD4. Pada tahun 1996, sebuah kecacatan ditemukan dalam desainnya, walau bukan kelemahan fatal, pengguna kriptografi mulai menganjurkan menggunakan algoritma lain, seperti SHA-1 (klaim terbaru menyatakan bahwa SHA-1 juga cacat). Pada tahun 2004, kecacatan-kecacatan yang lebih serius ditemukan menyebabkan penggunaan algoritma tersebut dalam tujuan untuk keamanan jadi makin dipertanyakan.

Hash-hash MD5 sepanjang 128-bit (16-byte), yang dikenal juga sebagai ringkasan pesan, secara tipikal ditampilkan dalam bilangan heksadesimal 32-digit. Berikut ini merupakan contoh pesan ASCII sebagai masukan dan hash MD5 yang dihasilkan :

MD5("The quick brown fox jumps over the lazy dog") = 9e107d9d372bb6826bd81d3542a419d6

Bahkan perubahan yang kecil pada pesan akan menghasilkan hash yang benar-benar berbeda, misalnya pada kata "dog", huruf d diganti menjadi c:

MD5("The quick brown fox jumps over the lazy cog") = 1055d3e698d289f2af8663725127bd4b

Hash dari panjang-nol ialah:

MD5("") = d41d8cd98f00b204e9800998ecf8427e

Dapat disimpulkan bahwa berapapun panjang kata atau kalimat yang dienkripsi melalui MD5, hasilnya akan mengeluarkan serangkaian huruf dan angka hasil enkripsi dengan panjang 32 karakter.